

Contents

[Linux VMs Documentation](#)

[Overview](#)

[About Virtual Machines](#)

[Quickstarts](#)

[Create VM - Azure CLI](#)

[Create VM - Portal](#)

[Create VM - Azure PowerShell](#)

[Tutorials](#)

[1 - Create / manage VMs](#)

[2 - Create / manage disks](#)

[3 - Automate configuration](#)

[4 - Create VM images](#)

[5 - Highly available VMs](#)

[6 - Create a scale set](#)

[7 - Load balance VMs](#)

[8 - Manage networking](#)

[9 - Backup virtual machines](#)

[10 - Manage VMs](#)

[11 - Track and update VMs](#)

[12 - Monitor VMs](#)

[13 - Manage VM security](#)

[14a - Build with Jenkins](#)

[14b - Integrate Jenkins with Azure DevOps](#)

[15a - DevOps for IaaS and PaaS on Azure](#)

[15b - CI/CD with Azure Pipelines\(YAML\)](#)

[16a - Create LAMP stack](#)

[16b - Create LEMP stack](#)

[16c - Create MEAN stack](#)

[17 - Secure web server with SSL](#)

Samples

[Azure CLI](#)

[Azure PowerShell](#)

Concepts

[Azure Resource Manager](#)

[Regions](#)

[Availability and performance](#)

[Availability](#)

[Co-location](#)

[Network performance](#)

[VM types and sizes](#)

[VM sizes](#)

[Generation 2 VMs](#)

[General purpose](#)

[Overview](#)

[Av2-series](#)

[B-series burstable](#)

[DCv2-series](#)

[Dv2 and DSv2-series](#)

[Dv3 and Dsv3-series](#)

[Dav4 and Dasv4-series](#)

[Compute optimized](#)

[Overview](#)

[Fsv2-series](#)

[Memory optimized](#)

[Overview](#)

[Dv2 and DSv2-series 11-15](#)

[Ev3 and Esv3-series](#)

[Eav4 and Easv4-series](#)

[M-series](#)

[Mv2-series](#)

[Constrained vCPUs](#)

- Storage optimized
 - Overview
 - Lsv2-series
- Optimize performance
- Accelerated compute
 - GPU optimized
 - Overview
 - NC-series
 - NCv2-series
 - NCv3-series
 - ND-series
 - NDv2-series
 - NV-series
 - NVv3-series
 - Setup GPU drivers
- High performance compute
 - Overview
 - H-series
 - HB-series
 - HBv2-series
 - HC-series
- Reserved instances
 - Prepay for VMs
 - What are Azure reservations?
 - VM instance size flexibility
- Spot VMs
- Previous generations
- Isolated sizes
- Azure compute units (ACU)
- vCPU quotas
- Reserved instances
 - Prepay for VMs

- [What are Azure reservations?](#)
- [VM instance size flexibility](#)
- [Benchmark scores](#)
- [Endorsed distros](#)
- [Dedicated hosts](#)
- [Maintenance and updates](#)
- [Disk storage](#)
 - [Introduction to managed disks](#)
 - [Select a disk type for IaaS VMs](#)
 - [Encryption](#)
 - [Disk Storage reservations](#)
 - [Designing for high performance](#)
 - [Disk bursting](#)
 - [Scalability targets for disks](#)
 - [Backup and disaster recovery for disks](#)
 - [Shared disks](#)
 - [Ephemeral OS disks](#)
- [Networking](#)
- [Scale sets](#)
- [Infrastructure automation](#)
- [Security](#)
 - [Security and policy](#)
 - [Azure Disk Encryption](#)
 - [Built-in security controls](#)
- [States and lifecycle](#)
- [Monitoring](#)
- [Backup and recovery](#)
- [Infrastructure guidelines](#)
- [How-to guides](#)
 - [Create VMs](#)
 - [Use the CLI](#)
 - [Use a template](#)

[Use REST API](#)

[Copy or clone a VM](#)

[Use dedicated hosts](#)

[CLI](#)

[Portal](#)

[Deploy spot VMs](#)

[CLI](#)

[Portal](#)

[Template](#)

[Error codes](#)

[Migrate from Classic to Azure Resource Manager](#)

[Retirement starting March 1, 2023](#)

[Overview](#)

[Deep dive on migration](#)

[Plan for migration](#)

[Migrate using the CLI](#)

[Common migration errors](#)

[Community tools for migration](#)

[FAQ](#)

[Secure VMs](#)

[Recommendations](#)

[Just-in-time access](#)

[Encrypt](#)

[Disk encryption scenarios for Linux](#)

[VM encryption with Azure CLI](#)

[VM encryption with Azure PowerShell](#)

[VM encryption with Azure portal](#)

[Key vault for Azure Disk Encryption](#)

[Disk encryption sample scripts](#)

[Disk encryption troubleshooting](#)

[Disk encryption FAQ](#)

[Disk encryption - previous version \(AAD\)](#)

Overview

Key vault for Azure Disk Encryption

Disk encryption scenarios for Linux

Use access controls

Use policies

Create a Key Vault

Create and use SSH keys

On Linux or macOS

On Windows

Detailed steps

Protect VMs

Disaster recovery

Back up VMs

Back up a single VM

Back up multiple VMs

Restore a disk

Restore individual files

Set up disaster recovery for VMs

Enable disaster recovery for a VM

Run a disaster recovery drill for a VM

Fail over a VM to another region

Manage VMs

VM usage

Common CLI tasks

Change VM size

Swap the OS disk

Time sync

Tag a VM

Run scripts on a VM

Custom Script Extension

Run Command

Use Remote Desktop

[Join VM to Azure Active Directory](#)

[Red Hat Enterprise Linux](#)

[CentOS](#)

[Ubuntu](#)

[Sign in with Azure Active Directory credentials](#)

[Updates and patches](#)

[Red Hat Update Infrastructure](#)

[Azure VM agent](#)

[Overview](#)

[Agent update](#)

[Mitigating speculative execution](#)

[Monitor metadata](#)

[Get usage metrics with REST](#)

[Platform maintenance](#)

[Maintenance notifications](#)

[Overview](#)

[CLI](#)

[Portal](#)

[PowerShell](#)

[Maintenance control](#)

[CLI](#)

[PowerShell](#)

[Scheduled events](#)

[Monitor VMs](#)

[Azure Monitor for VMs](#)

[Create metric alerts](#)

[Create log alerts](#)

[Use Images](#)

[Shared image galleries](#)

[Overview](#)

[CLI](#)

[Portal](#)

- [App registration for sharing](#)
- [Troubleshoot shared images](#)
- [Image builder \(preview\)](#)
 - [Overview](#)
 - [Use Azure CLI](#)
 - [Template reference](#)
 - [Build for image galleries](#)
 - [Update an existing image](#)
 - [Troubleshoot](#)
- [Find and use images](#)
- [Create custom image](#)
 - [Generic steps](#)
 - [Ubuntu](#)
 - [CentOS](#)
 - [Red Hat](#)
 - [Debian](#)
 - [SUSE](#)
 - [Oracle Linux](#)
 - [OpenBSD](#)
 - [FreeBSD](#)
- [Capture VM to image](#)
- [Build image with Packer](#)
- [RHEL images in Azure](#)
- [Download existing disk](#)
- [Availability and scale](#)
 - [Autoscale](#)
 - [High availability](#)
 - [Change availability set](#)
 - [Create a proximity placement group](#)
 - [CLI](#)
 - [Portal](#)
 - [Create VM in availability zone](#)

Use automation tools

Ansible

- Install and configure

- Create a Linux VM

- Manage a Linux VM

Terraform

- Install and configure

- Create a complete VM

Cloud-init

- Cloud-init overview

- Configure VM hostname

- Update packages in a VM

- Add a user on a VM

- Configure swapfile

- Run existing bash script

- Prepare existing VM for cloud-init

Jenkins

- Create a Jenkins server

- Scale with VM agents

- Publish artifacts to Storage

- Secure Jenkins

Run containers

Create Docker host

Use Docker Machine

Use Docker Compose

Run applications

Cloud Foundry

- Overview

- Deploy your first app

Cassandra

OpenShift

- OpenShift overview

- [OpenShift Container Platform 4.x](#)
- [OpenShift Container Platform 3.11 prerequisites](#)
- [OpenShift Container Platform 3.11](#)
- [OpenShift Container Platform 3.11 Marketplace Self-Managed](#)
- [Azure Stack](#)
- [OpenShift Container Platform 3.11 post-deployment tasks](#)
- [Troubleshooting OpenShift Container Platform 3.11 deployments](#)
- [SAP on Azure](#)
- [Oracle](#)
- [Elasticsearch](#)
- [FreeBSD Packet Filter](#)
- [Databases](#)
 - [MySQL on SUSE](#)
 - [MongoDB](#)
 - [PostgreSQL](#)
 - [MS SQL on Linux](#)
- [High Performance Computing \(HPC\)](#)
- [IBM Db2 pureScale](#)
 - [Architecture](#)
 - [Deployment](#)
- [Manage storage](#)
 - [Add a disk](#)
 - [Azure CLI](#)
 - [Azure portal](#)
 - [Detach a disk](#)
 - [Deploy disks with template](#)
 - [Enable shared disks](#)
 - [Upload a vhd to a disk - CLI](#)
 - [Resize a disk](#)
 - [Use Storage Explorer to manage disks](#)
 - [Snapshot a disk](#)
 - [Reserve Disk Storage](#)

- [Create an incremental snapshot](#)
- [Back up unmanaged disks](#)
- [Migration and conversion](#)
 - [Migrate to Premium storage with Azure Site Recovery](#)
 - [Convert to Managed Disks](#)
 - [Convert disk between Standard and Premium](#)
- [Copy files to a VM](#)
- [Performance](#)
 - [Using write accelerator](#)
 - [Using ultra disks](#)
 - [Benchmark a disk](#)
 - [Optimizing performance](#)
 - [Configure software RAID](#)
 - [Configure LVM](#)
- [Find unattached disks](#)
- [Use File storage](#)
- [Disks FAQs](#)
- [Manage networking](#)
 - [Create virtual network](#)
 - [Open ports to a VM](#)
 - [Assign public IP address](#)
 - [Use multiple NICs](#)
 - [Use accelerated networking](#)
 - [Assign public DNS name](#)
 - [Find and delete unattached NICs](#)
 - [DNS resolution](#)
 - [Use internal DNS](#)
- [Configure managed identities](#)
 - [Portal](#)
 - [CLI](#)
 - [PowerShell](#)
 - [Azure Resource Manager Template](#)

[REST](#)

[Azure SDKs](#)

[Use VM extensions](#)

[Move and migrate VMs](#)

[Change subscription or resource group](#)

[Move VMs to another region](#)

[Move to an availability zone](#)

[Migrate AWS and on-premises VMs](#)

[Migrate from Amazon Web Services \(AWS\) to Azure](#)

[Upload on-prem VM](#)

[Use Azure Site Recovery](#)

[Reference](#)

[Azure CLI](#)

[PowerShell](#)

[.NET](#)

[Java](#)

[Node.js](#)

[Python](#)

[REST](#)

[Resource Manager template](#)

[Resources](#)

[Author templates](#)

[Build your skills with Microsoft Learn](#)

[Azure Roadmap](#)

[Azure Quickstart templates](#)

[Pricing](#)

[Regional availability](#)

[Stack Overflow](#)

[Videos](#)

[FAQ](#)

[Troubleshoot](#)

Linux virtual machines in Azure

1/10/2020 • 6 minutes to read • [Edit Online](#)

Azure Virtual Machines (VM) is one of several types of [on-demand, scalable computing resources](#) that Azure offers. Typically, you choose a VM when you need more control over the computing environment than the other choices offer. This article gives you information about what you should consider before you create a VM, how you create it, and how you manage it.

An Azure VM gives you the flexibility of virtualization without having to buy and maintain the physical hardware that runs it. However, you still need to maintain the VM by performing tasks, such as configuring, patching, and installing the software that runs on it.

Azure virtual machines can be used in various ways. Some examples are:

- **Development and test** – Azure VMs offer a quick and easy way to create a computer with specific configurations required to code and test an application.
- **Applications in the cloud** – Because demand for your application can fluctuate, it might make economic sense to run it on a VM in Azure. You pay for extra VMs when you need them and shut them down when you don't.
- **Extended datacenter** – Virtual machines in an Azure virtual network can easily be connected to your organization's network.

The number of VMs that your application uses can scale up and out to whatever is required to meet your needs.

What do I need to think about before creating a VM?

There are always a multitude of [design considerations](#) when you build out an application infrastructure in Azure. These aspects of a VM are important to think about before you start:

- The names of your application resources
- The location where the resources are stored
- The size of the VM
- The maximum number of VMs that can be created
- The operating system that the VM runs
- The configuration of the VM after it starts
- The related resources that the VM needs

Locations

All resources created in Azure are distributed across multiple [geographical regions](#) around the world. Usually, the region is called **location** when you create a VM. For a VM, the location specifies where the virtual hard disks are stored.

This table shows some of the ways you can get a list of available locations.

METHOD	DESCRIPTION
Azure portal	Select a location from the list when you create a VM.
Azure PowerShell	Use the Get-AzLocation command.
REST API	Use the List locations operation.

METHOD	DESCRIPTION
Azure CLI	Use the az account list-locations operation.

Availability

Azure announced an industry leading single instance virtual machine Service Level Agreement of 99.9% provided you deploy the VM with premium storage for all disks. In order for your deployment to qualify for the standard 99.95% VM Service Level Agreement, you still need to deploy two or more VMs running your workload inside of an availability set. An availability set ensures that your VMs are distributed across multiple fault domains in the Azure data centers as well as deployed onto hosts with different maintenance windows. The full [Azure SLA](#) explains the guaranteed availability of Azure as a whole.

VM size

The [size](#) of the VM that you use is determined by 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. For partial hours, Azure charges only for the minutes used. Storage is priced and charged separately.

VM Limits

Your subscription has default [quota limits](#) in place that could impact the deployment of many VMs for your project. The current limit on a per subscription basis is 20 VMs per region. Limits can be raised by [filing a support ticket requesting an increase](#)

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. As you add disks or scale the VM up and down, you don't have to worry about the storage being used. If you're creating new VMs, [use the Azure CLI](#) or the Azure portal to create VMs with Managed OS and data disks. If you have VMs with unmanaged disks, you can [convert your VMs to be backed with Managed Disks](#).

You can also manage your custom images in one storage account per Azure region, and use them to create hundreds of VMs in the same subscription. For more information about Managed Disks, see the [Managed Disks Overview](#).

Distributions

Microsoft Azure supports running a number of popular Linux distributions provided and maintained by a number of partners. You can find distributions such as Red Hat Enterprise, CentOS, SUSE Linux Enterprise, Debian, Ubuntu, CoreOS, RancherOS, FreeBSD, and more in the Azure Marketplace. Microsoft actively works with various Linux communities to add even more flavors to the [Azure endorsed Linux Distros](#) list.

If your preferred Linux distro of choice is not currently present in the gallery, you can "Bring your own Linux" VM by [creating and uploading a Linux VHD in Azure](#).

Microsoft works closely with partners to ensure the images available are updated and optimized for an Azure runtime. For more information on Azure partners, see the following links:

- Linux on Azure - [Endorsed Distributions](#)
- SUSE - [Azure Marketplace](#) - SUSE Linux Enterprise Server
- Red Hat - [Azure Marketplace](#) - Red Hat Enterprise Linux 7.2
- Canonical - [Azure Marketplace](#) - Ubuntu Server 16.04 LTS
- Debian - [Azure Marketplace](#) - Debian 8 "Jessie"
- FreeBSD - [Azure Marketplace](#) - FreeBSD 10.4
- CoreOS - [Azure Marketplace](#) - CoreOS (Stable)
- RancherOS - [Azure Marketplace](#) - RancherOS
- Bitnami - [Bitnami Library for Azure](#)
- Mesosphere - [Azure Marketplace](#) - Mesosphere DC/OS on Azure
- Docker - [Azure Marketplace](#) - Azure Container Service with Docker Swarm
- Jenkins - [Azure Marketplace](#) - CloudBees Jenkins Platform

VM Sizes

The [size](#) of the VM that you use is determined by 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. For partial hours, Azure charges only for the minutes used. Storage is priced and charged separately.

Cloud-init

To achieve a proper DevOps culture, all infrastructure must be code. When all the infrastructure lives in code it can easily be recreated. Azure works with all the major automation tooling like Ansible, Chef, SaltStack, and Puppet. Azure also has its own tooling for automation:

- [Azure Templates](#)
- [Azure VMAccess](#)

Azure supports for [cloud-init](#) across most Linux Distros that support it. We are actively working with our endorsed Linux distro partners in order to have cloud-init enabled images available in the Azure marketplace. These images will make your cloud-init deployments and configurations work seamlessly with VMs and virtual machine scale sets.

- [Using cloud-init on Azure Linux VMs](#)

Quotas

Each Azure Subscription has default quota limits in place that could impact the deployment of a large number of VMs for your project. The current limit on a per subscription basis is 20 VMs per region. Quota limits can be raised quickly and easily by filing a support ticket requesting a limit increase. For more details on quota limits:

- [Azure Subscription Service Limits](#)

Storage

- [Introduction to Microsoft Azure Storage](#)
- [Add a disk to a Linux VM using the azure-cli](#)
- [How to attach a data disk to a Linux VM in the Azure portal](#)

Networking

- [Virtual Network Overview](#)
- [IP addresses in Azure](#)
- [Opening ports to a Linux VM in Azure](#)
- [Create a Fully Qualified Domain Name in the Azure portal](#)

Next steps

Create your first VM!

- [Portal](#)
- [Azure CLI](#)
- [PowerShell](#)

Quickstart: Create a Linux virtual machine with the Azure CLI

10/16/2019 • 3 minutes to read • [Edit Online](#)

This quickstart shows you how to use the Azure command-line interface (CLI) to deploy a Linux virtual machine (VM) in Azure. The Azure CLI is used to create and manage Azure resources from the command line or in scripts.

In this tutorial, we will be installing Ubuntu 16.04 LTS. To show the VM in action, you'll connect to it using SSH and install the NGINX web server.

If you don't have an Azure subscription, create a [free account](#) before you begin.

Launch Azure Cloud Shell

The Azure Cloud Shell is a free interactive shell that you can use to run the steps in this article. It has common Azure tools preinstalled and configured to use with your account.

To open the Cloud Shell, just select **Try it** from the upper right corner of a code block. You can also open Cloud Shell in a separate browser tab by going to <https://shell.azure.com/bash>. Select **Copy** to copy the blocks of code, paste it into the Cloud Shell, and select **Enter** to run it.

If you prefer to install and use the CLI locally, this quickstart requires Azure CLI version 2.0.30 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Create a resource group

Create a resource group with the [az group create](#) command. An Azure resource group is a logical container into which Azure resources are deployed and managed. The following example creates a resource group named *myResourceGroup* in the *eastus* location:

```
az group create --name myResourceGroup --location eastus
```

Create virtual machine

Create a VM with the [az vm create](#) command.

The following example creates a VM named *myVM* and adds a user account named *azureuser*. The `--generate-ssh-keys` parameter is used to automatically generate an SSH key, and put it in the default key location (`~/.ssh`). To use a specific set of keys instead, use the `--ssh-key-value` option.

```
az vm create \
--resource-group myResourceGroup \
--name myVM \
--image UbuntuLTS \
--admin-username azureuser \
--generate-ssh-keys
```

It takes a few minutes to create the VM and supporting resources. The following example output shows the VM create operation was successful.

```
{  
    "fqdns": "",  
    "id":  
        "/subscriptions/<guid>/resourceGroups/myResourceGroup/providers/Microsoft.Compute/virtualMachines/myVM",  
    "location": "eastus",  
    "macAddress": "00-0D-3A-23-9A-49",  
    "powerState": "VM running",  
    "privateIpAddress": "10.0.0.4",  
    "publicIpAddress": "40.68.254.142",  
    "resourceGroup": "myResourceGroup"  
}
```

Note your own `publicIpAddress` in the output from your VM. This address is used to access the VM in the next steps.

Open port 80 for web traffic

By default, only SSH connections are opened when you create a Linux VM in Azure. Use [az vm open-port](#) to open TCP port 80 for use with the NGINX web server:

```
az vm open-port --port 80 --resource-group myResourceGroup --name myVM
```

Connect to virtual machine

SSH to your VM as normal. Replace **publicIpAddress** with the public IP address of your VM as noted in the previous output from your VM:

```
ssh azureuser@publicIpAddress
```

Install web server

To see your VM in action, install the NGINX web server. Update your package sources and then install the latest NGINX package.

```
sudo apt-get -y update  
sudo apt-get -y install nginx
```

When done, type `exit` to leave the SSH session.

View the web server in action

Use a web browser of your choice to view the default NGINX welcome page. Use the public IP address of your VM as the web address. The following example shows the default NGINX web site:



Clean up resources

When no longer needed, you can use the `az group delete` command to remove the resource group, VM, and all related resources.

```
az group delete --name myResourceGroup
```

Next steps

In this quickstart, you deployed a simple virtual machine, open a network port for web traffic, and installed a basic web server. To learn more about Azure virtual machines, continue to the tutorial for Linux VMs.

[Azure Linux virtual machine tutorials](#)

Quickstart: Create a Linux virtual machine in the Azure portal

11/13/2019 • 4 minutes to read • [Edit Online](#)

Azure virtual machines (VMs) can be created through the Azure portal. The Azure portal is a browser-based user interface to create Azure resources. This quickstart shows you how to use the Azure portal to deploy a Linux virtual machine (VM) running Ubuntu 18.04 LTS. To see your VM in action, you also SSH to the VM and install the NGINX web server.

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create SSH key pair

You need an SSH key pair to complete this quickstart. If you already have an SSH key pair, you can skip this step.

Open a bash shell and use [ssh-keygen](#) to create an SSH key pair. If you don't have a bash shell on your local computer, you can use the [Azure Cloud Shell](#).

1. Sign in to the [Azure portal](#).
2. In the menu at the top of the page, select the  icon to open Cloud Shell.
3. Make sure the CloudShell says **Bash** in the upper left. If it says PowerShell, use the drop-down to select **Bash** and select **Confirm** to change to the Bash shell.
4. Type `ssh-keygen -t rsa -b 2048` to create the ssh key.
5. You will be prompted to enter a file in which to save the key pair. Just press **Enter** to save in the default location, listed in brackets.
6. You will be asked to enter a passphrase. You can type a passphrase for your SSH key or press **Enter** to continue without a passphrase.
7. The `ssh-keygen` command generates public and private keys with the default name of `id_rsa` in the `~/.ssh` directory. The command returns the full path to the public key. Use the path to the public key to display its contents with `cat` by typing `cat ~/.ssh/id_rsa.pub`.
8. Copy the output of this command and save it somewhere to use later in this article. This is your public key and you will need it when configuring your administrator account to log in to your VM.

Sign in to Azure

Sign in to the [Azure portal](#) if you haven't already.

Create virtual machine

1. Type **virtual machines** in the search.
2. Under **Services**, select **Virtual machines**.
3. In the **Virtual machines** page, select **Add**. The **Create a virtual machine** page opens.
4. In the **Basics** tab, under **Project details**, make sure the correct subscription is selected and then choose to **Create new** resource group. Type *myResourceGroup* for the name.*.

Project details

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

Subscription *	<input type="text" value="Pay-As-You-Go"/>
Resource group *	<input type="text" value="(New) myResourceGroup"/> Create new

5. Under **Instance details**, type *myVM* for the **Virtual machine name**, choose *East US* for your **Region**, and choose *Ubuntu 18.04 LTS* for your **Image**. Leave the other defaults.

Instance details

Virtual machine name *	<input type="text" value="myVM"/>
Region *	<input type="text" value="(US) East US"/>
Availability options	<input type="text" value="No infrastructure redundancy required"/>
Image *	<input type="text" value="Ubuntu Server 18.04 LTS"/> Browse all public and private images
Size *	Standard D2s v3 2 vcpus, 8 GiB memory Change size

6. Under **Administrator account**, select **SSH public key**, type your user name, then paste in your public key. Remove any leading or trailing white space in your public key.

Administrator account

Authentication type	<input type="radio"/> Password <input checked="" type="radio"/> SSH public key
Username *	<input type="text" value="azureuser"/>
SSH public key *	<input type="text"/> Learn more about creating and using SSH keys in Azure

7. Under **Inbound port rules > Public inbound ports**, choose **Allow selected ports** and then select **SSH (22)** and **HTTP (80)** from the drop-down.

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports *	<input type="radio"/> None <input checked="" type="radio"/> Allow selected ports
Select inbound ports *	<input type="text" value="HTTP (80), SSH (22)"/>

⚠️ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

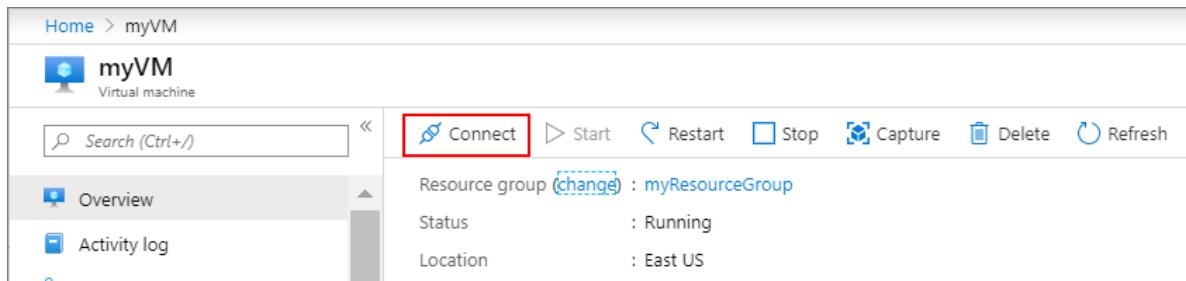
8. Leave the remaining defaults and then select the **Review + create** button at the bottom of the page.
9. On the **Create a virtual machine** page, you can see the details about the VM you are about to create. When you are ready, select **Create**.

It will take a few minutes for your VM to be deployed. When the deployment is finished, move on to the next section.

Connect to virtual machine

Create an SSH connection with the VM.

1. Select the **Connect** button on the overview page for your VM.



2. In the **Connect to virtual machine** page, keep the default options to connect by IP address over port 22.

In **Login using VM local account** a connection command is shown. Select the button to copy the command. The following example shows what the SSH connection command looks like:

```
ssh azureuser@10.111.12.123
```

3. Using the same bash shell you used to create your SSH key pair (you can reopen the Cloud Shell by selecting `>` again or going to <https://shell.azure.com/bash>), paste the SSH connection command into the shell to create an SSH session.

Install web server

To see your VM in action, install the NGINX web server. From your SSH session, update your package sources and then install the latest NGINX package.

```
sudo apt-get -y update  
sudo apt-get -y install nginx
```

When done, type `exit` to leave the SSH session.

View the web server in action

Use a web browser of your choice to view the default NGINX welcome page. Type the public IP address of the VM as the web address. The public IP address can be found on the VM overview page or as part of the SSH connection string you used earlier.



Clean up resources

When no longer needed, you can delete the resource group, virtual machine, and all related resources. To do so, select the resource group for the virtual machine, select **Delete**, then confirm the name of the resource group to delete.

Next steps

In this quickstart, you deployed a simple virtual machine, created a Network Security Group and rule, and installed a basic web server. To learn more about Azure virtual machines, continue to the tutorial for Linux VMs.

[Azure Linux virtual machine tutorials](#)

Quickstart: Create a Linux virtual machine in Azure with PowerShell

11/13/2019 • 5 minutes to read • [Edit Online](#)

The Azure PowerShell module is used to create and manage Azure resources from the PowerShell command line or in scripts. This quickstart shows you how to use the Azure PowerShell module to deploy a Linux virtual machine (VM) in Azure. This quickstart uses the Ubuntu 16.04 LTS marketplace image from Canonical. To see your VM in action, you'll also SSH to the VM and install the NGINX web server.

If you don't have an Azure subscription, create a [free account](#) before you begin.

Launch Azure Cloud Shell

The Azure Cloud Shell is a free interactive shell that you can use to run the steps in this article. It has common Azure tools preinstalled and configured to use with your account.

To open the Cloud Shell, just select **Try it** from the upper right corner of a code block. Select **Copy** to copy the blocks of code, paste it into the Cloud Shell, and press enter to run it.

Create SSH key pair

You need an SSH key pair to complete this quickstart. If you already have an SSH key pair, you can skip this step.

Open a bash shell and use [ssh-keygen](#) to create an SSH key pair. If you don't have a bash shell on your local computer, you can use the [Azure Cloud Shell](#).

```
ssh-keygen -t rsa -b 2048
```

For more detailed information on how to create SSH key pairs, including the use of PuTTY, see [How to use SSH keys with Windows](#).

If you create your SSH key pair using the Cloud Shell, it will be stored in a container image in a [storage account that is automatically created by Cloud Shell](#). Don't delete the storage account, or the files share within it, until after you have retrieved your keys or you will lose access to the VM.

Create a resource group

Create an Azure resource group with [New-AzResourceGroup](#). A resource group is a logical container into which Azure resources are deployed and managed:

```
New-AzResourceGroup -Name "myResourceGroup" -Location "EastUS"
```

Create virtual network resources

Create a virtual network, subnet, and a public IP address. These resources are used to provide network connectivity to the VM and connect it to the internet:

```

# Create a subnet configuration
$subnetConfig = New-AzVirtualNetworkSubnetConfig ` 
    -Name "mySubnet" ` 
    -AddressPrefix 192.168.1.0/24

# Create a virtual network
$vnet = New-AzVirtualNetwork ` 
    -ResourceGroupName "myResourceGroup" ` 
    -Location "EastUS" ` 
    -Name "myVNET" ` 
    -AddressPrefix 192.168.0.0/16 ` 
    -Subnet $subnetConfig

# Create a public IP address and specify a DNS name
$pip = New-AzPublicIpAddress ` 
    -ResourceGroupName "myResourceGroup" ` 
    -Location "EastUS" ` 
    -AllocationMethod Static ` 
    -IdleTimeoutInMinutes 4 ` 
    -Name "mypublicdns$(Get-Random)"

```

Create an Azure Network Security Group and traffic rule. The Network Security Group secures the VM with inbound and outbound rules. In the following example, an inbound rule is created for TCP port 22 that allows SSH connections. To allow incoming web traffic, an inbound rule for TCP port 80 is also created.

```

# Create an inbound network security group rule for port 22
$nsgRuleSSH = New-AzNetworkSecurityRuleConfig ` 
    -Name "myNetworkSecurityGroupRuleSSH" ` 
    -Protocol "Tcp" ` 
    -Direction "Inbound" ` 
    -Priority 1000 ` 
    -SourceAddressPrefix * ` 
    -SourcePortRange * ` 
    -DestinationAddressPrefix * ` 
    -DestinationPortRange 22 ` 
    -Access "Allow"

# Create an inbound network security group rule for port 80
$nsgRuleWeb = New-AzNetworkSecurityRuleConfig ` 
    -Name "myNetworkSecurityGroupRuleWWW" ` 
    -Protocol "Tcp" ` 
    -Direction "Inbound" ` 
    -Priority 1001 ` 
    -SourceAddressPrefix * ` 
    -SourcePortRange * ` 
    -DestinationAddressPrefix * ` 
    -DestinationPortRange 80 ` 
    -Access "Allow"

# Create a network security group
$nsg = New-AzNetworkSecurityGroup ` 
    -ResourceGroupName "myResourceGroup" ` 
    -Location "EastUS" ` 
    -Name "myNetworkSecurityGroup" ` 
    -SecurityRules $nsgRuleSSH,$nsgRuleWeb

```

Create a virtual network interface card (NIC) with [New-AzNetworkInterface](#). The virtual NIC connects the VM to a subnet, Network Security Group, and public IP address.

```
# Create a virtual network card and associate with public IP address and NSG
$nic = New-AzNetworkInterface ` 
    -Name "myNic" ` 
    -ResourceGroupName "myResourceGroup" ` 
    -Location "EastUS" ` 
    -SubnetId $vnet.Subnets[0].Id ` 
    -PublicIpAddressId $pip.Id ` 
    -NetworkSecurityGroupId $nsg.Id
```

Create a virtual machine

To create a VM in PowerShell, you create a configuration that has settings like the image to use, size, and authentication options. Then the configuration is used to build the VM.

Define the SSH credentials, OS information, and VM size. In this example, the SSH key is stored in

`~/.ssh/id_rsa.pub`.

```
# Define a credential object
$securePassword = ConvertTo-SecureString ' ' -AsPlainText -Force
$cred = New-Object System.Management.Automation.PSCredential ("azureuser", $securePassword)

# Create a virtual machine configuration
$vmConfig = New-AzVMConfig ` 
    -VMName "myVM" ` 
    -VMSize "Standard_D1" | ` 
Set-AzVMOperatingSystem ` 
    -Linux ` 
    -ComputerName "myVM" ` 
    -Credential $cred ` 
    -DisablePasswordAuthentication | ` 
Set-AzVMSourceImage ` 
    -PublisherName "Canonical" ` 
    -Offer "UbuntuServer" ` 
    -Skus "16.04-LTS" ` 
    -Version "latest" | ` 
Add-AzVMNetworkInterface ` 
    -Id $nic.Id

# Configure the SSH key
$sshPublicKey = cat ~/.ssh/id_rsa.pub
Add-AzVMSShPublicKey ` 
    -VM $vmConfig ` 
    -KeyData $sshPublicKey ` 
    -Path "/home/azureuser/.ssh/authorized_keys"
```

Now, combine the previous configuration definitions to create with [New-AzVM](#):

```
New-AzVM ` 
    -ResourceGroupName "myResourceGroup" ` 
    -Location eastus -VM $vmConfig
```

It will take a few minutes for your VM to be deployed. When the deployment is finished, move on to the next section.

Connect to the VM

Create an SSH connection with the VM using the public IP address. To see the public IP address of the VM, use the [Get-AzPublicIpAddress](#) cmdlet:

```
Get-AzPublicIpAddress -ResourceGroupName "myResourceGroup" | Select "IpAddress"
```

Using the same bash shell you used to create your SSH key pair (like the [Azure Cloud Shell](#) or your local bash shell) paste the SSH connection command into the shell to create an SSH session.

```
ssh azureuser@10.111.12.123
```

When prompted, the login user name is *azureuser*. If a passphrase is used with your SSH keys, you need to enter that when prompted.

Install NGINX

To see your VM in action, install the NGINX web server. From your SSH session, update your package sources and then install the latest NGINX package.

```
sudo apt-get -y update  
sudo apt-get -y install nginx
```

When done, type `exit` to leave the SSH session.

View the web server in action

Use a web browser of your choice to view the default NGINX welcome page. Enter the public IP address of the VM as the web address. The public IP address can be found on the VM overview page or as part of the SSH connection string you used earlier.



Clean up resources

When no longer needed, you can use the [Remove-AzResourceGroup](#) cmdlet to remove the resource group, VM, and all related resources:

```
Remove-AzResourceGroup -Name "myResourceGroup"
```

Next steps

In this quickstart, you deployed a simple virtual machine, created a Network Security Group and rule, and installed a basic web server. To learn more about Azure virtual machines, continue to the tutorial for Linux VMs.

Tutorial: Create and Manage Linux VMs with the Azure CLI

11/13/2019 • 8 minutes to read • [Edit Online](#)

Azure virtual machines provide a fully configurable and flexible computing environment. This tutorial covers basic Azure virtual machine deployment items such as selecting a VM size, selecting a VM image, and deploying a VM. You learn how to:

- Create and connect to a VM
- Select and use VM images
- View and use specific VM sizes
- Resize a VM
- View and understand VM state

This tutorial uses the CLI within the [Azure Cloud Shell](#), which is constantly updated to the latest version. To open the Cloud Shell, select **Try it** from the top of any code block.

If you choose to install and use the CLI locally, this tutorial requires that you are running the Azure CLI version 2.0.30 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Create resource group

Create a resource group with the [az group create](#) command.

An Azure resource group is a logical container into which Azure resources are deployed and managed. A resource group must be created before a virtual machine. In this example, a resource group named *myResourceGroupVM* is created in the *eastus* region.

```
az group create --name myResourceGroupVM --location eastus
```

The resource group is specified when creating or modifying a VM, which can be seen throughout this tutorial.

Create virtual machine

Create a virtual machine with the [az vm create](#) command.

When you create a virtual machine, several options are available such as operating system image, disk sizing, and administrative credentials. The following example creates a VM named *myVM* that runs Ubuntu Server. A user account named *azureuser* is created on the VM, and SSH keys are generated if they do not exist in the default key location (`~/ssh`):

```
az vm create \
  --resource-group myResourceGroupVM \
  --name myVM \
  --image UbuntuLTS \
  --admin-username azureuser \
  --generate-ssh-keys
```

It may take a few minutes to create the VM. Once the VM has been created, the Azure CLI outputs information about the VM. Take note of the `publicIpAddress`, this address can be used to access the virtual machine..

```
{  
  "fqdns": "",  
  "id": "/subscriptions/d5b9d4b7-6fc1-0000-0000-  
000000000000/resourceGroups/myResourceGroupVM/providers/Microsoft.Compute/virtualMachines/myVM",  
  "location": "eastus",  
  "macAddress": "00-0D-3A-23-9A-49",  
  "powerState": "VM running",  
  "privateIpAddress": "10.0.0.4",  
  "publicIpAddress": "52.174.34.95",  
  "resourceGroup": "myResourceGroupVM"  
}
```

Connect to VM

You can now connect to the VM with SSH in the Azure Cloud Shell or from your local computer. Replace the example IP address with the `publicIpAddress` noted in the previous step.

```
ssh azureuser@52.174.34.95
```

Once logged in to the VM, you can install and configure applications. When you are finished, you close the SSH session as normal:

```
exit
```

Understand VM images

The Azure marketplace includes many images that can be used to create VMs. In the previous steps, a virtual machine was created using an Ubuntu image. In this step, the Azure CLI is used to search the marketplace for a CentOS image, which is then used to deploy a second virtual machine.

To see a list of the most commonly used images, use the [az vm image list](#) command.

```
az vm image list --output table
```

The command output returns the most popular VM images on Azure.

Offer	Publisher	Sku	Urn
UrnAlias	Version		
WindowsServer	MicrosoftWindowsServer	2016-Datacenter	MicrosoftWindowsServer:WindowsServer:2016-Datacenter:latest
	Win2016Datacenter	latest	
WindowsServer	MicrosoftWindowsServer	2012-R2-Datacenter	MicrosoftWindowsServer:WindowsServer:2012-R2-Datacenter:latest
	Win2012R2Datacenter	latest	
WindowsServer	MicrosoftWindowsServer	2008-R2-SP1	MicrosoftWindowsServer:WindowsServer:2008-R2-SP1:latest
	Win2008R2SP1	latest	
WindowsServer	MicrosoftWindowsServer	2012-Datacenter	MicrosoftWindowsServer:WindowsServer:2012-Datacenter:latest
	Win2012Datacenter	latest	
UbuntuServer	Canonical	16.04-LTS	Canonical:UbuntuServer:16.04-LTS:latest
UbuntuLTS		latest	
CentOS	OpenLogic	7.3	OpenLogic:CentOS:7.3:latest
CentOS		latest	
openSUSE-Leap	SUSE	42.2	SUSE:openSUSE-Leap:42.2:latest
openSUSE-Leap		latest	
RHEL	RedHat	7.3	RedHat:RHEL:7.3:latest
RHEL		latest	
SLES	SUSE	12-SP2	SUSE:SLES:12-SP2:latest
SLES		latest	
Debian	creativ	8	creativ:Debian:8:latest
Debian		latest	
CoreOS	CoreOS	Stable	CoreOS:CoreOS:Stable:latest
CoreOS		latest	

A full list can be seen by adding the `--all` argument. The image list can also be filtered by `--publisher` or `--offer`. In this example, the list is filtered for all images with an offer that matches *CentOS*.

```
az vm image list --offer CentOS --all --output table
```

Partial output:

Offer	Publisher	Sku	Urn	Version
CentOS	OpenLogic	6.5	OpenLogic:CentOS:6.5:6.5.201501	6.5.201501
CentOS	OpenLogic	6.5	OpenLogic:CentOS:6.5:6.5.201503	6.5.201503
CentOS	OpenLogic	6.5	OpenLogic:CentOS:6.5:6.5.201506	6.5.201506
CentOS	OpenLogic	6.5	OpenLogic:CentOS:6.5:6.5.20150904	6.5.20150904
CentOS	OpenLogic	6.5	OpenLogic:CentOS:6.5:6.5.20160309	6.5.20160309
CentOS	OpenLogic	6.5	OpenLogic:CentOS:6.5:6.5.20170207	6.5.20170207

To deploy a VM using a specific image, take note of the value in the *Urn* column, which consists of the publisher, offer, SKU, and optionally a version number to [identify](#) the image. When specifying the image, the image version number can be replaced with "latest", which selects the latest version of the distribution. In this example, the `--image` argument is used to specify the latest version of a CentOS 6.5 image.

```
az vm create --resource-group myResourceGroupVM --name myVM2 --image OpenLogic:CentOS:6.5:latest --generate-ssh-keys
```

Understand VM sizes

A virtual machine size determines the amount of compute resources such as CPU, GPU, and memory that are made available to the virtual machine. Virtual machines need to be sized appropriately for the expected work load. If workload increases, an existing virtual machine can be resized.

VM Sizes

The following table categorizes sizes into use cases.

TYPE	COMMON SIZES	DESCRIPTION
General purpose	B, Dsv3, Dv3, DSv2, Dv2, Av2, DC	Balanced CPU-to-memory. Ideal for dev / test and small to medium applications and data solutions.
Compute optimized	Fsv2	High CPU-to-memory. Good for medium traffic applications, network appliances, and batch processes.
Memory optimized	Esv3, Ev3, M, DSv2, Dv2	High memory-to-core. Great for relational databases, medium to large caches, and in-memory analytics.
Storage optimized	Lsv2, Ls	High disk throughput and IO. Ideal for Big Data, SQL, and NoSQL databases.
GPU	NV, NVv2, NC, NCv2, NCv3, ND	Specialized VMs targeted for heavy graphic rendering and video editing.
High performance	H	Our most powerful CPU VMs with optional high-throughput network interfaces (RDMA).

Find available VM sizes

To see a list of VM sizes available in a particular region, use the [az vm list-sizes](#) command.

```
az vm list-sizes --location eastus --output table
```

Partial output:

ResourceDiskSizeInMb	MaxDataDiskCount	MemoryInMb	Name	NumberOfCores	OsDiskSizeInMb
7168	2	3584	Standard_DS1	1	1047552
14336	4	7168	Standard_DS2	2	1047552
28672	8	14336	Standard_DS3	4	1047552
57344	16	28672	Standard_DS4	8	1047552
114688	4	14336	Standard_DS11	2	1047552
28672	8	28672	Standard_DS12	4	1047552
57344	16	57344	Standard_DS13	8	1047552
114688	32	114688	Standard_DS14	16	1047552
229376	1	768	Standard_A0	1	1047552
20480	2	1792	Standard_A1	1	1047552
71680	4	3584	Standard_A2	2	1047552
138240	8	7168	Standard_A3	4	1047552
291840	4	14336	Standard_A5	2	1047552
138240	16	14336	Standard_A4	8	1047552
619520	8	28672	Standard_A6	4	1047552
291840	16	57344	Standard_A7	8	1047552
619520					

Create VM with specific size

In the previous VM creation example, a size was not provided, which results in a default size. A VM size can be selected at creation time using `az vm create` and the `--size` argument.

```
az vm create \
  --resource-group myResourceGroupVM \
  --name myVM3 \
  --image UbuntuLTS \
  --size Standard_F4s \
  --generate-ssh-keys
```

Resize a VM

After a VM has been deployed, it can be resized to increase or decrease resource allocation. You can view the current size of a VM with `az vm show`:

```
az vm show --resource-group myResourceGroupVM --name myVM --query hardwareProfile.vmSize
```

Before resizing a VM, check if the desired size is available on the current Azure cluster. The `az vm list-vm-resize-options` command returns the list of sizes.

```
az vm list-vm-resize-options --resource-group myResourceGroupVM --name myVM --query [].name
```

If the desired size is available, the VM can be resized from a powered-on state, however it is rebooted during the operation. Use the [az vm resize](#) command to perform the resize.

```
az vm resize --resource-group myResourceGroupVM --name myVM --size Standard_DS4_v2
```

If the desired size is not on the current cluster, the VM needs to be deallocated before the resize operation can occur. Use the [az vm deallocate](#) command to stop and deallocate the VM. Note, when the VM is powered back on, any data on the temp disk may be removed. The public IP address also changes unless a static IP address is being used.

```
az vm deallocate --resource-group myResourceGroupVM --name myVM
```

Once deallocated, the resize can occur.

```
az vm resize --resource-group myResourceGroupVM --name myVM --size Standard_GS1
```

After the resize, the VM can be started.

```
az vm start --resource-group myResourceGroupVM --name myVM
```

VM power states

An Azure VM can have one of many power states. This state represents the current state of the VM from the standpoint of the hypervisor.

Power states

POWER STATE	DESCRIPTION
Starting	Indicates the virtual machine is being started.
Running	Indicates that the virtual machine is running.
Stopping	Indicates that the virtual machine is being stopped.
Stopped	Indicates that the virtual machine is stopped. Virtual machines in the stopped state still incur compute charges.
Deallocating	Indicates that the virtual machine is being deallocated.
Deallocated	Indicates that the virtual machine is removed from the hypervisor but still available in the control plane. Virtual machines in the Deallocated state do not incur compute charges.
-	Indicates that the power state of the virtual machine is unknown.

Find the power state

To retrieve the state of a particular VM, use the [az vm get-instance-view](#) command. Be sure to specify a valid name for a virtual machine and resource group.

```
az vm get-instance-view \
--name myVM \
--resource-group myResourceGroupVM \
--query instanceView.statuses[1] --output table
```

Output:

Code	DisplayStatus	Level
PowerState/running	VM running	Info

Management tasks

During the life-cycle of a virtual machine, you may want to run management tasks such as starting, stopping, or deleting a virtual machine. Additionally, you may want to create scripts to automate repetitive or complex tasks. Using the Azure CLI, many common management tasks can be run from the command line or in scripts.

Get IP address

This command returns the private and public IP addresses of a virtual machine.

```
az vm list-ip-addresses --resource-group myResourceGroupVM --name myVM --output table
```

Stop virtual machine

```
az vm stop --resource-group myResourceGroupVM --name myVM
```

Start virtual machine

```
az vm start --resource-group myResourceGroupVM --name myVM
```

Delete resource group

Deleting a resource group also deletes all resources contained within, such as the VM, virtual network, and disk.

The `--no-wait` parameter returns control to the prompt without waiting for the operation to complete. The `--yes` parameter confirms that you wish to delete the resources without an additional prompt to do so.

```
az group delete --name myResourceGroupVM --no-wait --yes
```

Next steps

In this tutorial, you learned about basic VM creation and management such as how to:

- Create and connect to a VM
- Select and use VM images
- View and use specific VM sizes
- Resize a VM
- View and understand VM state

Advance to the next tutorial to learn about VM disks.

[Create and Manage VM disks](#)

Tutorial - Manage Azure disks with the Azure CLI

1/9/2020 • 8 minutes to read • [Edit Online](#)

Azure virtual machines (VMs) use disks to store the operating system, applications, and data. When you create a VM, it is important to choose a disk size and configuration appropriate to the expected workload. This tutorial shows you how to deploy and manage VM disks. You learn about:

- OS disks and temporary disks
- Data disks
- Standard and Premium disks
- Disk performance
- Attaching and preparing data disks
- Resizing disks
- Disk snapshots

Default Azure disks

When an Azure virtual machine is created, two disks are automatically attached to the virtual machine.

Operating system disk - Operating system disks can be sized up to 2 TB, and hosts the VMs operating system. The OS disk is labeled `/dev/sda` by default. The disk caching configuration of the OS disk is optimized for OS performance. Because of this configuration, the OS disk **should not** be used for applications or data. For applications and data, use data disks, which are detailed later in this tutorial.

Temporary disk - Temporary disks use a solid-state drive that is located on the same Azure host as the VM. Temp disks are highly performant and may be used for operations such as temporary data processing. However, if the VM is moved to a new host, any data stored on a temporary disk is removed. The size of the temporary disk is determined by the VM size. Temporary disks are labeled `/dev/sdb` and have a mountpoint of `/mnt`.

Azure data disks

To install applications and store data, additional data disks can be added. Data disks should be used in any situation where durable and responsive data storage is desired. The size of the virtual machine determines how many data disks can be attached to a VM.

VM disk types

Azure provides two types of disks, standard and Premium.

Standard disk

Standard Storage is backed by HDDs, and delivers cost-effective storage while still being performant. Standard disks are ideal for a cost effective dev and test workload.

Premium disk

Premium disks are backed by SSD-based high-performance, low-latency disk. Perfect for VMs running production workload. Premium Storage supports DS-series, DSv2-series, GS-series, and FS-series VMs. When you select a disk size, the value is rounded up to the next type. For example, if the disk size is less than 128 GB, the disk type is P10. If the disk size is between 129 GB and 512 GB, the size is a P20. Over, 512 GB, the size is a P30.

Premium disk performance

PRE MIU M SSD SIZE S	P1*	P2*	P3*	P4	P6	P10	P15	P20	P30	P40	P50	P60	P70	P80
Disk size in GiB	4	8	16	32	64	128	256	512	1,024	2,048	4,096	8,192	16,384	32,767
IOP S per disk	120	120	120	120	240	500	1,100	2,300	5,000	7,500	7,500	16,000	18,000	20,000
Throughput per disk	25 MiB /sec	25 MiB /sec	25 MiB /sec	25 MiB /sec	50 MiB /sec	100 MiB /sec	125 MiB /sec	150 MiB /sec	200 MiB /sec	250 MiB /sec	250 MiB /sec	500 MiB /sec	750 MiB /sec	900 MiB /sec
Max burst IOP S per disk **	3,500	3,500	3,500	3,500	3,500	3,500	3,500	3,500	3,500	3,500	3,500	3,500	3,500	3,500
Max burst throughput per disk **	170 MiB /sec	170 MiB /sec	170 MiB /sec	170 MiB /sec	170 MiB /sec	170 MiB /sec								
Max burst duration**	30 min	30 min	30 min	30 min	30 min	30 min								
Eligible for reservation	No	Yes, up to one year												

*Denotes a disk size that is currently in preview, for regional availability information see [New disk sizes: Managed and unmanaged](#).

**Denotes a feature that is currently in preview, see [Disk bursting](#) for more information.

While the above table identifies max IOPS per disk, a higher level of performance can be achieved by striping multiple data disks. For instance, a Standard_GS5 VM can achieve a maximum of 80,000 IOPS. For detailed information on max IOPS per VM, see [Linux VM sizes](#).

Launch Azure Cloud Shell

Azure Cloud Shell is a free interactive shell that you can use to run the steps in this article. It has common Azure tools preinstalled and configured to use with your account.

To open Cloud Shell, select **Try it** from the upper right corner of a code block. You can also launch Cloud Shell in a separate browser tab by going to <https://shell.azure.com/powershell>. Select **Copy** to copy the blocks of code, paste it into the Cloud Shell, and press enter to run it.

Create and attach disks

Data disks can be created and attached at VM creation time or to an existing VM.

Attach disk at VM creation

Create a resource group with the [az group create](#) command.

```
az group create --name myResourceGroupDisk --location eastus
```

Create a VM using the [az vm create](#) command. The following example creates a VM named *myVM*, adds a user account named *azureuser*, and generates SSH keys if they do not exist. The `--datadisk-sizes-gb` argument is used to specify that an additional disk should be created and attached to the virtual machine. To create and attach more than one disk, use a space-delimited list of disk size values. In the following example, a VM is created with two data disks, both 128 GB. Because the disk sizes are 128 GB, these disks are both configured as P10s, which provide maximum 500 IOPS per disk.

```
az vm create \
--resource-group myResourceGroupDisk \
--name myVM \
--image UbuntuLTS \
--size Standard_DS2_v2 \
--generate-ssh-keys \
--data-disk-sizes-gb 128 128
```

Attach disk to existing VM

To create and attach a new disk to an existing virtual machine, use the [az vm disk attach](#) command. The following example creates a premium disk, 128 gigabytes in size, and attaches it to the VM created in the last step.

```
az vm disk attach \
--resource-group myResourceGroupDisk \
--vm-name myVM \
--name myDataDisk \
--size-gb 128 \
--sku Premium_LRS \
--new
```

Prepare data disks

Once a disk has been attached to the virtual machine, the operating system needs to be configured to use the disk. The following example shows how to manually configure a disk. This process can also be automated using cloud-init, which is covered in a [later tutorial](#).

Create an SSH connection with the virtual machine. Replace the example IP address with the public IP of the virtual machine.

```
ssh 10.101.10.10
```

Partition the disk with `fdisk`.

```
(echo n; echo p; echo 1; echo ; echo ; echo w) | sudo fdisk /dev/sdc
```

Write a file system to the partition by using the `mkfs` command.

```
sudo mkfs -t ext4 /dev/sdc1
```

Mount the new disk so that it is accessible in the operating system.

```
sudo mkdir /datadrive && sudo mount /dev/sdc1 /datadrive
```

The disk can now be accessed through the `datadrive` mountpoint, which can be verified by running the `df -h` command.

```
df -h
```

The output shows the new drive mounted on `/datadrive`.

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/sda1	30G	1.4G	28G	5%	/
/dev/sdb1	6.8G	16M	6.4G	1%	/mnt
/dev/sdc1	50G	52M	47G	1%	/datadrive

To ensure that the drive is remounted after a reboot, it must be added to the `/etc/fstab` file. To do so, get the UUID of the disk with the `blkid` utility.

```
sudo -i blkid
```

The output displays the UUID of the drive, `/dev/sdc1` in this case.

```
/dev/sdc1: UUID="33333333-3b3b-3c3c-3d3d-3e3e3e3e3e" TYPE="ext4"
```

Add a line similar to the following to the `/etc/fstab` file.

```
UUID=33333333-3b3b-3c3c-3d3d-3e3e3e3e3e /datadrive ext4 defaults,nofail 1 2
```

Now that the disk has been configured, close the SSH session.

```
exit
```

Take a disk snapshot

When you take a disk snapshot, Azure creates a read only, point-in-time copy of the disk. Azure VM snapshots are useful to quickly save the state of a VM before you make configuration changes. In the event of an issue or error, VM can be restored using a snapshot. When a VM has more than one disk, a snapshot is taken of each disk independently of the others. To take application consistent backups, consider stopping the VM before you take disk snapshots. Alternatively, use the [Azure Backup service](#), which enables you to perform automated backups while the VM is running.

Create snapshot

Before you create a virtual machine disk snapshot, the ID or name of the disk is needed. Use the [az vm show](#) command to return the disk ID. In this example, the disk ID is stored in a variable so that it can be used in a later step.

```
osdiskid=$(az vm show \
    -g myResourceGroupDisk \
    -n myVM \
    --query "storageProfile.osDisk.managedDisk.id" \
    -o tsv)
```

Now that you have the ID of the virtual machine disk, the following command creates a snapshot of the disk.

```
az snapshot create \
    --resource-group myResourceGroupDisk \
    --source "$osdiskid" \
    --name osDisk-backup
```

Create disk from snapshot

This snapshot can then be converted into a disk, which can be used to recreate the virtual machine.

```
az disk create \
    --resource-group myResourceGroupDisk \
    --name mySnapshotDisk \
    --source osDisk-backup
```

Restore virtual machine from snapshot

To demonstrate virtual machine recovery, delete the existing virtual machine.

```
az vm delete \
    --resource-group myResourceGroupDisk \
    --name myVM
```

Create a new virtual machine from the snapshot disk.

```
az vm create \
    --resource-group myResourceGroupDisk \
    --name myVM \
    --attach-os-disk mySnapshotDisk \
    --os-type linux
```

Reattach data disk

All data disks need to be reattached to the virtual machine.

First find the data disk name using the [az disk list](#) command. This example places the name of the disk in a variable named *datadisk*, which is used in the next step.

```
datadisk=$(az disk list \
-g myResourceGroupDisk \
--query "[?contains(name,'myVM')].[id]" \
-o tsv)
```

Use the [az vm disk attach](#) command to attach the disk.

```
az vm disk attach \
-g myResourceGroupDisk \
--vm-name myVM \
--name $datadisk
```

Next steps

In this tutorial, you learned about VM disks topics such as:

- OS disks and temporary disks
- Data disks
- Standard and Premium disks
- Disk performance
- Attaching and preparing data disks
- Resizing disks
- Disk snapshots

Advance to the next tutorial to learn about automating VM configuration.

[Automate VM configuration](#)

Tutorial - How to use cloud-init to customize a Linux virtual machine in Azure on first boot

11/13/2019 • 8 minutes to read • [Edit Online](#)

In a previous tutorial, you learned how to SSH to a virtual machine (VM) and manually install NGINX. To create VMs in a quick and consistent manner, some form of automation is typically desired. A common approach to customize a VM on first boot is to use [cloud-init](#). In this tutorial you learn how to:

- Create a cloud-init config file
- Create a VM that uses a cloud-init file
- View a running Node.js app after the VM is created
- Use Key Vault to securely store certificates
- Automate secure deployments of NGINX with cloud-init

If you choose to install and use the CLI locally, this tutorial requires that you are running the Azure CLI version 2.0.30 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Cloud-init overview

[Cloud-init](#) is a widely used approach to customize a Linux VM as it boots for the first time. You can use cloud-init to install packages and write files, or to configure users and security. As cloud-init runs during the initial boot process, there are no additional steps or required agents to apply your configuration.

Cloud-init also works across distributions. For example, you don't use **apt-get install** or **yum install** to install a package. Instead you can define a list of packages to install. Cloud-init automatically uses the native package management tool for the distro you select.

We are working with our partners to get cloud-init included and working in the images that they provide to Azure. The following table outlines the current cloud-init availability on Azure platform images:

PUBLISHER	OFFER	SKU	VERSION	CLOUD-INIT READY
Canonical	UbuntuServer	18.04-LTS	latest	yes
Canonical	UbuntuServer	16.04-LTS	latest	yes
Canonical	UbuntuServer	14.04.5-LTS	latest	yes
CoreOS	CoreOS	Stable	latest	yes
OpenLogic 7.6	CentOS	7-Cl	latest	preview
RedHat 7.6	RHEL	7-RAW-Cl	7.6.2019072418	yes
RedHat 7.7	RHEL	7-RAW-Cl	7.7.2019081601	preview

Create cloud-init config file

To see cloud-init in action, create a VM that installs NGINX and runs a simple 'Hello World' Node.js app. The

following cloud-init configuration installs the required packages, creates a Node.js app, then initialize and starts the app.

At your bash prompt or in the Cloud Shell, create a file named *cloud-init.txt* and paste the following configuration. For example, type `sensible-editor cloud-init.txt` to create the file and see a list of available editors. Make sure that the whole cloud-init file is copied correctly, especially the first line:

```
#cloud-config
package_upgrade: true
packages:
- nginx
- nodejs
- npm
write_files:
- owner: www-data:www-data
  path: /etc/nginx/sites-available/default
  content: |
    server {
      listen 80;
      location / {
        proxy_pass http://localhost:3000;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection keep-alive;
        proxy_set_header Host $host;
        proxy_cache_bypass $http_upgrade;
      }
    }
- owner: azureuser:azureuser
  path: /home/azureuser/myapp/index.js
  content: |
    var express = require('express')
    var app = express()
    var os = require('os');
    app.get('/', function (req, res) {
      res.send('Hello World from host ' + os.hostname() + '!')
    })
    app.listen(3000, function () {
      console.log('Hello world app listening on port 3000!')
    })
runcmd:
- service nginx restart
- cd "/home/azureuser/myapp"
- npm init
- npm install express -y
- nodejs index.js
```

For more information about cloud-init configuration options, see [cloud-init config examples](#).

Create virtual machine

Before you can create a VM, create a resource group with [az group create](#). The following example creates a resource group named *myResourceGroupAutomate* in the *eastus* location:

```
az group create --name myResourceGroupAutomate --location eastus
```

Now create a VM with [az vm create](#). Use the `--custom-data` parameter to pass in your cloud-init config file. Provide the full path to the *cloud-init.txt* config if you saved the file outside of your present working directory. The following example creates a VM named *myVM*:

```
az vm create \
--resource-group myResourceGroupAutomate \
--name myAutomatedVM \
--image UbuntuLTS \
--admin-username azureuser \
--generate-ssh-keys \
--custom-data cloud-init.txt
```

It takes a few minutes for the VM to be created, the packages to install, and the app to start. There are background tasks that continue to run after the Azure CLI returns you to the prompt. It may be another couple of minutes before you can access the app. When the VM has been created, take note of the `publicIpAddress` displayed by the Azure CLI. This address is used to access the Node.js app via a web browser.

To allow web traffic to reach your VM, open port 80 from the Internet with [az vm open-port](#):

```
az vm open-port --port 80 --resource-group myResourceGroupAutomate --name myAutomatedVM
```

Test web app

Now you can open a web browser and enter `http://<publicIpAddress>` in the address bar. Provide your own public IP address from the VM create process. Your Node.js app is displayed as shown in the following example:



Inject certificates from Key Vault

This optional section shows how you can securely store certificates in Azure Key Vault and inject them during the VM deployment. Rather than using a custom image that includes the certificates baked-in, this process ensures that the most up-to-date certificates are injected to a VM on first boot. During the process, the certificate never leaves the Azure platform or is exposed in a script, command-line history, or template.

Azure Key Vault safeguards cryptographic keys and secrets, such as certificates or passwords. Key Vault helps streamline the key management process and enables you to maintain control of keys that access and encrypt your data. This scenario introduces some Key Vault concepts to create and use a certificate, though is not an exhaustive overview on how to use Key Vault.

The following steps show how you can:

- Create an Azure Key Vault
- Generate or upload a certificate to the Key Vault
- Create a secret from the certificate to inject in to a VM
- Create a VM and inject the certificate

Create an Azure Key Vault

First, create a Key Vault with [az keyvault create](#) and enable it for use when you deploy a VM. Each Key Vault requires a unique name, and should be all lower case. Replace `mykeyvault` in the following example with your own unique Key Vault name:

```
keyvault_name=mykeyvault
az keyvault create \
--resource-group myResourceGroupAutomate \
--name $keyvault_name \
--enabled-for-deployment
```

Generate certificate and store in Key Vault

For production use, you should import a valid certificate signed by trusted provider with [az keyvault certificate import](#). For this tutorial, the following example shows how you can generate a self-signed certificate with [az keyvault certificate create](#) that uses the default certificate policy:

```
az keyvault certificate create \
--vault-name $keyvault_name \
--name mycert \
--policy "$(az keyvault certificate get-default-policy --output json)"
```

Prepare certificate for use with VM

To use the certificate during the VM create process, obtain the ID of your certificate with [az keyvault secret list-versions](#). The VM needs the certificate in a certain format to inject it on boot, so convert the certificate with [az vm secret format](#). The following example assigns the output of these commands to variables for ease of use in the next steps:

```
secret=$(az keyvault secret list-versions \
--vault-name $keyvault_name \
--name mycert \
--query "[?attributes.enabled].id" --output tsv)
vm_secret=$(az vm secret format --secret "$secret" --output json)
```

Create cloud-init config to secure NGINX

When you create a VM, certificates and keys are stored in the protected `/var/lib/waagent` directory. To automate adding the certificate to the VM and configuring NGINX, you can use an updated cloud-init config from the previous example.

Create a file named `cloud-init-secured.txt` and paste the following configuration. If you use the Cloud Shell, create the cloud-init config file there and not on your local machine. For example, type

```
sensible-editor cloud-init-secured.txt
```

 to create the file and see a list of available editors. Make sure that the whole cloud-init file is copied correctly, especially the first line:

```

#cloud-config
package_upgrade: true
packages:
- nginx
- nodejs
- npm
write_files:
- owner: www-data:www-data
  path: /etc/nginx/sites-available/default
  content: |
    server {
      listen 80;
      listen 443 ssl;
      ssl_certificate /etc/nginx/ssl/mycert.cert;
      ssl_certificate_key /etc/nginx/ssl/mycert.prv;
      location / {
        proxy_pass http://localhost:3000;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection keep-alive;
        proxy_set_header Host $host;
        proxy_cache_bypass $http_upgrade;
      }
    }
- owner: azureuser:azureuser
  path: /home/azureuser/myapp/index.js
  content: |
    var express = require('express')
    var app = express()
    var os = require('os');
    app.get('/', function (req, res) {
      res.send('Hello World from host ' + os.hostname() + '!')
    })
    app.listen(3000, function () {
      console.log('Hello world app listening on port 3000!')
    })
runcmd:
- secretsname=$(find /var/lib/waagent/ -name "*.prv" | cut -c -57)
- mkdir /etc/nginx/ssl
- cp $secretsname.crt /etc/nginx/ssl/mycert.cert
- cp $secretsname.prv /etc/nginx/ssl/mycert.prv
- service nginx restart
- cd "/home/azureuser/myapp"
- npm init
- npm install express -y
- nodejs index.js

```

Create secure VM

Now create a VM with `az vm create`. The certificate data is injected from Key Vault with the `--secrets` parameter. As in the previous example, you also pass in the cloud-init config with the `--custom-data` parameter:

```

az vm create \
--resource-group myResourceGroupAutomate \
--name myVMWithCerts \
--image UbuntuLTS \
--admin-username azureuser \
--generate-ssh-keys \
--custom-data cloud-init-secured.txt \
--secrets "$vm_secret"

```

It takes a few minutes for the VM to be created, the packages to install, and the app to start. There are background tasks that continue to run after the Azure CLI returns you to the prompt. It may be another couple of minutes before you can access the app. When the VM has been created, take note of the `publicIpAddress`

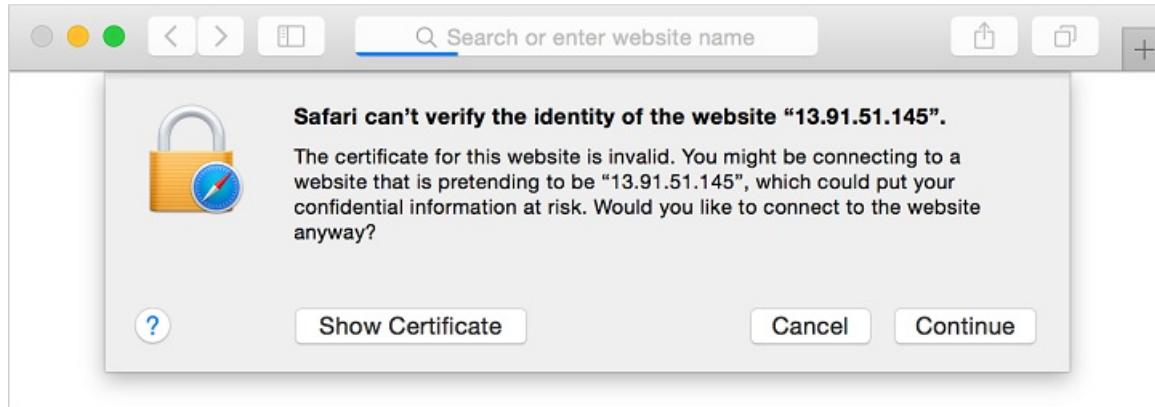
displayed by the Azure CLI. This address is used to access the Node.js app via a web browser.

To allow secure web traffic to reach your VM, open port 443 from the Internet with [az vm open-port](#):

```
az vm open-port \
--resource-group myResourceGroupAutomate \
--name myVMWithCerts \
--port 443
```

Test secure web app

Now you can open a web browser and enter `https://<publicIpAddress>` in the address bar. Provide your own public IP address as shown in the output of the previous VM create process. Accept the security warning if you used a self-signed certificate:



Your secured NGINX site and Nodejs app is then displayed as in the following example:



Next steps

In this tutorial, you configured VMs on first boot with cloud-init. You learned how to:

- Create a cloud-init config file
- Create a VM that uses a cloud-init file
- View a running Node.js app after the VM is created
- Use Key Vault to securely store certificates
- Automate secure deployments of NGINX with cloud-init

Advance to the next tutorial to learn how to create custom VM images.

[Create custom VM images](#)

Tutorial: Create a custom image of an Azure VM with the Azure CLI

11/13/2019 • 3 minutes to read • [Edit Online](#)

Custom images are like marketplace images, but you create them yourself. Custom images can be used to bootstrap configurations such as preloading applications, application configurations, and other OS configurations. In this tutorial, you create your own custom image of an Azure virtual machine. You learn how to:

- Deprovision and generalize VMs
- Create a custom image
- Create a VM from a custom image
- List all the images in your subscription
- Delete an image

This tutorial uses the CLI within the [Azure Cloud Shell](#), which is constantly updated to the latest version. To open the Cloud Shell, select **Try it** from the top of any code block.

If you choose to install and use the CLI locally, this tutorial requires that you are running the Azure CLI version 2.0.30 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Before you begin

The steps below detail how to take an existing VM and turn it into a reusable custom image that you can use to create new VM instances.

To complete the example in this tutorial, you must have an existing virtual machine. If needed, this [script sample](#) can create one for you. When working through the tutorial, replace the resource group and VM names where needed.

Create a custom image

To create an image of a virtual machine, you need to prepare the VM by deprovisioning, deallocating, and then marking the source VM as generalized. Once the VM has been prepared, you can create an image.

Deprovision the VM

Deprovisioning generalizes the VM by removing machine-specific information. This generalization makes it possible to deploy many VMs from a single image. During deprovisioning, the host name is reset to `localhost.localdomain`. SSH host keys, nameserver configurations, root password, and cached DHCP leases are also deleted.

WARNING

Deprovisioning and marking the VM as generalized will make source VM unusable, and it cannot be restarted.

To deprovision the VM, use the Azure VM agent (waagent). The Azure VM agent is installed on the VM and manages provisioning and interacting with the Azure Fabric Controller. For more information, see the [Azure Linux Agent user guide](#).

Connect to your VM using SSH and run the command to deprovision the VM. With the `+user` argument, the last provisioned user account and any associated data are also deleted. Replace the example IP address with the public

IP address of your VM.

SSH to the VM.

```
ssh azureuser@52.174.34.95
```

Deprovision the VM.

```
sudo waagent -deprovision+user -force
```

Close the SSH session.

```
exit
```

Deallocate and mark the VM as generalized

To create an image, the VM needs to be deallocated. Deallocate the VM using [az vm deallocate](#).

```
az vm deallocate --resource-group myResourceGroup --name myVM
```

Finally, set the state of the VM as generalized with [az vm generalize](#) so the Azure platform knows the VM has been generalized. You can only create an image from a generalized VM.

```
az vm generalize --resource-group myResourceGroup --name myVM
```

Create the image

Now you can create an image of the VM by using [az image create](#). The following example creates an image named *myImage* from a VM named *myVM*.

```
az image create \
--resource-group myResourceGroup \
--name myImage \
--source myVM
```

Create VMs from the image

Now that you have an image, you can create one or more new VMs from the image using [az vm create](#). The following example creates a VM named *myVMfromImage* from the image named *myImage*.

```
az vm create \
--resource-group myResourceGroup \
--name myVMfromImage \
--image myImage \
--admin-username azureuser \
--generate-ssh-keys
```

We recommend that you limit the number of concurrent deployments to 20 VMs from a single image. If you are planning large-scale, concurrent deployments of over 20 VMs from the same custom image, you should use a [Shared Image Gallery](#) with multiple image replicas.

Image management

Here are some examples of common image management tasks and how to complete them using the Azure CLI.

List all images by name in a table format.

```
az image list \
--resource-group myResourceGroup
```

Delete an image. This example deletes the image named *myOldImage* from the *myResourceGroup*.

```
az image delete \
--name myOldImage \
--resource-group myResourceGroup
```

Next steps

In this tutorial, you created a custom VM image. You learned how to:

- Deprovision and generalize VMs
- Create a custom image
- Create a VM from a custom image
- List all the images in your subscription
- Delete an image

Advance to the next tutorial to learn about highly available virtual machines.

[Create highly available VMs.](#)

Tutorial: Create and deploy highly available virtual machines with the Azure CLI

1/19/2020 • 4 minutes to read • [Edit Online](#)

In this tutorial, you learn how to increase the availability and reliability of your Virtual Machine solutions on Azure using a capability called Availability Sets. Availability sets ensure that the VMs you deploy on Azure are distributed across multiple isolated hardware clusters. Doing this ensures that if a hardware or software failure within Azure happens, only a subset of your VMs is impacted and that your overall solution remains available and operational.

In this tutorial, you learn how to:

- Create an availability set
- Create a VM in an availability set
- Check available VM sizes

This tutorial uses the CLI within the [Azure Cloud Shell](#), which is constantly updated to the latest version. To open the Cloud Shell, select **Try it** from the top of any code block.

If you choose to install and use the CLI locally, this tutorial requires that you are running the Azure CLI version 2.0.30 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Overview

An Availability Set is a logical grouping capability that you can use in Azure to ensure that the VM resources you place within it are isolated from each other when they are deployed within an Azure datacenter. Azure ensures that the VMs you place within 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 your VMs are impacted, and your overall application stays up and continues to be available to your customers. Availability Sets are an essential capability when you want to build reliable cloud solutions.

Let's consider a typical VM-based solution where you might have four front-end web servers and use two back-end VMs that host a database. With Azure, you'd want to define two availability sets before you deploy your VMs: one availability set for the "web" tier and one availability set for the "database" tier. When you create a new VM you can then specify the availability set as a parameter to the `az vm create` command, and Azure automatically ensures that the VMs you create within the available set are isolated across multiple physical hardware resources. If the physical hardware that one of your Web Server or Database Server VMs is running on has a problem, you know that the other instances of your Web Server and Database VMs remain running because they are on different hardware.

Create an availability set

You can create an availability set using [az vm availability-set create](#). In this example, the number of update and fault domains is set to 2 for the availability set named `myAvailabilitySet` in the `myResourceGroupAvailability` resource group.

First, create a resource group with [az group create](#), then create the availability set:

```

az group create --name myResourceGroupAvailability --location eastus

az vm availability-set create \
    --resource-group myResourceGroupAvailability \
    --name myAvailabilitySet \
    --platform-fault-domain-count 2 \
    --platform-update-domain-count 2

```

Availability Sets allow you to isolate resources across fault domains and update domains. A **fault domain** represents an isolated collection of server + network + storage resources. In the preceding example, the availability set is distributed across at least two fault domains when the VMs are deployed. The availability set is also distributed across two **update domains**. Two update domains ensure that when Azure performs software updates, the VM resources are isolated, preventing all the software that runs on the VM from being updated at the same time.

Create VMs inside an availability set

VMs must be created within the availability set to make sure they are correctly distributed across the hardware. An existing VM cannot be added to an availability set after it is created.

When a VM is created with `az vm create`, use the `--availability-set` parameter to specify the name of the availability set.

```

for i in `seq 1 2`; do
    az vm create \
        --resource-group myResourceGroupAvailability \
        --name myVM$i \
        --availability-set myAvailabilitySet \
        --size Standard_DS1_v2 \
        --vnet-name myVnet \
        --subnet mySubnet \
        --image UbuntuLTS \
        --admin-username azureuser \
        --generate-ssh-keys
done

```

There are now two virtual machines within the availability set. Because they are in the same availability set, Azure ensures that the VMs and all their resources (including data disks) are distributed across isolated physical hardware. This distribution helps ensure much higher availability of the overall VM solution.

The availability set distribution can be viewed in the portal by going to Resource Groups > myResourceGroupAvailability > myAvailabilitySet. The VMs are distributed across the two fault and update domains, as shown in the following example:

NAME	STATUS	FAULT DOMAIN	UPDATE DOMAIN
myVM1	Running	0	0
myVM2	Running	1	1

Check for available VM sizes

Additional VMs can be added to the availability set later, where VM sizes are available on the hardware. Use `az vm availability-set list-sizes` to list all the available sizes on the hardware cluster for the availability set:

```
az vm availability-set list-sizes \
--resource-group myResourceGroupAvailability \
--name myAvailabilitySet \
--output table
```

Next steps

In this tutorial, you learned how to:

- Create an availability set
- Create a VM in an availability set
- Check available VM sizes

Advance to the next tutorial to learn about virtual machine scale sets.

[Create a virtual machine scale set](#)

- To learn more about availability zones, visit the [Availability Zones documentation](#).
- More documentation about both availability sets and availability zones is also available [here](#).
- To try out availability zones, visit [Create a Linux virtual machine in an availability zone with the Azure CLI](#)

Tutorial: Create a virtual machine scale set and deploy a highly available app on Linux with the Azure CLI

1/23/2020 • 7 minutes to read • [Edit Online](#)

A virtual machine scale set allows you to deploy and manage a set of identical, auto-scaling virtual machines. You can scale the number of VMs in the scale set manually, or define rules to autoscale based on resource usage such as CPU, memory demand, or network traffic. In this tutorial, you deploy a virtual machine scale set in Azure. You learn how to:

- Use cloud-init to create an app to scale
- Create a virtual machine scale set
- Increase or decrease the number of instances in a scale set
- Create autoscale rules
- View connection info for scale set instances
- Use data disks in a scale set

This tutorial uses the CLI within the [Azure Cloud Shell](#), which is constantly updated to the latest version. To open the Cloud Shell, select **Try it** from the top of any code block.

If you choose to install and use the CLI locally, this tutorial requires that you are running the Azure CLI version 2.0.30 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Scale Set overview

A virtual machine scale set allows you to deploy and manage a set of identical, auto-scaling virtual machines. VMs in a scale set are distributed across logic fault and update domains in one or more *placement groups*. These are groups of similarly configured VMs, similar to [availability sets](#).

VMs are created as needed in a scale set. You define autoscale rules to control how and when VMs are added or removed from the scale set. These rules can be triggered based on metrics such as CPU load, memory usage, or network traffic.

Scale sets support up to 1,000 VMs when you use an Azure platform image. For workloads with significant installation or VM customization requirements, you may wish to [Create a custom VM image](#). You can create up to 300 VMs in a scale set when using a custom image.

Create an app to scale

For production use, you may wish to [Create a custom VM image](#) that includes your application installed and configured. For this tutorial, let's customize the VMs on first boot to quickly see a scale set in action.

In a previous tutorial, you learned [How to customize a Linux virtual machine on first boot](#) with cloud-init. You can use the same cloud-init configuration file to install NGINX and run a simple 'Hello World' Node.js app.

In your current shell, create a file named `cloud-init.txt` and paste the following configuration. For example, create the file in the Cloud Shell not on your local machine. Enter `sensible-editor cloud-init.txt` to create the file and see a list of available editors. Make sure that the whole cloud-init file is copied correctly, especially the first line:

```

#cloud-config
package_upgrade: true
packages:
- nginx
- nodejs
- npm
write_files:
- owner: www-data:www-data
- path: /etc/nginx/sites-available/default
  content: |
    server {
      listen 80;
      location / {
        proxy_pass http://localhost:3000;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection keep-alive;
        proxy_set_header Host $host;
        proxy_cache_bypass $http_upgrade;
      }
    }
- owner: azureuser:azureuser
- path: /home/azureuser/myapp/index.js
  content: |
    var express = require('express')
    var app = express()
    var os = require('os');
    app.get('/', function (req, res) {
      res.send('Hello World from host ' + os.hostname() + '!')
    })
    app.listen(3000, function () {
      console.log('Hello world app listening on port 3000!')
    })
runcmd:
- service nginx restart
- cd "/home/azureuser/myapp"
- npm init
- npm install express -y
- nodejs index.js

```

Create a scale set

Before you can create a scale set, create a resource group with [az group create](#). The following example creates a resource group named *myResourceGroupScaleSet* in the *eastus* location:

```
az group create --name myResourceGroupScaleSet --location eastus
```

Now create a virtual machine scale set with [az vmss create](#). The following example creates a scale set named *myScaleSet*, uses the cloud-init file to customize the VM, and generates SSH keys if they do not exist:

```
az vmss create \
--resource-group myResourceGroupScaleSet \
--name myScaleSet \
--image UbuntuLTS \
--upgrade-policy-mode automatic \
--custom-data cloud-init.txt \
--admin-username azureuser \
--generate-ssh-keys
```

It takes a few minutes to create and configure all the scale set resources and VMs. There are background tasks that continue to run after the Azure CLI returns you to the prompt. It may be another couple of minutes before you can

access the app.

Allow web traffic

A load balancer was created automatically as part of the virtual machine scale set. The load balancer distributes traffic across a set of defined VMs using load balancer rules. You can learn more about load balancer concepts and configuration in the next tutorial, [How to load balance virtual machines in Azure](#).

To allow traffic to reach the web app, create a rule with [az network lb rule create](#). The following example creates a rule named *myLoadBalancerRuleWeb*:

```
az network lb rule create \
--resource-group myResourceGroupScaleSet \
--name myLoadBalancerRuleWeb \
--lb-name myScaleSetLB \
--backend-pool-name myScaleSetLBBEPool \
--backend-port 80 \
--frontend-ip-name loadBalancerFrontEnd \
--frontend-port 80 \
--protocol tcp
```

Test your app

To see your Node.js app on the web, obtain the public IP address of your load balancer with [az network public-ip show](#). The following example obtains the IP address for *myScaleSetLBPublicIP* created as part of the scale set:

```
az network public-ip show \
--resource-group myResourceGroupScaleSet \
--name myScaleSetLBPublicIP \
--query [ipAddress] \
--output tsv
```

Enter the public IP address in to a web browser. The app is displayed, including the hostname of the VM that the load balancer distributed traffic to:



To see the scale set in action, you can force-refresh your web browser to see the load balancer distribute traffic across all the VMs running your app.

Management tasks

Throughout the lifecycle of the scale set, you may need to run one or more management tasks. Additionally, you may want to create scripts that automate various lifecycle-tasks. The Azure CLI provides a quick way to do those tasks. Here are a few common tasks.

View VMs in a scale set

To view a list of VMs running in your scale set, use [az vmss list-instances](#) as follows:

```
az vmss list-instances \
--resource-group myResourceGroupScaleSet \
--name myScaleSet \
--output table
```

The output is similar to the following example:

InstanceId	LatestModelApplied	Location	Name	ProvisioningState	ResourceGroup
VmId					
1	True	eastus	myScaleSet_1	Succeeded	MYRESOURCEGROUPSCALESET
c72ddc34-6c41-4a53-b89e-dd24f27b30ab					
3	True	eastus	myScaleSet_3	Succeeded	MYRESOURCEGROUPSCALESET
44266022-65c3-49c5-92dd-88ffa64f95da					

Manually increase or decrease VM instances

To see the number of instances you currently have in a scale set, use [az vmss show](#) and query on `sku.capacity`:

```
az vmss show \
--resource-group myResourceGroupScaleSet \
--name myScaleSet \
--query [sku.capacity] \
--output table
```

You can then manually increase or decrease the number of virtual machines in the scale set with [az vmss scale](#). The following example sets the number of VMs in your scale set to 3:

```
az vmss scale \
--resource-group myResourceGroupScaleSet \
--name myScaleSet \
--new-capacity 3
```

Get connection info

To obtain connection information about the VMs in your scale sets, use [az vmss list-instance-connection-info](#). This command outputs the public IP address and port for each VM that allows you to connect with SSH:

```
az vmss list-instance-connection-info \
--resource-group myResourceGroupScaleSet \
--name myScaleSet
```

Use data disks with scale sets

You can create and use data disks with scale sets. In a previous tutorial, you learned how to [Manage Azure disks](#) that outlines the best practices and performance improvements for building apps on data disks rather than the OS disk.

Create scale set with data disks

To create a scale set and attach data disks, add the `--data-disk-sizes-gb` parameter to the [az vmss create](#) command. The following example creates a scale set with 50Gb data disks attached to each instance:

```
az vmss create \
--resource-group myResourceGroupScaleSet \
--name myScaleSetDisks \
--image UbuntuLTS \
--upgrade-policy-mode automatic \
--custom-data cloud-init.txt \
--admin-username azureuser \
--generate-ssh-keys \
--data-disk-sizes-gb 50
```

When instances are removed from a scale set, any attached data disks are also removed.

Add data disks

To add a data disk to instances in your scale set, use [az vmss disk attach](#). The following example adds a 50Gb disk to each instance:

```
az vmss disk attach \
--resource-group myResourceGroupScaleSet \
--name myScaleSet \
--size-gb 50 \
--lun 2
```

Detach data disks

To remove a data disk to instances in your scale set, use [az vmss disk detach](#). The following example removes the data disk at LUN 2 from each instance:

```
az vmss disk detach \
--resource-group myResourceGroupScaleSet \
--name myScaleSet \
--lun 2
```

Next steps

In this tutorial, you created a virtual machine scale set. You learned how to:

- Use cloud-init to create an app to scale
- Create a virtual machine scale set
- Increase or decrease the number of instances in a scale set
- Create autoscale rules
- View connection info for scale set instances
- Use data disks in a scale set

Advance to the next tutorial to learn more about load balancing concepts for virtual machines.

[Load balance virtual machines](#)

Tutorial: Load balance Linux virtual machines in Azure to create a highly available application with the Azure CLI

11/13/2019 • 9 minutes to read • [Edit Online](#)

Load balancing provides a higher level of availability by spreading incoming requests across multiple virtual machines. In this tutorial, you learn about the different components of the Azure load balancer that distribute traffic and provide high availability. You learn how to:

- Create an Azure load balancer
- Create a load balancer health probe
- Create load balancer traffic rules
- Use cloud-init to create a basic Node.js app
- Create virtual machines and attach to a load balancer
- View a load balancer in action
- Add and remove VMs from a load balancer

This tutorial uses the CLI within the [Azure Cloud Shell](#), which is constantly updated to the latest version. To open the Cloud Shell, select **Try it** from the top of any code block.

If you choose to install and use the CLI locally, this tutorial requires that you are running the Azure CLI version 2.0.30 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Azure load balancer overview

An Azure load balancer is a Layer-4 (TCP, UDP) load balancer that provides high availability by distributing incoming traffic among healthy VMs. A load balancer health probe monitors a given port on each VM and only distributes traffic to an operational VM.

You define a front-end IP configuration that contains one or more public IP addresses. This front-end IP configuration allows your load balancer and applications to be accessible over the Internet.

Virtual machines connect to a load balancer using their virtual network interface card (NIC). To distribute traffic to the VMs, a back-end address pool contains the IP addresses of the virtual (NICs) connected to the load balancer.

To control the flow of traffic, you define load balancer rules for specific ports and protocols that map to your VMs.

If you followed the previous tutorial to [create a virtual machine scale set](#), a load balancer was created for you. All these components were configured for you as part of the scale set.

Create Azure load balancer

This section details how you can create and configure each component of the load balancer. Before you can create your load balancer, create a resource group with [az group create](#). The following example creates a resource group named *myResourceGroupLoadBalancer* in the *eastus* location:

```
az group create --name myResourceGroupLoadBalancer --location eastus
```

Create a public IP address

To access your app on the Internet, you need a public IP address for the load balancer. Create a public IP address with [az network public-ip create](#). The following example creates a public IP address named *myPublicIP* in the *myResourceGroupLoadBalancer* resource group:

```
az network public-ip create \
--resource-group myResourceGroupLoadBalancer \
--name myPublicIP
```

Create a load balancer

Create a load balancer with [az network lb create](#). The following example creates a load balancer named *myLoadBalancer* and assigns the *myPublicIP* address to the front-end IP configuration:

```
az network lb create \
--resource-group myResourceGroupLoadBalancer \
--name myLoadBalancer \
--frontend-ip-name myFrontEndPool \
--backend-pool-name myBackEndPool \
--public-ip-address myPublicIP
```

Create a health probe

To allow the load balancer to monitor the status of your app, you use a health probe. The health probe dynamically adds or removes VMs from the load balancer rotation based on their response to health checks. By default, a VM is removed from the load balancer distribution after two consecutive failures at 15-second intervals. You create a health probe based on a protocol or a specific health check page for your app.

The following example creates a TCP probe. You can also create custom HTTP probes for more fine grained health checks. When using a custom HTTP probe, you must create the health check page, such as *healthcheck.js*. The probe must return an **HTTP 200 OK** response for the load balancer to keep the host in rotation.

To create a TCP health probe, you use [az network lb probe create](#). The following example creates a health probe named *myHealthProbe*:

```
az network lb probe create \
--resource-group myResourceGroupLoadBalancer \
--lb-name myLoadBalancer \
--name myHealthProbe \
--protocol tcp \
--port 80
```

Create a load balancer rule

A load balancer rule is used to define how traffic is distributed to the VMs. You define the front-end IP configuration for the incoming traffic and the back-end IP pool to receive the traffic, along with the required source and destination port. To make sure only healthy VMs receive traffic, you also define the health probe to use.

Create a load balancer rule with [az network lb rule create](#). The following example creates a rule named *myLoadBalancerRule*, uses the *myHealthProbe* health probe, and balances traffic on port 80:

```
az network lb rule create \
--resource-group myResourceGroupLoadBalancer \
--lb-name myLoadBalancer \
--name myLoadBalancerRule \
--protocol tcp \
--frontend-port 80 \
--backend-port 80 \
--frontend-ip-name myFrontEndPool \
--backend-pool-name myBackEndPool \
--probe-name myHealthProbe
```

Configure virtual network

Before you deploy some VMs and can test your balancer, create the supporting virtual network resources. For more information about virtual networks, see the [Manage Azure Virtual Networks](#) tutorial.

Create network resources

Create a virtual network with [az network vnet create](#). The following example creates a virtual network named *myVnet* with a subnet named *mySubnet*:

```
az network vnet create \
--resource-group myResourceGroupLoadBalancer \
--name myVnet \
--subnet-name mySubnet
```

To add a network security group, you use [az network nsg create](#). The following example creates a network security group named *myNetworkSecurityGroup*:

```
az network nsg create \
--resource-group myResourceGroupLoadBalancer \
--name myNetworkSecurityGroup
```

Create a network security group rule with [az network nsg rule create](#). The following example creates a network security group rule named *myNetworkSecurityGroupRule*:

```
az network nsg rule create \
--resource-group myResourceGroupLoadBalancer \
--nsg-name myNetworkSecurityGroup \
--name myNetworkSecurityGroupRule \
--priority 1001 \
--protocol tcp \
--destination-port-range 80
```

Virtual NICs are created with [az network nic create](#). The following example creates three virtual NICs. (One virtual NIC for each VM you create for your app in the following steps). You can create additional virtual NICs and VMs at any time and add them to the load balancer:

```
for i in `seq 1 3`; do
    az network nic create \
        --resource-group myResourceGroupLoadBalancer \
        --name myNic$i \
        --vnet-name myVnet \
        --subnet mySubnet \
        --network-security-group myNetworkSecurityGroup \
        --lb-name myLoadBalancer \
        --lb-address-pools myBackEndPool
done
```

When all three virtual NICs are created, continue on to the next step

Create virtual machines

Create cloud-init config

In a previous tutorial on [How to customize a Linux virtual machine on first boot](#), you learned how to automate VM customization with cloud-init. You can use the same cloud-init configuration file to install NGINX and run a simple 'Hello World' Node.js app in the next step. To see the load balancer in action, at the end of the tutorial you access this simple app in a web browser.

In your current shell, create a file named *cloud-init.txt* and paste the following configuration. For example, create the file in the Cloud Shell not on your local machine. Enter `sensible-editor cloud-init.txt` to create the file and see a list of available editors. Make sure that the whole cloud-init file is copied correctly, especially the first line:

```

#cloud-config
package_upgrade: true
packages:
- nginx
- nodejs
- npm
write_files:
- owner: www-data:www-data
- path: /etc/nginx/sites-available/default
  content: |
    server {
      listen 80;
      location / {
        proxy_pass http://localhost:3000;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection keep-alive;
        proxy_set_header Host $host;
        proxy_cache_bypass $http_upgrade;
      }
    }
- owner: azureuser:azureuser
- path: /home/azureuser/myapp/index.js
  content: |
    var express = require('express')
    var app = express()
    var os = require('os');
    app.get('/', function (req, res) {
      res.send('Hello World from host ' + os.hostname() + '!')
    })
    app.listen(3000, function () {
      console.log('Hello world app listening on port 3000!')
    })
runcmd:
- service nginx restart
- cd "/home/azureuser/myapp"
- npm init
- npm install express -y
- nodejs index.js

```

Create virtual machines

To improve the high availability of your app, place your VMs in an availability set. For more information about availability sets, see the previous [How to create highly available virtual machines](#) tutorial.

Create an availability set with `az vm availability-set create`. The following example creates an availability set named `myAvailabilitySet`:

```

az vm availability-set create \
--resource-group myResourceGroupLoadBalancer \
--name myAvailabilitySet

```

Now you can create the VMs with `az vm create`. The following example creates three VMs and generates SSH keys if they do not already exist:

```

for i in `seq 1 3`; do
    az vm create \
        --resource-group myResourceGroupLoadBalancer \
        --name myVM$i \
        --availability-set myAvailabilitySet \
        --nics myNic$i \
        --image UbuntuLTS \
        --admin-username azureuser \
        --generate-ssh-keys \
        --custom-data cloud-init.txt \
        --no-wait
done

```

There are background tasks that continue to run after the Azure CLI returns you to the prompt. The `--no-wait` parameter does not wait for all the tasks to complete. It may be another couple of minutes before you can access the app. The load balancer health probe automatically detects when the app is running on each VM. Once the app is running, the load balancer rule starts to distribute traffic.

Test load balancer

Obtain the public IP address of your load balancer with [az network public-ip show](#). The following example obtains the IP address for *myPublicIP* created earlier:

```

az network public-ip show \
    --resource-group myResourceGroupLoadBalancer \
    --name myPublicIP \
    --query [ipAddress] \
    --output tsv

```

You can then enter the public IP address in to a web browser. Remember - it takes a few minutes for the VMs to be ready before the load balancer starts to distribute traffic to them. The app is displayed, including the hostname of the VM that the load balancer distributed traffic to as in the following example:



To see the load balancer distribute traffic across all three VMs running your app, you can force-refresh your web browser.

Add and remove VMs

You may need to perform maintenance on the VMs running your app, such as installing OS updates. To deal with increased traffic to your app, you may need to add additional VMs. This section shows you how to remove or add a VM from the load balancer.

Remove a VM from the load balancer

You can remove a VM from the backend address pool with [az network nic ip-config address-pool remove](#). The following example removes the virtual NIC for **myVM2** from *myLoadBalancer*:

```
az network nic ip-config address-pool remove \
--resource-group myResourceGroupLoadBalancer \
--nic-name myNic2 \
--ip-config-name ipConfig1 \
--lb-name myLoadBalancer \
--address-pool myBackEndPool
```

To see the load balancer distribute traffic across the remaining two VMs running your app you can force-refresh your web browser. You can now perform maintenance on the VM, such as installing OS updates or performing a VM reboot.

To view a list of VMs with virtual NICs connected to the load balancer, use [az network lb address-pool show](#). Query and filter on the ID of the virtual NIC as follows:

```
az network lb address-pool show \
--resource-group myResourceGroupLoadBalancer \
--lb-name myLoadBalancer \
--name myBackEndPool \
--query backendIpConfigurations \
--output tsv | cut -f4
```

The output is similar to the following example, which shows that the virtual NIC for VM 2 is no longer part of the backend address pool:

```
/subscriptions/<guid>/resourceGroups/myResourceGroupLoadBalancer/providers/Microsoft.Network/networkInterfaces
/myNic1/ipConfigurations/ipconfig1
/subscriptions/<guid>/resourceGroups/myResourceGroupLoadBalancer/providers/Microsoft.Network/networkInterfaces
/myNic3/ipConfigurations/ipconfig1
```

Add a VM to the load balancer

After performing VM maintenance, or if you need to expand capacity, you can add a VM to the backend address pool with [az network nic ip-config address-pool add](#). The following example adds the virtual NIC for **myVM2** to *myLoadBalancer*:

```
az network nic ip-config address-pool add \
--resource-group myResourceGroupLoadBalancer \
--nic-name myNic2 \
--ip-config-name ipConfig1 \
--lb-name myLoadBalancer \
--address-pool myBackEndPool
```

To verify that the virtual NIC is connected to the backend address pool, use [az network lb address-pool show](#) again from the preceding step.

Next steps

In this tutorial, you created a load balancer and attached VMs to it. You learned how to:

- Create an Azure load balancer
- Create a load balancer health probe
- Create load balancer traffic rules
- Use cloud-init to create a basic Node.js app
- Create virtual machines and attach to a load balancer
- View a load balancer in action

- Add and remove VMs from a load balancer

Advance to the next tutorial to learn more about Azure virtual network components.

[Manage VMs and virtual networks](#)

Tutorial: Create and manage Azure virtual networks for Linux virtual machines with the Azure CLI

11/13/2019 • 10 minutes to read • [Edit Online](#)

Azure virtual machines use Azure networking for internal and external network communication. This tutorial walks through deploying two virtual machines and configuring Azure networking for these VMs. The examples in this tutorial assume that the VMs are hosting a web application with a database back-end, however an application is not deployed in the tutorial. In this tutorial, you learn how to:

- Create a virtual network and subnet
- Create a public IP address
- Create a front-end VM
- Secure network traffic
- Create a back-end VM

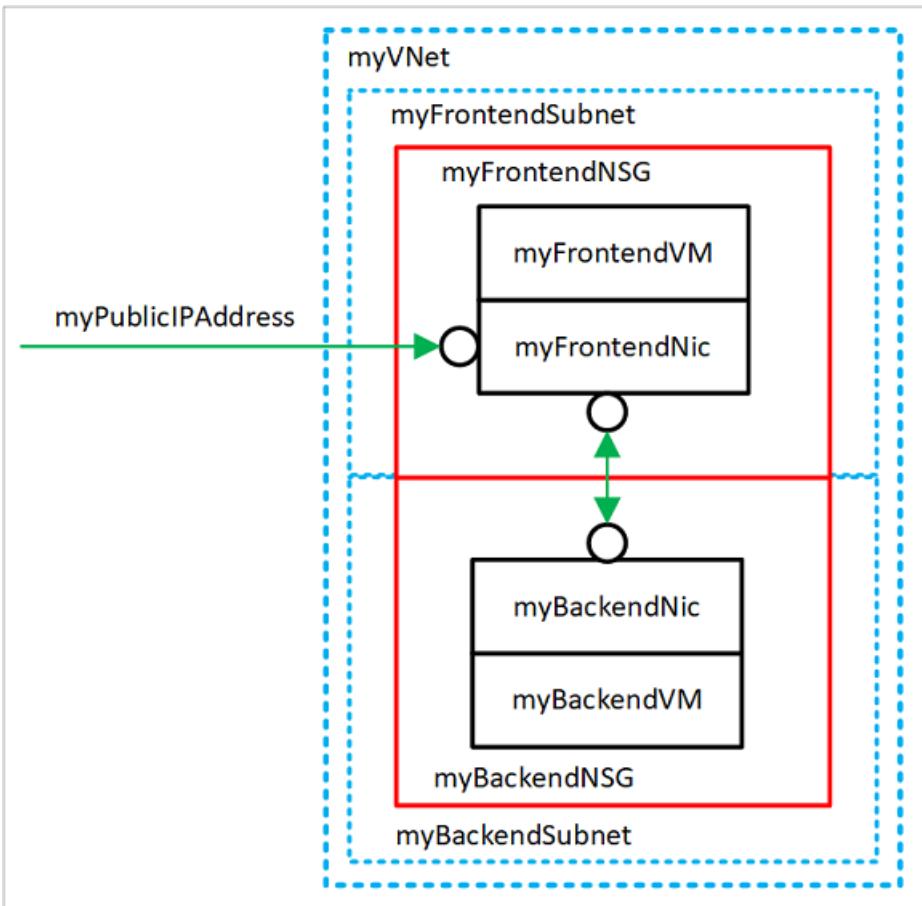
This tutorial uses the CLI within the [Azure Cloud Shell](#), which is constantly updated to the latest version. To open the Cloud Shell, select **Try it** from the top of any code block.

If you choose to install and use the CLI locally, this tutorial requires that you are running the Azure CLI version 2.0.30 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

VM networking overview

Azure virtual networks enable secure network connections between virtual machines, the internet, and other Azure services such as Azure SQL database. Virtual networks are broken down into logical segments called subnets. Subnets are used to control network flow, and as a security boundary. When deploying a VM, it generally includes a virtual network interface, which is attached to a subnet.

As you complete the tutorial, the following virtual network resources are created:



- `myVNet` - The virtual network that the VMs use to communicate with each other and the internet.
- `myFrontendSubnet` - The subnet in `myVNet` used by the front-end resources.
- `myPublicIPAddress` - The public IP address used to access `myFrontendVM` from the internet.
- `myFrontendNic` - The network interface used by `myFrontendVM` to communicate with `myBackendVM`.
- `myFrontendVM` - The VM used to communicate between the internet and `myBackendVM`.
- `myBackendNSG` - The network security group that controls communication between the `myFrontendVM` and `myBackendVM`.
- `myBackendSubnet` - The subnet associated with `myBackendNSG` and used by the back-end resources.
- `myBackendNic` - The network interface used by `myBackendVM` to communicate with `myFrontendVM`.
- `myBackendVM` - The VM that uses port 22 and 3306 to communicate with `myFrontendVM`.

Create a virtual network and subnet

For this tutorial, a single virtual network is created with two subnets. A front-end subnet for hosting a web application, and a back-end subnet for hosting a database server.

Before you can create a virtual network, create a resource group with [az group create](#). The following example creates a resource group named `myRGNetwork` in the `eastus` location.

```
az group create --name myRGNetwork --location eastus
```

Create virtual network

Use the [az network vnet create](#) command to create a virtual network. In this example, the network is named `mvVNet` and is given an address prefix of `10.0.0.0/16`. A subnet is also created with a name of `myFrontendSubnet` and a prefix of `10.0.1.0/24`. Later in this tutorial a front-end VM is connected to this subnet.

```
az network vnet create \
--resource-group myRGNetwork \
--name myVNet \
--address-prefix 10.0.0.0/16 \
--subnet-name myFrontendSubnet \
--subnet-prefix 10.0.1.0/24
```

Create subnet

A new subnet is added to the virtual network using the [az network vnet subnet create](#) command. In this example, the subnet is named *myBackendSubnet* and is given an address prefix of *10.0.2.0/24*. This subnet is used with all back-end services.

```
az network vnet subnet create \
--resource-group myRGNetwork \
--vnet-name myVNet \
--name myBackendSubnet \
--address-prefix 10.0.2.0/24
```

At this point, a network has been created and segmented into two subnets, one for front-end services, and another for back-end services. In the next section, virtual machines are created and connected to these subnets.

Create a public IP address

A public IP address allows Azure resources to be accessible on the internet. The allocation method of the public IP address can be configured as dynamic or static. By default, a public IP address is dynamically allocated. Dynamic IP addresses are released when a VM is deallocated. This behavior causes the IP address to change during any operation that includes a VM deallocation.

The allocation method can be set to static, which ensures that the IP address remains assigned to a VM, even during a deallocated state. When using a statically allocated IP address, the IP address itself cannot be specified. Instead, it is allocated from a pool of available addresses.

```
az network public-ip create --resource-group myRGNetwork --name myPublicIPAddress
```

When creating a VM with the [az vm create](#) command, the default public IP address allocation method is dynamic.

When creating a virtual machine using the [az vm create](#) command, include the

`--public-ip-address-allocation static` argument to assign a static public IP address. This operation is not demonstrated in this tutorial, however in the next section a dynamically allocated IP address is changed to a statically allocated address.

Change allocation method

The IP address allocation method can be changed using the [az network public-ip update](#) command. In this example, the IP address allocation method of the front-end VM is changed to static.

First, deallocate the VM.

```
az vm deallocate --resource-group myRGNetwork --name myFrontendVM
```

Use the [az network public-ip update](#) command to update the allocation method. In this case, the

`--allocation-method` is being set to *static*.

```
az network public-ip update --resource-group myRGNetwork --name myPublicIPAddress --allocation-method static
```

Start the VM.

```
az vm start --resource-group myRGNetwork --name myFrontendVM --no-wait
```

No public IP address

Often, a VM does not need to be accessible over the internet. To create a VM without a public IP address, use the `--public-ip-address ""` argument with an empty set of double quotes. This configuration is demonstrated later in this tutorial.

Create a front-end VM

Use the `az vm create` command to create the VM named *myFrontendVM* using *myPublicIPAddress*.

```
az vm create \
--resource-group myRGNetwork \
--name myFrontendVM \
--vnet-name myVNet \
--subnet myFrontendSubnet \
--nsg myFrontendNSG \
--public-ip-address myPublicIPAddress \
--image UbuntuLTS \
--generate-ssh-keys
```

Secure network traffic

A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure Virtual Networks (VNet). NSGs can be associated to subnets or individual network interfaces. When an NSG is associated with a network interface, it applies only the associated VM. When an NSG is associated to a subnet, the rules apply to all resources connected to the subnet.

Network security group rules

NSG rules define networking ports over which traffic is allowed or denied. The rules can include source and destination IP address ranges so that traffic is controlled between specific systems or subnets. NSG rules also include a priority (between 1—and 4096). Rules are evaluated in the order of priority. A rule with a priority of 100 is evaluated before a rule with priority 200.

All NSGs contain a set of default rules. The default rules cannot be deleted, but because they are assigned the lowest priority, they can be overridden by the rules that you create.

The default rules for NSGs are:

- **Virtual network** - Traffic originating and ending in a virtual network is allowed both in inbound and outbound directions.
- **Internet** - Outbound traffic is allowed, but inbound traffic is blocked.
- **Load balancer** - Allow Azure's load balancer to probe the health of your VMs and role instances. If you are not using a load balanced set, you can override this rule.

Create network security groups

A network security group can be created at the same time as a VM using the `az vm create` command. When doing so, the NSG is associated with the VMs network interface and an NSG rule is auto created to allow traffic on port 22 from any source. Earlier in this tutorial, the front-end NSG was auto-created with the front-end VM. An NSG rule was also auto created for port 22.

In some cases, it may be helpful to pre-create an NSG, such as when default SSH rules should not be created, or when the NSG should be attached to a subnet.

Use the [az network nsg create](#) command to create a network security group.

```
az network nsg create --resource-group myRGNetwork --name myBackendNSG
```

Instead of associating the NSG to a network interface, it is associated with a subnet. In this configuration, any VM that is attached to the subnet inherits the NSG rules.

Update the existing subnet named *myBackendSubnet* with the new NSG.

```
az network vnet subnet update \
--resource-group myRGNetwork \
--vnet-name myVNet \
--name myBackendSubnet \
--network-security-group myBackendNSG
```

Secure incoming traffic

When the front-end VM was created, an NSG rule was created to allow incoming traffic on port 22. This rule allows SSH connections to the VM. For this example, traffic should also be allowed on port 80. This configuration allows a web application to be accessed on the VM.

Use the [az network nsg rule create](#) command to create a rule for port 80.

```
az network nsg rule create \
--resource-group myRGNetwork \
--nsg-name myFrontendNSG \
--name http \
--access allow \
--protocol Tcp \
--direction Inbound \
--priority 200 \
--source-address-prefix "*" \
--source-port-range "*" \
--destination-address-prefix "*" \
--destination-port-range 80
```

The front-end VM is only accessible on port 22 and port 80. All other incoming traffic is blocked at the network security group. It may be helpful to visualize the NSG rule configurations. Return the NSG rule configuration with the [az network rule list](#) command.

```
az network nsg rule list --resource-group myRGNetwork --nsg-name myFrontendNSG --output table
```

Secure VM to VM traffic

Network security group rules can also apply between VMs. For this example, the front-end VM needs to communicate with the back-end VM on port 22 and 3306. This configuration allows SSH connections from the front-end VM, and also allow an application on the front-end VM to communicate with a back-end MySQL database. All other traffic should be blocked between the front-end and back-end virtual machines.

Use the [az network nsg rule create](#) command to create a rule for port 22. Notice that the `--source-address-prefix` argument specifies a value of `10.0.1.0/24`. This configuration ensures that only traffic from the front-end subnet is allowed through the NSG.

```
az network nsg rule create \
--resource-group myRGNetwork \
--nsg-name myBackendNSG \
--name SSH \
--access Allow \
--protocol Tcp \
--direction Inbound \
--priority 100 \
--source-address-prefix 10.0.1.0/24 \
--source-port-range "*" \
--destination-address-prefix "*" \
--destination-port-range "22"
```

Now add a rule for MySQL traffic on port 3306.

```
az network nsg rule create \
--resource-group myRGNetwork \
--nsg-name myBackendNSG \
--name MySQL \
--access Allow \
--protocol Tcp \
--direction Inbound \
--priority 200 \
--source-address-prefix 10.0.1.0/24 \
--source-port-range "*" \
--destination-address-prefix "*" \
--destination-port-range "3306"
```

Finally, because NSGs have a default rule allowing all traffic between VMs in the same VNet, a rule can be created for the back-end NSGs to block all traffic. Notice here that the `--priority` is given a value of *300*, which is lower than both the NSG and MySQL rules. This configuration ensures that SSH and MySQL traffic is still allowed through the NSG.

```
az network nsg rule create \
--resource-group myRGNetwork \
--nsg-name myBackendNSG \
--name denyAll \
--access Deny \
--protocol Tcp \
--direction Inbound \
--priority 300 \
--source-address-prefix "*" \
--source-port-range "*" \
--destination-address-prefix "*" \
--destination-port-range "*"
```

Create back-end VM

Now create a virtual machine, which is attached to the *myBackendSubnet*. Notice that the `--nsg` argument has a value of empty double quotes. An NSG does not need to be created with the VM. The VM is attached to the back-end subnet, which is protected with the pre-created back-end NSG. This NSG applies to the VM. Also, notice here that the `--public-ip-address` argument has a value of empty double quotes. This configuration creates a VM without a public IP address.

```
az vm create \
--resource-group myRGNetwork \
--name myBackendVM \
--vnet-name myVNet \
--subnet myBackendSubnet \
--public-ip-address "" \
--nsg "" \
--image UbuntuLTS \
--generate-ssh-keys
```

The back-end VM is only accessible on port 22 and port 3306 from the front-end subnet. All other incoming traffic is blocked at the network security group. It may be helpful to visualize the NSG rule configurations. Return the NSG rule configuration with the [az network rule list](#) command.

```
az network nsg rule list --resource-group myRGNetwork --nsg-name myBackendNSG --output table
```

Next steps

In this tutorial, you created and secured Azure networks as related to virtual machines. You learned how to:

- Create a virtual network and subnet
- Create a public IP address
- Create a front-end VM
- Secure network traffic
- Create back-end VM

Advance to the next tutorial to learn about securing data on virtual machines using Azure backup.

[Back up Linux virtual machines in Azure](#)

Tutorial: Back up and restore files for Linux virtual machines in Azure

11/13/2019 • 5 minutes to read • [Edit Online](#)

You can protect your data by taking backups at regular intervals. Azure Backup creates recovery points that are stored in geo-redundant recovery vaults. When you restore from a recovery point, you can restore the whole VM or specific files. This article explains how to restore a single file to a Linux VM running nginx. If you don't already have a VM to use, you can create one using the [Linux quickstart](#). In this tutorial you learn how to:

- Create a backup of a VM
- Schedule a daily backup
- Restore a file from a backup

Backup overview

When the Azure Backup service initiates a backup, it triggers the backup extension to take a point-in-time snapshot. The Azure Backup service uses the *VMSnapshotLinux* extension in Linux. The extension is installed during the first VM backup if the VM is running. If the VM is not running, the Backup service takes a snapshot of the underlying storage (since no application writes occur while the VM is stopped).

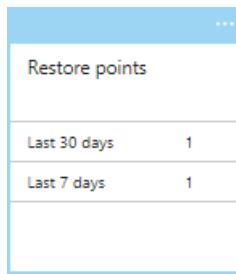
By default, Azure Backup takes a file system consistent backup for Linux VM but it can be configured to take [application consistent backup using pre-script and post-script framework](#). Once the Azure Backup service takes the snapshot, the data is transferred to the vault. To maximize efficiency, the service identifies and transfers only the blocks of data that have changed since the previous backup.

When the data transfer is complete, the snapshot is removed and a recovery point is created.

Create a backup

Create a scheduled daily backup to a Recovery Services Vault:

1. Sign in to the [Azure portal](#).
2. In the menu on the left, select **Virtual machines**.
3. From the list, select a VM to back up.
4. On the VM blade, in the **Settings** section, click **Backup**. The **Enable backup** blade opens.
5. In **Recovery Services vault**, click **Create new** and provide the name for the new vault. A new vault is created in the same Resource Group and location as the virtual machine.
6. Click **Backup policy**. For this example, keep the defaults and click **OK**.
7. On the **Enable backup** blade, click **Enable Backup**. This creates a daily backup based on the default schedule.
8. To create an initial recovery point, on the **Backup** blade click **Backup now**.
9. On the **Backup Now** blade, click the calendar icon, use the calendar control to select the last day this recovery point is retained, and click **Backup**.
10. In the **Backup** blade for your VM, you see the number of recovery points that are complete.



The first backup takes about 20 minutes. Proceed to the next part of this tutorial after your backup is finished.

Restore a file

If you accidentally delete or make changes to a file, you can use File Recovery to recover the file from your backup vault. File Recovery uses a script that runs on the VM, to mount the recovery point as a local drive. These drives remain mounted for 12 hours so that you can copy files from the recovery point and restore them to the VM.

In this example, we show how to recover the default nginx web page /var/www/html/index.nginx-debian.html. The public IP address of our VM in this example is 13.69.75.209. You can find the IP address of your vm using:

```
az vm show --resource-group myResourceGroup --name myVM -d --query [publicIps] --o tsv
```

1. On your local computer, open a browser and type in the public IP address of your VM to see the default nginx web page.



2. SSH into your VM.

```
ssh 13.69.75.209
```

3. Delete /var/www/html/index.nginx-debian.html.

```
sudo rm /var/www/html/index.nginx-debian.html
```

4. On your local computer, refresh the browser by hitting CTRL + F5 to see that default nginx page is gone.



5. On your local computer, sign in to the [Azure portal](#).
6. In the menu on the left, select **Virtual machines**.
7. From the list, select the VM.
8. On the VM blade, in the **Settings** section, click **Backup**. The **Backup** blade opens.
9. In the menu at the top of the blade, select **File Recovery**. The **File Recovery** blade opens.
10. In **Step 1: Select recovery point**, select a recovery point from the drop-down.
11. In **Step 2: Download script to browse and recover files**, click the **Download Executable** button. Save the downloaded file to your local computer.
12. Click **Download script** to download the script file locally.
13. Open a Bash prompt and type the following, replacing *Linux_myVM_05-05-2017.sh* with the correct path and filename for the script that you downloaded, *azureuser* with the username for the VM and *13.69.75.209* with the public IP address for your VM.

```
scp Linux_myVM_05-05-2017.sh azureuser@13.69.75.209:
```

14. On your local computer, open an SSH connection to the VM.

```
ssh 13.69.75.209
```

15. On your VM, add execute permissions to the script file.

```
chmod +x Linux_myVM_05-05-2017.sh
```

16. On your VM, run the script to mount the recovery point as a filesystem.

```
./Linux_myVM_05-05-2017.sh
```

17. The output from the script gives you the path for the mount point. The output looks similar to this:

Microsoft Azure VM Backup - File Recovery

Connecting to recovery point using ISCSI service...

Connection succeeded!

Please wait while we attach volumes of the recovery point to this machine...

***** Volumes of the recovery point and their mount paths on this machine *****

Sr.No.	Disk	Volume	MountPath
--------	------	--------	-----------

1)	/dev/sdc	/dev/sdc1	/home/azureuser/myVM-20170505191055/Volume1
----	----------	-----------	---

***** Open File Explorer to browse for files. *****

After recovery, to remove the disks and close the connection to the recovery point, please click 'Unmount Disks' in step 3 of the portal.

Please enter 'q/Q' to exit...

18. On your VM, copy the nginx default web page from the mount point back to where you deleted the file.

```
sudo cp ~/myVM-20170505191055/Volume1/var/www/html/index.nginx-debian.html /var/www/html/
```

19. On your local computer, open the browser tab where you are connected to the IP address of the VM showing the nginx default page. Press CTRL + F5 to refresh the browser page. You should now see that the default page is working again.



20. On your local computer, go back to the browser tab for the Azure portal and in **Step 3: Unmount the disks after recovery** click the **Unmount Disks** button. If you forget to do this step, the connection to the mountpoint is automatically closed after 12 hours. After those 12 hours, you need to download a new script to create a new mountpoint.

Next steps

In this tutorial, you learned how to:

- Create a backup of a VM
- Schedule a daily backup
- Restore a file from a backup

Advance to the next tutorial to learn about monitoring virtual machines.

[Govern virtual machines](#)

Tutorial: Learn about Linux virtual machine management with Azure CLI

1/14/2020 • 11 minutes to read • [Edit Online](#)

When deploying resources to Azure, you have tremendous flexibility when deciding what types of resources to deploy, where they are located, and how to set them up. However, that flexibility may open more options than you would like to allow in your organization. As you consider deploying resources to Azure, you might be wondering:

- How do I meet legal requirements for data sovereignty in certain countries/regions?
- How do I control costs?
- How do I ensure that someone does not inadvertently change a critical system?
- How do I track resource costs and bill it accurately?

This article addresses those questions. Specifically, you:

- Assign users to roles and assign the roles to a scope so users have permission to perform expected actions but not more actions.
- Apply policies that prescribe conventions for resources in your subscription.
- Lock resources that are critical to your system.
- Tag resources so you can track them by values that make sense to your organization.

This article focuses on the tasks you take to implement governance. For a broader discussion of the concepts, see [Governance in Azure](#).

Use Azure Cloud Shell

Azure hosts Azure Cloud Shell, an interactive shell environment that you can use through your browser. You can use either Bash or PowerShell with Cloud Shell to work with Azure services. You can use the Cloud Shell preinstalled commands to run the code in this article without having to install anything on your local environment.

To start Azure Cloud Shell:

OPTION	EXAMPLE/LINK
Select Try It in the upper-right corner of a code block. Selecting Try It doesn't automatically copy the code to Cloud Shell.	
Go to https://shell.azure.com , or select the Launch Cloud Shell button to open Cloud Shell in your browser.	
Select the Cloud Shell button on the menu bar at the upper right in the Azure portal .	

To run the code in this article in Azure Cloud Shell:

1. Start Cloud Shell.
2. Select the **Copy** button on a code block to copy the code.
3. Paste the code into the Cloud Shell session by selecting **Ctrl+Shift+V** on Windows and Linux or by

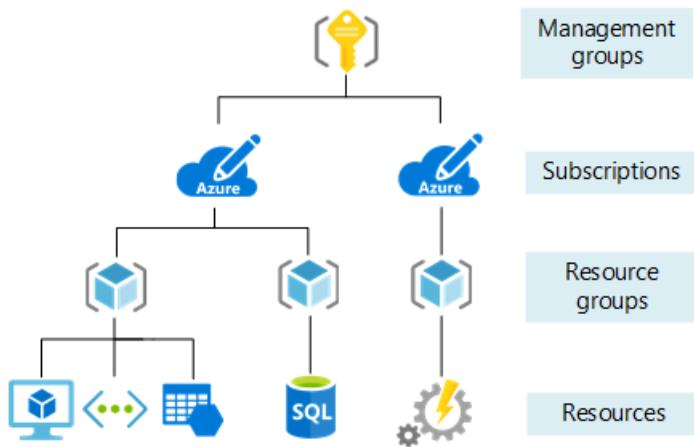
selecting **Cmd+Shift+V** on macOS.

4. Select **Enter** to run the code.

If you choose to install and use Azure CLI locally, this tutorial requires that you're running the Azure CLI version 2.0.30 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Understand scope

Before creating any items, let's review the concept of scope. Azure provides four levels of management: management groups, subscription, resource group, and resource. [Management groups](#) are in a preview release. The following image shows an example of these layers.



You apply management settings at any of these levels of scope. The level you select determines how widely the setting is applied. Lower levels inherit settings from higher levels. When you apply a setting to the subscription, that setting is applied to all resource groups and resources in your subscription. When you apply a setting on the resource group, that setting is applied to the resource group and all its resources. However, another resource group does not have that setting.

Usually, it makes sense to apply critical settings at higher levels and project-specific requirements at lower levels. For example, you might want to make sure all resources for your organization are deployed to certain regions. To accomplish this requirement, apply a policy to the subscription that specifies the allowed locations. As other users in your organization add new resource groups and resources, the allowed locations are automatically enforced.

In this tutorial, you apply all management settings to a resource group so you can easily remove those settings when done.

Let's create that resource group.

```
az group create --name myResourceGroup --location "East US"
```

Currently, the resource group is empty.

Role-based access control

You want to make sure users in your organization have the right level of access to these resources. You don't want to grant unlimited access to users, but you also need to make sure they can do their work. [Role-based access control](#) enables you to manage which users have permission to complete specific actions at a scope.

To create and remove role assignments, users must have `Microsoft.Authorization/roleAssignments/*` access. This access is granted through the Owner or User Access Administrator roles.

For managing virtual machine solutions, there are three resource-specific roles that provide commonly needed

access:

- [Virtual Machine Contributor](#)
- [Network Contributor](#)
- [Storage Account Contributor](#)

Instead of assigning roles to individual users, it's often easier to use an Azure Active Directory group that has users who need to take similar actions. Then, assign that group to the appropriate role. For this article, either use an existing group for managing the virtual machine, or use the portal to [create an Azure Active Directory group](#).

After creating a new group or finding an existing one, use the [az role assignment create](#) command to assign the new Azure Active Directory group to the Virtual Machine Contributor role for the resource group.

```
adgroupId=$(az ad group show --group <your-group-name> --query objectId --output tsv)

az role assignment create --assignee-object-id $adgroupId --role "Virtual Machine Contributor" --resource-
group myResourceGroup
```

If you receive an error stating **Principal <guid> does not exist in the directory**, the new group hasn't propagated throughout Azure Active Directory. Try running the command again.

Typically, you repeat the process for *Network Contributor* and *Storage Account Contributor* to make sure users are assigned to manage the deployed resources. In this article, you can skip those steps.

Azure Policy

[Azure Policy](#) helps you make sure all resources in subscription meet corporate standards. Your subscription already has several policy definitions. To see the available policy definitions, use the [az policy definition list](#) command:

```
az policy definition list --query "[].[displayName, policyType, name]" --output table
```

You see the existing policy definitions. The policy type is either **BuiltIn** or **Custom**. Look through the definitions for ones that describe a condition you want assign. In this article, you assign policies that:

- Limit the locations for all resources.
- Limit the SKUs for virtual machines.
- Audit virtual machines that don't use managed disks.

In the following example, you retrieve three policy definitions based on the display name. You use the [az policy assignment create](#) command to assign those definitions to the resource group. For some policies, you provide parameter values to specify the allowed values.

```

# Get policy definitions for allowed locations, allowed SKUs, and auditing VMs that don't use managed disks
locationDefinition=$(az policy definition list --query "[?displayName=='Allowed locations'].name | [0]" --output tsv)
skuDefinition=$(az policy definition list --query "[?displayName=='Allowed virtual machine SKUs'].name | [0]" --output tsv)
auditDefinition=$(az policy definition list --query "[?displayName=='Audit VMs that do not use managed disks'].name | [0]" --output tsv)

# Assign policy for allowed locations
az policy assignment create --name "Set permitted locations" \
--resource-group myResourceGroup \
--policy $locationDefinition \
--params '{
    "listOfAllowedLocations": {
        "value": [
            "eastus",
            "eastus2"
        ]
    }
}'

# Assign policy for allowed SKUs
az policy assignment create --name "Set permitted VM SKUs" \
--resource-group myResourceGroup \
--policy $skuDefinition \
--params '{
    "listOfAllowedSKUs": {
        "value": [
            "Standard_DS1_v2",
            "Standard_E2s_v2"
        ]
    }
}'

# Assign policy for auditing unmanaged disks
az policy assignment create --name "Audit unmanaged disks" \
--resource-group myResourceGroup \
--policy $auditDefinition

```

The preceding example assumes you already know the parameters for a policy. If you need to view the parameters, use:

```
az policy definition show --name $locationDefinition --query parameters
```

Deploy the virtual machine

You have assigned roles and policies, so you're ready to deploy your solution. The default size is Standard_DS1_v2, which is one of your allowed SKUs. The command creates SSH keys if they don't exist in a default location.

```
az vm create --resource-group myResourceGroup --name myVM --image UbuntuLTS --generate-ssh-keys
```

After your deployment finishes, you can apply more management settings to the solution.

Lock resources

[Resource locks](#) prevent users in your organization from accidentally deleting or modifying critical resources. Unlike role-based access control, resource locks apply a restriction across all users and roles. You can set the lock level to *CanNotDelete* or *ReadOnly*.

To create or delete management locks, you must have access to `Microsoft.Authorization/locks/*` actions. Of the built-in roles, only **Owner** and **User Access Administrator** are granted those actions.

To lock the virtual machine and network security group, use the [az lock create](#) command:

```
# Add CanNotDelete lock to the VM
az lock create --name LockVM \
--lock-type CanNotDelete \
--resource-group myResourceGroup \
--resource-name myVM \
--resource-type Microsoft.Compute/virtualMachines

# Add CanNotDelete lock to the network security group
az lock create --name LockNSG \
--lock-type CanNotDelete \
--resource-group myResourceGroup \
--resource-name myVMNSG \
--resource-type Microsoft.Network/networkSecurityGroups
```

To test the locks, try running the following command:

```
az group delete --name myResourceGroup
```

You see an error stating that the delete operation can't be completed because of a lock. The resource group can only be deleted if you specifically remove the locks. That step is shown in [Clean up resources](#).

Tag resources

You apply [tags](#) to your Azure resources to logically organize them by categories. Each tag consists of a name and a value. For example, you can apply the name "Environment" and the value "Production" to all the resources in production.

To add two tags to a resource group, use the [az group update](#) command:

```
az group update -n myResourceGroup --set tags.Environment=Test tags.Dept=IT
```

Let's suppose you want to add a third tag. Run the command again with the new tag. It is appended to the existing tags.

```
az group update -n myResourceGroup --set tags.Project=Documentation
```

Resources don't inherit tags from the resource group. Currently, your resource group has three tags but the resources do not have any tags. To apply all tags from a resource group to its resources, and retain existing tags on resources, use the following script:

```

# Get the tags for the resource group
jsontag=$(az group show -n myResourceGroup --query tags)

# Reformat from JSON to space-delimited and equals sign
t=$(echo $jsontag | tr -d '"{},' | sed 's/: /=g')

# Get the resource IDs for all resources in the resource group
r=$(az resource list -g myResourceGroup --query [].id --output tsv)

# Loop through each resource ID
for resid in $r
do
    # Get the tags for this resource
    jsonrtag=$(az resource show --id $resid --query tags)

    # Reformat from JSON to space-delimited and equals sign
    rt=$(echo $jsonrtag | tr -d '"{},' | sed 's/: /=g')

    # Reapply the updated tags to this resource
    az resource tag --tags $t$rt --id $resid
done

```

Alternatively, you can apply tags from the resource group to the resources without keeping the existing tags:

```

# Get the tags for the resource group
jsontag=$(az group show -n myResourceGroup --query tags)

# Reformat from JSON to space-delimited and equals sign
t=$(echo $jsontag | tr -d '"{},' | sed 's/: /=g')

# Get the resource IDs for all resources in the resource group
r=$(az resource list -g myResourceGroup --query [].id --output tsv)

# Loop through each resource ID
for resid in $r
do
    # Apply tags from resource group to this resource
    az resource tag --tags $t --id $resid
done

```

To combine several values in a single tag, use a JSON string.

```
az group update -n myResourceGroup --set tags.CostCenter='{"Dept":"IT","Environment":"Test"}'
```

To remove all tags on a resource group, use:

```
az group update -n myResourceGroup --remove tags
```

To apply tags to a virtual machine, use the [az resource tag](#) command. Any existing tags on the resource aren't retained.

```
az resource tag -n myVM \
-g myResourceGroup \
--tags Dept=IT Environment=Test Project=Documentation \
--resource-type "Microsoft.Compute/virtualMachines"
```

Find resources by tag

To find resources with a tag name and value, use the [az resource list](#) command:

```
az resource list --tag Environment=Test --query [].name
```

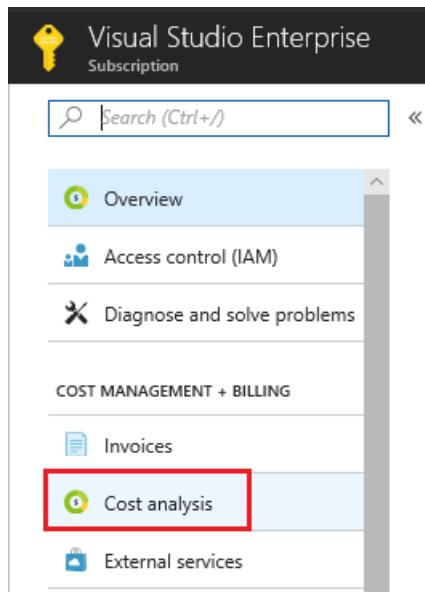
You can use the returned values for management tasks like stopping all virtual machines with a tag value.

```
az vm stop --ids $(az resource list --tag Environment=Test --query "[? type=='Microsoft.Compute/virtualMachines'].id" --output tsv)
```

View costs by tag values

After applying tags to resources, you can view costs for resources with those tags. It takes a while for cost analysis to show the latest usage, so you may not see the costs yet. When the costs are available, you can view costs for resources across resource groups in your subscription. Users must have [subscription level access to billing information](#) to see the costs.

To view costs by tag in the portal, select your subscription and select **Cost Analysis**.



Then, filter by the tag value, and select **Apply**.

A screenshot of the "Costs by service" blade in the Azure portal. It shows the following fields: Subscription (Visual Studio Enterprise), Resource type (3 selected), Resource group (2 selected). Under "Timespan" is "Current period". There are "Apply" and "Download" buttons. A note says: "There is a delay between the time when reported here may be delayed. Amount reaches the billing system. Due to this, costs me recent usage. Taxes are not included." On the left, there's a "Total cost" of "0.24 USD". A "Tag" dropdown is open, showing a list of tags: "Environment: Test" (selected), "Select all", "Project: Documentation", "Dept: IT", "-- No Tags --". A tooltip for "Environment: Test" says: "reaches the billing system. Due to this, costs me recent usage. Taxes are not included."

You can also use the [Azure Billing APIs](#) to programmatically view costs.

Clean up resources

The locked network security group can't be deleted until the lock is removed. To remove the lock, retrieve the IDs

of the locks and provide them to the [az lock delete](#) command:

```
vmlock=$(az lock show --name LockVM \
--resource-group myResourceGroup \
--resource-type Microsoft.Compute/virtualMachines \
--resource-name myVM --output tsv --query id)
nsglock=$(az lock show --name LockNSG \
--resource-group myResourceGroup \
--resource-type Microsoft.Network/networkSecurityGroups \
--resource-name myVMNSG --output tsv --query id)
az lock delete --ids $vmlock $nsglock
```

When no longer needed, you can use the [az group delete](#) command to remove the resource group, VM, and all related resources. Exit the SSH session to your VM, then delete the resources as follows:

```
az group delete --name myResourceGroup
```

Next steps

In this tutorial, you created a custom VM image. You learned how to:

- Assign users to a role
- Apply policies that enforce standards
- Protect critical resources with locks
- Tag resources for billing and management

Advance to the next tutorial to learn how to identify changes and manage package updates on a virtual machine.

[Manage virtual machines](#)

Tutorial: Monitor changes and update a Linux virtual machine in Azure

11/13/2019 • 9 minutes to read • [Edit Online](#)

Azure [Change Tracking](#) allows you to easily identify changes and [Update Management](#) allows you to manage operating system updates for your Azure Linux VMs.

In this tutorial, you learn how to:

- Manage Windows updates
- Monitor changes and inventory

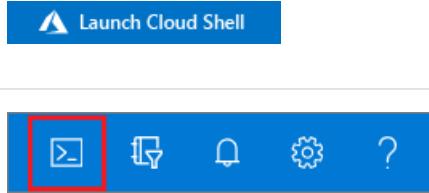
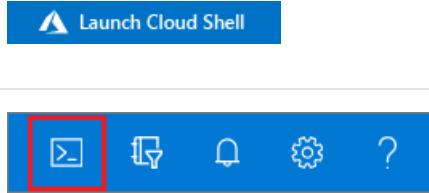
Launch Azure Cloud Shell

The Azure Cloud Shell is a free interactive shell that you can use to run the steps in this article. It has common Azure tools preinstalled and configured to use with your account.

Use Azure Cloud Shell

Azure hosts Azure Cloud Shell, an interactive shell environment that you can use through your browser. You can use either Bash or PowerShell with Cloud Shell to work with Azure services. You can use the Cloud Shell preinstalled commands to run the code in this article without having to install anything on your local environment.

To start Azure Cloud Shell:

OPTION	EXAMPLE/LINK
Select Try It in the upper-right corner of a code block. Selecting Try It doesn't automatically copy the code to Cloud Shell.	
Go to https://shell.azure.com , or select the Launch Cloud Shell button to open Cloud Shell in your browser.	
Select the Cloud Shell button on the menu bar at the upper right in the Azure portal .	

To run the code in this article in Azure Cloud Shell:

1. Start Cloud Shell.
2. Select the **Copy** button on a code block to copy the code.
3. Paste the code into the Cloud Shell session by selecting **Ctrl+Shift+V** on Windows and Linux or by selecting **Cmd+Shift+V** on macOS.
4. Select **Enter** to run the code.

If you choose to install and use the CLI locally, this tutorial requires that you are running the Azure CLI version 2.0.30 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Create VM

To see diagnostics and metrics in action, you need a VM. First, create a resource group with [az group create](#). The following example creates a resource group named *myResourceGroupMonitor* in the *eastus* location.

```
az group create --name myResourceGroupMonitor --location eastus
```

Now create a VM with [az vm create](#). The following example creates a VM named *myVM* and generates SSH keys if they do not already exist in *~/.ssh/*:

```
az vm create \
--resource-group myResourceGroupMonitor \
--name myVM \
--image UbuntuLTS \
--admin-username azureuser \
--generate-ssh-keys
```

Manage software updates

Update management allows you to manage updates and patches for your Azure Linux VMs. Directly from your VM, you can quickly assess the status of available updates, schedule installation of required updates, and review deployment results to verify updates were applied successfully to the VM.

For pricing information, see [Automation pricing for Update management](#)

Enable Update management

Enable Update management for your VM:

1. On the left-hand side of the screen, select **Virtual machines**.
2. From the list, select a VM.
3. On the VM screen, in the **Operations** section, select **Update management**. The **Enable Update Management** screen opens.

Validation is performed to determine if Update management is enabled for this VM. The validation includes checks for a Log Analytics workspace and linked Automation account, and if the solution is in the workspace.

A [Log Analytics](#) workspace is used to collect data that is generated by features and services such as Update management. The workspace provides a single location to review and analyze data from multiple sources. To perform additional actions on VMs that require updates, Azure Automation allows you to run runbooks against VMs, such as download and apply updates.

The validation process also checks to see if the VM is provisioned with the Log Analytics agent and Automation hybrid runbook worker. This agent is used to communicate with the VM and obtain information about the update status.

Choose the Log Analytics workspace and automation account and select **Enable** to enable the solution. The solution takes up to 15 minutes to enable.

If any of the following prerequisites were found to be missing during onboarding, they're automatically added:

- [Log Analytics workspace](#)
- [Automation account](#)
- A [Hybrid runbook worker](#) is enabled on the VM

The **Update Management** screen opens. Configure the location, Log Analytics workspace and Automation account to use and select **Enable**. If the fields are grayed out, that means another automation solution is enabled

for the VM and the same workspace and Automation account must be used.

Search (Ctrl+ /)

Automation script

OPERATIONS

- Auto-shutdown
- Backup
- Disaster recovery (Preview)
- Update management
- Inventory
- Change tracking

MONITORING

- Metrics
- Alert rules

Update Management

Enable consistent control and compliance of this VM with Update Management.

This service is included with Azure virtual 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.

Location ⓘ

East US

Log Analytics workspace ⓘ

defaultworkspace

Automation account ⓘ

Automate

Enable

Enabling the solution can take up to 15 minutes. During this time, you shouldn't close the browser window. After the solution is enabled, information about missing updates on the VM flows to Azure Monitor logs. It can take between 30 minutes and 6 hours for the data to be available for analysis.

View update assessment

After **Update management** is enabled, the **Update management** screen appears. After the evaluation of updates is complete, you see a list of missing updates on the **Missing updates** tab.

UPDATE NAME	CLASSIFICATION	INFORMATION LINK
apport	critical updates	
sudo	critical updates	
linux-firmware	critical updates	
dosfstools	security updates	
bash	security updates	
cpio	security updates	
curl	security updates	
patch	security updates	

Schedule an update deployment

To install updates, schedule a deployment that follows your release schedule and service window. You can choose which update types to include in the deployment. For example, you can include critical or security updates and exclude update rollups.

Schedule a new Update Deployment for the VM by clicking **Schedule update deployment** at the top of the

Update management screen. In the **New update deployment** screen, specify the following information:

To create a new update deployment, select **Schedule update deployment**. The **New update deployment** page opens. Enter values for the properties described in the following table and then click **Create**:

PROPERTY	DESCRIPTION
Name	Unique name to identify the update deployment.
Operating System	Linux or Windows
Groups to update	For Azure machines, define a query based on a combination of subscription, resource groups, locations, and tags to build a dynamic group of Azure VMs to include in your deployment. For Non-Azure machines, select an existing saved search to select a group of Non-Azure machines to include in the deployment. To learn more, see Dynamic Groups
Machines to update	Select a Saved search, Imported group, or pick Machine from the drop-down and select individual machines. If you choose Machines , the readiness of the machine is shown in the UPDATE AGENT READINESS column. To learn about the different methods of creating computer groups in Azure Monitor logs, see Computer groups in Azure Monitor logs
Update classifications	Select all the update classifications that you need
Include/exclude updates	This opens the Include/Exclude page. Updates to be included or excluded are on separate tabs. For more information on how inclusion is handled, see Schedule an Update Deployment
Schedule settings	Select the time to start, and select either Once or recurring for the recurrence
Pre-scripts + Post-scripts	Select the scripts to run before and after your deployment
Maintenance window	Number of minutes set for updates. The value can't be less than 30 minutes and no more than 6 hours
Reboot control	Determines how reboots should be handled. Available options are: Reboot if required (Default) Always reboot Never reboot Only reboot - will not install updates

Update Deployments can also be created programmatically. To learn how to create an Update Deployment with the REST API, see [Software Update Configurations - Create](#). There is also a sample runbook that can be used to create a weekly Update Deployment. To learn more about this runbook, see [Create a weekly update deployment for one or more VMs in a resource group](#).

After you have completed configuring the schedule, click **Create** button and you return to the status dashboard. Notice that the **Scheduled** table shows the deployment schedule you created.

View results of an update deployment

After the scheduled deployment starts, you can see the status for that deployment on the **Update deployments** tab on the **Update management** screen. If it is currently running, its status shows as **In progress**. After it completes, if successful, it changes to **Succeeded**. If there is a failure with one or more updates in the deployment, the status is **Partially failed**. Select the completed update deployment to see the dashboard for that update deployment.

The screenshot shows the Update management dashboard for a VM named Marketing10. At the top, it displays deployment details: Status (Succeeded), Start time (5/20/2019, 8:24:33 AM), and End time (5/20/2019, 8:55:53 AM). Below this, the 'Update results' section includes a donut chart showing 89 Updates (89 Succeeded, 0 Failed, 0 Not attempted, 0 Not selected) and a table of update names and their statuses (all succeeded). The 'Diagnostics and Logs' section includes tabs for All Logs, Output, and Errors, with 0 errors indicated.

In **Update results** tile is a summary of the total number of updates and deployment results on the VM. In the table to the right is a detailed breakdown of each update and the installation results, which could be one of the following values:

- **Not attempted** - the update was not installed because there was insufficient time available based on the maintenance window duration defined.
- **Succeeded** - the update succeeded
- **Failed** - the update failed

Select **All logs** to see all log entries that the deployment created.

Select the **Output** tile to see job stream of the runbook responsible for managing the update deployment on the target VM.

Select **Errors** to see detailed information about any errors from the deployment.

Monitor changes and inventory

You can collect and view inventory for software, files, Linux daemons, Windows Services, and Windows registry keys on your computers. Tracking the configurations of your machines can help you pinpoint operational issues across your environment and better understand the state of your machines.

Enable Change and Inventory management

Enable Change and Inventory management for your VM:

1. On the left-hand side of the screen, select **Virtual machines**.
2. From the list, select a VM.
3. On the VM screen, in the **Operations** section, select **Inventory** or **Change tracking**. The **Enable Change Tracking and Inventory** screen opens.

Configure the location, Log Analytics workspace and Automation account to use and select **Enable**. If the fields are grayed out, that means another automation solution is enabled for the VM and the same workspace and Automation account must be used. Even though the solutions are separate on the menu, they are the same

solution. Enabling one enables both for your VM.

Home > Resource groups > myResourceGroupMonitor > myVM - Inventory

myVM - Inventory

Virtual machine

Search (Ctrl+ /)

Auto-shutdown

Backup

Disaster recovery (Preview)

Update management

Inventory

Change tracking

MONITORING

Metrics

Alert rules

Diagnostics settings

Advisor recommendations

Diagram

Inventory

Enable consistent control and compliance of this VM with Change Tracking and Inventory.

This service is included with Azure virtual 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.

Location: East US

Log Analytics workspace: defaultworkspace

Automation account: Automate

Enable

After the solution has been enabled, it may take some time while inventory is being collected on the VM before data appears.

Track changes

On your VM, select **Change Tracking** under **OPERATIONS**. Select **Edit Settings**, the **Change Tracking** page is displayed. Select the type of setting you want to track and then select **+ Add** to configure the settings. The available option Linux is **Linux Files**

For detailed information on Change Tracking see, [Troubleshoot changes on a VM](#)

View inventory

On your VM, select **Inventory** under **OPERATIONS**. On the **Software** tab, there is a table list the software that had been found. The high-level details for each software record are viewable in the table. These details include the software name, version, publisher, last refreshed time.

New software 7 Last 24 hours

Learn more
Inventory
Provide feedback

Software Files Linux Daemons

Search to filter items...

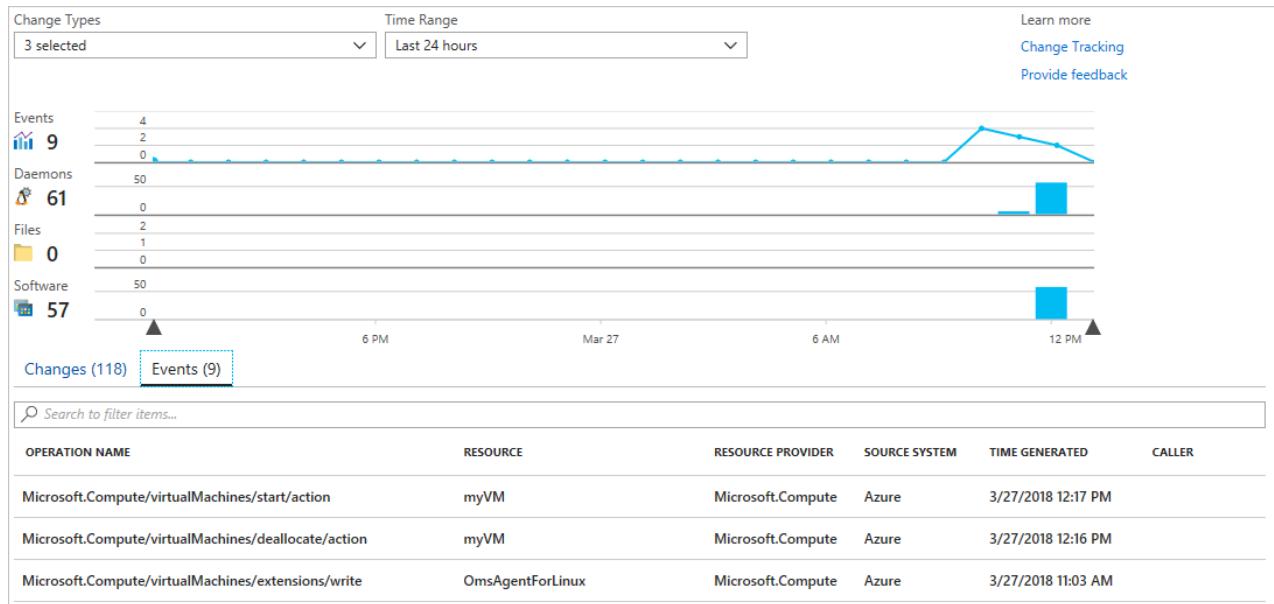
NAME	VERSION	PUBLISHER	LAST REFRESHED TIME
accountsservice	0.6.40-2ubuntu11.3	Ubuntu Developers <ubun...	3/27/2018 11:51 AM
acl	2.2.52-3	Ubuntu Developers <ubun...	3/27/2018 11:51 AM
acpid	1:2.0.26-1ubuntu2	Ubuntu Developers <ubun...	3/27/2018 11:51 AM
adduser	3.113+nmu3ubuntu4	Ubuntu Core Developers <...	3/27/2018 11:51 AM
apparmor	2.10.95-0ubuntu2.8	Ubuntu Developers <ubun...	3/27/2018 11:51 AM
apport	2.20.1-0ubuntu2.15	Martin Pitt <martin.pitt@u...	3/27/2018 11:51 AM
apport-symptoms	0.20	Ubuntu Developers <ubun...	3/27/2018 11:51 AM
apt	1.2.25	Ubuntu Developers <ubun...	3/27/2018 11:51 AM

Monitor Activity logs and changes

From the **Change tracking** page on your VM, select **Manage Activity Log Connection**. This task opens the **Azure Activity log** page. Select **Connect** to connect Change tracking to the Azure activity log for your VM.

With this setting enabled, navigate to the **Overview** page for your VM and select **Stop** to stop your VM. When prompted, select **Yes** to stop the VM. When it is deallocated, select **Start** to restart your VM.

Stopping and starting a VM logs an event in its activity log. Navigate back to the **Change tracking** page. Select the **Events** tab at the bottom of the page. After a while, the events shown in the chart and the table. Each event can be selected to view detailed information on the event.



The chart shows changes that have occurred over time. After you have added an Activity Log connection, the line graph at the top displays Azure Activity Log events. Each row of bar graphs represents a different trackable Change type. These types are Linux daemons, files, and software. The change tab shows the details for the changes shown in the visualization in descending order of time that the change occurred (most recent first).

Next steps

In this tutorial, you configured and reviewed Change Tracking and Update Management for your VM. You learned how to:

- Create a resource group and VM
- Manage Linux updates
- Monitor changes and inventory

Advance to the next tutorial to learn about monitoring your VM.

[Monitor virtual machines](#)

Tutorial: Monitor a Linux virtual machine in Azure

1/8/2020 • 5 minutes to read • [Edit Online](#)

Azure monitoring uses agents to collect boot and performance data from Azure VMs, store this data in Azure storage, and make it accessible through portal, the Azure PowerShell module, and Azure CLI. Advanced monitoring is delivered with Azure Monitor for VMs by collecting performance metrics, discover application components installed on the VM, and includes performance charts and dependency map.

In this tutorial, you learn how to:

- Enable boot diagnostics on a VM
- View boot diagnostics
- View VM host metrics
- Enable Azure Monitor for VMs
- View VM performance metrics
- Create an alert

Launch Azure Cloud Shell

The Azure Cloud Shell is a free interactive shell that you can use to run the steps in this article. It has common Azure tools preinstalled and configured to use with your account.

To open the Cloud Shell, just select **Try it** from the upper right corner of a code block. You can also launch Cloud Shell in a separate browser tab by going to <https://shell.azure.com/powershell>. Select **Copy** to copy the blocks of code, paste it into the Cloud Shell, and press enter to run it.

If you choose to install and use the CLI locally, this tutorial requires that you are running the Azure CLI version 2.0.30 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install the Azure CLI](#).

Create VM

To see diagnostics and metrics in action, you need a VM. First, create a resource group with [az group create](#). The following example creates a resource group named *myResourceGroupMonitor* in the *eastus* location.

```
az group create --name myResourceGroupMonitor --location eastus
```

Now create a VM with [az vm create](#). The following example creates a VM named *myVM* and generates SSH keys if they do not already exist in *~/ssh/*:

```
az vm create \
  --resource-group myResourceGroupMonitor \
  --name myVM \
  --image UbuntuLTS \
  --admin-username azureuser \
  --generate-ssh-keys
```

Enable boot diagnostics

As Linux VMs boot, the boot diagnostic extension captures boot output and stores it in Azure storage. This data can be used to troubleshoot VM boot issues. Boot diagnostics are not automatically enabled when you create a

Linux VM using the Azure CLI.

Before enabling boot diagnostics, a storage account needs to be created for storing boot logs. Storage accounts must have a globally unique name, be between 3 and 24 characters, and must contain only numbers and lowercase letters. Create a storage account with the [az storage account create](#) command. In this example, a random string is used to create a unique storage account name.

```
storageacct=mydiagdata$RANDOM

az storage account create \
--resource-group myResourceGroupMonitor \
--name $storageacct \
--sku Standard_LRS \
--location eastus
```

When enabling boot diagnostics, the URI to the blob storage container is needed. The following command queries the storage account to return this URI. The URI value is stored in a variable names *bloburi*, which is used in the next step.

```
bloburi=$(az storage account show --resource-group myResourceGroupMonitor --name $storageacct --query
'primaryEndpoints.blob' -o tsv)
```

Now enable boot diagnostics with [az vm boot-diagnostics enable](#). The `--storage` value is the blob URI collected in the previous step.

```
az vm boot-diagnostics enable \
--resource-group myResourceGroupMonitor \
--name myVM \
--storage $bloburi
```

View boot diagnostics

When boot diagnostics are enabled, each time you stop and start the VM, information about the boot process is written to a log file. For this example, first deallocate the VM with the [az vm deallocate](#) command as follows:

```
az vm deallocate --resource-group myResourceGroupMonitor --name myVM
```

Now start the VM with the [az vm start](#) command as follows:

```
az vm start --resource-group myResourceGroupMonitor --name myVM
```

You can get the boot diagnostic data for *myVM* with the [az vm boot-diagnostics get-boot-log](#) command as follows:

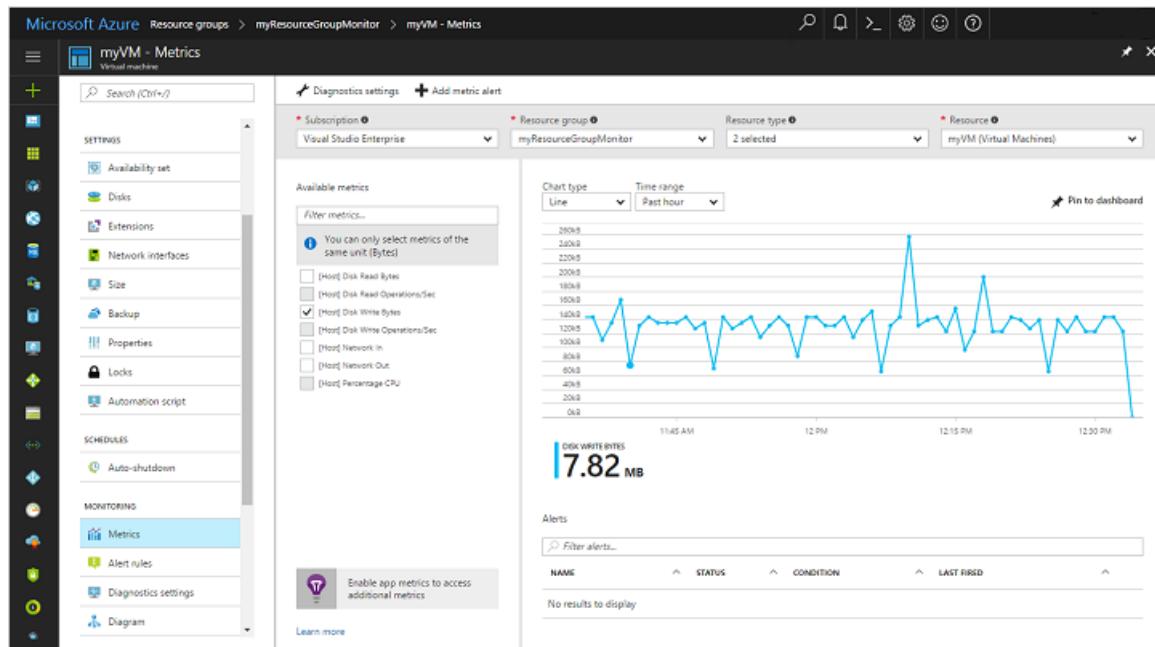
```
az vm boot-diagnostics get-boot-log --resource-group myResourceGroupMonitor --name myVM
```

View host metrics

A Linux VM has a dedicated host in Azure that it interacts with. Metrics are automatically collected for the host and can be viewed in the Azure portal as follows:

1. In the Azure portal, select **Resource Groups**, choose **myResourceGroupMonitor**, and then select **myVM** in the resource list.

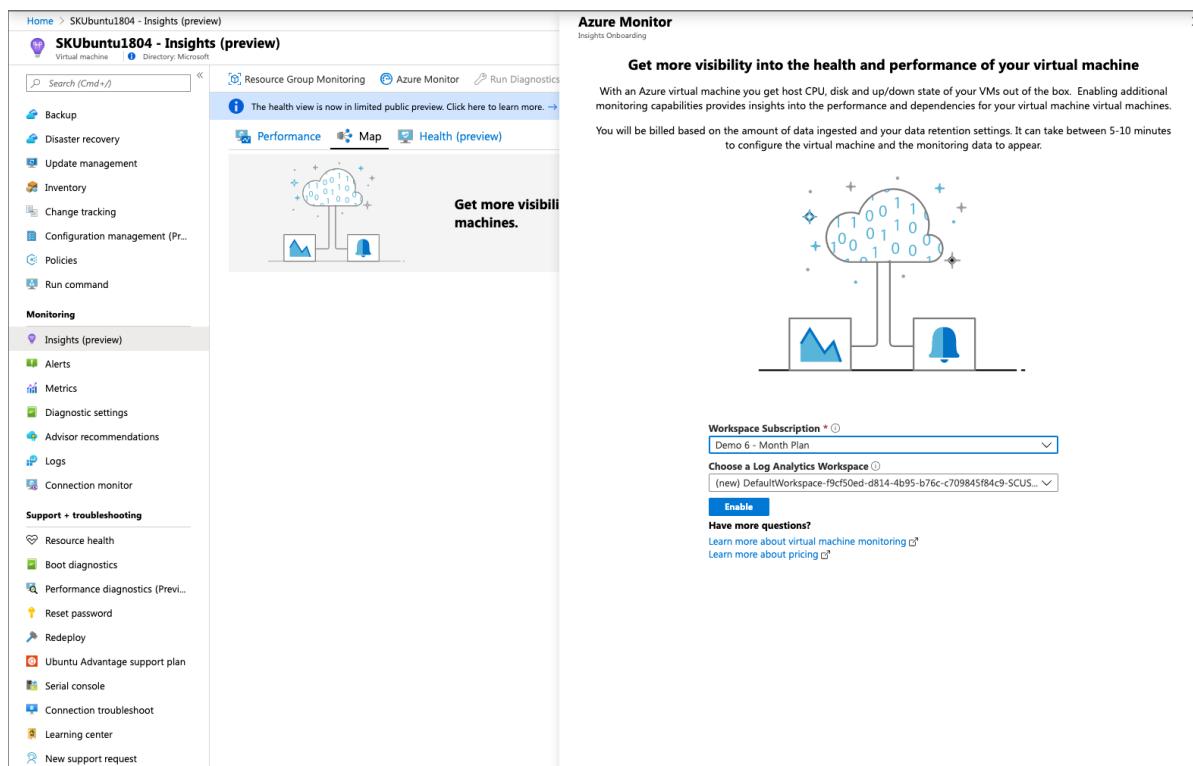
- To see how the host VM is performing, select **Metrics** on the VM window, then choose any of the [Host] metrics under **Available metrics**.



Enable advanced monitoring

To enable monitoring of your Azure VM with Azure Monitor for VMs:

- In the Azure portal, click **Resource Groups**, select **myResourceGroupMonitor**, and then select **myVM** in the resource list.
- On the VM page, in the **Monitoring** section, select **Insights (preview)**.
- On the **Insights (preview)** page, select **Try now**.



- On the **Azure Monitor Insights Onboarding** page, if you have an existing Log Analytics workspace in the same subscription, select it in the drop-down list.

The list preselects the default workspace and location where the VM is deployed in the subscription.

NOTE

To create a new Log Analytics workspace to store the monitoring data from the VM, see [Create a Log Analytics workspace](#). Your Log Analytics workspace must belong to one of the [supported regions](#).

After you've enabled monitoring, you might need to wait several minutes before you can view the performance metrics for the VM.

 Monitoring data is being collected and routed to Insights. It can take up to 10 minutes to arrive. Please try again in a few minutes.

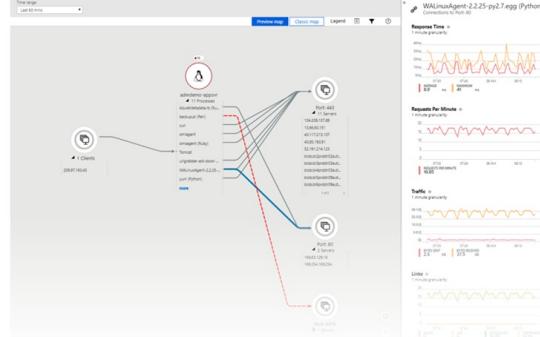
AZURE MONITOR

 Get more visibility into the health and performance of your virtual machines

With an Azure virtual machine you get host CPU, disk and up/down state of your virtual machine out of the box. Enabling additional monitoring capabilities provides insights into the performance, topology, and health for the single VM and across your entire fleet of virtual machines.

You will be billed based on the amount of data ingested and your data retention settings. It can take between 5-10 minutes to get data into virtual machine health and insights.

Have more questions?
[Learn more about virtual machine health and performance monitoring](#) 
[Learn more about pricing](#) 



View VM performance metrics

Azure Monitor for VMs includes a set of performance charts that target several key performance indicators (KPIs) to help you determine how well a virtual machine is performing. To access from your VM, perform the following steps.

1. In the Azure portal, click **Resource Groups**, select **myResourceGroupMonitor**, and then select **myVM** in the resource list.
2. On the VM page, in the **Monitoring** section, select **Insights (preview)**.
3. Select the **Performance** tab.

This page not only includes performance utilization charts, but also a table showing for each logical disk discovered, its capacity, utilization, and total average by each measure.

Create alerts

You can create alerts based on specific performance metrics. Alerts can be used to notify you when average CPU usage exceeds a certain threshold or available free disk space drops below a certain amount, for example. Alerts are displayed in the Azure portal or can be sent via email. You can also trigger Azure Automation runbooks or Azure Logic Apps in response to alerts being generated.

The following example creates an alert for average CPU usage.

1. In the Azure portal, click **Resource Groups**, select **myResourceGroupMonitor**, and then select **myVM** in the resource list.
2. Click **Alert rules** on the VM blade, then click **Add metric alert** across the top of the alerts blade.
3. Provide a **Name** for your alert, such as *myAlertRule*
4. To trigger an alert when CPU percentage exceeds 1.0 for five minutes, leave all the other defaults selected.

5. Optionally, check the box for *Email owners, contributors, and readers* to send email notification. The default action is to present a notification in the portal.
6. Click the **OK** button.

Next steps

In this tutorial, you configured and viewed performance of your VM. You learned how to:

- Create a resource group and VM
- Enable boot diagnostics on the VM
- View boot diagnostics
- View host metrics
- Enable Azure Monitor for VMs
- View VM metrics
- Create an alert

Advance to the next tutorial to learn about Azure Security Center.

[Manage VM security](#)

Tutorial: Use Azure Security Center to monitor Linux virtual machines

2/25/2020 • 4 minutes to read • [Edit Online](#)

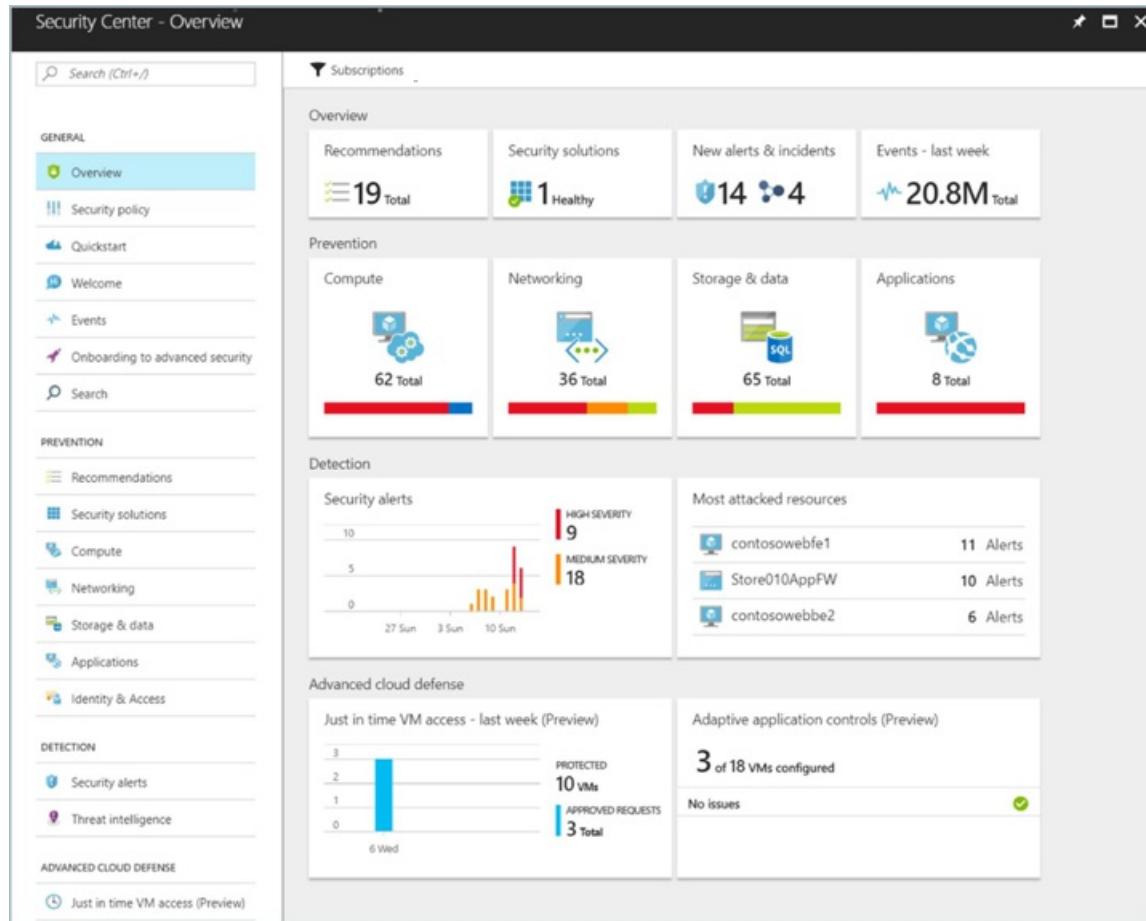
Azure Security Center can help you gain visibility into your Azure resource security practices. Security Center offers integrated security monitoring. It can detect threats that otherwise might go unnoticed. In this tutorial, you learn about Azure Security Center, and how to:

- Set up data collection
- Set up security policies
- View and fix configuration health issues
- Review detected threats

Security Center overview

Security Center identifies potential virtual machine (VM) configuration issues and targeted security threats. These might include VMs that are missing network security groups, unencrypted disks, and brute-force Remote Desktop Protocol (RDP) attacks. The information is shown on the Security Center dashboard in easy-to-read graphs.

To access the Security Center dashboard, in the Azure portal, on the menu, select **Security Center**. On the dashboard, you can see the security health of your Azure environment, find a count of current recommendations, and view the current state of threat alerts. You can expand each high-level chart to see more detail.



Security Center goes beyond data discovery to provide recommendations for issues that it detects. For example, if a VM was deployed without an attached network security group, Security Center displays a recommendation, with

remediation steps you can take. You get automated remediation without leaving the context of Security Center.

Recommendations					X
Filter					
Description	Resource	State	Severity		
Install Endpoint Protection	2016OMSAA	Open	! High	...	
Add a Next Generation Firewall	2 endpoints	Open	! High	...	
Enable Network Security Groups on sub...	2 subnets	Open	! High	...	
Apply disk encryption	3 virtual mac...	Open	! High	...	
Enable encryption for Azure Storage Acc...	9 storage acc...	Open	! High	...	
Restrict access through Internet facing e...	2 virtual mac...	Open	⚠ Medium	...	
Add a vulnerability assessment solution	2016OMSAA	Open	⚠ Medium	...	
Remediate OS vulnerabilities (by Micros...	2016OMSLin...	Open	ℹ Low	...	

Set up data collection

Before you can get visibility into VM security configurations, you need to set up Security Center data collection. This involves turning on data collection which automatically installs the Microsoft Monitoring Agent on all the VMs in your subscription.

1. On the Security Center dashboard, click **Security policy**, and then select your subscription.
2. For **Data collection**, in **Auto Provisioning** select **On**.
3. For **Default workspace configuration** leave it as **Use workspace(s) created by Security Center (default)**.
4. Under **Security Events** keep the default option of **Common**.
5. Click **Save** at the top of the page.

The Security Center data collection agent is then installed on all VMs, and data collection begins.

Set up a security policy

Security policies are used to define the items for which Security Center collects data and makes recommendations. You can apply different security policies to different sets of Azure resources. Although by default Azure resources are evaluated against all policy items, you can turn off individual policy items for all Azure resources or for a resource group. For in-depth information about Security Center security policies, see [Set security policies in Azure Security Center](#).

To set up a security policy for an entire subscription:

1. On the Security Center dashboard, select **Security policy** and then select your subscription.
2. On the **Security policy** blade, select **Security policy**.
3. On the **Security policy - Security policy** blade, turn on or turn off policy items that you want to apply to the subscription.
4. When you're finished selecting your settings, select **Save** at the top of the blade.

Search (Ctrl+ /) Save

POLICY COMPONENTS

- Data Collection
- Security policy**
- Email notifications
- Pricing tier

Show recommendations for

System updates <small>i</small>	On	Off	
Security configurations <small>i</small>	On	Off	
Endpoint protection <small>i</small>	On	Off	
Disk encryption	On	Off	
Network security groups	On	Off	
Web application firewall	On	Off	
Next generation firewall	On	Off	
Vulnerability Assessment	On	Off	
Storage Encryption	On	Off	
JIT Network Access	On	Off	UPGRADE
Adaptive Application Controls	On	Off	UPGRADE
SQL auditing & Threat detection	On	Off	
SQL Encryption	On	Off	

View VM configuration health

After you've turned on data collection and set a security policy, Security Center begins to provide alerts and recommendations. As VMs are deployed, the data collection agent is installed. Security Center is then populated with data for the new VMs. For in-depth information about VM configuration health, see [Protect your VMs in Security Center](#).

As data is collected, the resource health for each VM and related Azure resource is aggregated. The information is shown in an easy-to-read chart.

To view resource health:

1. On the Security Center dashboard, under **Prevention**, select **Compute**.
2. On the **Compute** blade, select **VMs and computers**. This view provides a summary of the configuration status for all your VMs.

The screenshot shows the Azure Security Center Compute dashboard. At the top, there are three navigation tabs: 'Overview' (with a bar chart icon), 'VMs and computers' (with a computer monitor icon), and 'Cloud services' (with a cloud icon). Below the tabs, a message says 'Filtered By: Power State: Running'. A search bar is followed by a table with columns: NAME, MONITORED, SYSTEM UPDATES, ENDPOINT PROTECT..., VULNERABILITIES, and DISK ENCRYPTION. The table lists four VMs: myVM, BackEnd, Database, and FrontEnd. Each row has a red status bar at the bottom.

NAME	MONITORED	SYSTEM UPDATES	ENDPOINT PROTECT...	VULNERABILITIES	DISK ENCRYPTION
myVM	✓	!	✓	⚠	!
BackEnd	✓	✓	✓	⚠	!
Database	✓	✓	✓	⚠	!
FrontEnd	✓	✓	✓	⚠	!

To see all recommendations for a VM, select the VM.

Remediate configuration issues

After Security Center begins to populate with configuration data, recommendations are made based on the security policy you set up. For instance, if a VM was set up without an associated network security group, a recommendation is made to create one.

To see a list of all recommendations:

1. On the Security Center dashboard, select **Recommendations**.
2. Select a specific recommendation. A list of all resources for which the recommendation applies appears.
3. To apply a recommendation, select the resource.
4. Follow the instructions for remediation steps.

In many cases, Security Center provides actionable steps you can take to address a recommendation without leaving Security Center. In the following example, Security Center detects a network security group that has an unrestricted inbound rule. On the recommendation page, you can select the **Edit inbound rules** button. The UI that is needed to modify the rule appears.

The screenshot shows the 'Edit inbound rules' dialog for the 'FrontEnd' VM. It has two main sections: 'Network security group info' and 'Related inbound rules'.

Network security group info:

- NETWORK SECURITY GROUP: FrontEnd
- LOCATION: eastus
- DESCRIPTION: Your NSG has inbound rules that open access to 'Any' or 'Internet' which might enable attackers to access your resources. We recommend that you edit the below inbound rules to restrict access to a specified set of sources.

Related inbound rules:

PRIORITY	NAME	SOURCE	SERVICE	ACTIONS
1000	FrontEnd3389	*	Tcp	Allow
1001	FrontEnd5985	*	Tcp	Allow

Associated with:

NAME	VIRTUAL MACHINE
FrontEnd	FrontEnd

As recommendations are remediated, they are marked as resolved.

View detected threats

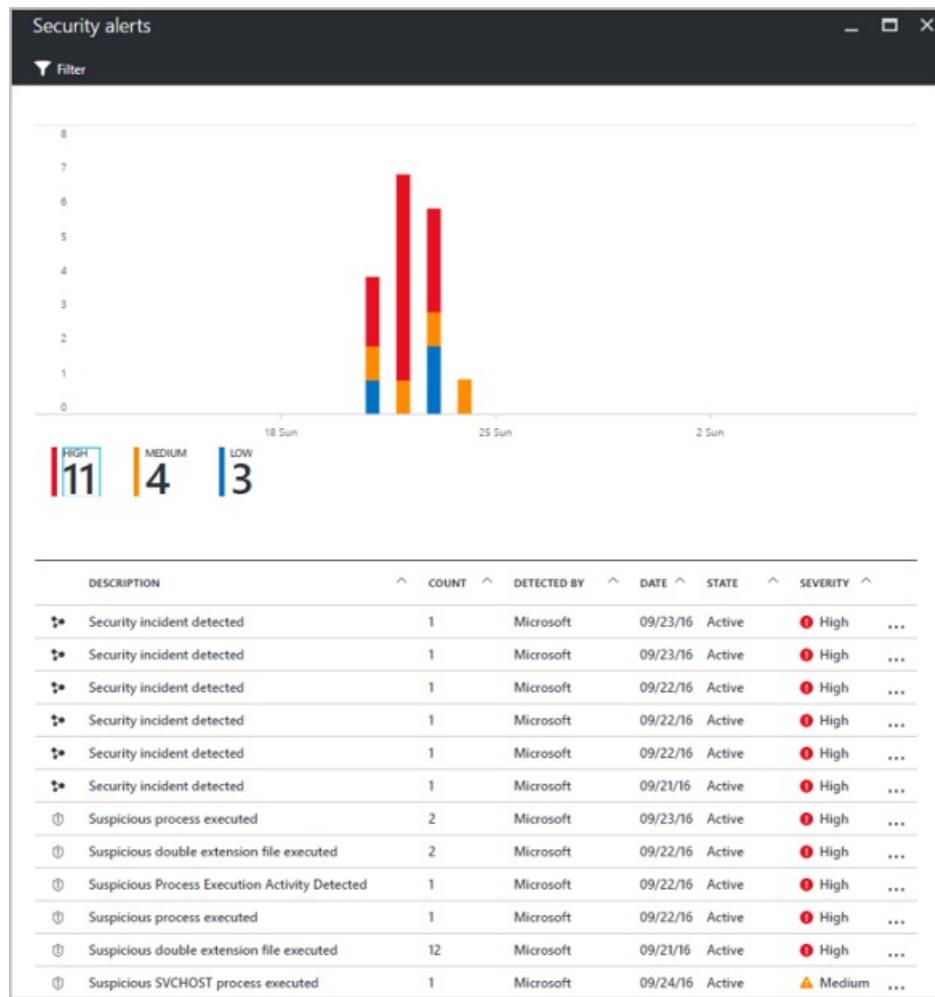
In addition to resource configuration recommendations, Security Center displays threat detection alerts. The security alerts feature aggregates data collected from each VM, Azure networking logs, and connected partner solutions to detect security threats against Azure resources. For in-depth information about Security Center threat detection capabilities, see [How does Security Center detect threats?](#).

The security alerts feature requires the Security Center pricing tier to be increased from *Free* to *Standard*. A **free trial** is available when you move to this higher pricing tier.

To change the pricing tier:

1. On the Security Center dashboard, click **Security policy**, and then select your subscription.
2. Select **Pricing tier**.
3. Select **Standard** and then click **Save** at the top of the blade.

After you've changed the pricing tier, the security alerts graph begins to populate as security threats are detected.



Select an alert to view information. For example, you can see a description of the threat, the detection time, all threat attempts, and the recommended remediation. In the following example, an RDP brute-force attack was detected, with 294 failed RDP attempts. A recommended resolution is provided.

Failed RDP Brute Force Attack	
myVMWindows	
DESCRIPTION	Several Remote Desktop login attempts were detected from 5.9.57.202, none of them succeeded. Event logs analysis shows that in the last 59 minutes there were 198 failed attempts. Some of the failed login attempts aimed at 2 existing user(s).
DETECTION TIME	Saturday, April 29, 2017, 10:59:56 PM
SEVERITY	 Medium
STATE	Active
ATTACKED RESOURCE	myVMWindows
SUBSCRIPTION	Free Trial (248352d0-5fc9-4c2e-8db3-d8b3462a0020)
DETECTED BY	 Microsoft
ACTION TAKEN	Detected
ALERT START TIME (UTC)	04/30/2017 05:00:06
NON-EXISTENT USERS	97
SUCCESSFUL LOGINS	0
FAILED USER LOGONS	server, administrator
REPORTS	Report: RDP Brute Forcing
REMEDIATION STEPS	<ol style="list-style-type: none"> 1. If available, add the source IP to NSG block list for 24 hours (see https://azure.microsoft.com/en-us/documentation/articles/virtual-networks-nsg/) 2. Enforce the use of strong passwords and do not reuse them across multiple VMs and services (see http://windows.microsoft.com/en-us/Windows7/Tips-for-creating-strong-passwords-and-passphrases) 3. Create an allow list for RDP access in NSG (see https://azure.microsoft.com/en-us/documentation/articles/virtual-networks-nsg/)

Next steps

In this tutorial, you set up Azure Security Center, and then reviewed VMs in Security Center. You learned how to:

- Set up data collection
- Set up security policies
- View and fix configuration health issues
- Review detected threats

Advance to the next tutorial to learn more about creating a CI/CD pipeline with Jenkins, GitHub, and Docker.

[Create CI/CD infrastructure with Jenkins, GitHub, and Docker](#)

Tutorial: Create a development infrastructure on a Linux VM in Azure with Jenkins, GitHub, and Docker

2/25/2020 • 8 minutes to read • [Edit Online](#)

To automate the build and test phase of application development, you can use a continuous integration and deployment (CI/CD) pipeline. In this tutorial, you create a CI/CD pipeline on an Azure VM including how to:

- Create a Jenkins VM
- Install and configure Jenkins
- Create webhook integration between GitHub and Jenkins
- Create and trigger Jenkins build jobs from GitHub commits
- Create a Docker image for your app
- Verify GitHub commits build new Docker image and updates running app

This tutorial uses the CLI within the [Azure Cloud Shell](#), which is constantly updated to the latest version. To open the Cloud Shell, select **Try it** from the top of any code block.

If you choose to install and use the CLI locally, this tutorial requires that you are running the Azure CLI version 2.0.30 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Create Jenkins instance

In a previous tutorial on [How to customize a Linux virtual machine on first boot](#), you learned how to automate VM customization with cloud-init. This tutorial uses a cloud-init file to install Jenkins and Docker on a VM. Jenkins is a popular open-source automation server that integrates seamlessly with Azure to enable continuous integration (CI) and continuous delivery (CD). For more tutorials on how to use Jenkins, see the [Jenkins in Azure hub](#).

In your current shell, create a file named *cloud-init-jenkins.txt* and paste the following configuration. For example, create the file in the Cloud Shell not on your local machine. Enter `sensible-editor cloud-init-jenkins.txt` to create the file and see a list of available editors. Make sure that the whole cloud-init file is copied correctly, especially the first line:

```

#cloud-config
package_upgrade: true
write_files:
- path: /etc/systemd/system/docker.service.d/docker.conf
  content: |
    [Service]
    ExecStart=
    ExecStart=/usr/bin/dockerd
- path: /etc/docker/daemon.json
  content: |
  {
    "hosts": ["fd://", "tcp://127.0.0.1:2375"]
  }
runcmd:
- apt install openjdk-8-jre-headless -y
- wget -q -O - https://pkg.jenkins.io/debian/jenkins-ci.org.key | sudo apt-key add -
- sh -c 'echo deb https://pkg.jenkins.io/debian-stable binary/ > /etc/apt/sources.list.d/jenkins.list'
- apt-get update && apt-get install jenkins -y
- curl -sSL https://get.docker.com/ | sh
- usermod -AG docker azureuser
- usermod -AG docker jenkins
- service jenkins restart

```

Before you can create a VM, create a resource group with [az group create](#). The following example creates a resource group named *myResourceGroupJenkins* in the *eastus* location:

```
az group create --name myResourceGroupJenkins --location eastus
```

Now create a VM with [az vm create](#). Use the `--custom-data` parameter to pass in your cloud-init config file. Provide the full path to *cloud-init-jenkins.txt* if you saved the file outside of your present working directory.

```
az vm create --resource-group myResourceGroupJenkins \
--name myVM \
--image UbuntuLTS \
--admin-username azureuser \
--generate-ssh-keys \
--custom-data cloud-init-jenkins.txt
```

It takes a few minutes for the VM to be created and configured.

To allow web traffic to reach your VM, use [az vm open-port](#) to open port *8080* for Jenkins traffic and port *1337* for the Node.js app that is used to run a sample app:

```
az vm open-port --resource-group myResourceGroupJenkins --name myVM --port 8080 --priority 1001
az vm open-port --resource-group myResourceGroupJenkins --name myVM --port 1337 --priority 1002
```

Configure Jenkins

To access your Jenkins instance, obtain the public IP address of your VM:

```
az vm show --resource-group myResourceGroupJenkins --name myVM -d --query [publicIps] --o tsv
```

For security purposes, you need to enter the initial admin password that is stored in a text file on your VM to start the Jenkins install. Use the public IP address obtained in the previous step to SSH to your VM:

```
ssh azureuser@<publicIps>
```

Verify Jenkins is running using the `service` command:

```
$ service jenkins status
● jenkins.service - LSB: Start Jenkins at boot time
  Loaded: loaded (/etc/init.d/jenkins; generated)
  Active: active (exited) since Tue 2019-02-12 16:16:11 UTC; 55s ago
    Docs: man:systemd-sysv-generator(8)
   Tasks: 0 (limit: 4103)
  CGroup: /system.slice/jenkins.service

Feb 12 16:16:10 myVM systemd[1]: Starting LSB: Start Jenkins at boot time...
...
...
```

View the `initialAdminPassword` for your Jenkins install and copy it:

```
sudo cat /var/lib/jenkins/secrets/initialAdminPassword
```

If the file isn't available yet, wait a couple more minutes for cloud-init to complete the Jenkins and Docker install.

Now open a web browser and go to `http://<publicIps>:8080`. Complete the initial Jenkins setup as follows:

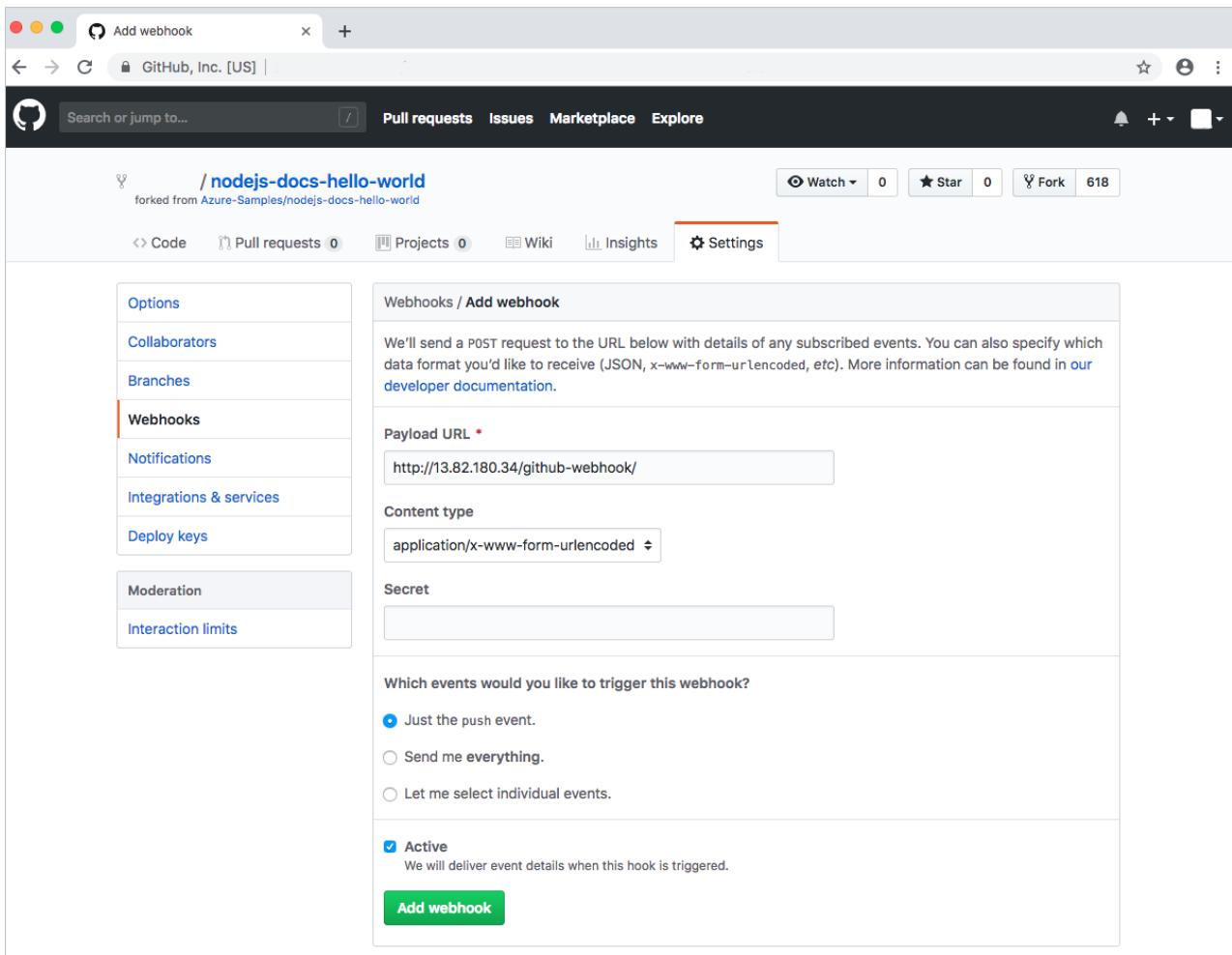
- Choose **Select plugins to install**
- Search for *GitHub* in the text box across the top. Check the box for *GitHub*, then select **Install**
- Create the first admin user. Enter a username, such as **admin**, then provide your own secure password. Finally, type a full name and e-mail address.
- Select **Save and Finish**
- Once Jenkins is ready, select **Start using Jenkins**
 - If your web browser displays a blank page when you start using Jenkins, restart the Jenkins service.
From your SSH session, type `sudo service jenkins restart`, then refresh your web browser.
- If needed, log in to Jenkins with the username and password you created.

Create GitHub webhook

To configure the integration with GitHub, open the [Node.js Hello World sample app](#) from the Azure samples repo. To fork the repo to your own GitHub account, select the **Fork** button in the top right-hand corner.

Create a webhook inside the fork you created:

- Select **Settings**, then select **Webhooks** on the left-hand side.
- Choose **Add webhook**, then enter *Jenkins* in filter box.
- For the **Payload URL**, enter `http://<publicIps>:8080/github-webhook/`. Make sure you include the trailing /
- For **Content type**, select *application/x-www-form-urlencoded*.
- For **Which events would you like to trigger this webhook?**, select *Just the push event*.
- Set **Active** to checked.
- Click **Add webhook**.



Create Jenkins job

To have Jenkins respond to an event in GitHub such as committing code, create a Jenkins job. Use the URLs for your own GitHub fork.

In your Jenkins website, select **Create new jobs** from the home page:

- Enter *HelloWorld* as job name. Choose **Freestyle project**, then select **OK**.
- Under the **General** section, select **GitHub project** and enter your forked repo URL, such as <https://github.com/cynthn/nodejs-docs-hello-world>
- Under the **Source code management** section, select **Git**, enter your forked repo .git URL, such as <https://github.com/cynthn/nodejs-docs-hello-world.git>
- Under the **Build Triggers** section, select **GitHub hook trigger for GITscm polling**.
- Under the **Build** section, choose **Add build step**. Select **Execute shell**, then enter `echo "Test"` in the command window.
- Select **Save** at the bottom of the jobs window.

Test GitHub integration

To test the GitHub integration with Jenkins, commit a change in your fork.

Back in GitHub web UI, select your forked repo, and then select the **index.js** file. Select the pencil icon to edit this file so line 6 reads:

```
response.end("Hello World!");
```

To commit your changes, select the **Commit changes** button at the bottom.

In Jenkins, a new build starts under the **Build history** section of the bottom left-hand corner of your job page. Choose the build number link and select **Console output** on the left-hand side. You can view the steps Jenkins takes as your code is pulled from GitHub and the build action outputs the message `Test` to the console. Each time a commit is made in GitHub, the webhook reaches out to Jenkins and triggers a new build in this way.

Define Docker build image

To see the Node.js app running based on your GitHub commits, let's build a Docker image to run the app. The image is built from a Dockerfile that defines how to configure the container that runs the app.

From the SSH connection to your VM, change to the Jenkins workspace directory named after the job you created in a previous step. In this example, that was named *HelloWorld*.

```
cd /var/lib/jenkins/workspace/HelloWorld
```

Create a file in this workspace directory with `sudo sensible-editor Dockerfile` and paste the following contents. Make sure that the whole Dockerfile is copied correctly, especially the first line:

```
FROM node:alpine

EXPOSE 1337

WORKDIR /var/www
COPY package.json /var/www/
RUN npm install
COPY index.js /var/www/
```

This Dockerfile uses the base Node.js image using Alpine Linux, exposes port 1337 that the Hello World app runs on, then copies the app files and initializes it.

Create Jenkins build rules

In a previous step, you created a basic Jenkins build rule that output a message to the console. Let's create the build step to use our Dockerfile and run the app.

Back in your Jenkins instance, select the job you created in a previous step. Select **Configure** on the left-hand side and scroll down to the **Build** section:

- Remove your existing `echo "Test"` build step. Select the red cross on the top right-hand corner of the existing build step box.
- Choose **Add build step**, then select **Execute shell**
- In the **Command** box, enter the following Docker commands, then select **Save**:

```
docker build --tag helloworld:$BUILD_NUMBER .
docker stop helloworld && docker rm helloworld
docker run --name helloworld -p 1337:1337 helloworld:$BUILD_NUMBER node /var/www/index.js &
```

The Docker build steps create an image and tag it with the Jenkins build number so you can maintain a history of images. Any existing containers running the app are stopped and then removed. A new container is then started using the image and runs your Node.js app based on the latest commits in GitHub.

Test your pipeline

To see the whole pipeline in action, edit the `index.js` file in your forked GitHub repo again and select **Commit change**. A new job starts in Jenkins based on the webhook for GitHub. It takes a few seconds to create the Docker image and start your app in a new container.

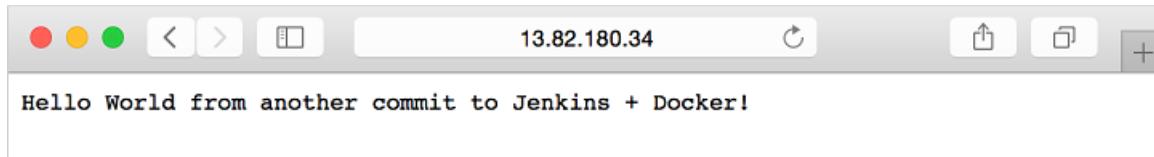
If needed, obtain the public IP address of your VM again:

```
az vm show --resource-group myResourceGroupJenkins --name myVM -d --query [publicIps] --o tsv
```

Open a web browser and enter `http://<publicIps>:1337`. Your Node.js app is displayed and reflects the latest commits in your GitHub fork as follows:



Now make another edit to the `index.js` file in GitHub and commit the change. Wait a few seconds for the job to complete in Jenkins, then refresh your web browser to see the updated version of your app running in a new container as follows:



Next steps

In this tutorial, you configured GitHub to run a Jenkins build job on each code commit and then deploy a Docker container to test your app. You learned how to:

- Create a Jenkins VM
- Install and configure Jenkins
- Create webhook integration between GitHub and Jenkins
- Create and trigger Jenkins build jobs from GitHub commits
- Create a Docker image for your app
- Verify GitHub commits build new Docker image and updates running app

Advance to the next tutorial to learn more about how to integrate Jenkins with Azure DevOps Services.

[Deploy apps with Jenkins and Azure DevOps Services](#)

Tutorial: Deploy your app to Linux virtual machines in Azure with using Jenkins and Azure DevOps Services

2/25/2020 • 7 minutes to read • [Edit Online](#)

Continuous integration (CI) and continuous deployment (CD) form a pipeline by which you can build, release, and deploy your code. Azure DevOps Services provides a complete, fully featured set of CI/CD automation tools for deployment to Azure. Jenkins is a popular third-party CI/CD server-based tool that also provides CI/CD automation. You can use Azure DevOps Services and Jenkins together to customize how you deliver your cloud app or service.

In this tutorial, you use Jenkins to build a Node.js web app. You then use Azure DevOps to deploy it to a [deployment group](#) that contains Linux virtual machines (VMs). You learn how to:

- Get the sample app.
- Configure Jenkins plug-ins.
- Configure a Jenkins Freestyle project for Node.js.
- Configure Jenkins for Azure DevOps Services integration.
- Create a Jenkins service endpoint.
- Create a deployment group for the Azure virtual machines.
- Create an Azure Pipelines release pipeline.
- Execute manual and CI-triggered deployments.

Before you begin

- You need access to a Jenkins server. If you have not yet created a Jenkins server, see [Create a Jenkins master on an Azure virtual machine](#).
- Sign in to your Azure DevOps Services organization (<https://{{yourorganization}}.visualstudio.com>). You can get a [free Azure DevOps Services organization](#).

NOTE

For more information, see [Connect to Azure DevOps Services](#).

- You need a Linux virtual machine for a deployment target. For more information, see [Create and manage Linux VMs with the Azure CLI](#).
- Open inbound port 80 for your virtual machine. For more information, see [Create network security groups using the Azure portal](#).

Get the sample app

You need an app to deploy, stored in a Git repository. For this tutorial, we recommend that you use [this sample app available from GitHub](#). This tutorial contains a sample script that's used for installing Node.js and an application. If you want to work with your own repository, you should configure a similar sample.

Create a fork of this app and take note of the location (URL) for use in later steps of this tutorial. For more information, see [Fork a repo](#).

NOTE

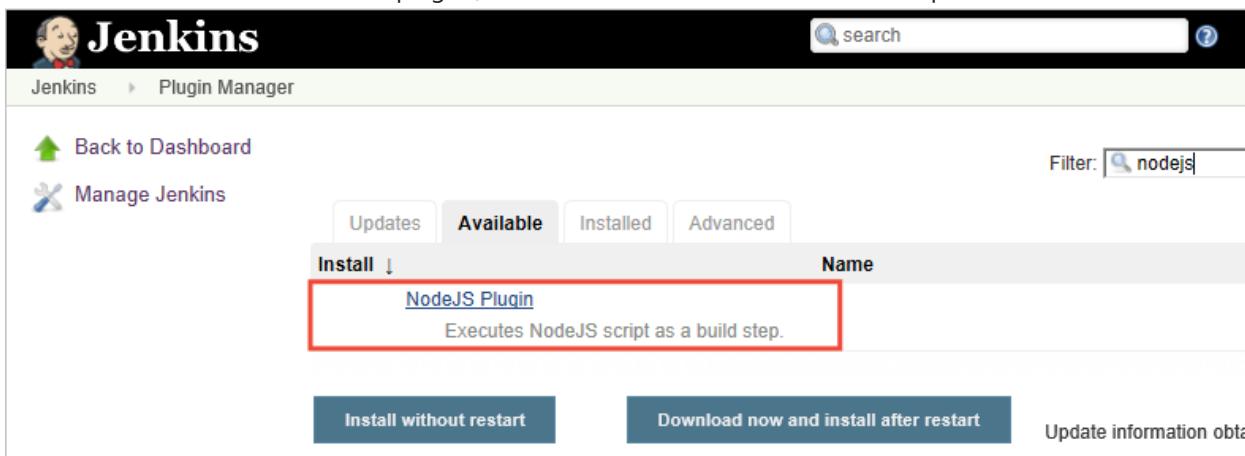
The app was built through [Yeoman](#). It uses Express, bower, and grunt. And it has some npm packages as dependencies. The sample also contains a script that sets up Nginx and deploys the app. It is executed on the virtual machines. Specifically, the script:

1. Installs Node, Nginx, and PM2.
2. Configures Nginx and PM2.
3. Starts the Node app.

Configure Jenkins plug-ins

First, you must configure two Jenkins plug-ins: **NodeJS** and **VS Team Services Continuous Deployment**.

1. Open your Jenkins account and select **Manage Jenkins**.
2. On the **Manage Jenkins** page, select **Manage Plugins**.
3. Filter the list to locate the **NodeJS** plug-in, and select the **Install without restart** option.



The screenshot shows the Jenkins Plugin Manager interface. At the top, there's a navigation bar with the Jenkins logo, a search bar, and a help icon. Below the navigation bar, the title 'Plugin Manager' is displayed. On the left, there are links for 'Back to Dashboard' and 'Manage Jenkins'. In the center, there are four tabs: 'Updates' (disabled), 'Available' (selected), 'Installed', and 'Advanced'. A filter bar at the top right contains a search icon and the text 'nodejs'. Below the tabs, a table lists available plugins. One plugin, 'NodeJS Plugin', is highlighted with a red border. Its details are shown in a tooltip: 'Executes NodeJS script as a build step.' At the bottom of the table, there are two buttons: 'Install without restart' (highlighted in red) and 'Download now and install after restart'. To the right of these buttons, a link says 'Update information obtained'.

4. Filter the list to find the **VS Team Services Continuous Deployment** plug-in and select the **Install without restart** option.
5. Go back to the Jenkins dashboard and select **Manage Jenkins**.
6. Select **Global Tool Configuration**. Find **NodeJS** and select **NodeJS installations**.
7. Select the **Install automatically** option, and then enter a **Name** value.
8. Select **Save**.

Configure a Jenkins Freestyle project for Node.js

1. Select **New Item**. Enter an item name.
2. Select **Freestyle project**. Select **OK**.
3. On the **Source Code Management** tab, select **Git** and enter the details of the repository and the branch that contain your app code.

- On the **Build Triggers** tab, select **Poll SCM** and enter the schedule `H/03 * * * *` to poll the Git repository for changes every three minutes.
- On the **Build Environment** tab, select **Provide Node & npm bin/ folder PATH** and select the **NodeJS Installation** value. Leave **npmrc file** set to **use system default**.
- On the **Build** tab, select **Execute shell** and enter the command `npm install` to ensure that all dependencies are updated.

Configure Jenkins for Azure DevOps Services integration

NOTE

Ensure that the personal access token (PAT) you use for the following steps contains the *Release* (read, write, execute and manage) permission in Azure DevOps Services.

- Create a PAT in your Azure DevOps Services organization if you don't already have one. Jenkins requires this information to access your Azure DevOps Services organization. Be sure to store the token information for upcoming steps in this section.
To learn how to generate a token, read [How do I create a personal access token for Azure DevOps Services?](#).
- In the **Post-build Actions** tab, select **Add post-build action**. Select **Archive the artifacts**.
- For **Files to archive**, enter `**/*` to include all files.
- To create another action, select **Add post-build action**.
- Select **Trigger release in TFS/Team Services**. Enter the URI for your Azure DevOps Services organization, such as `https://<your-organization-name>.visualstudio.com`.
- Enter the **Project** name.
- Choose a name for the release pipeline. (You create this release pipeline later in Azure DevOps Services.)

8. Choose credentials to connect to your Azure DevOps Services or Team Foundation Server environment:

- Leave **Username** blank if you are using Azure DevOps Services.
- Enter a username and password if you are using an on-premises version of Team Foundation Server.

Trigger release in TFS/Team Services	
Collection url	<input type="text" value="https://adventworks.visualstudio.com"/>
Team project	<input type="text" value="AW"/>
Release definition	<input type="text" value="Adventworks Linux CD"/>
Username	<input type="text" value="admin"/>
Password or PAT	<input type="password" value="*****"/>

9. Save the Jenkins project.

Create a Jenkins service endpoint

A service endpoint allows Azure DevOps Services to connect to Jenkins.

1. Open the **Services** page in Azure DevOps Services, open the **New Service Endpoint** list, and select **Jenkins**.

The screenshot shows the 'Endpoints' section of the Azure DevOps Services 'Services' page. A red box highlights the 'Jenkins' option in the list, which is currently selected. Other options shown include 'Generic', 'GitHub', and 'Kubernetes'. The top navigation bar has a 'Fabrikam' dropdown, a search icon, and tabs for Home, Code, Work, Build & Release, Test, and Services (which is the active tab). A red box also highlights the 'Services' tab itself.

2. Enter a name for the connection.
3. Enter the URL of your Jenkins server, and select the **Accept untrusted SSL certificates** option. An example URL is <http://YourJenkinsURL.westcentralus.cloudapp.azure.com>.
4. Enter the username and password for your Jenkins account.
5. Select **Verify connection** to check that the information is correct.
6. Select **OK** to create the service endpoint.

Create a deployment group for Azure virtual machines

You need a [deployment group](#) to register the Azure DevOps Services agent so the release pipeline can be deployed to your virtual machine. Deployment groups make it easy to define logical groups of target machines for deployment, and to install the required agent on each machine.

NOTE

In the following procedure, be sure to install the prerequisites and *don't run the script with sudo privileges*.

1. Open the **Releases** tab of the **Build & Release** hub, open **Deployment groups**, and select **+ New**.
2. Enter a name for the deployment group, and an optional description. Then select **Create**.
3. Choose the operating system for your deployment target virtual machine. For example, select **Ubuntu 16.04+**.

4. Select **Use a personal access token in the script for authentication.**
5. Select the **System prerequisites** link. Install the prerequisites for your operating system.
6. Select **Copy script to clipboard** to copy the script.
7. Log in to your deployment target virtual machine and run the script. Don't run the script with sudo privileges.
8. After the installation, you are prompted for deployment group tags. Accept the defaults.
9. In Azure DevOps Services, check for your newly registered virtual machine in **Targets** under **Deployment Groups**.

Create an Azure Pipelines release pipeline

A release pipeline specifies the process that Azure Pipelines uses to deploy the app. In this example, you execute a shell script.

To create the release pipeline in Azure Pipelines:

1. Open the **Releases** tab of the **Build & Release** hub, and select **Create release pipeline**.
2. Select the **Empty** template by choosing to start with an **Empty process**.
3. In the **Artifacts** section, select **+ Add Artifact** and choose **Jenkins** for **Source type**. Select your Jenkins service endpoint connection. Then select the Jenkins source job and select **Add**.
4. Select the ellipsis next to **Environment 1**. Select **Add deployment group phase**.
5. Choose your deployment group.
6. Select **+** to add a task to **Deployment group phase**.
7. Select the **Shell Script** task and select **Add**. The **Shell Script** task provides the configuration for a script to run on each server in order to install Node.js and start the app.
8. For **Script Path**, enter `$(System.DefaultWorkingDirectory)/Fabrikam-Node/deployscript.sh`.
9. Select **Advanced**, and then enable **Specify Working Directory**.
10. For **Working Directory**, enter `$(System.DefaultWorkingDirectory)/Fabrikam-Node`.
11. Edit the name of the release pipeline to the name that you specified on the **Post-build Actions** tab of the build in Jenkins. Jenkins requires this name to be able to trigger a new release when the source artifacts are updated.
12. Select **Save** and select **OK** to save the release pipeline.

Execute manual and CI-triggered deployments

1. Select **+** **Release** and select **Create Release**.
2. Select the build that you completed in the highlighted drop-down list, and select **Queue**.
3. Choose the release link in the pop-up message. For example: "Release **Release-1** has been created."
4. Open the **Logs** tab to watch the release console output.
5. In your browser, open the URL of one of the servers that you added to your deployment group. For example, enter `http://{your-server-ip-address}`.
6. Go to the source Git repository and modify the contents of the **h1** heading in the file `app/views/index.jade` with some changed text.
7. Commit your change.
8. After a few minutes, you will see a new release created on the **Releases** page of Azure DevOps. Open the release to see the deployment taking place. Congratulations!

Troubleshooting the Jenkins plugin

If you encounter any bugs with the Jenkins plugins, file an issue in the [Jenkins JIRA](#) for the specific component.

Next steps

In this tutorial, you automated the deployment of an app to Azure by using Jenkins for build and Azure DevOps Services for release. You learned how to:

- Build your app in Jenkins.
- Configure Jenkins for Azure DevOps Services integration.
- Create a deployment group for the Azure virtual machines.
- Create an Azure Pipeline that configures the VMs and deploys the app.

To learn about how to use Azure Pipelines for both Build and Release steps, refer to [this](#).

To learn about how to author a YAML based CI/CD pipeline to deploy to VMs, advance to the next tutorial.

[Jenkins on Azure](#)

Tutorial: Integrated DevOps for IaaS and PaaS on Azure

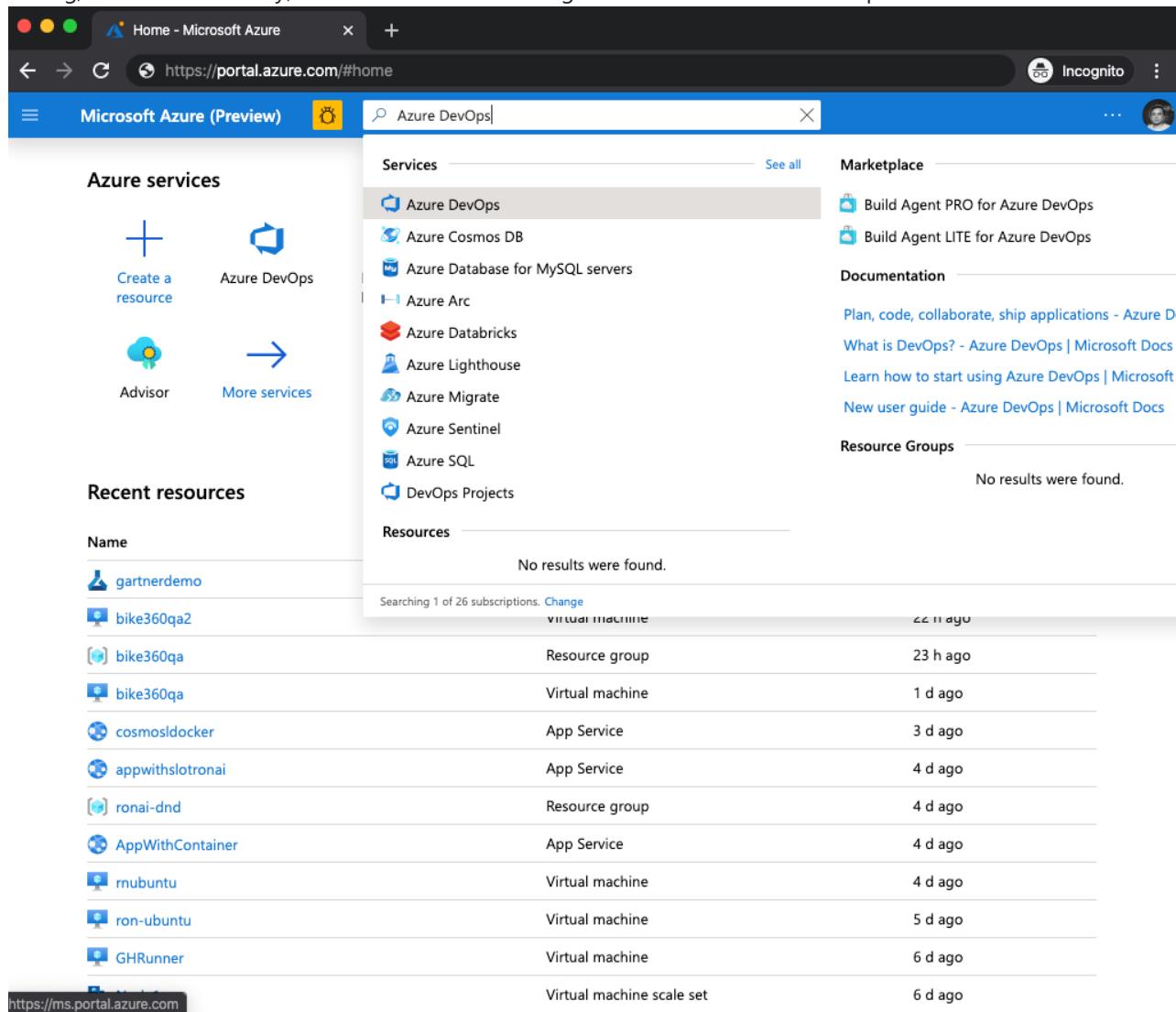
2/28/2020 • 5 minutes to read • [Edit Online](#)

With end-to-end solutions on Azure, teams can implement DevOps practices in each of the application lifecycle phases: plan, develop, deliver, and operate.

Below are some of the Azure Services that simplify cloud workloads and can be combined to enable amazingly powerful scenarios. These technologies, combined with people and processes, enable teams to continually provide value to customers.

- Azure: <https://portal.azure.com> – Portal for building cloud workloads. Manage and monitor everything from simple web apps to complex cloud applications
- Azure DevOps: <https://dev.azure.com> – Plan smarter, collaborate better, and ship faster with a set of modern dev services
- Azure Machine Learning studio: <https://ml.azure.com> - Prep data, train, and deploy machine learning models

Azure DevOps is a built-in Azure service that automates each part of the DevOps process with continuous integration and continuous delivery for any Azure resource. Whether your app uses virtual machines, web apps, Kubernetes, or any other resource, you can implement infrastructure as code, continuous integration, continuous testing, continuous delivery, and continuous monitoring with Azure and Azure DevOps.



The screenshot shows the Microsoft Azure (Preview) portal interface. The search bar at the top contains the text "Azure DevOps". On the left sidebar, under "Azure services", there are icons for "Create a resource", "Azure DevOps", "Advisor", and "More services". Under "Recent resources", there is a list of 13 items, mostly virtual machines, with names like "gartnerdemo", "bike360qa2", "bike360qa", "cosmosldocker", "appwithslotronai", "ronai-dnd", "AppWithContainer", "rnubuntu", "ron-ubuntu", "GHRunner", and "ms.portal.azure.com". The main content area shows a list of services under "Services": Azure DevOps, Azure Cosmos DB, Azure Database for MySQL servers, Azure Arc, Azure Databricks, Azure Lighthouse, Azure Migrate, Azure Sentinel, and Azure SQL. There are also sections for "Marketplace", "Documentation" (links to "Plan, code, collaborate, ship applications - Azure DevOps", "What is DevOps?", "Learn how to start using Azure DevOps", and "New user guide"), and "Resource Groups" (which is currently empty). The bottom of the screen shows the URL "https://ms.portal.azure.com".

IaaS - Configure CI/CD

Azure Pipelines provides a complete, fully featured set of CI/CD automation tools for deployments to virtual machines. You can configure a continuous delivery pipeline for an Azure VM directly from Azure portal. This document contains the steps associated with setting up a CI/CD pipeline for multi-machine deployments from Azure portal. Configure CI/CD on Virtual Machines.

Virtual machines can be added as targets to a [deployment group](#) and can be targeted for multi-machine rolling updates. Deployment history views within Deployment groups provide traceability from VM to the pipeline and then to the commit.

Rolling updates: A rolling deployment replaces instances of the previous version of an application with instances of the new version of the application on a fixed set of machines (rolling set) in each iteration. Let's walkthrough how you can configure a rolling update to virtual machines.

You can configure rolling updates to your "**virtual machines**" within the Azure portal using continuous delivery option.

Here is the step-by-step walkthrough.

1. Sign in to your Azure portal and navigate to a virtual machine.
2. In the VM left pane, navigate to the **continuous delivery** menu. Then click on **Configure**.

The screenshot shows the Azure portal interface for a virtual machine named "bike360qa". The left sidebar lists various management options like Overview, Activity log, and Settings. Under Settings, the "Continuous delivery" option is selected and highlighted with a grey background. The main content area is titled "Continuous delivery" and contains descriptive text about how it simplifies deployment pipelines. It also includes a section for provisioning additional resources and a "Configure" button at the bottom right. The URL in the browser bar is "Home > bike360qa - Continuous delivery (Preview)".

3. In the configuration panel, click on "Azure DevOps Organization" to select an existing account or create one. Then select the project under which you would like to configure the pipeline.

Microsoft Azure (Preview) Search resources, services, and docs (G+/)

Home > bike360qa - Continuous delivery (Preview)

bike360qa - Continuous delivery (Preview)

Virtual machine

Search (Cmd+ /)

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

Settings

- Networking
- Disks
- Size
- Security
- Extensions

Continuous delivery

Continuous delivery pipeline for deploying your application to a virtual machine.

Do you need help with application deployment?

Learn more about continuous delivery pipelines.

Azure DevOps Organization *
 Create Use existing

devopsworld

Project
DevOps

Deployment group
 Create Use existing

Deployment group name *
bike360qa

Tags: web Tags

OK

4. A deployment group is a logical set of deployment target machines that represent the physical environments; for example, "Dev", "Test", "UAT", and "Production". You can create a new deployment group or select an existing deployment group. You can optionally tag the machine with the role. For example, 'web', 'db' etc.
5. Click **OK** on the dialog to configure the continuous delivery pipeline.
6. Once done, you will have a continuous delivery pipeline configured to deploy to the virtual machine.

Microsoft Azure (Preview)  Search resources, services, and docs (G+/-) ... 

Home > bike360qa - Continuous delivery (Preview)

bike360qa - Continuous delivery (Preview)

 Search (Cmd+/) <<  Disconnect  Refresh

 Continuous delivery

Continuous delivery in Azure DevOps simplifies setting up a robust deployment pipeline for your application. [Learn more](#)

Deployment history
12/01/2020

 bike360qa - CD > Release-1 / dev 19:46:37 

Settings

-  Networking
-  Disks
-  Size
-  Security
-  Extensions
-  Continuous delivery
-  Availability + scaling
-  Configuration
-  Identity
-  Properties
-  Locks

7. You will see that the deployment to the virtual machine is in progress. You can click on the link to navigate to the pipeline. Click on **Release-1** to view the deployment. Or you can click on the **Edit** to modify the release pipeline definition.
8. If you have multiple VMs to be configured, repeat the steps 2-5, for other VMs to be added to the deployment group.
9. Once done, click on the pipeline definition, navigate to the Azure DevOps organization, and click on **Edit** release pipeline.

Azure DevOps

All pipelines > bike360qa - CD

Pipeline Tasks Variables Retention Options History

Save ...

Artifacts | + Add

+ Add an artifact

Schedule not set

Stages | + Add

dev
1 job, 1 task

The screenshot shows the Azure DevOps Pipeline editor interface. On the left, there's a vertical toolbar with icons for different pipeline components like Artifacts, Stages, and Deployments. The main area is divided into two sections: 'Artifacts' and 'Stages'. The 'Artifacts' section has a button '+ Add' and a note 'Schedule not set'. The 'Stages' section contains a single stage named 'dev' which is described as having '1 job, 1 task'. The stage is currently empty.

10. Click on the link **1 job, 1 task** in **dev** stage. Click on the **Deploy** phase.

The screenshot shows the Azure DevOps interface for managing pipelines. On the left, there's a sidebar with various icons for different pipeline components like CI, CD, and release. The main area shows a pipeline named 'bike360qa - CD' with a single stage called 'dev'. Under the 'Tasks' tab, there's a 'Deploy' task. The configuration for this task includes:

- Display name:** Deploy
- Deployment targets:** Deployment group: bike360qa, Targets to deploy to in parallel: Multiple (selected), Maximum number of targets in parallel: Set to 100%.
- Required tags:** web

11. From the configuration pane on the right, you can see that by default the pipeline is configured to do a rolling update to all targets in parallel. You can configure the deployments to happen either one at a time or in terms of percentage by using the slider.

Canary reduces the risk by slowly rolling out the change to a small subset of users. As you gain more confidence in the new version, you can start releasing it to more servers in your infrastructure and routing more users to it. You can configure canary deployments to your “**virtual machines**” with the Azure portal using continuous delivery option. Here is the step-by-step walkthrough.

1. Sign in to your Azure portal and navigate to a virtual machine
2. Follow the steps 2-5 in the previous section to add multiple VMs to the deployment group.
3. Add a custom tag to the VMs that are to be part of canary deployments. For example, “canary”.
4. Once the pipeline is configured for the VMs, click on the pipeline, launch Azure DevOps organization, **Edit** the pipeline, and navigate to the **dev** stage. Add tag to the filter “canary”.
5. Add another deployment group phase, configure the phase with the tags to target remaining VMs in the deployment group.
6. Optionally, configure a manual validation step that can promote/reject the canary deployments.

All pipelines > **bike360qa - CD**

D Pipeline Tasks Variables Retention Options History

dev
Deployment process

Canary Deploy Run on deployment group ... + ⋮

Bash Script Bash

Manual Approval Run on server +

Manual validation step Manual intervention

Deploy Run on deployment group +

Bash Script Bash

Deployment group job ⋮ Remove

Display name * Canary Deploy

Deployment targets ^

Deployment group * bike360qa ⋮ ⟳ ⚙️

Required tags canary X

No matching targets in bike360qa deployment group

Targets to deploy to in parallel i

Multiple One target at a time

Maximum number of targets in parallel 1

Timeout * 10 minutes

Blue-Green reduces deployment downtime by having identical standby environment. At any time one of the environments is live. As you prepare for a new release, you do your final stage of testing in the green environment. Once the software is working in the green environment, switch the traffic so that all incoming requests go to the green environment - the blue environment is now idle. You can configure Blue-Green deployments to your “**virtual machines**” from the Azure portal using the continuous delivery option.

Here is the step-by-step walkthrough.

1. Sign in to your Azure portal and navigate to a Virtual Machine
2. Follow the steps 2-5 under the **Rolling updates** section to add multiple VMs to the deployment group. Add a custom tag to the VMs that are to be part of blue-green deployments. For example, “blue” or “green” for the VMs that are for the stand-by role.
3. Once the pipeline is configured for the VMs, click on the pipeline, launch Azure DevOps organization, **Edit** the pipeline, navigate to the **dev** stage. Add tag to the filter “green”.
4. Add an agent-less phase, configure the phase with manual validation step and an invoke-REST api step to swap the tags.

All pipelines > bike360qa - CD - bl...

Pipeline Tasks Variables Retention Options History

dev Deployment process

Green Deploy Run on deployment group

Bash Script Bash

Validate and swap Run on server

Manual validation step Manual intervention

Swap Blue-Green Invoke REST API

Agentless job

Display name *

Validate and swap

Execution plan

Parallelism

None Multi-con

Timeout *

0

Additional options

Run this job

Only when all previous jobs

Azure DevOps project

Get started with Azure more easily than ever.

With DevOps Projects, start running your application on any Azure service in just three steps: select an application language, a runtime, and an Azure service.

[Learn more.](#)

Additional resources

- [Deploy to Azure Virtual Machines using DevOps project](#)
- [Implement continuous deployment of your app to an Azure Virtual Machine Scale Set](#)

Tutorial: Deploy your app to Linux virtual machines in Azure using Azure DevOps Services and Azure Pipelines

2/4/2020 • 8 minutes to read • [Edit Online](#)

Continuous integration (CI) and continuous deployment (CD) form a pipeline by which you can build, release, and deploy your code after every code commit. This document contains the steps associated with setting up a CI/CD pipeline for doing multi-machine deployments using Azure Pipelines.

Azure Pipelines provides a complete, fully featured set of CI/CD automation tools for deployments to Virtual machines, both on-prem or on any cloud.

In this tutorial, you will set up a YAML based CI/CD pipeline to deploy your app to an Azure Pipelines [Environment](#) with Linux Virtual machines as resources, each of which serve as web servers to run the app.

You learn how to:

- Get a sample app.
- Create a YAML based Azure Pipelines CI pipeline for building the sample app.
- Create an Azure Pipelines Environment for the Azure virtual machines
- Create an Azure Pipelines CD pipeline.
- Execute manual and CI-triggered deployments.

Before you begin

- Sign in to your Azure DevOps Services organization (<https://dev.azure.com/>). You can get a [free Azure DevOps Services organization](#).

NOTE

For more information, see [Connect to Azure DevOps Services](#).

- You need a Linux virtual machine for a deployment target. For more information, see [Create and manage Linux VMs with the Azure CLI](#).
- Open inbound port 80 for your virtual machine. For more information, see [Create network security groups using the Azure portal](#).

Get your sample app code

If you already have an app in GitHub that you want to deploy, you can try creating a pipeline for that code.

However, if you are a new user, then you might get a better start by using our sample code. In that case, fork this repo in GitHub:

- [Java](#)
- [JavaScript](#)

<https://github.com/spring-projects/spring-petclinic>

NOTE

Petclinic is a [Java Spring Boot](#) application built using [Maven](#).

Prerequisites for the Linux VM

Sample apps mentioned above have been tested on Ubuntu 16.04, and we recommend you use the same version of Linux VM for this quickstart. Follow the additional steps described below based on the runtime stack used for the app.

- [Java](#)
- [JavaScript](#)
- For deploying Java Spring Boot and Spring Cloud based apps, create a Linux VM in Azure using [this template](#), which provides a fully supported OpenJDK-based runtime.
- For deploying Java servlets on Tomcat server, create a Linux VM with Java 8 using [this Azure template](#) and [configure Tomcat 9.x as a service](#).
- For deploying Java EE based app, use an Azure template to create a [Linux VM + Java + WebSphere 9.x](#) or a [Linux VM + Java + WebLogic 12.x](#) or a [Linux VM + Java + WildFly/JBoss 14](#)

Create an Azure Pipelines environment with Azure virtual machines

Virtual machines can be added as resources within [environments](#) and can be targeted for multi-machine deployments. Deployment history views within environment provide traceability from VM to the pipeline and then to the commit.

You can create an environment in the “**Environments**” hub within the “**Pipelines**” section.

1. Sign in to your Azure DevOps organization and navigate to your project.
2. In your project, navigate to the **Pipelines** page. Then choose **Environments** and click **Create Environment**. Specify a **Name** (required) for the environment and a **Description**.
3. Choose **Virtual Machines** as a **Resource** to be added to the environment and click **Next**.
4. Choose Operating System (Windows/Linux), and **copy PS registration script**.
5. Now run the copied script from an administrator PowerShell command prompt on each of the target VMs to be registered with this Environment.

NOTE

- Personal Access Token of the logged in user is pre-inserted in the script which expires on the same day making the copied script unusable thereon.
- If your VM already has any agent running on it, provide a unique name for “agent” to register with environment.

6. Once the VM is registered, it will start appearing as an environment resource under “resources” tab of the environment.

New environment

X

Virtual machine resource

Provider

Generic provider

Operating system

Windows

Registration script

1. Run `$ErrorActionPreference="Stop"` in administrative powershell

7. For adding more VMs, you can view and copy the script again by clicking on "Add resource" and choosing "Virtual Machines" as resource. This script would remain same for all the VMs to be added to this environment.
8. Each machine interacts with Azure Pipelines to coordinate deployment of your app.

The screenshot shows the 'VMenv' resources view. At the top, there are tabs for 'Resources' and 'Deployments', with 'Resources' being the active tab. Below the tabs is a table with two columns: 'Name' and 'Latest job'. A single row is present, representing the VM 'USHAN-PC'. The 'Name' column contains an icon of a computer monitor and the text 'USHAN-PC'. The 'Latest job' column contains the text 'Never deployed'.

9. You can add tags to the VM as part of the interactive PS registration script (or) you can also add/remove the same from the resource view by clicking on the triple dots at the end of each VM resource in the resources view.

The tags you assign allow you to limit deployment to specific virtual machines when the environment is used in a Deployment job. Tags are each limited to 256 characters, but there is no limit to the number of tags you can use.

The screenshot shows the 'VMenv' resources view with a modal dialog titled 'Manage tags for USHAN-PC'. The dialog contains a text input field with the tag 'web' and a '+' button. At the bottom of the dialog are 'Cancel' and 'Save' buttons. In the background, the main resources view shows the 'USHAN-PC' entry with the 'Never deployed' status and a three-dot menu icon.

Define your CI build pipeline

You'll need a continuous integration (CI) build pipeline that publishes your web application, as well as a deployment script that can be run locally on the Ubuntu server. Set up a CI build pipeline based on the runtime you want to use.

1. Sign in to your Azure DevOps organization and navigate to your project.
2. In your project, navigate to the **Pipelines** page. Then choose the action to create a new pipeline.
3. Walk through the steps of the wizard by first selecting **GitHub** as the location of your source code.
4. You might be redirected to GitHub to sign in. If so, enter your GitHub credentials.
5. When the list of repositories appears, select your desired sample app repository.
6. Azure Pipelines will analyze your repository and recommend a suitable pipeline template.
 - [Java](#)
 - [JavaScript](#)

Select the **starter** template and copy the below YAML snippet that builds your Java project and runs tests with Apache Maven:

```
- job: Build
  displayName: Build Maven Project
  steps:
    - task: Maven@3
      displayName: 'Maven Package'
      inputs:
        mavenPomFile: 'pom.xml'
    - task: CopyFiles@2
      displayName: 'Copy Files to artifact staging directory'
      inputs:
        SourceFolder: '$(System.DefaultWorkingDirectory)'
        Contents: '**/target/*.(war|jar)'
        TargetFolder: $(Build.ArtifactStagingDirectory)
    - upload: $(Build.ArtifactStagingDirectory)
      artifact: drop
```

For more guidance, follow the steps mentioned in [Build your Java app with Maven](#).

Define CD steps to deploy to the Linux VM

1. Edit the above pipeline and include a [deployment job](#) by referencing the environment and the VM resources which you have earlier using the YAML syntax below:

```
jobs:
- deployment: VMDeploy
  displayName: web
  environment:
    name: <environment name>
    resourceType: VirtualMachine
    tags: web1
  strategy:
```

2. You can select specific sets of virtual machines from the environment to receive the deployment by specifying the **tags** that you have defined for each virtual machine in the environment. [Here](#) is the complete YAML schema for Deployment job.

3. You can specify either `runOnce` or `rolling` as deployment strategy.

`runOnce` is the simplest deployment strategy wherein all the life cycle hooks, namely `preDeploy`, `deploy`, `routeTraffic`, and `postRouteTraffic`, are executed once. Then, either `on: success` or `on: failure` is executed.

Below is the example YAML snippet for `runOnce` :

```
jobs:
- deployment: VMDeploy
  displayName: web
  pool:
    vmImage: 'Ubuntu-16.04'
  environment:
    name: <environment name>
    resourceType: VirtualMachine
  strategy:
    runOnce:
      deploy:
        steps:
          - script: echo my first deployment
```

4. Below is an example of the YAML snippet that you can use to define a rolling strategy for Virtual machines updates upto 5 targets in each iteration. `maxParallel` will determine the number of targets that can be deployed to, in parallel. The selection accounts for absolute number or percentage of targets that must remain available at any time excluding the targets that are being deployed to. It is also used to determine the success and failure conditions during deployment.

```

jobs:
- deployment: VMDeploy
  displayName: web
  environment:
    name: <environment name>
    resourceType: VirtualMachine
  strategy:
    rolling:
      maxParallel: 5 #for percentages, mention as x%
    preDeploy:
      steps:
        - download: current
          artifact: drop
        - script: echo initialize, cleanup, backup, install certs
    deploy:
      steps:
        - task: Bash@3
          inputs:
            targetType: 'inline'
            script: |
              # Modify deployment script based on the app type
              echo "Starting deployment script run"
              sudo java -jar '$(Pipeline.Workspace)/drop/**/target/*.jar'
    routeTraffic:
      steps:
        - script: echo routing traffic
  postRouteTraffic:
    steps:
      - script: echo health check post-route traffic
  on:
    failure:
      steps:
        - script: echo Restore from backup! This is on failure
    success:
      steps:
        - script: echo Notify! This is on success

```

With each run of this job, deployment history is recorded against the <environment name> environment that you have created and registered the VMs.

Run your pipeline and get traceability views in environment

Deployments view of the environment provides complete traceability of commits and work items, and a cross-pipeline deployment history per environment/resource.

Run	Jobs	Date	Duration
Update rolling-deployment.yml for Azure Pipelines #20191209.1 on niadak.AspDotNetCore	VMDeploy	Monday	<1s
Update rolling-deployment.yml for Azure Pipelines #20191206.1 on niadak.AspDotNetCore	VMDeploy	Friday	<1s
Update rolling-deployment.yml for Azure Pipelines #20191205.1 on niadak.AspDotNetCore	VMDeploy	Thursday	<1s

← Deployment by 20191205.1

#2016 on niadak.AspDotNetCore targeting Niadak-VM-Env

Jobs Changes Workitems

Jobs

web_VM01_PreDeploy	Thursday 12s
web_VM01_Deploy	Thursday 15s
web_VM01_RouteTraffic	Thursday 13s
web_VM01_PostRouteTraffic	Thursday 11s
web_VM01_OnSuccess	Thursday 11s

Next steps

- You can proceed to [customize the pipeline](#) you just created.
- To learn what else you can do in YAML pipelines, see [YAML schema reference](#).
- To learn about how to deploy a LAMP (Linux, Apache, MySQL, and PHP) stack, advance to the next tutorial.

[Deploy LAMP stack](#)

Tutorial: Install a LAMP web server on a Linux virtual machine in Azure

11/13/2019 • 6 minutes to read • [Edit Online](#)

This article walks you through how to deploy an Apache web server, MySQL, and PHP (the LAMP stack) on an Ubuntu VM in Azure. If you prefer the NGINX web server, see the [LEMP stack](#) tutorial. To see the LAMP server in action, you can optionally install and configure a WordPress site. In this tutorial you learn how to:

- Create an Ubuntu VM (the 'L' in the LAMP stack)
- Open port 80 for web traffic
- Install Apache, MySQL, and PHP
- Verify installation and configuration
- Install WordPress on the LAMP server

This setup is for quick tests or proof of concept. For more on the LAMP stack, including recommendations for a production environment, see the [Ubuntu documentation](#).

This tutorial uses the CLI within the [Azure Cloud Shell](#), which is constantly updated to the latest version. To open the Cloud Shell, select **Try it** from the top of any code block.

If you choose to install and use the CLI locally, this tutorial requires that you are running the Azure CLI version 2.0.30 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Create a resource group

Create a resource group with the [az group create](#) command. An Azure resource group is a logical container into which Azure resources are deployed and managed.

The following example creates a resource group named *myResourceGroup* in the *eastus* location.

```
az group create --name myResourceGroup --location eastus
```

Create a virtual machine

Create a VM with the [az vm create](#) command.

The following example creates a VM named *myVM* and creates SSH keys if they do not already exist in a default key location. To use a specific set of keys, use the `--ssh-key-value` option. The command also sets *azureuser* as an administrator user name. You use this name later to connect to the VM.

```
az vm create \
  --resource-group myResourceGroup \
  --name myVM \
  --image UbuntuLTS \
  --admin-username azureuser \
  --generate-ssh-keys
```

When the VM has been created, the Azure CLI shows information similar to the following example. Take note of the `publicIpAddress`. This address is used to access the VM in later steps.

```
{  
    "fqdns": "",  
    "id": "/subscriptions/<subscription  
ID>/resourceGroups/myResourceGroup/providers/Microsoft.Compute/virtualMachines/myVM",  
    "location": "eastus",  
    "macAddress": "00-0D-3A-23-9A-49",  
    "powerState": "VM running",  
    "privateIpAddress": "10.0.0.4",  
    "publicIpAddress": "40.68.254.142",  
    "resourceGroup": "myResourceGroup"  
}
```

Open port 80 for web traffic

By default, only SSH connections are allowed into Linux VMs deployed in Azure. Because this VM is going to be a web server, you need to open port 80 from the internet. Use the [az vm open-port](#) command to open the desired port.

```
az vm open-port --port 80 --resource-group myResourceGroup --name myVM
```

SSH into your VM

If you don't already know the public IP address of your VM, run the [az network public-ip list](#) command. You need this IP address for several later steps.

```
az network public-ip list --resource-group myResourceGroup --query []. ipAddress
```

Use the following command to create an SSH session with the virtual machine. Substitute the correct public IP address of your virtual machine. In this example, the IP address is *40.68.254.142*. *azureuser* is the administrator user name set when you created the VM.

```
ssh azureuser@40.68.254.142
```

Install Apache, MySQL, and PHP

Run the following command to update Ubuntu package sources and install Apache, MySQL, and PHP. Note the caret (^) at the end of the command, which is part of the `lamp-server^` package name.

```
sudo apt update && sudo apt install lamp-server^
```

You are prompted to install the packages and other dependencies. This process installs the minimum required PHP extensions needed to use PHP with MySQL.

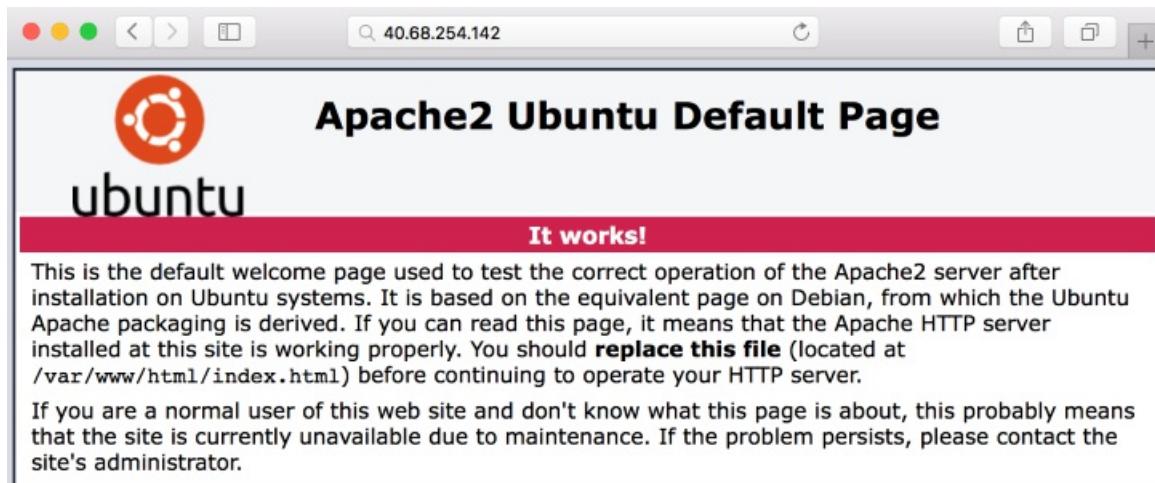
Verify installation and configuration

Verify Apache

Check the version of Apache with the following command:

```
apache2 -v
```

With Apache installed, and port 80 open to your VM, the web server can now be accessed from the internet. To view the Apache2 Ubuntu Default Page, open a web browser, and enter the public IP address of the VM. Use the public IP address you used to SSH to the VM:



Verify and secure MySQL

Check the version of MySQL with the following command (note the capital `v` parameter):

```
mysql -V
```

To help secure the installation of MySQL, including setting a root password, run the `mysql_secure_installation` script.

```
sudo mysql_secure_installation
```

You can optionally set up the Validate Password Plugin (recommended). Then, set a password for the MySQL root user, and configure the remaining security settings for your environment. We recommend that you answer "Y" (yes) to all questions.

If you want to try MySQL features (create a MySQL database, add users, or change configuration settings), login to MySQL. This step is not required to complete this tutorial.

```
sudo mysql -u root -p
```

When done, exit the mysql prompt by typing `\q`.

Verify PHP

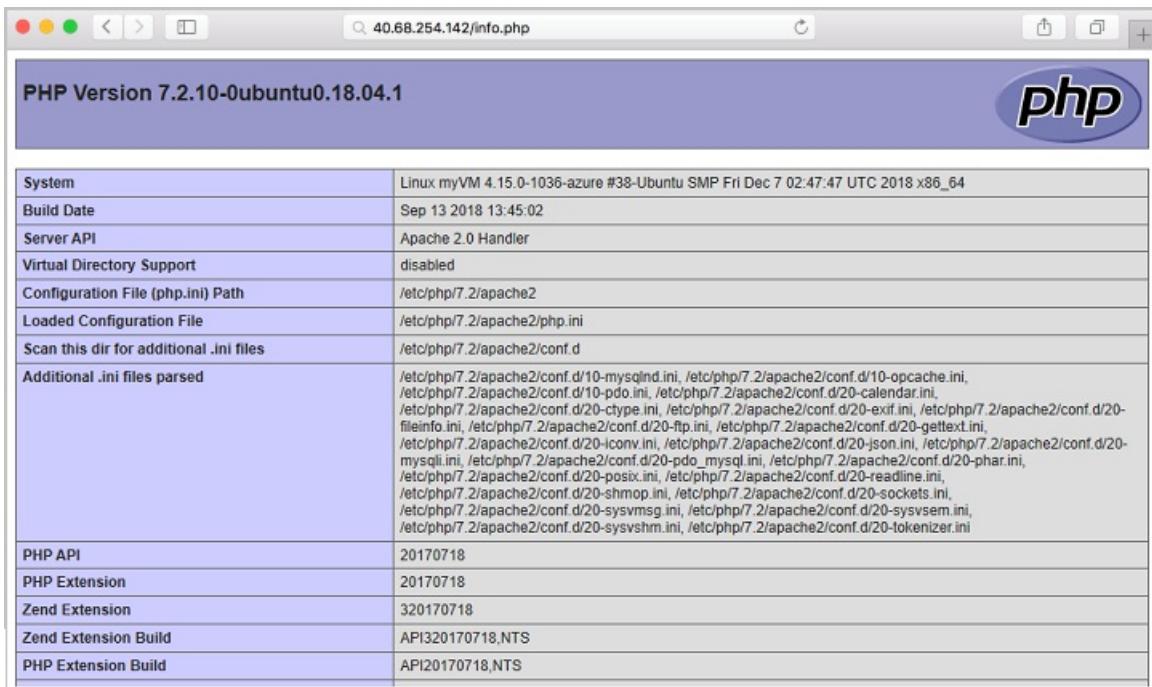
Check the version of PHP with the following command:

```
php -v
```

If you want to test further, create a quick PHP info page to view in a browser. The following command creates the PHP info page:

```
sudo sh -c 'echo "<?php phpinfo(); ?>" > /var/www/html/info.php'
```

Now you can check the PHP info page you created. Open a browser and go to `http://yourPublicIPAddress/info.php`. Substitute the public IP address of your VM. It should look similar to this image.



PHP Version 7.2.10-0ubuntu0.18.04.1	
System	Linux myVM 4.15.0-1036-azure #38-Ubuntu SMP Fri Dec 7 02:47:47 UTC 2018 x86_64
Build Date	Sep 13 2018 13:45:02
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.2/apache2
Loaded Configuration File	/etc/php/7.2/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.2/apache2/conf.d
Additional .ini files parsed	/etc/php/7.2/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.2/apache2/conf.d/10-opcache.ini, /etc/php/7.2/apache2/conf.d/10-pdo.ini, /etc/php/7.2/apache2/conf.d/20-calendar.ini, /etc/php/7.2/apache2/conf.d/20-ctype.ini, /etc/php/7.2/apache2/conf.d/20-exif.ini, /etc/php/7.2/apache2/conf.d/20-filinfo.ini, /etc/php/7.2/apache2/conf.d/20-ftp.ini, /etc/php/7.2/apache2/conf.d/20-gettext.ini, /etc/php/7.2/apache2/conf.d/20-iconv.ini, /etc/php/7.2/apache2/conf.d/20-json.ini, /etc/php/7.2/apache2/conf.d/20-mysqli.ini, /etc/php/7.2/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.2/apache2/conf.d/20-phar.ini, /etc/php/7.2/apache2/conf.d/20-posix.ini, /etc/php/7.2/apache2/conf.d/20-readline.ini, /etc/php/7.2/apache2/conf.d/20-shmop.ini, /etc/php/7.2/apache2/conf.d/20-sockets.ini, /etc/php/7.2/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.2/apache2/conf.d/20-sysvsem.ini, /etc/php/7.2/apache2/conf.d/20-sysvshm.ini, /etc/php/7.2/apache2/conf.d/20-tokenizer.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718.NTS
PHP Extension Build	API20170718.NTS

Install WordPress

If you want to try your stack, install a sample app. As an example, the following steps install the open source [WordPress](#) platform to create websites and blogs. Other workloads to try include [Drupal](#) and [Moodle](#).

This WordPress setup is only for proof of concept. To install the latest WordPress in production with recommended security settings, see the [WordPress documentation](#).

Install the WordPress package

Run the following command:

```
sudo apt install wordpress
```

Configure WordPress

Configure WordPress to use MySQL and PHP.

In a working directory, create a text file `wordpress.sql` to configure the MySQL database for WordPress:

```
sudo sensible-editor wordpress.sql
```

Add the following commands, substituting a database password of your choice for `yourPassword` (leave other values unchanged). If you previously set up a MySQL security policy to validate password strength, make sure the password meets the strength requirements. Save the file.

```
CREATE DATABASE wordpress;
GRANT SELECT,INSERT,UPDATE,DELETE,CREATE,DROP,ALTER
ON wordpress.* 
TO wordpress@localhost
IDENTIFIED BY 'yourPassword';
```

Run the following command to create the database:

```
cat wordpress.sql | sudo mysql --defaults-extra-file=/etc/mysql/debian.cnf
```

Because the file `wordpress.sql` contains database credentials, delete it after use:

```
sudo rm wordpress.sql
```

To configure PHP, run the following command to open a text editor of your choice and create the file `/etc/wordpress/config-localhost.php`:

```
sudo sensible-editor /etc/wordpress/config-localhost.php
```

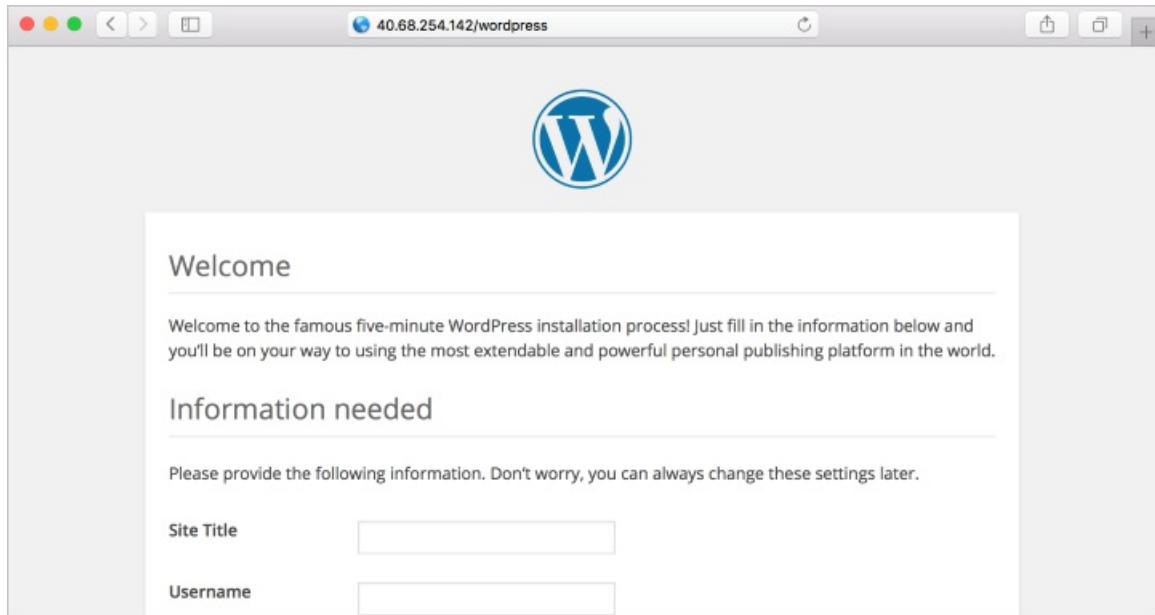
Copy the following lines to the file, substituting your WordPress database password for `yourPassword` (leave other values unchanged). Then save the file.

```
<?php  
define('DB_NAME', 'wordpress');  
define('DB_USER', 'wordpress');  
define('DB_PASSWORD', 'yourPassword');  
define('DB_HOST', 'localhost');  
define('WP_CONTENT_DIR', '/usr/share/wordpress/wp-content');  
?>
```

Move the WordPress installation to the web server document root:

```
sudo ln -s /usr/share/wordpress /var/www/html/wordpress  
sudo mv /etc/wordpress/config-localhost.php /etc/wordpress/config-default.php
```

Now you can complete the WordPress setup and publish on the platform. Open a browser and go to `http://yourPublicIPAddress/wordpress`. Substitute the public IP address of your VM. It should look similar to this image.



Next steps

In this tutorial, you deployed a LAMP server in Azure. You learned how to:

- Create an Ubuntu VM
- Open port 80 for web traffic

- Install Apache, MySQL, and PHP
- Verify installation and configuration
- Install WordPress on the LAMP server

Advance to the next tutorial to learn how to secure web servers with SSL certificates.

[Secure web server with SSL](#)

Tutorial: Install a LEMP web server on a Linux virtual machine in Azure

11/13/2019 • 6 minutes to read • [Edit Online](#)

This article walks you through how to deploy an NGINX web server, MySQL, and PHP (the LEMP stack) on an Ubuntu VM in Azure. The LEMP stack is an alternative to the popular [LAMP stack](#), which you can also install in Azure. To see the LEMP server in action, you can optionally install and configure a WordPress site. In this tutorial you learn how to:

- Create an Ubuntu VM (the 'L' in the LEMP stack)
- Open port 80 for web traffic
- Install NGINX, MySQL, and PHP
- Verify installation and configuration
- Install WordPress on the LEMP server

This setup is for quick tests or proof of concept.

This tutorial uses the CLI within the [Azure Cloud Shell](#), which is constantly updated to the latest version. To open the Cloud Shell, select **Try it** from the top of any code block.

If you choose to install and use the CLI locally, this tutorial requires that you are running the Azure CLI version 2.0.30 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Create a resource group

Create a resource group with the [az group create](#) command. An Azure resource group is a logical container into which Azure resources are deployed and managed.

The following example creates a resource group named *myResourceGroup* in the *eastus* location.

```
az group create --name myResourceGroup --location eastus
```

Create a virtual machine

Create a VM with the [az vm create](#) command.

The following example creates a VM named *myVM* and creates SSH keys if they do not already exist in a default key location. To use a specific set of keys, use the `--ssh-key-value` option. The command also sets *azureuser* as an administrator user name. You use this name later to connect to the VM.

```
az vm create \
  --resource-group myResourceGroup \
  --name myVM \
  --image UbuntuLTS \
  --admin-username azureuser \
  --generate-ssh-keys
```

When the VM has been created, the Azure CLI shows information similar to the following example. Take note of the `publicIpAddress`. This address is used to access the VM in later steps.

```
{  
    "fqdns": "",  
    "id": "/subscriptions/<subscription  
ID>/resourceGroups/myResourceGroup/providers/Microsoft.Compute/virtualMachines/myVM",  
    "location": "eastus",  
    "macAddress": "00-0D-3A-23-9A-49",  
    "powerState": "VM running",  
    "privateIpAddress": "10.0.0.4",  
    "publicIpAddress": "40.68.254.142",  
    "resourceGroup": "myResourceGroup"  
}
```

Open port 80 for web traffic

By default, only SSH connections are allowed into Linux VMs deployed in Azure. Because this VM is going to be a web server, you need to open port 80 from the internet. Use the [az vm open-port](#) command to open the desired port.

```
az vm open-port --port 80 --resource-group myResourceGroup --name myVM
```

SSH into your VM

If you don't already know the public IP address of your VM, run the [az network public-ip list](#) command. You need this IP address for several later steps.

```
az network public-ip list --resource-group myResourceGroup --query [].ipAddress
```

Use the following command to create an SSH session with the virtual machine. Substitute the correct public IP address of your virtual machine. In this example, the IP address is *40.68.254.142*. *azureuser* is the administrator user name set when you created the VM.

```
ssh azureuser@40.68.254.142
```

Install NGINX, MySQL, and PHP

Run the following command to update Ubuntu package sources and install NGINX, MySQL, and PHP.

```
sudo apt update && sudo apt install nginx && sudo apt install mysql-server php-mysql php-fpm
```

You are prompted to install the packages and other dependencies. This process installs the minimum required PHP extensions needed to use PHP with MySQL.

Verify installation and configuration

Verify NGINX

Check the version of NGINX with the following command:

```
nginx -v
```

With NGINX installed, and port 80 open to your VM, the web server can now be accessed from the internet. To

view the NGINX welcome page, open a web browser, and enter the public IP address of the VM. Use the public IP address you used to SSH to the VM:



Verify and secure MySQL

Check the version of MySQL with the following command (note the capital `v` parameter):

```
mysql -v
```

To help secure the installation of MySQL, including setting a root password, run the `mysql_secure_installation` script.

```
sudo mysql_secure_installation
```

You can optionally set up the Validate Password Plugin (recommended). Then, set a password for the MySQL root user, and configure the remaining security settings for your environment. We recommend that you answer "Y" (yes) to all questions.

If you want to try MySQL features (create a MySQL database, add users, or change configuration settings), login to MySQL. This step is not required to complete this tutorial.

```
sudo mysql -u root -p
```

When done, exit the mysql prompt by typing `\q`.

Verify PHP

Check the version of PHP with the following command:

```
php -v
```

Configure NGINX to use the PHP FastCGI Process Manager (PHP-FPM). Run the following commands to back up the original NGINX server block config file and then edit the original file in an editor of your choice:

```
sudo cp /etc/nginx/sites-available/default /etc/nginx/sites-available/default_backup  
sudo sensible-editor /etc/nginx/sites-available/default
```

In the editor, replace the contents of `/etc/nginx/sites-available/default` with the following. See the comments for explanation of the settings. Substitute the public IP address of your VM for `yourPublicIPAddress`, confirm the PHP

version in `fastcgi_pass`, and leave the remaining settings. Then save the file.

```
server {
    listen 80 default_server;
    listen [::]:80 default_server;

    root /var/www/html;
    # Homepage of website is index.php
    index index.php;

    server_name yourPublicIPAddress;

    location / {
        try_files $uri $uri/ =404;
    }

    # Include FastCGI configuration for NGINX
    location ~ \.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/run/php/php7.2-fpm.sock;
    }
}
```

Check the NGINX configuration for syntax errors:

```
sudo nginx -t
```

If the syntax is correct, restart NGINX with the following command:

```
sudo service nginx restart
```

If you want to test further, create a quick PHP info page to view in a browser. The following command creates the PHP info page:

```
sudo sh -c 'echo "<?php phpinfo(); ?>" > /var/www/html/info.php'
```

Now you can check the PHP info page you created. Open a browser and go to

<http://yourPublicIPAddress/info.php>. Substitute the public IP address of your VM. It should look similar to this image.

PHP Version 7.2.10-0ubuntu0.18.04.1	
System	Linux myVM 4.15.0-1036-azure #38-Ubuntu SMP Fri Dec 7 02:47:47 UTC 2018 x86_64
Build Date	Sep 13 2018 13:45:02
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.2/apache2
Loaded Configuration File	/etc/php/7.2/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.2/apache2/conf.d
Additional .ini files parsed	/etc/php/7.2/apache2/conf.d/10-mysqlind.ini, /etc/php/7.2/apache2/conf.d/10-opcache.ini, /etc/php/7.2/apache2/conf.d/10-pdo.ini, /etc/php/7.2/apache2/conf.d/20-calendar.ini, /etc/php/7.2/apache2/conf.d/20-ctype.ini, /etc/php/7.2/apache2/conf.d/20-exif.ini, /etc/php/7.2/apache2/conf.d/20-fileinfo.ini, /etc/php/7.2/apache2/conf.d/20-ftp.ini, /etc/php/7.2/apache2/conf.d/20-gettext.ini, /etc/php/7.2/apache2/conf.d/20-iconv.ini, /etc/php/7.2/apache2/conf.d/20-json.ini, /etc/php/7.2/apache2/conf.d/20-mysqli.ini, /etc/php/7.2/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.2/apache2/conf.d/20-phar.ini, /etc/php/7.2/apache2/conf.d/20-posix.ini, /etc/php/7.2/apache2/conf.d/20-readline.ini, /etc/php/7.2/apache2/conf.d/20-shmop.ini, /etc/php/7.2/apache2/conf.d/20-sockets.ini, /etc/php/7.2/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.2/apache2/conf.d/20-sysvsem.ini, /etc/php/7.2/apache2/conf.d/20-sysvshm.ini, /etc/php/7.2/apache2/conf.d/20-tokenizer.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718.NTS
PHP Extension Build	API20170718.NTS

Install WordPress

If you want to try your stack, install a sample app. As an example, the following steps install the open source [WordPress](#) platform to create websites and blogs. Other workloads to try include [Drupal](#) and [Moodle](#).

This WordPress setup is only for proof of concept. To install the latest WordPress in production with recommended security settings, see the [WordPress documentation](#).

Install the WordPress package

Run the following command:

```
sudo apt install wordpress
```

Configure WordPress

Configure WordPress to use MySQL and PHP.

In a working directory, create a text file `wordpress.sql` to configure the MySQL database for WordPress:

```
sudo sensible-editor wordpress.sql
```

Add the following commands, substituting a database password of your choice for `yourPassword` (leave other values unchanged). If you previously set up a MySQL security policy to validate password strength, make sure the password meets the strength requirements. Save the file.

```
CREATE DATABASE wordpress;
GRANT SELECT,INSERT,UPDATE,DELETE,CREATE,DROP,ALTER
ON wordpress.* 
TO wordpress@localhost
IDENTIFIED BY 'yourPassword';
```

Run the following command to create the database:

```
cat wordpress.sql | sudo mysql --defaults-extra-file=/etc/mysql/debian.cnf
```

Because the file `wordpress.sql` contains database credentials, delete it after use:

```
sudo rm wordpress.sql
```

To configure PHP, run the following command to open a text editor of your choice and create the file

```
/etc/wordpress/config-localhost.php :
```

```
sudo sensible-editor /etc/wordpress/config-localhost.php
```

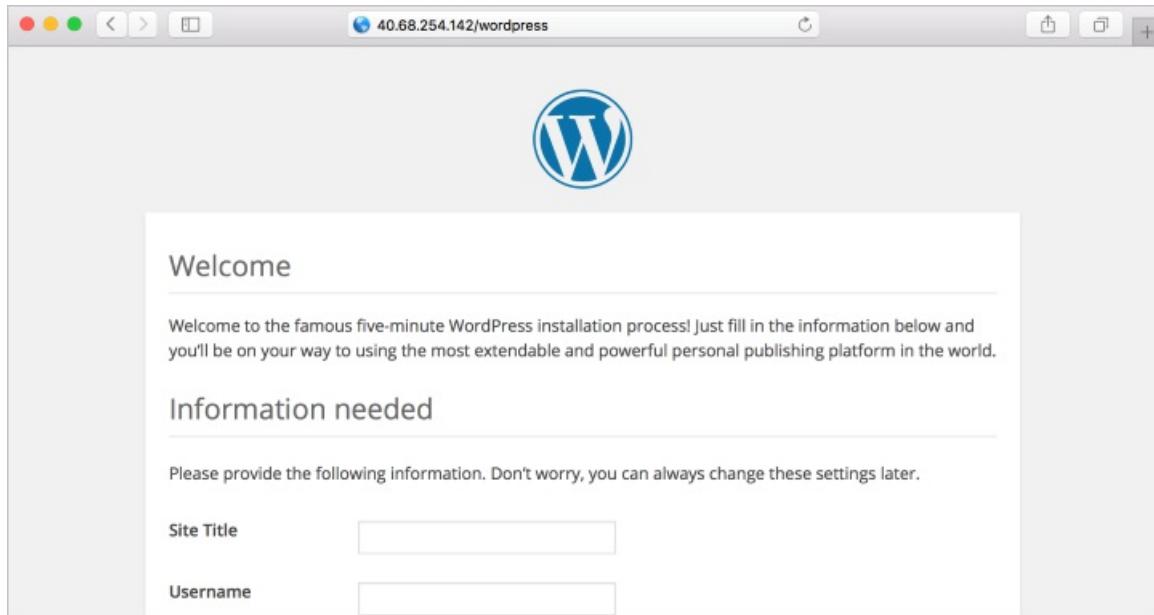
Copy the following lines to the file, substituting your WordPress database password for *yourPassword* (leave other values unchanged). Then save the file.

```
<?php
define('DB_NAME', 'wordpress');
define('DB_USER', 'wordpress');
define('DB_PASSWORD', 'yourPassword');
define('DB_HOST', 'localhost');
define('WP_CONTENT_DIR', '/usr/share/wordpress/wp-content');
?>
```

Move the WordPress installation to the web server document root:

```
sudo ln -s /usr/share/wordpress /var/www/html/wordpress
sudo mv /etc/wordpress/config-localhost.php /etc/wordpress/config-default.php
```

Now you can complete the WordPress setup and publish on the platform. Open a browser and go to <http://yourPublicIPAddress/wordpress>. Substitute the public IP address of your VM. It should look similar to this image.



Next steps

In this tutorial, you deployed a LEMP server in Azure. You learned how to:

- Create an Ubuntu VM
- Open port 80 for web traffic

- Install NGINX, MySQL, and PHP
- Verify installation and configuration
- Install WordPress on the LEMP stack

Advance to the next tutorial to learn how to secure web servers with SSL certificates.

[Secure web server with SSL](#)

Tutorial: Create a MongoDB, Express, AngularJS, and Node.js (MEAN) stack on a Linux virtual machine in Azure

11/13/2019 • 6 minutes to read • [Edit Online](#)

This tutorial shows you how to implement a MongoDB, Express, AngularJS, and Nodejs (MEAN) stack on a Linux virtual machine (VM) in Azure. The MEAN stack that you create enables adding, deleting, and listing books in a database. You learn how to:

- Create a Linux VM
- Install Nodejs
- Install MongoDB and set up the server
- Install Express and set up routes to the server
- Access the routes with AngularJS
- Run the application

This tutorial uses the CLI within the [Azure Cloud Shell](#), which is constantly updated to the latest version. To open the Cloud Shell, select **Try it** from the top of any code block.

If you choose to install and use the CLI locally, this tutorial requires that you are running the Azure CLI version 2.0.30 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Create a Linux VM

Create a resource group with the `az group create` command and create a Linux VM with the `az vm create` command. An Azure resource group is a logical container into which Azure resources are deployed and managed.

The following example uses the Azure CLI to create a resource group named *myResourceGroupMEAN* in the *eastus* location. A VM is created named *myVM* with SSH keys if they do not already exist in a default key location. To use a specific set of keys, use the `--ssh-key-value` option.

```
az group create --name myResourceGroupMEAN --location eastus
az vm create \
    --resource-group myResourceGroupMEAN \
    --name myVM \
    --image UbuntuLTS \
    --admin-username azureuser \
    --admin-password 'Azure12345678!' \
    --generate-ssh-keys
az vm open-port --port 3300 --resource-group myResourceGroupMEAN --name myVM
```

When the VM has been created, the Azure CLI shows information similar to the following example:

```
{  
    "fqdns": "",  
    "id": "/subscriptions/{subscription-  
id}/resourceGroups/myResourceGroupMEAN/providers/Microsoft.Compute/virtualMachines/myVM",  
    "location": "eastus",  
    "macAddress": "00-0D-3A-23-9A-49",  
    "powerState": "VM running",  
    "privateIpAddress": "10.0.0.4",  
    "publicIpAddress": "13.72.77.9",  
    "resourceGroup": "myResourceGroupMEAN"  
}
```

Take note of the `publicIpAddress`. This address is used to access the VM.

Use the following command to create an SSH session with the VM. Make sure to use the correct public IP address. In our example above our IP address was 13.72.77.9.

```
ssh azureuser@13.72.77.9
```

Install Node.js

[Node.js](#) is a JavaScript runtime built on Chrome's V8 JavaScript engine. Node.js is used in this tutorial to set up the Express routes and AngularJS controllers.

On the VM, using the bash shell that you opened with SSH, install Node.js.

```
sudo apt-get install -y nodejs
```

Install MongoDB and set up the server

[MongoDB](#) stores data in flexible, JSON-like documents. Fields in a database can vary from document to document and data structure can be changed over time. For our example application, we are adding book records to MongoDB that contain book name, isbn number, author, and number of pages.

1. On the VM, using the bash shell that you opened with SSH, set the MongoDB key.

```
sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv  
0C49F3730359A14518585931BC711F9BA15703C6  
echo "deb [ arch=amd64 ] https://repo.mongodb.org/apt/ubuntu trusty/mongodb-org/3.4 multiverse" | sudo  
tee /etc/apt/sources.list.d/mongodb-org-3.4.list
```

2. Update the package manager with the key.

```
sudo apt-get update
```

3. Install MongoDB.

```
sudo apt-get install -y mongodb
```

4. Start the server.

```
sudo service mongodb start
```

5. We also need to install the [body-parser](#) package to help us process the JSON passed in requests to the server.

Install the npm package manager.

```
sudo apt-get install npm
```

Install the body parser package.

```
sudo npm install body-parser
```

6. Create a folder named *Books* and add a file to it named *server.js* that contains the configuration for the web server.

```
var express = require('express');
var bodyParser = require('body-parser');
var app = express();
app.use(express.static(__dirname + '/public'));
app.use(bodyParser.json());
require('./apps/routes')(app);
app.set('port', 3300);
app.listen(app.get('port'), function() {
  console.log('Server up: http://localhost:' + app.get('port'));
});
```

Install Express and set up routes to the server

[Express](#) is a minimal and flexible Node.js web application framework that provides features for web and mobile applications. Express is used in this tutorial to pass book information to and from our MongoDB database.

[Mongoose](#) provides a straight-forward, schema-based solution to model your application data. Mongoose is used in this tutorial to provide a book schema for the database.

1. Install Express and Mongoose.

```
sudo npm install express mongoose
```

2. In the *Books* folder, create a folder named *apps* and add a file named *routes.js* with the express routes defined.

```

var Book = require('./models/book');
module.exports = function(app) {
  app.get('/book', function(req, res) {
    Book.find({}, function(err, result) {
      if (err) throw err;
      res.json(result);
    });
  });
  app.post('/book', function(req, res) {
    var book = new Book({
      name: req.body.name,
      isbn: req.body.isbn,
      author: req.body.author,
      pages: req.body.pages
    });
    book.save(function(err, result) {
      if (err) throw err;
      res.json({
        message: "Successfully added book",
        book: result
      });
    });
  });
  app.delete("/book/:isbn", function(req, res) {
    Book.findOneAndRemove(req.query, function(err, result) {
      if (err) throw err;
      res.json({
        message: "Successfully deleted the book",
        book: result
      });
    });
  });
  var path = require('path');
  app.get('*', function(req, res) {
    res.sendfile(path.join(__dirname + '/public', 'index.html'));
  });
};

```

- In the `apps` folder, create a folder named `models` and add a file named `book.js` with the book model configuration defined.

```

var mongoose = require('mongoose');
var dbHost = 'mongodb://localhost:27017/test';
mongoose.connect(dbHost);
mongoose.connection;
mongoose.set('debug', true);
var bookSchema = mongoose.Schema({
  name: String,
  isbn: {type: String, index: true},
  author: String,
  pages: Number
});
var Book = mongoose.model('Book', bookSchema);
module.exports = mongoose.model('Book', bookSchema);

```

Access the routes with AngularJS

[AngularJS](#) provides a web framework for creating dynamic views in your web applications. In this tutorial, we use AngularJS to connect our web page with Express and perform actions on our book database.

- Change the directory back up to `Books` (`cd ../../`), and then create a folder named `public` and add a file named `script.js` with the controller configuration defined.

```

var app = angular.module('myApp', []);
app.controller('myCtrl', function($scope, $http) {
  $http({
    method: 'GET',
    url: '/book'
  }).then(function successCallback(response) {
    $scope.books = response.data;
  }, function errorCallback(response) {
    console.log('Error: ' + response);
  });
  $scope.del_book = function(book) {
    $http({
      method: 'DELETE',
      url: '/book/:isbn',
      params: {'isbn': book.isbn}
    }).then(function successCallback(response) {
      console.log(response);
    }, function errorCallback(response) {
      console.log('Error: ' + response);
    });
  };
  $scope.add_book = function() {
    var body = '{ "name": "' + $scope.Name +
    '", "isbn": "' + $scope.Isbn +
    '", "author": "' + $scope.Author +
    '", "pages": "' + $scope.Pages + '" }';
    $http({
      method: 'POST',
      url: '/book',
      data: body
    }).then(function successCallback(response) {
      console.log(response);
    }, function errorCallback(response) {
      console.log('Error: ' + response);
    });
  };
});

```

2. In the *public* folder, create a file named *index.html* with the web page defined.

```

<!doctype html>
<html ng-app="myApp" ng-controller="myCtrl">
  <head>
    <script src="https://ajax.googleapis.com/ajax/libs/angularjs/1.6.4/angular.min.js"></script>
    <script src="script.js"></script>
  </head>
  <body>
    <div>
      <table>
        <tr>
          <td>Name:</td>
          <td><input type="text" ng-model="Name"></td>
        </tr>
        <tr>
          <td>Isbn:</td>
          <td><input type="text" ng-model="Isbn"></td>
        </tr>
        <tr>
          <td>Author:</td>
          <td><input type="text" ng-model="Author"></td>
        </tr>
        <tr>
          <td>Pages:</td>
          <td><input type="number" ng-model="Pages"></td>
        </tr>
      </table>
      <button ng-click="add_book()">Add</button>
    </div>
    <hr>
    <div>
      <table>
        <tr>
          <th>Name</th>
          <th>Isbn</th>
          <th>Author</th>
          <th>Pages</th>
        </tr>
        <tr ng-repeat="book in books">
          <td><input type="button" value="Delete" data-ng-click="del_book(book)"></td>
          <td>{{book.name}}</td>
          <td>{{book.isbn}}</td>
          <td>{{book.author}}</td>
          <td>{{book.pages}}</td>
        </tr>
      </table>
    </div>
  </body>
</html>

```

Run the application

1. Change the directory back up to *Books* (`cd ..`) and start the server by running this command:

```
nodejs server.js
```

2. Open a web browser to the address that you recorded for the VM. For example, `http://13.72.77.9:3300`. You should see something like the following page:

The screenshot shows a web browser window with the URL `13.72.77.9:3300`. The page contains a form for adding a book. It has four text input fields labeled `Name`, `Isbn`, `Author`, and `Pages`, each with a placeholder value. Below the form is a horizontal line, followed by a table header row with columns `Name`, `Isbn`, `Author`, and `Pages`.

3. Enter data into the textboxes and click **Add**. For example:

The screenshot shows the same web browser window after data has been entered into the form. The `Name` field now contains `MyBook`, the `Isbn` field contains `000001`, the `Author` field contains `Me`, and the `Pages` field contains `200`. The **Add** button is visible below the form.

4. After refreshing the page, you should see something like this page:

The screenshot shows the web browser after a refresh. The page displays a table with one row of data. The columns are labeled `Name`, `Isbn`, `Author`, and `Pages`. The data row contains the values `MyBook`, `000001`, `Me`, and `200`. A **Delete** button is located to the left of the first column.

5. You could click **Delete** and remove the book record from the database.

Next steps

In this tutorial, you created a web application that keeps track of book records using a MEAN stack on a Linux VM. You learned how to:

- Create a Linux VM
- Install Node.js
- Install MongoDB and set up the server
- Install Express and set up routes to the server
- Access the routes with AngularJS
- Run the application

Advance to the next tutorial to learn how to secure web servers with SSL certificates.

[Secure web server with SSL](#)

Tutorial: Secure a web server on a Linux virtual machine in Azure with SSL certificates stored in Key Vault

12/9/2019 • 4 minutes to read • [Edit Online](#)

To secure web servers, a Secure Sockets Layer (SSL) certificate can be used to encrypt web traffic. These SSL certificates can be stored in Azure Key Vault, and allow secure deployments of certificates to Linux virtual machines (VMs) in Azure. In this tutorial you learn how to:

- Create an Azure Key Vault
- Generate or upload a certificate to the Key Vault
- Create a VM and install the NGINX web server
- Inject the certificate into the VM and configure NGINX with an SSL binding

This tutorial uses the CLI within the [Azure Cloud Shell](#), which is constantly updated to the latest version. To open the Cloud Shell, select **Try it** from the top of any code block.

If you choose to install and use the CLI locally, this tutorial requires that you are running the Azure CLI version 2.0.30 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Overview

Azure Key Vault safeguards cryptographic keys and secrets, such as certificates or passwords. Key Vault helps streamline the certificate management process and enables you to maintain control of keys that access those certificates. You can create a self-signed certificate inside Key Vault, or upload an existing, trusted certificate that you already own.

Rather than using a custom VM image that includes certificates baked-in, you inject certificates into a running VM. This process ensures that the most up-to-date certificates are installed on a web server during deployment. If you renew or replace a certificate, you don't also have to create a new custom VM image. The latest certificates are automatically injected as you create additional VMs. During the whole process, the certificates never leave the Azure platform or are exposed in a script, command-line history, or template.

Create an Azure Key Vault

Before you can create a Key Vault and certificates, create a resource group with [az group create](#). The following example creates a resource group named *myResourceGroupSecureWeb* in the *eastus* location:

```
az group create --name myResourceGroupSecureWeb --location eastus
```

Next, create a Key Vault with [az keyvault create](#) and enable it for use when you deploy a VM. Each Key Vault requires a unique name, and should be all lowercase. Replace *<mykeyvault>* in the following example with your own unique Key Vault name:

```
keyvault_name=<mykeyvault>
az keyvault create \
--resource-group myResourceGroupSecureWeb \
--name $keyvault_name \
--enabled-for-deployment
```

Generate a certificate and store in Key Vault

For production use, you should import a valid certificate signed by trusted provider with [az keyvault certificate import](#). For this tutorial, the following example shows how you can generate a self-signed certificate with [az keyvault certificate create](#) that uses the default certificate policy:

```
az keyvault certificate create \
--vault-name $keyvault_name \
--name mycert \
--policy "$(az keyvault certificate get-default-policy)"
```

Prepare a certificate for use with a VM

To use the certificate during the VM create process, obtain the ID of your certificate with [az keyvault secret list-versions](#). Convert the certificate with [az vm secret format](#). The following example assigns the output of these commands to variables for ease of use in the next steps:

```
secret=$(az keyvault secret list-versions \
--vault-name $keyvault_name \
--name mycert \
--query "[?attributes.enabled].id" --output tsv)
vm_secret=$(az vm secret format --secrets "$secret" -g myResourceGroupSecureWeb --keyvault $keyvault_name)
```

Create a cloud-init config to secure NGINX

[Cloud-init](#) is a widely used approach to customize a Linux VM as it boots for the first time. You can use cloud-init to install packages and write files, or to configure users and security. As cloud-init runs during the initial boot process, there are no additional steps or required agents to apply your configuration.

When you create a VM, certificates and keys are stored in the protected `/var/lib/waagent/` directory. To automate adding the certificate to the VM and configuring the web server, use cloud-init. In this example, you install and configure the NGINX web server. You can use the same process to install and configure Apache.

Create a file named `cloud-init-web-server.txt` and paste the following configuration:

```
#cloud-config
package_upgrade: true
packages:
- nginx
write_files:
- owner: www-data:www-data
- path: /etc/nginx/sites-available/default
content: |
  server {
    listen 443 ssl;
    ssl_certificate /etc/nginx/ssl/mycert.cert;
    ssl_certificate_key /etc/nginx/ssl/mycert.prv;
  }
runcmd:
- secretsname=$(find /var/lib/waagent/ -name "*.prv" | cut -c -57)
- mkdir /etc/nginx/ssl
- cp $secretsname.crt /etc/nginx/ssl/mycert.cert
- cp $secretsname.prv /etc/nginx/ssl/mycert.prv
- service nginx restart
```

Create a secure VM

Now create a VM with [az vm create](#). The certificate data is injected from Key Vault with the `--secrets` parameter. You pass in the cloud-init config with the `--custom-data` parameter:

```
az vm create \
--resource-group myResourceGroupSecureWeb \
--name myVM \
--image UbuntuLTS \
--admin-username azureuser \
--generate-ssh-keys \
--custom-data cloud-init-web-server.txt \
--secrets "$vm_secret"
```

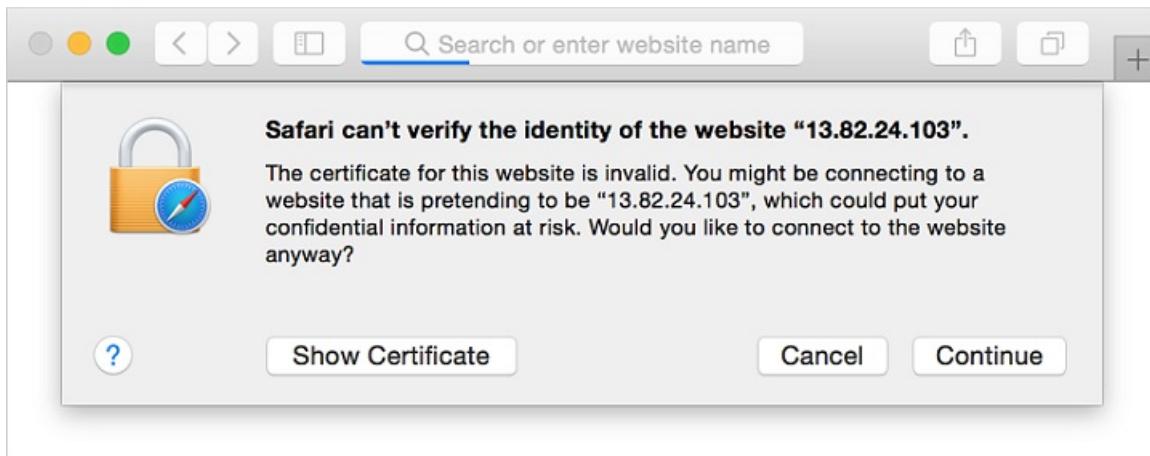
It takes a few minutes for the VM to be created, the packages to install, and the app to start. When the VM has been created, take note of the `publicIpAddress` displayed by the Azure CLI. This address is used to access your site in a web browser.

To allow secure web traffic to reach your VM, open port 443 from the Internet with [az vm open-port](#):

```
az vm open-port \
--resource-group myResourceGroupSecureWeb \
--name myVM \
--port 443
```

Test the secure web app

Now you can open a web browser and enter `https://<publicIpAddress>` in the address bar. Provide your own public IP address from the VM create process. Accept the security warning if you used a self-signed certificate:



Your secured NGINX site is then displayed as in the following example:



Next steps

In this tutorial, you secured an NGINX web server with an SSL certificate stored in Azure Key Vault. You learned how to:

- Create an Azure Key Vault
- Generate or upload a certificate to the Key Vault
- Create a VM and install the NGINX web server
- Inject the certificate into the VM and configure NGINX with an SSL binding

Follow this link to see pre-built virtual machine script samples.

[Linux virtual machine script samples](#)

Azure CLI Samples for Linux virtual machines

11/13/2019 • 2 minutes to read • [Edit Online](#)

The following table includes links to bash scripts built using the Azure CLI.

Create virtual machines	
Create a virtual machine	Creates a Linux virtual machine with minimal configuration.
Create a fully configured virtual machine	Creates a resource group, virtual machine, and all related resources.
Create highly available virtual machines	Creates several virtual machines in a highly available and load balanced configuration.
Create a VM and run configuration script	Creates a virtual machine and uses the Azure Custom Script extension to install NGINX.
Create a VM with WordPress installed	Creates a virtual machine and uses the Azure Custom Script extension to install WordPress.
Create a VM from a managed OS disk	Creates a virtual machine by attaching an existing Managed Disk as OS disk.
Create a VM from a snapshot	Creates a virtual machine from a snapshot by first creating a managed disk from snapshot and then attaching the new managed disk as OS disk.
Manage storage	
Create managed disk from a VHD	Creates a managed disk from a specialized VHD as an OS disk or from a data VHD as data disk.
Create a managed disk from a snapshot	Creates a managed disk from a snapshot.
Copy managed disk to same or different subscription	Copies managed disk to same or different subscription but in the same region as the parent managed disk.
Export a snapshot as VHD to a storage account	Exports a managed snapshot as VHD to a storage account in different region.
Export the VHD of a managed disk to a storage account	Exports the underlying VHD of a managed disk to a storage account in different region.
Copy snapshot to same or different subscription	Copies snapshot to same or different subscription but in the same region as the parent snapshot.
Network virtual machines	

Secure network traffic between virtual machines	Creates two virtual machines, all related resources, and an internal and external network security groups (NSG).
Secure virtual machines	
Encrypt a VM and data disks	Creates an Azure Key Vault, encryption key, and service principal, then encrypts a VM.
Monitor virtual machines	
Monitor a VM with Azure Monitor logs	Creates a virtual machine, installs the Log Analytics agent, and enrolls the VM in an Log Analytics workspace.
Troubleshoot virtual machines	
Troubleshoot a VMs operating system disk	Mounts the operating system disk from one VM as a data disk on a second VM.

Azure Virtual Machine PowerShell samples

11/13/2019 • 2 minutes to read • [Edit Online](#)

The following table includes links to PowerShell scripts samples that create and manage Linux virtual machines.

Create virtual machines	
Create a fully configured virtual machine	Creates a resource group, virtual machine, and all related resources.
Create a VM with Docker enabled	Creates a virtual machine, configures this VM as a Docker host, and runs an NGINX container.
Create a VM and run configuration script	Creates a virtual machine and uses the Azure Custom Script extension to install NGINX.
Create a VM with WordPress installed	Creates a virtual machine and uses the Azure Custom Script extension to install WordPress.
Create a VM from a managed OS disk	Creates a virtual machine by attaching an existing Managed Disk as OS disk.
Create a VM from a snapshot	Creates a virtual machine from a snapshot by first creating a managed disk from the snapshot and then attaching the new managed disk as OS disk.
Manage storage	
Create a managed disk from a VHD in the same or a different subscription	Creates a managed disk from a specialized VHD as an OS disk, or from a data VHD as a data disk, in the same or a different subscription.
Create a managed disk from a snapshot	Creates a managed disk from a snapshot.
Export a snapshot as a VHD to a storage account	Exports a managed snapshot as a VHD to a storage account in a different region.
Export the VHD of a managed disk to a storage account	Exports the underlying VHD of a managed disk to a storage account in a different region.
Create a snapshot from a VHD	Creates a snapshot from a VHD and then uses that snapshot to create multiple identical managed disks quickly.
Copy a snapshot to the same or a different subscription	Copies snapshot to the same or a different subscription that is in the same region as the parent snapshot.
Monitor virtual machines	
Monitor a VM with Azure Monitor logs	Creates a virtual machine, installs the Log Analytics agent, and enrolls the VM in a Log Analytics workspace.

Copy a managed disk to the same or a different subscription	Copies a managed disk to the same or a different subscription that is in the same region as the parent managed disk.
Collect details about all VMs in a subscription with PowerShell	Creates a csv that contains the VM Name, Resource Group Name, Region, Virtual Network, Subnet, Private IP Address, OS Type, and Public IP Address of the VMs in the provided subscription.

Azure Resource Manager overview

12/23/2019 • 5 minutes to read • [Edit Online](#)

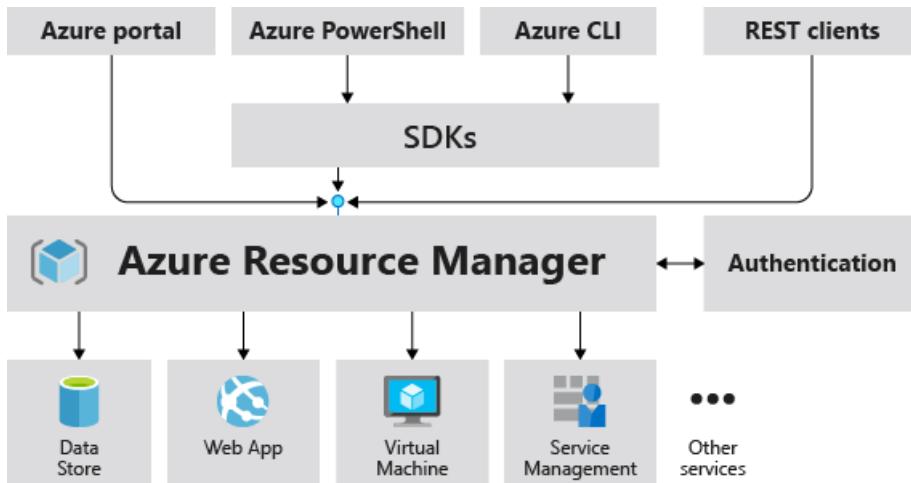
Azure Resource Manager is the deployment and management service for Azure. It provides a management layer that enables you to create, update, and delete resources in your Azure subscription. You use management features, like access control, locks, and tags, to secure and organize your resources after deployment.

To learn about Azure Resource Manager templates, see [Template deployment overview](#).

Consistent management layer

When a user sends a request from any of the Azure tools, APIs, or SDKs, Resource Manager receives the request. It authenticates and authorizes the request. Resource Manager sends the request to the Azure service, which takes the requested action. Because all requests are handled through the same API, you see consistent results and capabilities in all the different tools.

The following image shows the role Azure Resource Manager plays in handling Azure requests.



All capabilities that are available in the portal are also available through PowerShell, Azure CLI, REST APIs, and client SDKs. Functionality initially released through APIs will be represented in the portal within 180 days of initial release.

Terminology

If you're new to Azure Resource Manager, there are some terms you might not be familiar with.

- **resource** - A manageable item that is available through Azure. Virtual machines, storage accounts, web apps, databases, and virtual networks are examples of resources.
- **resource group** - A container that holds related resources for an Azure solution. The resource group includes those resources that you want to manage as a group. You decide which resources belong in a resource group based on what makes the most sense for your organization. See [Resource groups](#).
- **resource provider** - A service that supplies Azure resources. For example, a common resource provider is Microsoft.Compute, which supplies the virtual machine resource. Microsoft.Storage is another common resource provider. See [Resource providers and types](#).
- **Resource Manager template** - A JavaScript Object Notation (JSON) file that defines one or more resources to deploy to a resource group or subscription. The template can be used to deploy the resources consistently and repeatedly. See [Template deployment overview](#).

- **declarative syntax** - Syntax that lets you state "Here is what I intend to create" without having to write the sequence of programming commands to create it. The Resource Manager template is an example of declarative syntax. In the file, you define the properties for the infrastructure to deploy to Azure. See [Template deployment overview](#).

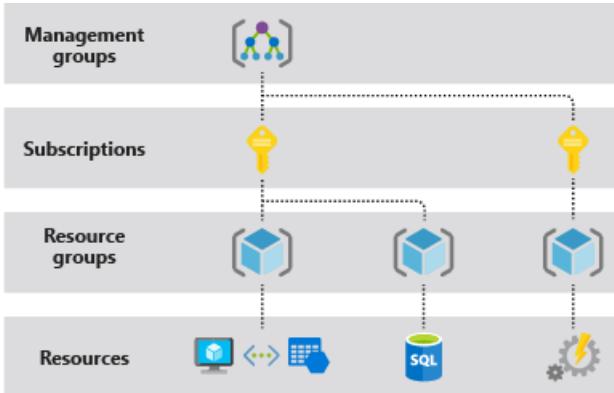
The benefits of using Resource Manager

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 in your resource group because Role-Based Access Control (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.

Understand scope

Azure provides four levels of scope: [management groups](#), subscriptions, [resource groups](#), and resources. The following image shows an example of these layers.



You apply management settings at any of these levels of scope. The level you select determines how widely the setting is applied. Lower levels inherit settings from higher levels. For example, when you apply a [policy](#) to the subscription, the policy is applied to all resource groups and resources in your subscription. When you apply a policy on the resource group, that policy is applied to the resource group and all its resources. However, another resource group doesn't have that policy assignment.

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

Resource groups

There are some important factors to consider when defining your resource group:

- All the resources in your group should share the same lifecycle. You deploy, update, and delete them together. If one resource, such as a database server, needs to exist on a different deployment cycle it should be in another resource group.

- Each resource can only exist in 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. For more information, see [Move resources to new resource group or subscription](#).
- A resource group can contain resources that are located in different regions.
- A resource group can be used to scope access control for administrative actions.
- A resource can interact with resources in other resource groups. This interaction is common when the two resources are related but don't share the same lifecycle (for example, web apps connecting to a database).

When creating a resource group, you need to provide a location for that resource group. You may be wondering, "Why does a resource group need a location? And, if the resources can have different locations than the resource group, why does the resource group location matter at all?" The resource group stores metadata about the resources. When you specify a location for the resource group, you're specifying where that metadata is stored. For compliance reasons, you may need to ensure that your data is stored in a particular region.

If the resource group's region is temporarily unavailable, you can't update resources in the resource group because the metadata is unavailable. The resources in other regions will still function as expected, but you can't update them. For more information about building reliable applications, see [Designing reliable Azure applications](#).

Resiliency of Azure Resource Manager

The Azure Resource Manager service is designed for resiliency and continuous availability. Resource Manager and control plane operations (requests sent to management.azure.com) in the REST API are:

- Distributed across regions. Some services are regional.
- Distributed across Availability Zones (as well regions) in locations that have multiple Availability Zones.
- Not dependent on a single logical data center.
- Never taken down for maintenance activities.

This resiliency applies to services that receive requests through Resource Manager. For example, Key Vault benefits from this resiliency.

Next steps

- For all the operations offered by resource providers, see the [Azure REST APIs](#).
- To learn about moving resources, see [Move resources to new resource group or subscription](#).
- To learn about tagging resources, see [Use tags to organize your Azure resources](#).
- To learn about locking resources, see [Lock resources to prevent unexpected changes](#).
- For information about creating templates for deployments, see [Template deployment overview](#).

Regions for virtual machines in Azure

1/19/2020 • 4 minutes to read • [Edit Online](#)

It is important to understand how and where your virtual machines (VMs) operate in Azure, along with your options to maximize performance, availability, and redundancy. This article provides you with an overview of the availability and redundancy features of Azure.

What are Azure regions?

Azure operates in multiple datacenters around the world. These datacenters are grouped in to geographic regions, giving you flexibility in choosing where to build your applications.

You create Azure resources in defined geographic regions like 'West US', 'North Europe', or 'Southeast Asia'. You can review the [list of regions and their locations](#). Within each region, multiple datacenters exist to provide for redundancy and availability. This approach gives you flexibility as you design applications to create VMs closest to your users and to meet any legal, compliance, or tax purposes.

Special Azure regions

Azure has some special regions that you may wish to use when building out your applications for compliance or legal purposes. These special regions include:

- **US Gov Virginia and US Gov Iowa**

- A physical and logical network-isolated instance of Azure for US government agencies and partners, operated by screened US persons. Includes additional compliance certifications such as [FedRAMP](#) and [DISA](#). Read more about [Azure Government](#).

- **China East and China North**

- These regions are available through a unique partnership between Microsoft and 21Vianet, whereby Microsoft does not directly maintain the datacenters. See more about [Azure China 21Vianet](#).

- **Germany Central and Germany Northeast**

- These regions are available via a data trustee model whereby customer data remains in Germany under control of T-Systems, a Deutsche Telekom company, acting as the German data trustee.

Region pairs

Each Azure region is paired with another region within the same geography (such as US, Europe, or Asia). This approach allows for the replication of resources, such as VM storage, across a geography that should reduce the likelihood of natural disasters, civil unrest, power outages, or physical network outages affecting both regions at once. Additional advantages of region pairs include:

- 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.
- 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 (except for Brazil South) for tax and law enforcement jurisdiction purposes.

Examples of region pairs include:

PRIMARY	SECONDARY
West US	East US
North Europe	West Europe
Southeast Asia	East Asia

You can see the full [list of regional pairs here](#).

Feature availability

Some services or VM features are only available in certain regions, such as specific VM sizes or storage types. There are also some global Azure services that do not require you to select a particular region, such as [Azure Active Directory](#), [Traffic Manager](#), or [Azure DNS](#). To assist you in designing your application environment, you can check the [availability of Azure services across each region](#). You can also [programmatically query the supported VM sizes and restrictions in each region](#).

Storage availability

Understanding Azure regions and geographies becomes important when you consider the available storage replication options. Depending on the storage type, you have different replication options.

Azure Managed Disks

- Locally redundant storage (LRS)
 - Replicates your data three times within the region in which you created your storage account.

Storage account-based disks

- Locally redundant storage (LRS)
 - Replicates your data three times within the region in which you created your storage account.
- Zone redundant storage (ZRS)
 - Replicates your data three times across two to three facilities, either within a single region or across two regions.
- Geo-redundant storage (GRS)
 - Replicates your data to a secondary region that is hundreds of miles away from the primary region.
- Read-access geo-redundant storage (RA-GRS)
 - Replicates your data to a secondary region, as with GRS, but also then provides read-only access to the data in the secondary location.

The following table provides a quick overview of the differences between the storage replication types:

REPLICATION STRATEGY	LRS	ZRS	GRS	RA-GRS
Data is replicated across multiple facilities.	No	Yes	Yes	Yes
Data can be read from the secondary location and from the primary location.	No	No	No	Yes

REPLICATION STRATEGY	LRS	ZRS	GRS	RA-GRS
Number of copies of data maintained on separate nodes.	3	3	6	6

You can read more about [Azure Storage replication options here](#). For more information about managed disks, see [Azure Managed Disks overview](#).

Storage costs

Prices vary depending on the storage type and availability that you select.

Azure Managed Disks

- Premium Managed Disks are backed by Solid-State Drives (SSDs) and Standard Managed Disks are backed by regular spinning disks. Both Premium and Standard Managed Disks are charged based on the provisioned capacity for the disk.

Unmanaged disks

- Premium storage is backed by Solid-State Drives (SSDs) and is charged based on the capacity of the disk.
- Standard storage is backed by regular spinning disks and is charged based on the in-use capacity and desired storage availability.
 - For RA-GRS, there is an additional Geo-Replication Data Transfer charge for the bandwidth of replicating that data to another Azure region.

See [Azure Storage Pricing](#) for pricing information on the different storage types and availability options.

Availability options for virtual machines in Azure

1/19/2020 • 5 minutes to read • [Edit Online](#)

This article provides you with an overview of the availability features of Azure virtual machines (VMs).

High availability

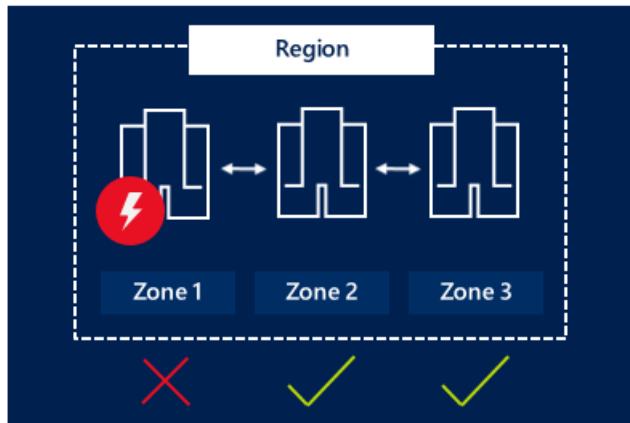
Workloads are typically spread across different virtual machines to gain high throughput, performance, and to create redundancy in case a VM is impacted due to an update or other event.

There are few options that Azure provides to achieve High Availability. First let's talk about basic constructs.

Availability zones

[Availability zones](#) expand the level of control you have to maintain the availability of the applications and data on your VMs. An Availability Zone is a physically separate zone, within an Azure region. There are three Availability Zones per supported Azure region.

Each Availability Zone has a distinct power source, network, and cooling. By architecting your solutions to use replicated VMs in zones, you can protect your apps and data from the loss of a datacenter. If one zone is compromised, then replicated apps and data are instantly available in another zone.



Learn more about deploying a [Windows](#) or [Linux](#) VM in an Availability Zone.

Fault domains

A fault domain is a logical group of underlying hardware that share a common power source and network switch, similar to a rack within an on-premises datacenter.

Update domains

An update domain is a logical group of underlying hardware that can undergo maintenance or be rebooted at the same time.

This approach ensures that at least one instance of your application always remains running as the Azure platform undergoes periodic maintenance. The order of update domains being rebooted may not proceed sequentially during maintenance, but only one update domain is rebooted at a time.

Virtual Machines Scale Sets

Azure virtual machine scale sets let you create and manage a group of load balanced VMs. The number of VM instances can automatically increase or decrease in response to demand or a defined schedule. Scale sets provide high availability to your applications, and allow you to centrally manage, configure, and update many VMs. We

recommended that two or more VMs are created within a scale set to provide for a highly available application and to meet the [99.95% Azure SLA](#). There is no cost for the scale set itself, you only pay for each VM instance that you create. When a single VM is using [Azure premium SSDs](#), the Azure SLA applies for unplanned maintenance events. Virtual machines in a scale set can be deployed across multiple update domains and fault domains to maximize availability and resilience to outages due to data center outages, and planned or unplanned maintenance events. Virtual machines in a scale set can also be deployed into a single Availability zone, or regionally. Availability zone deployment options may differ based on the orchestration mode.

Preview: Orchestration mode Preview

Virtual machines scale sets allow you to specify orchestration mode. With the virtual machine scale set orchestration mode (preview), you can now choose whether the scale set should orchestrate virtual machines which are created explicitly outside of a scale set configuration model, or virtual machine instances created implicitly based on the configuration model. Choose the orchestration mode that VM orchestration model allows you group explicitly defined Virtual Machines together in a region or in an availability zone. Virtual machines deployed in an Availability Zone provides zonal isolation to VMs as they are bound to the availability zone boundary and are not subjected to any failures that may occur in other availability zone in the region.

	"ORCHESTRATIONMODE": "VM" (VIRTUALMACHINE)	"ORCHESTRATIONMODE": "SCALESETVM" (VIRTUALMACHINESCALESET VM)
VM configuration model	None. VirtualMachineProfile is undefined in the scale set model.	Required. VirtualMachineProfile is populated in the scale set model.
Adding new VM to Scale Set	VMs are explicitly added to the scale set when the VM is created.	VMs are implicitly created and added to the scale set based on the VM configuration model, instance count, and AutoScaling rules.
Availability Zones	Supports regional deployment or VMs in one Availability Zone	Supports regional deployment or multiple Availability Zones; Can define the zone balancing strategy
Fault domains	Can define fault domains count. 2 or 3 based on regional support and 5 for Availability zone. The assigned VM fault domain will persist with VM lifecycle, including deallocate and restart.	Can define 1, 2, or 3 fault domains for non-zonal deployments, and 5 for Availability zone deployments. The assigned VM fault domain does not persist with VM lifecycle, virtual machines are assigned a fault domain at time of allocation.
Update domains	N/A. Update domains are automatically mapped to fault domains	N/A. Update domains are automatically mapped to fault domains

Fault domains and update domains

Virtual machine scale sets simplify designing for high availability by aligning fault domains and update domains. You will only have to define fault domains count for the scale set. The number of fault domains available to the scale sets may vary by region. See [Manage the availability of virtual machines in Azure](#).

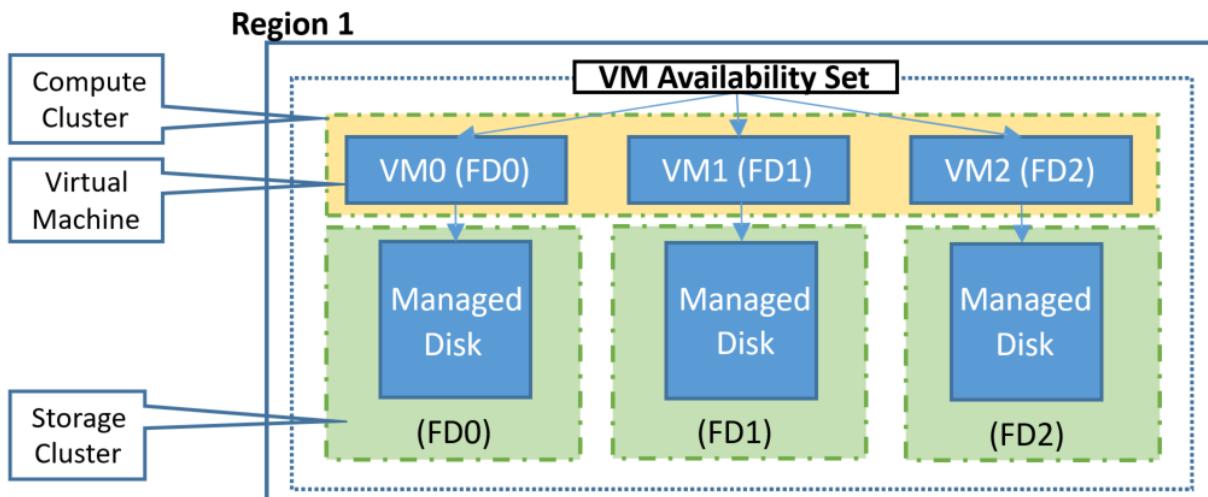
Availability sets

An availability set is a logical grouping of VMs within a datacenter 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](#). There is no cost for the Availability Set itself, you only pay for each VM instance that you create. When a single VM is using [Azure premium SSDs](#), the Azure SLA applies for unplanned maintenance events.

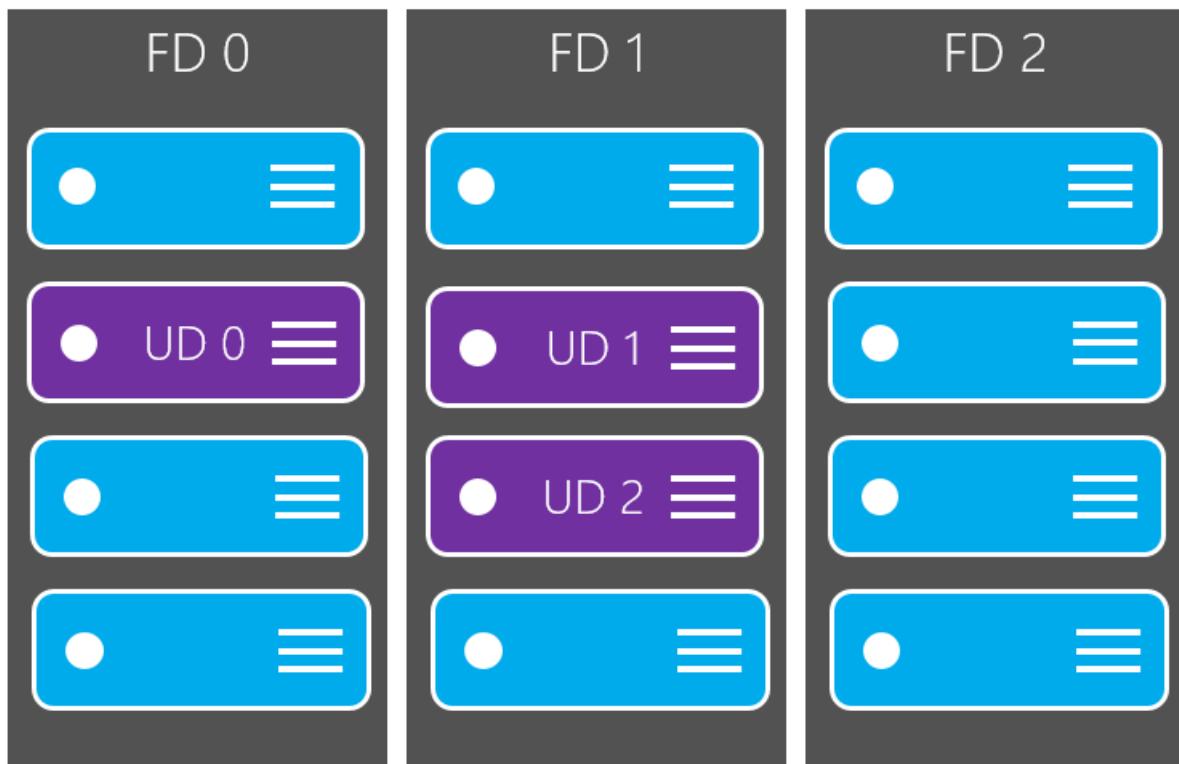
In an availability set, VMs are automatically distributed across these fault domains. This approach limits the impact of potential physical hardware failures, network outages, or power interruptions.

For VMs using [Azure Managed Disks](#), VMs are aligned with managed disk fault domains when using a managed availability set. This alignment ensures that all the managed disks attached to a VM are within the same managed disk fault domain.

Only VMs with managed disks can be created in a managed availability set. The number of managed disk fault domains varies by region - either two or three managed disk fault domains per region. You can read more about these managed disk fault domains for [Linux VMs](#) or [Windows VMs](#).



VMs within an availability set are also automatically distributed across update domains.



Next steps

You can now start to use these availability and redundancy features to build your Azure environment. For best practices information, see [Azure availability best practices](#).

Co-locate resources for improved latency

10/30/2019 • 3 minutes to read • [Edit Online](#)

When deploying your application in Azure, spreading instances across regions or availability zones creates network latency, which may impact the overall performance of your application.

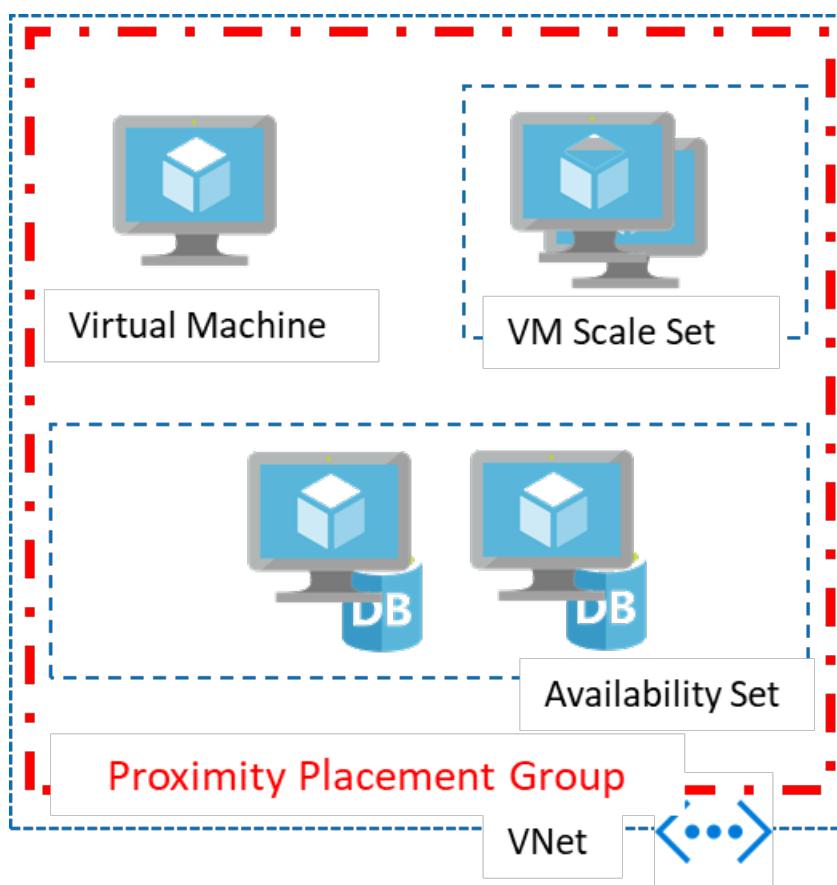
Proximity placement groups

Placing VMs in a single region reduces the physical distance between the instances. Placing them within a single availability zone will also bring them physically closer together. However, as the Azure footprint grows, a single availability zone may span multiple physical data centers, which may result in a network latency impacting your application.

To get VMs as close as possible, achieving the lowest possible latency, you should deploy them within a proximity placement group.

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.

- Low latency between stand-alone VMs.
- Low Latency between VMs in a single availability set or a virtual machine scale set.
- Low latency between stand-alone VMs, VMs in multiple Availability Sets, or multiple scale sets. You can have multiple compute resources in a single placement group to bring together a multi-tiered application.
- Low latency between multiple application tiers using different hardware types. For example, running the backend using M-series in an availability set and the front end on a D-series instance, in a scale set, in a single proximity placement group.



Using Proximity Placement Groups

A proximity placement group is a new resource type in Azure. You need to create one before using it with other resources. Once created, it could be used with virtual machines, availability sets, or virtual machine scale sets. You specify a proximity placement group when creating compute resources providing the proximity placement group ID.

You can also move an existing resource into a proximity placement group. When moving a resource into a proximity placement group, you should stop (deallocate) the asset first since it will be redeployed potentially into a different data center in the region so satisfy the colocation constraint.

In the case of availability sets and virtual machine scale sets, you should set the proximity placement group at the resource level rather than the individual virtual machines.

A proximity placement group is a colocation constraint rather than a pinning mechanism. It is pinned to a specific data center with the deployment of the first resource to use it. Once all resources using the proximity placement group have been stopped (deallocated) or deleted, it is no longer pinned. Therefore, when using a proximity placement group with multiple VM series, it is important to specify all the required types upfront in a template when possible or follow a deployment sequence which will improve your chances for a successful deployment. If your deployment fails, restart the deployment with the VM size which has failed as the first size to be deployed.

Best practices

- For the lowest latency, use proximity placement groups together with accelerated networking. For more information, see [Create a Linux virtual machine with Accelerated Networking](#) or [Create a Windows virtual machine with Accelerated Networking](#).
- Deploy all VM sizes in a single template. In order to avoid landing on hardware that doesn't support all the VM SKUs and sizes you require, include all of the application tiers in a single template so that they will all be deployed at the same time.
- If you are scripting your deployment using PowerShell, CLI or the SDK, you may get an allocation error `OverconstrainedAllocationRequest`. In this case, you should stop/deallocate all the existing VMs, and change the sequence in the deployment script to begin with the VM SKU/sizes that failed.
- When reusing an existing placement group from which VMs were deleted, wait for the deletion to fully complete before adding VMs to it.
- If latency is your first priority, put VMs in a proximity placement group and the entire solution in an availability zone. But, if resiliency is your top priority, spread your instances across multiple availability zones (a single proximity placement group cannot span zones).

Next steps

Deploy a VM to a [proximity placement group](#) using the Azure CLI.

Learn how to [test network latency](#).

Learn how to [optimize network throughput](#).

Learn how to [use proximity placement groups with SAP applications](#).

Optimize network throughput for Azure virtual machines

1/6/2020 • 3 minutes to read • [Edit Online](#)

Azure virtual machines (VM) have default network settings that can be further optimized for network throughput. This article describes how to optimize network throughput for Microsoft Azure Windows and Linux VMs, including major distributions such as Ubuntu, CentOS, and Red Hat.

Windows VM

If your Windows VM supports [Accelerated Networking](#), enabling that feature would be the optimal configuration for throughput. For all other Windows VMs, using Receive Side Scaling (RSS) can reach higher maximal throughput than a VM without RSS. RSS may be disabled by default in a Windows VM. To determine whether RSS is enabled, and enable it if it's currently disabled, complete the following steps:

1. See if RSS is enabled for a network adapter with the `Get-NetAdapterRss` PowerShell command. In the following example output returned from the `Get-NetAdapterRss`, RSS is not enabled.

```
Name      : Ethernet
InterfaceDescription : Microsoft Hyper-V Network Adapter
Enabled    : False
```

2. To enable RSS, enter the following command:

```
Get-NetAdapter | % {Enable-NetAdapterRss -Name $_.Name}
```

The previous command does not have an output. The command changed NIC settings, causing temporary connectivity loss for about one minute. A Reconnecting dialog box appears during the connectivity loss. Connectivity is typically restored after the third attempt.

3. Confirm that RSS is enabled in the VM by entering the `Get-NetAdapterRss` command again. If successful, the following example output is returned:

```
Name      : Ethernet
InterfaceDescription : Microsoft Hyper-V Network Adapter
Enabled    : True
```

Linux VM

RSS is always enabled by default in an Azure Linux VM. Linux kernels released since October 2017 include new network optimizations options that enable a Linux VM to achieve higher network throughput.

Ubuntu for new deployments

The Ubuntu Azure kernel provides the best network performance on Azure and has been the default kernel since September 21, 2017. In order to get this kernel, first install the latest supported version of 16.04-LTS, as follows:

```
"Publisher": "Canonical",
"Offer": "UbuntuServer",
"Sku": "16.04-LTS",
"Version": "latest"
```

After the creation is complete, enter the following commands to get the latest updates. These steps also work for VMs currently running the Ubuntu Azure kernel.

```
#run as root or preface with sudo
apt-get -y update
apt-get -y upgrade
apt-get -y dist-upgrade
```

The following optional command set may be helpful for existing Ubuntu deployments that already have the Azure kernel but that have failed to further updates with errors.

```
#optional steps may be helpful in existing deployments with the Azure kernel
#run as root or preface with sudo
apt-get -f install
apt-get --fix-missing install
apt-get clean
apt-get -y update
apt-get -y upgrade
apt-get -y dist-upgrade
```

Ubuntu Azure kernel upgrade for existing VMs

Significant throughput performance can be achieved by upgrading to the Azure Linux kernel. To verify whether you have this kernel, check your kernel version.

```
#Azure kernel name ends with "-azure"
uname -r

#sample output on Azure kernel:
#4.13.0-1007-azure
```

If your VM does not have the Azure kernel, the version number usually begins with "4.4." If the VM does not have the Azure kernel, run the following commands as root:

```
#run as root or preface with sudo
apt-get update
apt-get upgrade -y
apt-get dist-upgrade -y
apt-get install "linux-azure"
reboot
```

CentOS

In order to get the latest optimizations, it is best to create a VM with the latest supported version by specifying the following parameters:

```
"Publisher": "OpenLogic",
"Offer": "CentOS",
"Sku": "7.4",
"Version": "latest"
```

New and existing VMs can benefit from installing the latest Linux Integration Services (LIS). The throughput

optimization is in LIS, starting from 4.2.2-2, although later versions contain further improvements. Enter the following commands to install the latest LIS:

```
sudo yum update  
sudo reboot  
sudo yum install microsoft-hyper-v
```

Red Hat

In order to get the optimizations, it is best to create a VM with the latest supported version by specifying the following parameters:

```
"Publisher": "RedHat"  
"Offer": "RHEL"  
"Sku": "7-RAW"  
"Version": "latest"
```

New and existing VMs can benefit from installing the latest Linux Integration Services (LIS). The throughput optimization is in LIS, starting from 4.2. Enter the following commands to download and install LIS:

```
wget https://aka.ms/lis  
tar xvf lis  
cd LISISO  
sudo ./install.sh #or upgrade.sh if prior LIS was previously installed
```

Learn more about Linux Integration Services Version 4.2 for Hyper-V by viewing the [download page](#).

Next steps

- See the optimized result with [Bandwidth/Throughput testing Azure VM](#) for your scenario.
- Read about how [bandwidth is allocated to virtual machines](#)
- Learn more with [Azure Virtual Network frequently asked questions \(FAQ\)](#)

Sizes for Linux virtual machines in Azure

2/20/2020 • 2 minutes to read • [Edit Online](#)

This article describes the available sizes and options for the Azure virtual machines you can use to run your Linux apps and workloads. It also provides deployment considerations to be aware of when you're planning to use these resources. This article is also available for [Windows virtual machines](#).

Type	Sizes	Description
General purpose	B, Dsv3, Dv3, Dasv4, Dav4, DSv2, Dv2, Av2, DC	Balanced CPU-to-memory ratio. Ideal for testing and development, small to medium databases, and low to medium traffic web servers.
Compute optimized	Fsv2	High CPU-to-memory ratio. Good for medium traffic web servers, network appliances, batch processes, and application servers.
Memory optimized	Esv3, Ev3, Easv4, Eav4, 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	High disk throughput and IO ideal for Big Data, SQL, NoSQL databases, data warehousing and large transactional databases.
GPU	NC, NCv2, NCv3, ND, NDv2 (Preview), NV, NVv3, NVv4	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, HC, H	Our fastest and most powerful CPU virtual machines with optional high-throughput network interfaces (RDMA).

- For information about pricing of the various sizes, see [Virtual Machines Pricing](#).
- For availability of VM sizes in Azure regions, see [Products available by region](#).
- To see general limits on Azure VMs, see [Azure subscription and service limits, quotas, and constraints](#).
- Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

REST API

For information on using the REST API to query for VM sizes, see the following:

- [List available virtual machine sizes for resizing](#)
- [List available virtual machine sizes for a subscription](#)
- [List available virtual machine sizes in an availability set](#)

ACU

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

Benchmark scores

Learn more about compute performance for Linux VMs using the [CoreMark benchmark scores](#).

Next steps

Learn more about the different VM sizes that are available:

- [General purpose](#)
- [Compute optimized](#)
- [Memory optimized](#)
- [Storage optimized](#)
- [GPU](#)
- [High performance compute](#)
- Check the [Previous generation](#) page for A Standard, Dv1 (D1-4 and D11-14 v1), and A8-A11 series

Support for generation 2 VMs on Azure

2/28/2020 • 6 minutes to read • [Edit Online](#)

Support for generation 2 virtual machines (VMs) is now available on Azure. You can't change a virtual machine's generation after you've created it, so review the considerations on this page before you choose a generation.

Generation 2 VMs support key features that aren't supported in generation 1 VMs. These features include increased memory, Intel Software Guard Extensions (Intel SGX), and virtualized persistent memory (vPMEM). Generation 2 VMs running on-premises, have some features that aren't supported in Azure yet. For more information, see the [Features and capabilities](#) section.

Generation 2 VMs use the new UEFI-based boot architecture rather than the BIOS-based architecture used by generation 1 VMs. Compared to generation 1 VMs, generation 2 VMs might have improved boot and installation times. For an overview of generation 2 VMs and some of the differences between generation 1 and generation 2, see [Should I create a generation 1 or 2 virtual machine in Hyper-V?](#).

Generation 2 VM sizes

Generation 1 VMs are supported by all VM sizes in Azure (except for Mv2-series VMs). Azure now offers generation 2 support for the following selected VM series:

- [B-series](#)
- [DC-series](#)
- [DSv2-series](#) and [Dsv3-series](#)
- [Esv3-series](#)
- [Fsv2-series](#)
- [GS-series](#)
- [HB-series](#)
- [HC-series](#)
- [Ls-series](#) and [Lsv2-series](#)
- [Mv2-series](#)
- [NCv2-series](#) and [NCv3-series](#)
- [ND-series](#)
- [NVv3-series](#)

NOTE

The usage of generation 2 VM images for Mv2-series VMs is generally available since the Mv2-series works with generation 2 VM images exclusively. Generation 1 VM images are not supported on Mv2-series VMs.

Generation 2 VM images in Azure Marketplace

Generation 2 VMs support the following Marketplace images:

- Windows Server 2019, 2016, 2012 R2, 2012
- Windows 10
- SUSE Linux Enterprise Server 15 SP1
- SUSE Linux Enterprise Server 12 SP4

- Ubuntu Server 16.04, 18.04, 19.04, 19.10
- RHEL 8.1, 8.0, 7.7, 7.6, 7.5, 7.4, 7.0
- Cent OS 8.0, 7.7, 7.6, 7.5, 7.4
- Oracle Linux 7.7, 7.7-CI

On-premises vs. Azure generation 2 VMs

Azure doesn't currently support some of the features that on-premises Hyper-V supports for generation 2 VMs.

GENERATION 2 FEATURE	ON-PREMISES HYPER-V	AZURE
Secure boot	✓□	□
Shielded VM	✓□	□
vTPM	✓□	□
Virtualization-based security (VBS)	✓□	□
VHDX format	✓□	□

Features and capabilities

Generation 1 vs. generation 2 features

FEATURE	GENERATION 1	GENERATION 2
Boot	PCAT	UEFI
Disk controllers	IDE	SCSI
VM sizes	All VM sizes	Only VMs that support premium storage

Generation 1 vs. generation 2 capabilities

CAPABILITY	GENERATION 1	GENERATION 2
OS disk > 2 TB	□	✓□
Custom disk/image/swap OS	✓□	✓□
Virtual machine scale set support	✓□	✓□
Azure Site Recovery	✓□	✓□
Backup/restore	✓□	✓□
Shared image gallery	✓□	✓□
Azure disk encryption	✓□	□

Creating a generation 2 VM

Marketplace image

In the Azure portal or Azure CLI, you can create generation 2 VMs from a Marketplace image that supports UEFI boot.

Azure portal

Below are the steps to create a generation 2 (Gen2) VM in Azure portal.

1. Sign in to the Azure portal at <https://portal.azure.com>.
2. Select **Create a resource**.
3. Click **See all** from the Azure Marketplace on the left.
4. Select an image which supports Gen2.
5. Click **Create**.
6. In the **Advanced** tab, under the **VM generation** section, select the **Gen 2** option.
7. In the **Basics** tab, Under **Instance details**, go to **Size** and open the **Select a VM size** blade.
8. Select a [supported generation 2 VM](#).
9. Go through the [Azure portal creation flow](#) to finish creating the VM.



PowerShell

You can also use PowerShell to create a VM by directly referencing the generation 1 or generation 2 SKU.

For example, use the following PowerShell cmdlet to get a list of the SKUs in the `WindowsServer` offer.

```
Get-AzVMImageSku -Location westus2 -PublisherName MicrosoftWindowsServer -Offer WindowsServer
```

Alternatively, you can use the Azure CLI to see any available generation 2 images, listed by **Publisher**.

```
az vm image list --publisher Canonical --sku gen2 --output table --all
```

If you're creating a VM with Windows Server 2012 as the OS, then you will select either the generation 1 (BIOS) or generation 2 (UEFI) VM SKU, which look like this:

```
2012-Datacenter  
2012-datacenter-gensecond
```

See the [Features and capabilities](#) section for a current list of supported Marketplace images.

Managed image or managed disk

You can create a generation 2 VM from a managed image or managed disk in the same way you would create a generation 1 VM.

Virtual machine scale sets

You can also create generation 2 VMs by using virtual machine scale sets. In the Azure CLI, use Azure scale sets to create generation 2 VMs.

Frequently asked questions

- **Are generation 2 VMs available in all Azure regions?**

Yes. But not all [generation 2 VM sizes](#) are available in every region. The availability of the generation 2 VM depends on the availability of the VM size.

- **Is there a price difference between generation 1 and generation 2 VMs?**

No.

- **I have a .vhf file from my on-premises generation 2 VM. Can I use that .vhf file to create a generation 2 VM in Azure?** Yes, you can bring your generation 2 .vhf file to Azure and use that to create a generation 2 VM. Use the following steps to do so:

1. Upload the .vhf to a storage account in the same region where you'd like to create your VM.
2. Create a managed disk from the .vhf file. Set the Hyper-V Generation property to V2. The following PowerShell commands set Hyper-V Generation property when creating managed disk.

```
$sourceUri = 'https://xyzstorage.blob.core.windows.net/vhd/abcd.vhd'. #<Provide location to your
uploaded .vhf file>
$osDiskName = 'gen2Diskfrmgenvhf' #<Provide a name for your disk>
$diskconfig = New-AzDiskConfig -Location '<location>' -DiskSizeGB 127 -AccountType Standard_LRS -
OsType Windows -HyperVGeneration "V2" -SourceUri $sourceUri -CreateOption 'Import'
New-AzDisk -DiskName $osDiskName -ResourceGroupName '<Your Resource Group>' -Disk $diskconfig
```

3. Once the disk is available, create a VM by attaching this disk. The VM created will be a generation 2 VM. When the generation 2 VM is created, you can optionally generalize the image of this VM. By generalizing the image you can use it to create multiple VMs.

- **How do I increase the OS disk size?**

OS disks larger than 2 TB are new to generation 2 VMs. By default, OS disks are smaller than 2 TB for generation 2 VMs. You can increase the disk size up to a recommended maximum of 4 TB. Use the Azure CLI or the Azure portal to increase the OS disk size. For information about how to expand disks programmatically, see [Resize a disk](#).

To increase the OS disk size from the Azure portal:

1. In the Azure portal, go to the VM properties page.
2. To shut down and deallocate the VM, select the **Stop** button.
3. In the **Disk**s section, select the OS disk you want to increase.
4. In the **Disk**s section, select **Configuration**, and update the **Size** to the value you want.
5. Go back to the VM properties page and **Start** the VM.

You might see a warning for OS disks larger than 2 TB. The warning doesn't apply to generation 2 VMs. However, OS disk sizes larger than 4 TB are *not recommended*.

- **Do generation 2 VMs support accelerated networking?**

Yes. For more information, see [Create a VM with accelerated networking](#).

- **Is VHDX supported on generation 2?**

No, generation 2 VMs support only VHD.

- **Do generation 2 VMs support Azure Ultra Disk Storage?**

Yes.

- **Can I migrate a VM from generation 1 to generation 2?**

No, you can't change the generation of a VM after you create it. If you need to switch between VM generations, create a new VM of a different generation.

- **Why is my VM size not enabled in the size selector when I try to create a Gen2 VM?**

This may be solved by doing the following:

1. Verify that the **VM generation** property is set to **Gen 2** in the **Advanced** tab.
2. Verify you are searching for a [VM size which supports Gen2 VMs](#).

Next steps

- Learn about [generation 2 virtual machines in Hyper-V](#).

General purpose virtual machine sizes

2/25/2020 • 2 minutes to read • [Edit Online](#)

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.

- The [Av2-series](#) VMs can be deployed on a variety of hardware types and processors. A-series VMs have CPU performance and memory configurations best suited for entry level workloads like development and test. The size is throttled, based upon the hardware, to offer consistent processor performance for the running instance, regardless of the hardware it is deployed on. To determine the physical hardware on which this size is deployed, query the virtual hardware from within the Virtual Machine. Example use cases include development and test servers, low traffic web servers, small to medium databases, proof-of-concepts, and code repositories.
- [B-series burstable](#) VMs are ideal for workloads that do not need the full performance of the CPU continuously, like web servers, small databases and development and test environments. These workloads typically have burstable performance requirements. The B-Series provides these customers the ability to purchase a VM size with a price conscious baseline performance that allows the VM instance to build up credits when the VM is utilizing less than its base performance. When the VM has accumulated credit, the VM can burst above the VM's baseline using up to 100% of the CPU when your application requires the higher CPU performance.
- [Dav4 and Dasv4-series](#) are new sizes utilizing AMD's 2.35Ghz EPYC™ 7452 processor in a multi-threaded configuration with up to 256 MB L3 cache dedicating 8 GB of that L3 cache to every 8 cores increasing customer options for running their general purpose workloads. The Dav4-series and Dasv4-series have the same memory and disk configurations as the D & Dsv3-series.
- The [DCv2-series](#) can help protect the confidentiality and integrity of your data and code while it's processed in the public cloud. These machines are backed by the latest generation of Intel XEON E-2288G Processor with SGX technology. With the Intel Turbo Boost Technology these machines can go up to 5.0GHz. DCv2 series instances enable customers to build secure enclave-based applications to protect their code and data while it's in use.
- [Dv2 and Dsv2-series](#) VMs, a follow-on to the original D-series, features a more powerful CPU and optimal CPU-to-memory configuration making them suitable for most production workloads. The Dv2-series is about 35% faster than the D-series. Dv2-series runs on the Intel® Xeon® 8171M 2.1GHz (Skylake), Intel® Xeon® E5-2673 v4 2.3 GHz (Broadwell), or the Intel® Xeon® E5-2673 v3 2.4 GHz (Haswell) processors with the Intel Turbo Boost Technology 2.0. The Dv2-series has the same memory and disk configurations as the D-series.
- [Dv3 and Dsv3-series](#) VMs run on the Intel® Xeon® 8171M 2.1GHz (Skylake), Intel® Xeon® E5-2673 v4 2.3 GHz (Broadwell), or the Intel® Xeon® E5-2673 v3 2.4 GHz (Haswell) processors in a hyper-threaded configuration, providing a better value proposition for most general purpose workloads. Memory has been expanded (from ~3.5 GiB/vCPU to 4 GiB/vCPU) while disk and network limits have been adjusted on a per core basis to align with the move to hyperthreading. The Dv3-series no longer has the high memory VM sizes of the D/Dv2-series, those have been moved to the memory optimized [Ev3 and Esv3-series](#).

Example D-series use cases include enterprise-grade applications, relational databases, in-memory caching, and analytics.

Other sizes

- [Compute optimized](#)
- [Memory optimized](#)
- [Storage optimized](#)
- [GPU optimized](#)
- [High performance compute](#)
- [Previous generations](#)

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

Av2-series

2/28/2020 • 2 minutes to read • [Edit Online](#)

The Av2-series VMs can be deployed on a variety of hardware types and processors. Av2-series VMs have CPU performance and memory configurations best suited for entry level workloads like development and test. The size is throttled to offer consistent processor performance for the running instance, regardless of the hardware it is deployed on. To determine the physical hardware on which this size is deployed, query the virtual hardware from within the Virtual Machine. Some example use cases include development and test servers, low traffic web servers, small to medium databases, proof-of-concepts, and code repositories.

ACU: 100

Premium Storage: Not Supported

Premium Storage caching: Not Supported

SIZE	VCPUs	MEMORY: GiB	TEMP STORAGE (SSD) GiB	MAX TEMP STORAGE THROUGHPUT: IOPS/READ MBPS/WRITE MBPS	MAX DATA DISKS/THROUGHPUT: IOPS	MAX NICs/EXPECTED NETWORK BANDWIDTH (MBPS)
Standard_A1_v2	1	2	10	1000/20/10	2/2x500	2/250
Standard_A2_v2	2	4	20	2000/40/20	4/4x500	2/500
Standard_A4_v2	4	8	40	4000/80/40	8/8x500	4/1000
Standard_A8_v2	8	16	80	8000/160/80	16/16x500	8/2000
Standard_A2_m_v2	2	16	20	2000/40/20	4/4x500	2/500
Standard_A4_m_v2	4	32	40	4000/80/40	8/8x500	4/1000
Standard_A8_m_v2	8	64	80	8000/160/80	16/16x500	8/2000

Size table definitions

- Storage capacity is shown in units of GiB or 1024^3 bytes. When you compare disks measured in GB (1000^3 bytes) to disks measured in GiB (1024^3) remember that capacity numbers given in GiB may appear smaller. For example, 1023 GiB = 1098.4 GB.
- Disk throughput is measured in input/output operations per second (IOPS) and MBps where MBps = 10^6 bytes/sec.
- Data disks can operate in cached or uncached modes. For cached data disk operation, the host cache mode

is set to **ReadOnly** or **ReadWrite**. For uncached data disk operation, the host cache mode is set to **None**.

- If you want to get the best performance for your VMs, you should limit the number of data disks to two disks per vCPU.
- **Expected network bandwidth** is the maximum aggregated bandwidth allocated per VM type across all NICs, for all destinations. For more information, see [Virtual machine network bandwidth](#).

Upper limits aren't guaranteed. Limits offer guidance for selecting the right VM type for the intended application. Actual network performance will depend on several factors including network congestion, application loads, and network settings. For information on optimizing network throughput, see [Optimize network throughput for Azure virtual machines](#). To achieve the expected network performance on Linux or Windows, you may need to select a specific version or optimize your VM. For more information, see [Bandwidth/Throughput testing \(NTTCP\)](#).

Other sizes

- [General purpose](#)
- [Memory optimized](#)
- [Storage optimized](#)
- [GPU optimized](#)
- [High performance compute](#)
- [Previous generations](#)

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

B-series burstable virtual machine sizes

2/20/2020 • 6 minutes to read • [Edit Online](#)

The B-series VMs are ideal for workloads that do not need the full performance of the CPU continuously, like web servers, proof of concepts, small databases and development build environments. These workloads typically have burstable performance requirements. The B-series provides you with the ability to purchase a VM size with baseline performance and the VM instance builds up credits when it is using less than its baseline. When the VM has accumulated credit, the VM can burst above the baseline using up to 100% of the vCPU when your application requires higher CPU performance.

The B-series comes in the following VM sizes:

Premium Storage: Supported

Premium Storage caching: Not Supported

SIZE	VCPUs	MEMORY: GIB	TEMP STORAGE (SSD) GIB	BASE CPU PERF OF VM	MAX CPU PERF OF VM	INITIAL CREDITS	CREDITS BANKED/HOUR	MAX BANKED CREDITS	MAX DATA DISKS	MAX CACHED AND TEMP STORAGE THROUGHPUT: IOPS/MBPS	MAX UNCACHED DISK THROUGHPUT: IOPS/MBPS	MAX NICS
Standard_B_1ls ¹	1	0.5	4	5%	100%	30	3	72	2	200/10	160/10	2
Standard_B_1s	1	1	4	10%	100%	30	6	144	2	400/10	320/10	2
Standard_B_1ms	1	2	4	20%	100%	30	12	288	2	800/10	640/10	2
Standard_B_2s	2	4	8	40%	200%	60	24	576	4	1600/15	1280/15	3
Standard_B_2ms	2	8	16	60%	200%	60	36	864	4	2400/22.5	1920/22.5	3
Standard_B_4ms	4	16	32	90%	400%	120	54	1296	8	3600/35	2880/35	4
Standard_B_8ms	8	32	64	135%	800%	240	81	1944	16	4320/50	4320/50	4

SIZE	VCPU	MEM ORY: GiB	TEMP STOR AGE (SSD) GiB	BASE CPU PERF OF VM	MAX CPU PERF OF VM	INITI AL CREDI TS	CREDI TS BANK ED/H OUR	MAX BANK ED CREDI TS	MAX DATA DISKS	MAX CACH ED AND TEMP STOR AGE	MAX UNCA CHED DISK	MAX NICS
										THRO UGHP UT:	IOPS/ MBPS	
Standard_B 12ms	12	48	96	202%	1200 %	360	121	2909	16	6480 /75	4320 /50	6
Standard_B 16ms	16	64	128	270%	1600 %	480	162	3888	32	8640 /100	4320 /50	8
Standard_B 20ms	20	80	160	337%	2000 %	600	203	4860	32	1080 0/12 5	4320 /50	8

¹ B11s is supported only on Linux

Workload example

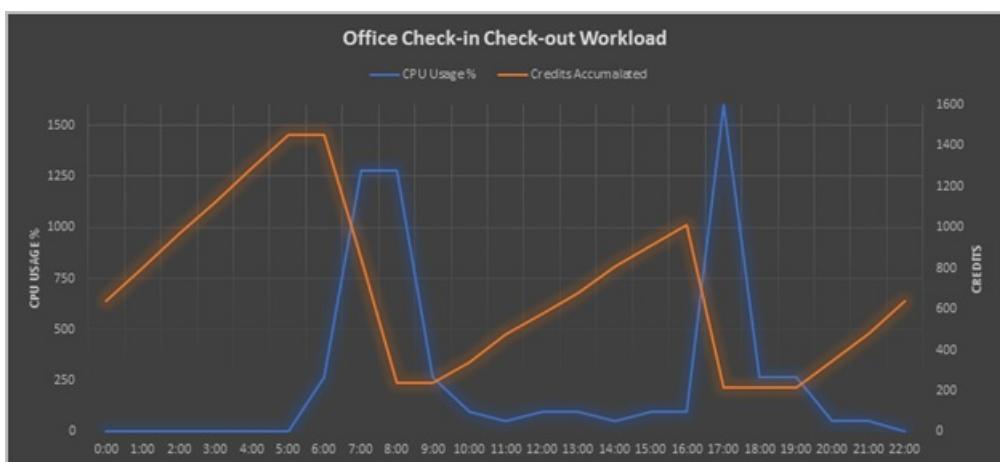
Consider an office check-in/out application. The application needs CPU bursts during business hours, but not a lot of computing power during off hours. In this example, the workload requires a 16vCPU virtual machine with 64GiB of RAM to work efficiently.

The table shows the hourly traffic data and the chart is a visual representation of that traffic.

B16 characteristics:

Max CPU perf: 16vCPU * 100% = 1600%

Baseline: 270%



SCENARIO	TIME	CPU USAGE (%)	CREDITS ACCUMULATED ¹	CREDITS AVAILABLE
B16ms Deployment	Deployment	Deployment	480 (Initial Credits)	480
No traffic	0:00	0	162	642

SCENARIO	TIME	CPU USAGE (%)	CREDITS ACCUMULATED	CREDITS AVAILABLE
No traffic	1:00	0	162	804
No traffic	2:00	0	162	966
No traffic	3:00	0	162	1128
No traffic	4:00	0	162	1290
No traffic	5:00	0	162	1452
Low Traffic	6:00	270	0	1452
Employees come to office (app needs 80% vCPU)	7:00	1280	-606	846
Employees continue coming to office (app needs 80% vCPU)	8:00	1280	-606	240
Low Traffic	9:00	270	0	240
Low Traffic	10:00	100	102	342
Low Traffic	11:00	50	132	474
Low Traffic	12:00	100	102	576
Low Traffic	13:00	100	102	678
Low Traffic	14:00	50	132	810
Low Traffic	15:00	100	102	912
Low Traffic	16:00	100	102	1014
Employees checking out (app needs 100% vCPU)	17:00	1600	-798	216
Low Traffic	18:00	270	0	216
Low Traffic	19:00	270	0	216
Low Traffic	20:00	50	132	348
Low Traffic	21:00	50	132	480
No traffic	22:00	0	162	642
No traffic	23:00	0	162	804

¹ Credits accumulated/credits used in an hour is equivalent to:

$$((\text{Base CPU perf of VM} - \text{CPU Usage}) / 100) * 60 \text{ minutes}$$

For a D16s_v3 which has 16 vCPUs and 64 GiB of memory the hourly rate is \$0.936 per hour (monthly \$673.92) and for B16ms with 16 vCPUs and 64 GiB memory the rate is \$0.794 per hour (monthly \$547.86). **This results in 15% savings!**

Q & A

Q: How do you get 135% baseline performance from a VM?

A: The 135% is shared amongst the 8 vCPU's that make up the VM size. For example, if your application uses 4 of the 8 cores working on batch processing and each of those 4 vCPU's are running at 30% utilization the total amount of VM CPU performance would equal 120%. Meaning that your VM would be building credit time based on the 15% delta from your baseline performance. But it also means that when you have credits available that same VM can use 100% of all 8 vCPU's giving that VM a Max CPU performance of 800%.

Q: How can I monitor my credit balance and consumption

A: We will be introducing 2 new metrics in the coming weeks, the **Credit** metric will allow you to view how many credits your VM has banked and the **ConsumedCredit** metric will show how many CPU credits your VM has consumed from the bank. You will be able to view these metrics from the metrics pane in the portal or programmatically through the Azure Monitor APIs.

For more information on how to access the metrics data for Azure, see [Overview of metrics in Microsoft Azure](#).

Q: How are credits accumulated?

A: The VM accumulation and consumption rates are set such that a VM running at exactly its base performance level will have neither a net accumulation or consumption of bursting credits. A VM will have a net increase in credits whenever it is running below its base performance level and will have a net decrease in credits whenever the VM is utilizing the CPU more than its base performance level.

Example: I deploy a VM using the B1ms size for my small time and attendance database application. This size allows my application to use up to 20% of a vCPU as my baseline, which is 0.2 credits per minute I can use or bank.

My application is busy at the beginning and end of my employees work day, between 7:00-9:00 AM and 4:00 - 6:00PM. During the other 20 hours of the day, my application is typically at idle, only using 10% of the vCPU. For the non-peak hours, I earn 0.2 credits per minute but only consume 0.1 credits per minute, so my VM will bank 0.1 x 60 = 6 credits per hour. For the 20 hours that I am off-peak, I will bank 120 credits.

During peak hours my application averages 60% vCPU utilization, I still earn 0.2 credits per minute but I consume 0.6 credits per minute, for a net cost of 0.4 credits a minute or 0.4 x 60 = 24 credits per hour. I have 4 hours per day of peak usage, so it costs 4 x 24 = 96 credits for my peak usage.

If I take the 120 credits I earned off-peak and subtract the 96 credits I used for my peak times, I bank an additional 24 credits per day that I can use for other bursts of activity.

Q: How can I calculate credits accumulated and used?

A: You can use the following formula:

$$(\text{Base CPU perf of VM} - \text{CPU Usage}) / 100 = \text{Credits bank or use per minute}$$

e.g in above instance your baseline is 20% and if you use 10% of the CPU you are accumulating $(20\% - 10\%) / 100 = 0.1$ credit per minute.

Q: Does the B-Series support Premium Storage data disks?

A: Yes, all B-Series sizes support Premium Storage data disks.

Q: Why is my remaining credit set to 0 after a redeploy or a stop/start?

A : When a VM is “REDPLOYED” and the VM moves to another node, the accumulated credit is lost. If the VM is stopped/started, but remains on the same node, the VM retains the accumulated credit. Whenever the VM starts fresh on a node, it gets an initial credit, for Standard_B8ms it is 240 mins.

Q: What happens if I deploy an unsupported OS image on B1ls?

A : B1ls only supports Linux images and if you deploy any another OS image you might not get the best customer experience.

Other sizes

- [General purpose](#)
- [Compute optimized](#)
- [Memory optimized](#)
- [Storage optimized](#)
- [GPU optimized](#)
- [High performance compute](#)

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

Preview: DCv2-series

2/28/2020 • 2 minutes to read • [Edit Online](#)

The DCv2-series can help protect the confidentiality and integrity of your data and code while it's processed in the public cloud. These machines are backed by the latest generation of Intel XEON E-2288G Processor with SGX technology. With the Intel Turbo Boost Technology these machines can go up to 5.0GHz. DCv2 series instances enable customers to build secure enclave-based applications to protect their code and data while it's in use.

Example use cases include confidential multiparty data sharing, fraud detection, anti-money laundering, blockchain, confidential usage analytics, intelligence analysis and confidential machine learning.

Premium Storage: Supported*

Premium Storage caching: Supported*

*Except for Standard_DC8_v2

SIZE	VCPU	MEMORY: GIB	TEMP STORAGE (SSD) GIB	MAX DATA DISKS	MAX CACHED AND TEMP STORAGE THROUGHPUT: IOPS / MBPS (CACHE SIZE IN GIB)	MAX UNCACHED DISK THROUGHPUT: IOPS / MBPS	MAX NICS / EXPECTED NETWORK BANDWIDTH (MBPS)
Standard_D_C1s_v2	1	4	50	1	2000/16 (21)	1600/24	2
Standard_D_C2s_v2	2	8	100	2	4000/32 (43)	3200/48	2
Standard_D_C4s_v2	4	16	200	4	8000/64 (86)	6400/96	2
Standard_D_C8_v2	8	32	400	8	16000/128 (172)	12800/192	2

- DCv2-series VMs are [generation 2 VMs](#) and only support [Gen2](#) images.

Other sizes

- [General purpose](#)
- [Memory optimized](#)
- [Storage optimized](#)
- [GPU optimized](#)
- [High performance compute](#)
- [Previous generations](#)

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

Dv2 and DSv2-series

2/28/2020 • 2 minutes to read • [Edit Online](#)

The Dv2 and DSv2-series, a follow-on to the original D-series, feature a more powerful CPU and optimal CPU-to-memory configuration making them suitable for most production workloads. The Dv2-series is about 35% faster than the D-series. Dv2-series runs on the Intel® Xeon® 8171M 2.1GHz (Skylake), Intel® Xeon® E5-2673 v4 2.3 GHz (Broadwell), or the Intel® Xeon® E5-2673 v3 2.4 GHz (Haswell) processors with the Intel Turbo Boost Technology 2.0. The Dv2-series has the same memory and disk configurations as the D-series.

Dv2-series

Dv2-series sizes run on the Intel® Xeon® 8171M 2.1GHz (Skylake) or the Intel® Xeon® E5-2673 v4 2.3 GHz (Broadwell) or the Intel® Xeon® E5-2673 v3 2.4 GHz (Haswell) processors with Intel Turbo Boost Technology 2.0.

ACU: 210-250

Premium Storage: Not Supported

Premium Storage caching: Not Supported

SIZE	VCPU	MEMORY: GIB	TEMP STORAGE (SSD) GIB	MAX TEMP STORAGE THROUGHPUT: IOPS/READ MBPS/WRITE MBPS	MAX DATA DISKS	THROUGHPUT UT: IOPS	MAX NICs/EXPECTED NETWORK BANDWIDTH (MBPS)
Standard_D1_v2	1	3.5	50	3000/46/23	4	4x500	2/750
Standard_D2_v2	2	7	100	6000/93/46	8	8x500	2/1500
Standard_D3_v2	4	14	200	12000/187/93	16	16x500	4/3000
Standard_D4_v2	8	28	400	24000/375/187	32	32x500	8/6000
Standard_D5_v2	16	56	800	48000/750/375	64	64x500	8/12000

DSv2-series

DSv2-series sizes run on the Intel® Xeon® 8171M 2.1GHz (Skylake) or the Intel® Xeon® E5-2673 v4 2.3 GHz (Broadwell) or the Intel® Xeon® E5-2673 v3 2.4 GHz (Haswell) processors with Intel Turbo Boost Technology 2.0 and use premium storage.

ACU: 210-250

Premium Storage: Supported

Premium Storage caching: Supported

SIZE	VCPU	MEMORY: GiB	TEMP STORAGE (SSD) GiB	MAX DATA DISKS	MAX CACHED AND TEMP STORAGE THROUGHPUT: IOPS/MBPS (CACHE SIZE IN GiB)	MAX UNCACHED DISK THROUGHPUT: IOPS/MBPS	MAX NICs/EXPECTED NETWORK BANDWIDTH (MBPS)
Standard_D1_v2	1	3.5	7	4	4000/32 (43)	3200/48	2/750
Standard_D2_v2	2	7	14	8	8000/64 (86)	6400/96	2/1500
Standard_D3_v2	4	14	28	16	16000/128 (172)	12800/192	4/3000
Standard_D4_v2	8	28	56	32	32000/256 (344)	25600/384	8/6000
Standard_D5_v2	16	56	112	64	64000/512 (688)	51200/768	8/12000

Size table definitions

- Storage capacity is shown in units of GiB or 1024^3 bytes. When you compare disks measured in GB (1000^3 bytes) to disks measured in GiB (1024^3) remember that capacity numbers given in GiB may appear smaller. For example, 1023 GiB = 1098.4 GB.
- Disk throughput is measured in input/output operations per second (IOPS) and MBps where MBps = 10^6 bytes/sec.
- Data disks can operate in cached or uncached modes. For cached data disk operation, the host cache mode is set to **ReadOnly** or **ReadWrite**. For uncached data disk operation, the host cache mode is set to **None**.
- If you want to get the best performance for your VMs, you should limit the number of data disks to two disks per vCPU.
- Expected network bandwidth** is the maximum aggregated bandwidth allocated per VM type across all NICs, for all destinations. For more information, see [Virtual machine network bandwidth](#).

Upper limits aren't guaranteed. Limits offer guidance for selecting the right VM type for the intended application. Actual network performance will depend on several factors including network congestion, application loads, and network settings. For information on optimizing network throughput, see [Optimize network throughput for Azure virtual machines](#). To achieve the expected network performance on Linux or Windows, you may need to select a specific version or optimize your VM. For more information, see [Bandwidth/Throughput testing \(NTTTCP\)](#).

Other sizes

- [General purpose](#)
- [Memory optimized](#)
- [Storage optimized](#)
- [GPU optimized](#)
- [High performance compute](#)

- Previous generations

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

Dv3 and Dsv3-series

2/28/2020 • 3 minutes to read • [Edit Online](#)

The Dv3-series runs on the Intel® Xeon® 8171M 2.1GHz (Skylake), Intel® Xeon® E5-2673 v4 2.3 GHz (Broadwell), or the Intel® Xeon® E5-2673 v3 2.4 GHz (Haswell) processors in a hyper-threaded configuration, providing a better value proposition for most general purpose workloads. Memory has been expanded (from ~3.5 GiB/vCPU to 4 GiB/vCPU) while disk and network limits have been adjusted on a per core basis to align with the move to hyperthreading. The Dv3-series no longer has the high memory VM sizes of the D/Dv2-series, those have been moved to the memory optimized [Ev3 and Esv3-series](#).

Example D-series use cases include enterprise-grade applications, relational databases, in-memory caching, and analytics.

Dv3-series

Dv3-series sizes run on the Intel® Xeon® 8171M 2.1GHz (Skylake), Intel® Xeon® E5-2673 v4 2.3 GHz (Broadwell), or the Intel® Xeon® E5-2673 v3 2.4 GHz (Haswell) processors with Intel Turbo Boost Technology 2.0. The Dv3-series sizes offer a combination of vCPU, memory, and temporary storage for most production workloads.

Data disk storage is billed separately from virtual machines. To use premium storage disks, use the Dsv3 sizes. The pricing and billing meters for Dsv3 sizes are the same as Dv3-series.

Dv3-series VMs feature Intel® Hyper-Threading Technology.

ACU: 160-190

Premium Storage: Not Supported

Premium Storage caching: Not Supported

SIZE	VCPUs	MEMORY: GiB	TEMP STORAGE (SSD) GiB	MAX DATA DISKS	MAX TEMP STORAGE THROUGHPUT: IOPS/READ MBPS/WRITE MBPS	MAX NICs/NETWORK BANDWIDTH
Standard_D2_v3	2	8	50	4	3000/46/23	2/1000
Standard_D4_v3	4	16	100	8	6000/93/46	2/2000
Standard_D8_v3	8	32	200	16	12000/187/93	4/4000
Standard_D16_v3	16	64	400	32	24000/375/187	8/8000
Standard_D32_v3	32	128	800	32	48000/750/375	8/16000

SIZE	VCPU	MEMORY: GIB	TEMP STORAGE (SSD) GIB	MAX DATA DISKS	MAX TEMP STORAGE THROUGHPUT: IOPS/READ MBPS/WRITE MBPS	MAX NICS/NETWORK BANDWIDTH
Standard_D48_v3	48	192	1200	32	96000/1000/500	8/24000
Standard_D64_v3	64	256	1600	32	96000/1000/500	8/30000

Dsv3-series

Dsv3-series sizes run on the Intel® Xeon® 8171M 2.1GHz (Skylake), Intel® Xeon® E5-2673 v4 2.3 GHz (Broadwell), or the Intel® Xeon® E5-2673 v3 2.4 GHz (Haswell) processors with Intel Turbo Boost Technology 2.0 and use premium storage. The Dsv3-series sizes offer a combination of vCPU, memory, and temporary storage for most production workloads.

Dsv3-series VMs feature Intel® Hyper-Threading Technology.

ACU: 160-190

Premium Storage: Supported

Premium Storage caching: Supported

SIZE	VCPU	MEMORY: GIB	TEMP STORAGE (SSD) GIB	MAX DATA DISKS	MAX CACHED AND TEMP STORAGE THROUGHPUT: IOPS/MBPS (CACHE SIZE IN GIB)	MAX UNCACHED DISK THROUGHPUT: IOPS/MBPS	MAX NICS/EXPECTED NETWORK BANDWIDTH (MBPS)
Standard_D2s_v3	2	8	16	4	4000/32 (50)	3200/48	2/1000
Standard_D4s_v3	4	16	32	8	8000/64 (100)	6400/96	2/2000
Standard_D8s_v3	8	32	64	16	16000/128 (200)	12800/192	4/4000
Standard_D16s_v3	16	64	128	32	32000/256 (400)	25600/384	8/8000
Standard_D32s_v3	32	128	256	32	64000/512 (800)	51200/768	8/16000
Standard_D48s_v3	48	192	384	32	96000/768 (1200)	76800/1152	8/24000
Standard_D64s_v3	64	256	512	32	128000/1024 (1600)	80000/1200	8/30000

Size table definitions

- Storage capacity is shown in units of GiB or 1024^3 bytes. When you compare disks measured in GB (1000^3 bytes) to disks measured in GiB (1024^3) remember that capacity numbers given in GiB may appear smaller. For example, 1023 GiB = 1098.4 GB.
- Disk throughput is measured in input/output operations per second (IOPS) and MBps where MBps = 10^6 bytes/sec.
- Data disks can operate in cached or uncached modes. For cached data disk operation, the host cache mode is set to **ReadOnly** or **ReadWrite**. For uncached data disk operation, the host cache mode is set to **None**.
- If you want to get the best performance for your VMs, you should limit the number of data disks to two disks per vCPU.
- **Expected network bandwidth** is the maximum aggregated bandwidth allocated per VM type across all NICs, for all destinations. For more information, see [Virtual machine network bandwidth](#).

Upper limits aren't guaranteed. Limits offer guidance for selecting the right VM type for the intended application. Actual network performance will depend on several factors including network congestion, application loads, and network settings. For information on optimizing network throughput, see [Optimize network throughput for Azure virtual machines](#). To achieve the expected network performance on Linux or Windows, you may need to select a specific version or optimize your VM. For more information, see [Bandwidth/Throughput testing \(NTTCP\)](#).

Other sizes

- [General purpose](#)
- [Memory optimized](#)
- [Storage optimized](#)
- [GPU optimized](#)
- [High performance compute](#)
- [Previous generations](#)

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

Dav4 and Dasv4-series

2/28/2020 • 3 minutes to read • [Edit Online](#)

The Dav4-series and Dasv4-series are new sizes utilizing AMD's 2.35Ghz EPYC™ 7452 processor in a multi-threaded configuration with up to 256 MB L3 cache dedicating 8 GB of that L3 cache to every 8 cores increasing customer options for running their general purpose workloads. The Dav4-series and Dasv4-series have the same memory and disk configurations as the D & Dsv3-series.

Dav4-series

ACU: 230-260

Premium Storage: Not Supported

Premium Storage caching: Not Supported

Dav4-series sizes are based on the 2.35Ghz AMD EPYC™ 7452 processor that can achieve a boosted maximum frequency of 3.35GHz. The Dav4-series sizes offer a combination of vCPU, memory and temporary storage for most production workloads. Data disk storage is billed separately from virtual machines. To use premium SSD, use the Dasv4 sizes. The pricing and billing meters for Dasv4 sizes are the same as the Dav4-series.

SIZE	VCPUs	MEMORY: GIB	TEMP STORAGE (SSD) GIB	MAX DATA DISKS	MAX TEMP STORAGE THROUGHPUT: IOPS / READ MBPS / WRITE MBPS	MAX NICs / EXPECTED NETWORK BANDWIDTH (MBPS)
Standard_D2a_v4	2	8	50	4	3000 / 46 / 23	2 / 1000
Standard_D4a_v4	4	16	100	8	6000 / 93 / 46	2 / 2000
Standard_D8a_v4	8	32	200	16	12000 / 187 / 93	4 / 4000
Standard_D16a_v4	16	64	400	32	24000 / 375 / 187	8 / 8000
Standard_D32a_v4	32	128	800	32	48000 / 750 / 375	8 / 16000
Standard_D48a_v4 **	48	192	1200	32		
Standard_D64a_v4 **	64	256	1600	32		
Standard_D96a_v4 **	96	384	2400	32		

** These sizes are in Preview. If you are interested in trying out these larger sizes, sign up at <https://aka.ms/AzureAMDLargeVMPreview>.

Dasv4-series

ACU: 230-260

Premium Storage: Supported

Premium Storage caching: Supported

Dasv4-series sizes are based on the 2.35Ghz AMD EPYC™ 7452 processor that can achieve a boosted maximum frequency of 3.35GHz and use premium SSD. The Dasv4-series sizes offer a combination of vCPU, memory and temporary storage for most production workloads.

SIZE	VCPUs	MEMORY: GiB	TEMP STORAGE (SSD) GiB	MAX DATA DISKS	MAX CACHED AND TEMP STORAGE THROUGHPUT: IOPS / MBPS (CACHE SIZE IN GiB)	MAX UNCACHED DISK THROUGHPUT: IOPS / MBPS	MAX NICs / EXPECTED NETWORK BANDWIDTH (MBPS)
Standard_D_2as_v4	2	8	16	4	4000 / 32 (50)	3200 / 48	2 / 1000
Standard_D_4as_v4	4	16	32	8	8000 / 64 (100)	6400 / 96	2 / 2000
Standard_D_8as_v4	8	32	64	16	16000 / 128 (200)	12800 / 192	4 / 4000
Standard_D_16as_v4	16	64	128	32	32000 / 255 (400)	25600 / 384	8 / 8000
Standard_D_32as_v4	32	128	256	32	64000 / 510 (800)	51200 / 768	8 / 16000
Standard_D_48as_v4 **	48	192	384	32			
Standard_D_64as_v4 **	64	256	512	32			
Standard_D_96as_v4 **	96	384	768	32			

** These sizes are in Preview. If you are interested in trying out these larger sizes, sign up at <https://aka.ms/AzureAMDLargeVMPreview>.

Size table definitions

- Storage capacity is shown in units of GiB or 1024^3 bytes. When you compare disks measured in GB (1000^3 bytes) to disks measured in GiB (1024^3) remember that capacity numbers given in GiB may appear smaller. For example, 1023 GiB = 1098.4 GB.
- Disk throughput is measured in input/output operations per second (IOPS) and MBps where MBps = 10^6 bytes/sec.
- Data disks can operate in cached or uncached modes. For cached data disk operation, the host cache mode

is set to **ReadOnly** or **ReadWrite**. For uncached data disk operation, the host cache mode is set to **None**.

- If you want to get the best performance for your VMs, you should limit the number of data disks to two disks per vCPU.
- **Expected network bandwidth** is the maximum aggregated bandwidth allocated per VM type across all NICs, for all destinations. For more information, see [Virtual machine network bandwidth](#).

Upper limits aren't guaranteed. Limits offer guidance for selecting the right VM type for the intended application. Actual network performance will depend on several factors including network congestion, application loads, and network settings. For information on optimizing network throughput, see [Optimize network throughput for Azure virtual machines](#). To achieve the expected network performance on Linux or Windows, you may need to select a specific version or optimize your VM. For more information, see [Bandwidth/Throughput testing \(NTTCP\)](#).

Other sizes

- [General purpose](#)
- [Memory optimized](#)
- [Storage optimized](#)
- [GPU optimized](#)
- [High performance compute](#)
- [Previous generations](#)

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

Compute optimized virtual machine sizes

2/20/2020 • 2 minutes to read • [Edit Online](#)

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.

The [Fsv2-series](#) is based on the Intel® Xeon® Platinum 8168 processor. It features a sustained all core Turbo clock speed of 3.4 GHz and a maximum single-core turbo frequency of 3.7 GHz. Intel® AVX-512 instructions are new on Intel Scalable Processors. These instructions provide up to a 2X performance boost to vector processing workloads on both single and double precision floating point operations. In other words, they're really fast for any computational workload.

At a lower per-hour list price, the Fsv2-series is the best value in price-performance in the Azure portfolio based on the Azure Compute Unit (ACU) per vCPU.

Other sizes

- [General purpose](#)
- [Memory optimized](#)
- [Storage optimized](#)
- [GPU optimized](#)
- [High performance compute](#)
- [Previous generations](#)

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

Fsv2-series

2/28/2020 • 2 minutes to read • [Edit Online](#)

The Fsv2-series is based on the Intel® Xeon® Platinum 8168 processor. It features a sustained all core Turbo clock speed of 3.4 GHz and a maximum single-core turbo frequency of 3.7 GHz. Intel® AVX-512 instructions are new on Intel Scalable Processors. These instructions provide up to a 2X performance boost to vector processing workloads on both single and double precision floating point operations. In other words, they're really fast for any computational workload.

Fsv2-series VMs feature Intel® Hyper-Threading Technology.

ACU: 195 - 210

Premium Storage: Supported

Premium Storage caching: Supported

SIZE	VCPU'S	MEMORY: GIB	TEMP STORAGE (SSD) GIB	MAX DATA DISKS	MAX CACHED AND TEMP STORAGE THROUHPUT: IOPS/MBPS (CACHE SIZE IN GIB)	MAX UNCACHED DISK THROUHPUT: IOPS/MBPS	MAX NICS/EXPECTED NETWORK BANDWIDTH (MBPS)
Standard_F_2s_v2	2	4	16	4	4000/31 (32)	3200/47	2/875
Standard_F_4s_v2	4	8	32	8	8000/63 (64)	6400/95	2/1750
Standard_F_8s_v2	8	16	64	16	16000/127 (128)	12800/190	4/3500
Standard_F_16s_v2	16	32	128	32	32000/255 (256)	25600/380	4/7000
Standard_F_32s_v2	32	64	256	32	64000/512 (512)	51200/750	8/14000
Standard_F_48s_v2	48	96	384	32	96000/768 (768)	76800/1100	8/21000
Standard_F_64s_v2	64	128	512	32	128000/1024 (1024)	80000/1100	8/28000
Standard_F_72s_v2 ^{1, 2}	72	144	576	32	144000/1152 (1520)	80000/1100	8/30000

¹ The use of more than 64 vCPU require one of these supported guest operating systems:

- Windows Server 2016 or later
- Ubuntu 16.04 LTS or later, with Azure tuned kernel (4.15 kernel or later)

- SLES 12 SP2 or later
- RHEL or CentOS version 6.7 through 6.10, with Microsoft-provided LIS package 4.3.1 (or later) installed
- RHEL or CentOS version 7.3, with Microsoft-provided LIS package 4.2.1 (or later) installed
- RHEL or CentOS version 7.6 or later
- Oracle Linux with UEK4 or later
- Debian 9 with the backports kernel, Debian 10 or later
- CoreOS with a 4.14 kernel or later

² Instance is isolated to hardware dedicated to a single customer.

Size table definitions

- Storage capacity is shown in units of GiB or 1024^3 bytes. When you compare disks measured in GB (1000^3 bytes) to disks measured in GiB (1024^3) remember that capacity numbers given in GiB may appear smaller. For example, 1023 GiB = 1098.4 GB.
- Disk throughput is measured in input/output operations per second (IOPS) and MBps where MBps = 10^6 bytes/sec.
- Data disks can operate in cached or uncached modes. For cached data disk operation, the host cache mode is set to **ReadOnly** or **ReadWrite**. For uncached data disk operation, the host cache mode is set to **None**.
- If you want to get the best performance for your VMs, you should limit the number of data disks to two disks per vCPU.
- **Expected network bandwidth** is the maximum aggregated bandwidth allocated per VM type across all NICs, for all destinations. For more information, see [Virtual machine network bandwidth](#).

Upper limits aren't guaranteed. Limits offer guidance for selecting the right VM type for the intended application. Actual network performance will depend on several factors including network congestion, application loads, and network settings. For information on optimizing network throughput, see [Optimize network throughput for Azure virtual machines](#). To achieve the expected network performance on Linux or Windows, you may need to select a specific version or optimize your VM. For more information, see [Bandwidth/Throughput testing \(NTTCP\)](#).

Other sizes

- [General purpose](#)
- [Memory optimized](#)
- [Storage optimized](#)
- [GPU optimized](#)
- [High performance compute](#)
- [Previous generations](#)

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

Memory optimized virtual machine sizes

2/20/2020 • 2 minutes to read • [Edit Online](#)

Memory optimized VM sizes offer a high memory-to-CPU ratio that are 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 as well as storage throughput and network bandwidth for each size in this grouping.

- [Dv2 and DSv2-series](#), a follow-on to the original D-series, features a more powerful CPU. The Dv2-series is about 35% faster than the D-series. It runs on the Intel® Xeon® 8171M 2.1 GHz (Skylake) or the Intel® Xeon® E5-2673 v4 2.3 GHz (Broadwell) or the Intel® Xeon® E5-2673 v3 2.4 GHz (Haswell) processors, and with the Intel Turbo Boost Technology 2.0. The Dv2-series has the same memory and disk configurations as the D-series.

Dv2 and DSv2-series are ideal for applications that demand faster vCPUs, better temporary storage performance, or have higher memory demands. They offer a powerful combination for many enterprise-grade applications.

- The [Eav4 and Easv4-series](#) utilize AMD's 2.35Ghz EPYC™ 7452 processor in a multi-threaded configuration with up to 256MB L3 cache, increasing options for running most memory optimized workloads. The Eav4-series and Easv4-series have the same memory and disk configurations as the Ev3 & Esv3-series.
- The [Ev3 and Esv3-series](#) Intel® Xeon® 8171M 2.1 GHz (Skylake) or the Intel® Xeon® E5-2673 v4 2.3 GHz (Broadwell) processor in a hyper-threaded configuration, providing a better value proposition for most general purpose workloads, and bringing the Ev3 into alignment with the general purpose VMs of most other clouds. Memory has been expanded (from 7 GiB/vCPU to 8 GiB/vCPU) while disk and network limits have been adjusted on a per core basis to align with the move to hyper-threading. The Ev3 is the follow up to the high memory VM sizes of the D/Dv2 families.
- The [M-series](#) offers a high vCPU count (up to 128 vCPUs) and a large amount of memory (up to 3.8 TiB). It's also ideal for extremely large databases or other applications that benefit from high vCPU counts and large amounts of memory.
- The [Mv2-series](#) offers the highest vCPU count (up to 416 vCPUs) and largest memory (up to 8.19 TiB) of any VM in the cloud. It's ideal for extremely large databases or other applications that benefit from high vCPU counts and large amounts of memory.

Azure Compute offers virtual machine sizes that are isolated to a specific hardware type and dedicated to a single customer. These virtual machine sizes are best suited for workloads that require a high degree of isolation from other customers for workloads involving elements like compliance and regulatory requirements. Customers can also choose to further subdivide the resources of these isolated virtual machines by using [Azure support for nested virtual machines](#). See the pages for virtual machine families below for your isolated VM options.

Other sizes

- [General purpose](#)
- [Compute optimized](#)
- [Storage optimized](#)
- [GPU optimized](#)

- High performance compute
- Previous generations

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

Memory optimized Dv2 and DSv2-series

2/28/2020 • 3 minutes to read • [Edit Online](#)

Dv2 and DSv2-series, a follow-on to the original D-series, features a more powerful CPU. DSv2-series sizes run on the Intel® Xeon® 8171M 2.1 GHz (Skylake) or the Intel® Xeon® E5-2673 v4 2.3 GHz (Broadwell) or the Intel® Xeon® E5-2673 v3 2.4 GHz (Haswell) processors. The Dv2-series has the same memory and disk configurations as the D-series.

Dv2-series 11-15

Dv2-series sizes run on the Intel® Xeon® 8171M 2.1 GHz (Skylake) or the Intel® Xeon® E5-2673 v4 2.3 GHz (Broadwell) or the Intel® Xeon® E5-2673 v3 2.4 GHz (Haswell) processors.

ACU: 210 - 250

Premium Storage: Not Supported

Premium Storage caching: Not Supported

SIZE	VCPU	MEMORY: GIB	TEMP STORAGE (SSD) GIB	MAX TEMP STORAGE THROUGHPUT: IOPS/READ MBPS/WRITE MBPS	MAX DATA DISKS/THROUGHPUT: IOPS	MAX NICs/EXPECTED NETWORK BANDWIDTH (MBPS)
Standard_D11_v2	2	14	100	6000/93/46	8/8x500	2/1500
Standard_D12_v2	4	28	200	12000/187/93	16/16x500	4/3000
Standard_D13_v2	8	56	400	24000/375/187	32/32x500	8/6000
Standard_D14_v2	16	112	800	48000/750/375	64/64x500	8/12000
Standard_D15_v2 ¹	20	140	1000	60000/937/468	64/64x500	8/25000 ²

¹ Instance is isolated to hardware dedicated to a single customer. ² 25000 Mbps with Accelerated Networking.

DSv2-series 11-15

DSv2-series sizes run on the Intel® Xeon® 8171M 2.1 GHz (Skylake) or the Intel® Xeon® E5-2673 v4 2.3 GHz (Broadwell) or the Intel® Xeon® E5-2673 v3 2.4 GHz (Haswell) processors.

ACU: 210 - 250¹

Premium Storage: Supported

Premium Storage caching: Supported

SIZE	VCPU	MEMORY: GIB	TEMP STORAGE (SSD) GIB	MAX DATA DISKS	MAX CACHED AND TEMP STORAGE THROUGHPUT: IOPS/MBPS (CACHE SIZE IN GIB)	MAX UNCACHED DISK THROUGHPUT: IOPS/MBPS	MAX NICs/EXPECTED NETWORK BANDWIDTH (MBPS)
Standard_D S11_v2 ³	2	14	28	8	8000/64 (72)	6400/96	2/1500
Standard_D S12_v2 ³	4	28	56	16	16000/128 (144)	12800/192	4/3000
Standard_D S13_v2 ³	8	56	112	32	32000/256 (288)	25600/384	8/6000
Standard_D S14_v2 ³	16	112	224	64	64000/512 (576)	51200/768	8/12000
Standard_D S15_v2 ²	20	140	280	64	80000/640 (720)	64000/960	8/25000 ⁴

¹ The maximum disk throughput (IOPS or MBps) possible with a DSv2 series VM may be limited by the number, size and striping of the attached disk(s). For details, see [Designing for high performance](#). ² Instance is isolated to the Intel Haswell based hardware and dedicated to a single customer.

³ Constrained core sizes available.

⁴ 25000 Mbps with Accelerated Networking.

Size table definitions

- Storage capacity is shown in units of GiB or 1024^3 bytes. When you compare disks measured in GB (1000^3 bytes) to disks measured in GiB (1024^3) remember that capacity numbers given in GiB may appear smaller. For example, 1023 GiB = 1098.4 GB.
- Disk throughput is measured in input/output operations per second (IOPS) and MBps where MBps = 10^6 bytes/sec.
- Data disks can operate in cached or uncached modes. For cached data disk operation, the host cache mode is set to **ReadOnly** or **ReadWrite**. For uncached data disk operation, the host cache mode is set to **None**.
- If you want to get the best performance for your VMs, you should limit the number of data disks to two disks per vCPU.
- Expected network bandwidth** is the maximum aggregated bandwidth allocated per VM type across all NICs, for all destinations. For more information, see [Virtual machine network bandwidth](#).

Upper limits aren't guaranteed. Limits offer guidance for selecting the right VM type for the intended application. Actual network performance will depend on several factors including network congestion, application loads, and network settings. For information on optimizing network throughput, see [Optimize network throughput for Azure virtual machines](#). To achieve the expected network performance on Linux or Windows, you may need to select a specific version or optimize your VM. For more information, see [Bandwidth/Throughput testing \(NTTCP\)](#).

Other sizes

- General purpose
- Memory optimized
- Storage optimized
- GPU optimized
- High performance compute
- Previous generations

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

Ev3 and Esv3-series

2/28/2020 • 3 minutes to read • [Edit Online](#)

The Ev3 and Esv3-series feature the Intel® Xeon® 8171M 2.1 GHz (Skylake) or the Intel® Xeon® E5-2673 v4 2.3 GHz (Broadwell) processor in a hyper-threaded configuration, providing a better value proposition for most general purpose workloads, and bringing the Ev3 into alignment with the general purpose VMs of most other clouds. Memory has been expanded (from 7 GiB/vCPU to 8 GiB/vCPU) while disk and network limits have been adjusted on a per core basis to align with the move to hyperthreading. The Ev3 is the follow up to the high memory VM sizes of the D/Dv2 families.

Ev3-series

Ev3-series instances are based on feature the Intel® Xeon® 8171M 2.1 GHz (Skylake) or the Intel® Xeon® E5-2673 v4 2.3 GHz (Broadwell) processor and Intel Turbo Boost Technology 2.0. Ev3-series instances are ideal for memory-intensive enterprise applications.

Data disk storage is billed separately from virtual machines. To use premium storage disks, use the ESv3 sizes. The pricing and billing meters for ESv3 sizes are the same as Ev3-series.

Ev3-series VM's feature Intel® Hyper-Threading Technology.

ACU: 160 - 190

Premium Storage: Not Supported

Premium Storage caching: Not Supported

SIZE	VCPUs	MEMORY: GiB	TEMP STORAGE (SSD) GiB	MAX DATA DISKS	MAX TEMP STORAGE THROUGHPUT: IOPS / READ MBPS / WRITE MBPS	MAX NICs / NETWORK BANDWIDTH
Standard_E2_v3	2	16	50	4	3000/46/23	2/1000
Standard_E4_v3	4	32	100	8	6000/93/46	2/2000
Standard_E8_v3	8	64	200	16	12000/187/93	4/4000
Standard_E16_v3	16	128	400	32	24000/375/187	8/8000
Standard_E20_v3	20	160	500	32	30000/469/234	8/10000
Standard_E32_v3	32	256	800	32	48000/750/375	8/16000
Standard_E48_v3	48	384	1200	32	96000/1000/500	8/24000

SIZE	VCPU	MEMORY: GIB	TEMP STORAGE (SSD) GIB	MAX DATA DISKS	MAX TEMP STORAGE THROUGHPUT: IOPS / READ MBPS / WRITE MBPS	MAX NICs / NETWORK BANDWIDTH
Standard_E64_v3	64	432	1600	32	96000/1000/500	8/30000
Standard_E64i_v3 ^{1,2}	64	432	1600	32	96000/1000/500	8/30000

¹ Constrained core sizes available.

² Instance is isolated to hardware dedicated to a single customer.

Esv3-series

Esv3-series instances are based on feature the Intel® Xeon® 8171M 2.1 GHz (Skylake) or the Intel® Xeon® E5-2673 v4 2.3 GHz (Broadwell) processor, Intel Turbo Boost Technology 2.0, and use premium storage. Esv3-series instances are ideal for memory-intensive enterprise applications.

Esv3-series VM's feature Intel® Hyper-Threading Technology.

ACU: 160-190

Premium Storage: Supported

Premium Storage caching: Supported

SIZE	VCPU	MEMORY: GIB	TEMP STORAGE (SSD) GIB	MAX DATA DISKS	MAX CACHED AND TEMP STORAGE THROUGHPUT: IOPS/MBPS (CACHE SIZE IN GIB)	MAX UNCACHED DISK THROUGHPUT: IOPS/MBPS	MAX NICs/EXPECTED NETWORK BANDWIDTH (MBPS)
Standard_E2s_v3	2	16	32	4	4000/32 (50)	3200/48	2/1000
Standard_E4s_v3 ¹	4	32	64	8	8000/64 (100)	6400/96	2/2000
Standard_E8s_v3 ¹	8	64	128	16	16000/128 (200)	12800/192	4/4000
Standard_E16s_v3 ¹	16	128	256	32	32000/256 (400)	25600/384	8/8000
Standard_E20s_v3	20	160	320	32	40000/320 (400)	32000/480	8/10000
Standard_E32s_v3 ¹	32	256	512	32	64000/512 (800)	51200/768	8/16000
Standard_E48s_v3 ¹	48	384	768	32	96000/768 (1200)	76800/1152	8/24000

SIZE	VCPU	MEMORY: GiB	TEMP STORAGE (SSD) GiB	MAX DATA DISKS	MAX CACHED AND TEMP STORAGE THROUGHPUT: IOPS/MBPS (CACHE SIZE IN GiB)	MAX UNCACHED DISK THROUGHPUT: IOPS/MBPS	MAX NICs/EXPECTED NETWORK BANDWIDTH (MBPS)
------	------	----------------	------------------------------	-------------------	--	---	---

Standard_E 64s_v3 ¹	64	432	864	32	128000/10 24 (1600)	80000/120 0	8/30000
Standard_E 64is_v3 ²	64	432	864	32	128000/10 24 (1600)	80000/120 0	8/30000

¹ Constrained core sizes available.

² Instance is isolated to hardware dedicated to a single customer.

Size table definitions

- Storage capacity is shown in units of GiB or 1024^3 bytes. When you compare disks measured in GB (1000^3 bytes) to disks measured in GiB (1024^3) remember that capacity numbers given in GiB may appear smaller. For example, 1023 GiB = 1098.4 GB.
- Disk throughput is measured in input/output operations per second (IOPS) and MBps where MBps = 10^6 bytes/sec.
- Data disks can operate in cached or uncached modes. For cached data disk operation, the host cache mode is set to **ReadOnly** or **ReadWrite**. For uncached data disk operation, the host cache mode is set to **None**.
- If you want to get the best performance for your VMs, you should limit the number of data disks to two disks per vCPU.
- Expected network bandwidth** is the maximum aggregated bandwidth allocated per VM type across all NICs, for all destinations. For more information, see [Virtual machine network bandwidth](#).

Upper limits aren't guaranteed. Limits offer guidance for selecting the right VM type for the intended application. Actual network performance will depend on several factors including network congestion, application loads, and network settings. For information on optimizing network throughput, see [Optimize network throughput for Azure virtual machines](#). To achieve the expected network performance on Linux or Windows, you may need to select a specific version or optimize your VM. For more information, see [Bandwidth/Throughput testing \(NTTCP\)](#).

Other sizes

- [General purpose](#)
- [Memory optimized](#)
- [Storage optimized](#)
- [GPU optimized](#)
- [High performance compute](#)
- [Previous generations](#)

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

Eav4 and Easv4-series

2/28/2020 • 3 minutes to read • [Edit Online](#)

The Eav4-series and Easv4-series utilize AMD's 2.35Ghz EPYC™ 7452 processor in a multi-threaded configuration with up to 256MB L3 cache, increasing options for running most memory optimized workloads. The Eav4-series and Easv4-series have the same memory and disk configurations as the Ev3 & Esv3-series.

Eav4-series

ACU: 230 - 260

Premium Storage: Not Supported

Premium Storage caching: Not Supported

Eav4-series sizes are based on the 2.35Ghz AMD EPYC™ 7452 processor that can achieve a boosted maximum frequency of 3.35GHz and use premium SSD. The Eav4-series sizes are ideal for memory-intensive enterprise applications. Data disk storage is billed separately from virtual machines. To use premium SSD, use the Easv4-series sizes. The pricing and billing meters for Easv4 sizes are the same as the Eav3-series.

SIZE	VCPU	MEMORY: GIB	TEMP STORAGE (SSD) GIB	MAX DATA DISKS	MAX TEMP STORAGE THROUGHPUT: IOPS / READ MBPS / WRITE MBPS	MAX NICs / EXPECTED NETWORK BANDWIDTH (MBPS)
Standard_E2a_v4	2	16	50	4	3000 / 46 / 23	2 / 1000
Standard_E4a_v4	4	32	100	8	6000 / 93 / 46	2 / 2000
Standard_E8a_v4	8	64	200	16	12000 / 187 / 93	4 / 4000
Standard_E16a_v4	16	128	400	32	24000 / 375 / 187	8 / 8000
Standard_E20a_v4	20	160	500	32	30000 / 468 / 234	8 / 10000
Standard_E32a_v4	32	256	800	32	48000 / 750 / 375	8 / 16000
Standard_E48a_v4 **	48	384	1200	32		
Standard_E64a_v4 **	64	512	1600	32		
Standard_E96a_v4 **	96	672	2400	32		

** These sizes are in Preview. If you are interested in trying out these larger sizes, sign up at <https://aka.ms/AzureAMDLargeVMPreview>.

Easv4-series

ACU: 230 - 260

Premium Storage: Supported

Premium Storage caching: Supported

Easv4-series sizes are based on the 2.35Ghz AMD EPYC™ 7452 processor that can achieve a boosted maximum frequency of 3.35GHz and use premium SSD. The Easv4-series sizes are ideal for memory-intensive enterprise applications.

SIZE	VCPU	MEMORY: GIB	TEMP STORAGE (SSD) GIB	MAX DATA DISKS	MAX CACHED AND TEMP STORAGE THROUGHPUT: IOPS / MBPS (CACHE SIZE IN GIB)	MAX UNCACHED DISK THROUGHPUT: IOPS / MBPS	MAX NICs / EXPECTED NETWORK BANDWIDTH (MBPS)
Standard_E_2as_v4	2	16	32	4	4000 / 32 (50)	3200 / 48	2 / 1000
Standard_E_4as_v4	4	32	64	8	8000 / 64 (100)	6400 / 96	2 / 2000
Standard_E_8as_v4	8	64	128	16	16000 / 128 (200)	12800 / 192	4 / 4000
Standard_E_16as_v4	16	128	256	32	32000 / 255 (400)	25600 / 384	8 / 8000
Standard_E_20as_v4	20	160	320	32	40000 / 320 (500)	32000 / 480	8 / 10000
Standard_E_32as_v4	32	256	512	32	64000 / 510 (800)	51200 / 768	8 / 16000
Standard_E_48as_v4 **	48	384	768	32			
Standard_E_64as_v4 **	64	512	1024	32			
Standard_E_96as_v4 **	96	672	1344	32			

** These sizes are in Preview. If you are interested in trying out these larger sizes, sign up at <https://aka.ms/AzureAMDLargeVMPreview>.

Size table definitions

- Storage capacity is shown in units of GiB or 1024^3 bytes. When you compare disks measured in GB (1000^3 bytes) to disks measured in GiB (1024^3) remember that capacity numbers given in GiB may

appear smaller. For example, 1023 GiB = 1098.4 GB.

- Disk throughput is measured in input/output operations per second (IOPS) and MBps where MBps = 10^6 bytes/sec.
- Data disks can operate in cached or uncached modes. For cached data disk operation, the host cache mode is set to **ReadOnly** or **ReadWrite**. For uncached data disk operation, the host cache mode is set to **None**.
- If you want to get the best performance for your VMs, you should limit the number of data disks to two disks per vCPU.
- **Expected network bandwidth** is the maximum aggregated bandwidth allocated per VM type across all NICs, for all destinations. For more information, see [Virtual machine network bandwidth](#).

Upper limits aren't guaranteed. Limits offer guidance for selecting the right VM type for the intended application. Actual network performance will depend on several factors including network congestion, application loads, and network settings. For information on optimizing network throughput, see [Optimize network throughput for Azure virtual machines](#). To achieve the expected network performance on Linux or Windows, you may need to select a specific version or optimize your VM. For more information, see [Bandwidth/Throughput testing \(NTTCP\)](#).

Other sizes

- [General purpose](#)
- [Memory optimized](#)
- [Storage optimized](#)
- [GPU optimized](#)
- [High performance compute](#)
- [Previous generations](#)

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

M-series

2/28/2020 • 2 minutes to read • [Edit Online](#)

The M-series offers a high vCPU count (up to 128 vCPUs) and a large amount of memory (up to 3.8 TiB). It's also ideal for extremely large databases or other applications that benefit from high vCPU counts and large amounts of memory. M-series sizes are based on the Intel® Xeon® CPU E7-8890 v3 @ 2.50GHz

M-series VM's feature Intel® Hyper-Threading Technology

ACU: 160-180

Premium Storage: Supported

Premium Storage caching: Supported

Write Accelerator: [Supported](#)

SIZE	VCPU	MEMORY: GIB	TEMP STORAGE (SSD) GIB	MAX DATA DISKS	MAX CACHED AND TEMP STORAGE THROUGHPUT: IOPS/MBPS (CACHE SIZE IN GIB)	MAX UNCACHED DISK THROUGHPUT: IOPS/MBPS	MAX NICs/EXPECTED NETWORK BANDWIDTH (MBPS)
Standard_M 8ms ²	8	218.75	256	8	10000/100 (793)	5000/125	4/2000
Standard_M 16ms ²	16	437.5	512	16	20000/200 (1587)	10000/250	8/4000
Standard_M 32ts	32	192	1024	32	40000/400 (3174)	20000/500	8/8000
Standard_M 32ls	32	256	1024	32	40000/400 (3174)	20000/500	8/8000
Standard_M 32ms ²	32	875	1024	32	40000/400 (3174)	20000/500	8/8000
Standard_M 64s	64	1024	2048	64	80000/800 (6348)	40000/1000	8/16000
Standard_M 64ls	64	512	2048	64	80000/800 (6348)	40000/1000	8/16000
Standard_M 64ms ³	64	1792	2048	64	80000/800 (6348)	40000/1000	8/16000
Standard_M 128s ¹	128	2048	4096	64	160000/1600 (12696)	80000/2000	8/30000

SIZE	VCPUs	MEMORY: GiB	TEMP STORAGE (SSD) GiB	MAX DATA DISKS	MAX CACHED AND TEMP STORAGE THROUGHPUT: IOPS/MBPS (CACHE SIZE IN GiB)	MAX UNCACHED DISK THROUGHPUT: IOPS/MBPS	MAX NICs/EXPECT ED NETWORK BANDWIDTH (MBPS)
Standard_M 128ms ^{1,2,3}	128	3892	4096	64	160000/16 00 (12696)	80000/200 0	8/30000
Standard_M 64	64	1024	7168	64	80000/800 (1228)	40000/100 0	8/16000
Standard_M 64m	64	1792	7168	64	80000/800 (1228)	40000/100 0	8/16000
Standard_M 128 ¹	128	2048	14336	64	250000/16 00 (2456)	80000/200 0	8/32000
Standard_M 128m ¹	128	3892	14336	64	250000/16 00 (2456)	80000/200 0	8/32000

¹ More than 64 vCPU's require one of these supported guest OSes: Windows Server 2016, Ubuntu 16.04 LTS, SLES 12 SP2, and Red Hat Enterprise Linux, CentOS 7.3 or Oracle Linux 7.3 with LIS 4.2.1.

² Constrained core sizes available.

³ Instance is isolated to hardware dedicated to a single customer.

Size table definitions

- Storage capacity is shown in units of GiB or 1024^3 bytes. When you compare disks measured in GB (1000^3 bytes) to disks measured in GiB (1024^3) remember that capacity numbers given in GiB may appear smaller. For example, 1023 GiB = 1098.4 GB.
- Disk throughput is measured in input/output operations per second (IOPS) and MBps where MBps = 10^6 bytes/sec.
- Data disks can operate in cached or uncached modes. For cached data disk operation, the host cache mode is set to **ReadOnly** or **ReadWrite**. For uncached data disk operation, the host cache mode is set to **None**.
- If you want to get the best performance for your VMs, you should limit the number of data disks to two disks per vCPU.
- Expected network bandwidth** is the maximum aggregated bandwidth allocated per VM type across all NICs, for all destinations. For more information, see [Virtual machine network bandwidth](#).

Upper limits aren't guaranteed. Limits offer guidance for selecting the right VM type for the intended application. Actual network performance will depend on several factors including network congestion, application loads, and network settings. For information on optimizing network throughput, see [Optimize network throughput for Azure virtual machines](#). To achieve the expected network performance on Linux or Windows, you may need to select a specific version or optimize your VM. For more information, see [Bandwidth/Throughput testing \(NTTCP\)](#).

Other sizes

- General purpose
- Memory optimized
- Storage optimized
- GPU optimized
- High performance compute
- Previous generations

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

Mv2-series

2/28/2020 • 2 minutes to read • [Edit Online](#)

The Mv2-series features high throughput, low latency platform running on a hyper-threaded Intel® Xeon® Platinum 8180M 2.5GHz (Skylake) processor with an all core base frequency of 2.5 GHz and a max turbo frequency of 3.8 GHz. All Mv2-series virtual machine sizes can use both standard and premium persistent disks. Mv2-series instances are memory optimized VM sizes providing unparalleled computational performance to support large in-memory databases and workloads, with a high memory-to-CPU ratio that is ideal for relational database servers, large caches, and in-memory analytics.

Mv2-series VM's feature Intel® Hyper-Threading Technology

Premium Storage: Supported

Premium Storage caching: Supported

Write Accelerator: [Supported](#)

SIZE	VCPU	MEMORY: GIB	TEMP STORAGE (SSD) GIB	MAX DATA DISKS	MAX CACHED AND TEMP STORAGE THROUGHPUT: IOPS / MBPS (CACHE SIZE IN GIB)	MAX UNCACHED DISK THROUGHPUT: IOPS / MBPS	MAX NICs / EXPECTED NETWORK BANDWIDTH (MBPS)
Standard_M_208ms_v2 ¹	208	5700	4096	64	80000 / 800 (7040)	40000 / 1000	8 / 16000
Standard_M_208s_v2 ¹	208	2850	4096	64	80000 / 800 (7040)	40000 / 1000	8 / 16000
Standard_M_416ms_v2 ^{1, 2}	416	11400	8192	64	250000 / 1600 (14080)	80000 / 2000	8 / 32000
Standard_M_416s_v2 ^{1, 2}	416	5700	8192	64	250000 / 1600 (14080)	80000 / 2000	8 / 32000

¹ Mv2-series VMs are generation 2 only. If you're using Linux, see [Support for generation 2 VMs on Azure](#) for instructions on how to find and select an image.

² For the M416ms_v2 and M416s_v2 sizes, note that there is initial support for the following image only: "GEN2: SUSE Linux Enterprise Server (SLES) 12 SP4 for SAP Applications."

Size table definitions

- Storage capacity is shown in units of GiB or 1024^3 bytes. When you compare disks measured in GB (1000^3 bytes) to disks measured in GiB (1024^3) remember that capacity numbers given in GiB may appear smaller. For example, 1023 GiB = 1098.4 GB.
- Disk throughput is measured in input/output operations per second (IOPS) and MBps where MBps = 10^6 bytes/sec.

- Data disks can operate in cached or uncached modes. For cached data disk operation, the host cache mode is set to **ReadOnly** or **ReadWrite**. For uncached data disk operation, the host cache mode is set to **None**.
- If you want to get the best performance for your VMs, you should limit the number of data disks to two disks per vCPU.
- **Expected network bandwidth** is the maximum aggregated bandwidth allocated per VM type across all NICs, for all destinations. For more information, see [Virtual machine network bandwidth](#).

Upper limits aren't guaranteed. Limits offer guidance for selecting the right VM type for the intended application. Actual network performance will depend on several factors including network congestion, application loads, and network settings. For information on optimizing network throughput, see [Optimize network throughput for Azure virtual machines](#). To achieve the expected network performance on Linux or Windows, you may need to select a specific version or optimize your VM. For more information, see [Bandwidth/Throughput testing \(NTTCP\)](#).

Other sizes

- [General purpose](#)
- [Memory optimized](#)
- [Storage optimized](#)
- [GPU optimized](#)
- [High performance compute](#)
- [Previous generations](#)

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

Constrained vCPU capable VM sizes

11/13/2019 • 2 minutes to read • [Edit Online](#)

Some database workloads like SQL Server or Oracle require high memory, storage, and I/O bandwidth, but not a high core count. Many database workloads are not CPU-intensive. Azure offers certain VM sizes where you can constrain the VM vCPU count to reduce the cost of software licensing, while maintaining the same memory, storage, and I/O bandwidth.

The vCPU count can be constrained to one half or one quarter of the original VM size. These new VM sizes have a suffix that specifies the number of active vCPUs to make them easier for you to identify.

For example, the current VM size Standard_GS5 comes with 32 vCPUs, 448 GB RAM, 64 disks (up to 256 TB), and 80,000 IOPs or 2 GB/s of I/O bandwidth. The new VM sizes Standard_GS5-16 and Standard_GS5-8 comes with 16 and 8 active vCPUs respectively, while maintaining the rest of the specs of the Standard_GS5 for memory, storage, and I/O bandwidth.

The licensing fees charged for SQL Server or Oracle are constrained to the new vCPU count, and other products should be charged based on the new vCPU count. This results in a 50% to 75% increase in the ratio of the VM specs to active (billable) vCPUs. These new VM sizes allow customer workloads to use the same memory, storage, and I/O bandwidth while optimizing their software licensing cost. At this time, the compute cost, which includes OS licensing, remains the same one as the original size. For more information, see [Azure VM sizes for more cost-effective database workloads](#).

NAME	VCPU	SPECS
Standard_M8-2ms	2	Same as M8ms
Standard_M8-4ms	4	Same as M8ms
Standard_M16-4ms	4	Same as M16ms
Standard_M16-8ms	8	Same as M16ms
Standard_M32-8ms	8	Same as M32ms
Standard_M32-16ms	16	Same as M32ms
Standard_M64-32ms	32	Same as M64ms
Standard_M64-16ms	16	Same as M64ms
Standard_M128-64ms	64	Same as M128ms
Standard_M128-32ms	32	Same as M128ms
Standard_E4-2s_v3	2	Same as E4s_v3
Standard_E8-4s_v3	4	Same as E8s_v3
Standard_E8-2s_v3	2	Same as E8s_v3

NAME	VCPUs	SPECS
Standard_E16-8s_v3	8	Same as E16s_v3
Standard_E16-4s_v3	4	Same as E16s_v3
Standard_E32-16s_v3	16	Same as E32s_v3
Standard_E32-8s_v3	8	Same as E32s_v3
Standard_E64-32s_v3	32	Same as E64s_v3
Standard_E64-16s_v3	16	Same as E64s_v3
Standard_GS4-8	8	Same as GS4
Standard_GS4-4	4	Same as GS4
Standard_GS5-16	16	Same as GS5
Standard_GS5-8	8	Same as GS5
Standard_DS11-1_v2	1	Same as DS11_v2
Standard_DS12-2_v2	2	Same as DS12_v2
Standard_DS12-1_v2	1	Same as DS12_v2
Standard_DS13-4_v2	4	Same as DS13_v2
Standard_DS13-2_v2	2	Same as DS13_v2
Standard_DS14-8_v2	8	Same as DS14_v2
Standard_DS14-4_v2	4	Same as DS14_v2

Other sizes

- [Compute optimized](#)
- [Memory optimized](#)
- [Storage optimized](#)
- [GPU](#)
- [High performance compute](#)

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

Storage optimized virtual machine sizes

2/28/2020 • 2 minutes to read • [Edit Online](#)

Storage optimized 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, and NICs as well as local storage throughput and network bandwidth for each optimized size.

The [Lsv2-series](#) features high throughput, low latency, directly mapped local NVMe storage running on the [AMD EPYC™ 7551 processor](#) with an all core boost of 2.55GHz and a max boost of 3.0GHz. The Lsv2-series VMs come in sizes from 8 to 80 vCPU in a simultaneous multi-threading configuration. There is 8 GiB of memory per vCPU, and one 1.92TB NVMe SSD M.2 device per 8 vCPUs, with up to 19.2TB (10x1.92TB) available on the L80s v2.

Other sizes

- [General purpose](#)
- [Compute optimized](#)
- [Memory optimized](#)
- [GPU optimized](#)
- [High performance compute](#)
- [Previous generations](#)

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

Learn how to optimize performance on the Lsv2-series virtual machines for [Windows](#) or [Linux](#).

Lsv2-series

2/28/2020 • 3 minutes to read • [Edit Online](#)

The Lsv2-series features high throughput, low latency, directly mapped local NVMe storage running on the [AMD EPYC™ 7551 processor](#) with an all core boost of 2.55GHz and a max boost of 3.0GHz. The Lsv2-series VMs come in sizes from 8 to 80 vCPU in a simultaneous multi-threading configuration. There is 8 GiB of memory per vCPU, and one 1.92TB NVMe SSD M.2 device per 8 vCPUs, with up to 19.2TB (10x1.92TB) available on the L80s v2.

NOTE

The Lsv2-series VMs are optimized to use the local disk on the node attached directly to the VM rather than using durable data disks. This allows for greater IOPs / throughput for your workloads. The Lsv2 and Ls-series do not support the creation of a local cache to increase the IOPs achievable by durable data disks.

The high throughput and IOPs of the local disk makes the Lsv2-series VMs ideal for NoSQL stores such as Apache Cassandra and MongoDB which replicate data across multiple VMs to achieve persistence in the event of the failure of a single VM.

To learn more, see Optimize performance on the Lsv2-series virtual machines for [Windows](#) or [Linux](#).

ACU: 150-175

Premium Storage: Supported

Premium Storage caching: Not Supported

SIZE	VCPU	MEMORY (GiB)	TEMP DISK ¹ (GiB)	NVME DISKS ²	NVME DISK THROUGHPUT ³ (READ IOPS/MBPS)	MAX UNCACHE D DATA DISK THROUGHPUT (IOPS/MBPS) ⁴	MAX DATA DISKS	MAX NICs / EXPECTED NETWORK BANDWIDTH (Mbps)
Standard_L8s_v2	8	64	80	1x1.92 TB	400000/2000	8000/160	16	2 / 3200
Standard_L16s_v2	16	128	160	2x1.92 TB	800000/4000	16000/320	32	4 / 6400
Standard_L32s_v2	32	256	320	4x1.92 TB	1.5M/8000	32000/640	32	8 / 12800
Standard_L48s_v2	48	384	480	6x1.92 TB	2.2M/14000	48000/960	32	8 / 16000+
Standard_L64s_v2	64	512	640	8x1.92 TB	2.9M/16000	64000/1280	32	8 / 16000+
Standard_L80s_v2 ⁵	80	640	800	10x1.92TB	3.8M/20000	80000/1400	32	8 / 16000+

¹ Lsv2-series VMs have a standard SCSI based temp resource disk for OS paging/swap file use (D: on Windows, /dev/sdb on Linux). This disk provides 80 GiB of storage, 4,000 IOPS, and 80 MBps transfer rate for every 8

vCPUs (e.g. Standard_L80s_v2 provides 800 GiB at 40,000 IOPS and 800 MBPS). This ensures the NVMe drives can be fully dedicated to application use. This disk is Ephemeral, and all data will be lost on stop/deallocate.

² Local NVMe Disks are ephemeral, data will be lost on these disks if you stop/deallocate your VM.

³ Hyper-V NVMe Direct technology provides unthrottled access to local NVMe drives mapped securely into the guest VM space. Achieving maximum performance requires using either the latest WS2019 build or Ubuntu 18.04 or 16.04 from the Azure Marketplace. Write performance varies based on IO size, drive load, and capacity utilization.

⁴ Lsv2-series VMs do not provide host cache for data disk as it does not benefit the Lsv2 workloads. However, Lsv2 VMs can accommodate Azure's Ephemeral VM OS disk option (up to 30 GiB).

⁵ VMs with more than 64 vCPUs require one of these supported guest operating systems:

- Windows Server 2016 or later
- Ubuntu 16.04 LTS or later, with Azure tuned kernel (4.15 kernel or later)
- SLES 12 SP2 or later
- RHEL or CentOS version 6.7 through 6.10, with Microsoft-provided LIS package 4.3.1 (or later) installed
- RHEL or CentOS version 7.3, with Microsoft-provided LIS package 4.2.1 (or later) installed
- RHEL or CentOS version 7.6 or later
- Oracle Linux with UEK4 or later
- Debian 9 with the backports kernel, Debian 10 or later
- CoreOS with a 4.14 kernel or later

Size table definitions

- Storage capacity is shown in units of GiB or 1024^3 bytes. When comparing disks measured in GB (1000^3 bytes) to disks measured in GiB (1024^3) remember that capacity numbers given in GiB may appear smaller. For example, 1023 GiB = 1098.4 GB
- Disk throughput is measured in input/output operations per second (IOPS) and MBps where MBps = 10^6 bytes/sec.
- If you want to get the best performance for your VMs, you should limit the number of data disks to 2 disks per vCPU.
- **Expected network bandwidth** is the maximum aggregated [bandwidth allocated per VM type](#) across all NICs, for all destinations. Upper limits are not guaranteed, but are intended to provide guidance for selecting the right VM type for the intended application. Actual network performance will depend on a variety of factors including network congestion, application loads, and network settings. For information on optimizing network throughput, see [Optimizing network throughput for Windows and Linux](#). To achieve the expected network performance on Linux or Windows, it may be necessary to select a specific version or optimize your VM. For more information, see [How to reliably test for virtual machine throughput](#).

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

Optimize performance on the Lsv2-series virtual machines

11/13/2019 • 6 minutes to read • [Edit Online](#)

Lsv2-series virtual machines support a variety of workloads that need high I/O and throughput on local storage across a wide range of applications and industries. The Lsv2-series is ideal for Big Data, SQL, NoSQL databases, data warehousing and large transactional databases, including Cassandra, MongoDB, Cloudera, and Redis.

The design of the Lsv2-series Virtual Machines (VMs) maximizes the AMD EPYC™ 7551 processor to provide the best performance between the processor, memory, NVMe devices, and the VMs. Working with partners in Linux, several builds are available Azure Marketplace that are optimized for Lsv2-series performance and currently include:

- Ubuntu 18.04
- Ubuntu 16.04
- RHEL 8.0
- Debian 9
- Debian 10

This article provides tips and suggestions to ensure your workloads and applications achieve the maximum performance designed into the VMs. The information on this page will be continuously updated as more Lsv2 optimized images are added to the Azure Marketplace.

AMD EYPC™ chipset architecture

Lsv2-series VMs use AMD EYPC™ server processors based on the Zen microarchitecture. AMD developed Infinity Fabric (IF) for EYPC™ as scalable interconnect for its NUMA model that could be used for on-die, on-package, and multi-package communications. Compared with QPI (Quick-Path Interconnect) and UPI (Ultra-Path Interconnect) used on Intel modern monolithic-die processors, AMD's many-NUMA small-die architecture may bring both performance benefits as well as challenges. The actual impact of memory bandwidth and latency constraints could vary depending on the type of workloads running.

Tips to maximize performance

- If you are uploading a custom Linux GuestOS for your workload, note that Accelerated Networking will be **OFF** by default. If you intend to enable Accelerated Networking, enable it at the time of VM creation for best performance.
- The hardware that powers the Lsv2-series VMs utilizes NVMe devices with eight I/O Queue Pairs (QP)s. Every NVMe device I/O queue is actually a pair: a submission queue and a completion queue. The NVMe driver is set up to optimize the utilization of these eight I/O QPs by distributing I/O's in a round robin schedule. To gain max performance, run eight jobs per device to match.
- Avoid mixing NVMe admin commands (for example, NVMe SMART info query, etc.) with NVMe I/O commands during active workloads. Lsv2 NVMe devices are backed by Hyper-V NVMe Direct technology, which switches into "slow mode" whenever any NVMe admin commands are pending. Lsv2 users could see a dramatic performance drop in NVMe I/O performance if that happens.
- Lsv2 users should not rely on device NUMA information (all 0) reported from within the VM for data drives to decide the NUMA affinity for their apps. The recommended way for better performance is to spread

workloads across CPUs if possible.

- The maximum supported queue depth per I/O queue pair for Lsv2 VM NVMe device is 1024 (vs. Amazon i3 QD 32 limit). Lsv2 users should limit their (synthetic) benchmarking workloads to queue depth 1024 or lower to avoid triggering queue full conditions, which can reduce performance.

Utilizing local NVMe storage

Local storage on the 1.92 TB NVMe disk on all Lsv2 VMs is ephemeral. During a successful standard reboot of the VM, the data on the local NVMe disk will persist. The data will not persist on the NVMe if the VM is redeployed, de-allocated, or deleted. Data will not persist if another issue causes the VM, or the hardware it is running on, to become unhealthy. When this happens, any data on the old host is securely erased.

There will also be cases when the VM needs to be moved to a different host machine, for example, during a planned maintenance operation. Planned maintenance operations and some hardware failures can be anticipated with [Scheduled Events](#). Scheduled Events should be used to stay updated on any predicted maintenance and recovery operations.

In the case that a planned maintenance event requires the VM to be recreated on a new host with empty local disks, the data will need to be resynchronized (again, with any data on the old host being securely erased). This occurs because Lsv2-series VMs do not currently support live migration on the local NVMe disk.

There are two modes for planned maintenance.

Standard VM customer-controlled maintenance

- The VM is moved to an updated host during a 30-day window.
- Lsv2 local storage data could be lost, so backing-up data prior to the event is recommended.

Automatic maintenance

- Occurs if the customer does not execute customer-controlled maintenance, or in the event of emergency procedures such as a security zero-day event.
- Intended to preserve customer data, but there is a small risk of a VM freeze or reboot.
- Lsv2 local storage data could be lost, so backing-up data prior to the event is recommended.

For any upcoming service events, use the controlled maintenance process to select a time most convenient to you for the update. Prior to the event, you may back up your data in premium storage. After the maintenance event completes, you can return your data to the refreshed Lsv2 VMs local NVMe storage.

Scenarios that maintain data on local NVMe disks include:

- The VM is running and healthy.
- The VM is rebooted in place (by you or Azure).
- The VM is paused (stopped without de-allocation).
- The majority of the planned maintenance servicing operations.

Scenarios that securely erase data to protect the customer include:

- The VM is redeployed, stopped (de-allocated), or deleted (by you).
- The VM becomes unhealthy and has to service heal to another node due to a hardware issue.
- A small number of the planned maintenance servicing operations that requires the VM to be reallocated to another host for servicing.

To learn more about options for backing up data in local storage, see [Backup and disaster recovery for Azure IaaS disks](#).

Frequently asked questions

- **How do I start deploying Lsv2-series VMs?**

Much like any other VM, use the [Portal](#), [Azure CLI](#), or [PowerShell](#) to create a VM.

- **Will a single NVMe disk failure cause all VMs on the host to fail?**

If a disk failure is detected on the hardware node, the hardware is in a failed state. When this occurs, all VMs on the node are automatically de-allocated and moved to a healthy node. For Lsv2-series VMs, this means that the customer's data on the failing node is also securely erased and will need to be recreated by the customer on the new node. As noted, before live migration becomes available on Lsv2, the data on the failing node will be proactively moved with the VMs as they are transferred to another node.

- **Do I need to make any adjustments to rq_affinity for performance?**

The rq_affinity setting is a minor adjustment when using the absolute maximum input/output operations per second (IOPS). Once everything else is working well, then try to set rq_affinity to 0 to see if it makes a difference.

- **Do I need to change the blk_mq settings?**

RHEL/CentOS 7.x automatically uses blk-mq for the NVMe devices. No configuration changes or settings are necessary. The scsi_mod.use_blk_mq setting is for SCSI only and was used during Lsv2 Preview because the NVMe devices were visible in the guest VMs as SCSI devices. Currently, the NVMe devices are visible as NVMe devices, so the SCSI blk-mq setting is irrelevant.

- **Do I need to change "fio"?**

To get maximum IOPS with a performance measuring tool like 'fio' in the L64v2 and L80v2 VM sizes, set "rq_affinity" to 0 on each NVMe device. For example, this command line will set "rq_affinity" to zero for all 10 NVMe devices in an L80v2 VM:

```
for i in `seq 0 9`; do echo 0 >/sys/block/nvme${i}n1/queue/rq_affinity; done
```

Also note that the best performance is obtained when I/O is done directly to each of the raw NVMe devices with no partitioning, no file systems, no RAID 0 config, etc. Before starting a testing session, ensure the configuration is in a known fresh/clean state by running `blkdiscard` on each of the NVMe devices.

Next steps

- See specifications for all VMs optimized for storage performance on Azure

GPU optimized virtual machine sizes

2/28/2020 • 2 minutes to read • [Edit Online](#)

GPU optimized VM sizes are specialized virtual machines available with single or multiple NVIDIA 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.

- [NC-series](#), [NCv2-series](#), [NCv3-series](#) sizes are optimized for compute-intensive and network-intensive applications and algorithms. Some examples are CUDA and OpenCL-based applications and simulations, AI, and Deep Learning. The NCv3-series is focused on high-performance computing workloads featuring NVIDIA's Tesla V100 GPU. The NC-series uses the Intel Xeon E5-2690 v3 2.60GHz v3 (Haswell) processor, and the NCv2-series and NCv3-series VMs use the Intel Xeon E5-2690 v4 (Broadwell) processor.
- [ND-series](#), and [NDv2-series](#) sizes are focused on training and inference scenarios for deep learning. They use the NVIDIA Tesla P40 GPU and the Intel Xeon E5-2690 v4 (Broadwell) processor. The NDv2-series uses the Intel Xeon Platinum 8168 (Skylake) processor.
- [NV-series](#) and [NVv3-series](#) sizes are optimized and designed for remote visualization, streaming, gaming, encoding, and VDI scenarios using frameworks such as OpenGL and DirectX. These VMs are backed by the NVIDIA Tesla M60 GPU.
- [NVv4-series](#) VM sizes optimized and designed for VDI and remote visualization. With partitioned GPUs, NVv4 offers the right size for workloads requiring smaller GPU resources. These VMs are backed by the AMD Radeon Instinct MI25 GPU. NVv4 VMs currently support only Windows guest operating system.

Supported operating systems and drivers

To take advantage of the GPU capabilities of Azure N-series VMs, NVIDIA GPU drivers must be installed.

The [NVIDIA GPU Driver Extension](#) installs appropriate NVIDIA CUDA or GRID drivers on an N-series VM. Install or manage the extension using the Azure portal or tools such as Azure PowerShell or Azure Resource Manager templates. See the [NVIDIA GPU Driver Extension documentation](#) for supported operating systems and deployment steps. For general information about VM extensions, see [Azure virtual machine extensions and features](#).

If you choose to install NVIDIA GPU drivers manually, see [N-series GPU driver setup for Windows](#) or [N-series GPU driver setup for Linux](#) for supported operating systems, drivers, installation, and verification steps.

Deployment considerations

- For availability of N-series VMs, see [Products available by region](#).
- N-series VMs can only be deployed in the Resource Manager deployment model.
- N-series VMs differ in the type of Azure Storage they support for their disks. NC and NV VMs only support VM disks that are backed by Standard Disk Storage (HDD). NCv2, NCv3, ND, NDv2, and NVv2 VMs only support VM disks that are backed by Premium Disk Storage (SSD).
- If you want to deploy more than a few N-series VMs, consider a pay-as-you-go subscription or other

purchase options. If you're using an [Azure free account](#), you can use only a limited number of Azure compute cores.

- You might need to increase the cores quota (per region) in your Azure subscription, and increase the separate quota for NC, NCv2, NCv3, ND, NDv2, NV, or NVv2 cores. To request a quota increase, [open an online customer support request](#) at no charge. Default limits may vary depending on your subscription category.

Other sizes

- [General purpose](#)
- [Compute optimized](#)
- [High performance compute](#)
- [Memory optimized](#)
- [Storage optimized](#)
- [Previous generations](#)

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

NC-series

2/28/2020 • 2 minutes to read • [Edit Online](#)

NC-series VMs are powered by the [NVIDIA Tesla K80](#) card and the Intel Xeon E5-2690 v3 (Haswell) processor. Users can crunch through data faster by leveraging CUDA for energy exploration applications, crash simulations, ray traced rendering, deep learning, and more. The NC24r configuration provides a low latency, high-throughput network interface optimized for tightly coupled parallel computing workloads.

Premium Storage: Not Supported

Premium Storage caching: Not Supported

SIZE	VCPUs	MEMORY: GiB	TEMP STORAGE (SSD) GiB	GPU	GPU MEMORY: GiB	MAX DATA DISKS	MAX NICs
Standard_N_C6	6	56	340	1	12	24	1
Standard_N_C12	12	112	680	2	24	48	2
Standard_N_C24	24	224	1440	4	48	64	4
Standard_N_C24r*	24	224	1440	4	48	64	4

1 GPU = one-half K80 card.

*RDMA capable

Size table definitions

- Storage capacity is shown in units of GiB or 1024^3 bytes. When you compare disks measured in GB (1000^3 bytes) to disks measured in GiB (1024^3) remember that capacity numbers given in GiB may appear smaller. For example, 1023 GiB = 1098.4 GB.
- Disk throughput is measured in input/output operations per second (IOPS) and MBps where MBps = 10^6 bytes/sec.
- Data disks can operate in cached or uncached modes. For cached data disk operation, the host cache mode is set to **ReadOnly** or **ReadWrite**. For uncached data disk operation, the host cache mode is set to **None**.
- If you want to get the best performance for your VMs, you should limit the number of data disks to two disks per vCPU.
- **Expected network bandwidth** is the maximum aggregated bandwidth allocated per VM type across all NICs, for all destinations. For more information, see [Virtual machine network bandwidth](#).

Upper limits aren't guaranteed. Limits offer guidance for selecting the right VM type for the intended application. Actual network performance will depend on several factors including network congestion, application loads, and network settings. For information on optimizing network throughput, see [Optimize network throughput for Azure virtual machines](#). To achieve the expected network performance on Linux or

Windows, you may need to select a specific version or optimize your VM. For more information, see [Bandwidth/Throughput testing \(NTTCP\)](#).

Supported operating systems and drivers

To take advantage of the GPU capabilities of Azure N-series VMs, NVIDIA GPU drivers must be installed.

The [NVIDIA GPU Driver Extension](#) installs appropriate NVIDIA CUDA or GRID drivers on an N-series VM. Install or manage the extension using the Azure portal or tools such as Azure PowerShell or Azure Resource Manager templates. See the [NVIDIA GPU Driver Extension documentation](#) for supported operating systems and deployment steps. For general information about VM extensions, see [Azure virtual machine extensions and features](#).

If you choose to install NVIDIA GPU drivers manually, see [N-series GPU driver setup for Windows](#) or [N-series GPU driver setup for Linux](#) for supported operating systems, drivers, installation, and verification steps.

Other sizes

- [General purpose](#)
- [Memory optimized](#)
- [Storage optimized](#)
- [GPU optimized](#)
- [High performance compute](#)
- [Previous generations](#)

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

NCv2-series

2/28/2020 • 2 minutes to read • [Edit Online](#)

NCv2-series VMs are powered by [NVIDIA Tesla P100](#) GPUs. These GPUs can provide more than 2x the computational performance of the NC-series. Customers can take advantage of these updated GPUs for traditional HPC workloads such as reservoir modeling, DNA sequencing, protein analysis, Monte Carlo simulations, and others. In addition to the GPUs, the NCv2-series VMs are also powered by Intel Xeon E5-2690 v4 (Broadwell) CPUs.

The NC24rs v2 configuration provides a low latency, high-throughput network interface optimized for tightly coupled parallel computing workloads.

Premium Storage: Supported

Premium Storage caching: Supported

IMPORTANT

For this VM series, the vCPU (core) quota in your subscription is initially set to 0 in each region. [Request a vCPU quota increase](#) for this series in an [available region](#).

SIZE	VCPUs	MEMORY: GiB	TEMP STORAGE (SSD) GiB	GPU	GPU MEMORY: GiB	MAX DATA DISKS	MAX UNCACHE D DISK THROUGHPUT: IOPS/MBPS	MAX NICs
Standard_NC6s_v2	6	112	736	1	16	12	20000/200	4
Standard_NC12s_v2	12	224	1474	2	32	24	40000/400	8
Standard_NC24s_v2	24	448	2948	4	64	32	80000/800	8
Standard_NC24rs_v2*	24	448	2948	4	64	32	80000/800	8

1 GPU = one P100 card.

*RDMA capable

Size table definitions

- Storage capacity is shown in units of GiB or 1024^3 bytes. When you compare disks measured in GB (1000^3 bytes) to disks measured in GiB (1024^3) remember that capacity numbers given in GiB may appear smaller. For example, 1023 GiB = 1098.4 GB.
- Disk throughput is measured in input/output operations per second (IOPS) and MBps where MBps = 10^6 bytes/sec.

- Data disks can operate in cached or uncached modes. For cached data disk operation, the host cache mode is set to **ReadOnly** or **ReadWrite**. For uncached data disk operation, the host cache mode is set to **None**.
- If you want to get the best performance for your VMs, you should limit the number of data disks to two disks per vCPU.
- **Expected network bandwidth** is the maximum aggregated bandwidth allocated per VM type across all NICs, for all destinations. For more information, see [Virtual machine network bandwidth](#).

Upper limits aren't guaranteed. Limits offer guidance for selecting the right VM type for the intended application. Actual network performance will depend on several factors including network congestion, application loads, and network settings. For information on optimizing network throughput, see [Optimize network throughput for Azure virtual machines](#). To achieve the expected network performance on Linux or Windows, you may need to select a specific version or optimize your VM. For more information, see [Bandwidth/Throughput testing \(NTTCP\)](#).

Supported operating systems and drivers

To take advantage of the GPU capabilities of Azure N-series VMs, NVIDIA GPU drivers must be installed.

The [NVIDIA GPU Driver Extension](#) installs appropriate NVIDIA CUDA or GRID drivers on an N-series VM. Install or manage the extension using the Azure portal or tools such as Azure PowerShell or Azure Resource Manager templates. See the [NVIDIA GPU Driver Extension documentation](#) for supported operating systems and deployment steps. For general information about VM extensions, see [Azure virtual machine extensions and features](#).

If you choose to install NVIDIA GPU drivers manually, see [N-series GPU driver setup for Windows](#) or [N-series GPU driver setup for Linux](#) for supported operating systems, drivers, installation, and verification steps.

Other sizes

- [General purpose](#)
- [Memory optimized](#)
- [Storage optimized](#)
- [GPU optimized](#)
- [High performance compute](#)
- [Previous generations](#)

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

NCv3-series

2/28/2020 • 2 minutes to read • [Edit Online](#)

NCv3-series VMs are powered by [NVIDIA Tesla V100](#) GPUs. These GPUs can provide 1.5x the computational performance of the NCv2-series. Customers can take advantage of these updated GPUs for traditional HPC workloads such as reservoir modeling, DNA sequencing, protein analysis, Monte Carlo simulations, and others. The NC24rs v3 configuration provides a low latency, high-throughput network interface optimized for tightly coupled parallel computing workloads. In addition to the GPUs, the NCv3-series VMs are also powered by Intel Xeon E5-2690 v4 (Broadwell) CPUs.

Premium Storage: Supported

Premium Storage caching: Supported

IMPORTANT

For this VM series, the vCPU (core) quota in your subscription is initially set to 0 in each region. [Request a vCPU quota increase](#) for this series in an [available region](#).

SIZE	VCPUs	MEMORY: GiB	TEMP STORAGE (SSD) GiB	GPU	GPU MEMORY: GiB	MAX DATA DISKS	MAX UNCACHED DISK THROUGHPUT: IOPS/MBPS	MAX NICs
Standard_NC6s_v3	6	112	736	1	16	12	20000/200	4
Standard_NC12s_v3	12	224	1474	2	32	24	40000/400	8
Standard_NC24s_v3	24	448	2948	4	64	32	80000/800	8
Standard_NC24rs_v3*	24	448	2948	4	64	32	80000/800	8

1 GPU = one V100 card.

*RDMA capable

Size table definitions

- Storage capacity is shown in units of GiB or 1024^3 bytes. When you compare disks measured in GB (1000^3 bytes) to disks measured in GiB (1024^3) remember that capacity numbers given in GiB may appear smaller. For example, 1023 GiB = 1098.4 GB.
- Disk throughput is measured in input/output operations per second (IOPS) and MBps where MBps = 10^6 bytes/sec.
- Data disks can operate in cached or uncached modes. For cached data disk operation, the host cache mode

is set to **ReadOnly** or **ReadWrite**. For uncached data disk operation, the host cache mode is set to **None**.

- If you want to get the best performance for your VMs, you should limit the number of data disks to two disks per vCPU.
- **Expected network bandwidth** is the maximum aggregated bandwidth allocated per VM type across all NICs, for all destinations. For more information, see [Virtual machine network bandwidth](#).

Upper limits aren't guaranteed. Limits offer guidance for selecting the right VM type for the intended application. Actual network performance will depend on several factors including network congestion, application loads, and network settings. For information on optimizing network throughput, see [Optimize network throughput for Azure virtual machines](#). To achieve the expected network performance on Linux or Windows, you may need to select a specific version or optimize your VM. For more information, see [Bandwidth/Throughput testing \(NTTCP\)](#).

Supported operating systems and drivers

To take advantage of the GPU capabilities of Azure N-series VMs, NVIDIA GPU drivers must be installed.

The [NVIDIA GPU Driver Extension](#) installs appropriate NVIDIA CUDA or GRID drivers on an N-series VM. Install or manage the extension using the Azure portal or tools such as Azure PowerShell or Azure Resource Manager templates. See the [NVIDIA GPU Driver Extension documentation](#) for supported operating systems and deployment steps. For general information about VM extensions, see [Azure virtual machine extensions and features](#).

If you choose to install NVIDIA GPU drivers manually, see [N-series GPU driver setup for Windows](#) or [N-series GPU driver setup for Linux](#) for supported operating systems, drivers, installation, and verification steps.

Other sizes

- [General purpose](#)
- [Memory optimized](#)
- [Storage optimized](#)
- [GPU optimized](#)
- [High performance compute](#)
- [Previous generations](#)

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

ND-series

2/28/2020 • 3 minutes to read • [Edit Online](#)

The ND-series virtual machines are a new addition to the GPU family designed for AI, and Deep Learning workloads. They offer excellent performance for training and inference. ND instances are powered by [NVIDIA Tesla P40](#) GPUs and Intel Xeon E5-2690 v4 (Broadwell) CPUs. These instances provide excellent performance for single-precision floating point operations, for AI workloads utilizing Microsoft Cognitive Toolkit, TensorFlow, Caffe, and other frameworks. The ND-series also offers a much larger GPU memory size (24 GB), enabling to fit much larger neural net models. Like the NC-series, the ND-series offers a configuration with a secondary low-latency, high-throughput network through RDMA, and InfiniBand connectivity so you can run large-scale training jobs spanning many GPUs.

Premium Storage: Supported

Premium Storage caching: Supported

IMPORTANT

For this VM series, the vCPU (core) quota per region in your subscription is initially set to 0. [Request a vCPU quota increase](#) for this series in an [available region](#).

SIZE	VCPU	MEMORY: GIB	TEMP STORAGE (SSD) GIB	GPU	GPU MEMORY: GIB	MAX DATA DISKS	MAX UNCACHE D DISK THROUGH PUT: IOPS/MBPS	MAX NICs
Standard_ND6s	6	112	736	1	24	12	20000/200	4
Standard_ND12s	12	224	1474	2	48	24	40000/400	8
Standard_ND24s	24	448	2948	4	96	32	80000/800	8
Standard_ND24rs*	24	448	2948	4	96	32	80000/800	8

1 GPU = one P40 card.

*RDMA capable

Size table definitions

- Storage capacity is shown in units of GiB or 1024^3 bytes. When you compare disks measured in GB (1000^3 bytes) to disks measured in GiB (1024^3) remember that capacity numbers given in GiB may appear smaller. For example, 1023 GiB = 1098.4 GB.
- Disk throughput is measured in input/output operations per second (IOPS) and MBps where MBps = 10^6 bytes/sec.

- Data disks can operate in cached or uncached modes. For cached data disk operation, the host cache mode is set to **ReadOnly** or **ReadWrite**. For uncached data disk operation, the host cache mode is set to **None**.
- If you want to get the best performance for your VMs, you should limit the number of data disks to two disks per vCPU.
- **Expected network bandwidth** is the maximum aggregated bandwidth allocated per VM type across all NICs, for all destinations. For more information, see [Virtual machine network bandwidth](#).

Upper limits aren't guaranteed. Limits offer guidance for selecting the right VM type for the intended application. Actual network performance will depend on several factors including network congestion, application loads, and network settings. For information on optimizing network throughput, see [Optimize network throughput for Azure virtual machines](#). To achieve the expected network performance on Linux or Windows, you may need to select a specific version or optimize your VM. For more information, see [Bandwidth/Throughput testing \(NTTCP\)](#).

Supported operating systems and drivers

To take advantage of the GPU capabilities of Azure N-series VMs, NVIDIA GPU drivers must be installed.

The [NVIDIA GPU Driver Extension](#) installs appropriate NVIDIA CUDA or GRID drivers on an N-series VM. Install or manage the extension using the Azure portal or tools such as Azure PowerShell or Azure Resource Manager templates. See the [NVIDIA GPU Driver Extension documentation](#) for supported operating systems and deployment steps. For general information about VM extensions, see [Azure virtual machine extensions and features](#).

If you choose to install NVIDIA GPU drivers manually, see [N-series GPU driver setup for Windows](#) or [N-series GPU driver setup for Linux](#) for supported operating systems, drivers, installation, and verification steps.

Other sizes

- [General purpose](#)
- [Memory optimized](#)
- [Storage optimized](#)
- [GPU optimized](#)
- [High performance compute](#)
- [Previous generations](#)

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

Updated NDv2-series (Preview)

2/28/2020 • 3 minutes to read • [Edit Online](#)

The NDv2-series virtual machine is a new addition to the GPU family designed for the needs of the most demanding GPU-accelerated AI, machine learning, simulation, and HPC workloads.

NDv2 is powered by 8 NVIDIA Tesla V100 NVLINK-connected GPUs, each with 32 GB of GPU memory. Each NDv2 VM also has 40 non-HyperThreaded Intel Xeon Platinum 8168 (Skylake) cores and 672 GiB of system memory.

NDv2 instances provide excellent performance for HPC and AI workloads utilizing CUDA GPU-optimized computation kernels, and the many AI, ML, and analytics tools that support GPU acceleration 'out-of-box,' such as TensorFlow, Pytorch, Caffe, RAPIDS, and other frameworks.

Critically, the NDv2 is built for both computationally intense scale-up (harnessing 8 GPUs per VM) and scale-out (harnessing multiple VMs working together) workloads. The NDv2 series now supports 100-Gigabit InfiniBand EDR backend networking, similar to that available on the HB series of HPC VM, to allow high-performance clustering for parallel scenarios including distributed training for AI and ML. This backend network supports all major InfiniBand protocols, including those employed by NVIDIA's NCCL2 libraries, allowing for seamless clustering of GPUs.

NOTE

When enabling [InfiniBand](#) on the ND40rs_v2 VM, please use the 4.7-1.0.0.1 Mellanox OFED driver.

Due to increased GPU memory, the new ND40rs_v2 VM requires the use of [Generation 2 VMs](#) and marketplace images.

[Sign-up to request early access to the NDv2 virtual machine preview.](#)

Please note: The ND40s_v2 featuring 16 GB of per-GPU memory is no longer available for preview and has been superceded by the updated ND40rs_v2.

Premium Storage: Supported

Premium Storage caching: Supported

InfiniBand: Supported

SIZE	VCPU	MEMORY : GIB	TEMP STORAGE (SSD): GIB	GPU	GPU MEMORY : GIB	MAX DATA DISKS	MAX UNCACHED DISK THROUHPUT: IOPS / MBPS	MAX NETWORK BANDWIDTH: DTH	MAX NICs
Standard_ND40rs_v2	40	672	2948	8 V100 32 GB (NVLink)	16	32	80000 / 800	24000 Mbps	8

Size table definitions

- Storage capacity is shown in units of GiB or 1024^3 bytes. When you compare disks measured in GB (1000^3 bytes) to disks measured in GiB (1024^3) remember that capacity numbers given in GiB may

appear smaller. For example, 1023 GiB = 1098.4 GB.

- Disk throughput is measured in input/output operations per second (IOPS) and MBps where MBps = 10^6 bytes/sec.
- Data disks can operate in cached or uncached modes. For cached data disk operation, the host cache mode is set to **ReadOnly** or **ReadWrite**. For uncached data disk operation, the host cache mode is set to **None**.
- If you want to get the best performance for your VMs, you should limit the number of data disks to two disks per vCPU.
- **Expected network bandwidth** is the maximum aggregated bandwidth allocated per VM type across all NICs, for all destinations. For more information, see [Virtual machine network bandwidth](#).

Upper limits aren't guaranteed. Limits offer guidance for selecting the right VM type for the intended application. Actual network performance will depend on several factors including network congestion, application loads, and network settings. For information on optimizing network throughput, see [Optimize network throughput for Azure virtual machines](#). To achieve the expected network performance on Linux or Windows, you may need to select a specific version or optimize your VM. For more information, see [Bandwidth/Throughput testing \(NTTCP\)](#).

Supported operating systems and drivers

To take advantage of the GPU capabilities of Azure N-series VMs, NVIDIA GPU drivers must be installed.

The [NVIDIA GPU Driver Extension](#) installs appropriate NVIDIA CUDA or GRID drivers on an N-series VM. Install or manage the extension using the Azure portal or tools such as Azure PowerShell or Azure Resource Manager templates. See the [NVIDIA GPU Driver Extension documentation](#) for supported operating systems and deployment steps. For general information about VM extensions, see [Azure virtual machine extensions and features](#).

If you choose to install NVIDIA GPU drivers manually, see [N-series GPU driver setup for Windows](#) or [N-series GPU driver setup for Linux](#) for supported operating systems, drivers, installation, and verification steps.

Other sizes

- [General purpose](#)
- [Memory optimized](#)
- [Storage optimized](#)
- [GPU optimized](#)
- [High performance compute](#)
- [Previous generations](#)

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

NV-series

2/28/2020 • 2 minutes to read • [Edit Online](#)

The NV-series virtual machines are powered by [NVIDIA Tesla M60](#) GPUs and NVIDIA GRID technology for desktop accelerated applications and virtual desktops where customers are able to visualize their data or simulations. Users are able to visualize their graphics intensive workflows on the NV instances to get superior graphics capability and additionally run single precision workloads such as encoding and rendering. NV-series VMs are also powered by Intel Xeon E5-2690 v3 (Haswell) CPUs.

Each GPU in NV instances comes with a GRID license. This license gives you the flexibility to use an NV instance as a virtual workstation for a single user, or 25 concurrent users can connect to the VM for a virtual application scenario.

Premium Storage: Not Supported

Premium Storage caching: Not Supported

SIZE	VCPU	MEMORY : GIB	TEMP STORAGE (SSD) GIB	GPU	GPU MEMORY : GIB	MAX DATA DISKS	MAX NICS	VIRTUAL WORKSTATIONS	VIRTUAL APPLICATIONS
Standar d_NV6	6	56	340	1	8	24	1	1	25
Standar d_NV12	12	112	680	2	16	48	2	2	50
Standar d_NV24	24	224	1440	4	32	64	4	4	100

1 GPU = one-half M60 card.

Size table definitions

- Storage capacity is shown in units of GiB or 1024^3 bytes. When you compare disks measured in GB (1000^3 bytes) to disks measured in GiB (1024^3) remember that capacity numbers given in GiB may appear smaller. For example, 1023 GiB = 1098.4 GB.
- Disk throughput is measured in input/output operations per second (IOPS) and MBps where MBps = 10^6 bytes/sec.
- Data disks can operate in cached or uncached modes. For cached data disk operation, the host cache mode is set to **ReadOnly** or **ReadWrite**. For uncached data disk operation, the host cache mode is set to **None**.
- If you want to get the best performance for your VMs, you should limit the number of data disks to two disks per vCPU.
- **Expected network bandwidth** is the maximum aggregated bandwidth allocated per VM type across all NICs, for all destinations. For more information, see [Virtual machine network bandwidth](#).

Upper limits aren't guaranteed. Limits offer guidance for selecting the right VM type for the intended application. Actual network performance will depend on several factors including network congestion, application loads, and network settings. For information on optimizing network throughput, see [Optimize](#)

network throughput for Azure virtual machines. To achieve the expected network performance on Linux or Windows, you may need to select a specific version or optimize your VM. For more information, see [Bandwidth/Throughput testing \(NTTCP\)](#).

Supported operating systems and drivers

To take advantage of the GPU capabilities of Azure N-series VMs, NVIDIA GPU drivers must be installed.

The [NVIDIA GPU Driver Extension](#) installs appropriate NVIDIA CUDA or GRID drivers on an N-series VM. Install or manage the extension using the Azure portal or tools such as Azure PowerShell or Azure Resource Manager templates. See the [NVIDIA GPU Driver Extension documentation](#) for supported operating systems and deployment steps. For general information about VM extensions, see [Azure virtual machine extensions and features](#).

If you choose to install NVIDIA GPU drivers manually, see [N-series GPU driver setup for Windows](#) or [N-series GPU driver setup for Linux](#) for supported operating systems, drivers, installation, and verification steps.

Other sizes

- [General purpose](#)
- [Memory optimized](#)
- [Storage optimized](#)
- [GPU optimized](#)
- [High performance compute](#)
- [Previous generations](#)

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

NVv3-series

2/28/2020 • 2 minutes to read • [Edit Online](#)

The NVv3-series virtual machines are powered by [NVIDIA Tesla M60](#) GPUs and NVIDIA GRID technology with Intel E5-2690 v4 (Broadwell) CPUs and Intel Hyper-Threading Technology. These virtual machines are targeted for GPU accelerated graphics applications and virtual desktops where customers want to visualize their data, simulate results to view, work on CAD, or render and stream content. Additionally, these virtual machines can run single precision workloads such as encoding and rendering. NVv3 virtual machines support Premium Storage and come with twice the system memory (RAM) when compared with its predecessor NV-series.

Each GPU in NVv3 instances comes with a GRID license. This license gives you the flexibility to use an NV instance as a virtual workstation for a single user, or 25 concurrent users can connect to the VM for a virtual application scenario.

Premium Storage caching: Supported

SIZE	VCPU	MEMORY: GiB	TEMP STORAGE (SSD) GiB	GPU	GPU MEMORY: GiB	MAX DATA DISKS	MAX UNCACHED DISK THROUGHPUT: IOPS/Mbps	MAX NICs	VIRTUAL WORKSTATIONS	VIRTUAL APPLICATIONS
Standard_NV1_2s_v3	12	112	320	1	8	12	20000/200	4	1	25
Standard_NV2_4s_v3	24	224	640	2	16	24	40000/400	8	2	50
Standard_NV4_8s_v3	48	448	1280	4	32	32	80000/800	8	4	100

1 GPU = one-half M60 card.

Size table definitions

- Storage capacity is shown in units of GiB or 1024^3 bytes. When you compare disks measured in GB (1000^3 bytes) to disks measured in GiB (1024^3) remember that capacity numbers given in GiB may appear smaller. For example, 1023 GiB = 1098.4 GB.
- Disk throughput is measured in input/output operations per second (IOPS) and MBps where MBps = 10^6 bytes/sec.
- Data disks can operate in cached or uncached modes. For cached data disk operation, the host cache mode is set to **ReadOnly** or **ReadWrite**. For uncached data disk operation, the host cache mode is set to **None**.
- If you want to get the best performance for your VMs, you should limit the number of data disks to two disks per vCPU.
- **Expected network bandwidth** is the maximum aggregated bandwidth allocated per VM type across all

NICs, for all destinations. For more information, see [Virtual machine network bandwidth](#).

Upper limits aren't guaranteed. Limits offer guidance for selecting the right VM type for the intended application. Actual network performance will depend on several factors including network congestion, application loads, and network settings. For information on optimizing network throughput, see [Optimize network throughput for Azure virtual machines](#). To achieve the expected network performance on Linux or Windows, you may need to select a specific version or optimize your VM. For more information, see [Bandwidth/Throughput testing \(NTTCP\)](#).

Supported operating systems and drivers

To take advantage of the GPU capabilities of Azure N-series VMs, NVIDIA GPU drivers must be installed.

The [NVIDIA GPU Driver Extension](#) installs appropriate NVIDIA CUDA or GRID drivers on an N-series VM. Install or manage the extension using the Azure portal or tools such as Azure PowerShell or Azure Resource Manager templates. See the [NVIDIA GPU Driver Extension documentation](#) for supported operating systems and deployment steps. For general information about VM extensions, see [Azure virtual machine extensions and features](#).

If you choose to install NVIDIA GPU drivers manually, see [N-series GPU driver setup for Windows](#) or [N-series GPU driver setup for Linux](#) for supported operating systems, drivers, installation, and verification steps.

Other sizes

- [General purpose](#)
- [Memory optimized](#)
- [Storage optimized](#)
- [GPU optimized](#)
- [High performance compute](#)
- [Previous generations](#)

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

Install NVIDIA GPU drivers on N-series VMs running Linux

11/13/2019 • 9 minutes to read • [Edit Online](#)

To take advantage of the GPU capabilities of Azure N-series VMs running Linux, NVIDIA GPU drivers must be installed. The [NVIDIA GPU Driver Extension](#) installs appropriate NVIDIA CUDA or GRID drivers on an N-series VM. Install or manage the extension using the Azure portal or tools such as the Azure CLI or Azure Resource Manager templates. See the [NVIDIA GPU Driver Extension documentation](#) for supported distributions and deployment steps.

If you choose to install GPU drivers manually, this article provides supported distributions, drivers, and installation and verification steps. Manual driver setup information is also available for [Windows VMs](#).

For N-series VM specs, storage capacities, and disk details, see [GPU Linux VM sizes](#).

Supported distributions and drivers

NVIDIA CUDA drivers

NVIDIA CUDA drivers for NC, NCv2, NCv3, ND, and NDv2-series VMs (optional for NV-series) are supported only on the Linux distributions listed in the following table. CUDA driver information is current at time of publication. For the latest CUDA drivers, visit the [NVIDIA](#) website. Ensure that you install or upgrade to the latest CUDA drivers for your distribution.

TIP

As an alternative to manual CUDA driver installation on a Linux VM, you can deploy an Azure [Data Science Virtual Machine](#) image. The DSVM editions for Ubuntu 16.04 LTS or CentOS 7.4 pre-install NVIDIA CUDA drivers, the CUDA Deep Neural Network Library, and other tools.

DISTRIBUTION	DRIVER
Ubuntu 16.04 LTS, 18.04 LTS	NVIDIA CUDA 10.1, driver branch R418
Red Hat Enterprise Linux 7.3, 7.4, 7.5, 7.6	
CentOS-based 7.3, 7.4, 7.5, 7.6, CentOS-based 7.4 HPC	

NVIDIA GRID drivers

Microsoft redistributes NVIDIA GRID driver installers for NV and NVv3-series VMs used as virtual workstations or for virtual applications. Install only these GRID drivers on Azure NV VMs, only on the operating systems listed in the following table. These drivers include licensing for GRID Virtual GPU Software in Azure. You do not need to set up an NVIDIA vGPU software license server.

DISTRIBUTION	DRIVER
Ubuntu 18.04 LTS	NVIDIA GRID 10.1, driver branch R440
Ubuntu 16.04 LTS	
Red Hat Enterprise Linux 7.0 to 7.6	
CentOS-based 7.0 to 7.6	
SUSE Linux Enterprise Server 12 SP2	

WARNING

Installation of third-party software on Red Hat products can affect the Red Hat support terms. See the [Red Hat Knowledgebase article](#).

Install CUDA drivers on N-series VMs

Here are steps to install CUDA drivers from the NVIDIA CUDA Toolkit on N-series VMs.

C and C++ developers can optionally install the full Toolkit to build GPU-accelerated applications. For more information, see the [CUDA Installation Guide](#).

To install CUDA drivers, make an SSH connection to each VM. To verify that the system has a CUDA-capable GPU, run the following command:

```
lspci | grep -i NVIDIA
```

You will see output similar to the following example (showing an NVIDIA Tesla K80 card):

```
af8a:00:00.0 3D controller: NVIDIA Corporation GK210GL [Tesla K80] (rev a1)
```

Then run installation commands specific for your distribution.

Ubuntu

1. Download and install the CUDA drivers from the NVIDIA website. For example, for Ubuntu 16.04 LTS:

```
CUDA_REPO_PKG=cuda-repo-ubuntu1604_10.0.130-1_amd64.deb

wget -O /tmp/${CUDA_REPO_PKG}
http://developer.download.nvidia.com/compute/cuda/repos/ubuntu1604/x86_64/${CUDA_REPO_PKG}

sudo dpkg -i /tmp/${CUDA_REPO_PKG}

sudo apt-key adv --fetch-keys
https://developer.download.nvidia.com/compute/cuda/repos/ubuntu1604/x86_64/7fa2af80.pub

rm -f /tmp/${CUDA_REPO_PKG}

sudo apt-get update

sudo apt-get install cuda-drivers
```

The installation can take several minutes.

2. To optionally install the complete CUDA toolkit, type:

```
sudo apt-get install cuda
```

3. Reboot the VM and proceed to verify the installation.

CUDA driver updates

We recommend that you periodically update CUDA drivers after deployment.

```
sudo apt-get update  
  
sudo apt-get upgrade -y  
  
sudo apt-get dist-upgrade -y  
  
sudo apt-get install cuda-drivers  
  
sudo reboot
```

CentOS or Red Hat Enterprise Linux

1. Update the kernel (recommended). If you choose not to update the kernel, ensure that the versions of `kernel-devel` and `dkms` are appropriate for your kernel.

```
sudo yum install kernel kernel-tools kernel-headers kernel-devel  
  
sudo reboot
```

2. Install the latest [Linux Integration Services for Hyper-V and Azure](#).

```
wget https://aka.ms/lis  
  
tar xvzf lis  
  
cd LISISO  
  
sudo ./install.sh  
  
sudo reboot
```

3. Reconnect to the VM and continue installation with the following commands:

```
sudo rpm -Uvh https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm  
  
sudo yum install dkms  
  
CUDA_REPO_PKG=cuda-repo-rhel7-10.0.130-1.x86_64.rpm  
  
wget http://developer.download.nvidia.com/compute/cuda/repos/rhel7/x86_64/${CUDA_REPO_PKG} -O /tmp/${CUDA_REPO_PKG}  
  
sudo rpm -ivh /tmp/${CUDA_REPO_PKG}  
  
rm -f /tmp/${CUDA_REPO_PKG}  
  
sudo yum install cuda-drivers
```

The installation can take several minutes.

4. To optionally install the complete CUDA toolkit, type:

```
sudo yum install cuda
```

5. Reboot the VM and proceed to verify the installation.

Verify driver installation

To query the GPU device state, SSH to the VM and run the [nvidia-smi](#) command-line utility installed with the driver.

If the driver is installed, you will see output similar to the following. Note that **GPU-Util** shows 0% unless you are currently running a GPU workload on the VM. Your driver version and GPU details may be different from the ones shown.

```
Tue Oct 10 20:48:53 2017
+-----+
| NVIDIA-SMI 384.81      Driver Version: 384.81 |
+-----+
| GPU  Name     Persistence-M | Bus-Id     Disp.A  | Volatile Uncorr. ECC |
| Fan  Temp     Perf  Pwr:Usage/Cap| Memory-Usage | GPU-Util  Compute M. |
|-----+-----+-----+-----+-----+-----+
| 0  Tesla K80        off    | 000007D1:00:00.0 off |          0%      Default |
| N/A   51C     P0    58W / 149W |           0MiB / 11439MiB |             |
+-----+-----+-----+-----+-----+-----+
+
| Processes:                               GPU Memory |
| GPU     PID  Type  Process name        Usage      |
|-----+-----+-----+-----|
| No running processes found            |
+-----+
```

RDMA network connectivity

RDMA network connectivity can be enabled on RDMA-capable N-series VMs such as NC24r deployed in the same availability set or in a single placement group in a VM scale set. The RDMA network supports Message Passing Interface (MPI) traffic for applications running with Intel MPI 5.x or a later version. Additional requirements follow:

Distributions

Deploy RDMA-capable N-series VMs from one of the images in the Azure Marketplace that supports RDMA connectivity on N-series VMs:

- **Ubuntu 16.04 LTS** - Configure RDMA drivers on the VM and register with Intel to download Intel MPI:

1. Install dapl, rdmacm, ibverbs, and mlx4

```
sudo apt-get update
sudo apt-get install libdapl12 libmlx4-1
```

2. In /etc/waagent.conf, enable RDMA by uncommenting the following configuration lines. You need root access to edit this file.

```
OS.EnableRDMA=y
OS.UpdateRdmaDriver=y
```

3. Add or change the following memory settings in KB in the /etc/security/limits.conf file. You need

root access to edit this file. For testing purposes you can set memlock to unlimited. For example:

```
<User or group name> hard memlock unlimited .
```

```
<User or group name> hard     memlock <memory required for your application in KB>
<User or group name> soft     memlock <memory required for your application in KB>
```

4. Install Intel MPI Library. Either [purchase and download](#) the library from Intel or download the [free evaluation version](#).

```
wget http://registrationcenter-download.intel.com/akdlm/irc_nas/tec/9278/l_mpi_p_5.1.3.223.tgz
```

Only Intel MPI 5.x runtimes are supported.

For installation steps, see the [Intel MPI Library Installation Guide](#).

5. Enable ptrace for non-root non-debugger processes (needed for the most recent versions of Intel MPI).

```
echo 0 | sudo tee /proc/sys/kernel/yama/ptrace_scope
```

- **CentOS-based 7.4 HPC** - RDMA drivers and Intel MPI 5.1 are installed on the VM.

Install GRID drivers on NV or NVv3-series VMs

To install NVIDIA GRID drivers on NV or NVv3-series VMs, make an SSH connection to each VM and follow the steps for your Linux distribution.

Ubuntu

1. Run the `lspci` command. Verify that the NVIDIA M60 card or cards are visible as PCI devices.
2. Install updates.

```
sudo apt-get update
sudo apt-get upgrade -y
sudo apt-get dist-upgrade -y
sudo apt-get install build-essential ubuntu-desktop -y
sudo apt-get install linux-azure -y
```

3. Disable the Nouveau kernel driver, which is incompatible with the NVIDIA driver. (Only use the NVIDIA driver on NV or NVv2 VMs.) To do this, create a file in `/etc/modprobe.d` named `nouveau.conf` with the following contents:

```
blacklist nouveau
blacklist lbm-nouveau
```

4. Reboot the VM and reconnect. Exit X server:

```
sudo systemctl stop lightdm.service
```

5. Download and install the GRID driver:

```
wget -O NVIDIA-Linux-x86_64-grid.run https://go.microsoft.com/fwlink/?LinkId=874272  
chmod +x NVIDIA-Linux-x86_64-grid.run  
sudo ./NVIDIA-Linux-x86_64-grid.run
```

6. When you're asked whether you want to run the nvidia-xconfig utility to update your X configuration file, select **Yes**.
7. After installation completes, copy /etc/nvidia/gridd.conf.template to a new file gridd.conf at location /etc/nvidia/

```
sudo cp /etc/nvidia/gridd.conf.template /etc/nvidia/gridd.conf
```

8. Add the following to `/etc/nvidia/gridd.conf`:

```
IgnoreSP=False  
EnableUI=False
```

9. Remove the following from `/etc/nvidia/gridd.conf` if it is present:

```
FeatureType=0
```

10. Reboot the VM and proceed to verify the installation.

CentOS or Red Hat Enterprise Linux

1. Update the kernel and DKMS (recommended). If you choose not to update the kernel, ensure that the versions of `kernel-devel` and `dkms` are appropriate for your kernel.

```
sudo yum update  
  
sudo yum install kernel-devel  
  
sudo rpm -Uvh https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm  
  
sudo yum install dkms  
  
sudo yum install hyperv-daemons
```

2. Disable the Nouveau kernel driver, which is incompatible with the NVIDIA driver. (Only use the NVIDIA driver on NV or NV2 VMs.) To do this, create a file in `/etc/modprobe.d` named `nouveau.conf` with the following contents:

```
blacklist nouveau  
  
blacklist lbm-nouveau
```

3. Reboot the VM, reconnect, and install the latest [Linux Integration Services for Hyper-V and Azure](#).

```
wget https://aka.ms/lis

tar xvzf lis

cd LISISO

sudo ./install.sh

sudo reboot
```

4. Reconnect to the VM and run the `lspci` command. Verify that the NVIDIA M60 card or cards are visible as PCI devices.
5. Download and install the GRID driver:

```
wget -O NVIDIA-Linux-x86_64-grid.run https://go.microsoft.com/fwlink/?LinkId=874272

chmod +x NVIDIA-Linux-x86_64-grid.run

sudo ./NVIDIA-Linux-x86_64-grid.run
```

6. When you're asked whether you want to run the nvidia-xconfig utility to update your X configuration file, select **Yes**.
7. After installation completes, copy `/etc/nvidia/gridd.conf.template` to a new file `gridd.conf` at location `/etc/nvidia/`

```
sudo cp /etc/nvidia/gridd.conf.template /etc/nvidia/gridd.conf
```

8. Add the following to `/etc/nvidia/gridd.conf`:

```
IgnoreSP=False
EnableUI=False
```

9. Remove the following from `/etc/nvidia/gridd.conf` if it is present:

```
FeatureType=0
```

10. Reboot the VM and proceed to verify the installation.

Verify driver installation

To query the GPU device state, SSH to the VM and run the `nvidia-smi` command-line utility installed with the driver.

If the driver is installed, you will see output similar to the following. Note that **GPU-Util** shows 0% unless you are currently running a GPU workload on the VM. Your driver version and GPU details may be different from the ones shown.

```
[azureuser@danlepnvr3 nvidia]$ nvidia-smi
Wed May 24 00:19:43 2017
+-----+
| NVIDIA-SMI 367.92                    Driver Version: 367.92 |
+-----+
| GPU  Name      Persistence-M | Bus-Id     Disp.A  | Volatile Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap | Memory-Usage | GPU-Util  Compute M. |
|-----+
| 0  Tesla M60        off      8342:00:00.0  off   |          0%          off |
| N/A   31C    P0    39W / 150W |     0MiB /  8123MiB |             0%          Default |
+-----+
+-----+
| Processes:                               GPU Memory |
| GPU     PID  Type  Process name        Usage      |
|-----+
| No running processes found            |
+-----+
```

X11 server

If you need an X11 server for remote connections to an NV or NVv2 VM, [x11vnc](#) is recommended because it allows hardware acceleration of graphics. The BusID of the M60 device must be manually added to the X11 configuration file (usually, `/etc/X11/xorg.conf`). Add a "Device" section similar to the following:

```
Section "Device"
    Identifier      "Device0"
    Driver          "nvidia"
    VendorName     "NVIDIA Corporation"
    BoardName       "Tesla M60"
    BusID          "PCI:0@your-BusID:0:0"
EndSection
```

Additionally, update your "Screen" section to use this device.

The decimal BusID can be found by running

```
nvidia-xconfig --query-gpu-info | awk '/PCI BusID/{print $4}'
```

The BusID can change when a VM gets reallocated or rebooted. Therefore, you may want to create a script to update the BusID in the X11 configuration when a VM is rebooted. For example, create a script named `busidupdate.sh` (or another name you choose) with contents similar to the following:

```
#!/bin/bash
XCONFIG="/etc/X11/xorg.conf"
OLDBUSID=`awk '/BusID/{gsub(/\//, "", $2); print $2}' ${XCONFIG}`
NEWBUSID=`nvidia-xconfig --query-gpu-info | awk '/PCI BusID/{print $4}`

if [[ "${OLDBUSID}" == "${NEWBUSID}" ]] ; then
    echo "NVIDIA BUSID not changed - nothing to do"
else
    echo "NVIDIA BUSID changed from \"${OLDBUSID}\" to \"${NEWBUSID}\": Updating ${XCONFIG}"
    sed -e 's|BusID.*|BusID      \'\"${NEWBUSID}\\"|' -i ${XCONFIG}
fi
```

Then, create an entry for your update script in `/etc/rc.d/rc3.d` so the script is invoked as root on boot.

Troubleshooting

- You can set persistence mode using `nvidia-smi` so the output of the command is faster when you need to query cards. To set persistence mode, execute `nvidia-smi -pm 1`. Note that if the VM is restarted, the mode setting goes away. You can always script the mode setting to execute upon startup.

- If you updated the NVIDIA CUDA drivers to the latest version and find RDMA connectivity is no longer working, [reinstall the RDMA drivers](#) to reestablish that connectivity.

Next steps

- To capture a Linux VM image with your installed NVIDIA drivers, see [How to generalize and capture a Linux virtual machine](#).

High performance compute VM sizes

2/27/2020 • 6 minutes to read • [Edit Online](#)

Azure H-series virtual machines (VMs) are designed to deliver leadership-class performance, MPI scalability, and cost efficiency for a variety of real-world HPC workloads.

HBv2-series VMs feature 200 Gb/sec Mellanox HDR InfiniBand, while both HB and HC-series VMs feature 100 Gb/sec Mellanox EDR InfiniBand. Each of these VM types are connected in a non-blocking fat tree for optimized and consistent RDMA performance. HBv2 VMs support Adaptive Routing and the Dynamic Connected Transport (DCT, in addition to standard RC and UD transports). These features enhance application performance, scalability, and consistency, and usage of them is strongly recommended.

HB-series VMs are optimized for applications driven by memory bandwidth, such as fluid dynamics, explicit finite element analysis, and weather modeling. HB VMs feature 60 AMD EPYC 7551 processor cores, 4 GB of RAM per CPU core, and no hyperthreading. The AMD EPYC platform provides more than 260 GB/sec of memory bandwidth.

HC-series VMs are optimized for applications driven by dense computation, such as implicit finite element analysis, molecular dynamics, and computational chemistry. HC VMs feature 44 Intel Xeon Platinum 8168 processor cores, 8 GB of RAM per CPU core, and no hyperthreading. The Intel Xeon Platinum platform supports Intel's rich ecosystem of software tools such as the Intel Math Kernel Library.

H-series VMs are optimized for applications driven by high CPU frequencies or large memory per core requirements. H-series VMs feature 8 or 16 Intel Xeon E5 2667 v3 processor cores, 7 or 14 GB of RAM per CPU core, and no hyperthreading. H-series features 56 Gb/sec Mellanox FDR InfiniBand in a non-blocking fat tree configuration for consistent RDMA performance. H-series VMs support Intel MPI 5.x and MS-MPI.

Deployment considerations

- **Azure subscription** – To deploy more than a few compute-intensive instances, consider a pay-as-you-go subscription or other purchase options. If you're using an [Azure free account](#), you can use only a limited number of Azure compute cores.
- **Pricing and availability** - These VM sizes are offered only in the Standard pricing tier. Check [Products available by region](#) for availability in Azure regions.
- **Cores quota** – You might need to increase the cores quota in your Azure subscription from the default value. Your subscription might also limit the number of cores you can deploy in certain VM size families, including the H-series. To request a quota increase, [open an online customer support request](#) at no charge. (Default limits may vary depending on your subscription category.)

NOTE

Contact Azure Support if you have large-scale capacity needs. Azure quotas are credit limits, not capacity guarantees. Regardless of your quota, you are only charged for cores that you use.

- **Virtual network** – An Azure [virtual network](#) is not required to use the compute-intensive instances. However, for many deployments you need at least a cloud-based Azure virtual network, or a site-to-site connection if you need to access on-premises resources. When needed, create a new virtual network to deploy the instances. Adding compute-intensive VMs to a virtual network in an affinity group is not supported.

- **Resizing** – Because of their specialized hardware, you can only resize compute-intensive instances within the same size family (H-series or compute-intensive A-series). For example, you can only resize an H-series VM from one H-series size to another. In addition, resizing from a non-compute-intensive size to a compute-intensive size is not supported.

RDMA-capable instances

A subset of the compute-intensive instances (A8, A9, H16r, H16mr, HB and HC) feature a network interface for remote direct memory access (RDMA) connectivity. Selected N-series sizes designated with 'r' such as the NC24rs configurations (NC24rs_v2 and NC24rs_v3) are also RDMA-capable. This interface is in addition to the standard Azure network interface available to other VM sizes.

This interface allows the RDMA-capable instances to communicate over an InfiniBand (IB) network, operating at EDR rates for HB, HC, FDR rates for H16r, H16mr, and RDMA-capable N-series virtual machines, and QDR rates for A8 and A9 virtual machines. These RDMA capabilities can boost the scalability and performance of certain Message Passing Interface (MPI) applications. For more information on speed, see the details in the tables on this page.

NOTE

In Azure, IP over IB is only supported on the SR-IOV enabled VMs (SR-IOV for InfiniBand, currently HB and HC). RDMA over IB is supported for all RDMA-capable instances.

- **Operating system** - Windows Server 2016 on all the above HPC series VMs. Windows Server 2012 R2, Windows Server 2012 are also supported on the non-SR-IOV enabled VMs (hence excluding HB and HC).
- **MPI** - The SR-IOV enabled VM sizes on Azure (HB, HC) allow almost any flavor of MPI to be used with Mellanox OFED. On non-SR-IOV enabled VMs, supported MPI implementations use the Microsoft Network Direct (ND) interface to communicate between instances. Hence, only Microsoft MPI (MS-MPI) 2012 R2 or later and Intel MPI 5.x versions are supported. Later versions (2017, 2018) of the Intel MPI runtime library may or may not be compatible with the Azure RDMA drivers.
- **InfiniBandDriverWindows VM extension** - On RDMA-capable VMs, add the InfiniBandDriverWindows extension to enable InfiniBand. This Windows VM extension installs Windows Network Direct drivers (on non-SR-IOV VMs) or Mellanox OFED drivers (on SR-IOV VMs) for RDMA connectivity. In certain deployments of A8 and A9 instances, the HpcVmDrivers extension is added automatically. Note that the HpcVmDrivers VM extension is being deprecated; it will not be updated. To add the VM extension to a VM, you can use [Azure PowerShell](#) cmdlets.

The following command installs the latest version 1.0 InfiniBandDriverWindows extension on an existing RDMA-capable VM named *myVM* deployed in the resource group named *myResourceGroup* in the *West US* region:

```
Set-AzVMExtension -ResourceGroupName "myResourceGroup" -Location "westus" -VMName "myVM" -ExtensionName "InfiniBandDriverWindows" -Publisher "Microsoft.HpcCompute" -Type "InfiniBandDriverWindows" -TypeHandlerVersion "1.0"
```

Alternatively, VM extensions can be included in Azure Resource Manager templates for easy deployment, with the following JSON element:

```
"properties":{  
    "publisher": "Microsoft.HpcCompute",  
    "type": "InfiniBandDriverWindows",  
    "typeHandlerVersion": "1.0",  
}
```

The following command installs the latest version 1.0 InfiniBandDriverWindows extension on all RDMA-capable VMs in an existing VM scale set named *myVMSS* deployed in the resource group named *myResourceGroup*:

```
$VMSS = Get-AzVmss -ResourceGroupName "myResourceGroup" -VMScaleSetName "myVMSS"  
Add-AzVmssExtension -VirtualMachineScaleSet $VMSS -Name "InfiniBandDriverWindows" -Publisher  
"Microsoft.HpcCompute" -Type "InfiniBandDriverWindows" -TypeHandlerVersion "1.0"  
Update-AzVmss -ResourceGroupName "myResourceGroup" -VMScaleSetName "MyVMSS" -  
VirtualMachineScaleSet $VMSS  
Update-AzVmssInstance -ResourceGroupName "myResourceGroup" -VMScaleSetName "myVMSS" -InstanceId  
"**"
```

For more information, see [Virtual machine extensions and features](#). You can also work with extensions for VMs deployed in the [classic deployment model](#).

- **RDMA network address space** - The RDMA network in Azure reserves the address space 172.16.0.0/16. To run MPI applications on instances deployed in an Azure virtual network, make sure that the virtual network address space does not overlap the RDMA network.

Cluster configuration options

Azure provides several options to create clusters of Windows HPC VMs that can communicate using the RDMA network, including:

- **Virtual machines** - Deploy the RDMA-capable HPC VMs in the same availability set (when you use the Azure Resource Manager deployment model). If you use the classic deployment model, deploy the VMs in the same cloud service.
- **Virtual machine scale sets** - In a virtual machine scale set, ensure that you limit the deployment to a single placement group. For example, in a Resource Manager template, set the `singlePlacementGroup` property to `true`.
- **MPI among virtual machines** - If MPI communication is required between virtual machines (VMs), ensure that the VMs are in the same availability set or the virtual machine same scale set.
- **Azure CycleCloud** - Create an HPC cluster in [Azure CycleCloud](#) to run MPI jobs on Windows nodes.
- **Azure Batch** - Create an [Azure Batch](#) pool to run MPI workloads on Windows Server compute nodes. For more information, see [Use RDMA-capable or GPU-enabled instances in Batch pools](#). Also see the [Batch Shipyard](#) project, for running container-based workloads on Batch.
- **Microsoft HPC Pack** - [HPC Pack](#) includes a runtime environment for MS-MPI that uses the Azure RDMA network when deployed on RDMA-capable Linux VMs. For example deployments, see [Set up a Linux RDMA cluster with HPC Pack to run MPI applications](#).

Other sizes

- [General purpose](#)
- [Compute optimized](#)

- [Memory optimized](#)
- [Storage optimized](#)
- [GPU optimized](#)
- [Previous generations](#)

Next steps

- For checklists to use the compute-intensive instances with HPC Pack on Windows Server, see [Set up a Linux RDMA cluster with HPC Pack to run MPI applications](#).
- To use compute-intensive instances when running MPI applications with Azure Batch, see [Use multi-instance tasks to run Message Passing Interface \(MPI\) applications in Azure Batch](#).
- Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

H-series

2/20/2020 • 2 minutes to read • [Edit Online](#)

H-series VMs are optimized for applications driven by high CPU frequencies or large memory per core requirements. H-series VMs feature 8 or 16 Intel Xeon E5 2667 v3 processor cores, up to 14 GB of RAM per CPU core, and no hyperthreading. H-series features 56 Gb/sec Mellanox FDR InfiniBand in a non-blocking fat tree configuration for consistent RDMA performance. H-series VMs support Intel MPI 5.x and MS-MPI.

ACU: 290-300

Premium Storage: Not Supported

Premium Storage Caching: Not Supported

SIZE	VCPU	PROC ESSO R	MEM ORY (GB)	MEM ORY BAND WIDT H GB/S	BASE CPU FREQ Y (GHZ)	ALL- CORE S FREQ UENC Y (GHZ, PEAK)	SINGL E- CORE FREQ UENC Y (GHZ, PEAK)	RDM A PERF ORM ANCE (GB/S)	MPI SUPP ORT	TEMP STOR AGE (GB)	MAX DATA DISKS	MAX ETHE RNET NICS
Stand ard_ H8	8	Intel Xeon E5 2667 v3	56	40	3.2	3.3	3.6	-	Intel 5.x, MS- MPI	1000	32	2
Stand ard_ H16	16	Intel Xeon E5 2667 v3	112	80	3.2	3.3	3.6	-	Intel 5.x, MS- MPI	2000	64	4
Stand ard_ H8m	8	Intel Xeon E5 2667 v3	112	40	3.2	3.3	3.6	-	Intel 5.x, MS- MPI	1000	32	2
Stand ard_ H16 m	16	Intel Xeon E5 2667 v3	224	80	3.2	3.3	3.6	-	Intel 5.x, MS- MPI	2000	64	4
Stand ard_ H16r 1	16	Intel Xeon E5 2667 v3	112	80	3.2	3.3	3.6	56	Intel 5.x, MS- MPI	2000	64	4

SIZE	VCPU	PROC ESSO R	MEM ORY (GB)	MEM BAND WIDT H GB/S	BASE CPU FREQ UENC Y (GHZ)	ALL-CORE S FREQ UENC Y (GHZ, PEAK)	SINGL E-CORE FREQ UENC Y (GHZ, PEAK)	RDMA PERFORM ANCE (GB/S)	MPI SUPP ORT	TEMP STOR AGE (GB)	MAX DATA DISKS	MAX ETHERNET NICs
Standard_H16_mr ¹	16	Intel Xeon E5 2667 v3	224	80	3.2	3.3	3.6	56	Intel 5.x, MS-MPI	2000	64	4

¹ For MPI applications, dedicated RDMA backend network is enabled by FDR InfiniBand network.

Size table definitions

- Storage capacity is shown in units of GiB or 1024^3 bytes. When you compare disks measured in GB (1000^3 bytes) to disks measured in GiB (1024^3) remember that capacity numbers given in GiB may appear smaller. For example, 1023 GiB = 1098.4 GB.
- Disk throughput is measured in input/output operations per second (IOPS) and MBps where MBps = 10^6 bytes/sec.
- Data disks can operate in cached or uncached modes. For cached data disk operation, the host cache mode is set to **ReadOnly** or **ReadWrite**. For uncached data disk operation, the host cache mode is set to **None**.
- If you want to get the best performance for your VMs, you should limit the number of data disks to two disks per vCPU.
- Expected network bandwidth** is the maximum aggregated bandwidth allocated per VM type across all NICs, for all destinations. For more information, see [Virtual machine network bandwidth](#).

Upper limits aren't guaranteed. Limits offer guidance for selecting the right VM type for the intended application. Actual network performance will depend on several factors including network congestion, application loads, and network settings. For information on optimizing network throughput, see [Optimize network throughput for Azure virtual machines](#). To achieve the expected network performance on Linux or Windows, you may need to select a specific version or optimize your VM. For more information, see [Bandwidth/Throughput testing \(NTTCP\)](#).

Other sizes

- [General purpose](#)
- [Memory optimized](#)
- [Storage optimized](#)
- [GPU optimized](#)
- [High performance compute](#)
- [Previous generations](#)

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

HB-series

2/20/2020 • 2 minutes to read • [Edit Online](#)

HB-series VMs are optimized for applications driven by memory bandwidth, such as fluid dynamics, explicit finite element analysis, and weather modeling. HB VMs feature 60 AMD EPYC 7551 processor cores, 4 GB of RAM per CPU core, and no simultaneous multithreading. An HB VM provides up to 260 GB/sec of memory bandwidth.

ACU: 199-216

Premium Storage: Supported

Premium Storage Caching: Supported

SIZE	VCPU	PROC ESSO R	MEM ORY (GB)	MEM BAND WIDT H GB/S	BASE FREQ UENC Y (GHZ)	ALL-CORE S FREQ UENC Y (GHZ, PEAK)	SINGL E-CORE FREQ UENC Y (GHZ, PEAK)	RDM A PERFORM ANCE (GB/S)	MPI SUPP ORT	TEMP STOR AGE (GB)	MAX DATA DISKS	MAX ETHERNET NICs
Standard_HB60rs	60	AMD EPYC 7551	240	263	2.0	2.55	2.55	100	All	700	4	1

Size table definitions

- Storage capacity is shown in units of GiB or 1024^3 bytes. When you compare disks measured in GB (1000^3 bytes) to disks measured in GiB (1024^3) remember that capacity numbers given in GiB may appear smaller. For example, 1023 GiB = 1098.4 GB.
- Disk throughput is measured in input/output operations per second (IOPS) and MBps where MBps = 10^6 bytes/sec.
- Data disks can operate in cached or uncached modes. For cached data disk operation, the host cache mode is set to **ReadOnly** or **ReadWrite**. For uncached data disk operation, the host cache mode is set to **None**.
- If you want to get the best performance for your VMs, you should limit the number of data disks to two disks per vCPU.
- Expected network bandwidth** is the maximum aggregated bandwidth allocated per VM type across all NICs, for all destinations. For more information, see [Virtual machine network bandwidth](#).

Upper limits aren't guaranteed. Limits offer guidance for selecting the right VM type for the intended application. Actual network performance will depend on several factors including network congestion, application loads, and network settings. For information on optimizing network throughput, see [Optimize network throughput for Azure virtual machines](#). To achieve the expected network performance on Linux or Windows, you may need to select a specific version or optimize your VM. For more information, see [Bandwidth/Throughput testing \(NTTTCP\)](#).

Other sizes

- [General purpose](#)

- [Memory optimized](#)
- [Storage optimized](#)
- [GPU optimized](#)
- [High performance compute](#)
- [Previous generations](#)

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

HBv2-series

2/20/2020 • 2 minutes to read • [Edit Online](#)

HBv2-series VMs are optimized for applications driven by memory bandwidth, such as fluid dynamics, finite element analysis, and reservoir simulation. HBv2 VMs feature 120 AMD EPYC 7742 processor cores, 4 GB of RAM per CPU core, and no simultaneous multithreading. Each HBv2 VM provides up to 340 GB/sec of memory bandwidth, and up to 4 teraFLOPS of FP64 compute.

Premium Storage: Supported

SIZE	vCPU	PROC ESSO R	MEM ORY (GB)	MEM BAND WIDTH GB/S	BASE CPU FREQ Y (GHZ)	ALL-CORE S FREQ UENC Y (GHZ, PEAK)	SINGL E-CORE FREQ UENC Y (GHZ, PEAK)	RDM A PERF ORM ANCE (GB/S)	MPI SUPP ORT	TEMP STOR AGE (GB)	MAX DATA DISKS	MAX ETHER NET NICs
Standard_HB12_0rs_v2	120	AMD EPYC 7V12	480	350	2.45	3.1	3.3	200	All	480 + 960	8	1

Size table definitions

- Storage capacity is shown in units of GiB or 1024^3 bytes. When you compare disks measured in GB (1000^3 bytes) to disks measured in GiB (1024^3) remember that capacity numbers given in GiB may appear smaller. For example, 1023 GiB = 1098.4 GB.
- Disk throughput is measured in input/output operations per second (IOPS) and MBps where MBps = 10^6 bytes/sec.
- Data disks can operate in cached or uncached modes. For cached data disk operation, the host cache mode is set to **ReadOnly** or **ReadWrite**. For uncached data disk operation, the host cache mode is set to **None**.
- If you want to get the best performance for your VMs, you should limit the number of data disks to two disks per vCPU.
- Expected network bandwidth** is the maximum aggregated bandwidth allocated per VM type across all NICs, for all destinations. For more information, see [Virtual machine network bandwidth](#).

Upper limits aren't guaranteed. Limits offer guidance for selecting the right VM type for the intended application. Actual network performance will depend on several factors including network congestion, application loads, and network settings. For information on optimizing network throughput, see [Optimize network throughput for Azure virtual machines](#). To achieve the expected network performance on Linux or Windows, you may need to select a specific version or optimize your VM. For more information, see [Bandwidth/Throughput testing \(NTTCP\)](#).

Other sizes

- [General purpose](#)
- [Memory optimized](#)

- Storage optimized
- GPU optimized
- High performance compute
- Previous generations

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

HC-series

2/20/2020 • 2 minutes to read • [Edit Online](#)

HC-series VMs are optimized for applications driven by dense computation, such as implicit finite element analysis, molecular dynamics, and computational chemistry. HC VMs feature 44 Intel Xeon Platinum 8168 processor cores, 8 GB of RAM per CPU core, and no hyperthreading. The Intel Xeon Platinum platform supports Intel's rich ecosystem of software tools such as the Intel Math Kernel Library.

ACU: 297-315

Premium Storage: Supported

Premium Storage Caching: Supported

SIZE	vCPU	PROC ESSO R	MEM ORY (GB)	MEM ORY BAND WIDT H GB/S	BASE CPU FREQ Y (GHZ)	ALL-CORE S FREQ Y (GHZ, PEAK)	SINGL E-CORE FREQ Y (GHZ, PEAK)	RDM A PERFOR MANCE (GB/S)	MPI SUPP ORT	TEMP STOR AGE (GB)	MAX DATA DISKS	MAX ETHERNET NICs
Standard_HC4_4rs	44	Intel Xeon Platinum 8168	352	191	2.7	3.4	3.7	100	All	700	4	1

Size table definitions

- Storage capacity is shown in units of GiB or 1024^3 bytes. When you compare disks measured in GB (1000^3 bytes) to disks measured in GiB (1024^3) remember that capacity numbers given in GiB may appear smaller. For example, 1023 GiB = 1098.4 GB.
- Disk throughput is measured in input/output operations per second (IOPS) and MBps where MBps = 10^6 bytes/sec.
- Data disks can operate in cached or uncached modes. For cached data disk operation, the host cache mode is set to **ReadOnly** or **ReadWrite**. For uncached data disk operation, the host cache mode is set to **None**.
- If you want to get the best performance for your VMs, you should limit the number of data disks to two disks per vCPU.
- Expected network bandwidth** is the maximum aggregated bandwidth allocated per VM type across all NICs, for all destinations. For more information, see [Virtual machine network bandwidth](#).

Upper limits aren't guaranteed. Limits offer guidance for selecting the right VM type for the intended application. Actual network performance will depend on several factors including network congestion, application loads, and network settings. For information on optimizing network throughput, see [Optimize network throughput for Azure virtual machines](#). To achieve the expected network performance on Linux or Windows, you may need to select a specific version or optimize your VM. For more information, see [Bandwidth/Throughput testing \(NTTCP\)](#).

Other sizes

- General purpose
- Memory optimized
- Storage optimized
- GPU optimized
- High performance compute
- Previous generations

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

Save costs with Azure Reserved VM Instances

11/13/2019 • 7 minutes to read • [Edit Online](#)

When you commit to an Azure reserved VM instance you can save money. The reservation discount is applied automatically to the number of running virtual machines that match the reservation scope and attributes. You don't need to assign a reservation to a virtual machine to get the discounts. A reserved instance purchase covers only the compute part of your VM usage. For Windows VMs, the usage meter is split into two separate meters. There's a compute meter, which is same as the Linux meter, and a Windows IP meter. The charges that you see when you make the purchase are only for the compute costs. Charges don't include Windows software costs. For more information about software costs, see [Software costs not included with Azure Reserved VM Instances](#).

Determine the right VM size before you buy

Before you buy a reservation, you should determine the size of the VM that you need. The following sections will help you determine the right VM size.

Use reservation recommendations

You can use reservation recommendations to help determine the reservations you should purchase.

- Purchase recommendations and recommended quantity are shown when you purchase a VM reserved instance in the Azure portal.
- Azure Advisor provides purchase recommendations for individual subscriptions.
- You can use the APIs to get purchase recommendations for both shared scope and single subscription scope. For more information, see [Reserved instance purchase recommendation APIs for enterprise customers](#).
- For Enterprise Agreement (EA) and Microsoft Customer Agreement (MCA) customers, purchase recommendations for shared and single subscription scopes are available with the [Azure Consumption Insights Power BI content pack](#).

Services that get VM reservation discounts

Your VM reservations can apply to VM usage emitted from multiple services - not just for your VM deployments. Resources that get reservation discounts change depending on the instance size flexibility setting.

Instance size flexibility setting

The instance size flexibility setting determines which services get the reserved instance discounts.

Whether the setting is on or off, reservation discounts automatically apply to any matching VM usage when the *ConsumedService* is `Microsoft.Compute`. So, check your usage data for the *ConsumedService* value. Some examples include:

- Virtual machines
- Virtual machine scale sets
- Container service
- Azure Batch deployments (in user subscriptions mode)
- Azure Kubernetes Service (AKS)
- Service Fabric

When the setting is on, reservation discounts automatically apply to matching VM usage when the *ConsumedService* is any of the following items:

- `Microsoft.Compute`
- `Microsoft.ClassicCompute`

- Microsoft.Batch
- Microsoft.MachineLearningServices
- Microsoft.Kusto

Check the *ConsumedService* value in your usage data to determine if the usage is eligible for reservation discounts.

For more information about instance size flexibility, see [Virtual machine size flexibility with Reserved VM Instances](#).

Analyze your usage information

Analyze your usage information to help determine which reservations you should purchase.

Usage data is available in the usage file and APIs. Use them together to determine which reservation to purchase. Check for VM instances that have high usage on daily basis to determine the quantity of reservations to purchase.

Avoid the `Meter` subcategory and `Product` fields in usage data. They don't distinguish between VM sizes that use premium storage. If you use these fields to determine the VM size for reservation purchase, you may buy the wrong size. Then you won't get the reservation discount you expect. Instead, refer to the `AdditionalInfo` field in your usage file or usage API to determine the correct VM size.

Purchase restriction considerations

Reserved VM Instances are available for most VM sizes with some exceptions. Reservation discounts don't apply for the following VMs:

- **VM series** - A-series, Av2-series, or G-series.
- **Preview or Promo VMs** - Any VM-series or size that is in preview or uses promotional meter.
- **Clouds** - Reservations aren't available for purchase in Germany or China regions.
- **Insufficient quota** - A reservation that is scoped to a single subscription must have vCPU quota available in the subscription for the new RI. For example, if the target subscription has a quota limit of 10 vCPUs for D-Series, then you can't buy a reservation for 11 Standard_D1 instances. The quota check for reservations includes the VMs already deployed in the subscription. For example, if the subscription has a quota of 10 vCPUs for D-Series and has two standard_D1 instances deployed, then you can buy a reservation for 10 standard_D1 instances in this subscription. You can [create quote increase request](#) to resolve this issue.
- **Capacity restrictions** - In rare circumstances, Azure limits the purchase of new reservations for subset of VM sizes, because of low capacity in a region.

Buy a Reserved VM Instance

You can buy a reserved VM instance in the [Azure portal](#). Pay for the reservation [up front or with monthly payments](#). These requirements apply to buying a reserved VM instance:

- You must be in an Owner role for at least one EA subscription or a subscription with a pay-as-you-go rate.
- For EA subscriptions, the **Add Reserved Instances** option must be enabled in the [EA portal](#). Or, if that setting is disabled, you must be an EA Admin for the subscription.
- For the Cloud Solution Provider (CSP) program, only the admin agents or sales agents can buy reservations.

To buy an instance:

1. Sign in to the [Azure portal](#).
2. Select **All services > Reservations**.
3. Select **Add** to purchase a new reservation and then click **Virtual machine**.
4. Enter required fields. Running VM instances that match the attributes you select qualify to get the reservation discount. The actual number of your VM instances that get the discount depend on the scope and quantity selected.

If you have an EA agreement, you can use the **Add more option** to quickly add additional instances. The option isn't available for other subscription types.

FIELD	DESCRIPTION
Subscription	The subscription used to pay for the reservation. The payment method on the subscription is charged the costs for the reservation. The subscription type must be an enterprise agreement (offer numbers: MS-AZR-0017P or MS-AZR-0148P) or Microsoft Customer Agreement or an individual subscription with pay-as-you-go rates (offer numbers: MS-AZR-0003P or MS-AZR-0023P). The charges are deducted from the monetary commitment balance, if available, or charged as overage. For a subscription with pay-as-you-go rates, the charges are billed to the credit card or invoice payment method on the subscription.
Scope	The reservation's scope can cover one subscription or multiple subscriptions (shared scope). If you select: <ul style="list-style-type: none"> • Single resource group scope — Applies the reservation discount to the matching resources in the selected resource group only. • Single subscription scope — Applies the reservation discount to the matching resources in the selected subscription. • Shared scope — Applies the reservation discount to matching resources in eligible subscriptions that are in the billing context. For EA customers, the billing context is the enrollment. For individual subscriptions with pay-as-you-go rates, the billing scope is all eligible subscriptions created by the account administrator.
Region	The Azure region that's covered by the reservation.
VM Size	The size of the VM instances.
Optimize for	VM instance size flexibility is selected by default. Click Advanced settings to change the instance size flexibility value to apply the reservation discount to other VMs in the same VM size group . Capacity priority prioritizes data center capacity for your deployments. It offers additional confidence in your ability to launch the VM instances when you need them. Capacity priority is only available when the reservation scope is single subscription.
Term	One year or three years.
Quantity	The number of instances being purchased within the reservation. The quantity is the number of running VM instances that can get the billing discount. For example, if you are running 10 Standard_D2 VMs in the East US, then you would specify quantity as 10 to maximize the benefit for all running VMs.

Usage data and reservation utilization

Your usage data has an effective price of zero for the usage that gets a reservation discount. You can see which VM

instance received the reservation discount for each reservation.

For more information about how reservation discounts appear in usage data, see [Understand Azure reservation usage for your Enterprise enrollment](#) if you are an EA customer. If you have an individual subscription, see [Understand Azure reservation usage for your Pay-As-You-Go subscription](#).

Change a reservation after purchase

You can make the following types of changes to a reservation after purchase:

- Update reservation scope
- Instance size flexibility (if applicable)
- Ownership

You can also split a reservation into smaller chunks and merge already split reservations. None of the changes cause a new commercial transaction or change the end date of the reservation.

You can't make the following types of changes after purchase, directly:

- An existing reservation's region
- SKU
- Quantity
- Duration

However, you can *exchange* a reservation if you want to make changes.

Cancel, exchange, or refund reservations

You can cancel, exchange, or refund reservations with certain limitations. For more information, see [Self-service exchanges and refunds for Azure Reservations](#).

Need help? Contact us.

If you have questions or need help, [create a support request](#).

Next steps

- To learn how to manage a reservation, see [Manage Azure Reservations](#).
- To learn more about Azure Reservations, see the following articles:
 - [What are Azure Reservations?](#)
 - [Manage Reservations in Azure](#)
 - [Understand how the reservation discount is applied](#)
 - [Understand reservation usage for a subscription with pay-as-you-go rates](#)
 - [Understand reservation usage for your Enterprise enrollment](#)
 - [Windows software costs not included with reservations](#)
 - [Azure Reservations in Partner Center Cloud Solution Provider \(CSP\) program](#)

2 minutes to read

Virtual machine size flexibility with Reserved VM Instances

11/13/2019 • 2 minutes to read • [Edit Online](#)

When you buy a Reserved VM Instance, you can choose to optimize for instance size flexibility or capacity priority. For more information about setting or changing the optimize setting for reserved VM instances, see [Change the optimize setting for reserved VM instances](#).

With a reserved virtual machine instance that's optimized for instance size flexibility, the reservation you buy can apply to the virtual machines (VMs) sizes in the same instance size flexibility group. For example, if you buy a reservation for a VM size that's listed in the DSv2 Series, like Standard_DS5_v2, the reservation discount can apply to the other four sizes that are listed in that same instance size flexibility group:

- Standard_DS1_v2
- Standard_DS2_v2
- Standard_DS3_v2
- Standard_DS4_v2

But that reservation discount doesn't apply to VMs sizes that are listed in different instance size flexibility groups, like SKUs in DSv2 Series High Memory: Standard_DS11_v2, Standard_DS12_v2, and so on.

Within the instance size flexibility group, the number of VMs the reservation discount applies to depends on the VM size you pick when you buy a reservation. It also depends on the sizes of the VMs that you have running. The ratio column compares the relative footprint for each VM size in that instance size flexibility group. Use the ratio value to calculate how the reservation discount applies to the VMs you have running.

Examples

The following examples use the sizes and ratios in the DSv2-series table.

You buy a reserved VM instance with the size Standard_DS4_v2 where the ratio or relative footprint compared to the other sizes in that series is 8.

- Scenario 1: Run eight Standard_DS1_v2 sized VMs with a ratio of 1. Your reservation discount applies to all eight of those VMs.
- Scenario 2: Run two Standard_DS2_v2 sized VMs with a ratio of 2 each. Also run a Standard_DS3_v2 sized VM with a ratio of 4. The total footprint is $2+2+4=8$. So your reservation discount applies to all three of those VMs.
- Scenario 3: Run one Standard_DS5_v2 with a ratio of 16. Your reservation discount applies to half that VM's compute cost.

The following sections show what sizes are in the same size series group when you buy a reserved VM instance optimized for instance size flexibility.

Instance size flexibility ratio for VMs

CSV below has the instance size flexibility groups, ArmSkuName and the ratios.

Instance size flexibility ratios

We will keep the file URL and the schema fixed so you can consume this file programmatically. The data will also be available through API soon.

Preview: Use Spot VMs in Azure

12/3/2019 • 4 minutes to read • [Edit Online](#)

Using Spot VMs 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 Spot VMs. Therefore, Spot VMs are great for workloads that can handle interruptions like batch processing jobs, dev/test environments, large compute workloads, and more.

The amount of available capacity can vary based on size, region, time of day, and more. When deploying Spot VMs, Azure will allocate the VMs if there is capacity available, but there is no SLA for these VMs. A Spot VM offers no high availability guarantees. At any point in time when Azure needs the capacity back, the Azure infrastructure will evict Spot VMs with 30 seconds notice.

IMPORTANT

Spot instances are currently in public preview. This preview version is not recommended for production workloads. Certain features might not be supported or might have constrained capabilities. For more information, see [Supplemental Terms of Use for Microsoft Azure Previews](#).

Eviction policy

VMs can be evicted based on capacity or the max price you set. For virtual machines, the eviction policy is set to *Deallocate* which moves your evicted VMs to the stopped-deallocated state, allowing you to redeploy the evicted VMs at a later time. However, reallocating Spot VMs will be dependent on there being available Spot capacity. The deallocated VMs will count against your spot vCPU quota and you will be charged for your underlying disks.

Users can opt-in to receive in-VM notifications through [Azure Scheduled Events](#). This will notify you if your VMs are being evicted and you will have 30 seconds to finish any jobs and perform shutdown tasks prior to the eviction.

OPTION	OUTCOME
Max price is set to \geq the current price.	VM is deployed if capacity and quota are available.
Max price is set to $<$ the current price.	The VM is not deployed. You will get an error message that the max price needs to be \geq current price.
Restarting a stop/deallocate VM if the max price is \geq the current price	If there is capacity and quota, then the VM is deployed.
Restarting a stop/deallocate VM if the max price is $<$ the current price	You will get an error message that the max price needs to be \geq current price.
Price for the VM has gone up and is now $>$ the max price.	The VM gets evicted. You get a 30s notification before actual eviction.
After eviction the price for the VM goes back to being $<$ the max price.	The VM will not be automatically re-started. You can restart the VM yourself, and it will be charged at the current price.

OPTION	OUTCOME
If the max price is set to <input type="text" value="-1"/>	The VM will not be evicted for pricing reasons. The max price will be the current price, up to the price for standard VMs. You will never be charged above the standard price.
Changing the max price	You need to deallocate the VM to change the max price. Deallocate the VM, set it a new max price, then update the VM.

Limitations

The following VM sizes are not supported for Spot VMs:

- B-series
- Promo versions of any size (like Dv2, NV, NC, H promo sizes)

Spot VMs can't currently use ephemeral OS disks.

Spot VMs can be deployed to any region, except Microsoft Azure China 21Vianet.

Pricing

Pricing for Spot VMs is variable, based on region and SKU. For more information, see VM pricing for [Linux](#) and [Windows](#).

With variable pricing, you have option to set a max price, in US dollars (USD), using up to 5 decimal places. For example, the value would be a max price of \$0.98765 USD per hour. If you set the max price to be , the VM won't be evicted based on price. The price for the VM will be the current price for spot or the price for a standard VM, whichever is less, as long as there is capacity and quota available.

Frequently asked questions

Q: Once created, is a Spot VM the same as regular standard VM?

A: Yes, except there is no SLA for Spot VMs and they can be evicted at any time.

Q: What to do when you get evicted, but still need capacity?

A: We recommend you use standard VMs instead of Spot VMs if you need capacity right away.

Q: How is quota managed for Spot VMs?

A: Spot VMs will have a separate quota pool. Spot quota will be shared between VMs and scale-set instances. For more information, see [Azure subscription and service limits, quotas, and constraints](#).

Q: Can I request for additional quota for Spot?

A: Yes, you will be able to submit the request to increase your quota for Spot VMs through the [standard quota request process](#).

Q: What channels support Spot VMs?

A: See the table below for Spot VM availability.

AZURE CHANNELS	AZURE SPOT VMs AVAILABILITY
Enterprise Agreement	Yes

AZURE CHANNELS	AZURE SPOT VMs AVAILABILITY
Pay As You Go	Yes
Cloud Service Provider (CSP)	Contact your partner
Benefits	Not available
Sponsored	Not available
Free Trial	Not available

Q: Where can I post questions?

A: You can post and tag your question with `azure-spot` at [Q&A](#).

Next steps

Use the [CLI](#), [portal](#) or [PowerShell](#) to deploy Spot VMs.

You can also deploy a [scale set with Spot VM instances](#).

Previous generations of virtual machine sizes

2/28/2020 • 11 minutes to read • [Edit Online](#)

This section provides information on previous generations of virtual machine sizes. These sizes can still be used, but there are newer generations available.

F-series

F-series is based on the 2.4 GHz Intel Xeon® E5-2673 v3 (Haswell) processor, which can achieve clock speeds as high as 3.1 GHz with the Intel Turbo Boost Technology 2.0. This is the same CPU performance as the Dv2-series of VMs.

F-series VMs are an excellent choice for workloads that demand faster CPUs but do not need as much memory or temporary storage per vCPU. Workloads such as analytics, gaming servers, web servers, and batch processing will benefit from the value of the F-series.

ACU: 210 - 250

Premium Storage: Not Supported

Premium Storage caching: Not Supported

SIZE	VCPUs	MEMORY: GIB	TEMP STORAGE (SSD) GIB	MAX TEMP STORAGE THROUGHPUT: IOPS/READ MBPS/WRITE MBPS	MAX DATA DISKS/THROUGHPUT: IOPS	MAX NICs/EXPECTED NETWORK BANDWIDTH (MBPS)
Standard_F1	1	2	16	3000/46/23	4/4x500	2/750
Standard_F2	2	4	32	6000/93/46	8/8x500	2/1500
Standard_F4	4	8	64	12000/187/93	16/16x500	4/3000
Standard_F8	8	16	128	24000/375/187	32/32x500	8/6000
Standard_F16	16	32	256	48000/750/375	64/64x500	8/12000

Fs-series ¹

The Fs-series provides all the advantages of the F-series, in addition to Premium storage.

ACU: 210 - 250

Premium Storage: Supported

Premium Storage caching: Supported

SIZE	VCPU	MEMORY: GIB	TEMP STORAGE (SSD) GIB	MAX DATA DISKS	MAX CACHED AND TEMP STORAGE THROUGHPUT: IOPS/MBPS (CACHE SIZE IN GIB)	MAX UNCACHED DISK THROUGHPUT: IOPS/MBPS	MAX NICS/EXPECTED NETWORK BANDWIDTH (MBPS)
Standard_F1s	1	2	4	4	4000/32 (12)	3200/48	2/750
Standard_F2s	2	4	8	8	8000/64 (24)	6400/96	2/1500
Standard_F4s	4	8	16	16	16000/128 (48)	12800/192	4/3000
Standard_F8s	8	16	32	32	32000/256 (96)	25600/384	8/6000
Standard_F16s	16	32	64	64	64000/512 (192)	51200/768	8/12000

MBps = 10^6 bytes per second, and GiB = 1024^3 bytes.

¹ The maximum disk throughput (IOPS or MBps) possible with a Fs series VM may be limited by the number, size, and striping of the attached disk(s). For details, see designing for high performance for [Windows](#) or [Linux](#).

NVv2-series

Newer size recommendation: [NVv3-series](#)

The NVv2-series virtual machines are powered by [NVIDIA Tesla M60](#) GPUs and NVIDIA GRID technology with Intel Broadwell CPUs. These virtual machines are targeted for GPU accelerated graphics applications and virtual desktops where customers want to visualize their data, simulate results to view, work on CAD, or render and stream content. Additionally, these virtual machines can run single precision workloads such as encoding and rendering. NVv2 virtual machines support Premium Storage and come with twice the system memory (RAM) when compared with its predecessor NV-series.

Each GPU in NVv2 instances comes with a GRID license. This license gives you the flexibility to use an NV instance as a virtual workstation for a single user, or 25 concurrent users can connect to the VM for a virtual application scenario.

SIZE	VCPU	MEMORY: GIB	TEMP STORAGE (SSD) GIB	GPU	GPU MEMORY: GIB	MAX DATA DISKS	MAX NICS	VIRTUAL WORKSTATIONS	VIRTUAL APPLICATIONS
Standard_NV6s_v2	6	112	320	1	8	12	4	1	25
Standard_NV12s_v2	12	224	640	2	16	24	8	2	50

SIZE	VCPU	MEMORY: GiB	TEMP STORAGE (SSD) GiB	GPU	GPU MEMORY: GiB	MAX DATA DISKS	MAX NICs	VIRTUAL WORKSTATIONS	VIRTUAL APPLICATIONS
Standard_NV2_4s_v2	24	448	1280	4	32	32	8	4	100

Size table definitions

- Storage capacity is shown in units of GiB or 1024^3 bytes. When you compare disks measured in GB (1000^3 bytes) to disks measured in GiB (1024^3) remember that capacity numbers given in GiB may appear smaller. For example, 1023 GiB = 1098.4 GB.
- Disk throughput is measured in input/output operations per second (IOPS) and MBps where MBps = 10^6 bytes/sec.
- Data disks can operate in cached or uncached modes. For cached data disk operation, the host cache mode is set to **ReadOnly** or **ReadWrite**. For uncached data disk operation, the host cache mode is set to **None**.
- If you want to get the best performance for your VMs, you should limit the number of data disks to two disks per vCPU.
- Expected network bandwidth** is the maximum aggregated bandwidth allocated per VM type across all NICs, for all destinations. For more information, see [Virtual machine network bandwidth](#).

Upper limits aren't guaranteed. Limits offer guidance for selecting the right VM type for the intended application. Actual network performance will depend on several factors including network congestion, application loads, and network settings. For information on optimizing network throughput, see [Optimize network throughput for Azure virtual machines](#). To achieve the expected network performance on Linux or Windows, you may need to select a specific version or optimize your VM. For more information, see [Bandwidth/Throughput testing \(NTTCP\)](#).

Older generations of virtual machine sizes

This section provides information on older generations of virtual machine sizes. These sizes are still supported but will not receive additional capacity. There are newer or alternative sizes that are generally available. Please refer to [Sizes for Linux virtual machines in Azure](#) to choose the VM sizes that will best fit your need.

For more information on resizing a Windows VM, see [Resize a Linux VM](#).

Basic A

Newer size recommendation: [Av2-series](#)

Premium Storage: Not Supported

Premium Storage caching: Not Supported

The basic tier sizes are primarily for development workloads and other applications that don't require load balancing, auto-scaling, or memory-intensive virtual machines.

SIZE – SIZE\NAME	VCPUs	MEMORY	NICs (MAX)	MAX TEMPORARY DISK SIZE	MAX. DATA DISKS (1023 GB EACH)	MAX. IOPS (300 PER DISK)
A0\Basic_A0	1	768 MB	2	20 GB	1	1x300
A1\Basic_A1	1	1.75 GB	2	40 GB	2	2x300
A2\Basic_A2	2	3.5 GB	2	60 GB	4	4x300
A3\Basic_A3	4	7 GB	2	120 GB	8	8x300
A4\Basic_A4	8	14 GB	2	240 GB	16	16x300

Standard A0 - A4 using CLI and PowerShell

In the classic deployment model, some VM size names are slightly different in CLI and PowerShell:

- Standard_A0 is ExtraSmall
- Standard_A1 is Small
- Standard_A2 is Medium
- Standard_A3 is Large
- Standard_A4 is ExtraLarge

A-series

Newer size recommendation: [Av2-series](#)

ACU: 50-100

Premium Storage: Not Supported

Premium Storage caching: Not Supported

SIZE	VCPUs	MEMORY: GIB	TEMP STORAGE (HDD): GIB	MAX DATA DISKS	MAX DATA DISK THROUGHPUT: IOPS	MAX NICs/EXPECTED NETWORK BANDWIDTH (MBPS)
Standard_A0_1	1	0.768	20	1	1x500	2/100
Standard_A1	1	1.75	70	2	2x500	2/500
Standard_A2	2	3.5	135	4	4x500	2/500
Standard_A3	4	7	285	8	8x500	2/1000
Standard_A4	8	14	605	16	16x500	4/2000
Standard_A5	2	14	135	4	4x500	2/500
Standard_A6	4	28	285	8	8x500	2/1000
Standard_A7	8	56	605	16	16x500	4/2000

¹ The A0 size is over-subscribed on the physical hardware. For this specific size only, other customer deployments may impact the performance of your running workload. The relative performance is outlined below as the expected baseline, subject to an approximate variability of 15 percent.

A-series - compute-intensive instances

Newer size recommendation: [Av2-series](#)

ACU: 225

Premium Storage: Not Supported

Premium Storage caching: Not Supported

The A8-A11 and H-series sizes are also known as *compute-intensive instances*. The hardware that runs these sizes is designed and optimized for compute-intensive and network-intensive applications, including high-performance computing (HPC) cluster applications, modeling, and simulations. The A8-A11 series uses Intel Xeon E5-2670 @ 2.6 GHZ and the H-series uses Intel Xeon E5-2667 v3 @ 3.2 GHz.

SIZE	VCPU	MEMORY: GIB	TEMP STORAGE (HDD): GIB	MAX DATA DISKS	MAX DATA DISK THROUGHPUT: IOPS	MAX NICs
Standard_A8 ¹	8	56	382	32	32x500	2
Standard_A9 ¹	16	112	382	64	64x500	4
Standard_A10	8	56	382	32	32x500	2
Standard_A11	16	112	382	64	64x500	4

¹For MPI applications, dedicated RDMA backend network is enabled by FDR InfiniBand network, which delivers ultra-low-latency and high bandwidth.

D-series

Newer size recommendation: [Dv3-series](#)

ACU: 160-250¹

Premium Storage: Not Supported

Premium Storage caching: Not Supported

SIZE	VCPU	MEMORY: GIB	TEMP STORAGE (SSD): GIB	MAX TEMP STORAGE THROUGHPUT: IOPS/READ MBPS/WRITE MBPS	MAX DATA DISKS/THROUGHPUT: IOPS	MAX NICS/EXPECTED NETWORK BANDWIDTH (MBPS)
Standard_D1	1	3.5	50	3000/46/23	4/4x500	2/500

SIZE	VCPU	MEMORY: GIB	TEMP STORAGE (SSD) GIB	MAX TEMP STORAGE THROUGHPUT: IOPS/READ MBPS/WRITE MBPS	MAX DATA DISKS/THROUGHPUT: IOPS	MAX NICs/EXPECTED NETWORK BANDWIDTH (MBPS)
Standard_D2	2	7	100	6000/93/46	8/8x500	2/1000
Standard_D3	4	14	200	12000/187/93	16/16x500	4/2000
Standard_D4	8	28	400	24000/375/187	32/32x500	8/4000

¹ VM Family can run on one of the following CPU's: 2.2 GHz Intel Xeon® E5-2660 v2, 2.4 GHz Intel Xeon® E5-2673 v3 (Haswell) or 2.3 GHz Intel XEON® E5-2673 v4 (Broadwell)

D-series - memory optimized

Newer size recommendation: [Dv3-series](#)

ACU: 160-250 ¹

Premium Storage: Not Supported

Premium Storage caching: Not Supported

SIZE	VCPU	MEMORY: GIB	TEMP STORAGE (SSD) GIB	MAX TEMP STORAGE THROUGHPUT: IOPS/READ MBPS/WRITE MBPS	MAX DATA DISKS/THROUGHPUT: IOPS	MAX NICs/EXPECTED NETWORK BANDWIDTH (MBPS)
Standard_D1 1	2	14	100	6000/93/46	8/8x500	2/1000
Standard_D1 2	4	28	200	12000/187/93	16/16x500	4/2000
Standard_D1 3	8	56	400	24000/375/187	32/32x500	8/4000
Standard_D1 4	16	112	800	48000/750/375	64/64x500	8/8000

¹ VM Family can run on one of the following CPU's: 2.2 GHz Intel Xeon® E5-2660 v2, 2.4 GHz Intel Xeon® E5-2673 v3 (Haswell) or 2.3 GHz Intel XEON® E5-2673 v4 (Broadwell)

Preview: DC-series

Premium Storage: Supported

Premium Storage caching: Supported

The DC-series uses the latest generation of 3.7GHz Intel XEON E-2176G Processor with SGX technology,

and with the Intel Turbo Boost Technology can go up to 4.7GHz.

SIZE	VCPU	MEMORY: GIB	TEMP STORAGE (SSD) GIB	MAX DATA DISKS	MAX CACHED AND TEMP STORAGE THROUGHPUT: IOPS / MBPS (CACHE SIZE IN GIB)	MAX UNCACHED DISK THROUGHPUT: IOPS / MBPS	MAX NICs / EXPECTED NETWORK BANDWIDTH (MBPS)
Standard_DC2s	2	8	100	2	4000 / 32 (43)	3200 /48	2 / 1500
Standard_DC4s	4	16	200	4	8000 / 64 (86)	6400 /96	2 / 3000

IMPORTANT

DC-series VMs are [generation 2 VMs](#) and only support [Gen2](#) images.

DS-series

Newer size recommendation: [Dsv3-series](#)

ACU: 160-250 ¹

Premium Storage: Supported

Premium Storage caching: Supported

SIZE	VCPU	MEMORY: GIB	TEMP STORAGE (SSD) GIB	MAX DATA DISKS	MAX CACHED AND TEMP STORAGE THROUGHPUT: IOPS/MBPS (CACHE SIZE IN GIB)	MAX UNCACHED DISK THROUGHPUT: IOPS/MBPS	MAX NICs/EXPECTED NETWORK BANDWIDTH (MBPS)
Standard_DS1	1	3.5	7	4	4000/32 (43)	3200/32	2/500
Standard_DS2	2	7	14	8	8000/64 (86)	6400/64	2/1000
Standard_DS3	4	14	28	16	16000/128 (172)	12800/128	4/2000
Standard_DS4	8	28	56	32	32000/256 (344)	25600/256	8/4000

¹ VM Family can run on one of the following CPU's: 2.2 GHz Intel Xeon® E5-2660 v2, 2.4 GHz Intel Xeon® E5-2673 v3 (Haswell) or 2.3 GHz Intel XEON® E5-2673 v4 (Broadwell)

DS-series - memory optimized

Newer size recommendation: [Dsv3-series](#)

ACU: 160-250^{1,2}

Premium Storage: Supported

Premium Storage caching: Supported

SIZE	VCPUs	MEMORY: GIB	TEMP STORAGE (SSD) GIB	MAX DATA DISKS	MAX CACHED AND TEMP STORAGE THROUGHPUT: IOPS/MBPS (CACHE SIZE IN GIB)	MAX UNCACHED DISK THROUGHPUT: IOPS/MBPS	MAX NICs/EXPEC TED NETWORK BANDWIDTH (MBPS)
Standard_DS11	2	14	28	8	8000/64 (72)	6400/64	2/1000
Standard_DS12	4	28	56	16	16000/128 (144)	12800/128	4/2000
Standard_DS13	8	56	112	32	32000/256 (288)	25600/256	8/4000
Standard_DS14	16	112	224	64	64000/512 (576)	51200/512	8/8000

¹ The maximum disk throughput (IOPS or MBps) possible with a DS series VM may be limited by the number, size and striping of the attached disk(s). For details, see designing for high performance for [Windows](#) or [Linux](#).² VM Family can run on one of the following CPU's: 2.2 GHz Intel Xeon® E5-2660 v2, 2.4 GHz Intel Xeon® E5-2673 v3 (Haswell) or 2.3 GHz Intel XEON® E5-2673 v4 (Broadwell)

Ls-series

The Ls-series offers up to 32 vCPUs, using the [Intel® Xeon® processor E5 v3 family](#). The Ls-series gets the same CPU performance as the G/GS-Series and comes with 8 GiB of memory per vCPU.

The Ls-series does not support the creation of a local cache to increase the IOPS achievable by durable data disks. The high throughput and IOPS of the local disk makes Ls-series VMs ideal for NoSQL stores such as Apache Cassandra and MongoDB which replicate data across multiple VMs to achieve persistence in the event of the failure of a single VM.

ACU: 180-240

Premium Storage: Supported

Premium Storage caching: Not Supported

SIZE	VCPUs	MEMORY (GIB)	TEMP STORAGE (GIB)	MAX DATA DISKS	MAX TEMP STORAGE THROUGHPUT (IOPS/MBPS)	MAX UNCACHED DISK THROUGHPUT (IOPS/MBPS)	MAX NICs/EXPEC TED NETWORK BANDWIDTH (MBPS)
Standard_L4s	4	32	678	16	20000/200	5000/125	2/4000

SIZE	VCPUs	MEMORY (GiB)	TEMP STORAGE (GiB)	MAX DATA DISKS	MAX TEMP STORAGE THROUHPUT (IOPS/MBPS)	MAX UNCACHED DISK THROUHPUT (IOPS/MBPS)	MAX NICS/EXPEC TED NETWORK BANDWIDTH (Mbps)
Standard_L8s	8	64	1388	32	40000/400	10000/250	4/8000
Standard_L16s	16	128	2807	64	80000/800	20000/500	8/16000
Standard_L32s ¹	32	256	5630	64	160000/1600	40000/1000	8/20000

The maximum disk throughput possible with Ls-series VMs may be limited by the number, size, and striping of any attached disks. For details, see designing for high performance for [Windows](#) or [Linux](#).

¹ Instance is isolated to hardware dedicated to a single customer.

GS-series

ACU: 180 - 240¹

Premium Storage: Supported

Premium Storage caching: Supported

SIZE	VCPUs	MEMORY: GiB	TEMP STORAGE (SSD) GiB	MAX DATA DISKS	MAX CACHED AND TEMP STORAGE THROUHPUT: IOPS / MBPS (CACHE SIZE IN GiB)	MAX UNCACHED DISK THROUHPUT: IOPS/MBPS	MAX NICS/EXPEC TED NETWORK BANDWIDTH (Mbps)
Standard_GS1	2	28	56	8	10000/100 (264)	5000/ 125	2/2000
Standard_GS2	4	56	112	16	20000/200 (528)	10000/ 250	2/4000
Standard_GS3	8	112	224	32	40000/400 (1056)	20000/ 500	4/8000
Standard_GS4 ³	16	224	448	64	80000/800 (2112)	40000/1000	8/16000
Standard_GS5 ^{2, 3}	32	448	896	64	160000/1600 (4224)	80000/2000	8/20000

¹ The maximum disk throughput (IOPS or MBps) possible with a GS series VM may be limited by the number, size and striping of the attached disk(s). For details, see designing for high performance for [Windows](#) or [Linux](#).

² Instance is isolated to hardware dedicated to a single customer.

³ Constrained core sizes available.

G-series

ACU: 180 - 240

Premium Storage: Not Supported

Premium Storage caching: Not Supported

SIZE	VCPU	MEMORY: GIB	TEMP STORAGE (SSD) GIB	MAX TEMP STORAGE THROUGHPUT: IOPS/READ MBPS/WRITE MBPS	MAX DATA DISKS/THROUGHPUT: IOPS	MAX NICS/EXPECTED NETWORK BANDWIDTH (MBPS)
Standard_G1	2	28	384	6000/93/46	8/8x500	2/2000
Standard_G2	4	56	768	12000/187/93	16/16x500	2/4000
Standard_G3	8	112	1536	24000/375/187	32/32x500	4/8000
Standard_G4	16	224	3072	48000/750/375	64/64x500	8/16000
Standard_G5 ¹	32	448	6144	96000/1500/750	64/64x500	8/20000

¹ Instance is isolated to hardware dedicated to a single customer.

Other sizes

- General purpose
- Compute optimized
- Memory optimized
- Storage optimized
- GPU
- High performance compute

Next steps

Learn more about how [Azure compute units \(ACU\)](#) can help you compare compute performance across Azure SKUs.

Virtual machine isolation in Azure

11/18/2019 • 4 minutes to read • [Edit Online](#)

Azure Compute offers virtual machine sizes that are isolated to a specific hardware type and dedicated to a single customer. These virtual machine sizes are best suited for workloads that require a high degree of isolation from other customers for workloads involving elements like compliance and regulatory requirements. Customers can also choose to further subdivide the resources of these isolated virtual machines by using [Azure support for nested virtual machines](#).

Utilizing an isolated size guarantees that your virtual machine will be the only one running on that specific server instance. The current isolated virtual machine offerings include:

- Standard_E64is_v3
- Standard_E64i_v3
- Standard_M128ms
- Standard_GS5
- Standard_G5
- Standard_DS15_v2
- Standard_D15_v2
- Standard_F72s_v2

You can learn more about each available isolated size [here](#).

Retiring D15_v2/DS15_v2 isolation on May 15, 2020

Update on February 10, 2020: The "isolation" retirement timeline has been extended to May 15, 2020"

Azure Dedicated Host is now GA, which allows you to run your organization's Linux and Windows virtual machines on single-tenant physical servers. We plan to fully replace isolated Azure VMs with Azure Dedicated Host. After **May 15, 2020** the D15_v2/DS15_v2 Azure VMs will no longer be hardware isolated.

How does this affect me?

After May 15, 2020, we will no longer provide an isolation guarantee for your D15_v2/DS15_v2 Azure virtual machines.

What actions should I take?

If hardware isolation is not required for you, there is no action you need to take.

If isolation is required to you, before May 15, 2020, you would need to either:

- [Migrate](#) your workload to Azure Dedicated Host.
- [Request access](#) to a D15i_v2 and DS15i_v2 Azure VM, to get the same price performance. This option is only available for pay-as-you-go and one-year reserved instance scenarios.
- [Migrate](#) your workload to another Azure isolated virtual machine.

For details see below:

Timeline

DATE	ACTION
November 18, 2019	Availability of D/DS15i_v2 (PAYG, 1-year RI)
May 14, 2020	Last day to buy D/DS15i_v2 1-year RI
May 15, 2020	D/DS15_v2 isolation guarantee removed
May 15, 2021	Retire D/DS15i_v2 (all customers except who bought 3-year RI of D/DS15_v2 before November 18, 2019)
November 17, 2022	Retire D/DS15i_v2 when 3-year RIs done (for customers who bought 3-year RI of D/DS15_v2 before November 18, 2019)

FAQ

Q: Is the size D/DS15_v2 going to get retired?

A: No, only "isolation" feature is going to get retired. If you do not need isolation, you do not need to take any action.

Q: Is the size D/DS15i_v2 going to get retired?

A: Yes, the size is only available until May 15, 2021. For customers who have bought 3-year RIs on D/DS15_v2 before November 18, 2019 will have access to D/DS15i_v2 until November 17, 2022.

Q: Why am I not seeing the new D/DS15i_v2 sizes in the portal?

A: If you are a current D/DS15_v2 customer and want to use the new D/DS15i_v2 sizes, fill this [form](#)

Q: Why I am not seeing any quota for the new D/DS15i_v2 sizes?

A: If you are a current D/DS15_v2 customer and want to use the new D/DS15i_v2 sizes, fill this [form](#)

Q: When are the other isolated sizes going to retire?

A: We will provide reminders 12 months in advance of the official decommissioning of the sizes.

Q: Is there a downtime when my vm lands on a non-isolated hardware?

A: If you do not need isolation, you do not need to take any action and you would not see any downtime.

Q: Are there any cost changes for moving to a non-isolated virtual machine?

A: No

Q: I already purchased 1- or 3-year Reserved Instance for D15_v2 or Ds15_v2. How will the discount be applied to my VM usage?

A: RIs purchased before November 18, 2019 will automatically extend coverage to the new isolated VM series.

RI	INSTANCE SIZE FLEXIBILITY	BENEFIT ELIGIBILITY
D15_v2	Off	D15_v2 and D15i_v2
D15_v2	On	D15_v2 series and D15i_v2 will all receive the RI benefit.
D14_v2	On	D15_v2 series and D15i_v2 will all receive the RI benefit.

Likewise for Dsv2 series.

Q: I want to purchase additional Reserved Instances for Dv2. Which one should I choose?

A: All RIs purchased after Nov 18, 2019, have the following behavior.

RI	INSTANCE SIZE FLEXIBILITY	BENEFIT ELIGIBILITY
D15_v2	Off	D15_v2 only
D15_v2	On	D15_v2 series will receive the RI benefit. The new D15i_v2 will not be eligible for RI benefit from this RI type.
D15i_v2	Off	D15i_v2 only
D15i_v2	On	D15i_v2 only

Instance Size Flexibility cannot be used to apply to any other sizes such as D2_v2, D4_v2, or D15_v2. Likewise, for Dsv2 series.

Q: Can I buy a new 3-year RI for D15i_v2 and DS15i_v2?

A: Unfortunately no, only 1-year RI is available for new purchase.

Q: Can I move my existing D15_v2/DS15_v2 Reserve Instance to an isolated size Reserved Instance?

A: This action is not necessary since the benefit will apply to both isolated and non-isolated sizes. But Azure will support changing existing D15_v2/DS15_v2 Reserved Instances to D15i_v2/DS15i_v2. For all other Dv2/Dsv2 Reserved Instances, use the existing Reserved Instance or buy new Reserved Instances for the isolated sizes.

Q: I'm an Azure Service Fabric Customer relying on the Silver or Gold Durability Tiers. Does this change impact me?

A: No. The guarantees provided by Service Fabric's [Durability Tiers](#) will continue to function even after this change. If you require physical hardware isolation for other reasons, you may still need to take one of the actions described above.

Azure compute unit (ACU)

2/28/2020 • 2 minutes to read • [Edit Online](#)

The concept of the Azure Compute Unit (ACU) provides a way of comparing compute (CPU) performance across Azure SKUs. This will help you easily identify which SKU is most likely to satisfy your performance needs. ACU is currently standardized on a Small (Standard_A1) VM being 100 and all other SKUs then represent approximately how much faster that SKU can run a standard benchmark.

IMPORTANT

The ACU is only a guideline. The results for your workload may vary.

SKU FAMILY	ACU \ VCPU	VCPU: CORE
A0	50	1:1
A1 - A4	100	1:1
A5 - A7	100	1:1
A1_v2 - A8_v2	100	1:1
A2m_v2 - A8m_v2	100	1:1
A8 - A11	225*	1:1
D1 - D14	160 - 250	1:1
D1_v2 - D15_v2	210 - 250*	1:1
DS1 - DS14	160 - 250	1:1
DS1_v2 - DS15_v2	210 - 250*	1:1
D_v3	160 - 190*	2:1***
Ds_v3	160 - 190*	2:1***
E_v3	160 - 190*	2:1***
Es_v3	160 - 190*	2:1***
F2s_v2 - F72s_v2	195 - 210*	2:1***
F1 - F16	210 - 250*	1:1
F1s - F16s	210 - 250*	1:1

SKU FAMILY	ACU \ VCPU	VCPU: CORE
G1 - G5	180 - 240*	1:1
GS1 - GS5	180 - 240*	1:1
H	290 - 300*	1:1
HB	199 - 216**	1:1
HC	297 - 315*	1:1
L4s - L32s	180 - 240*	1:1
L8s_v2 - L80s_v2	150 - 175**	2:1
M	160 - 180	2:1***

*ACUs use Intel® Turbo technology to increase CPU frequency and provide a performance increase. The amount of the performance increase can vary based on the VM size, workload, and other workloads running on the same host. **ACUs use AMD® Boost technology to increase CPU frequency and provide a performance increase. The amount of the performance increase can vary based on the VM size, workload, and other workloads running on the same host. ***Hyper-threaded and capable of running nested virtualization

Here are links to more information about the different sizes:

- [General-purpose](#)
- [Memory optimized](#)
- [Compute optimized](#)
- [GPU optimized](#)
- [High performance compute](#)
- [Storage optimized](#)

Virtual machine vCPU quotas

1/10/2020 • 2 minutes to read • [Edit Online](#)

The vCPU quotas for virtual machines and virtual machine scale sets are arranged in two tiers for each subscription, in each region. The first tier is the Total Regional vCPUs, and the second tier is the various VM size family cores such as the D-series vCPUs. Any time a new VM is deployed the vCPUs for the VM must not exceed the vCPU quota for the VM size family or the total regional vCPU quota. If either of those quotas are exceeded, the VM deployment will not be allowed. There is also a quota for the overall number of virtual machines in the region. The details on each of these quotas can be seen in the **Usage + quotas** section of the **Subscription** page in the [Azure portal](#), or you can query for the values using the Azure CLI.

Check usage

You can check your quota usage using `az vm list-usage`.

```
az vm list-usage --location "East US" -o table
```

The output should look something like this:

Name	CurrentValue	Limit
Availability Sets	0	2000
Total Regional vCPUs	29	100
Virtual Machines	7	10000
Virtual Machine Scale Sets	0	2000
Standard DSv3 Family vCPUs	8	100
Standard DSv2 Family vCPUs	3	100
Standard Dv3 Family vCPUs	2	100
Standard D Family vCPUs	8	100
Standard Dv2 Family vCPUs	8	100
Basic A Family vCPUs	0	100
Standard A0-A7 Family vCPUs	0	100
Standard A8-A11 Family vCPUs	0	100
Standard DS Family vCPUs	0	100
Standard G Family vCPUs	0	100
Standard GS Family vCPUs	0	100
Standard F Family vCPUs	0	100
Standard FS Family vCPUs	0	100
Standard Storage Managed Disks	5	10000
Premium Storage Managed Disks	5	10000

Reserved VM Instances

Reserved VM Instances, which are scoped to a single subscription without VM size flexibility, will add a new aspect to the vCPU quotas. These values describe the number of instances of the stated size that must be deployable in the subscription. They work as a placeholder in the quota system to ensure that quota is reserved to ensure Azure reservations are deployable in the subscription. For example, if a specific subscription has 10 Standard_D1 reservations the usages limit for Standard_D1 reservations will be 10. This will cause Azure to ensure that there are always at least 10 vCPUs available in the Total Regional vCPUs quota to be used for Standard_D1 instances and there are at least 10 vCPUs available in the Standard D Family vCPU quota to be used for Standard_D1 instances.

If a quota increase is required to either purchase a Single Subscription RI, you can [request a quota increase](#) on your subscription.

Next steps

For more information about billing and quotas, see [Azure subscription and service limits, quotas, and constraints](#).

Save costs with Azure Reserved VM Instances

11/13/2019 • 7 minutes to read • [Edit Online](#)

When you commit to an Azure reserved VM instance you can save money. The reservation discount is applied automatically to the number of running virtual machines that match the reservation scope and attributes. You don't need to assign a reservation to a virtual machine to get the discounts. A reserved instance purchase covers only the compute part of your VM usage. For Windows VMs, the usage meter is split into two separate meters. There's a compute meter, which is same as the Linux meter, and a Windows IP meter. The charges that you see when you make the purchase are only for the compute costs. Charges don't include Windows software costs. For more information about software costs, see [Software costs not included with Azure Reserved VM Instances](#).

Determine the right VM size before you buy

Before you buy a reservation, you should determine the size of the VM that you need. The following sections will help you determine the right VM size.

Use reservation recommendations

You can use reservation recommendations to help determine the reservations you should purchase.

- Purchase recommendations and recommended quantity are shown when you purchase a VM reserved instance in the Azure portal.
- Azure Advisor provides purchase recommendations for individual subscriptions.
- You can use the APIs to get purchase recommendations for both shared scope and single subscription scope. For more information, see [Reserved instance purchase recommendation APIs for enterprise customers](#).
- For Enterprise Agreement (EA) and Microsoft Customer Agreement (MCA) customers, purchase recommendations for shared and single subscription scopes are available with the [Azure Consumption Insights Power BI content pack](#).

Services that get VM reservation discounts

Your VM reservations can apply to VM usage emitted from multiple services - not just for your VM deployments. Resources that get reservation discounts change depending on the instance size flexibility setting.

Instance size flexibility setting

The instance size flexibility setting determines which services get the reserved instance discounts.

Whether the setting is on or off, reservation discounts automatically apply to any matching VM usage when the *ConsumedService* is `Microsoft.Compute`. So, check your usage data for the *ConsumedService* value. Some examples include:

- Virtual machines
- Virtual machine scale sets
- Container service
- Azure Batch deployments (in user subscriptions mode)
- Azure Kubernetes Service (AKS)
- Service Fabric

When the setting is on, reservation discounts automatically apply to matching VM usage when the *ConsumedService* is any of the following items:

- Microsoft.Compute
- Microsoft.ClassicCompute

- Microsoft.Batch
- Microsoft.MachineLearningServices
- Microsoft.Kusto

Check the *ConsumedService* value in your usage data to determine if the usage is eligible for reservation discounts.

For more information about instance size flexibility, see [Virtual machine size flexibility with Reserved VM Instances](#).

Analyze your usage information

Analyze your usage information to help determine which reservations you should purchase.

Usage data is available in the usage file and APIs. Use them together to determine which reservation to purchase. Check for VM instances that have high usage on daily basis to determine the quantity of reservations to purchase.

Avoid the `Meter` subcategory and `Product` fields in usage data. They don't distinguish between VM sizes that use premium storage. If you use these fields to determine the VM size for reservation purchase, you may buy the wrong size. Then you won't get the reservation discount you expect. Instead, refer to the `AdditionalInfo` field in your usage file or usage API to determine the correct VM size.

Purchase restriction considerations

Reserved VM Instances are available for most VM sizes with some exceptions. Reservation discounts don't apply for the following VMs:

- **VM series** - A-series, Av2-series, or G-series.
- **Preview or Promo VMs** - Any VM-series or size that is in preview or uses promotional meter.
- **Clouds** - Reservations aren't available for purchase in Germany or China regions.
- **Insufficient quota** - A reservation that is scoped to a single subscription must have vCPU quota available in the subscription for the new RI. For example, if the target subscription has a quota limit of 10 vCPUs for D-Series, then you can't buy a reservation for 11 Standard_D1 instances. The quota check for reservations includes the VMs already deployed in the subscription. For example, if the subscription has a quota of 10 vCPUs for D-Series and has two standard_D1 instances deployed, then you can buy a reservation for 10 standard_D1 instances in this subscription. You can [create quote increase request](#) to resolve this issue.
- **Capacity restrictions** - In rare circumstances, Azure limits the purchase of new reservations for subset of VM sizes, because of low capacity in a region.

Buy a Reserved VM Instance

You can buy a reserved VM instance in the [Azure portal](#). Pay for the reservation [up front or with monthly payments](#). These requirements apply to buying a reserved VM instance:

- You must be in an Owner role for at least one EA subscription or a subscription with a pay-as-you-go rate.
- For EA subscriptions, the **Add Reserved Instances** option must be enabled in the [EA portal](#). Or, if that setting is disabled, you must be an EA Admin for the subscription.
- For the Cloud Solution Provider (CSP) program, only the admin agents or sales agents can buy reservations.

To buy an instance:

1. Sign in to the [Azure portal](#).
2. Select **All services > Reservations**.
3. Select **Add** to purchase a new reservation and then click **Virtual machine**.
4. Enter required fields. Running VM instances that match the attributes you select qualify to get the reservation

discount. The actual number of your VM instances that get the discount depend on the scope and quantity selected.

If you have an EA agreement, you can use the **Add more option** to quickly add additional instances. The option isn't available for other subscription types.

FIELD	DESCRIPTION
Subscription	The subscription used to pay for the reservation. The payment method on the subscription is charged the costs for the reservation. The subscription type must be an enterprise agreement (offer numbers: MS-AZR-0017P or MS-AZR-0148P) or Microsoft Customer Agreement or an individual subscription with pay-as-you-go rates (offer numbers: MS-AZR-0003P or MS-AZR-0023P). The charges are deducted from the monetary commitment balance, if available, or charged as overage. For a subscription with pay-as-you-go rates, the charges are billed to the credit card or invoice payment method on the subscription.
Scope	The reservation's scope can cover one subscription or multiple subscriptions (shared scope). If you select: <ul style="list-style-type: none">• Single resource group scope — Applies the reservation discount to the matching resources in the selected resource group only.• Single subscription scope — Applies the reservation discount to the matching resources in the selected subscription.• Shared scope — Applies the reservation discount to matching resources in eligible subscriptions that are in the billing context. For EA customers, the billing context is the enrollment. For individual subscriptions with pay-as-you-go rates, the billing scope is all eligible subscriptions created by the account administrator.
Region	The Azure region that's covered by the reservation.
VM Size	The size of the VM instances.
Optimize for	VM instance size flexibility is selected by default. Click Advanced settings to change the instance size flexibility value to apply the reservation discount to other VMs in the same VM size group . Capacity priority prioritizes data center capacity for your deployments. It offers additional confidence in your ability to launch the VM instances when you need them. Capacity priority is only available when the reservation scope is single subscription.
Term	One year or three years.
Quantity	The number of instances being purchased within the reservation. The quantity is the number of running VM instances that can get the billing discount. For example, if you are running 10 Standard_D2 VMs in the East US, then you would specify quantity as 10 to maximize the benefit for all running VMs.

Usage data and reservation utilization

Your usage data has an effective price of zero for the usage that gets a reservation discount. You can see which VM instance received the reservation discount for each reservation.

For more information about how reservation discounts appear in usage data, see [Understand Azure reservation usage for your Enterprise enrollment](#) if you are an EA customer. If you have an individual subscription, see [Understand Azure reservation usage for your Pay-As-You-Go subscription](#).

Change a reservation after purchase

You can make the following types of changes to a reservation after purchase:

- Update reservation scope
- Instance size flexibility (if applicable)
- Ownership

You can also split a reservation into smaller chunks and merge already split reservations. None of the changes cause a new commercial transaction or change the end date of the reservation.

You can't make the following types of changes after purchase, directly:

- An existing reservation's region
- SKU
- Quantity
- Duration

However, you can *exchange* a reservation if you want to make changes.

Cancel, exchange, or refund reservations

You can cancel, exchange, or refund reservations with certain limitations. For more information, see [Self-service exchanges and refunds for Azure Reservations](#).

Need help? Contact us.

If you have questions or need help, [create a support request](#).

Next steps

- To learn how to manage a reservation, see [Manage Azure Reservations](#).
- To learn more about Azure Reservations, see the following articles:
 - [What are Azure Reservations?](#)
 - [Manage Reservations in Azure](#)
 - [Understand how the reservation discount is applied](#)
 - [Understand reservation usage for a subscription with pay-as-you-go rates](#)
 - [Understand reservation usage for your Enterprise enrollment](#)
 - [Windows software costs not included with reservations](#)
 - [Azure Reservations in Partner Center Cloud Solution Provider \(CSP\) program](#)

2 minutes to read

Virtual machine size flexibility with Reserved VM Instances

11/13/2019 • 2 minutes to read • [Edit Online](#)

When you buy a Reserved VM Instance, you can choose to optimize for instance size flexibility or capacity priority. For more information about setting or changing the optimize setting for reserved VM instances, see [Change the optimize setting for reserved VM instances](#).

With a reserved virtual machine instance that's optimized for instance size flexibility, the reservation you buy can apply to the virtual machines (VMs) sizes in the same instance size flexibility group. For example, if you buy a reservation for a VM size that's listed in the DSv2 Series, like Standard_DS5_v2, the reservation discount can apply to the other four sizes that are listed in that same instance size flexibility group:

- Standard_DS1_v2
- Standard_DS2_v2
- Standard_DS3_v2
- Standard_DS4_v2

But that reservation discount doesn't apply to VMs sizes that are listed in different instance size flexibility groups, like SKUs in DSv2 Series High Memory: Standard_DS11_v2, Standard_DS12_v2, and so on.

Within the instance size flexibility group, the number of VMs the reservation discount applies to depends on the VM size you pick when you buy a reservation. It also depends on the sizes of the VMs that you have running. The ratio column compares the relative footprint for each VM size in that instance size flexibility group. Use the ratio value to calculate how the reservation discount applies to the VMs you have running.

Examples

The following examples use the sizes and ratios in the DSv2-series table.

You buy a reserved VM instance with the size Standard_DS4_v2 where the ratio or relative footprint compared to the other sizes in that series is 8.

- Scenario 1: Run eight Standard_DS1_v2 sized VMs with a ratio of 1. Your reservation discount applies to all eight of those VMs.
- Scenario 2: Run two Standard_DS2_v2 sized VMs with a ratio of 2 each. Also run a Standard_DS3_v2 sized VM with a ratio of 4. The total footprint is $2+2+4=8$. So your reservation discount applies to all three of those VMs.
- Scenario 3: Run one Standard_DS5_v2 with a ratio of 16. Your reservation discount applies to half that VM's compute cost.

The following sections show what sizes are in the same size series group when you buy a reserved VM instance optimized for instance size flexibility.

Instance size flexibility ratio for VMs

CSV below has the instance size flexibility groups, ArmSkuName and the ratios.

Instance size flexibility ratios

We will keep the file URL and the schema fixed so you can consume this file programmatically. The data will also be available through API soon.

Compute benchmark scores for Linux VMs

2/26/2020 • 22 minutes to read • [Edit Online](#)

The following CoreMark benchmark scores show compute performance for Azure's high-performance VM lineup running Ubuntu. Compute benchmark scores are also available for [Windows VMs](#).

Av2 - General Compute

(3/15/2019 12:06:55 AM pbi 3897709)

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_A1_v2	Intel(R) Xeon(R) CPU E5-2660 0 @ 2.20GHz	1	1	1.9	6,483	120	1.85%	273
Standard_A1_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	1	1	1.9	6,059	208	3.43%	217
Standard_A1_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	1	1	1.9	6,367	453	7.12%	217
Standard_A2_v2	Intel(R) Xeon(R) CPU E5-2660 0 @ 2.20GHz	2	1	3.9	13,161	194	1.48%	266
Standard_A2_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	2	1	3.9	12,067	401	3.32%	203
Standard_A2_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	2	1	3.9	12,527	797	6.37%	238

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_A2m_v2	Intel(R) Xeon(R) CPU E5-2660 0 @ 2.20GHz	2	1	15.7	13,167	179	1.36%	273
Standard_A2m_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	2	1	15.7	12,133	336	2.77%	210
Standard_A2m_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	2	1	15.7	12,401	656	5.29%	224
Standard_A4_v2	Intel(R) Xeon(R) CPU E5-2660 0 @ 2.20GHz	4	1	7.8	26,307	231	0.88%	231
Standard_A4_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	4	1	7.8	24,552	720	2.93%	224
Standard_A4_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	4	1	7.8	24,963	1,625	6.51%	252
Standard_A4m_v2	Intel(R) Xeon(R) CPU E5-2660 0 @ 2.20GHz	4	1	31.4	26,238	292	1.11%	259
Standard_A4m_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	4	1	31.4	24,250	491	2.02%	189

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	Avg Score	STDDEV	STDDEV%	#RUNS
Standard_A4m_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	4	1	31.4	24,725	1,553	6.28%	259
Standard_A8_v2	Intel(R) Xeon(R) CPU E5-2660 0 @ 2.20GHz	8	1	15.7	53,237	687	1.29%	266
Standard_A8_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	8	1	15.7	49,655	585	1.18%	147
Standard_A8_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	8	1	15.7	49,005	2,162	4.41%	294
Standard_A8m_v2	Intel(R) Xeon(R) CPU E5-2660 0 @ 2.20GHz	8	2	62.9	52,627	902	1.71%	266
Standard_A8m_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	8	1	62.9	49,838	633	1.27%	182
Standard_A8m_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	8	1	62.9	49,123	2,483	5.05%	259

Note: Av2-series VMs can be deployed on a variety of hardware types and processors (as seen above). Av2-series VMs have CPU performance and memory configurations best suited for entry level workloads like development and test. The size is throttled to offer relatively consistent processor performance for the running instance, regardless of the hardware it is deployed on; however, software that takes advantage of specific newer processor optimizations may see more significant variation across processor types.

B - Burstable

(3/15/2019 12:27:08 AM pbi 3897709)

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_B1ms	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	1	1	1.9	13,593	307	2.26%	28
Standard_B1ms	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	1	1	1.9	14,069	495	3.52%	672
Standard_B1s	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	1	1	0.9	13,736	211	1.54%	28
Standard_B1s	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	1	1	0.9	13,965	457	3.27%	672
Standard_B2ms	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	2	1	7.8	27,361	1,110	4.06%	28
Standard_B2ms	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	2	1	7.8	27,432	771	2.81%	672
Standard_B2s	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	2	1	3.9	27,488	822	2.99%	28
Standard_B2s	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	2	1	3.9	27,548	864	3.14%	672

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	Avg Score	STDDEV	STDDEV%	#RUNS
Standard_B4ms	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	4	1	15.7	54,951	1,868	3.40%	28
Standard_B4ms	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	4	1	15.7	54,051	1,260	2.33%	672
Standard_B8ms	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	8	1	31.4	111,929	1,562	1.40%	35
Standard_B8ms	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	8	1	31.4	109,537	1,354	1.24%	665

Note: B-Series VMs are for workloads with burstable performance requirements. VM instances accumulate credits when using less than its baseline. When the VM has accumulated credit, the VM can burst above the baseline using up to 100% to meet short CPU burst requirements. Burst time depends on available credits which is a function of VM size and time.

CoreMark is a short running test that typically completes within available burst credits. Therefore the numbers above typically represent the burst performance of the VM, reflecting what the short, bursty, workloads (typical on B-Series) performance will typically see.

DSv3 - General Compute + Premium Storage

(3/12/2019 6:52:03 PM pbi 3897709)

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	Avg Score	STDDEV	STDDEV%	#RUNS
Standard_D2s_v3	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	2	1	7.8	20,153	838	4.16%	147

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_D2s_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	2	1	7.8	20,903	1,324	6.33%	553
Standard_D4s_v3	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	4	1	15.7	39,502	1,257	3.18%	189
Standard_D4s_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	4	1	15.7	40,547	1,935	4.77%	511
Standard_D8s_v3	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	8	1	31.4	80,191	1,054	1.31%	168
Standard_D8s_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	8	1	31.4	79,884	3,073	3.85%	532
Standard_D16s_v3	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	16	1	62.9	160,319	1,213	0.76%	105
Standard_D16s_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	16	1	62.9	156,325	2,176	1.39%	588
Standard_D32s_v3	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	32	2	125.9	315,457	2,647	0.84%	105

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	Avg Score	STDDEV	STDDEV%	#RUNS
Standard_D32s_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	32	1	125.9	312,058	1,661	0.53%	595
Standard_D64s_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	64	2	251.9	627,378	4,447	0.71%	700

Dv3 - General Compute

(3/12/2019 6:54:27 PM pbi 3897709)

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	Avg Score	STDDEV	STDDEV%	#RUNS
Standard_D2_v3	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	2	1	7.8	20,359	799	3.93%	154
Standard_D2_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	2	1	7.8	20,737	1,422	6.86%	546
Standard_D4_v3	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	4	1	15.7	40,095	1,501	3.74%	147
Standard_D4_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	4	1	15.7	41,147	2,706	6.58%	546
Standard_D8_v3	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	8	1	31.4	80,383	1,486	1.85%	133

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_D8_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	8	1	31.4	80,511	3,916	4.86%	560
Standard_D16_v3	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	16	1	62.9	160,932	2,200	1.37%	140
Standard_D16_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	16	1	62.9	158,679	4,550	2.87%	560
Standard_D32_v3	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	32	2	125.9	314,208	4,250	1.35%	189
Standard_D32_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	32	1	125.9	312,472	3,173	1.02%	511
Standard_D64_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	64	2	251.9	627,470	9,651	1.54%	700

DSv2 - Storage Optimized

(3/15/2019 12:53:13 AM pbi 3897709)

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_DS1_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	1	1	3.4	14,642	600	4.10%	259

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_DS1_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	1	1	3.4	14,808	904	6.10%	434
Standard_DS2_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	2	1	6.8	28,654	877	3.06%	301
Standard_DS2_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	2	1	6.8	29,089	1,421	4.89%	406
Standard_DS3_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	4	1	13.7	57,255	1,633	2.85%	238
Standard_DS3_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	4	1	13.7	57,255	2,265	3.96%	462
Standard_DS4_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	8	1	27.5	116,681	1,097	0.94%	231
Standard_DS4_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	8	1	27.5	112,512	1,261	1.12%	462
Standard_DS5_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	16	1	55.0	225,661	2,370	1.05%	189

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_DS5_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	16	2	55.0	229,145	2,878	1.26%	21
Standard_DS5_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	16	1	55.0	226,818	1,797	0.79%	497
Standard_DS11_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	2	1	13.7	28,571	920	3.22%	238
Standard_DS11_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	2	1	13.7	29,049	1,614	5.56%	469
Standard_DS11-1_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	1	1	13.7	14,594	617	4.23%	287
Standard_DS11-1_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	1	1	13.7	14,951	852	5.70%	413
Standard_DS12_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	4	1	27.5	57,503	1,398	2.43%	217
Standard_DS12_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	4	1	27.5	57,082	2,372	4.16%	483

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_DS12-1_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	1	1	27.5	14,698	564	3.84%	238
Standard_DS12-1_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	1	1	27.5	15,127	941	6.22%	462
Standard_DS12-2_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	2	1	27.5	28,711	981	3.42%	259
Standard_DS12-2_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	2	1	27.5	29,305	1,241	4.24%	441
Standard_DS13_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	8	1	55.0	116,875	1,286	1.10%	203
Standard_DS13_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	8	1	55.0	112,318	1,356	1.21%	504
Standard_DS13-2_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	2	1	55.0	29,105	1,154	3.97%	224
Standard_DS13-2_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	2	1	55.0	29,936	1,720	5.75%	483

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	Avg Score	STDDEV	STDDEV%	#RUNS
Standard_DS13-4_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	4	1	55.0	56,992	1,814	3.18%	280
Standard_DS13-4_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	4	1	55.0	57,781	2,122	3.67%	427
Standard_DS14_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	16	2	110.2	224,149	3,450	1.54%	196
Standard_DS14_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	16	1	110.2	227,108	1,267	0.56%	504
Standard_DS14-4_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	4	2	110.2	56,211	2,154	3.83%	189
Standard_DS14-4_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	4	1	110.2	59,651	2,560	4.29%	518
Standard_DS14-8_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	8	2	110.2	112,280	4,430	3.95%	196
Standard_DS14-8_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	8	1	110.2	113,375	1,442	1.27%	511

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	Avg Score	STDDEV	STDDEV%	#RUNS
Standard_DS15_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	20	2	137.7	279,359	4,032	1.44%	665

Dv2 - General Compute

(3/12/2019 6:53:48 PM pbi 3897709)

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	Avg Score	STDDEV	STDDEV%	#RUNS
Standard_D1_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	1	1	3.4	14,730	663	4.50%	385
Standard_D1_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	1	1	3.4	15,057	1,319	8.76%	322
Standard_D2_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	2	1	6.8	29,395	1,073	3.65%	329
Standard_D2_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	2	1	6.8	29,564	2,145	7.26%	378
Standard_D3_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	4	1	13.7	58,150	1,340	2.30%	343
Standard_D3_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	4	1	13.7	57,820	2,944	5.09%	364

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_D4_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	8	1	27.5	117,448	1,612	1.37%	308
Standard_D4_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	8	1	27.5	114,082	3,369	2.95%	399
Standard_D5_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	16	1	55.0	226,370	4,722	2.09%	147
Standard_D5_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	16	2	55.0	225,035	5,026	2.23%	119
Standard_D5_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	16	1	55.0	227,883	3,259	1.43%	441
Standard_D11_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	2	1	13.7	29,260	1,012	3.46%	308
Standard_D11_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	2	1	13.7	29,306	1,763	6.02%	399
Standard_D12_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	4	1	27.5	58,322	1,391	2.39%	329

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_D12_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	4	1	27.5	57,999	3,533	6.09%	371
Standard_D13_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	8	1	55.0	117,218	1,514	1.29%	329
Standard_D13_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	8	1	55.0	114,344	3,307	2.89%	378
Standard_D14_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	16	2	110.2	224,348	5,477	2.44%	280
Standard_D14_v2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	16	1	110.2	228,221	2,733	1.20%	427
Standard_D15_v2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	20	2	137.7	281,494	7,976	2.83%	672

Esv3 - Memory Optimized + Premium Storage

(3/12/2019 7:17:33 PM pbi 3897709)

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_E2s_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	2	1	15.7	20,957	1,200	5.73%	672

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_E4s_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	4	1	31.4	40,420	1,993	4.93%	672
Standard_E4-2s_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	2	1	31.4	20,774	1,133	5.45%	672
Standard_E8s_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	8	1	62.9	80,153	3,308	4.13%	665
Standard_E8-2s_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	2	1	62.9	21,178	1,334	6.30%	665
Standard_E8-4s_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	4	1	62.9	40,614	2,216	5.46%	672
Standard_E16s_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	16	1	125.9	156,137	2,160	1.38%	672
Standard_E16-4s_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	4	1	125.9	41,950	2,309	5.50%	637
Standard_E16-8s_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	8	1	125.9	81,196	3,179	3.91%	658

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_E20s_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	20	1	157.4	196,619	1,325	0.67%	672
Standard_E32s_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	32	2	251.9	304,707	5,719	1.88%	672
Standard_E32-8s_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	8	2	251.9	83,576	3,693	4.42%	672
Standard_E32-16s_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	16	2	251.9	158,023	4,317	2.73%	672
Standard_E64s_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	64	2	425.2	628,540	3,982	0.63%	49
Standard_E64-16s_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	16	2	425.2	169,611	3,265	1.92%	42
Standard_E64-32s_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	32	2	425.2	307,584	3,569	1.16%	56

Eisv3 - Memory Opt + Premium Storage (isolated)

(4/11/2019 10:07:29 PM pbi 3897709)

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	Avg Score	STDDEV	STDDEV%	#RUNS
Standard_E64is_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	64	2	425.2	627,745	4,062	0.65%	196

Ev3 - Memory Optimized

(3/12/2019 6:52:13 PM pbi 3897709)

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	Avg Score	STDDEV	STDDEV%	#RUNS
Standard_E2_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	2	1	15.7	21,171	1,772	8.37%	693
Standard_E4_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	4	1	31.4	41,181	3,148	7.64%	700
Standard_E8_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	8	1	62.9	81,211	5,055	6.22%	700
Standard_E16_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	16	1	125.9	158,152	4,033	2.55%	700
Standard_E20_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	20	1	157.4	197,739	2,731	1.38%	693
Standard_E32_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	32	2	251.9	307,286	8,353	2.72%	700

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_E64_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	64	2	425.2	628,451	9,235	1.47%	707

Eiv3 - Memory Optimized (isolated)

(3/12/2019 6:57:51 PM pbi 3897709)

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_E64i_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	64	2	425.2	625,855	4,881	0.78%	7
Standard_E64i_v3	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	64	2	425.2	629,151	9,756	1.55%	217

Fsv2 - Compute + Storage Optimized

(3/12/2019 6:51:35 PM pbi 3897709)

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_F2s_v2	Intel(R) Xeon(R) Platinum 8168 CPU @ 2.70GHz	2	1	3.9	28,219	1,843	6.53%	700
Standard_F4s_v2	Intel(R) Xeon(R) Platinum 8168 CPU @ 2.70GHz	4	1	7.8	53,911	1,002	1.86%	707
Standard_F8s_v2	Intel(R) Xeon(R) Platinum 8168 CPU @ 2.70GHz	8	1	15.7	106,467	1,101	1.03%	707

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	Avg Score	STDDEV	STDDEV%	#RUNS
Standard_F16s_v2	Intel(R) Xeon(R) Platinum 8168 CPU @ 2.70GHz	16	1	31.4	211,311	1,724	0.82%	707
Standard_F32s_v2	Intel(R) Xeon(R) Platinum 8168 CPU @ 2.70GHz	32	1	62.9	423,175	4,346	1.03%	707
Standard_F64s_v2	Intel(R) Xeon(R) Platinum 8168 CPU @ 2.70GHz	64	2	125.9	829,537	21,574	2.60%	707
Standard_F72s_v2	Intel(R) Xeon(R) Platinum 8168 CPU @ 2.70GHz	72	2	141.7	933,800	26,783	2.87%	707

Fs - Compute and Storage Optimized

(3/15/2019 12:12:51 AM pbi 3897709)

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	Avg Score	STDDEV	STDDEV%	#RUNS
Standard_F1s	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	1	1	1.9	14,552	504	3.46%	350
Standard_F1s	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	1	1	1.9	14,784	858	5.80%	357
Standard_F2s	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	2	1	3.9	28,664	895	3.12%	245

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_F2s	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	2	1	3.9	29,188	1,228	4.21%	455
Standard_F4s	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	4	1	7.8	57,192	1,700	2.97%	259
Standard_F4s	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	4	1	7.8	57,412	2,215	3.86%	448
Standard_F8s	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	8	1	15.7	117,008	1,139	0.97%	259
Standard_F8s	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	8	1	15.7	112,610	1,595	1.42%	441
Standard_F16s	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	16	1	31.4	225,444	2,328	1.03%	210
Standard_F16s	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	16	2	31.4	228,919	3,380	1.48%	28
Standard_F16s	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	16	1	31.4	227,015	1,543	0.68%	462

F - Compute Optimized

(3/12/2019 6:53:59 PM pbi 3897709)

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_F1	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	1	1	1.9	14,937	593	3.97%	350
Standard_F1	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	1	1	1.9	15,460	1,326	8.58%	350
Standard_F2	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	2	1	3.9	29,324	1,196	4.08%	343
Standard_F2	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	2	1	3.9	29,299	1,908	6.51%	364
Standard_F4	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	4	1	7.8	58,314	1,245	2.14%	364
Standard_F4	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	4	1	7.8	58,280	3,581	6.14%	336
Standard_F8	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	8	1	15.7	117,516	1,460	1.24%	308

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_F8	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	8	1	15.7	114,361	3,868	3.38%	399
Standard_F16	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	16	1	31.4	226,487	4,140	1.83%	154
Standard_F16	Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz	16	2	31.4	226,683	4,723	2.08%	133
Standard_F16	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz	16	1	31.4	228,592	2,371	1.04%	392

GS - Storage Optimized

(3/12/2019 10:22:33 PM pbi 3897709)

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_GS1	Intel(R) Xeon(R) CPU E5-2698B v3 @ 2.00GHz	2	1	27.5	28,835	2,222	7.71%	287
Standard_GS2	Intel(R) Xeon(R) CPU E5-2698B v3 @ 2.00GHz	4	1	55.0	55,568	3,139	5.65%	287
Standard_GS3	Intel(R) Xeon(R) CPU E5-2698B v3 @ 2.00GHz	8	1	110.2	106,567	2,188	2.05%	287

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_GS4	Intel(R) Xeon(R) CPU E5-2698B v3 @ 2.00GHz	16	1	220.4	210,586	4,130	1.96%	287
Standard_GS4-4	Intel(R) Xeon(R) CPU E5-2698B v3 @ 2.00GHz	4	1	220.4	58,598	2,670	4.56%	287
Standard_GS4-8	Intel(R) Xeon(R) CPU E5-2698B v3 @ 2.00GHz	8	1	220.4	108,234	2,392	2.21%	287
Standard_GS5	Intel(R) Xeon(R) CPU E5-2698B v3 @ 2.00GHz	32	2	440.9	399,835	8,694	2.17%	287
Standard_GS5-8	Intel(R) Xeon(R) CPU E5-2698B v3 @ 2.00GHz	8	2	440.9	116,643	2,354	2.02%	287
Standard_GS5-16	Intel(R) Xeon(R) CPU E5-2698B v3 @ 2.00GHz	16	2	440.9	210,984	2,995	1.42%	287

G - Compute Optimized

(3/12/2019 10:23:51 PM pbi 3897709)

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_G1	Intel(R) Xeon(R) CPU E5-2698B v3 @ 2.00GHz	2	1	27.5	32,808	2,679	8.17%	287

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_G2	Intel(R) Xeon(R) CPU E5-2698B v3 @ 2.00GHz	4	1	55.0	62,907	4,465	7.10%	287
Standard_G3	Intel(R) Xeon(R) CPU E5-2698B v3 @ 2.00GHz	8	1	110.2	113,471	4,346	3.83%	287
Standard_G4	Intel(R) Xeon(R) CPU E5-2698B v3 @ 2.00GHz	16	1	220.4	212,092	2,857	1.35%	287
Standard_G5	Intel(R) Xeon(R) CPU E5-2698B v3 @ 2.00GHz	32	2	440.9	403,315	6,947	1.72%	273

H - High Performance Compute (HPC)

(3/12/2019 10:50:51 PM pbi 3897709)

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_H8	Intel(R) Xeon(R) CPU E5-2667 v3 @ 3.20GHz	8	1	55.0	149,859	734	0.49%	175
Standard_H8m	Intel(R) Xeon(R) CPU E5-2667 v3 @ 3.20GHz	8	1	110.2	149,931	657	0.44%	147
Standard_H16	Intel(R) Xeon(R) CPU E5-2667 v3 @ 3.20GHz	16	2	110.2	282,083	6,738	2.39%	84

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	Avg Score	STDDEV	STDDEV%	#RUNS
Standard_H16m	Intel(R) Xeon(R) CPU E5-2667 v3 @ 3.20GHz	16	2	220.4	282,106	7,013	2.49%	84
Standard_H16mr	Intel(R) Xeon(R) CPU E5-2667 v3 @ 3.20GHz	16	2	220.4	282,167	6,889	2.44%	84
Standard_H16r	Intel(R) Xeon(R) CPU E5-2667 v3 @ 3.20GHz	16	2	110.2	280,837	6,587	2.35%	84

Lv2 - Storage Optimized

(3/14/2019 5:49:04 PM pbi 3897709)

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	Avg Score	STDDEV	STDDEV%	#RUNS
Standard_L8s_v2	AMD EPYC 7551 32-Core Processor	8	1	62.9	80,528	404	0.50%	119
Standard_L16s_v2	AMD EPYC 7551 32-Core Processor	16	2	125.9	154,829	3,708	2.40%	119
Standard_L32s_v2	AMD EPYC 7551 32-Core Processor	32	4	251.9	310,811	7,751	2.49%	119
Standard_L64s_v2	AMD EPYC 7551 32-Core Processor	64	8	503.9	595,140	14,572	2.45%	112

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	Avg Score	STDDEV	STDDEV%	#RUNS
Standard_L80s_v2	AMD EPYC 7551 32-Core Processor	80	10	629.9	773,171	19,559	2.53%	119

Ls - Storage Optimized

(3/12/2019 10:22:29 PM pbi 3897709)

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	Avg Score	STDDEV	STDDEV%	#RUNS
Standard_L4s	Intel(R) Xeon(R) CPU E5-2698B v3 @ 2.00GHz	4	1	31.4	56,488	2,916	5.16%	287
Standard_L8s	Intel(R) Xeon(R) CPU E5-2698B v3 @ 2.00GHz	8	1	62.9	107,017	2,323	2.17%	287
Standard_L16s	Intel(R) Xeon(R) CPU E5-2698B v3 @ 2.00GHz	16	1	125.9	210,865	3,653	1.73%	280
Standard_L32s	Intel(R) Xeon(R) CPU E5-2698B v3 @ 2.00GHz	32	2	251.9	399,963	9,254	2.31%	287

M - Memory Optimized

(4/11/2019 7:30:39 PM pbi 3897709)

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	Avg Score	STDDEV	STDDEV%	#RUNS
Standard_M8-2ms	Intel(R) Xeon(R) CPU E7-8890 v3 @ 2.50GHz	2	1	215.2	22,605	29	0.13%	42

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_M8-4ms	Intel(R) Xeon(R) CPU E7-8890 v3 @ 2.50GHz	4	1	215.2	44,488	183	0.41%	42
Standard_M16-4ms	Intel(R) Xeon(R) CPU E7-8890 v3 @ 2.50GHz	4	1	430.6	44,451	269	0.61%	42
Standard_M16-8ms	Intel(R) Xeon(R) CPU E7-8890 v3 @ 2.50GHz	8	1	430.6	88,238	1,243	1.41%	42
Standard_M32-8ms	Intel(R) Xeon(R) CPU E7-8890 v3 @ 2.50GHz	8	1	861.2	88,521	1,353	1.53%	42
Standard_M32-16ms	Intel(R) Xeon(R) CPU E7-8890 v3 @ 2.50GHz	16	1	861.2	174,674	3,104	1.78%	42
Standard_M64	Intel(R) Xeon(R) CPU E7-8890 v3 @ 2.50GHz	64	2	1,007.9	683,022	11,929	1.75%	42
Standard_M64-16ms	Intel(R) Xeon(R) CPU E7-8890 v3 @ 2.50GHz	16	2	1,763.9	169,386	4,737	2.80%	42
Standard_M64-32ms	Intel(R) Xeon(R) CPU E7-8890 v3 @ 2.50GHz	32	2	1,763.9	337,599	4,738	1.40%	42

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_M64m	Intel(R) Xeon(R) CPU E7-8890 v3 @ 2.50GHz	64	2	1,763.9	677,466	14,478	2.14%	42
Standard_M64ms	Intel(R) Xeon(R) CPU E7-8890 v3 @ 2.50GHz	64	2	1,763.9	675,342	16,577	2.45%	42
Standard_M64s	Intel(R) Xeon(R) CPU E7-8890 v3 @ 2.50GHz	64	2	1,007.9	674,785	15,983	2.37%	42
Standard_M128	Intel(R) Xeon(R) CPU E7-8890 v3 @ 2.50GHz	128	4	2,015.9	1,334,218	21,126	1.58%	42
Standard_M128-32ms	Intel(R) Xeon(R) CPU E7-8890 v3 @ 2.50GHz	32	4	3,831.1	334,873	5,005	1.49%	42
Standard_M128-64ms	Intel(R) Xeon(R) CPU E7-8890 v3 @ 2.50GHz	64	4	3,831.1	667,808	18,145	2.72%	42
Standard_M128m	Intel(R) Xeon(R) CPU E7-8890 v3 @ 2.50GHz	128	4	3,831.1	1,335,873	19,642	1.47%	42
Standard_M128ms	Intel(R) Xeon(R) CPU E7-8890 v3 @ 2.50GHz	128	4	3,831.1	1,329,151	24,295	1.83%	42

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_M128s	Intel(R) Xeon(R) CPU E7-8890 v3 @ 2.50GHz	128	4	2,015.9	1,329,923	20,117	1.51%	42
Standard_M16ms	Intel(R) Xeon(R) CPU E7-8890 v3 @ 2.50GHz	16	1	430.6	174,686	2,704	1.55%	35
Standard_M32ls	Intel(R) Xeon(R) CPU E7-8890 v3 @ 2.50GHz	32	1	251.9	344,069	3,372	0.98%	42
Standard_M32ms	Intel(R) Xeon(R) CPU E7-8890 v3 @ 2.50GHz	32	1	861.2	343,226	4,884	1.42%	84
Standard_M32ms	Intel(R) Xeon(R) CPU E7-8890 v3 @ 2.50GHz	32	2	861.2	336,526	4,396	1.31%	7
Standard_M32ts	Intel(R) Xeon(R) CPU E7-8890 v3 @ 2.50GHz	32	1	188.9	341,112	5,491	1.61%	35
Standard_M64ls	Intel(R) Xeon(R) CPU E7-8890 v3 @ 2.50GHz	64	2	503.9	676,026	18,078	2.67%	42
Standard_M8ms	Intel(R) Xeon(R) CPU E7-8890 v3 @ 2.50GHz	8	1	215.2	88,066	1,391	1.58%	42

NCSV3 - GPU Enabled

(3/21/2019 5:48:37 PM pbi 3897709)

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_NC6s_v3	Intel(R) Xeon(R) CPU E5-2690 v4 @ 2.60GHz	6	1	110.2	106,929	353	0.33%	49
Standard_NC12s_v3	Intel(R) Xeon(R) CPU E5-2690 v4 @ 2.60GHz	12	1	220.4	213,585	875	0.41%	42
Standard_NC24rs_v3	Intel(R) Xeon(R) CPU E5-2690 v4 @ 2.60GHz	24	2	440.9	403,554	6,705	1.66%	42
Standard_NC24s_v3	Intel(R) Xeon(R) CPU E5-2690 v4 @ 2.60GHz	24	2	440.9	403,874	7,603	1.88%	42

NCSV2 - GPU Enabled

(3/12/2019 11:19:19 PM pbi 3897709)

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_NC6s_v2	Intel(R) Xeon(R) CPU E5-2690 v4 @ 2.60GHz	6	1	110.2	107,115	321	0.30%	63
Standard_NC12s_v2	Intel(R) Xeon(R) CPU E5-2690 v4 @ 2.60GHz	12	1	220.4	213,814	656	0.31%	63

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	Avg Score	STDDEV	STDDEV%	#RUNS
Standard_NC24rs_v2	Intel(R) Xeon(R) CPU E5-2690 v4 @ 2.60GHz	24	2	440.9	401,728	6,995	1.74%	63
Standard_NC24s_v2	Intel(R) Xeon(R) CPU E5-2690 v4 @ 2.60GHz	24	2	440.9	402,808	7,923	1.97%	63

NC - GPU Enabled

(3/12/2019 11:08:03 PM pbi 3897709)

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	Avg Score	STDDEV	STDDEV%	#RUNS
Standard_NC6	Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.60GHz	6	1	55.0	102,211	658	0.64%	259
Standard_NC12	Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.60GHz	12	1	110.2	203,523	2,293	1.13%	259
Standard_NC24	Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.60GHz	24	2	220.4	382,897	8,712	2.28%	259
Standard_NC24r	Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.60GHz	24	2	220.4	383,171	9,166	2.39%	259

NDs- GPU Enabled

(3/12/2019 11:19:10 PM pbi 3897709)

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_ND6s	Intel(R) Xeon(R) CPU E5-2690 v4 @ 2.60GHz	6	1	110.2	107,095	353	0.33%	63
Standard_ND12s	Intel(R) Xeon(R) CPU E5-2690 v4 @ 2.60GHz	12	1	220.4	212,298	3,457	1.63%	63
Standard_ND24rs	Intel(R) Xeon(R) CPU E5-2690 v4 @ 2.60GHz	24	2	440.9	402,749	7,838	1.95%	56
Standard_ND24s	Intel(R) Xeon(R) CPU E5-2690 v4 @ 2.60GHz	24	2	440.9	401,822	7,776	1.94%	63

NV - GPU Enabled

(3/12/2019 11:08:13 PM pbi 3897709)

VM SIZE	CPU	VCPUS	NUMA NODES	MEMORY(GIB)	AVG SCORE	STDDEV	STDDEV%	#RUNS
Standard_NV6	Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.60GHz	6	1	55.0	101,728	2,094	2.06%	259
Standard_NV12	Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.60GHz	12	1	110.2	203,903	1,724	0.85%	252
Standard_NV24	Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.60GHz	24	2	220.4	379,879	8,737	2.30%	259

About CoreMark

Linux numbers were computed by running [CoreMark](#) on Ubuntu. CoreMark was configured with the number of threads set to the number of virtual CPUs, and concurrency set to PThreads. The target number of iterations was adjusted based on expected performance to provide a runtime of at least 20 seconds (typically much longer). The final score represents the number of iterations completed divided by the number of seconds it took to run the test. Each test was run at least seven times on each VM. Test run dates shown above. Tests run on multiple VMs across Azure public regions the VM was supported in on the date run. Basic A and B (Burstable) series not shown because performance is variable. N series not shown as they are GPU centric and Coremark doesn't measure GPU performance.

Next steps

- For storage capacities, disk details, and additional considerations for choosing among VM sizes, see [Sizes for virtual machines](#).
- To run the CoreMark scripts on Linux VMs, download the [CoreMark script pack](#).

Endorsed Linux distributions on Azure

1/8/2020 • 5 minutes to read • [Edit Online](#)

Partners provide Linux images in the Azure Marketplace. We are working with various Linux communities to add even more flavors to the Endorsed Distribution list. In the meantime, for distributions that are not available from the Marketplace, you can always bring your own Linux by following the guidelines at [Create and upload a virtual hard disk that contains the Linux operating system](#).

Supported distributions and versions

The following table lists the Linux distributions and versions that are supported on Azure. Refer to [Support for Linux images in Microsoft Azure](#) for more detailed information about support for Linux and open-source technology in Azure.

The Linux Integration Services (LIS) drivers for Hyper-V and Azure are kernel modules that Microsoft contributes directly to the upstream Linux kernel. Some LIS drivers are built into the distribution's kernel by default. Older distributions that are based on Red Hat Enterprise (RHEL)/CentOS are available as a separate download at [Linux Integration Services Version 4.2 for Hyper-V and Azure](#). See [Linux kernel requirements](#) for more information about the LIS drivers.

The Azure Linux Agent is already pre-installed on the Azure Marketplace images and is typically available from the distribution's package repository. Source code can be found on [GitHub](#).

DISTRIBUTION	VERSION	DRIVERS	AGENT
CentOS	CentOS 6.3+, 7.0+, 8.0+	CentOS 6.3: LIS download CentOS 6.4+: In kernel	Package: In repo under "WALinuxAgent" Source code: GitHub
CoreOS	494.4.0+	In kernel	Source code: GitHub
Debian	Debian 7.9+, 8.2+, 9, 10	In kernel	Package: In repo under "waagent" Source code: GitHub
Oracle Linux	6.4+, 7.0+	In kernel	Package: In repo under "WALinuxAgent" Source code: GitHub
Red Hat Enterprise Linux	RHEL 6.7+, 7.1+, 8.0+	In kernel	Package: In repo under "WALinuxAgent" Source code: GitHub
SUSE Linux Enterprise	SLES/SLES for SAP 11 SP4 12 SP1+ 15	In kernel	Package: for 11 in Cloud:Tools repo for 12 included in "Public Cloud" Module under "python-azure-agent" Source code: GitHub

DISTRIBUTION	VERSION	DRIVERS	AGENT
openSUSE	openSUSE Leap 42.2+	In kernel	Package: In Cloud:Tools repo under "python-azure-agent" Source code: GitHub
Ubuntu	Ubuntu 12.04+ ¹	In kernel	Package: In repo under "walinuxagent" Source code: GitHub

- ¹ Information about extended support for Ubuntu 12.04 and 14.04 can be found here: [Ubuntu Extended Security Maintenance](#).

Image update cadence

Azure requires that the publishers of the endorsed Linux distributions regularly update their images in the Azure Marketplace with the latest patches and security fixes, at a quarterly or faster cadence. Updated images in the Azure Marketplace are available automatically to customers as new versions of an image SKU. More information about how to find Linux images: [Find Linux VM images in the Azure Marketplace](#).

Additional links

- [SUSE Public Cloud Image Lifecycle](#)

Azure-tuned kernels

Azure works closely with various endorsed Linux distributions to optimize the images that they published to the Azure Marketplace. One aspect of this collaboration is the development of "tuned" Linux kernels that are optimized for the Azure platform and delivered as fully supported components of the Linux distribution. The Azure-Tuned kernels incorporate new features and performance improvements, and at a faster (typically quarterly) cadence compared to the default or generic kernels that are available from the distribution.

In most cases you will find these kernels pre-installed on the default images in the Azure Marketplace, and so Azure customers will immediately get the benefit of these optimized kernels. More information about these Azure-Tuned kernels can be found in the following links:

- CentOS Azure-Tuned Kernel - Available via the CentOS Virtualization SIG - [More Info](#)
- Debian Cloud Kernel - Available with the Debian 10 and Debian 9 "backports" image on Azure - [More Info](#)
- SLES Azure-Tuned Kernel - [More Info](#)
- Ubuntu Azure-Tuned Kernel - [More Info](#)

Partners

CoreOS

<https://coreos.com/docs/running-coreos/cloud-providers/azure/>

From the CoreOS website:

CoreOS is designed for security, consistency, and reliability. Instead of installing packages via yum or apt, CoreOS uses Linux containers to manage your services at a higher level of abstraction. A single service's code and all dependencies are packaged within a container that can be run on one or many CoreOS machines.

Creativ

<https://www.creativ.co.uk/creativ-blog/debian-images-microsoft-azure>

Creativ is an independent consulting and services company that specializes in the development and

implementation of professional solutions by using free software. As leading open-source specialists, Credativ has international recognition with many IT departments that use their support. In conjunction with Microsoft, Credativ is currently preparing corresponding Debian images for Debian 8 (Jessie) and Debian before 7 (Wheezy). Both images are specially designed to run on Azure and can be easily managed via the platform. Credativ will also support the long-term maintenance and updating of the Debian images for Azure through its Open Source Support Centers.

Oracle

<https://www.oracle.com/technetwork/topics/cloud/faq-1963009.html>

Oracle's strategy is to offer a broad portfolio of solutions for public and private clouds. The strategy gives customers choice and flexibility in how they deploy Oracle software in Oracle clouds and other clouds. Oracle's partnership with Microsoft enables customers to deploy Oracle software in Microsoft public and private clouds with the confidence of certification and support from Oracle. Oracle's commitment and investment in Oracle public and private cloud solutions is unchanged.

Red Hat

<https://www.redhat.com/en/partners/strategic-alliance/microsoft>

The world's leading provider of open source solutions, Red Hat helps more than 90% of Fortune 500 companies solve business challenges, align their IT and business strategies, and prepare for the future of technology. Red Hat does this by providing secure solutions through an open business model and an affordable, predictable subscription model.

SUSE

<https://www.suse.com/suse-linux-enterprise-server-on-azure>

SUSE Linux Enterprise Server on Azure is a proven platform that provides superior reliability and security for cloud computing. SUSE's versatile Linux platform seamlessly integrates with Azure cloud services to deliver an easily manageable cloud environment. With more than 9,200 certified applications from more than 1,800 independent software vendors for SUSE Linux Enterprise Server, SUSE ensures that workloads running supported in the data center can be confidently deployed on Azure.

Canonical

<https://www.ubuntu.com/cloud/azure>

Canonical engineering and open community governance drive Ubuntu's success in client, server, and cloud computing, which includes personal cloud services for consumers. Canonical's vision of a unified, free platform in Ubuntu, from phone to cloud, provides a family of coherent interfaces for the phone, tablet, TV, and desktop. This vision makes Ubuntu the first choice for diverse institutions from public cloud providers to the makers of consumer electronics and a favorite among individual technologists.

With developers and engineering centers around the world, Canonical is uniquely positioned to partner with hardware makers, content providers, and software developers to bring Ubuntu solutions to market for PCs, servers, and handheld devices.

Azure Dedicated Hosts

1/9/2020 • 7 minutes to read • [Edit Online](#)

Azure Dedicated Host is a service that provides physical servers - able to host one or more virtual machines - dedicated to one Azure subscription. Dedicated hosts are the same physical servers used in our data centers, provided as a resource. You can provision dedicated hosts within a region, availability zone, and fault domain. Then, you can place VMs directly into your provisioned hosts, in whatever configuration best meets your needs.

Limitations

- Virtual machine scale sets are not currently supported on dedicated hosts.
- The following VM series are supported: DSv3, ESv3 and Fsv2.

Benefits

Reserving the entire host provides the following benefits:

- Hardware isolation at the physical server level. No other VMs will be placed on your hosts. Dedicated hosts are deployed in the same data centers and share the same network and underlying storage infrastructure as other, non-isolated hosts.
- Control over maintenance events initiated by the Azure platform. While the majority of maintenance events have little to no impact on your virtual machines, there are some sensitive workloads where each second of pause can have an impact. With dedicated hosts, you can opt-in to a maintenance window to reduce the impact to your service.
- With the Azure hybrid benefit, you can bring your own licenses for Windows and SQL to Azure. Using the hybrid benefits provides you with additional benefits. For more information, see [Azure Hybrid Benefit](#).

Groups, hosts, and VMs



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.

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.

When creating a VM in Azure, you can select which dedicated host to use for your VM. You have full control as to which VMs are placed on your hosts.

High Availability considerations

For high availability, you should deploy multiple VMs, spread across multiple hosts (minimum of 2). With Azure Dedicated Hosts, you have several options to provision your infrastructure to shape your fault isolation

boundaries.

Use Availability Zones for fault isolation

Availability zones are unique physical locations within an Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking. A host group is created in a single availability zone. Once created, all hosts will be placed within that zone. To achieve high availability across zones, you need to create multiple host groups (one per zone) and spread your hosts accordingly.

If you assign a host group to an availability zone, all VMs created on that host must be created in the same zone.

Use Fault Domains for fault isolation

A host can be created in a specific fault domain. Just like VM in a scale set or availability set, hosts in different fault domains will be placed on different physical racks in the data center. When you create a host group, you are required to specify the fault domain count. When creating hosts within the host group, you assign fault domain for each host. The VMs do not require any fault domain assignment.

Fault domains are not the same as collocation. Having the same fault domain for two hosts does not mean they are in proximity with each other.

Fault domains are scoped to the host group. You should not make any assumption on anti-affinity between two host groups (unless they are in different availability zones).

VMs deployed to hosts with different fault domains, will have their underlying managed disks services on multiple storage stamps, to increase the fault isolation protection.

Using Availability Zones and Fault Domains

You can use both capabilities together to achieve even more fault isolation. In this case, you will specify the availability zone and fault domain count in for each host group, assign a fault domain to each of your hosts in the group, and assign an availability zone to each of your VMs

The Resource Manager sample template found [here](#) uses zones and fault domains to spread hosts for maximum resiliency in a region.

Maintenance control

The infrastructure supporting your virtual machines may occasionally be updated to improve reliability, performance, security, and to launch new features. The Azure platform tries to minimize the impact of platform maintenance whenever possible, but customers with *maintenance sensitive* workloads can't tolerate even few seconds that the VM needs to be frozen or disconnected for maintenance.

Maintenance Control provides customers with an option to skip regular platform updates scheduled on their dedicated hosts, then apply it at the time of their choice within a 35-day rolling window.

NOTE

Maintenance control is currently in public preview. For more information, see [Control updates with Maintenance Control using CLI or PowerShell](#).

Capacity considerations

Once a dedicated host is provisioned, Azure assigns it to physical server. This guarantees the availability of the capacity when you need to provision your VM. Azure uses the entire capacity in the region (or zone) to pick a physical server for your host. It also means that customers can expect to be able to grow their dedicated host footprint without the concern of running out of space in the cluster.

Quotas

There is a default quota limit of 3000 vCPUs for dedicated hosts, per region. But, the number of hosts you can deploy is also limited by the quota for the VM size family used for the host. For example, a **Pay-as-you-go** subscription may only have a quota of 10 vCPUs available for the Dsv3 size series, in the East US region. In this case, you need to request a quota increase to at least 64 vCPUs before you can deploy a dedicated host. Select the **Request increase** button in the upper right corner to file a request if needed.

QUOTA	PROVIDER	LOCATION	USAGE
Standard DSV3 Family vCPUs	Microsoft.Compute	East US	0 % 0 of 10

For more information, see [Virtual machine vCPU quotas](#).

Free trial and MSDN subscriptions do not have quota for Azure Dedicated Hosts.

Pricing

Users are charged per dedicated host, regardless how many VMs are deployed. In your monthly statement you will see a new billable resource type of hosts. The VMs on a dedicated host will still be shown in your statement, but will carry a price of 0.

The host price is set based on VM family, type (hardware size), and region. A host price is relative to the largest VM size supported on the host.

Software licensing, storage and network usage are billed separately from the host and VMs. There is no change to those billable items.

For more information, see [Azure Dedicated Host pricing](#).

VM families and Hardware generations

A SKU is defined for a host and it represents the VM size series and type. You can mix multiple VMs of different sizes within a single host as long as they are of the same size series. The type is the hardware generation currently available in the region.

Different **types** for the same VM series will be from different CPU vendors and have different CPU generations and number of cores.

Refer to the host [pricing page](#) to learn more.

Dedicated hosts support the following host SKU\types: DSv3_Type1 and ESv3_Type1

Host life cycle

Azure monitors and manages the health status of your hosts. The following states will be returned when you query your host:

Health State	Description
Host Available	There are no known issues with your host.
Host Under Investigation	We're having some issues with the host which we're looking into. This is a transitional state required for Azure to try and identify the scope and root cause for the issue identified. Virtual machines running on the host may be impacted.
Host Pending Deallocate	Azure can't restore the host back to a healthy state and ask you to redeploy your virtual machines out of this host. If <code>autoReplaceOnFailure</code> is enabled, your virtual machines are <i>service healed</i> to healthy hardware. Otherwise, your virtual machine may be running on a host that is about to fail.
Host deallocated	All virtual machines have been removed from the host. You are no longer being charged for this host since the hardware was taken out of rotation.

Next steps

- You can deploy a dedicated host using the [Azure CLI](#), [portal](#), and [PowerShell](#).
- For more information, see the [Dedicated hosts](#) overview.
- There is sample template, found [here](#), that uses both zones and fault domains for maximum resiliency in a region.

Maintenance for virtual machines in Azure

2/10/2020 • 6 minutes to read • [Edit Online](#)

Azure periodically updates its platform to improve the reliability, performance, and security of the host infrastructure for virtual machines. The purpose of these updates ranges from patching software components in the hosting environment to upgrading networking components or decommissioning hardware.

Updates rarely affect the hosted VMs. When updates do have an effect, Azure chooses the least impactful method for updates:

- If the update doesn't require a reboot, the VM is paused while the host is updated, or the VM is live-migrated to an already updated host.
- If maintenance requires a reboot, you're notified of the planned maintenance. Azure also provides a time window in which you can start the maintenance yourself, at a time that works for you. The self-maintenance window is typically 30 days unless the maintenance is urgent. Azure is investing in technologies to reduce the number of cases in which planned platform maintenance requires the VMs to be rebooted. For instructions on managing planned maintenance, see [Handling planned maintenance notifications using the Azure CLI](#), [PowerShell](#) or [portal](#).

This page describes how Azure performs both types of maintenance. For more information about unplanned events (outages), see [Manage the availability of VMs for Windows](#) or the corresponding article for [Linux](#).

Within a VM, you can get notifications about upcoming maintenance by [using Scheduled Events for Windows](#) or for [Linux](#).

Maintenance that doesn't require a reboot

Most platform updates don't affect customer VMs. When a no-impact update isn't possible, Azure chooses the update mechanism that's least impactful to customer VMs.

Most nonzero-impact maintenance pauses the VM for less than 10 seconds. In certain cases, Azure uses memory-preserving maintenance mechanisms. These mechanisms pause the VM for up to 30 seconds and preserve the memory in RAM. The VM is then resumed, and its clock is automatically synchronized.

Memory-preserving maintenance works for more than 90 percent of Azure VMs. It doesn't work for G, M, N, and H series. Azure increasingly uses live-migration technologies and improves memory-preserving maintenance mechanisms to reduce the pause durations.

These maintenance operations that don't require a reboot are applied one fault domain at a time. They stop if they receive any warning health signals.

These types of updates can affect some applications. When the VM is live-migrated to a different host, some sensitive workloads might show a slight performance degradation in the few minutes leading up to the VM pause. To prepare for VM maintenance and reduce impact during Azure maintenance, try [using Scheduled Events for Windows](#) or [Linux](#) for such applications.

There is also a feature, maintenance control, in public preview that can help manage maintenance that doesn't require a reboot. You must be using either [Azure Dedicated Hosts](#) or an [isolated VM](#). Maintenance control gives you the option to skip platform updates and apply the updates at your choice of time within a 35-day rolling window. For more information, see [Control updates with Maintenance Control and the Azure CLI](#).

Live migration

Live migration is an operation that doesn't require a reboot and that preserves memory for the VM. It causes a

pause or freeze, typically lasting no more than 5 seconds. Except for G, M, N, and H series, all infrastructure as a service (IaaS) VMs, are eligible for live migration. Eligible VMs represent more than 90 percent of the IaaS VMs that are deployed to the Azure fleet.

The Azure platform starts live migration in the following scenarios:

- Planned maintenance
- Hardware failure
- Allocation optimizations

Some planned-maintenance scenarios use live migration, and you can use Scheduled Events to know in advance when live migration operations will start.

Live migration can also be used to move VMs when Azure Machine Learning algorithms predict an impending hardware failure or when you want to optimize VM allocations. For more information about predictive modeling that detects instances of degraded hardware, see [Improving Azure VM resiliency with predictive machine learning and live migration](#). Live-migration notifications appear in the Azure portal in the Monitor and Service Health logs as well as in Scheduled Events if you use these services.

Maintenance that requires a reboot

In the rare case where VMs need to be rebooted for planned maintenance, you'll be notified in advance. Planned maintenance has two phases: the self-service phase and a scheduled maintenance phase.

During the *self-service phase*, which typically lasts four weeks, you start the maintenance on your VMs. As part of the self-service, you can query each VM to see its status and the result of your last maintenance request.

When you start self-service maintenance, your VM is redeployed to an already updated node. Because the VM reboots, the temporary disk is lost and dynamic IP addresses associated with the virtual network interface are updated.

If an error arises during self-service maintenance, the operation stops, the VM isn't updated, and you get the option to retry the self-service maintenance.

When the self-service phase ends, the *scheduled maintenance phase* begins. During this phase, you can still query for the maintenance phase, but you can't start the maintenance yourself.

For more information on managing maintenance that requires a reboot, see **Handling planned maintenance notifications** using the Azure [CLI](#), [PowerShell](#) or [portal](#).

Availability considerations during scheduled maintenance

If you decide to wait until the scheduled maintenance phase, there are a few things you should consider to maintain the highest availability of your VMs.

Paired regions

Each Azure region is paired with another region within the same geographical vicinity. Together, they make a region pair. During the scheduled maintenance phase, Azure updates only the VMs in a single region of a region pair. For example, while updating the VM in North Central US, Azure doesn't update any VM in South Central US at the same time. However, other regions such as North Europe can be under maintenance at the same time as East US. Understanding how region pairs work can help you better distribute your VMs across regions. For more information, see [Azure region pairs](#).

Availability sets and scale sets

When deploying a workload on Azure VMs, you can create the VMs within an *availability set* to provide high availability to your application. Using availability sets, you can ensure that during either an outage or maintenance events that require a reboot, at least one VM is available.

Within an availability set, individual VMs are spread across up to 20 update domains. During scheduled

maintenance, only one update domain is updated at any given time. Update domains aren't necessarily updated sequentially.

Virtual machine *scale sets* are an Azure compute resource that you can use to deploy and manage a set of identical VMs as a single resource. The scale set is automatically deployed across UD, like VMs in an availability set. As with availability sets, when you use scale sets, only one UD is updated at any given time during scheduled maintenance.

For more information about setting up your VMs for high availability, see [Manage the availability of your VMs for Windows](#) or the corresponding article for [Linux](#).

Availability zones

Availability zones are unique physical locations within an Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking. To ensure resiliency, there's a minimum of three separate zones in all enabled regions.

An availability zone is a combination of a fault domain and an update domain. If you create three or more VMs across three zones in an Azure region, your VMs are effectively distributed across three fault domains and three update domains. The Azure platform recognizes this distribution across update domains to make sure that VMs in different zones are not updated at the same time.

Each infrastructure update rolls out zone by zone, within a single region. But, you can have deployment going on in Zone 1, and different deployment going in Zone 2, at the same time. Deployments are not all serialized. But, a single deployment only rolls out one zone at a time to reduce risk.

Next steps

You can use the [Azure CLI](#), [Azure PowerShell](#) or the [portal](#) to manage planned maintenance.

Introduction to Azure managed disks

12/16/2019 • 9 minutes to read • [Edit Online](#)

Azure managed disks are block-level storage volumes that are managed by Azure and used with Azure Virtual Machines. Managed disks are like a physical disk in an on-premises server but, virtualized. With managed disks, all you have to do is specify the disk size, the disk type, and provision the disk. Once you provision the disk, Azure handles the rest.

The available types of disks are ultra disks, premium solid-state drives (SSD), standard SSDs, and standard hard disk drives (HDD). For information about each individual disk type, see [Select a disk type for IaaS VMs](#).

Benefits of managed disks

Let's go over some of the benefits you gain by using managed disks.

Highly durable and available

Managed disks are designed for 99.999% availability. Managed disks achieve this by providing you with three replicas of your data, allowing for high durability. If one or even two replicas experience issues, the remaining replicas help ensure persistence of your data and high tolerance against failures. This architecture has helped Azure consistently deliver enterprise-grade durability for infrastructure as a service (IaaS) disks, with an industry-leading ZERO% annualized failure rate.

Simple and scalable VM deployment

Using managed disks, you can create up to 50,000 VM **disks** of a type in a subscription per region, allowing you to create thousands of **VMs** in a single subscription. This feature also further increases the scalability of [virtual machine scale sets](#) by allowing you to create up to 1,000 VMs in a virtual machine scale set using a Marketplace image.

Integration with availability sets

Managed disks are integrated with availability sets to ensure that the disks of [VMs in an availability set](#) are sufficiently isolated from each other to avoid a single point of failure. Disks are automatically placed in different storage scale units (stamps). If a stamp fails due to hardware or software failure, only the VM instances with disks on those stamps fail. For example, let's say you have an application running on five VMs, and the VMs are in an Availability Set. The disks for those VMs won't all be stored in the same stamp, so if one stamp goes down, the other instances of the application continue to run.

Integration with Availability Zones

Managed disks support [Availability Zones](#), which is a high-availability offering that protects your applications from datacenter failures. Availability Zones are unique physical locations within an Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking. To ensure resiliency, there's a minimum of three separate zones in all enabled regions. With Availability Zones, Azure offers industry best 99.99% VM uptime SLA.

Azure Backup support

To protect against regional disasters, [Azure Backup](#) can be used to create a backup job with time-based backups and backup retention policies. This allows you to perform easy VM restorations at will. Currently Azure Backup supports disk sizes up to four tebibyte (TiB) disks. Azure Backup supports backup and restore of managed disks. [Learn more](#) about Azure VM backup support.

Granular access control

You can use [Azure role-based access control \(RBAC\)](#) to assign specific permissions for a managed disk to one or more users. Managed disks expose a variety of operations, including read, write (create/update), delete, and retrieving a [shared access signature \(SAS\) URI](#) for the disk. You can grant access to only the operations a person needs to perform their job. For example, if you don't want a person to copy a managed disk to a storage account, you can choose not to grant access to the export action for that managed disk. Similarly, if you don't want a person to use an SAS URI to copy a managed disk, you can choose not to grant that permission to the managed disk.

Upload your vhd

Direct upload makes it easy to transfer your vhd to an Azure managed disk. Previously, you had to follow a more involved process that included staging your data in a storage account. Now, there are fewer steps. It is easier to upload on premises VMs to Azure, upload to large managed disks, and the backup and restore process is simplified. It also reduces cost by allowing you to upload data to managed disks directly without attaching them to VMs. You can use direct upload to upload vhds up to 32 TiB in size.

To learn how to transfer your vhd to Azure, see the [CLI](#) or [PowerShell](#) articles.

Encryption

Managed disks offer two different kinds of encryption. The first is Server Side Encryption (SSE), which is performed by the storage service. The second one is Azure Disk Encryption (ADE), which you can enable on the OS and data disks for your VMs.

Server-side encryption

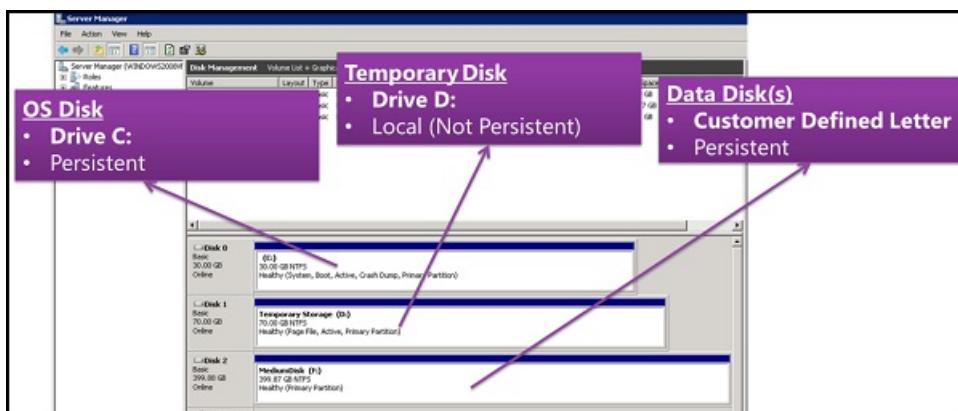
[Azure Server-side Encryption](#) provides encryption-at-rest and safeguards your data to meet your organizational security and compliance commitments. Server-side encryption is enabled by default for all managed disks, snapshots, and images in all the regions where managed disks are available. You can either allow Azure to manage your keys for you, these are platform-managed keys, or you can manage the keys yourself, these are customer-managed keys. Visit the [Managed Disks FAQ page](#) for more details.

Azure Disk Encryption

Azure Disk Encryption allows you to encrypt the OS and Data disks used by an IaaS Virtual Machine. This encryption includes managed disks. For Windows, the drives are encrypted using industry-standard BitLocker encryption technology. For Linux, the disks are encrypted using the DM-Crypt technology. The encryption process is integrated with Azure Key Vault to allow you to control and manage the disk encryption keys. For more information, see [Azure Disk Encryption for IaaS VMs](#).

Disk roles

There are three main disk roles in Azure: the data disk, the OS disk, and the temporary disk. These roles map to disks that are attached to your virtual machine.



Data disk

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 that you choose. Each data disk has a maximum capacity of 32,767 gibibytes (GiB). The size of the virtual machine determines how many data disks you can attach to it and the type of storage you can use to host the disks.

OS disk

Every virtual machine has one attached operating system disk. That OS disk has a pre-installed OS, which was selected when the VM was created. This disk contains the boot volume.

This disk has a maximum capacity of 2,048 GiB.

Temporary disk

Every VM contains a temporary disk, which is not a managed disk. The temporary disk provides short-term storage for applications and processes and is intended to only store data such as page or swap files. Data on the temporary disk may be lost during a [maintenance event](#) event or when you [redeploy a VM](#). On Azure Linux VMs, the temporary disk is /dev/sdb by default and on Windows VMs the temporary disk is D: by default. During a successful standard reboot of the VM, the data on the temporary disk will persist.

Managed disk snapshots

A managed disk snapshot is a read-only crash-consistent full copy of a managed disk that is stored as a standard managed disk by default. With snapshots, you can back up your managed disks at any point in time. These snapshots exist independent of the source disk and can be used to create new managed disks.

Snapshots are billed based on the used size. For example, if you create a snapshot of a managed disk with provisioned capacity of 64 GiB and actual used data size of 10 GiB, that snapshot is billed only for the used data size of 10 GiB. You can see the used size of your snapshots by looking at the [Azure usage report](#). For example, if the used data size of a snapshot is 10 GiB, the **daily** usage report will show $10 \text{ GiB} / (31 \text{ days}) = 0.3226$ as the consumed quantity.

To learn more about how to create snapshots for managed disks, see the following resources:

- [Create a snapshot of a managed disk in Windows](#)
- [Create a snapshot of a managed disk in Linux](#)

Images

Managed disks also support creating a managed custom image. You can create an image from your custom VHD in a storage account or directly from a generalized (sysprepped) VM. This process captures a single image. This image contains all managed disks associated with a VM, including both the OS and data disks. This managed custom image enables creating hundreds of VMs using your custom image without the need to copy or manage any storage accounts.

For information on creating images, see the following articles:

- [How to capture a managed image of a generalized VM in Azure](#)
- [How to generalize and capture a Linux virtual machine using the Azure CLI](#)

Images versus snapshots

It's important to understand the difference between images and snapshots. With managed disks, you can take an image of a generalized VM that has been deallocated. This image includes all of the disks attached to the VM. You can use this image to create a VM, and it includes all of the disks.

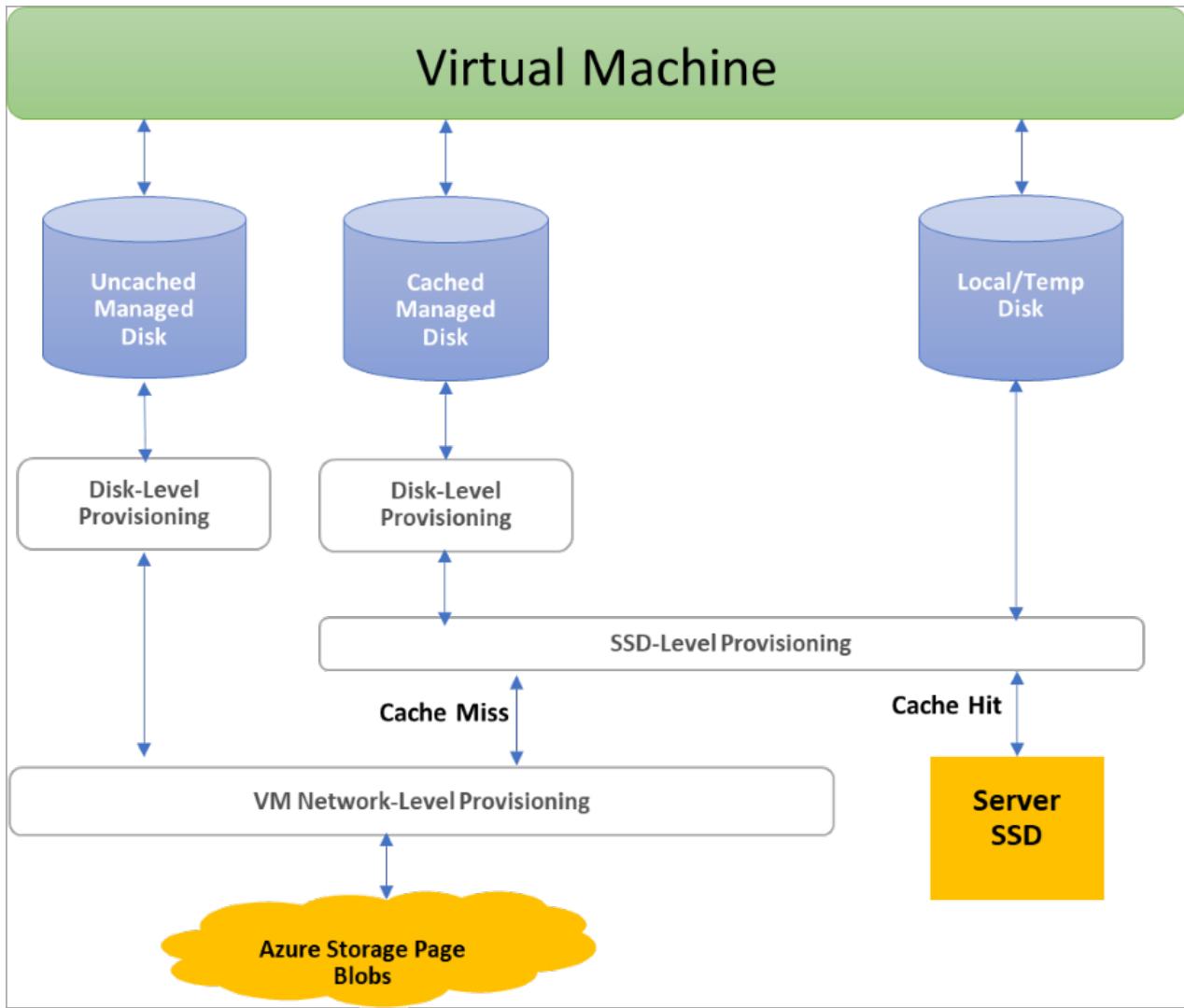
A snapshot is a copy of a disk at the point in time the snapshot is taken. It applies only to one disk. If you have a VM that has one disk (the OS disk), you can take a snapshot or an image of it and create a VM from either the snapshot or the image.

A snapshot doesn't have awareness of any disk except the one it contains. This makes it problematic to use in

scenarios that require the coordination of multiple disks, such as striping. Snapshots would need to be able to coordinate with each other and this is currently not supported.

Disk allocation and performance

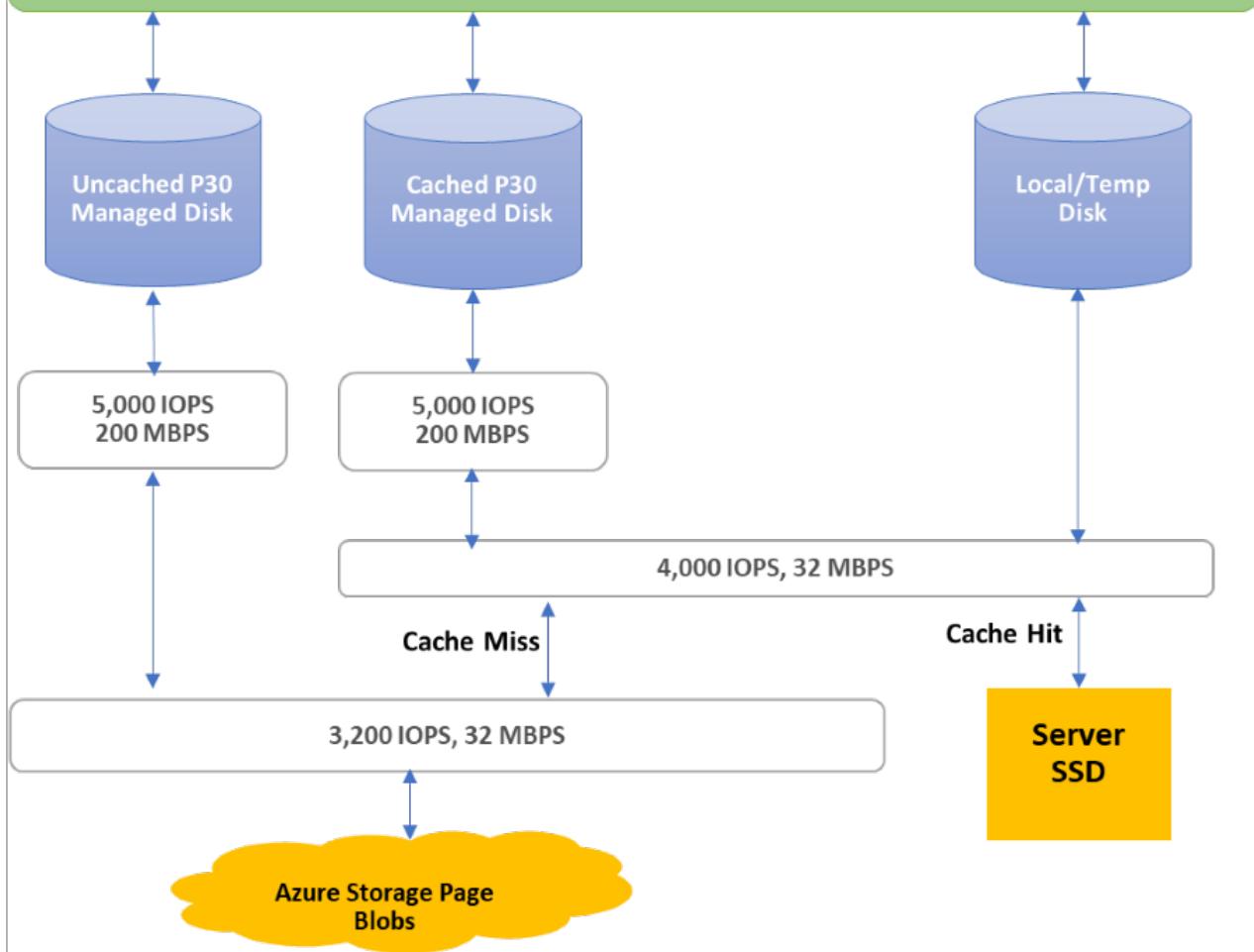
The following diagram depicts real-time allocation of bandwidth and IOPS for disks, using a three-level provisioning system:



The first level provisioning sets the per-disk IOPS and bandwidth assignment. At the second level, compute server host implements SSD provisioning, applying it only to data that is stored on the server's SSD, which includes disks with caching (ReadWrite and ReadOnly) as well as local and temp disks. Finally, VM network provisioning takes place at the third level for any I/O that the compute host sends to Azure Storage's backend. With this scheme, the performance of a VM depends on a variety of factors, from how the VM uses the local SSD, to the number of disks attached, as well as the performance and caching type of the disks it has attached.

As an example of these limitations, a Standard_DS1v1 VM is prevented from achieving the 5,000 IOPS potential of a P30 disk, whether it is cached or not, because of limits at the SSD and network levels:

Virtual Machine: Standard_DS1v1



Azure uses prioritized network channel for disk traffic, which gets the precedence over other low priority of network traffic. This helps disks maintain their expected performance in case of network contentions. Similarly, Azure Storage handles resource contentions and other issues in the background with automatic load balancing. Azure Storage allocates required resources when you create a disk, and applies proactive and reactive balancing of resources to handle the traffic level. This further ensures disks can sustain their expected IOPS and throughput targets. You can use the VM-level and Disk-level metrics to track the performance and setup alerts as needed.

Refer to our [design for high performance](#) article, to learn the best practices for optimizing VM + Disk configurations so that you can achieve your desired performance

Next steps

If you'd like a video going into more detail on managed disks, check out: [Better Azure VM Resiliency with Managed Disks](#).

Learn more about the individual disk types Azure offers, which type is a good fit for your needs, and learn about their performance targets in our article on disk types.

[Select a disk type for IaaS VMs](#)

What disk types are available in Azure?

11/12/2019 • 13 minutes to read • [Edit Online](#)

Azure managed disks currently offers four disk types, each type is aimed towards specific customer scenarios.

Disk comparison

The following table provides a comparison of ultra disks, premium solid-state drives (SSD), standard SSD, and standard hard disk drives (HDD) for managed disks to help you decide what to use.

	ULTRA DISK	PREMIUM SSD	STANDARD SSD	STANDARD HDD
Disk type	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	Web servers, lightly used enterprise applications and dev/test	Backup, non-critical, infrequent access
Max disk size	65,536 gibibyte (GiB)	32,767 GiB	32,767 GiB	32,767 GiB
Max throughput	2,000 MiB/s	900 MiB/s	750 MiB/s	500 MiB/s
Max IOPS	160,000	20,000	6,000	2,000

Ultra disk

Azure ultra disks deliver high throughput, high IOPS, and consistent low latency disk storage for Azure IaaS VMs. Some additional benefits of ultra disks include the ability to dynamically change the performance of the disk, along with your workloads, without the need to restart your virtual machines (VM). Ultra disks are suited for data-intensive workloads such as SAP HANA, top tier databases, and transaction-heavy workloads. Ultra disks can only be used as data disks. We recommend using premium SSDs as OS disks.

Performance

When you provision an ultra disk, you can independently configure the capacity and the performance of the disk. Ultra disks come in several fixed sizes, ranging from 4 GiB up to 64 TiB, and feature a flexible performance configuration model that allows you to independently configure IOPS and throughput.

Some key capabilities of ultra disks are:

- Disk capacity: Ultra disks capacity ranges from 4 GiB up to 64 TiB.
- Disk IOPS: Ultra disks support IOPS limits of 300 IOPS/GiB, up to a maximum of 160 K IOPS per disk. To achieve the IOPS that you provisioned, ensure that the selected Disk IOPS are less than the VM IOPS limit. The minimum IOPS per disk is 2 IOPS/GiB, with an overall baseline minimum of 100 IOPS. For example, if you had a 4 GiB ultra disk, you will have a minimum of 100 IOPS, instead of eight IOPS.
- Disk throughput: With ultra disks, the throughput limit of a single disk is 256 KiB/s for each provisioned IOPS, up to a maximum of 2000 MBps per disk (where MBps = 10^6 Bytes per second). The minimum throughput

per disk is 4KiB/s for each provisioned IOPS, with an overall baseline minimum of 1 MBps.

- Ultra disks support adjusting the disk performance attributes (IOPS and throughput) at runtime without detaching the disk from the virtual machine. Once a disk performance resize operation has been issued on a disk, it can take up to an hour for the change to actually take effect. There is a limit of four performance resize operations during a 24 hour window. It is possible for a performance resize operation to fail due to a lack of performance bandwidth capacity.

Disk size

DISK SIZE (GIB)	IOPS CAP	THROUGHPUT CAP (MBPS)
4	1,200	300
8	2,400	600
16	4,800	1,200
32	9,600	2,000
64	19,200	2,000
128	38,400	2,000
256	76,800	2,000
512	80,000	2,000
1,024-65,536 (sizes in this range increasing in increments of 1 TiB)	160,000	2,000

GA scope and limitations

For now, ultra disks have additional limitations, they are as follows:

- Are supported in the following regions, with a varying number of availability zones per region:
 - East US 2
 - East US
 - West US 2
 - SouthEast Asia
 - North Europe
 - West Europe
 - UK South
- Can only be used with availability zones (availability sets and single VM deployments outside of zones will not have the ability to attach an ultra disk)
- Are only supported on the following VM series:
 - [ESv3](#)
 - [DSv3](#)
 - [FSv2](#)
 - [M](#)
 - [Mv2](#)
- Not every VM size is available in every supported region with ultra disks
- Are only available as data disks and only support 4k physical sector size. Due to the 4K native sector size of Ultra Disk, there are some applications that won't be compatible with ultra disks. One example would be Oracle

Database, which requires release 12.2 or later in order to support ultra disks.

- Can only be created as empty disks
- Do not yet support disk snapshots, VM images, availability sets, and Azure disk encryption
- Do not yet support integration with Azure Backup or Azure Site Recovery
- The current maximum limit for IOPS on GA VMs is 80,000.
- If you would like to participate in a limited preview of a VM that can accomplish 160,000 IOPS with ultra disks, please email UltraDiskFeedback@microsoft.com

If you would like to start using ultra disks, see our article on the subject: [Using Azure ultra disks](#).

Premium SSD

Azure premium SSDs deliver high-performance and low-latency disk support for virtual machines (VMs) with input/output (IO)-intensive workloads. To take advantage of the speed and performance of premium storage disks, you can migrate existing VM disks to Premium SSDs. Premium SSDs are suitable for mission-critical production applications. Premium SSDs can only be used with VM series that are premium storage-compatible.

To learn more about individual VM types and sizes in Azure for Windows, including which sizes are premium storage-compatible, see [Windows VM sizes](#). To learn more about individual VM types and sizes in Azure for Linux, including which sizes are premium storage-compatible, see [Linux VM sizes](#).

Disk size

PRE MIU M SSD SIZE S	P1*	P2*	P3*	P4	P6	P10	P15	P20	P30	P40	P50	P60	P70	P80
Disk size in GiB	4	8	16	32	64	128	256	512	1,02 4	2,04 8	4,09 6	8,19 2	16,3 84	32,7 67
IOP S per disk	120	120	120	120	240	500	1,1 00	2,30 0	5,00 0	7,50 0	7,50 0	16,0 00	18,0 00	20,0 00
Thr oug hpu t per disk	25 MiB /sec	25 MiB /sec	25 MiB /sec	25 MiB /sec	50 MiB /sec	100 MiB /sec	125 MiB /sec	150 MiB /sec	200 MiB /sec	250 MiB /sec	250 MiB /sec	500 MiB /sec	750 MiB /sec	900 MiB /sec
Max bur st IOP S per disk **	3,5 00	3,5 00	3,5 00	3,5 00	3,5 00	3,5 00	3,5 00	3,5 0	3,50 0					

PRE MIU M SSD SIZE S	P1*	P2*	P3*	P4	P6	P10	P15	P20	P30	P40	P50	P60	P70	P80
Max burst throughput per disk **	170 MiB /sec													
Max burst duration**	30 min													
Eligible for reservation	No	Yes, up to one year												

*Denotes a disk size that is currently in preview, for regional availability information see [New disk sizes: Managed and unmanaged](#).

**Denotes a feature that is currently in preview, see [Disk bursting](#) for more information.

When you provision a premium storage disk, unlike standard storage, you are guaranteed the capacity, IOPS, and throughput of that disk. For example, if you create a P50 disk, Azure provisions 4,095-GB storage capacity, 7,500 IOPS, and 250-MB/s throughput for that disk. Your application can use all or part of the capacity and performance. Premium SSD disks are designed to provide low single-digit millisecond latencies and target IOPS and throughput described in the preceding table 99.9% of the time.

Bursting (preview)

Premium SSD sizes smaller than P30 now offer disk bursting (preview) and can burst their IOPS per disk up to 3,500 and their bandwidth up to 170 Mbps. Bursting is automated and operates based on a credit system. Credits are automatically accumulated in a burst bucket when disk traffic is below the provisioned performance target and credits are automatically consumed when traffic bursts beyond the target, up to the max burst limit. The max burst limit defines the ceiling of disk IOPS & Bandwidth even if you have burst credits to consume from. Disk bursting provides better tolerance on unpredictable changes of IO patterns. You can best leverage it for OS disk boot and applications with spiky traffic.

Disk bursting support will be enabled on new deployments of applicable disk sizes in the [preview regions](#) by default, with no user action required. For existing disks of the applicable sizes, you can enable bursting with either of two options: detach and reattach the disk or stop and restart the attached VM. All burst applicable disk sizes will start with a full burst credit bucket when the disk is attached to a Virtual Machine that supports a max duration at peak burst limit of 30 mins. To learn more about how bursting work on Azure Disks, see [Premium SSD bursting](#).

Transactions

For premium SSDs, each I/O operation less than or equal to 256 KiB of throughput is considered a single I/O operation. I/O operations larger than 256 KiB of throughput are considered multiple I/Os of size 256 KiB.

Standard SSD

Azure standard SSDs are a cost-effective storage option optimized for workloads that need consistent performance at lower IOPS levels. Standard SSD offers a good entry level experience for those who wish to move to the cloud, especially if you experience issues with the variance of workloads running on your HDD solutions on premises. Compared to standard HDDs, standard SSDs deliver better availability, consistency, reliability, and latency. Standard SSDs are suitable for Web servers, low IOPS application servers, lightly used enterprise applications, and Dev/Test workloads. Like standard HDDs, standard SSDs are available on all Azure VMs.

Disk size

STANDBY RD SSD SIZE S	E1*	E2*	E3*	E4	E6	E10	E15	E20	E30	E40	E50	E60	E70	E80
Disk size in GiB	4	8	16	32	64	128	256	512	1,024	2,048	4,096	8,192	16,384	32,767
IOPS per disk	Up to 120	Up to 120	Up to 120	Up to 120	Up to 240	Up to 500	Up to 2,000	Up to 4,000	Up to 6,000					
Throughput per disk	Up to 25 MiB /sec	Up to 50 MiB /sec	Up to 60 MiB /sec	Up to 400 MiB /sec	Up to 600 MiB /sec	Up to 750 MiB /sec								

*Denotes a disk size that is currently in preview, for regional availability information see [New disk sizes: Managed and unmanaged](#).

Standard SSDs are designed to provide single-digit millisecond latencies and the IOPS and throughput up to the limits described in the preceding table 99% of the time. Actual IOPS and throughput may vary sometimes depending on the traffic patterns. Standard SSDs will provide more consistent performance than the HDD disks with the lower latency.

Transactions

For standard SSDs, each I/O operation less than or equal to 256 KiB of throughput is considered a single I/O operation. I/O operations larger than 256 KiB of throughput are considered multiple I/Os of size 256 KiB. These transactions have a billing impact.

Standard HDD

Azure standard HDDs deliver reliable, low-cost disk support for VMs running latency-insensitive workloads. With standard storage, the data is stored on hard disk drives (HDDs). Latency, IOPS, and Throughput of Standard HDD disks may vary more widely as compared to SSD-based disks. Standard HDD Disks are designed to deliver write latencies under 10ms and read latencies under 20ms for most IO operations, however the actual performance may vary depending on the IO size and workload pattern. When working with VMs, you can use standard HDD

disks for dev/test scenarios and less critical workloads. Standard HDDs are available in all Azure regions and can be used with all Azure VMs.

Disk size

STANDARD DISK TYPE	S4	S6	S10	S15	S20	S30	S40	S50	S60	S70	S80
Disk size in GiB	32	64	128	256	512	1,024	2,048	4,096	8,192	16,384	32,767
IOPS per disk	Up to 500	Up to 1,300	Up to 2,000	Up to 2,000							
Throughput per disk	Up to 60 MiB/s ec	Up to 300 MiB/s ec	Up to 500 MiB/s ec	Up to 500 MiB/s ec							

Transactions

For Standard HDDs, each IO operation is considered as a single transaction, regardless of the I/O size. These transactions have a billing impact.

Billing

When using managed disks, the following billing considerations apply:

- Disk type
- managed disk Size
- Snapshots
- Outbound data transfers
- Number of transactions

Managed disk size: managed disks are billed on the provisioned size. Azure maps the provisioned size (rounded up) to the nearest offered disk size. For details of the disk sizes offered, see the previous tables. Each disk maps to a supported provisioned disk size offering and is billed accordingly. For example, if you provisioned a 200 GiB Standard SSD, it maps to the disk size offer of E15 (256 GiB). Billing for any provisioned disk is prorated hourly by using the monthly price for the Premium Storage offer. For example, if you provisioned an E10 disk and deleted it after 20 hours, you're billed for the E10 offering prorated to 20 hours. This is regardless of the amount of actual data written to the disk.

Snapshots: Snapshots are billed based on the size used. For example, if you create a snapshot of a managed disk with provisioned capacity of 64 GiB and actual used data size of 10 GiB, the snapshot is billed only for the used data size of 10 GiB.

For more information on snapshots, see the section on snapshots in the [managed disk overview](#).

Outbound data transfers: [Outbound data transfers](#) (data going out of Azure data centers) incur billing for bandwidth usage.

Transactions: You're billed for the number of transactions that you perform on a standard managed disk. For standard SSDs, each I/O operation less than or equal to 256 KiB of throughput is considered a single I/O operation. I/O operations larger than 256 KiB of throughput are considered multiple I/Os of size 256 KiB. For

Standard HDDs, each IO operation is considered as a single transaction, regardless of the I/O size.

For detailed information on pricing for Managed Disks, including transaction costs, see [Managed Disks Pricing](#).

Ultra disk VM reservation fee

Azure VMs have the capability to indicate if they are compatible with ultra disks. An ultra disk compatible VM allocates dedicated bandwidth capacity between the compute VM instance and the block storage scale unit to optimize the performance and reduce latency. Adding this capability on the VM results in a reservation charge that is only imposed if you enabled ultra disk capability on the VM without attaching an ultra disk to it. When an ultra disk is attached to the ultra disk compatible VM, this charge would not be applied. This charge is per vCPU provisioned on the VM.

NOTE

For [constrained core VM sizes](#), the reservation fee is based on the actual number of vCPUs and not the constrained cores.

For Standard_E32-8s_v3, the reservation fee will be based on 32 cores.

Refer to the [Azure Disks pricing page](#) for ultra disk pricing details.

Azure disk reservation

Disk reservation is the option to purchase one year of disk storage in advance at a discount, reducing your total cost. When purchasing a disk reservation, you select a specific Disk SKU in a target region, for example, 10 P30 (1TiB) premium SSDs in East US 2 region for a one year term. The reservation experience is similar to reserved virtual machine (VM) instances. You can bundle VM and Disk reservations to maximize your savings. For now, Azure Disks Reservation offers one year commitment plan for premium SSD SKUs from P30 (1TiB) to P80 (32 TiB) in all production regions. For more details on the Reserved Disks pricing, see [Azure Disks pricing page](#).

Server side encryption of Azure managed disks

2/14/2020 • 10 minutes to read • [Edit Online](#)

Azure managed disks automatically encrypt your data by default when persisting it to the cloud. Server-side encryption protects your data and helps you meet your organizational security and compliance commitments. Data in Azure managed disks is encrypted transparently using 256-bit [AES encryption](#), one of the strongest block ciphers available, and is FIPS 140-2 compliant.

Encryption does not impact the performance of managed disks. There is no additional cost for the encryption.

For more information about the cryptographic modules underlying Azure managed disks, see [Cryptography API: Next Generation](#)

About encryption key management

You can rely on platform-managed keys for the encryption of your managed disk, or you can manage encryption using your own keys. If you choose to manage encryption with your own keys, you can specify a *customer-managed key* to use for encrypting and decrypting all data in managed disks.

The following sections describe each of the options for key management in greater detail.

Platform-managed keys

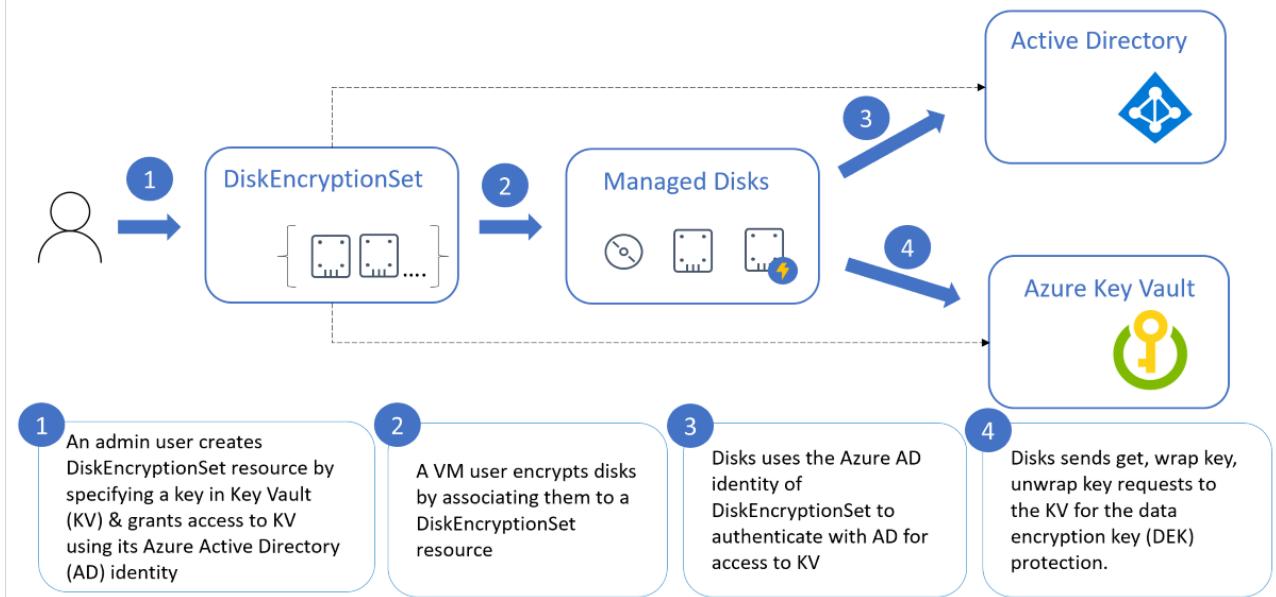
By default, managed disks use platform-managed encryption keys. As of June 10, 2017, all new managed disks, snapshots, images, and new data written to existing managed disks are automatically encrypted-at-rest with platform-managed keys.

Customer-managed keys

You can choose to manage encryption at the level of each managed disk, with your own keys. Server-side encryption for managed disks with customer-managed keys offers an integrated experience with Azure Key Vault. You can either import [your RSA keys](#) to your Key Vault or generate new RSA keys in Azure Key Vault. Azure managed disks handles the encryption and decryption in a fully transparent fashion using [envelope encryption](#). It encrypts data using an [AES 256](#) based data encryption key (DEK), which is, in turn, protected using your keys. You have to grant access to managed disks in your Key Vault to use your keys for encrypting and decrypting the DEK. This allows you full control of your data and keys. You can disable your keys or revoke access to managed disks at any time. You can also audit the encryption key usage with Azure Key Vault monitoring to ensure that only managed disks or other trusted Azure services are accessing your keys.

The following diagram shows how managed disks use Azure Active Directory and Azure Key Vault to make requests using the customer-managed key:

SSE+CMK Workflow



The following list explains the diagram in even more detail:

- 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.
- 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.

To revoke access to customer-managed keys, see [Azure Key Vault PowerShell](#) and [Azure Key Vault CLI](#). Revoking access effectively blocks access to all data in the storage account, as the encryption key is inaccessible by Azure Storage.

Supported regions

Only the following regions are currently supported:

- Available as a GA offering in the East US, West US 2, and South Central US regions.
- Available as a public preview in the West Central US, East US 2, Canada Central, and North Europe regions.

Restrictions

For now, customer-managed keys have the following restrictions:

- Only "soft" and "hard" RSA keys of size 2048 are supported, no other keys or sizes.
- Disks created from custom images that are encrypted using server-side encryption and customer-managed keys must be encrypted using the same customer-managed keys and must be in the same subscription.

- Snapshots created from disks that are encrypted with server-side encryption and customer-managed keys must be encrypted with the same customer-managed keys.
- Custom images encrypted using server-side encryption and customer-managed keys cannot be used in the shared image gallery.
- All resources related to your customer-managed keys (Azure Key Vaults, disk encryption sets, VMs, disks, and snapshots) must be in the same subscription and region.
- Disks, snapshots, and images encrypted with customer-managed keys cannot move to another subscription.
- If you use the Azure portal to create your disk encryption set, you cannot use snapshots for now.

CLI

Setting up your Azure Key Vault and DiskEncryptionSet

1. Make sure that you have installed the latest [Azure CLI](#) and logged to an Azure account in with [az login](#).
2. Create an instance of Azure Key Vault and encryption key.

When creating the Key Vault instance, you must enable soft delete and purge protection. Soft delete ensures that the Key Vault holds a deleted key for a given retention period (90 day default). Purge protection ensures that a deleted key cannot be permanently deleted until the retention period lapses. These settings protect you from losing data due to accidental deletion. These settings are mandatory when using a Key Vault for encrypting managed disks.

```
subscriptionId=yourSubscriptionID
rgName=yourResourceGroupName
location=WestCentralUS
keyVaultName=yourKeyVaultName
keyName=yourKeyName
diskEncryptionSetName=yourDiskEncryptionSetName
diskName=yourDiskName

az account set --subscription $subscriptionId

az keyvault create -n $keyVaultName -g $rgName -l $location --enable-purge-protection true --enable-soft-delete true

az keyvault key create --vault-name $keyVaultName -n $keyName --protection software
```

3. Create an instance of a DiskEncryptionSet.

```
keyVaultId=$(az keyvault show --name $keyVaultName --query [id] -o tsv)

keyVaultKeyUrl=$(az keyvault key show --vault-name $keyVaultName --name $keyName --query [key.kid] -o tsv)

az disk-encryption-set create -n $diskEncryptionSetName -l $location -g $rgName --source-vault $keyVaultId --key-url $keyVaultKeyUrl
```

4. Grant the DiskEncryptionSet resource access to the key vault.

NOTE

It may take few minutes for Azure to create the identity of your DiskEncryptionSet in your Azure Active Directory. If you get an error like "Cannot find the Active Directory object" when running the following command, wait a few minutes and try again.

```

desIdentity=$(az disk-encryption-set show -n $diskEncryptionSetName -g $rgName --query
[identity.principalId] -o tsv)

az keyvault set-policy -n $keyVaultName -g $rgName --object-id $desIdentity --key-permissions wrapkey
unwrapkey get

az role assignment create --assignee $desIdentity --role Reader --scope $keyVaultId

```

Create a VM using a Marketplace image, encrypting the OS and data disks with customer-managed keys

```

rgName=yourResourceGroupName
vmName=yourVMName
location=WestCentralUS
vmSize=Standard_DS3_V2
image=UbuntuLTS
diskEncryptionSetName=yourDiskEncryptionSetName

diskEncryptionSetId=$(az disk-encryption-set show -n $diskEncryptionSetName -g $rgName --query [id] -o tsv)

az vm create -g $rgName -n $vmName -l $location --image $image --size $vmSize --generate-ssh-keys --os-disk-
encryption-set $diskEncryptionSetId --data-disk-sizes-gb 128 128 --data-disk-encryption-sets
$diskEncryptionSetId $diskEncryptionSetId

```

Encrypt existing unattached managed disks

Your existing disks must not be attached to a running VM in order for you to encrypt them using the following script:

```

rgName=yourResourceGroupName
diskName=yourDiskName
diskEncryptionSetName=yourDiskEncryptionSetName

az disk update -n $diskName -g $rgName --encryption-type EncryptionAtRestWithCustomerKey --disk-encryption-set
$diskEncryptionSetId

```

Create a virtual machine scale set using a Marketplace image, encrypting the OS and data disks with customer-managed keys

```

rgName=yourResourceGroupName
vmssName=yourVMSName
location=WestCentralUS
vmSize=Standard_DS3_V2
image=UbuntuLTS
diskEncryptionSetName=yourDiskEncryptionSetName

diskEncryptionSetId=$(az disk-encryption-set show -n $diskEncryptionSetName -g $rgName --query [id] -o tsv)
az vmss create -g $rgName -n $vmssName --image UbuntuLTS --upgrade-policy automatic --admin-username azureuser
--generate-ssh-keys --os-disk-encryption-set $diskEncryptionSetId --data-disk-sizes-gb 64 128 --data-disk-
encryption-sets $diskEncryptionSetId $diskEncryptionSetId

```

Create an empty disk encrypted using server-side encryption with customer-managed keys and attach it to a VM

```

vmName=yourVMName
rgName=yourResourceGroupName
diskName=yourDiskName
diskSkuName=Premium_LRS
diskSizeinGiB=30
location=WestCentralUS
diskLUN=2
diskEncryptionSetName=yourDiskEncryptionSetName

```

```

diskEncryptionSetId=$(az disk-encryption-set show -n $diskEncryptionSetName -g $rgName --query [id] -o tsv)

az disk create -n $diskName -g $rgName -l $location --encryption-type EncryptionAtRestWithCustomerKey --disk-encryption-set $diskEncryptionSetId --size-gb $diskSizeinGiB --sku $diskSkuName

diskId=$(az disk show -n $diskName -g $rgName --query [id] -o tsv)

az vm disk attach --vm-name $vmName --lun $diskLUN --ids $diskId

```

IMPORTANT

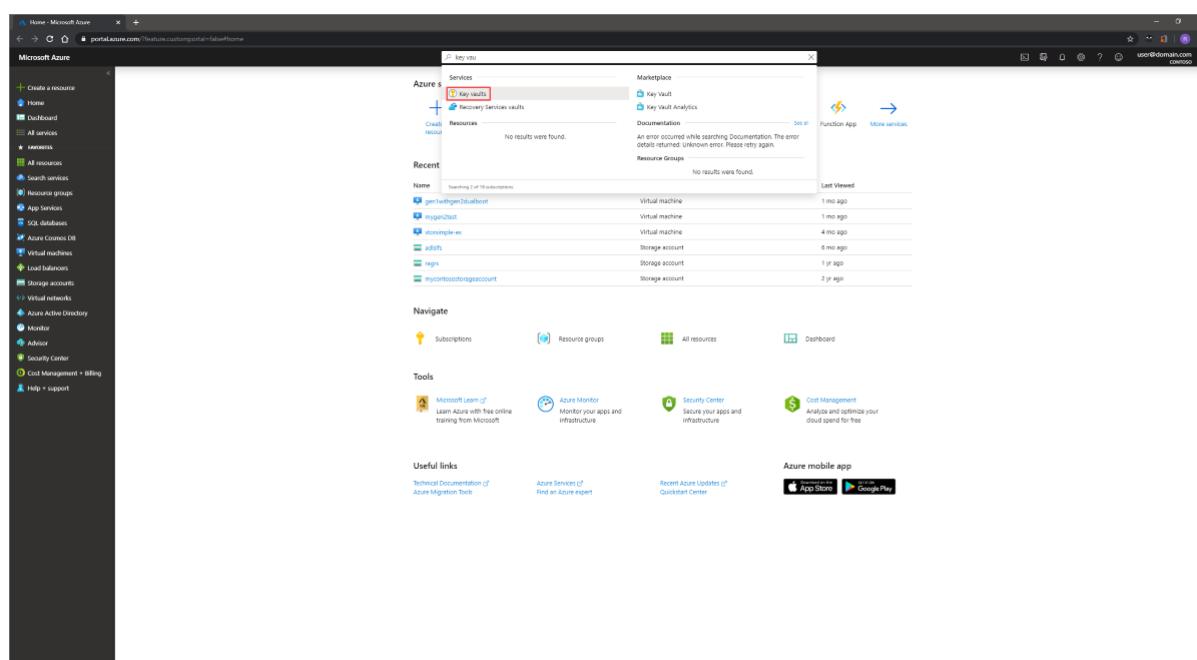
Customer-managed keys rely on managed identities for Azure resources, a feature of Azure Active Directory (Azure AD). When you configure customer-managed keys, a managed identity is automatically assigned to your resources under the covers. If you subsequently move the subscription, resource group, or managed disk from one Azure AD directory to another, the managed identity associated with managed disks is not transferred to the new tenant, so customer-managed keys may no longer work. For more information, see [Transferring a subscription between Azure AD directories](#).

Portal

Setting up customer-managed keys for your disks will require you to create resources in a particular order, if you're doing it for the first time. First, you will need to create and set up an Azure Key Vault.

Setting up your Azure Key Vault

1. Sign into the [Azure portal](#) and search for Key Vault
2. Search for and select **Key Vaults**.



IMPORTANT

Your Azure key vault, disk encryption set, VM, disks, and snapshots must all be in the same region and subscription for deployment to succeed.

3. Select **+Add** to create a new Key Vault.
4. Create a new resource group
5. Enter a key vault name, select a region, and select a pricing tier.
6. Select **Review + Create**, verify your choices, then select **Create**.

The screenshot shows the 'Create key vault' wizard in the Azure portal. The current step is 'Access policy'. At the bottom, there is a 'Create new' button for 'Resource group'. A modal window is open, asking for a 'Name' for the new resource group. The modal also contains a descriptive text about what a resource group is: 'A resource group is a container that holds related resources for an Azure solution.'

Dashboard > Key vaults > Create key vault

Create key vault

Basics **Access policy** **Networking** **Tags** **Review + create**

Azure Key Vault is a cloud service used to manage keys, secrets, and certificates. Key Vault eliminates the need for developers to store security information in their code. It allows you to centralize the storage of your application secrets which greatly reduces the chances that secrets may be leaked. Key Vault also allows you to securely store secrets and keys backed by Hardware Security Modules or HSMs. The HSMs used are Federal Information Processing Standards (FIPS) 140-2 Level 2 validated. In addition, key vault provides logs of all access and usage attempts of your secrets so you have a complete audit trail for compliance. [Learn more](#)

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

Subscription *: My Example Subscription

Resource group *:
Select existing... [Create new](#)

Instance details

Key vault name * ⓘ

Region *

Pricing tier * ⓘ

Review + create < Prev OK Cancel

7. Once your key vault finishes deploying, select it.
8. Select **Keys** under **Settings**.
9. Select **Generate/Import**

The screenshot shows the 'my-example-vault - Keys' page in the Azure portal. On the left, there's a sidebar with icons for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Events (preview), Settings, Keys (which is selected and highlighted with a red box), Secrets, and Certificates. At the top right, there are buttons for Generate/Import (highlighted with a red box), Refresh, and Restore Backup. The main content area shows a table with one row: 'Name' and 'There are no keys available.'

10. Leave both **Key Type** set to **RSA** and **RSA Key Size** set to **2048**.

11. Fill in the remaining selections as you like and then select **Create**.

The screenshot shows the 'Create a key' dialog box. It has sections for Options (set to Generate), Name (a required field), Key Type (set to RSA), RSA Key Size (set to 2048), and settings for activation and expiration dates. At the bottom is a 'Create' button.

Setting up your disk encryption set

To create and configure disk encryption sets, you must use the following link: <https://aka.ms/diskencryptionsets>. Disk encryption set creation is not yet available in the global Azure portal.

1. Open the [disk encryption sets link](#).

2. Select **+Add**.

Dashboard > Disk Encryption Sets

Disk Encryption Sets

Microsoft

+ Add Edit columns Refresh Export to CSV Assign tags Feedback Leave preview

Filter by name... Subscription == My Example Subscription Resource group == all Location == all Add filter

Showing 1 to 1 of 1 records.

3. Select your resource group, name your encryption set, and select the same region as your key vault.
4. Select **Key vault and key**.
5. Select the key vault and key you created previously, as well as the version.
6. Press **Select**.
7. Select **Review + Create** and then **Create**.

Dashboard > Disk Encryption Sets > Create a disk encryption set

Create a disk encryption set

Basics Tags Review + create

Disk encryption sets allow you to manage encryption keys using server-side encryption for Standard HDD, Standard SSD, and Premium SSD managed disks. It will give you control of the encryption keys to meet your security and compliance needs in a few clicks. [Learn more about disk encryption sets.](#)

Project details

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

Subscription * My Example Subscription

Resource group * southcmksseregion Create new

Instance details

Disk encryption set name * myexamplesetname

Region * (US) South Central US

Key vault and key * Click to select a key

Select key from Azure Key Vault

Key vault * (highlighted with red box)

Key (highlighted with red box)

Version (highlighted with red box)

Review + create < Previous Next : Tags > Select

8. Open the disk encryption set once it finishes creating and select the alert that pops up.

exampleSetName Disk Encryption Set - PREVIEW

Search (Ctrl+/) Delete

Overview

To associate a disk, image, or snapshot with this disk encryption set, you must grant permissions to the key vault my-example-vault.

Activity log

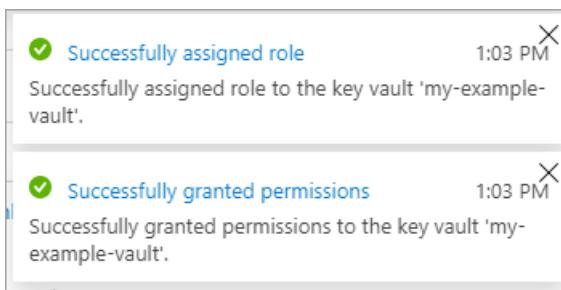
Access control (IAM)

Resource group (change) : southcmksseregion Key vault : my-example-vault

Status : --- Key : my-key

Location : South Central US

Two notifications should pop up and succeed. Doing this will allow you to use the disk encryption set with your key vault.



Deploy a VM

Now that you've created and set up your key vault and the disk encryption set, you can deploy a VM using the encryption. The VM deployment process is similar to the standard deployment process, the only differences are that you need to deploy the VM in the same region as your other resources and you opt to use a customer managed key.

1. Open the [disk encryption sets link](#).
2. Search for **Virtual Machines** and select **+ Add** to create a VM.
3. On the **Basic** tab, select the same region as your disk encryption set and Azure Key Vault.
4. Fill in the other values on the **Basic** tab as you like.

The screenshot shows the 'Create a virtual machine' wizard on the 'Basics' tab. The URL in the address bar is [Dashboard > Virtual machines > Create a virtual machine](#).

Create a virtual machine

Basics [Disks](#) [Networking](#) [Management](#) [Advanced](#) [Tags](#) [Review + create](#)

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image.

Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.

Looking for classic VMs? [Create VM from Azure Marketplace](#)

Project details

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

Subscription * [My Example Subscription](#)

Resource group * [exampleresourcegroup](#) [Create new](#)

Instance details

Virtual machine name * [examplevmname](#)

Region * [\(US\) South Central US](#)

Availability options [No infrastructure redundancy required](#)

Image * [Windows Server 2019 Datacenter](#) [Browse all public and private images](#)

Azure Spot instance Yes No

Size * [Standard DS1 v2](#)
1 vcpu, 3.5 GiB memory (\$87.05/month)
[Change size](#)

Review + create [< Previous](#) [Next : Disks >](#)

5. On the **Disks** tab, select **Encryption at rest with a customer-managed key**.

6. Select your disk encryption set in the **Disk encryption set** drop-down.

7. Make the remaining selections as you like.

The screenshot shows the 'Create a virtual machine' wizard with the 'Disks' tab selected. In the 'Encryption options' section, the radio button for 'Encryption at rest with a customer-managed key' is selected and highlighted with a red box. Below it, a warning message states: 'Once a customer-managed key is used, you can't change the selection back to a platform-managed key.' A link to 'Learn more about disk encryption' is provided. The 'Disk encryption set' dropdown is also highlighted with a red box and contains the value 'exampleSetName'. Under 'Data disks', there is a table with columns: LUN, Name, Size (GiB), Disk type, and Host caching. Two buttons are available: 'Create and attach a new disk' and 'Attach an existing disk'. The 'Advanced' section is collapsed, indicated by a downward arrow icon.

Enable on an existing disk

To manage and configure disk encryption on your existing disks, you must use the following link:

<https://aka.ms/diskencryptionsets>. Enabling customer-managed keys on existing disks is not yet available in the global Azure portal.

Caution

Enabling disk encryption on any disks attached to a VM will require that you stop the VM.

1. Open the [disk encryption sets link](#).
2. Navigate to a VM which is in the same region as one of your disk encryption sets.
3. Open the VM and select **Stop**.

my-example-vm
Virtual machine

Search (Ctrl+/
Resource group (change) : southcentralusregion
Status : Running
Location : South Central US
Subscription (change) : My Example Subscription

Connect Start Restart Stop Capture Delete Refresh

- After the VM has finished stopping, select **Disks** and then select the disk you want to encrypt.

my-example-vm - Disks
Virtual machine

Search (Ctrl+/
Edit Refresh Encryption Swap OS Disk

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

Settings

Networking Disks Size Security Extensions Continuous delivery (Preview) Availability + scaling

Managed disks created since June 10, 2017 are encrypted at rest with Storage Service Encry

Ultra Disk compatibility is not available for this location.

Disk settings

Enable Ultra Disk compatibility ⓘ
 Yes No

OS disk

Name	Size
my-example-vm_OsDisk_1_c6be1c817df34ea8bc60e4ef70404870...	127 GiB

Data disks

None

+ Add data disk

- Select **Encryption** and select **Encryption at rest with a customer-managed key** and then select your disk encryption set in the drop-down list.

- Select **Save**.

my-example-vm_OsDisk_1_c6be1c817df34ea8bc60e4ef70404870 - Encryption
Disk

Search (Ctrl+/
Save Discard

Encryption

Encryption at rest with a platform-managed key
 Encryption at rest with a customer-managed key

⚠ Once a customer-managed key is used, you can't change the selection back to a platform-managed key.
[Learn more about disk encryption.](#)

Disk encryption set * exampleSetName

- Repeat this process for any other disks attached to the VM you'd like to encrypt.

- When your disks finish switching over to customer-managed keys, if there are no other attached disks you'd like to encrypt, you may start your VM.

IMPORTANT

Customer-managed keys rely on managed identities for Azure resources, a feature of Azure Active Directory (Azure AD). When you configure customer-managed keys, a managed identity is automatically assigned to your resources under the covers. If you subsequently move the subscription, resource group, or managed disk from one Azure AD directory to another, the managed identity associated with managed disks is not transferred to the new tenant, so customer-managed keys may no longer work. For more information, see [Transferring a subscription between Azure AD directories](#).

Server-side encryption versus Azure disk encryption

[Azure Disk Encryption for virtual machines and virtual machine scale sets](#) leverages the BitLocker feature of Windows and the DM-Crypt feature of Linux to encrypt managed disks with customer-managed keys within the guest VM. 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.

Next steps

- [Explore the Azure Resource Manager templates for creating encrypted disks with customer-managed keys](#)
- [What is Azure Key Vault?](#)
- [Replicate machines with customer-managed keys enabled disks](#)
- [Set up disaster recovery of VMware VMs to Azure with PowerShell](#)
- [Set up disaster recovery to Azure for Hyper-V VMs using PowerShell and Azure Resource Manager](#)

Understand how your reservation discount is applied to Azure disk storage

2/24/2020 • 2 minutes to read • [Edit Online](#)

After you purchase Azure disk reserved capacity, a reservation discount is automatically applied to disk resources that match the terms of your reservation. The reservation discount applies to disk SKUs only. Disk snapshots are charged at pay-as-you-go rates.

For more information about Azure disk reservation, see [Save costs with Azure disk reservation](#). For information about pricing for Azure disk reservation, see [Azure Managed Disks pricing](#).

How the reservation discount is applied

The Azure disk reservation discount is a use-it-or-lose-it discount. It's applied to managed disk resources hourly. For a given hour, if you have no managed disk resources that meet the reservation terms, you lose a reservation quantity for that hour. Unused hours don't carry forward.

When you delete a resource, the reservation discount automatically applies to another matching resource in the specified scope. If no matching resource is found, the reserved hours are lost.

Discount examples

The following examples show how the Azure disk reservation discount applies depending on your deployment.

Suppose you purchase and reserve 100 P30 disks in the US West 2 region for a one-year term. Each disk has approximately 1 TiB of storage. Assume the cost of this sample reservation is \$140,100. You can choose to pay either the full amount up front or fixed monthly installments of \$11,675 for the next 12 months.

The following scenarios describe what happens if you underuse, overuse, or tier your reserved capacity. For these examples, assume you've signed up for a monthly reservation-payment plan.

Underusing your capacity

Suppose you deploy only 99 of your 100 reserved Azure premium solid-state drive (SSD) P30 disks for an hour within the reservation period. The remaining P30 disk isn't applied during that hour. It also doesn't carry over.

Overusing your capacity

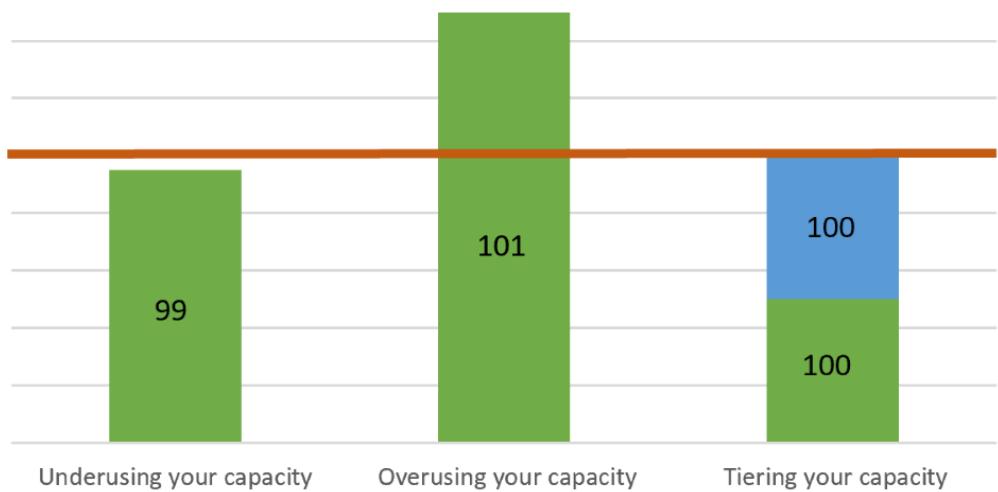
Suppose that for an hour within the reservation period, you use 101 premium SSD P30 disks. The reservation discount applies only to 100 P30 disks. The remaining P30 disk is charged at pay-as-you-go rates for that hour. For the next hour, if your usage goes down to 100 P30 disks, all usage is covered by the reservation.

Tiering your capacity

Suppose that in a given hour within your reservation period, you want to use a total of 200 P30 premium SSDs. Also suppose you use only 100 for the first 30 minutes. During this period, your use is fully covered because you made a reservation for 100 P30 disks. If you then discontinue the use of the first 100 (so that you're using zero) and then begin to use the other 100 for the remaining 30 minutes, that usage is also covered under your reservation.

Reserved disks example scenarios

One hour



Need help? Contact us

If you have questions or need help, [create a support request](#).

Next steps

- [Reduce costs with Azure Disks Reservation \(Linux\)](#)
- [Reduce costs with Azure Disks Reservation \(Windows\)](#)
- [What are Azure Reservations?](#)

Azure premium storage: design for high performance

12/23/2019 • 37 minutes to read • [Edit Online](#)

This article provides guidelines for building high performance applications using Azure Premium Storage. You can use the instructions provided in this document combined with performance best practices applicable to technologies used by your application. To illustrate the guidelines, we have used SQL Server running on Premium Storage as an example throughout this document.

While we address performance scenarios for the Storage layer in this article, you will need to optimize the application layer. For example, if you are hosting a SharePoint Farm on Azure Premium Storage, you can use the SQL Server examples from this article to optimize the database server. Additionally, optimize the SharePoint Farm's Web server and Application server to get the most performance.

This article will help answer following common questions about optimizing application performance on Azure Premium Storage,

- How to measure your application performance?
- Why are you not seeing expected high performance?
- Which factors influence your application performance on Premium Storage?
- How do these factors influence performance of your application on Premium Storage?
- How can you optimize for IOPS, Bandwidth and Latency?

We have provided these guidelines specifically for Premium Storage because workloads running on Premium Storage are highly performance sensitive. We have provided examples where appropriate. You can also apply some of these guidelines to applications running on IaaS VMs with Standard Storage disks.

NOTE

Sometimes, what appears to be a disk performance issue is actually a network bottleneck. In these situations, you should optimize your [network performance](#).

If you are looking to benchmark your disk, see our article on [Benchmarking a disk](#).

If your VM supports accelerated networking, you should make sure it is enabled. If it is not enabled, you can enable it on already deployed VMs on both [Windows](#) and [Linux](#).

Before you begin, if you are new to Premium Storage, first read the [Select an Azure disk type for IaaS VMs](#) and [Scalability targets for premium page blob storage accounts](#).

Application performance indicators

We assess whether an application is performing well or not using performance indicators like, how fast an application is processing a user request, how much data an application is processing per request, how many requests an application processing in a specific period of time, how long a user has to wait to get a response after submitting their request. The technical terms for these performance indicators are, IOPS, Throughput or Bandwidth, and Latency.

In this section, we will discuss the common performance indicators in the context of Premium Storage. In the following section, [Gathering Application Requirements](#), you will learn how to measure these performance indicators for your application. Later in [Optimizing Application Performance](#), you will learn about the factors

affecting these performance indicators and recommendations to optimize them.

IOPS

IOPS, or Input/output Operations Per Second, is the number of requests that your application is sending to the storage disks in one second. An input/output operation could be read or write, sequential, or random. Online Transaction Processing (OLTP) applications like an online retail website need to process many concurrent user requests immediately. The user requests are insert and update intensive database transactions, which the application must process quickly. Therefore, OLTP applications require very high IOPS. Such applications handle millions of small and random IO requests. If you have such an application, you must design the application infrastructure to optimize for IOPS. In the later section, *Optimizing Application Performance*, we discuss in detail all the factors that you must consider to get high IOPS.

When you attach a premium storage disk to your high scale VM, Azure provisions for you a guaranteed number of IOPS as per the disk specification. For example, a P50 disk provisions 7500 IOPS. Each high scale VM size also has a specific IOPS limit that it can sustain. For example, a Standard GS5 VM has 80,000 IOPS limit.

Throughput

Throughput, or bandwidth is the amount of data that your application is sending to the storage disks in a specified interval. If your application is performing input/output operations with large IO unit sizes, it requires high throughput. Data warehouse applications tend to issue scan intensive operations that access large portions of data at a time and commonly perform bulk operations. In other words, such applications require higher throughput. If you have such an application, you must design its infrastructure to optimize for throughput. In the next section, we discuss in detail the factors you must tune to achieve this.

When you attach a premium storage disk to a high scale VM, Azure provisions throughput as per that disk specification. For example, a P50 disk provisions 250 MB per second disk throughput. Each high scale VM size also has a specific throughput limit that it can sustain. For example, Standard GS5 VM has a maximum throughput of 2,000 MB per second.

There is a relation between throughput and IOPS as shown in the formula below.

$$\text{IOPS} \times \text{IO Size} = \text{Throughput}$$

Therefore, it is important to determine the optimal throughput and IOPS values that your application requires. As you try to optimize one, the other also gets affected. In a later section, *Optimizing Application Performance*, we will discuss in more details about optimizing IOPS and Throughput.

Latency

Latency is the time it takes an application to receive a single request, send it to the storage disks and send the response to the client. This is a critical measure of an application's performance in addition to IOPS and Throughput. The Latency of a premium storage disk is the time it takes to retrieve the information for a request and communicate it back to your application. Premium Storage provides consistent low latencies. Premium Disks are designed to provide single-digit millisecond latencies for most IO operations. If you enable ReadOnly host caching on premium storage disks, you can get much lower read latency. We will discuss Disk Caching in more detail in later section on *Optimizing Application Performance*.

When you are optimizing your application to get higher IOPS and Throughput, it will affect the latency of your application. After tuning the application performance, always evaluate the latency of the application to avoid unexpected high latency behavior.

The following control plane operations on Managed Disks may involve movement of the Disk from one Storage location to another. This is orchestrated via background copy of data that can take several hours to complete, typically less than 24 hours depending on the amount of data in the disks. During that time your application can experience higher than usual read latency as some reads can get redirected to the original location and can take longer to complete. There is no impact on write latency during this period.

- Update the storage type.
- Detach and attach a disk from one VM to another.
- Create a managed disk from a VHD.
- Create a managed disk from a snapshot.
- Convert unmanaged disks to managed disks.

Performance Application Checklist for disks

The first step in designing high-performance applications running on Azure Premium Storage is understanding the performance requirements of your application. After you have gathered performance requirements, you can optimize your application to achieve the most optimal performance.

In the previous section, we explained the common performance indicators, IOPS, Throughput, and Latency. You must identify which of these performance indicators are critical to your application to deliver the desired user experience. For example, high IOPS matters most to OLTP applications processing millions of transactions in a second. Whereas, high Throughput is critical for Data Warehouse applications processing large amounts of data in a second. Extremely low Latency is crucial for real-time applications like live video streaming websites.

Next, measure the maximum performance requirements of your application throughout its lifetime. Use the sample checklist below as a start. Record the maximum performance requirements during normal, peak, and off-hours workload periods. By identifying requirements for all workloads levels, you will be able to determine the overall performance requirement of your application. For example, the normal workload of an e-commerce website will be the transactions it serves during most days in a year. The peak workload of the website will be the transactions it serves during holiday season or special sale events. The peak workload is typically experienced for a limited period, but can require your application to scale two or more times its normal operation. Find out the 50 percentile, 90 percentile, and 99 percentile requirements. This helps filter out any outliers in the performance requirements and you can focus your efforts on optimizing for the right values.

Application performance requirements checklist

PERFORMANCE REQUIREMENTS	50 PERCENTILE	90 PERCENTILE	99 PERCENTILE
Max. Transactions per second			
% Read operations			
% Write operations			
% Random operations			
% Sequential operations			
IO request size			
Average Throughput			

PERFORMANCE REQUIREMENTS	50 PERCENTILE	90 PERCENTILE	99 PERCENTILE
Max. Throughput			
Min. Latency			
Average Latency			
Max. CPU			
Average CPU			
Max. Memory			
Average Memory			
Queue Depth			

NOTE

You should consider scaling these numbers based on expected future growth of your application. It is a good idea to plan for growth ahead of time, because it could be harder to change the infrastructure for improving performance later.

If you have an existing application and want to move to Premium Storage, first build the checklist above for the existing application. Then, build a prototype of your application on Premium Storage and design the application based on guidelines described in *Optimizing Application Performance* in a later section of this document. The next article describes the tools you can use to gather the performance measurements.

Counters to measure application performance requirements

The best way to measure performance requirements of your application, is to use performance-monitoring tools provided by the operating system of the server. You can use PerfMon for Windows and iostat for Linux. These tools capture counters corresponding to each measure explained in the above section. You must capture the values of these counters when your application is running its normal, peak, and off-hours workloads.

The PerfMon counters are available for processor, memory and, each logical disk and physical disk of your server. When you use premium storage disks with a VM, the physical disk counters are for each premium storage disk, and logical disk counters are for each volume created on the premium storage disks. You must capture the values for the disks that host your application workload. If there is a one to one mapping between logical and physical disks, you can refer to physical disk counters; otherwise refer to the logical disk counters. On Linux, the iostat command generates a CPU and disk utilization report. The disk utilization report provides statistics per physical device or partition. If you have a database server with its data and logs on separate disks, collect this data for both disks. Below table describes counters for disks, processors, and memory:

COUNTER	DESCRIPTION	PERFMON	IOSTAT
IOPS or Transactions per second	Number of I/O requests issued to the storage disk per second.	Disk Reads/sec Disk Writes/sec	tps r/s w/s
Disk Reads and Writes	% of Reads and Write operations performed on the disk.	% Disk Read Time % Disk Write Time	r/s w/s

COUNTER	DESCRIPTION	PERFMON	IOSTAT
Throughput	Amount of data read from or written to the disk per second.	Disk Read Bytes/sec Disk Write Bytes/sec	kB_read/s kB_wrtn/s
Latency	Total time to complete a disk IO request.	Average Disk sec/Read Average disk sec/Write	await svctm
IO size	The size of I/O requests issued to the storage disks.	Average Disk Bytes/Read Average Disk Bytes/Write	avgrq-sz
Queue Depth	Number of outstanding I/O requests waiting to be read from or written to the storage disk.	Current Disk Queue Length	avgqu-sz
Max. Memory	Amount of memory required to run application smoothly	% Committed Bytes in Use	Use vmstat
Max. CPU	Amount CPU required to run application smoothly	% Processor time	%util

Learn more about [iostat](#) and [PerfMon](#).

Optimize application performance

The main factors that influence performance of an application running on Premium Storage are Nature of IO requests, VM size, Disk size, Number of disks, disk caching, multithreading, and queue depth. You can control some of these factors with knobs provided by the system. Most applications may not give you an option to alter the IO size and Queue Depth directly. For example, if you are using SQL Server, you cannot choose the IO size and queue depth. SQL Server chooses the optimal IO size and queue depth values to get the most performance. It is important to understand the effects of both types of factors on your application performance, so that you can provision appropriate resources to meet performance needs.

Throughout this section, refer to the application requirements checklist that you created, to identify how much you need to optimize your application performance. Based on that, you will be able to determine which factors from this section you will need to tune. To witness the effects of each factor on your application performance, run benchmarking tools on your application setup. Refer to the Benchmarking article, linked at the end, for steps to run common benchmarking tools on Windows and Linux VMs.

Optimize IOPS, throughput, and latency at a glance

The table below summarizes performance factors and the steps necessary to optimize IOPS, throughput, and latency. The sections following this summary will describe each factor in much more depth.

For more information on VM sizes and on the IOPS, throughput, and latency available for each type of VM, see [Linux VM sizes](#) or [Windows VM sizes](#).

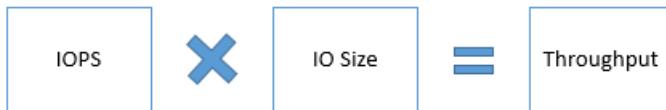
	IOPS	THROUGHPUT	LATENCY
Example Scenario	Enterprise OLTP application requiring very high transactions per second rate.	Enterprise Data warehousing application processing large amounts of data.	Near real-time applications requiring instant responses to user requests, like online gaming.

	IOPS	THROUGHPUT	LATENCY
Performance factors			
IO size	Smaller IO size yields higher IOPS.	Larger IO size to yields higher Throughput.	
VM size	Use a VM size that offers IOPS greater than your application requirement.	Use a VM size with throughput limit greater than your application requirement.	Use a VM size that offers scale limits greater than your application requirement.
Disk size	Use a disk size that offers IOPS greater than your application requirement.	Use a disk size with Throughput limit greater than your application requirement.	Use a disk size that offers scale limits greater than your application requirement.
VM and Disk Scale Limits	IOPS limit of the VM size chosen should be greater than total IOPS driven by storage disks attached to it.	Throughput limit of the VM size chosen should be greater than total Throughput driven by premium storage disks attached to it.	Scale limits of the VM size chosen must be greater than total scale limits of attached premium storage disks.
Disk Caching	Enable ReadOnly Cache on premium storage disks with Read heavy operations to get higher Read IOPS.		Enable ReadOnly Cache on premium storage disks with Ready heavy operations to get very low Read latencies.
Disk Striping	Use multiple disks and stripe them together to get a combined higher IOPS and Throughput limit. The combined limit per VM should be higher than the combined limits of attached premium disks.		
Stripe Size	Smaller stripe size for random small IO pattern seen in OLTP applications. For example, use stripe size of 64 KB for SQL Server OLTP application.	Larger stripe size for sequential large IO pattern seen in Data Warehouse applications. For example, use 256 KB stripe size for SQL Server Data warehouse application.	
Multithreading	Use multithreading to push higher number of requests to Premium Storage that will lead to higher IOPS and Throughput. For example, on SQL Server set a high MAXDOP value to allocate more CPUs to SQL Server.		
Queue Depth	Larger Queue Depth yields higher IOPS.	Larger Queue Depth yields higher Throughput.	Smaller Queue Depth yields lower latencies.

Nature of IO requests

An IO request is a unit of input/output operation that your application will be performing. Identifying the nature of IO requests, random or sequential, read or write, small or large, will help you determine the performance requirements of your application. It is important to understand the nature of IO requests, to make the right decisions when designing your application infrastructure. IOs must be distributed evenly to achieve the best performance possible.

IO size is one of the more important factors. The IO size is the size of the input/output operation request generated by your application. The IO size has a significant impact on performance especially on the IOPS and Bandwidth that the application is able to achieve. The following formula shows the relationship between IOPS, IO size, and Bandwidth/Throughput.



Some applications allow you to alter their IO size, while some applications do not. For example, SQL Server determines the optimal IO size itself, and does not provide users with any knobs to change it. On the other hand, Oracle provides a parameter called [DB_BLOCK_SIZE](#) using which you can configure the I/O request size of the database.

If you are using an application, which does not allow you to change the IO size, use the guidelines in this article to optimize the performance KPI that is most relevant to your application. For example,

- An OLTP application generates millions of small and random IO requests. To handle these types of IO requests, you must design your application infrastructure to get higher IOPS.
- A data warehousing application generates large and sequential IO requests. To handle these types of IO requests, you must design your application infrastructure to get higher Bandwidth or Throughput.

If you are using an application, which allows you to change the IO size, use this rule of thumb for the IO size in addition to other performance guidelines,

- Smaller IO size to get higher IOPS. For example, 8 KB for an OLTP application.
- Larger IO size to get higher Bandwidth/Throughput. For example, 1024 KB for a data warehouse application.

Here is an example on how you can calculate the IOPS and Throughput/Bandwidth for your application. Consider an application using a P30 disk. The maximum IOPS and Throughput/Bandwidth a P30 disk can achieve is 5000 IOPS and 200 MB per second respectively. Now, if your application requires the maximum IOPS from the P30 disk and you use a smaller IO size like 8 KB, the resulting Bandwidth you will be able to get is 40 MB per second. However, if your application requires the maximum Throughput/Bandwidth from P30 disk, and you use a larger IO size like 1024 KB, the resulting IOPS will be less, 200 IOPS. Therefore, tune the IO size such that it meets both your application's IOPS and Throughput/Bandwidth requirement. The following table summarizes the different IO sizes and their corresponding IOPS and Throughput for a P30 disk.

APPLICATION REQUIREMENT	I/O SIZE	IOPS	THROUGHPUT/BANDWIDTH
Max IOPS	8 KB	5,000	40 MB per second
Max Throughput	1024 KB	200	200 MB per second
Max Throughput + high IOPS	64 KB	3,200	200 MB per second
Max IOPS + high Throughput	32 KB	5,000	160 MB per second

To get IOPS and Bandwidth higher than the maximum value of a single premium storage disk, use multiple premium disks striped together. For example, stripe two P30 disks to get a combined IOPS of 10,000 IOPS or a combined Throughput of 400 MB per second. As explained in the next section, you must use a VM size that supports the combined disk IOPS and Throughput.

NOTE

As you increase either IOPS or Throughput the other also increases, make sure you do not hit throughput or IOPS limits of the disk or VM when increasing either one.

To witness the effects of IO size on application performance, you can run benchmarking tools on your VM and disks. Create multiple test runs and use different IO size for each run to see the impact. Refer to the Benchmarking article, linked at the end, for more details.

High scale VM sizes

When you start designing an application, one of the first things to do is, choose a VM to host your application. Premium Storage comes with High Scale VM sizes that can run applications requiring higher compute power and a high local disk I/O performance. These VMs provide faster processors, a higher memory-to-core ratio, and a Solid-State Drive (SSD) for the local disk. Examples of High Scale VMs supporting Premium Storage are the DS and GS series VMs.

High Scale VMs are available in different sizes with a different number of CPU cores, memory, OS, and temporary disk size. Each VM size also has maximum number of data disks that you can attach to the VM. Therefore, the chosen VM size will affect how much processing, memory, and storage capacity is available for your application. It also affects the Compute and Storage cost. For example, below are the specifications of the largest VM size in a DS series and a GS series:

VM SIZE	CPU CORES	MEMORY	VM DISK SIZES	MAX. DATA DISKS	CACHE SIZE	IOPS	BANDWIDTH CACHE IO LIMITS
Standard_D S14	16	112 GB	OS = 1023 GB Local SSD = 224 GB	32	576 GB	50,000 IOPS 512 MB per second	4,000 IOPS and 33 MB per second
Standard_G S5	32	448 GB	OS = 1023 GB Local SSD = 896 GB	64	4224 GB	80,000 IOPS 2,000 MB per second	5,000 IOPS and 50 MB per second

To view a complete list of all available Azure VM sizes, refer to [Windows VM sizes](#) or [Linux VM sizes](#). Choose a VM size that can meet and scale to your desired application performance requirements. In addition to this, take into account following important considerations when choosing VM sizes.

Scale Limits

The maximum IOPS limits per VM and per disk are different and independent of each other. Make sure that the application is driving IOPS within the limits of the VM as well as the premium disks attached to it. Otherwise, application performance will experience throttling.

As an example, suppose an application requirement is a maximum of 4,000 IOPS. To achieve this, you provision a P30 disk on a DS1 VM. The P30 disk can deliver up to 5,000 IOPS. However, the DS1 VM is limited to 3,200 IOPS. Consequently, the application performance will be constrained by the VM limit at 3,200 IOPS and there will be degraded performance. To prevent this situation, choose a VM and disk size that will both meet application requirements.

Cost of Operation

In many cases, it is possible that your overall cost of operation using Premium Storage is lower than using Standard Storage.

For example, consider an application requiring 16,000 IOPS. To achieve this performance, you will need a Standard_D14 Azure IaaS VM, which can give a maximum IOPS of 16,000 using 32 standard storage 1 TB disks. Each 1-TB standard storage disk can achieve a maximum of 500 IOPS. The estimated cost of this VM per month will be \$1,570. The monthly cost of 32 standard storage disks will be \$1,638. The estimated total monthly cost will be \$3,208.

However, if you hosted the same application on Premium Storage, you will need a smaller VM size and fewer premium storage disks, thus reducing the overall cost. A Standard_DS13 VM can meet the 16,000 IOPS requirement using four P30 disks. The DS13 VM has a maximum IOPS of 25,600 and each P30 disk has a maximum IOPS of 5,000. Overall, this configuration can achieve $5,000 \times 4 = 20,000$ IOPS. The estimated cost of this VM per month will be \$1,003. The monthly cost of four P30 premium storage disks will be \$544.34. The estimated total monthly cost will be \$1,544.

Table below summarizes the cost breakdown of this scenario for Standard and Premium Storage.

	STANDARD	PREMIUM
Cost of VM per month	\$1,570.58 (Standard_D14)	\$1,003.66 (Standard_DS13)
Cost of Disks per month	\$1,638.40 (32 x 1-TB disks)	\$544.34 (4 x P30 disks)
Overall Cost per month	\$3,208.98	\$1,544.34

Linux Distros

With Azure Premium Storage, you get the same level of Performance for VMs running Windows and Linux. We support many flavors of Linux distros, and you can see the complete list [here](#). It is important to note that different distros are better suited for different types of workloads. You will see different levels of performance depending on the distro your workload is running on. Test the Linux distros with your application and choose the one that works best.

When running Linux with Premium Storage, check the latest updates about required drivers to ensure high performance.

Premium storage disk sizes

Azure Premium Storage offers a variety of sizes so you can choose one that best suits your needs. Each disk size has a different scale limit for IOPS, bandwidth, and storage. Choose the right Premium Storage Disk size depending on the application requirements and the high scale VM size. The table below shows the disks sizes and their capabilities. P4, P6, P15, P60, P70, and P80 sizes are currently only supported for Managed Disks.

PRE MIU M SSD SIZE S	P1*	P2*	P3*	P4	P6	P10	P15	P20	P30	P40	P50	P60	P70	P80
Disk size in GiB	4	8	16	32	64	128	256	512	1,024	2,048	4,096	8,192	16,384	32,767

PRE MIU M SSD SIZE S	P1*	P2*	P3*	P4	P6	P10	P15	P20	P30	P40	P50	P60	P70	P80
IOP S per disk	120	120	120	120	240	500	1,1 00	2,3 00	5,0 00	7,5 00	7,5 00	16, 000	18,0 00	20,0 00
Thr oug hpu t per disk	25 MiB /sec	25 MiB /sec	25 MiB /sec	25 MiB /sec	50 MiB /sec	100 MiB /sec	125 MiB /sec	150 MiB /sec	200 MiB /sec	250 MiB /sec	250 MiB /sec	500 MiB /sec	750 MiB /sec	900 MiB /sec
Max bur st IOP S per disk **	3,5 00	3,5 00	3,5 00	3,5 00	3,5 00	3,5 00								
Max bur st thro ugh put per disk **	170 MiB /sec	170 MiB /sec	170 MiB /sec	170 MiB /sec	170 MiB /sec	170 MiB /sec								
Max bur st dur atio n**	30 min	30 min	30 min	30 min	30 min	30 min								
Eligi ble for rese rvat ion	No	Yes, up to one year	Yes, up to one year	Yes, up to one year	Yes, up to one year	Yes, up to one year	Yes, up to one year							

*Denotes a disk size that is currently in preview, for regional availability information see [New disk sizes: Managed and unmanaged](#).

**Denotes a feature that is currently in preview, see [Disk bursting](#) for more information.

How many disks you choose depends on the disk size chosen. You could use a single P50 disk or multiple P10 disks to meet your application requirement. Take into account considerations listed below when making the choice.

Scale Limits (IOPS and Throughput)

The IOPS and Throughput limits of each Premium disk size is different and independent from the VM scale limits. Make sure that the total IOPS and Throughput from the disks are within scale limits of the chosen VM size.

For example, if an application requirement is a maximum of 250 MB/sec Throughput and you are using a DS4 VM with a single P30 disk. The DS4 VM can give up to 256 MB/sec Throughput. However, a single P30 disk has Throughput limit of 200 MB/sec. Consequently, the application will be constrained at 200 MB/sec due to the disk limit. To overcome this limit, provision more than one data disks to the VM or resize your disks to P40 or P50.

NOTE

Reads served by the cache are not included in the disk IOPS and Throughput, hence not subject to disk limits. Cache has its separate IOPS and Throughput limit per VM.

For example, initially your reads and writes are 60MB/sec and 40MB/sec respectively. Over time, the cache warms up and serves more and more of the reads from the cache. Then, you can get higher write Throughput from the disk.

Number of Disks

Determine the number of disks you will need by assessing application requirements. Each VM size also has a limit on the number of disks that you can attach to the VM. Typically, this is twice the number of cores. Ensure that the VM size you choose can support the number of disks needed.

Remember, the Premium Storage disks have higher performance capabilities compared to Standard Storage disks. Therefore, if you are migrating your application from Azure IaaS VM using Standard Storage to Premium Storage, you will likely need fewer premium disks to achieve the same or higher performance for your application.

Disk caching

High Scale VMs that leverage Azure Premium Storage have a multi-tier caching technology called BlobCache. BlobCache uses a combination of the Virtual Machine RAM and local SSD for caching. This cache is available for the Premium Storage persistent disks and the VM local disks. By default, this cache setting is set to Read/Write for OS disks and ReadOnly for data disks hosted on Premium Storage. With disk caching enabled on the Premium Storage disks, the high scale VMs can achieve extremely high levels of performance that exceed the underlying disk performance.

WARNING

Disk Caching is not supported for disks 4 TiB and larger. If multiple disks are attached to your VM, each disk that is smaller than 4 TiB will support caching.

Changing the cache setting of an Azure disk detaches and re-attaches the target disk. If it is the operating system disk, the VM is restarted. Stop all applications/services that might be affected by this disruption before changing the disk cache setting.

To learn more about how BlobCache works, refer to the Inside [Azure Premium Storage](#) blog post.

It is important to enable cache on the right set of disks. Whether you should enable disk caching on a premium disk or not will depend on the workload pattern that disk will be handling. Table below shows the default cache settings for OS and Data disks.

DISK TYPE	DEFAULT CACHE SETTING
OS disk	ReadWrite

DISK TYPE	DEFAULT CACHE SETTING
Data disk	ReadOnly

Following are the recommended disk cache settings for data disks,

DISK CACHING SETTING	RECOMMENDATION ON WHEN TO USE THIS SETTING
None	Configure host-cache as None for write-only and write-heavy disks.
ReadOnly	Configure host-cache as ReadOnly for read-only and read-write disks.
ReadWrite	Configure host-cache as ReadWrite only if your application properly handles writing cached data to persistent disks when needed.

ReadOnly

By configuring ReadOnly caching on Premium Storage data disks, you can achieve low Read latency and get very high Read IOPS and Throughput for your application. This is due two reasons,

1. Reads performed from cache, which is on the VM memory and local SSD, are much faster than reads from the data disk, which is on the Azure blob storage.
2. Premium Storage does not count the Reads served from cache, towards the disk IOPS and Throughput.
Therefore, your application is able to achieve higher total IOPS and Throughput.

ReadWrite

By default, the OS disks have ReadWrite caching enabled. We have recently added support for ReadWrite caching on data disks as well. If you are using ReadWrite caching, you must have a proper way to write the data from cache to persistent disks. For example, SQL Server handles writing cached data to the persistent storage disks on its own. Using ReadWrite cache with an application that does not handle persisting the required data can lead to data loss, if the VM crashes.

None

Currently, **None** is only supported on data disks. It is not supported on OS disks. If you set **None** on an OS disk it will override this internally and set it to **ReadOnly**.

As an example, you can apply these guidelines to SQL Server running on Premium Storage by doing the following,

1. Configure "ReadOnly" cache on premium storage disks hosting data files.
 - a. The fast reads from cache lower the SQL Server query time since data pages are retrieved much faster from the cache compared to directly from the data disks.
 - b. Serving reads from cache, means there is additional Throughput available from premium data disks. SQL Server can use this additional Throughput towards retrieving more data pages and other operations like backup/restore, batch loads, and index rebuilds.
2. Configure "None" cache on premium storage disks hosting the log files.
 - a. Log files have primarily write-heavy operations. Therefore, they do not benefit from the ReadOnly cache.

Optimize performance on Linux VMs

For all premium SSDs or ultra disks with cache set to **ReadOnly** or **None**, you must disable "barriers" when you mount the file system. You don't need barriers in this scenario because the writes to premium storage disks are durable for these cache settings. When the write request successfully finishes, data has been written to the

persistent store. To disable "barriers," use one of the following methods. Choose the one for your file system:

- For **reiserFS**, to disable barriers, use the `barrier=none` mount option. (To enable barriers, use `barrier=flush`.)
- For **ext3/ext4**, to disable barriers, use the `barrier=0` mount option. (To enable barriers, use `barrier=1`.)
- For **XFS**, to disable barriers, use the `nobarrier` mount option. (To enable barriers, use `barrier`.)
- For premium storage disks with cache set to **ReadWrite**, enable barriers for write durability.
- For volume labels to persist after you restart the VM, you must update /etc/fstab with the universally unique identifier (UUID) references to the disks. For more information, see [Add a managed disk to a Linux VM](#).

The following Linux distributions have been validated for premium SSDs. For better performance and stability with premium SSDs, we recommend that you upgrade your VMs to one of these versions or newer.

Some of the versions require the latest Linux Integration Services (LIS), v4.0, for Azure. To download and install a distribution, follow the link listed in the following table. We add images to the list as we complete validation. Our validations show that performance varies for each image. Performance depends on workload characteristics and your image settings. Different images are tuned for different kinds of workloads.

DISTRIBUTION	VERSION	SUPPORTED KERNEL	DETAILS
Ubuntu	12.04 or newer	3.2.0-75.110+	
Ubuntu	14.04 or newer	3.13.0-44.73+	
Debian	7.x, 8.x or newer	3.16.7-ckt4-1+	
SUSE	SLES 12 or newer	3.12.36-38.1+	
SUSE	SLES 11 SP4 or newer	3.0.101-0.63.1+	
CoreOS	584.0.0+ or newer	3.18.4+	
CentOS	6.5, 6.6, 6.7, 7.0, or newer		LIS4 required <i>See note in the next section</i>
CentOS	7.1+ or newer	3.10.0-229.1.2.el7+	LIS4 recommended <i>See note in the next section</i>
Red Hat Enterprise Linux (RHEL)	6.8+, 7.2+, or newer		
Oracle	6.0+, 7.2+, or newer		UEK4 or RHCK
Oracle	7.0-7.1 or newer		UEK4 or RHCK w/ LIS4
Oracle	6.4-6.7 or newer		UEK4 or RHCK w/ LIS4

LIS drivers for OpenLogic CentOS

If you're running OpenLogic CentOS VMs, run the following command to install the latest drivers:

```
sudo yum remove hypervkvpd ## (Might return an error if not installed. That's OK.)  
sudo yum install microsoft-hyper-v  
sudo reboot
```

In some cases the command above will upgrade the kernel as well. If a kernel update is required then you may

need to run the above commands again after rebooting to fully install the microsoft-hyper-v package.

Disk striping

When a high scale VM is attached with several premium storage persistent disks, the disks can be striped together to aggregate their IOPs, bandwidth, and storage capacity.

On Windows, you can use Storage Spaces to stripe disks together. You must configure one column for each disk in a pool. Otherwise, the overall performance of striped volume can be lower than expected, due to uneven distribution of traffic across the disks.

Important: Using Server Manager UI, you can set the total number of columns up to 8 for a striped volume. When attaching more than eight disks, use PowerShell to create the volume. Using PowerShell, you can set the number of columns equal to the number of disks. For example, if there are 16 disks in a single stripe set; specify 16 columns in the *NumberOfColumns* parameter of the *New-VirtualDisk* PowerShell cmdlet.

On Linux, use the MDADM utility to stripe disks together. For detailed steps on striping disks on Linux refer to [Configure Software RAID on Linux](#).

Stripe Size

An important configuration in disk striping is the stripe size. The stripe size or block size is the smallest chunk of data that application can address on a striped volume. The stripe size you configure depends on the type of application and its request pattern. If you choose the wrong stripe size, it could lead to IO misalignment, which leads to degraded performance of your application.

For example, if an IO request generated by your application is bigger than the disk stripe size, the storage system writes it across stripe unit boundaries on more than one disk. When it is time to access that data, it will have to seek across more than one stripe units to complete the request. The cumulative effect of such behavior can lead to substantial performance degradation. On the other hand, if the IO request size is smaller than stripe size, and if it is random in nature, the IO requests may add up on the same disk causing a bottleneck and ultimately degrading the IO performance.

Depending on the type of workload your application is running, choose an appropriate stripe size. For random small IO requests, use a smaller stripe size. Whereas for large sequential IO requests use a larger stripe size. Find out the stripe size recommendations for the application you will be running on Premium Storage. For SQL Server, configure stripe size of 64 KB for OLTP workloads and 256 KB for data warehousing workloads. See [Performance best practices for SQL Server on Azure VMs](#) to learn more.

NOTE

You can stripe together a maximum of 32 premium storage disks on a DS series VM and 64 premium storage disks on a GS series VM.

Multi-threading

Azure has designed Premium Storage platform to be massively parallel. Therefore, a multi-threaded application achieves much higher performance than a single-threaded application. A multi-threaded application splits up its tasks across multiple threads and increases efficiency of its execution by utilizing the VM and disk resources to the maximum.

For example, if your application is running on a single core VM using two threads, the CPU can switch between the two threads to achieve efficiency. While one thread is waiting on a disk IO to complete, the CPU can switch to the other thread. In this way, two threads can accomplish more than a single thread would. If the VM has more than one core, it further decreases running time since each core can execute tasks in parallel.

You may not be able to change the way an off-the-shelf application implements single threading or multi-

threading. For example, SQL Server is capable of handling multi-CPU and multi-core. However, SQL Server decides under what conditions it will leverage one or more threads to process a query. It can run queries and build indexes using multi-threading. For a query that involves joining large tables and sorting data before returning to the user, SQL Server will likely use multiple threads. However, a user cannot control whether SQL Server executes a query using a single thread or multiple threads.

There are configuration settings that you can alter to influence this multi-threading or parallel processing of an application. For example, in case of SQL Server it is the maximum Degree of Parallelism configuration. This setting called MAXDOP, allows you to configure the maximum number of processors SQL Server can use when parallel processing. You can configure MAXDOP for individual queries or index operations. This is beneficial when you want to balance resources of your system for a performance critical application.

For example, say your application using SQL Server is executing a large query and an index operation at the same time. Let us assume that you wanted the index operation to be more performant compared to the large query. In such a case, you can set MAXDOP value of the index operation to be higher than the MAXDOP value for the query. This way, SQL Server has more number of processors that it can leverage for the index operation compared to the number of processors it can dedicate to the large query. Remember, you do not control the number of threads SQL Server will use for each operation. You can control the maximum number of processors being dedicated for multi-threading.

Learn more about [Degrees of Parallelism](#) in SQL Server. Find out such settings that influence multi-threading in your application and their configurations to optimize performance.

Queue depth

The queue depth or queue length or queue size is the number of pending IO requests in the system. The value of queue depth determines how many IO operations your application can line up, which the storage disks will be processing. It affects all the three application performance indicators that we discussed in this article viz., IOPS, throughput, and latency.

Queue Depth and multi-threading are closely related. The Queue Depth value indicates how much multi-threading can be achieved by the application. If the Queue Depth is large, application can execute more operations concurrently, in other words, more multi-threading. If the Queue Depth is small, even though application is multi-threaded, it will not have enough requests lined up for concurrent execution.

Typically, off the shelf applications do not allow you to change the queue depth, because if set incorrectly it will do more harm than good. Applications will set the right value of queue depth to get the optimal performance. However, it is important to understand this concept so that you can troubleshoot performance issues with your application. You can also observe the effects of queue depth by running benchmarking tools on your system.

Some applications provide settings to influence the Queue Depth. For example, the MAXDOP (maximum degree of parallelism) setting in SQL Server explained in previous section. MAXDOP is a way to influence Queue Depth and multi-threading, although it does not directly change the Queue Depth value of SQL Server.

High queue depth

A high queue depth lines up more operations on the disk. The disk knows the next request in its queue ahead of time. Consequently, the disk can schedule operations ahead of time and process them in an optimal sequence. Since the application is sending more requests to the disk, the disk can process more parallel IOs. Ultimately, the application will be able to achieve higher IOPS. Since application is processing more requests, the total Throughput of the application also increases.

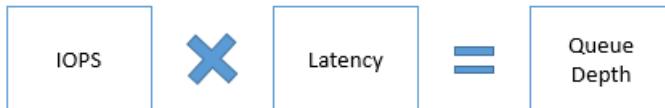
Typically, an application can achieve maximum Throughput with 8-16+ outstanding IOs per attached disk. If a queue depth is one, application is not pushing enough IOs to the system, and it will process less amount of in a given period. In other words, less Throughput.

For example, in SQL Server, setting the MAXDOP value for a query to "4" informs SQL Server that it can use up

to four cores to execute the query. SQL Server will determine what is best queue depth value and the number of cores for the query execution.

Optimal queue depth

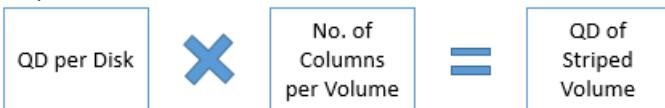
Very high queue depth value also has its drawbacks. If queue depth value is too high, the application will try to drive very high IOPS. Unless application has persistent disks with sufficient provisioned IOPS, this can negatively affect application latencies. Following formula shows the relationship between IOPS, latency, and queue depth.



You should not configure Queue Depth to any high value, but to an optimal value, which can deliver enough IOPS for the application without affecting latencies. For example, if the application latency needs to be 1 millisecond, the Queue Depth required to achieve 5,000 IOPS is, $QD = 5000 \times 0.001 = 5$.

Queue Depth for Striped Volume

For a striped volume, maintain a high enough queue depth such that, every disk has a peak queue depth individually. For example, consider an application that pushes a queue depth of 2 and there are four disks in the stripe. The two IO requests will go to two disks and remaining two disks will be idle. Therefore, configure the queue depth such that all the disks can be busy. Formula below shows how to determine the queue depth of striped volumes.



Throttling

Azure Premium Storage provisions specified number of IOPS and Throughput depending on the VM sizes and disk sizes you choose. Anytime your application tries to drive IOPS or Throughput above these limits of what the VM or disk can handle, Premium Storage will throttle it. This manifests in the form of degraded performance in your application. This can mean higher latency, lower Throughput, or lower IOPS. If Premium Storage does not throttle, your application could completely fail by exceeding what its resources are capable of achieving. So, to avoid performance issues due to throttling, always provision sufficient resources for your application. Take into consideration what we discussed in the VM sizes and Disk sizes sections above. Benchmarking is the best way to figure out what resources you will need to host your application.

Next steps

If you are looking to benchmark your disk, see our article on [Benchmarking a disk](#).

Learn more about the available disk types: [Select a disk type](#)

For SQL Server users, read articles on Performance Best Practices for SQL Server:

- [Performance Best Practices for SQL Server in Azure Virtual Machines](#)
- [Azure Premium Storage provides highest performance for SQL Server in Azure VM](#)

Premium SSD bursting (preview)

12/2/2019 • 4 minutes to read • [Edit Online](#)

Disk bursting is currently a preview feature for premium SSDs. Bursting is supported on any premium SSD disk sizes <= 512 GiB (P20 or below). These disk sizes support bursting on a best effort basis and utilize a credit system to manage bursting. Credits accumulate in a burst bucket whenever disk traffic is below the provisioned performance target for their disk size, and consume credits when traffic bursts beyond the target. Disk traffic is tracked against both IOPS and bandwidth in the provisioned target.

Disk bursting is enabled by default on new deployments of the disk sizes that support it. Existing disk sizes, if they support disk bursting, can enable bursting through either of the following methods:

- Detach and reattach the disk.
- Stop and start the VM.

Burst states

All burst applicable disk sizes will start with a full burst credit bucket when the disk is attached to a Virtual Machine. The max duration of bursting is determined by the size of the burst credit bucket. You can only accumulate unused credits up to the size of the credit bucket. At any point of time, your disk burst credit bucket can be in one of the following three states:

- Accruing, when the disk traffic is using less than the provisioned performance target. You can accumulate credit if disk traffic is beyond IOPS or bandwidth targets or both. You can still accumulate IO credits when you are consuming full disk bandwidth, vice versa.
- Declining, when the disk traffic is using more than the provisioned performance target. The burst traffic will independently consume credits from IOPS or bandwidth.
- Remaining constant, when the disk traffic is exactly at the provisioned performance target.

The disk sizes that provide bursting support along with the burst specifications are summarized in the table below.

Regional availability

Currently, disk bursting is only available in the West Central US region.

Disk sizes

PRE MIU M SSD SIZE S	P1*	P2*	P3*	P4	P6	P10	P15	P20	P30	P40	P50	P60	P70	P80
Disk size in GiB	4	8	16	32	64	128	256	512	1,024	2,048	4,096	8,192	16,384	32,767

PRE MIU M SSD SIZE S	P1*	P2*	P3*	P4	P6	P10	P15	P20	P30	P40	P50	P60	P70	P80
IOP S per disk	120	120	120	120	240	500	1,10 0	2,30 0	5,00 0	7,50 0	7,50 0	16,0 00	18,0 00	20,0 00
Thr oug hpu t per disk	25 MiB /sec	25 MiB /sec	25 MiB /sec	25 MiB /sec	50 MiB /sec	100 MiB /sec	125 MiB /sec	150 MiB /sec	200 MiB /sec	250 MiB /sec	250 MiB /sec	500 MiB /sec	750 MiB /sec	900 MiB /sec
Max bur st IOP S per disk **	3,5 00	3,5 00	3,5 00	3,5 00	3,50 0	3,50 0	3,50 0	3,50 0						
Max bur st thro ugh put per disk **	170 MiB /sec													
Max bur st dur at io n**	30 min													
Eligi ble for rese rvat ion	No	Yes, up to one year	Yes, up to one year	Yes, up to one year	Yes, up to one year	Yes, up to one year								

*Denotes a disk size that is currently in preview, for regional availability information see [New disk sizes: Managed and unmanaged](#).

**Denotes a feature that is currently in preview, see [Disk bursting](#) for more information.

Example scenarios

To give you a better idea of how this works, here's a few example scenarios:

- One common scenario that can benefit from disk bursting is faster VM boot and application launch on OS

disks. Take a Linux VM with an 8 GiB OS image as an example. If we use a P2 disk as the OS disk, the provisioned target is 120 IOPS and 25 MBps. When VM starts, there will be a read spike to the OS disk loading the boot files. With the introduction of bursting, you can read at the max burst speed of 3500 IOPS and 170 MBps, accelerating the load time by at least 6x. After VM boot, the traffic level on the OS disk is usually low, since most data operations by the application will be against the attached data disks. If the traffic is below the provisioned target, you will accumulate credits.

- If you are hosting a Remote Virtual Desktop environment, whenever an active user launches an application like AutoCAD, read traffic to the OS disk significantly increases. In this case, burst traffic will consume accumulated credits, allowing you to go beyond the provisioned target, and launching the application much faster.
- A P1 disk has a provisioned target of 120 IOPS and 25 MBps. If the actual traffic on the disk was 100 IOPS and 20 MBps in the past 1 second interval, then the unused 20 IOs and 5 MB are credited to the burst bucket of the disk. Credits in the burst bucket can later be used when the traffic exceeds the provisioned target, up to the max burst limit. The max burst limit defines the ceiling of disk traffic even if you have burst credits to consume from. In this case, even if you have 10,000 IOs in the credit bucket, a P1 disk cannot issue more than the max burst of 3,500 IO per sec.

Next steps

[Use the portal to attach a data disk to a Linux VM](#)

Scalability and performance targets for VM disks on Linux

1/3/2020 • 5 minutes to read • [Edit Online](#)

You can attach a number of data disks to an Azure virtual machine. Based on the scalability and performance targets for a VM's data disks, you can determine the number and type of disk that you need to meet your performance and capacity requirements.

IMPORTANT

For optimal performance, limit the number of highly utilized disks attached to the virtual machine to avoid possible throttling. If all attached disks aren't highly utilized at the same time, the virtual machine can support a larger number of disks.

For Azure managed disks:

The following table illustrates the default and maximum limits of the number of resources per region per subscription. There is no limit for the number of Managed Disks, snapshots and images per resource group.

RESOURCE	DEFAULT LIMIT	MAXIMUM LIMIT
Standard managed disks	50,000	50,000
Standard SSD managed disks	50,000	50,000
Premium managed disks	50,000	50,000
Standard_LRS snapshots	50,000	50,000
Standard_ZRS snapshots	50,000	50,000
Managed image	50,000	50,000

- **For Standard storage accounts:** A Standard storage account has a maximum total request rate of 20,000 IOPS. The total IOPS across all of your virtual machine disks in a Standard storage account should not exceed this limit.

You can roughly calculate the number of highly utilized disks supported by a single Standard storage account based on the request rate limit. For example, for a Basic tier VM, the maximum number of highly utilized disks is about 66, which is $20,000/300$ IOPS per disk. The maximum number of highly utilized disks for a Standard tier VM is about 40, which is $20,000/500$ IOPS per disk.

- **For Premium storage accounts:** A Premium storage account has a maximum total throughput rate of 50 Gbps. The total throughput across all of your VM disks should not exceed this limit.

See [Linux VM sizes](#) for additional details.

Managed virtual machine disks

Sizes denoted with an asterisk are currently in preview. See our [FAQ](#) to learn what regions they are available in.

Standard HDD managed disks

STANDARD DISK TYPE	S4	S6	S10	S15	S20	S30	S40	S50	S60	S70	S80
Disk size in GiB	32	64	128	256	512	1,024	2,048	4,096	8,192	16,384	32,767
IOPS per disk	Up to 500	Up to 1,300	Up to 2,000	Up to 2,000							
Throughput per disk	Up to 60 MiB/sec	Up to 300 MiB/sec	Up to 500 MiB/sec	Up to 500 MiB/sec							

Standard SSD managed disks

STANDARD SSD SIZE S	E1*	E2*	E3*	E4	E6	E10	E15	E20	E30	E40	E50	E60	E70	E80
Disk size in GiB	4	8	16	32	64	128	256	512	1,024	2,048	4,096	8,192	16,384	32,767
IOPS per disk	Up to 120	Up to 120	Up to 120	Up to 120	Up to 240	Up to 500	Up to 2,000	Up to 4,000	Up to 6,000					
Throughput per disk	Up to 25 MiB/sec	Up to 50 MiB/sec	Up to 60 MiB/sec	Up to 400 MiB/sec	Up to 600 MiB/sec	Up to 750 MiB/sec								

*Denotes a disk size that is currently in preview, for regional availability information see [New disk sizes: Managed and unmanaged](#).

Premium SSD managed disks: Per-disk limits

PREMIUM SSD SIZE S	P1*	P2*	P3*	P4	P6	P10	P15	P20	P30	P40	P50	P60	P70	P80
Disk size in GiB	4	8	16	32	64	128	256	512	1,024	2,048	4,096	8,192	16,384	32,767

PRE MIU M SSD SIZE S	P1*	P2*	P3*	P4	P6	P10	P15	P20	P30	P40	P50	P60	P70	P80
-------------------------------------	-----	-----	-----	----	----	-----	-----	-----	-----	-----	-----	-----	-----	-----

IOP S per disk	120	120	120	120	240	500	1,10 0	2,30 0	5,00 0	7,50 0	7,50 0	16,0 00	18,0 00	20,0 00
Throughput per disk	25 MiB /sec	25 MiB /sec	25 MiB /sec	25 MiB /sec	50 MiB /sec	100 MiB /sec	125 MiB /sec	150 MiB /sec	200 MiB /sec	250 MiB /sec	250 MiB /sec	500 MiB /sec	750 MiB /sec	900 MiB /sec
Max burst IOP S per disk **	3,5 00	3,5 00	3,50 0	3,50 0	3,50 0	3,50 0	3,50 0	3,50 0	3,50 0	3,50 0	3,50 0	3,50 0	3,50 0	3,50 0
Max burst throughput per disk **	170 MiB /sec	170 MiB /sec	170 MiB /sec	170 MiB /sec	170 MiB /sec	170 MiB /sec								
Max burst duration**	30 min	30 min	30 min	30 min	30 min	30 min								
Eligible for reservation	No	Yes, up to one year												

*Denotes a disk size that is currently in preview, for regional availability information see [New disk sizes: Managed and unmanaged](#).

**Denotes a feature that is currently in preview, see [Disk bursting](#) for more information.

Premium SSD managed disks: Per-VM limits

RESOURCE	DEFAULT LIMIT
Maximum IOPS Per VM	80,000 IOPS with GS5 VM
Maximum throughput per VM	2,000 MB/s with GS5 VM

Unmanaged virtual machine disks

Standard unmanaged virtual machine disks: Per-disk limits

VM TIER	BASIC TIER VM	STANDARD TIER VM
Disk size	4,095 GB	4,095 GB
Maximum 8-KB IOPS per persistent disk	300	500
Maximum number of disks that perform the maximum IOPS	66	40

Premium unmanaged virtual machine disks: Per-account limits

RESOURCE	DEFAULT LIMIT
Total disk capacity per account	35 TB
Total snapshot capacity per account	10 TB
Maximum bandwidth per account (ingress + egress) ¹	<=50 Gbps

¹*Ingress* refers to all data from requests that are sent to a storage account. *Egress* refers to all data from responses that are received from a storage account.

Premium unmanaged virtual machine disks: Per-disk limits

PREMIUM STORAGE DISK TYPE	P10	P20	P30	P40	P50
Disk size	128 GiB	512 GiB	1,024 GiB (1 TB)	2,048 GiB (2 TB)	4,095 GiB (4 TB)
Maximum IOPS per disk	500	2,300	5,000	7,500	7,500
Maximum throughput per disk	100 MB/sec	150 MB/sec	200 MB/sec	250 MB/sec	250 MB/sec
Maximum number of disks per storage account	280	70	35	17	8

Premium unmanaged virtual machine disks: Per-VM limits

RESOURCE	DEFAULT LIMIT
Maximum IOPS per VM	80,000 IOPS with GS5 VM
Maximum throughput per VM	2,000 MB/sec with GS5 VM

See also

[Azure subscription and service limits, quotas, and constraints](#)

Backup and disaster recovery for Azure IaaS disks

12/10/2019 • 21 minutes to read • [Edit Online](#)

This article explains how to plan for backup and disaster recovery (DR) of IaaS virtual machines (VMs) and disks in Azure. This document covers both managed and unmanaged disks.

First, we cover the built-in fault tolerance capabilities in the Azure platform that helps guard against local failures. We then discuss the disaster scenarios not fully covered by the built-in capabilities. We also show several examples of workload scenarios where different backup and DR considerations can apply. We then review possible solutions for the DR of IaaS disks.

Introduction

The Azure platform uses various methods for redundancy and fault tolerance to help protect customers from localized hardware failures. Local failures can include problems with an Azure Storage server machine that stores part of the data for a virtual disk or failures of an SSD or HDD on that server. Such isolated hardware component failures can happen during normal operations.

The Azure platform is designed to be resilient to these failures. Major disasters can result in failures or the inaccessibility of many storage servers or even a whole datacenter. Although your VMs and disks are normally protected from localized failures, additional steps are necessary to protect your workload from region-wide catastrophic failures, such as a major disaster, that can affect your VM and disks.

In addition to the possibility of platform failures, problems with a customer application or data can occur. For example, a new version of your application might inadvertently make a change to the data that causes it to break. In that case, you might want to revert the application and the data to a prior version that contains the last known good state. This requires maintaining regular backups.

For regional disaster recovery, you must back up your IaaS VM disks to a different region.

Before we look at backup and DR options, let's recap a few methods available for handling localized failures.

Azure IaaS resiliency

Resiliency refers to the tolerance for normal failures that occur in hardware components. Resiliency is the ability to recover from failures and continue to function. It's not about avoiding failures, but responding to failures in a way that avoids downtime or data loss. The goal of resiliency is to return the application to a fully functioning state following a failure. Azure virtual machines and disks are designed to be resilient to common hardware faults. Let's look at how the Azure IaaS platform provides this resiliency.

A virtual machine consists mainly of two parts: a compute server and the persistent disks. Both affect the fault tolerance of a virtual machine.

If the Azure compute host server that houses your VM experiences a hardware failure, which is rare, Azure is designed to automatically restore the VM on another server. If this scenario, your computer reboots, and the VM comes back up after some time. Azure automatically detects such hardware failures and executes recoveries to help ensure the customer VM is available as soon as possible.

Regarding IaaS disks, the durability of data is critical for a persistent storage platform. Azure customers have important business applications running on IaaS, and they depend on the persistence of the data. Azure designs protection for these IaaS disks, with three redundant copies of the data that is stored locally. These copies provide for high durability against local failures. If one of the hardware components that holds your disk fails, your VM is not affected, because there are two additional copies to support disk requests. It works fine, even if two different

hardware components that support a disk fail at the same time (which is rare).

To ensure that you always maintain three replicas, Azure Storage automatically spawns a new copy of the data in the background if one of the three copies becomes unavailable. Therefore, it should not be necessary to use RAID with Azure disks for fault tolerance. A simple RAID 0 configuration should be sufficient for striping the disks, if necessary, to create larger volumes.

Because of this architecture, Azure has consistently delivered enterprise-grade durability for IaaS disks, with an industry-leading zero percent [annualized failure rate](#).

Localized hardware faults on the compute host or in the Storage platform can sometimes result in the temporary unavailability of the VM that is covered by the [Azure SLA](#) for VM availability. Azure also provides an industry-leading SLA for single VM instances that use Azure premium SSDs.

To safeguard application workloads from downtime due to the temporary unavailability of a disk or VM, customers can use [availability sets](#). Two or more virtual machines in an availability set provide redundancy for the application. Azure then creates these VMs and disks in separate fault domains with different power, network, and server components.

Because of these separate fault domains, localized hardware failures typically do not affect multiple VMs in the set at the same time. Having separate fault domains provides high availability for your application. It's considered a good practice to use availability sets when high availability is required. The next section covers the disaster recovery aspect.

Backup and disaster recovery

Disaster recovery is the ability to recover from rare, but major, incidents. These incidents include non-transient, wide-scale failures, such as service disruption that affects an entire region. Disaster recovery includes data backup and archiving, and might include manual intervention, such as restoring a database from a backup.

The Azure platform's built-in protection against localized failures might not fully protect the VMs/disks if a major disaster causes large-scale outages. These large-scale outages include catastrophic events, such as if a datacenter is hit by a hurricane, earthquake, fire, or if there is a large-scale hardware unit failure. In addition, you might encounter failures due to application or data issues.

To help protect your IaaS workloads from outages, you should plan for redundancy and have backups to enable recovery. For disaster recovery, you should back up in a different geographic location away from the primary site. This approach helps ensure your backup is not affected by the same event that originally affected the VM or disks. For more information, see [Disaster recovery for Azure applications](#).

Your DR considerations might include the following aspects:

- High availability: The ability of the application to continue running in a healthy state, without significant downtime. By *healthy state*, this state means that the application is responsive, and users can connect to the application and interact with it. Certain mission-critical applications and databases might be required to always be available, even when there are failures in the platform. For these workloads, you might need to plan redundancy for the application, as well as the data.
- Data durability: In some cases, the main consideration is ensuring that the data is preserved if a disaster happens. Therefore, you might need a backup of your data in a different site. For such workloads, you might not need full redundancy for the application, but only a regular backup of the disks.

Backup and DR scenarios

Let's look at a few typical examples of application workload scenarios and the considerations for planning for disaster recovery.

Scenario 1: Major database solutions

Consider a production database server, like SQL Server or Oracle, that can support high availability. Critical production applications and users depend on this database. The disaster recovery plan for this system might need to support the following requirements:

- The data must be protected and recoverable.
- The server must be available for use.

The disaster recovery plan might require maintaining a replica of the database in a different region as a backup. Depending on the requirements for server availability and data recovery, the solution might range from an active-active or active-passive replica site to periodic offline backups of the data. Relational databases, such as SQL Server and Oracle, provide various options for replication. For SQL Server, use [SQL Server AlwaysOn Availability Groups](#) for high availability.

NoSQL databases, like MongoDB, also support [replicas](#) for redundancy. The replicas for high availability are used.

Scenario 2: A cluster of redundant VMs

Consider a workload handled by a cluster of VMs that provide redundancy and load balancing. One example is a Cassandra cluster deployed in a region. This type of architecture already provides a high level of redundancy within that region. However, to protect the workload from a regional-level failure, you should consider spreading the cluster across two regions or making periodic backups to another region.

Scenario 3: IaaS application workload

Let's look at the IaaS application workload. For example, this application might be a typical production workload running on an Azure VM. It might be a web server or file server holding the content and other resources of a site. It might also be a custom-built business application running on a VM that stored its data, resources, and application state on the VM disks. In this case, it's important to make sure you take backups on a regular basis. Backup frequency should be based on the nature of the VM workload. For example, if the application runs every day and modifies data, then the backup should be taken every hour.

Another example is a reporting server that pulls data from other sources and generates aggregated reports. The loss of this VM or disks might lead to the loss of the reports. However, it might be possible to rerun the reporting process and regenerate the output. In that case, you don't really have a loss of data, even if the reporting server is hit with a disaster. As a result, you might have a higher level of tolerance for losing part of the data on the reporting server. In that case, less frequent backups are an option to reduce costs.

Scenario 4: IaaS application data issues

IaaS application data issues are another possibility. Consider an application that computes, maintains, and serves critical commercial data, such as pricing information. A new version of your application had a software bug that incorrectly computed the pricing and corrupted the existing commerce data served by the platform. Here, the best course of action is to revert to the earlier version of the application and the data. To enable this, take periodic backups of your system.

Disaster recovery solution: Azure Backup

[Azure Backup](#) is used for backups and DR, and it works with [managed disks](#) as well as unmanaged disks. You can create a backup job with time-based backups, easy VM restoration, and backup retention policies.

If you use [premium SSDs](#), [managed disks](#), or other disk types with the [locally redundant storage](#) option, it's especially important to make periodic DR backups. Azure Backup stores the data in your recovery services vault for long-term retention. Choose the [geo-redundant storage](#) option for the backup recovery services vault. That option ensures that backups are replicated to a different Azure region for safeguarding from regional disasters.

For unmanaged disks, you can use the locally redundant storage type for IaaS disks, but ensure that Azure Backup is enabled with the geo-redundant storage option for the recovery services vault.

NOTE

If you use the [geo-redundant storage](#) or [read-access geo-redundant storage](#) option for your unmanaged disks, you still need consistent snapshots for backup and DR. Use either [Azure Backup](#) or [consistent snapshots](#).

The following table is a summary of the solutions available for DR.

SCENARIO	AUTOMATIC REPLICATION	DR SOLUTION
Premium SSD disks	Local (locally redundant storage)	Azure Backup
Managed disks	Local (locally redundant storage)	Azure Backup
Unmanaged locally redundant storage disks	Local (locally redundant storage)	Azure Backup
Unmanaged geo-redundant storage disks	Cross region (geo-redundant storage)	Azure Backup Consistent snapshots
Unmanaged read-access geo-redundant storage disks	Cross region (read-access geo-redundant storage)	Azure Backup Consistent snapshots

High availability is best met by using managed disks in an availability set along with Azure Backup. If you use unmanaged disks, you can still use Azure Backup for DR. If you are unable to use Azure Backup, then taking [consistent snapshots](#), as described in a later section, is an alternative solution for backup and DR.

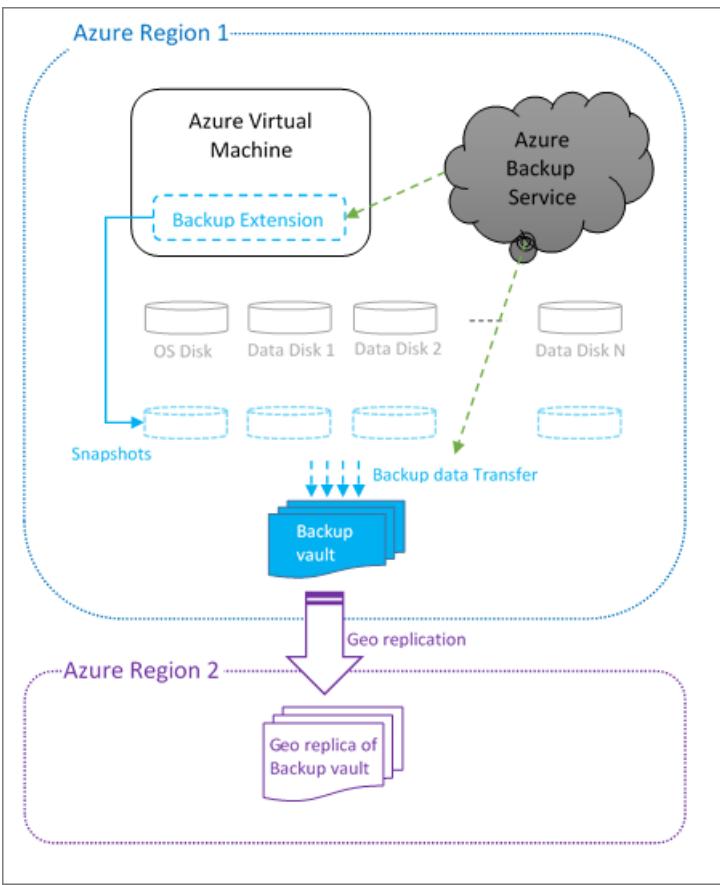
Your choices for high availability, backup, and DR at application or infrastructure levels can be represented as follows:

LEVEL	HIGH AVAILABILITY	BACKUP OR DR
Application	SQL Server AlwaysOn	Azure Backup
Infrastructure	Availability set	Geo-redundant storage with consistent snapshots

Using Azure Backup

[Azure Backup](#) can back up your VMs running Windows or Linux to the Azure recovery services vault. Backing up and restoring business-critical data is complicated by the fact that business-critical data must be backed up while the applications that produce the data are running.

To address this issue, Azure Backup provides application-consistent backups for Microsoft workloads. It uses the volume shadow service to ensure that data is written correctly to storage. For Linux VMs, the default backup consistency mode is file-consistent backups, because Linux does not have functionality equivalent to the volume shadow service as in the case of Windows. For Linux machines, see [Application-consistent backup of Azure Linux VMs](#).



When Azure Backup initiates a backup job at the scheduled time, it triggers the backup extension installed in the VM to take a point-in-time snapshot. A snapshot is taken in coordination with the volume shadow service to get a consistent snapshot of the disks in the virtual machine without having to shut it down. The backup extension in the VM flushes all writes before taking a consistent snapshot of all of the disks. After taking the snapshot, the data is transferred by Azure Backup to the backup vault. To make the backup process more efficient, the service identifies and transfers only the blocks of data that have changed after the last backup.

To restore, you can view the available backups through Azure Backup and then initiate a restore. You can create and restore Azure backups through the [Azure portal](#), by [using PowerShell](#), or by using the [Azure CLI](#).

Steps to enable a backup

Use the following steps to enable backups of your VMs by using the [Azure portal](#). There is some variation depending on your exact scenario. Refer to the [Azure Backup](#) documentation for full details. Azure Backup also [supports VMs with managed disks](#).

1. Create a recovery services vault for a VM:
 - a. In the [Azure portal](#), browse **All resources** and find **Recovery Services vaults**.
 - b. On the **Recovery Services vaults** menu, click **Add** and follow the steps to create a new vault in the same region as the VM. For example, if your VM is in the West US region, pick West US for the vault.
2. Verify the storage replication for the newly created vault. Access the vault under **Recovery Services vaults** and go to **Properties > Backup Configuration > Update**. Ensure the **geo-redundant storage** option is selected by default. This option ensures that your vault is automatically replicated to a secondary datacenter. For example, your vault in West US is automatically replicated to East US.
3. Configure the backup policy and select the VM from the same UI.
4. Make sure the Backup Agent is installed on the VM. If your VM is created by using an Azure gallery image, then the Backup Agent is already installed. Otherwise (that is, if you use a custom image), use the instructions to [install the VM agent on a virtual machine](#).

5. After the previous steps are completed, the backup runs at regular intervals as specified in the backup policy. If necessary, you can trigger the first backup manually from the vault dashboard on the Azure portal.

For automating Azure Backup by using scripts, refer to [PowerShell cmdlets for VM backup](#).

Steps for recovery

If you need to repair or rebuild a VM, you can restore the VM from any of the backup recovery points in the vault. There are a couple of different options for performing the recovery:

- You can create a new VM as a point-in-time representation of your backed-up VM.
- You can restore the disks, and then use the template for the VM to customize and rebuild the restored VM.

For more information, see the instructions to [use the Azure portal to restore virtual machines](#). This document also explains the specific steps for restoring backed-up VMs to a paired datacenter by using your geo-redundant backup vault if there is a disaster at the primary datacenter. In that case, Azure Backup uses the Compute service from the secondary region to create the restored virtual machine.

You can also use PowerShell for [creating a new VM from restored disks](#).

Alternative solution: Consistent snapshots

If you are unable to use Azure Backup, you can implement your own backup mechanism by using snapshots. Creating consistent snapshots for all the disks used by a VM and then replicating those snapshots to another region is complicated. For this reason, Azure considers using the Backup service as a better option than building a custom solution.

If you use read-access geo-redundant storage/geo-redundant storage for disks, snapshots are automatically replicated to a secondary datacenter. If you use locally redundant storage for disks, you need to replicate the data yourself. For more information, see [Back up Azure-unmanaged VM disks with incremental snapshots](#).

A snapshot is a representation of an object at a specific point in time. A snapshot incurs billing for the incremental size of the data it holds. For more information, see [Create a blob snapshot](#).

Create snapshots while the VM is running

Although you can take a snapshot at any time, if the VM is running, there is still data being streamed to the disks. The snapshots might contain partial operations that were in flight. Also, if there are several disks involved, the snapshots of different disks might have occurred at different times. These scenarios may cause the snapshots to be uncoordinated. This lack of co-ordination is especially problematic for striped volumes whose files might be corrupted if changes were being made during backup.

To avoid this situation, the backup process must implement the following steps:

1. Freeze all the disks.
2. Flush all the pending writes.
3. [Create a blob snapshot](#) for all the disks.

Some Windows applications, like SQL Server, provide a coordinated backup mechanism via a volume shadow service to create application-consistent backups. On Linux, you can use a tool like `fsfreeze` for coordinating the disks. This tool provides file-consistent backups, but not application-consistent snapshots. This process is complex, so you should consider using [Azure Backup](#) or a third-party backup solution that already implements this procedure.

The previous process results in a collection of coordinated snapshots for all of the VM disks, representing a specific point-in-time view of the VM. This is a backup restore point for the VM. You can repeat the process at scheduled intervals to create periodic backups. See [Copy the backups to another region](#) for steps to copy the snapshots to

another region for DR.

Create snapshots while the VM is offline

Another option to create consistent backups is to shut down the VM and take blob snapshots of each disk. Taking blob snapshots is easier than coordinating snapshots of a running VM, but it requires a few minutes of downtime.

1. Shut down the VM.
2. Create a snapshot of each virtual hard drive blob, which only takes a few seconds.

To create a snapshot, you can use [PowerShell](#), the [Azure Storage REST API](#), [Azure CLI](#), or one of the Azure Storage client libraries, such as [the Storage client library for .NET](#).

3. Start the VM, which ends the downtime. Typically, the entire process finishes within a few minutes.

This process yields a collection of consistent snapshots for all the disks, providing a backup restore point for the VM.

Copy the snapshots to another region

Creation of the snapshots alone might not be sufficient for DR. You must also replicate the snapshot backups to another region.

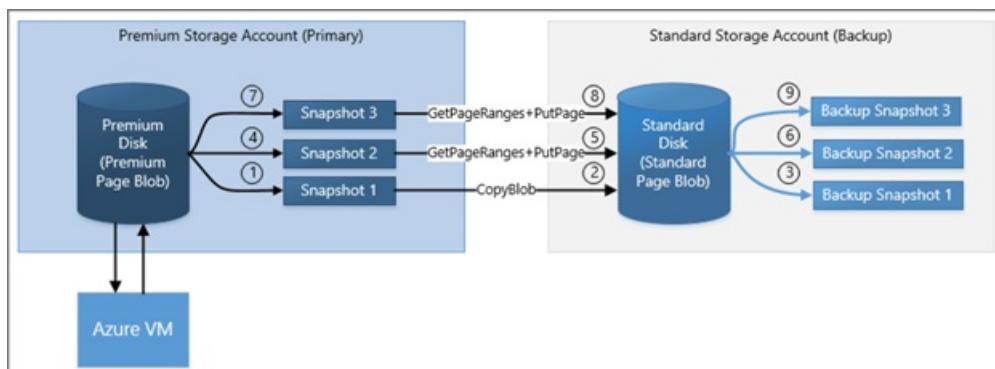
If you use geo-redundant storage or read-access geo-redundant storage for your disks, then the snapshots are replicated to the secondary region automatically. There can be a few minutes of lag before the replication. If the primary datacenter goes down before the snapshots finish replicating, you cannot access the snapshots from the secondary datacenter. The likelihood of this is small.

NOTE

Only having the disks in a geo-redundant storage or read-access geo-redundant storage account does not protect the VM from disasters. You must also create coordinated snapshots or use Azure Backup. This is required to recover a VM to a consistent state.

If you use locally redundant storage, you must copy the snapshots to a different storage account immediately after creating the snapshot. The copy target might be a locally redundant storage account in a different region, resulting in the copy being in a remote region. You can also copy the snapshot to a read-access geo-redundant storage account in the same region. In this case, the snapshot is lazily replicated to the remote secondary region. Your backup is protected from disasters at the primary site after the copying and replication is complete.

To copy your incremental snapshots for DR efficiently, review the instructions in [Back up Azure unmanaged VM disks with incremental snapshots](#).



Recovery from snapshots

To retrieve a snapshot, copy it to make a new blob. If you are copying the snapshot from the primary account, you can copy the snapshot over to the base blob of the snapshot. This process reverts the disk to the snapshot. This process is known as promoting the snapshot. If you are copying the snapshot backup from a secondary account, in

the case of a read-access geo-redundant storage account, you must copy it to a primary account. You can copy a snapshot by [using PowerShell](#) or by using the AzCopy utility. For more information, see [Transfer data with the AzCopy command-line utility](#).

For VMs with multiple disks, you must copy all the snapshots that are part of the same coordinated restore point. After you copy the snapshots to writable VHD blobs, you can use the blobs to recreate your VM by using the template for the VM.

Other options

SQL Server

SQL Server running in a VM has its own built-in capabilities to back up your SQL Server database to Azure Blob storage or a file share. If the storage account is geo-redundant storage or read-access geo-redundant storage, you can access those backups in the storage account's secondary datacenter in the event of a disaster, with the same restrictions as previously discussed. For more information, see [Back up and restore for SQL Server in Azure virtual machines](#). In addition to back up and restore, [SQL Server AlwaysOn availability groups](#) can maintain secondary replicas of databases. This ability greatly reduces the disaster recovery time.

Other considerations

This article has discussed how to back up or take snapshots of your VMs and their disks to support disaster recovery and how to use those backups or snapshots to recover your data. With the Azure Resource Manager model, many people use templates to create their VMs and other infrastructures in Azure. You can use a template to create a VM that has the same configuration every time. If you use custom images for creating your VMs, you must also make sure that your images are protected by using a read-access geo-redundant storage account to store them.

Consequently, your backup process can be a combination of two things:

- Back up the data (disks).
- Back up the configuration (templates and custom images).

Depending on the backup option you choose, you might have to handle the backup of both the data and the configuration, or the backup service might handle all of that for you.

Appendix: Understanding the impact of data redundancy

For storage accounts in Azure, there are three types of data redundancy that you should consider regarding disaster recovery: locally redundant, geo-redundant, or geo-redundant with read access.

Locally redundant storage retains three copies of the data in the same datacenter. When the VM writes the data, all three copies are updated before success is returned to the caller, so you know they are identical. Your disk is protected from local failures, because it's unlikely that all three copies are affected at the same time. In the case of locally redundant storage, there is no geo-redundancy, so the disk is not protected from catastrophic failures that can affect an entire datacenter or storage unit.

With geo-redundant storage and read-access geo-redundant storage, three copies of your data are retained in the primary region that is selected by you. Three more copies of your data are retained in a corresponding secondary region that is set by Azure. For example, if you store data in West US, the data is replicated to East US. Copy retention is done asynchronously, and there is a small delay between updates to the primary and secondary sites. Replicas of the disks on the secondary site are consistent on a per-disk basis (with the delay), but replicas of multiple active disks might not be in sync with each other. To have consistent replicas across multiple disks, consistent snapshots are needed.

The main difference between geo-redundant storage and read-access geo-redundant storage is that with read-

access geo-redundant storage, you can read the secondary copy at any time. If there is a problem that renders the data in the primary region inaccessible, the Azure team makes every effort to restore access. While the primary is down, if you have read-access geo-redundant storage enabled, you can access the data in the secondary datacenter. Therefore, if you plan to read from the replica while the primary is inaccessible, then read-access geo-redundant storage should be considered.

If it turns out to be a significant outage, the Azure team might trigger a geo-failover and change the primary DNS entries to point to secondary storage. At this point, if you have either geo-redundant storage or read-access geo-redundant storage enabled, you can access the data in the region that used to be the secondary. In other words, if your storage account is geo-redundant storage and there is a problem, you can access the secondary storage only if there is a geo-failover.

For more information, see [What to do if an Azure Storage outage occurs](#).

NOTE

Microsoft controls whether a failover occurs. Failover is not controlled per storage account, so it's not decided by individual customers. To implement disaster recovery for specific storage accounts or virtual machine disks, you must use the techniques described previously in this article.

Azure shared disks

2/19/2020 • 4 minutes to read • [Edit Online](#)

Azure shared disks (preview) is a new feature for Azure managed disks that enables attaching an Azure managed disk to multiple virtual machines (VMs) simultaneously. Attaching a managed disk to multiple VMs allows you to either deploy new or migrate existing clustered applications to Azure.

How it works

VMs in the cluster can read or write to your attached disk based on the reservation chosen by the clustered application using [SCSI Persistent Reservations](#) (SCSI PR). SCSI PR is a well-known industry standard leveraged by applications running on Storage Area Network (SAN) on-premises. Enabling SCSI PR on a managed disk allows you to migrate these applications to Azure as-is.

Managed disks with shared disks enabled offer shared block storage that can be accessed by multiple VMs, this is exposed as logical unit numbers (LUNs). LUNs are then presented to an initiator (VM) from a target (disk). These LUNs look like direct-attached-storage (DAS) or a local drive to the VM.

Managed disks with shared disks enabled do not natively offer a fully-managed file system that can be accessed using SMB/NFS. You will need to use a cluster manager, like Windows Server Failover Cluster (WSFC) or Pacemaker, that handles cluster node communication as well as write locking.

Limitations

While in preview, managed disks that have shared disks enabled are subject to the following limitations:

- Currently only available with premium SSDs.
- Currently only supported in the West Central US region.
- All virtual machines sharing a disk must be deployed in the same [proximity placement groups](#).
- Can only be enabled on data disks, not OS disks.
- Only basic disks can be used with some versions of Windows Server Failover Cluster, for details see [Failover clustering hardware requirements and storage options](#).
- ReadOnly host caching is not available for premium SSDs with `maxShares>1`.
- Availability sets and virtual machine scale sets can only be used with `FaultDomainCount` set to 1.
- Azure Backup and Azure Site Recovery support is not yet available.

If you're interested in trying shared disks then [sign up for our preview](#).

Disk sizes

For now, only premium SSDs can enable shared disks. The disk sizes that support this feature are P15 and greater. Different disk sizes may have a different `maxShares` limit, which you cannot exceed when setting the `maxshares` value.

For each disk, you can define a `maxShares` value that represents the maximum number of nodes that can simultaneously share the disk. For example, if you plan to set up a 2-node failover cluster, you would set `maxShares=2`. The maximum value is an upper bound. Nodes can join or leave the cluster (mount or unmount the disk) as long as the number of nodes is lower than the specified `maxShares` value.

NOTE

The `maxShares` value can only be set or edited when the disk is detached from all nodes.

The following table illustrates the allowed maximum values for `maxShares` by disk size:

DISK SIZES	MAXSHARES LIMIT
P15, P20	2
P30, P40, P50	5
P60, P70, P80	10

The IOPS and bandwidth limits for a disk are not affected by the `maxShares` value. For example, the max IOPS of a P15 disk are 1100 whether `maxShares = 1` or `maxShares > 1`.

Sample workloads

Windows

Most Windows-based clustering build on WSFC, which handles all core infrastructure for cluster node communication, allowing your applications to take advantage of parallel access patterns. WSFC enables both CSV and non-CVS-based options depending on your version of Windows Server. For details, refer to [Create a failover cluster](#).

Some popular applications running on WSFC include:

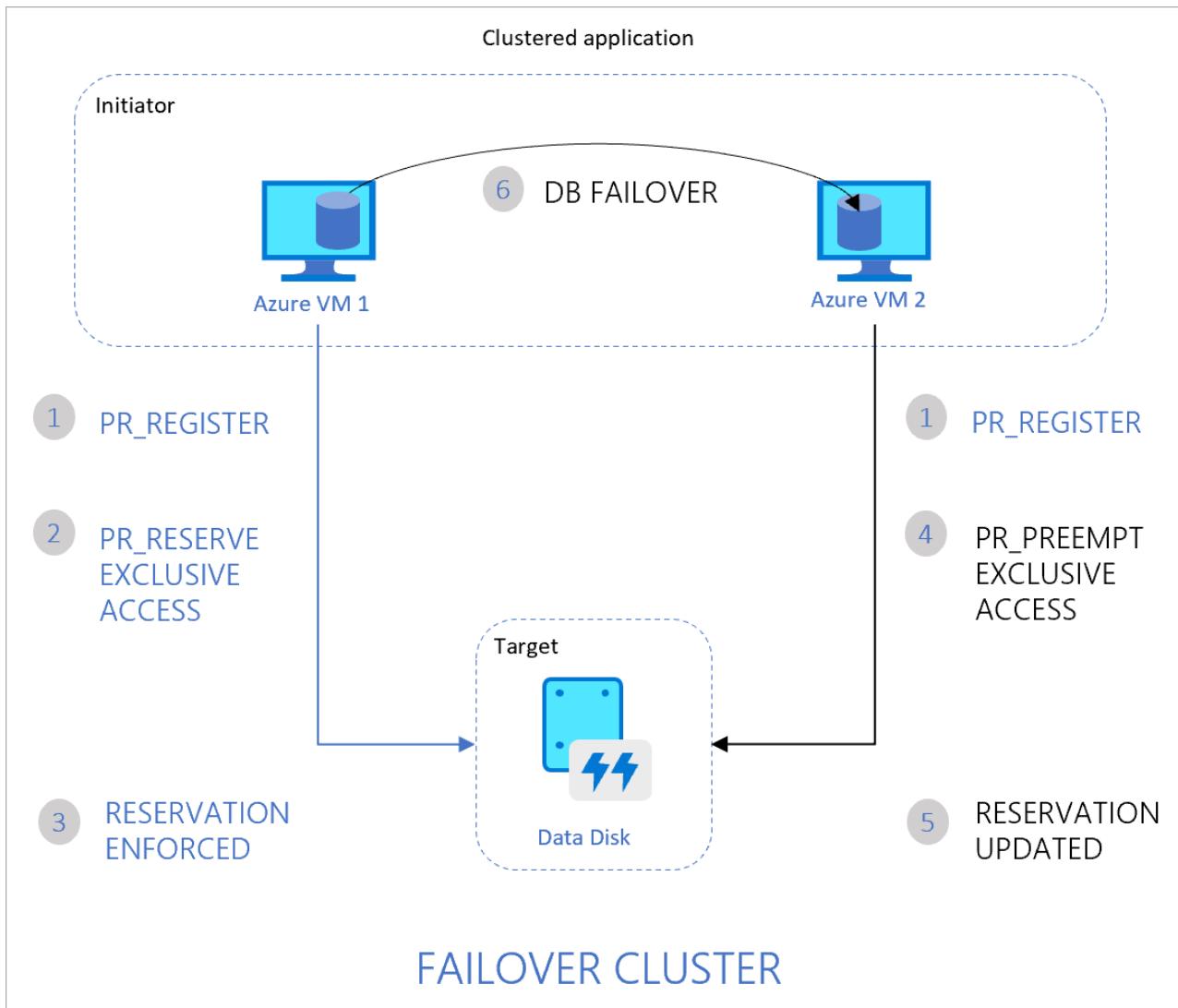
- SQL Server Failover Cluster Instances (FCI)
- Scale-out File Server (SoFS)
- File Server for General Use (IW workload)
- Remote Desktop Server User Profile Disk (RDS UPD)
- SAP ASCS/SCS

Linux

Linux clusters can leverage cluster managers such as [Pacemaker](#). Pacemaker builds on [Corosync](#), enabling cluster communications for applications deployed in highly available environments. Some common clustered filesystems include [ocfs2](#) and [gfs2](#). You can manipulate reservations and registrations using utilities such as [fence_scsi](#) and [sg_persist](#).

Persistent Reservation flow

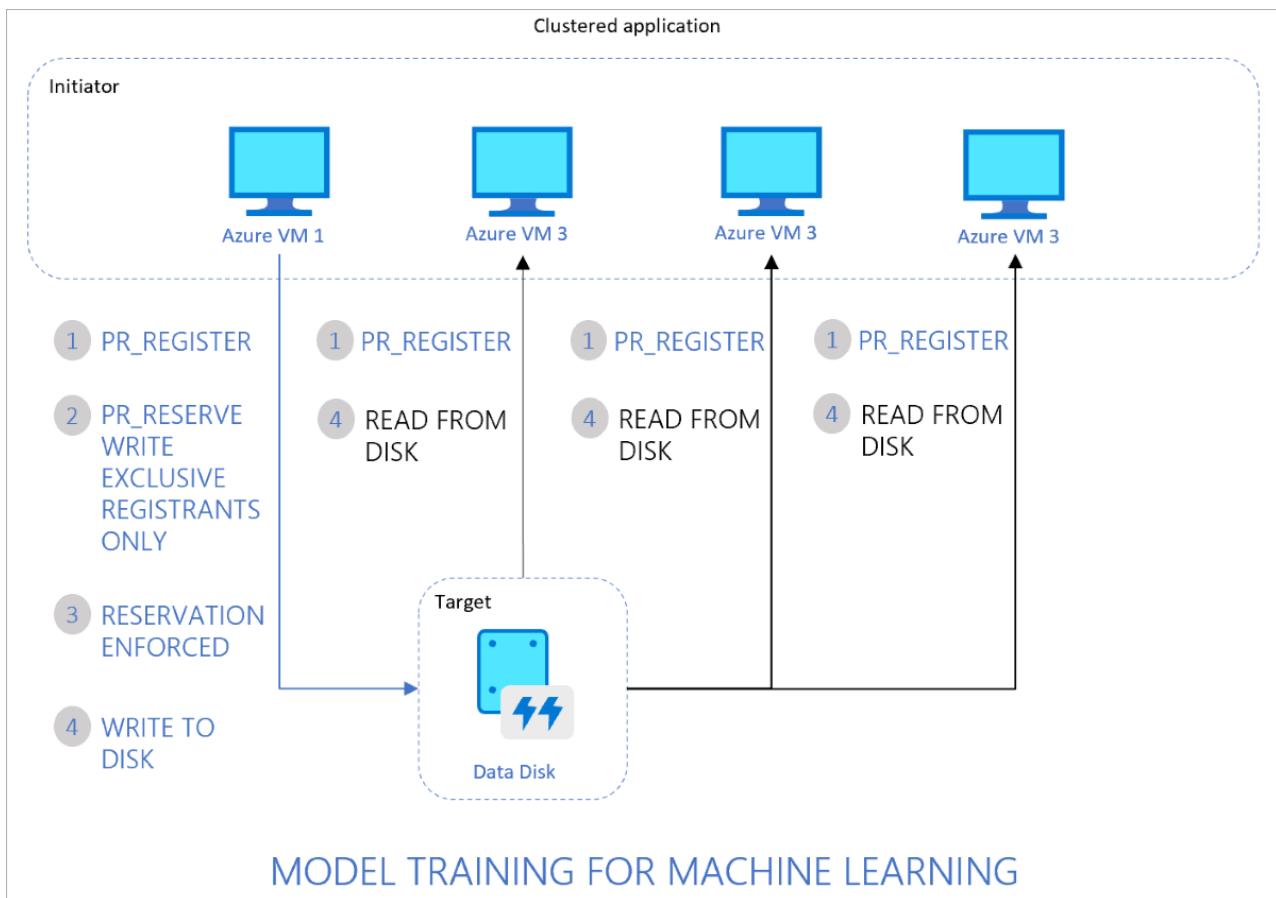
The following diagram illustrates a sample 2-node clustered database application that leverages SCSI PR to enable failover from one node to the other.



The flow is as follows:

1. The clustered application running on both Azure VM1 and VM2 registers its intent to read or write to the disk.
2. The application instance on VM1 then takes exclusive reservation to write to the disk.
3. This reservation is enforced on your Azure disk and the database can now exclusively write to the disk. Any writes from the application instance on VM2 will not succeed.
4. If the application instance on VM1 goes down, the instance on VM2 can now initiate a database failover and take-over of the disk.
5. This reservation is now enforced on the Azure disk and the disk will no longer accept writes from VM1. It will only accept writes from VM2.
6. The clustered application can complete the database failover and serve requests from VM2.

The following diagram illustrates another common clustered workload consisting of multiple nodes reading data from the disk for running parallel processes, such as training of machine learning models.



The flow is as follows:

1. The clustered application running on all VMs registers the intent to read or write to the disk.
2. The application instance on VM1 takes an exclusive reservation to write to the disk while opening up reads to the disk from other VMs.
3. This reservation is enforced on your Azure disk.
4. All nodes in the cluster can now read from the disk. Only one node writes back results to the disk, on behalf of all nodes in the cluster.

Next steps

If you're interested in enabling and using shared disks for your managed disks, proceed to our article [Enable shared disk](#)

Ephemeral OS disks for Azure VMs

11/13/2019 • 6 minutes to read • [Edit Online](#)

Ephemeral OS disks are created on the local virtual machine (VM) storage and not saved to the remote Azure Storage. Ephemeral OS disks work well for stateless workloads, where applications are tolerant of individual VM failures, but are more affected by VM deployment time or reimaging the individual VM instances. With Ephemeral OS disk, you get lower read/write latency to the OS disk and faster VM reimage.

The key features of ephemeral disks are:

- Ideal for stateless applications.
- They can be used with both Marketplace and custom images.
- Ability to fast reset or reimagine VMs and scale set instances to the original boot state.
- Lower latency, similar to a temporary disk.
- Ephemeral OS disks are free, you incur no storage cost for OS disk.
- They are available in all Azure regions.
- Ephemeral OS Disk is supported by [Shared Image Gallery](#).

Key differences between persistent and ephemeral OS disks:

	PERSISTENT OS DISK	EPHEMERAL OS DISK
Size limit for OS disk	2 TiB	Cache size for the VM size or 2TiB, whichever is smaller. For the cache size in GiB , see DS , ES , M , FS , and GS
VM sizes supported	All	DSv1, DSv2, DSv3, Esv3, Fs, FsV2, GS, M
Disk type support	Managed and unmanaged OS disk	Managed OS disk only
Region support	All regions	All regions
Data persistence	OS disk data written to OS disk are stored in Azure Storage	Data written to OS disk is stored to the local VM storage and is not persisted to Azure Storage.
Stop-deallocated state	VMs and scale set instances can be stop-deallocated and restarted from the stop-deallocated state	VMs and scale set instances cannot be stop-deallocated
Specialized OS disk support	Yes	No
OS disk resize	Supported during VM creation and after VM is stop-deallocated	Supported during VM creation only

	PERSISTENT OS DISK	EPHEMERAL OS DISK
Resizing to a new VM size	OS disk data is preserved	Data on the OS disk is deleted, OS is re-provisioned

Size requirements

You can deploy VM and instance images up to the size of the VM cache. For example, Standard Windows Server images from the marketplace are about 127 GiB, which means that you need a VM size that has a cache larger than 127 GiB. In this case, the [Standard_DS2_v2](#) has a cache size of 86 GiB, which is not large enough. The Standard_DS3_v2 has a cache size of 172 GiB, which is large enough. In this case, the Standard_DS3_v2 is the smallest size in the DSv2 series that you can use with this image. Basic Linux images in the Marketplace and Windows Server images that are denoted by `[smallsize]` tend to be around 30 GiB and can use most of the available VM sizes.

Ephemeral disks also require that the VM size supports Premium storage. The sizes usually (but not always) have an `s` in the name, like DSv2 and EsV3. For more information, see [Azure VM sizes](#) for details around which sizes support Premium storage.

PowerShell

To use an ephemeral disk for a PowerShell VM deployment, use [Set-AzVMOSDisk](#) in your VM configuration. Set the `-DiffDiskSetting` to `Local` and `-Caching` to `ReadOnly`.

```
Set-AzVMOSDisk -DiffDiskSetting Local -Caching ReadOnly
```

For scale set deployments, use the [Set-AzVmssStorageProfile](#) cmdlet in your configuration. Set the `-DiffDiskSetting` to `Local` and `-Caching` to `ReadOnly`.

```
Set-AzVmssStorageProfile -DiffDiskSetting Local -OsDiskCaching ReadOnly
```

CLI

To use an ephemeral disk for a CLI VM deployment, set the `--ephemeral-os-disk` parameter in [az vm create](#) to `true` and the `--os-disk-caching` parameter to `ReadOnly`.

```
az vm create \
--resource-group myResourceGroup \
--name myVM \
--image UbuntuLTS \
--ephemeral-os-disk true \
--os-disk-caching ReadOnly \
--admin-username azureuser \
--generate-ssh-keys
```

For scale sets, you use the same `--ephemeral-os-disk true` parameter for [az-vmss-create](#) and set the `--os-disk-caching` parameter to `ReadOnly`.

Portal

In the Azure portal, you can choose to use ephemeral disks when deploying a VM by opening the **Advanced** section of the **Disks** tab. For **Use ephemeral OS disk** select **Yes**.

Home > New > Create a virtual machine

Create a virtual machine

Basics **Disks** **Networking** **Management** **Advanced** **Tags** **Review + create**

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

Disk options

* OS disk type Ephemeral OS Disks only support the Standard HDD disk type.

Enable Ultra SSD compatibility (Preview) Yes No Ultra SSD disks are not available when using ephemeral disks.

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	NAME	SIZE (GiB)	DISK TYPE	HOST CACHING

[Create and attach a new disk](#) [Attach an existing disk](#)

Advanced

Use managed disks No Yes

Use ephemeral OS disk No Yes

If the option for using an ephemeral disk is greyed out, you might have selected a VM size that does not have a cache size larger than the OS image or that doesn't support Premium storage. Go back to the **Basics** page and try choosing another VM size.

You can also create scale-sets with ephemeral OS disks using the portal. Just make sure you select a VM size with a large enough cache size and then in **Use ephemeral OS disk** select **Yes**.

INSTANCES

* Instance count

* Instance size **Standard DS3 v2**
4 vcpus, 14 GiB memory [Change size](#)

Deploy as low priority (preview) No Yes

Use managed disks No Yes

Use ephemeral OS disk No Yes

Scale set template deployment

The process to create a scale set that uses an ephemeral OS disk is to add the `diffDiskSettings` property to the `Microsoft.Compute/virtualMachineScaleSets/virtualMachineProfile` resource type in the template. Also, the caching policy must be set to `ReadOnly` for the ephemeral OS disk.

```
{
  "type": "Microsoft.Compute/virtualMachineScaleSets",
  "name": "myScaleSet",
  "location": "East US 2",
  "apiVersion": "2018-06-01",
  "sku": {
    "name": "Standard_DS2_v2",
    "capacity": "2"
  },
  "properties": {
    "upgradePolicy": {
      "mode": "Automatic"
    },
    "virtualMachineProfile": {
      "storageProfile": {
        "osDisk": {
          "diffDiskSettings": {
            "option": "Local"
          },
          "caching": "ReadOnly",
          "createOption": "FromImage"
        },
        "imageReference": {
          "publisher": "Canonical",
          "offer": "UbuntuServer",
          "sku": "16.04-LTS",
          "version": "latest"
        }
      },
      "osProfile": {
        "computerNamePrefix": "myvmss",
        "adminUsername": "azureuser",
        "adminPassword": "P@ssw0rd!"
      }
    }
  }
}
```

VM template deployment

You can deploy a VM with an ephemeral OS disk using a template. The process to create a VM that uses ephemeral OS disks is to add the `diffDiskSettings` property to the `Microsoft.Compute/virtualMachines` resource type in the template. Also, the caching policy must be set to `ReadOnly` for the ephemeral OS disk.

```
{
  "type": "Microsoft.Compute/virtualMachines",
  "name": "myVirtualMachine",
  "location": "East US 2",
  "apiVersion": "2018-06-01",
  "properties": {
    "storageProfile": {
      "osDisk": {
        "diffDiskSettings": {
          "option": "Local"
        },
        "caching": "ReadOnly",
        "createOption": "FromImage"
      },
      "imageReference": {
        "publisher": "MicrosoftWindowsServer",
        "offer": "WindowsServer",
        "sku": "2016-Datacenter-smalldisk",
        "version": "latest"
      },
      "hardwareProfile": {
        "vmSize": "Standard_DS2_v2"
      }
    },
    "osProfile": {
      "computerNamePrefix": "myvirtualmachine",
      "adminUsername": "azureuser",
      "adminPassword": "P@ssw0rd!"
    }
  }
}
```

Reimage a VM using REST

You can reimage a Virtual Machine instance with ephemeral OS disk using REST API as described below and via Azure Portal by going to Overview pane of the VM. For scale sets, reimaging is already available through Powershell, CLI, and the portal.

```
POST https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/{rgName}/providers/Microsoft.Compute/VirtualMachines/{vmName}/reimage?api-version=2018-06-01"
```

Frequently asked questions

Q: What is the size of the local OS Disks?

A: We support platform and custom images, up to the VM cache size, where all read/writes to the OS disk will be local on the same node as the Virtual Machine.

Q: Can the ephemeral OS disk be resized?

A: No, once the ephemeral OS disk is provisioned, the OS disk cannot be resized.

Q: Can I attach a Managed Disks to an Ephemeral VM?

A: Yes, you can attach a managed data disk to a VM that uses an ephemeral OS disk.

Q: Will all VM sizes be supported for ephemeral OS disks?

A: No, all Premium Storage VM sizes are supported (DS, ES, FS, GS and M) except the B-series, N-series, and H-series sizes.

Q: Can the ephemeral OS disk be applied to existing VMs and scale sets?

A: No, ephemeral OS disk can only be used during VM and scale set creation.

Q: Can you mix ephemeral and normal OS disks in a scale set?

A: No, you can't have a mix of ephemeral and persistent OS disk instances within the same scale set.

Q: Can the ephemeral OS disk be created using Powershell or CLI?

A: Yes, you can create VMs with Ephemeral OS Disk using REST, Templates, PowerShell and CLI.

Q: What features are not supported with ephemeral OS disk?

A: Ephemeral disks do not support:

- Capturing VM images
- Disk snapshots
- Azure Disk Encryption
- Azure Backup
- Azure Site Recovery
- OS Disk Swap

Next steps

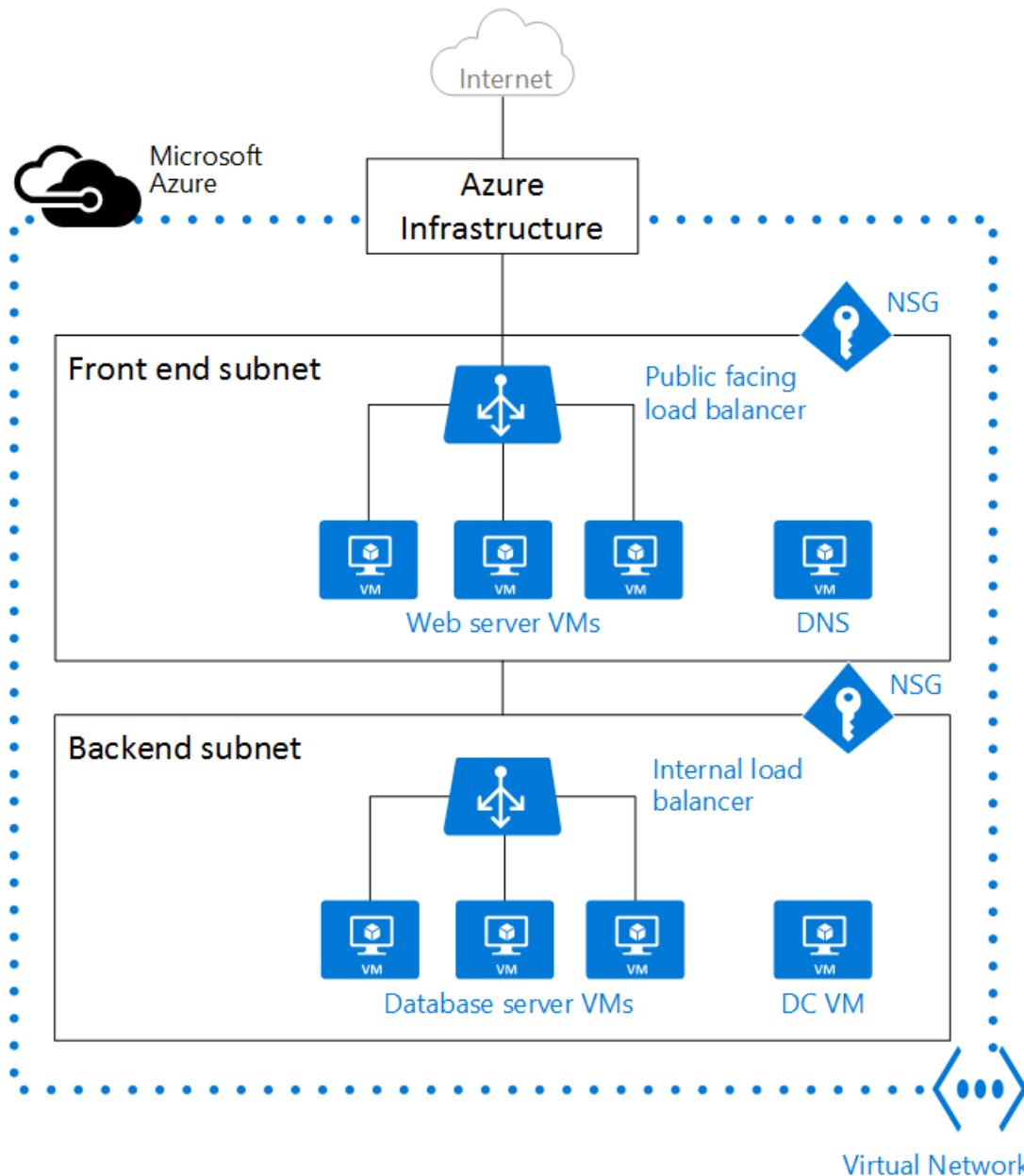
You can create a VM with an ephemeral OS disk using the [Azure CLI](#).

Virtual networks and virtual machines in Azure

11/13/2019 • 13 minutes to read • [Edit Online](#)

When you create an Azure virtual machine (VM), you must create a [virtual network](#) (VNet) or use an existing VNet. You also need to decide how your VMs are intended to be accessed on the VNet. It is important to [plan before creating resources](#) and make sure that you understand the [limits of networking resources](#).

In the following figure, VMs are represented as web servers and database servers. Each set of VMs are assigned to separate subnets in the VNet.



You can create a VNet before you create a VM or you can do so as you create a VM. You create these resources to support communication with a VM:

- Network interfaces
- IP addresses
- Virtual network and subnets

In addition to those basic resources, you should also consider these optional resources:

- Network security groups
- Load balancers

Network interfaces

A [network interface \(NIC\)](#) is the interconnection between a VM and a virtual network (VNet). A VM must have at least one NIC, but can have more than one, depending on the size of the VM you create. Learn about how many NICs each VM size supports for [Windows](#) or [Linux](#).

You can create a VM with multiple NICs, and add or remove NICs through the lifecycle of a VM. Multiple NICs allow a VM to connect to different subnets and send or receive traffic over the most appropriate interface. VMs with any number of network interfaces can exist in the same availability set, up to the number supported by the VM size.

Each NIC attached to a VM must exist in the same location and subscription as the VM. Each NIC must be connected to a VNet that exists in the same Azure location and subscription as the NIC. You can change the subnet a VM is connected to after it's created, but you cannot change the VNet. Each NIC attached to a VM is assigned a MAC address that doesn't change until the VM is deleted.

This table lists the methods that you can use to create a network interface.

METHOD	DESCRIPTION
Azure portal	When you create a VM in the Azure portal, a network interface is automatically created for you (you cannot use a NIC you create separately). The portal creates a VM with only one NIC. If you want to create a VM with more than one NIC, you must create it with a different method.
Azure PowerShell	Use New-AzNetworkInterface with the -PublicIpAddressId parameter to provide the identifier of the public IP address that you previously created.
Azure CLI	To provide the identifier of the public IP address that you previously created, use az network nic create with the --public-ip-address parameter.
Template	Use Network Interface in a Virtual Network with Public IP Address as a guide for deploying a network interface using a template.

IP addresses

You can assign these types of [IP addresses](#) to a NIC in Azure:

- **Public IP addresses** - Used to communicate inbound and outbound (without network address translation (NAT)) with the Internet and other Azure resources not connected to a VNet. Assigning a public IP address to a NIC is optional. Public IP addresses have a nominal charge, and there's a maximum number that can be used per subscription.
- **Private IP addresses** - Used for communication within a VNet, your on-premises network, and the Internet (with NAT). You must assign at least one private IP address to a VM. To learn more about NAT in Azure, read [Understanding outbound connections in Azure](#).

You can assign public IP addresses to VMs or internet-facing load balancers. You can assign private IP addresses to VMs and internal load balancers. You assign IP addresses to a VM using a network interface.

There are two methods in which an IP address is allocated to a resource - dynamic or static. The default allocation method is dynamic, where an IP address is not allocated when it's created. Instead, the IP address is allocated when you create a VM or start a stopped VM. The IP address is released when you stop or delete the VM.

To ensure the IP address for the VM remains the same, you can set the allocation method explicitly to static. In this case, an IP address is assigned immediately. It is released only when you delete the VM or change its allocation method to dynamic.

This table lists the methods that you can use to create an IP address.

METHOD	DESCRIPTION
Azure portal	By default, public IP addresses are dynamic and the address associated to them may change when the VM is stopped or deleted. To guarantee that the VM always uses the same public IP address, create a static public IP address. By default, the portal assigns a dynamic private IP address to a NIC when creating a VM. You can change this IP address to static after the VM is created.
Azure PowerShell	You use New-AzPublicIpAddress with the -AllocationMethod parameter as Dynamic or Static.
Azure CLI	You use az network public-ip create with the --allocation-method parameter as Dynamic or Static.
Template	Use Network Interface in a Virtual Network with Public IP Address as a guide for deploying a public IP address using a template.

After you create a public IP address, you can associate it with a VM by assigning it to a NIC.

Virtual network and subnets

A subnet is a range of IP addresses in the VNet. You can divide a VNet into multiple subnets for organization and security. Each NIC in a VM is connected to one subnet in one VNet. NICs connected to subnets (same or different) within a VNet can communicate with each other without any extra configuration.

When you set up a VNet, you specify the topology, including the available address spaces and subnets. If the VNet is to be connected to other VNets or on-premises networks, you must select address ranges that don't overlap. The IP addresses are private and can't be accessed from the Internet, which was true only for the non-routable IP addresses such as 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16. Now, Azure treats any address range as part of the private VNet IP address space that is only reachable within the VNet, within interconnected VNets, and from your on-premises location.

If you work within an organization in which someone else is responsible for the internal networks, you should talk to that person before selecting your address space. Make sure there is no overlap and let them know the space you want to use so they don't try to use the same range of IP addresses.

By default, there is no security boundary between subnets, so VMs in each of these subnets can talk to one another. However, you can set up Network Security Groups (NSGs), which allow you to control the traffic flow to and from subnets and to and from VMs.

This table lists the methods that you can use to create a VNet and subnets.

METHOD	DESCRIPTION
Azure portal	If you let Azure create a VNet when you create a VM, the name is a combination of the resource group name that contains the VNet and -vnet . The address space is 10.0.0.0/24, the required subnet name is default , and the subnet address range is 10.0.0.0/24.
Azure PowerShell	You use New-AzVirtualNetworkSubnetConfig and New-AzVirtualNetwork to create a subnet and a VNet. You can also use Add-AzVirtualNetworkSubnetConfig to add a subnet to an existing VNet.
Azure CLI	The subnet and the VNet are created at the same time. Provide a --subnet-name parameter to az network vnet create with the subnet name.
Template	The easiest way to create a VNet and subnets is to download an existing template, such as Virtual Network with two subnets , and modify it for your needs.

Network security groups

A [network security group \(NSG\)](#) contains a list of Access Control List (ACL) rules that allow or deny network traffic to subnets, NICs, or both. NSGs can be associated with either subnets or individual NICs connected to a subnet. When an NSG is associated with a subnet, the ACL rules apply to all the VMs in that subnet. In addition, traffic to an individual NIC can be restricted by associating an NSG directly to a NIC.

NSGs contain two sets of rules: inbound and outbound. The priority for a rule must be unique within each set. Each rule has properties of protocol, source and destination port ranges, address prefixes, direction of traffic, priority, and access type.

All NSGs contain a set of default rules. The default rules cannot be deleted, but because they are assigned the lowest priority, they can be overridden by the rules that you create.

When you associate an NSG to a NIC, the network access rules in the NSG are applied only to that NIC. If an NSG is applied to a single NIC on a multi-NIC VM, it does not affect traffic to the other NICs. You can associate different NSGs to a NIC (or VM, depending on the deployment model) and the subnet that a NIC or VM is bound to. Priority is given based on the direction of traffic.

Be sure to [plan](#) your NSGs when you plan your VMs and VNet.

This table lists the methods that you can use to create a network security group.

METHOD	DESCRIPTION
Azure portal	When you create a VM in the Azure portal, an NSG is automatically created and associated to the NIC the portal creates. The name of the NSG is a combination of the name of the VM and -nsg . This NSG contains one inbound rule with a priority of 1000, service set to RDP, the protocol set to TCP, port set to 3389, and action set to Allow. If you want to allow any other inbound traffic to the VM, you must add additional rules to the NSG.

METHOD	DESCRIPTION
Azure PowerShell	Use New-AzNetworkSecurityRuleConfig and provide the required rule information. Use New-AzNetworkSecurityGroup to create the NSG. Use Set-AzVirtualNetworkSubnetConfig to configure the NSG for the subnet. Use Set-AzVirtualNetwork to add the NSG to the VNet.
Azure CLI	Use az network nsg create to initially create the NSG. Use az network nsg rule create to add rules to the NSG. Use az network vnet subnet update to add the NSG to the subnet.
Template	Use Create a Network Security Group as a guide for deploying a network security group using a template.

Load balancers

[Azure Load Balancer](#) delivers high availability and network performance to your applications. A load balancer can be configured to [balance incoming Internet traffic](#) to VMs or [balance traffic between VMs in a VNet](#). A load balancer can also balance traffic between on-premises computers and VMs in a cross-premises network, or forward external traffic to a specific VM.

The load balancer maps incoming and outgoing traffic between the public IP address and port on the load balancer and the private IP address and port of the VM.

When you create a load balancer, you must also consider these configuration elements:

- **Front-end IP configuration** – A load balancer can include one or more front-end IP addresses, otherwise known as virtual IPs (VIPs). These IP addresses serve as ingress for the traffic.
- **Back-end address pool** – IP addresses that are associated with the NIC to which load is distributed.
- **NAT rules** - Defines how inbound traffic flows through the front-end IP and distributed to the back-end IP.
- **Load balancer rules** - Maps a given front-end IP and port combination to a set of back-end IP addresses and port combination. A single load balancer can have multiple load balancing rules. Each rule is a combination of a front-end IP and port and back-end IP and port associated with VMs.
- **Probes** - Monitors the health of VMs. When a probe fails to respond, the load balancer stops sending new connections to the unhealthy VM. The existing connections are not affected, and new connections are sent to healthy VMs.

This table lists the methods that you can use to create an internet-facing load balancer.

METHOD	DESCRIPTION
Azure portal	You can load balance internet traffic to VMs using the Azure portal .
Azure PowerShell	To provide the identifier of the public IP address that you previously created, use New-AzLoadBalancerFrontendIpConfig with the -PublicIpAddress parameter. Use New-AzLoadBalancerBackendAddressPoolConfig to create the configuration of the back-end address pool. Use New-AzLoadBalancerInboundNatRuleConfig to create inbound NAT rules associated with the front-end IP configuration that you created. Use New-AzLoadBalancerProbeConfig to create the probes that you need. Use New-AzLoadBalancerRuleConfig to create the load balancer configuration. Use New-AzLoadBalancer to create the load balancer.

METHOD	DESCRIPTION
Azure CLI	Use az network lb create to create the initial load balancer configuration. Use az network lb frontend-ip create to add the public IP address that you previously created. Use az network lb address-pool create to add the configuration of the back-end address pool. Use az network lb inbound-nat-rule create to add NAT rules. Use az network lb rule create to add the load balancer rules. Use az network lb probe create to add the probes.
Template	Use 2 VMs in a Load Balancer and configure NAT rules on the LB as a guide for deploying a load balancer using a template.

This table lists the methods that you can use to create an internal load balancer.

METHOD	DESCRIPTION
Azure portal	You can balance internal traffic load with a Basic load balancer in the Azure portal .
Azure PowerShell	To provide a private IP address in the network subnet, use New-AzLoadBalancerFrontendIpConfig with the -PrivateIpAddress parameter. Use New-AzLoadBalancerBackendAddressPoolConfig to create the configuration of the back-end address pool. Use New-AzLoadBalancerInboundNatRuleConfig to create inbound NAT rules associated with the front-end IP configuration that you created. Use New-AzLoadBalancerProbeConfig to create the probes that you need. Use New-AzLoadBalancerRuleConfig to create the load balancer configuration. Use New-AzLoadBalancer to create the load balancer.
Azure CLI	Use the az network lb create command to create the initial load balancer configuration. To define the private IP address, use az network lb frontend-ip create with the --private-ip-address parameter. Use az network lb address-pool create to add the configuration of the back-end address pool. Use az network lb inbound-nat-rule create to add NAT rules. Use az network lb rule create to add the load balancer rules. Use az network lb probe create to add the probes.
Template	Use 2 VMs in a Load Balancer and configure NAT rules on the LB as a guide for deploying a load balancer using a template.

VMs

VMs can be created in the same VNet and they can connect to each other using private IP addresses. They can connect even if they are in different subnets without the need to configure a gateway or use public IP addresses. To put VMs into a VNet, you create the VNet and then as you create each VM, you assign it to the VNet and subnet. VMs acquire their network settings during deployment or startup.

VMs are assigned an IP address when they are deployed. If you deploy multiple VMs into a VNet or subnet, they are assigned IP addresses as they boot up. You can also allocate a static IP to a VM. If you allocate a static IP, you should consider using a specific subnet to avoid accidentally reusing a static IP for another VM.

If you create a VM and later want to migrate it into a VNet, it is not a simple configuration change. You must redeploy the VM into the VNet. The easiest way to redeploy is to delete the VM, but not any disks attached to it,

and then re-create the VM using the original disks in the VNet.

This table lists the methods that you can use to create a VM in a VNet.

METHOD	DESCRIPTION
Azure portal	Uses the default network settings that were previously mentioned to create a VM with a single NIC. To create a VM with multiple NICs, you must use a different method.
Azure PowerShell	Includes the use of <code>Add-AzVMNetworkInterface</code> to add the NIC that you previously created to the VM configuration.
Azure CLI	Create and connect a VM to a Vnet, subnet, and NIC that build as individual steps.
Template	Use Very simple deployment of a Windows VM as a guide for deploying a VM using a template.

Next steps

For VM-specific steps on how to manage Azure virtual networks for VMs, see the [Windows](#) or [Linux](#) tutorials.

There are also tutorials on how to load balance VMs and create highly available applications for [Windows](#) or [Linux](#).

- Learn how to configure [user-defined routes and IP forwarding](#).
- Learn how to configure [VNet to VNet connections](#).
- Learn how to [Troubleshoot routes](#).
- Learn more about [Virtual machine network bandwidth](#).

What are virtual machine scale sets?

1/19/2020 • 4 minutes to read • [Edit Online](#)

Azure virtual machine scale sets let you create and manage a group of identical, load balanced VMs. The number of VM instances can automatically increase or decrease in response to demand or a defined schedule. Scale sets provide high availability to your applications, and allow you to centrally manage, configure, and update a large number of VMs. With virtual machine scale sets, you can build large-scale services for areas such as compute, big data, and container workloads.

Why use virtual machine scale sets?

To provide redundancy and improved performance, applications are typically distributed across multiple instances. Customers may access your application through a load balancer that distributes requests to one of the application instances. If you need to perform maintenance or update an application instance, your customers must be distributed to another available application instance. To keep up with additional customer demand, you may need to increase the number of application instances that run your application.

Azure virtual machine scale sets provide the management capabilities for applications that run across many VMs, [automatic scaling of resources](#), and load balancing of traffic. Scale sets provide the following key benefits:

- **Easy to create and manage multiple VMs**

- When you have many VMs that run your application, it's important to maintain a consistent configuration across your environment. For reliable performance of your application, the VM size, disk configuration, and application installs should match across all VMs.
- With scale sets, all VM instances are created from the same base OS image and configuration. This approach lets you easily manage hundreds of VMs without additional configuration tasks or network management.
- Scale sets support the use of the [Azure load balancer](#) for basic layer-4 traffic distribution, and [Azure Application Gateway](#) for more advanced layer-7 traffic distribution and SSL termination.

- **Provides high availability and application resiliency**

- Scale sets are used to run multiple instances of your application. If one of these VM instances has a problem, customers continue to access your application through one of the other VM instances with minimal interruption.
- For additional availability, you can use [Availability Zones](#) to automatically distribute VM instances in a scale set within a single datacenter or across multiple datacenters.

- **Allows your application to automatically scale as resource demand changes**

- Customer demand for your application may change throughout the day or week. To match customer demand, scale sets can automatically increase the number of VM instances as application demand increases, then reduce the number of VM instances as demand decreases.
- Autoscale also minimizes the number of unnecessary VM instances that run your application when demand is low, while customers continue to receive an acceptable level of performance as demand grows and additional VM instances are automatically added. This ability helps reduce costs and efficiently create Azure resources as required.

- **Works at large-scale**

- Scale sets support up to 1,000 VM instances. If you create and upload your own custom VM images, the limit is 600 VM instances.

- For the best performance with production workloads, use [Azure Managed Disks](#).

Differences between virtual machines and scale sets

Scale sets are built from virtual machines. With scale sets, the management and automation layers are provided to run and scale your applications. You could instead manually create and manage individual VMs, or integrate existing tools to build a similar level of automation. The following table outlines the benefits of scale sets compared to manually managing multiple VM instances.

SCENARIO	MANUAL GROUP OF VMs	VIRTUAL MACHINE SCALE SET
Add additional VM instances	Manual process to create, configure, and ensure compliance	Automatically create from central configuration
Traffic balancing and distribution	Manual process to create and configure Azure load balancer or Application Gateway	Can automatically create and integrate with Azure load balancer or Application Gateway
High availability and redundancy	Manually create Availability Set or distribute and track VMs across Availability Zones	Automatic distribution of VM instances across Availability Zones or Availability Sets
Scaling of VMs	Manual monitoring and Azure Automation	Autoscale based on host metrics, in-guest metrics, Application Insights, or schedule

There is no additional cost to scale sets. You only pay for the underlying compute resources such as the VM instances, load balancer, or Managed Disk storage. The management and automation features, such as autoscale and redundancy, incur no additional charges over the use of VMs.

How to monitor your scale sets

Use [Azure Monitor for VMs](#), which has a simple onboarding process and will automate the collection of important CPU, memory, disk, and network performance counters from the VMs in your scale set. It also includes additional monitoring capabilities and pre-defined visualizations that help you focus on the availability and performance of your scale sets.

Enable monitoring for your [virtual machine scale set application](#) with Application Insights to collect detailed information about your application including page views, application requests, and exceptions. Further verify the availability of your application by configuring an [availability test](#) to simulate user traffic.

Next steps

To get started, create your first virtual machine scale set in the Azure portal.

[Create a scale set in the Azure portal](#)

Use infrastructure automation tools with virtual machines in Azure

11/13/2019 • 6 minutes to read • [Edit Online](#)

To create and manage Azure virtual machines (VMs) in a consistent manner at scale, some form of automation is typically desired. There are many tools and solutions that allow you to automate the complete Azure infrastructure deployment and management lifecycle. This article introduces some of the infrastructure automation tools that you can use in Azure. These tools commonly fit in to one of the following approaches:

- Automate the configuration of VMs
 - Tools include [Ansible](#), [Chef](#), and [Puppet](#).
 - Tools specific to VM customization include [cloud-init](#) for Linux VMs, [PowerShell Desired State Configuration \(DSC\)](#), and the [Azure Custom Script Extension](#) for all Azure VMs.
- Automate infrastructure management
 - Tools include [Packer](#) to automate custom VM image builds, and [Terraform](#) to automate the infrastructure build process.
 - [Azure Automation](#) can perform actions across your Azure and on-premises infrastructure.
- Automate application deployment and delivery
 - Examples include [Azure DevOps Services](#) and [Jenkins](#).

Ansible

[Ansible](#) is an automation engine for configuration management, VM creation, or application deployment. Ansible uses an agent-less model, typically with SSH keys, to authenticate and manage target machines. Configuration tasks are defined in playbooks, with a number of Ansible modules available to carry out specific tasks. For more information, see [How Ansible works](#).

Learn how to:

- [Install and configure Ansible on Linux for use with Azure](#).
- [Create a Linux virtual machine](#).
- [Manage a Linux virtual machine](#).

Chef

[Chef](#) is an automation platform that helps define how your infrastructure is configured, deployed, and managed. Additional components included Chef Habitat for application lifecycle automation rather than the infrastructure, and Chef InSpec that helps automate compliance with security and policy requirements. Chef Clients are installed on target machines, with one or more central Chef Servers that store and manage the configurations. For more information, see [An Overview of Chef](#).

Learn how to:

- [Deploy Chef Automate from the Azure Marketplace](#).
- [Install Chef on Windows and create Azure VMs](#).

Puppet

Puppet is an enterprise-ready automation platform that handles the application delivery and deployment process. Agents are installed on target machines to allow Puppet Master to run manifests that define the desired configuration of the Azure infrastructure and VMs. Puppet can integrate with other solutions such as Jenkins and GitHub for an improved devops workflow. For more information, see [How Puppet works](#).

Learn how to:

- [Deploy Puppet from the Azure Marketplace](#).

Cloud-init

[Cloud-init](#) is a widely used approach to customize a Linux VM as it boots for the first time. You can use cloud-init to install packages and write files, or to configure users and security. Because cloud-init is called during the initial boot process, there are no additional steps or required agents to apply your configuration. For more information on how to properly format your `#cloud-config` files, see the [cloud-init documentation site](#). `#cloud-config` files are text files encoded in base64.

Cloud-init also works across distributions. For example, you don't use **apt-get install** or **yum install** to install a package. Instead you can define a list of packages to install. Cloud-init automatically uses the native package management tool for the distro you select.

We are actively working with our endorsed Linux distro partners in order to have cloud-init enabled images available in the Azure marketplace. These images make your cloud-init deployments and configurations work seamlessly with VMs and virtual machine scale sets. Learn more details about cloud-init on Azure:

- [Cloud-init support for Linux virtual machines in Azure](#)
- [Try a tutorial on automated VM configuration using cloud-init](#).

PowerShell DSC

[PowerShell Desired State Configuration \(DSC\)](#) is a management platform to define the configuration of target machines. DSC can also be used on Linux through the [Open Management Infrastructure \(OMI\) server](#).

DSC configurations define what to install on a machine and how to configure the host. A Local Configuration Manager (LCM) engine runs on each target node that processes requested actions based on pushed configurations. A pull server is a web service that runs on a central host to store the DSC configurations and associated resources. The pull server communicates with the LCM engine on each target host to provide the required configurations and report on compliance.

Learn how to:

- [Create a basic DSC configuration](#).
- [Configure a DSC pull server](#).
- [Use DSC for Linux](#).

Azure Custom Script Extension

The Azure Custom Script Extension for [Linux](#) or [Windows](#) downloads and executes scripts on Azure VMs. You can use the extension when you create a VM, or any time after the VM is in use.

Scripts can be downloaded from Azure storage or any public location such as a GitHub repository. With the Custom Script Extension, you can write scripts in any language that runs on the source VM. These scripts can be used to install applications or configure the VM as desired. To secure credentials, sensitive information such as passwords can be stored in a protected configuration. These credentials are only decrypted inside the VM.

Learn how to:

- [Create a Linux VM with the Azure CLI and use the Custom Script Extension.](#)
- [Create a Windows VM with Azure PowerShell and use the Custom Script Extension.](#)

Packer

[Packer](#) automates the build process when you create a custom VM image in Azure. You use Packer to define the OS and run post-configuration scripts that customize the VM for your specific needs. Once configured, the VM is then captured as a Managed Disk image. Packer automates the process to create the source VM, network and storage resources, run configuration scripts, and then create the VM image.

Learn how to:

- [Use Packer to create a Linux VM image in Azure.](#)
- [Use Packer to create a Windows VM image in Azure.](#)

Terraform

[Terraform](#) is an automation tool that allows you to define and create an entire Azure infrastructure with a single template format language - the HashiCorp Configuration Language (HCL). With Terraform, you define templates that automate the process to create network, storage, and VM resources for a given application solution. You can use your existing Terraform templates for other platforms with Azure to ensure consistency and simplify the infrastructure deployment without needing to convert to an Azure Resource Manager template.

Learn how to:

- [Install and configure Terraform with Azure.](#)
- [Create an Azure infrastructure with 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 Windows and Linux machines.

Learn how to:

- [Create a PowerShell runbook.](#)
- [Use Hybrid Runbook Worker to manage on-premises resources.](#)
- [Use Azure Automation DSC.](#)

Azure DevOps Services

[Azure DevOps Services](#) is a suite of tools that help you share and track code, use automated builds, and create a complete continuous integration and development (CI/CD) pipeline. Azure DevOps Services integrates with Visual Studio and other editors to simplify usage. Azure DevOps Services can also create and configure Azure VMs and then deploy code to them.

Learn more about:

- [Azure DevOps Services.](#)

Jenkins

Jenkins is a continuous integration server that helps deploy and test applications, and create automated pipelines for code delivery. There are hundreds of plugins to extend the core Jenkins platform, and you can also integrate with many other products and solutions through webhooks. You can manually install Jenkins on an Azure VM, run Jenkins from within a Docker container, or use a pre-built Azure Marketplace image.

Learn how to:

- [Create a development infrastructure on a Linux VM in Azure with Jenkins, GitHub, and Docker.](#)

Next steps

There are many different options to use infrastructure automation tools in Azure. You have the freedom to use the solution that best fits your needs and environment. To get started and try some of the tools built-in to Azure, see how to automate the customization of a [Linux](#) or [Windows](#) VM.

Secure and use policies on virtual machines in Azure

11/13/2019 • 4 minutes to read • [Edit Online](#)

It's important to keep your virtual machine (VM) secure for the applications that you run. Securing your VMs can include one or more Azure services and features that cover secure access to your VMs and secure storage of your data. This article provides information that enables you to keep your VM and applications secure.

Antimalware

The modern threat landscape for cloud environments is dynamic, increasing the pressure to maintain effective protection in order to meet compliance and security requirements. [Microsoft Antimalware for Azure](#) is a free real-time protection capability that helps identify and remove viruses, spyware, and other malicious software. Alerts can be configured to notify you when known malicious or unwanted software attempts to install itself or run on your VM. It is not supported on VMs running Linux or Windows Server 2008.

Azure Security Center

[Azure Security Center](#) helps you prevent, detect, and respond to threats to your VMs. Security Center provides integrated security monitoring and policy management across your Azure subscriptions, helps detect threats that might otherwise go unnoticed, and works with a broad ecosystem of security solutions.

Security Center's just-in-time access can be applied across your VM deployment to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed. When just-in-time is enabled and a user requests access to a VM, Security Center checks what permissions the user has for the VM. If they have the correct permissions, the request is approved and Security Center automatically configures the Network Security Groups (NSGs) to allow inbound traffic to the selected ports for a limited amount of time. After the time has expired, Security Center restores the NSGs to their previous states.

Encryption

For enhanced [Windows VM](#) and [Linux VM](#) security and compliance, virtual disks in Azure can be encrypted. Virtual disks on Windows VMs are encrypted at rest using BitLocker. Virtual disks on Linux VMs are encrypted at rest using dm-crypt.

There is no charge for encrypting virtual disks in Azure. Cryptographic keys are stored in Azure Key Vault using software-protection, or you can import or generate your keys in Hardware Security Modules (HSMs) certified to FIPS 140-2 level 2 standards. These cryptographic keys are used to encrypt and decrypt virtual disks attached to your VM. You retain control of these cryptographic keys and can audit their use. An Azure Active Directory service principal provides a secure mechanism for issuing these cryptographic keys as VMs are powered on and off.

Key Vault and SSH Keys

Secrets and certificates can be modeled as resources and provided by [Key Vault](#). You can use Azure PowerShell to create key vaults for [Windows VMs](#) and the Azure CLI for [Linux VMs](#). You can also create keys for encryption.

Key vault access policies grant permissions to keys, secrets, and certificates separately. For example, you can give a user access to only keys, but no permissions for secrets. However, permissions to access keys or secrets or certificates are at the vault level. In other words, [key vault access policy](#) does not support object level permissions.

When you connect to VMs, you should use public-key cryptography to provide a more secure way to sign in to them. This process involves a public and private key exchange using the secure shell (SSH) command to

authenticate yourself rather than a username and password. Passwords are vulnerable to brute-force attacks, especially on Internet-facing VMs such as web servers. With a secure shell (SSH) key pair, you can create a [Linux VM](#) that uses SSH keys for authentication, eliminating the need for passwords to sign-in. You can also use SSH keys to connect from a [Windows VM](#) to a Linux VM.

Managed identities for Azure resources

A common challenge when building cloud applications is how to manage the credentials in your code for authenticating to cloud services. Keeping the credentials secure is an important task. Ideally, the credentials never appear on developer workstations and aren't checked into source control. Azure Key Vault provides a way to securely store credentials, secrets, and other keys, but your code has to authenticate to Key Vault to retrieve them.

The managed identities for Azure resources feature in Azure Active Directory (Azure AD) solves this problem. The feature provides Azure services with an automatically managed identity in Azure AD. You can use the identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without any credentials in your code. Your code that's running on a VM can request a token from two endpoints that are accessible only from within the VM. For more detailed information about this service, review the [managed identities for Azure resources](#) overview page.

Policies

[Azure policies](#) can be used to define the desired behavior for your organization's [Windows VMs](#) and [Linux VMs](#). By using policies, an organization can enforce various conventions and rules throughout the enterprise. Enforcement of the desired behavior can help mitigate risk while contributing to the success of the organization.

Role-based access control

Using [role-based access control \(RBAC\)](#), you can segregate duties within your team and grant only the amount of access to users on your VM that they need to perform their jobs. Instead of giving everybody unrestricted permissions on the VM, you can allow only certain actions. You can configure access control for the VM in the [Azure portal](#), using the [Azure CLI](#), or [Azure PowerShell](#).

Next steps

- Walk through the steps to monitor virtual machine security by using Azure Security Center for [Linux](#) or [Windows](#).

Azure Disk Encryption for Linux VMs

2/4/2020 • 7 minutes to read • [Edit Online](#)

Azure Disk Encryption helps protect and safeguard your data to meet your organizational security and compliance commitments. It uses the [DM-Crypt](#) feature of Linux to provide volume encryption for the OS and data disks of Azure virtual machines (VMs), and is integrated with [Azure Key Vault](#) to help you control and manage the disk encryption keys and secrets.

If you use [Azure Security Center](#), you're alerted if you have VMs that aren't encrypted. The alerts show as High Severity and the recommendation is to encrypt these VMs.

VIRTUAL MACHINES RECOMMENDATIONS		TOTAL				
Missing disk encryption		2 of 2 VMs				
Virtual machines						
NAME	ONBOARDING	SYSTEM UPDATES	ANTIMALWARE	BASELINE	DISK ENCRYPTION	
ASC-VM1	✓	✓	✓	✓	!	
ASC-VM2	✓	✓	✓	✓	!	

WARNING

- If you have previously used Azure Disk Encryption with Azure AD to encrypt a VM, you must continue to use this option to encrypt your VM. See [Azure Disk Encryption with Azure AD \(previous release\)](#) for details.
- Certain recommendations might increase data, network, or compute resource usage, resulting in additional license or subscription costs. You must have a valid active Azure subscription to create resources in Azure in the supported regions.
- Currently Generation 2 VMs do not support Azure Disk Encryption. See [Support for Generation 2 VMs on Azure](#) for details.

You can learn the fundamentals of Azure Disk Encryption for Linux in just a few minutes with the [Create and encrypt a Linux VM with Azure CLI quickstart](#) or the [Create and encrypt a Linux VM with Azure Powershell quickstart](#).

Supported VMs and operating systems

Supported VM sizes

Linux VMs are available in a [range of sizes](#). Azure Disk Encryption is not available on [Basic, A-series VMs](#), or on virtual machines that do not meet these minimum memory requirements:

VIRTUAL MACHINE	MINIMUM MEMORY REQUIREMENT
Linux VMs when only encrypting data volumes	2 GB

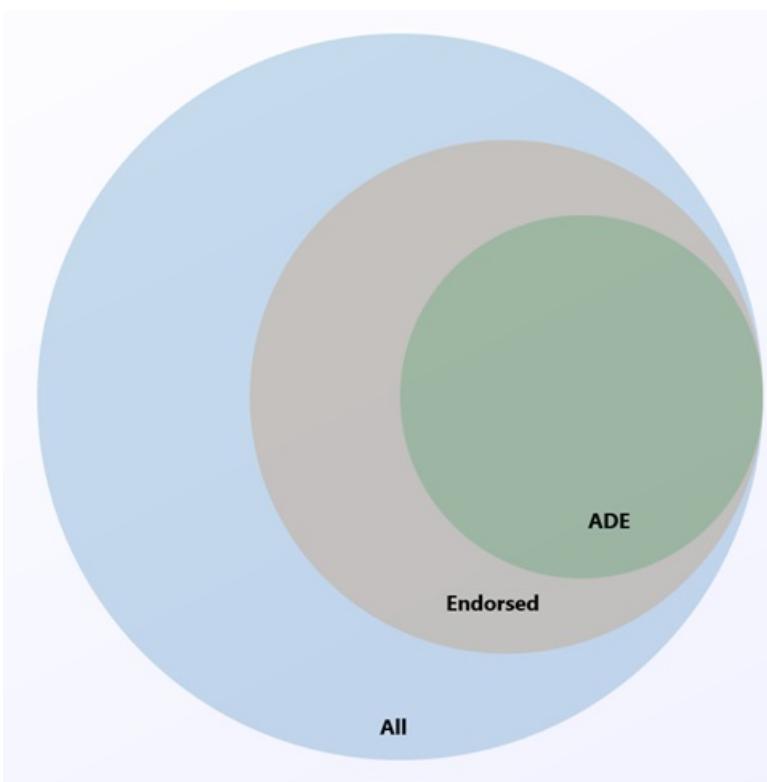
VIRTUAL MACHINE	MINIMUM MEMORY REQUIREMENT
Linux VMs when encrypting both data and OS volumes, and where the root (/) file system usage is 4GB or less	8 GB
Linux VMs when encrypting both data and OS volumes, and where the root (/) file system usage is greater than 4GB	The root file system usage * 2. For instance, a 16 GB of root file system usage requires at least 32GB of RAM

Once the OS disk encryption process is complete on Linux virtual machines, the VM can be configured to run with less memory.

Azure Disk Encryption is also available for VMs with premium storage.

Supported operating systems

Azure Disk Encryption is supported on a subset of the [Azure-endorsed Linux distributions](#), which is itself a subset of all Linux server possible distributions.



Linux server distributions that are not endorsed by Azure do not support Azure Disk Encryption; of those that are endorsed, only the following distributions and versions support Azure Disk Encryption:

LINUX DISTRIBUTION	VERSION	VOLUME TYPE SUPPORTED FOR ENCRYPTION
Ubuntu	18.04	OS and data disk
Ubuntu	16.04	OS and data disk
Ubuntu	14.04.5 with Azure tuned kernel updated to 4.15 or later	OS and data disk
RHEL	7.7	OS and data disk (see note below)
RHEL	7.6	OS and data disk (see note below)

LINUX DISTRIBUTION	VERSION	VOLUME TYPE SUPPORTED FOR ENCRYPTION
RHEL	7.5	OS and data disk (see note below)
RHEL	7.4	OS and data disk (see note below)
RHEL	7.3	OS and data disk (see note below)
RHEL	7.2	OS and data disk (see note below)
RHEL	6.8	Data disk (see note below)
RHEL	6.7	Data disk (see note below)
CentOS	7.7	OS and data disk
CentOS	7.6	OS and data disk
CentOS	7.5	OS and data disk
CentOS	7.4	OS and data disk
CentOS	7.3	OS and data disk
CentOS	7.2n	OS and data disk
CentOS	6.8	Data disk
openSUSE	42.3	Data disk
SLES	12-SP4	Data disk
SLES	12-SP3	Data disk

NOTE

The new Azure Disk Encryption implementation is supported for RHEL OS and data disk for RHEL7 Pay-As-You-Go images.

ADE is also supported for RHEL Bring-Your-Own-Subscription Gold Images, but only **after** the subscription has been registered . For more information, see [Red Hat Enterprise Linux Bring-Your-Own-Subscription Gold Images in Azure](#)

Additional VM requirements

Azure Disk Encryption requires the dm-crypt and vfat modules to be present on the system. Removing or disabling vfat from the default image will prevent the system from reading the key volume and obtaining the key needed to unlock the disks on subsequent reboots. System hardening steps that remove the vfat module from the system are not compatible with Azure Disk Encryption.

Before enabling encryption, the data disks to be encrypted must be properly listed in /etc/fstab. Use a persistent block device name for this entry, as device names in the "/dev/sdX" format can't be relied upon to be associated with the same disk across reboots, particularly after encryption is applied. For more detail on this behavior, see: [Troubleshoot Linux VM device name changes](#)

Make sure the /etc/fstab settings are configured properly for mounting. To configure these settings, run the mount -a command or reboot the VM and trigger the remount that way. Once that is complete, check the output of the lsblk command to verify that the drive is still mounted.

- If the /etc/fstab file doesn't mount the drive properly before enabling encryption, Azure Disk Encryption won't be able to mount it properly.
- The Azure Disk Encryption process will move the mount information out of /etc/fstab and into its own configuration file as part of the encryption process. Don't be alarmed to see the entry missing from /etc/fstab after data drive encryption completes.
- Before starting encryption, be sure to stop all services and processes that could be writing to mounted data disks and disable them, so that they do not restart automatically after a reboot. These could keep files open on these partitions, preventing the encryption procedure to remount them, causing failure of the encryption.
- After reboot, it will take time for the Azure Disk Encryption process to mount the newly encrypted disks. They won't be immediately available after a reboot. The process needs time to start, unlock, and then mount the encrypted drives before being available for other processes to access. This process may take more than a minute after reboot depending on the system characteristics.

An example of commands that can be used to mount the data disks and create the necessary /etc/fstab entries can be found in the [Azure Disk Encryption prerequisites CLI script](#) (lines 244-248) and the [Azure Disk Encryption prerequisites PowerShell script](#).

Networking requirements

To enable the Azure Disk Encryption feature, the Linux VMs must meet the following network endpoint configuration requirements:

- To get a token to connect to your key vault, the Linux VM must be able to connect to an Azure Active Directory endpoint, [login.microsoftonline.com].
- To write the encryption keys to your key vault, the Linux VM must be able to connect to the key vault endpoint.
- The Linux VM must be able to connect to an Azure storage endpoint that hosts the Azure extension repository and an Azure storage account that hosts the VHD files.
- If your security policy limits access from Azure VMs to the Internet, you can resolve the preceding URI and configure a specific rule to allow outbound connectivity to the IPs. For more information, see [Azure Key Vault behind a firewall](#).

Encryption key storage requirements

Azure Disk Encryption requires an Azure Key Vault to control and manage disk encryption keys and secrets. Your key vault and VMs must reside in the same Azure region and subscription.

For details, see [Creating and configuring a key vault for Azure Disk Encryption](#).

Terminology

The following table defines some of the common terms used in Azure disk encryption documentation:

TERMINOLOGY	DEFINITION
-------------	------------

TERMINOLOGY	DEFINITION
Azure Key Vault	Key Vault is a cryptographic, key management service that's based on Federal Information Processing Standards (FIPS) validated hardware security modules. These standards help to safeguard your cryptographic keys and sensitive secrets. For more information, see the Azure Key Vault documentation and Creating and configuring a key vault for Azure Disk Encryption .
Azure CLI	The Azure CLI is optimized for managing and administering Azure resources from the command line.
DM-Crypt	DM-Crypt is the Linux-based, transparent disk-encryption subsystem that's used to enable disk encryption on Linux VMs.
Key encryption key (KEK)	The asymmetric key (RSA 2048) that you can use to protect or wrap the secret. You can provide a hardware security module (HSM)-protected key or software-protected key. For more information, see the Azure Key Vault documentation and Creating and configuring a key vault for Azure Disk Encryption .
PowerShell cmdlets	For more information, see Azure PowerShell cmdlets .

Next steps

- [Quickstart - Create and encrypt a Linux VM with Azure CLI](#)
- [Quickstart - Create and encrypt a Linux VM with Azure Powershell](#)
- [Azure Disk Encryption scenarios on Linux VMs](#)
- [Azure Disk Encryption prerequisites CLI script](#)
- [Azure Disk Encryption prerequisites PowerShell script](#)
- [Creating and configuring a key vault for Azure Disk Encryption](#)

Security controls for Linux Virtual Machines

2/12/2020 • 2 minutes to read • [Edit Online](#)

This article documents the security controls built into Linux Virtual Machines.

A security control is a quality or feature of an Azure service that contributes to the service's ability to prevent, detect, and respond to security vulnerabilities.

For each control, we use "Yes" or "No" to indicate whether it is currently in place for the service, "N/A" for a control that is not applicable to the service. We might also provide a note or links to more information about an attribute.

Network

SECURITY CONTROL	YES/NO	NOTES
Service endpoint support	Yes	
VNet injection support	Yes	
Network Isolation and Firewalling support	Yes	
Forced tunneling support	Yes	See Configure forced tunneling using the Azure Resource Manager deployment model .

Monitoring & logging

SECURITY CONTROL	YES/NO	NOTES
Azure monitoring support (Log analytics, App insights, etc.)	Yes	See Monitor and update a Linux virtual machine in Azure .
Control and management plane logging and audit	Yes	
Data plane logging and audit	No	

Identity

SECURITY CONTROL	YES/NO	NOTES
Authentication	Yes	
Authorization	Yes	

Data protection

SECURITY CONTROL	YES/NO	NOTES
Server-side encryption at rest: Microsoft-managed keys	Yes	See Azure Disk Encryption for Linux VMs .
Encryption in transit (such as ExpressRoute encryption, in VNet encryption, and VNet-VNet encryption)	Yes	Azure Virtual Machines supports ExpressRoute and VNet encryption. See In-transit encryption in VMs .
Server-side encryption at rest: customer-managed keys (BYOK)	Yes	Customer-managed keys is a supported Azure encryption scenario; see Azure encryption overview .
Column level encryption (Azure Data Services)	N/A	
API calls encrypted	Yes	Via HTTPS and TLS.

Configuration management

SECURITY CONTROL	YES/NO	NOTES
Configuration management support (versioning of configuration, etc.)	Yes	

Next steps

- Learn more about the [built-in security controls across Azure services](#).

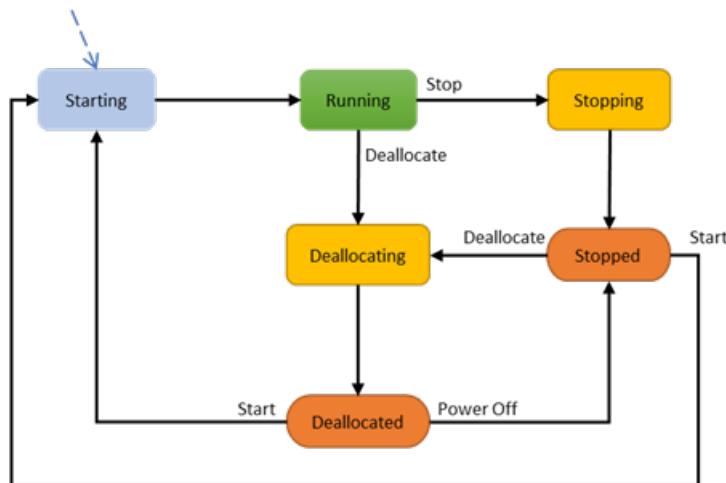
Virtual machines lifecycle and states

11/13/2019 • 3 minutes to read • [Edit Online](#)

Azure Virtual Machines (VMs) go through different states that can be categorized into *provisioning* and *power* states. The purpose of this article is to describe these states and specifically highlight when customers are billed for instance usage.

Power states

The power state represents the last known state of the VM.



The following table provides a description of each instance state and indicates whether it is billed for instance usage or not.

STATE	DESCRIPTION	INSTANCE USAGE BILLING
Starting	VM is starting up. <pre>"statuses": [{ "code": "PowerState/starting", "level": "Info", "displayStatus": "VM starting" }]</pre>	Not billed
Running	Normal working state for a VM <pre>"statuses": [{ "code": "PowerState/running", "level": "Info", "displayStatus": "VM running" }]</pre>	Billed

Stopping	This is a transitional state. When completed, it will show as **Stopped**. <pre>"statuses": [{ "code": "PowerState/stopping", "level": "Info", "displayStatus": "VM stopping" }]</pre>	Billed
Stopped	The VM has been shut down from within the guest OS or using the PowerOff APIs. Hardware is still allocated to the VM and it remains on the host. <pre>"statuses": [{ "code": "PowerState/stopped", "level": "Info", "displayStatus": "VM stopped" }]</pre>	Billed*
Deallocating	Transitional state. When completed, the VM will show as **Deallocated**. <pre>"statuses": [{ "code": "PowerState/deallocating", "level": "Info", "displayStatus": "VM deallocating" }]</pre>	Not billed*
Deallocated	The VM has been stopped successfully and removed from the host. <pre>"statuses": [{ "code": "PowerState/deallocated", "level": "Info", "displayStatus": "VM deallocated" }]</pre>	Not billed

*Some Azure resources, such as Disks and Networking, incur charges. Software licenses on the instance do not incur charges.

Provisioning states

A provisioning state is the status of a user-initiated, control-plane operation on the VM. These states are separate from the power state of a VM.

- **Create** – VM creation.
- **Update** – updates the model for an existing VM. Some non-model changes to VM such as Start/Restart also fall under update.
- **Delete** – VM deletion.

- **Deallocate** – is where a VM is stopped and removed from the host. Deallocating a VM is considered an update, so it will display provisioning states related to updating.

Here are the transitional operation states after the platform has accepted a user-initiated action:

States	Description
Creating	<pre>"statuses": [{ "code": "ProvisioningState/creating", "level": "Info", "displayStatus": "Creating" }]</pre>
Updating	<pre>"statuses": [{ "code": "ProvisioningState/updating", "level": "Info", "displayStatus": "Updating" }]</pre>
Deleting	<pre>"statuses": [{ "code": "ProvisioningState/deleting", "level": "Info", "displayStatus": "Deleting" }]</pre>
OS provisioning states	<p>If a VM is created with an OS image and not with a specialized image, then following substates can be observed:</p> <ol style="list-style-type: none"> 1. OSProvisioningInProgress – The VM is running, and installation of guest OS is in progress. <pre>"statuses": [{ "code": "ProvisioningState/creating/OSProvisioningInProgress", "level": "Info", "displayStatus": "OS Provisioning In progress" }]</pre> <ol style="list-style-type: none"> 2. OSProvisioningComplete – Short-lived state. The VM quickly transitions to **Success** unless any extensions need to be installed. Installing extensions can take time. <pre>"statuses": [{ "code": "ProvisioningState/creating/OSProvisioningComplete", "level": "Info", "displayStatus": "OS Provisioning Complete" }]</pre> <p>Note: OS Provisioning can transition to **Failed** if there is an OS failure or the OS doesn't install in time. Customers will be billed for the deployed VM on the infrastructure.</p>

Once the operation is complete, the VM will transition into one of the following states:

- **Succeeded** – the user-initiated actions have completed.

```
"statuses": [
{
  "code": "ProvisioningState/succeeded",
  "level": "Info",
  "displayStatus": "Provisioning succeeded",
  "time": "time"
}
]
```

- **Failed** – represents a failed operation. Refer to the error codes to get more information and possible solutions.

```
"statuses": [
{
  "code": "ProvisioningState/failed/InternalOperationError",
  "level": "Error",
  "displayStatus": "Provisioning failed",
  "message": "Operation abandoned due to internal error. Please try again later.",
  "time": "time"
}
]
```

VM instance view

The instance view API provides VM running-state information. For more information, see the [Virtual Machines - Instance View](#) API documentation.

Azure Resources explorer provides a simple UI for viewing the VM running state: [Resource Explorer](#).

Provisioning states are visible on VM properties and instance view. Power states are available in instance view of VM.

Next steps

To learn more about monitoring your VM, see [How to monitor virtual machines in Azure](#).

How to monitor virtual machines in Azure

11/13/2019 • 5 minutes to read • [Edit Online](#)

With the significant growth of VMs hosted in Azure, it's important to identify performance and health issues that impact applications and infrastructure services they support. Basic monitoring is delivered by default with Azure by the metric types CPU usage, disk utilization, memory utilization, and network traffic collected by the host hypervisor. Additional metric and log data can be collected using [extensions](#) to configure diagnostics on your VMs from the guest operating system.

To detect and help diagnose performance and health issues with the guest operating system, .NET based or Java web application components running inside the VM, Azure Monitor delivers centralized monitoring with comprehensive features such as Azure Monitor for VMs and Application Insights.

Diagnostics and metrics

You can set up and monitor the collection of [diagnostics data](#) using [metrics](#) in the Azure portal, the Azure CLI, Azure PowerShell, and programming Applications Programming Interfaces (APIs). For example, you can:

- **Observe basic metrics for the VM.** On the Overview screen of the Azure portal, the basic metrics shown include CPU usage, network usage, total of disk bytes, and disk operations per second.
- **Enable the collection of boot diagnostics and view it using the Azure portal.** When bringing your own image to Azure or even booting one of the platform images, there can be many reasons why a VM gets into a non-bootable state. You can easily enable boot diagnostics when you create a VM by clicking **Enabled** for Boot Diagnostics under the Monitoring section of the Settings screen.

As VMs boot, the boot diagnostic agent captures boot output and stores it in Azure storage. This data can be used to troubleshoot VM boot issues. Boot diagnostics are not automatically enabled when you create a VM from command-line tools. Before enabling boot diagnostics, a storage account needs to be created for storing boot logs. If you enable boot diagnostics in the Azure portal, a storage account is automatically created for you.

If you didn't enable boot diagnostics when the VM was created, you can always enable it later by using [Azure CLI](#), [Azure PowerShell](#), or an [Azure Resource Manager template](#).

- **Enable the collection of guest OS diagnostics data.** When you create a VM, you have the opportunity on the settings screen to enable guest OS diagnostics. When you do enable the collection of diagnostics data, the [IaaS Diagnostics extension for Linux](#) or the [IaaS Diagnostics extension for Windows](#) is added to the VM, which enables you to collect additional disk, CPU, and memory data.

Using the collected diagnostics data, you can configure autoscaling for your VMs. You can also configure [Azure Monitor Logs](#) to store the data and set up alerts to let you know when performance isn't right.

Alerts

You can create [alerts](#) based on specific performance metrics. Examples of the issues you can be alerted about include when average CPU usage exceeds a certain threshold, or available free disk space drops below a certain amount. Alerts can be configured in the [Azure portal](#), using [Azure Resource Manager templates](#), or [Azure CLI](#).

Azure Service Health

[Azure Service Health](#) provides personalized guidance and support when issues in Azure services affect you, and

helps you prepare for upcoming planned maintenance. Azure Service Health alerts you and your teams using targeted and flexible notifications.

Azure Resource Health

[Azure Resource health](#) helps you diagnose and get support when an Azure issue impacts your resources. It informs you about the current and past health of your resources and helps you mitigate issues. Resource health provides technical support when you need help with Azure service issues.

Azure Activity Log

The [Azure Activity Log](#) is a subscription log that provides insight into subscription-level events that have occurred in Azure. The log includes a range of data, from Azure Resource Manager operational data to updates on Service Health events. You can click Activity Log in the Azure portal to view the log for your VM.

Some of the things you can do with the activity log include:

- Create an [alert on an Activity Log event](#).
- [Stream it to an Event Hub](#) for ingestion by a third-party service or custom analytics solution such as Power BI.
- Analyze it in Power BI using the [Power BI content pack](#).
- [Save it to a storage account](#) for archival or manual inspection. You can specify the retention time (in days) using the Log Profile.

You can also access activity log data by using [Azure PowerShell](#), the [Azure CLI](#), or [Monitor REST APIs](#).

[Azure Resource Logs](#) are logs emitted by your VM that provide rich, frequent data about its operation. Resource logs differ from the activity log by providing insight about operations that were performed within the VM.

Some of the things you can do with diagnostics logs include:

- [Save them to a storage account](#) for auditing or manual inspection. You can specify the retention time (in days) using Resource Diagnostic Settings.
- [Stream them to Event Hubs](#) for ingestion by a third-party service or custom analytics solution such as Power BI.
- Analyze them with [Log Analytics](#).

Advanced monitoring

For visibility of the application or service supported by the Azure VM and virtual machine scale sets, identification of issues with the guest OS or workload running in the VM to understand if it is impacting availability or performance of the application, or is an issue with the application, enable both [Azure Monitor for VMs](#) and [Application Insights](#).

Azure Monitor for VMs monitors your Azure virtual machines (VM) at scale by analyzing the performance and health of your Windows and Linux VMs, including the different processes and interconnected dependencies on other resources and external processes it discovers. It includes several trend performance charts to help during investigation of problems and assess capacity of your VMs. The dependency map shows monitored and unmonitored machines, failed and active network connections between processes and these machines, and shows trend charts with standard network connection metrics. Combined with Application Insights, you monitor your application and capture telemetry such as HTTP requests, exceptions, etc. so you can correlate issues between the VMs and your application. Configure [Azure Monitor alerts](#) to alert you on important conditions detected from monitoring data collected by Azure Monitor for VMs.

Next steps

- Walk through the steps in [Monitor a Windows Virtual Machine with Azure PowerShell](#) or [Monitor a Linux](#)

[Virtual Machine with the Azure CLI.](#)

- Learn more about the best practices around [Monitoring and diagnostics](#).

Backup and restore options for Linux virtual machines in Azure

11/13/2019 • 2 minutes to read • [Edit Online](#)

You can protect your data by taking backups at regular intervals. There are several backup options available for VMs, depending on your use-case.

Azure Backup

For backing up Azure VMs running production workloads, use Azure Backup. 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 whole VM or just specific files.

For a simple, hands-on introduction to Azure Backup for Azure VMs, see the "Back up Azure virtual machines" tutorial for [Linux](#) or [Windows](#).

For more information on how Azure Backup works, see [Plan your VM backup infrastructure in Azure](#)

Azure Site Recovery

Azure Site Recovery protects your VMs from a major disaster scenario, when a whole region experiences an outage due to major natural disaster or widespread service interruption. You can configure Azure Site Recovery for your VMs so that you can recover your application with a single click in matter of minutes. You can replicate to an Azure region of your choice, it is not restricted to paired regions.

You can run disaster-recovery drills with on-demand test failovers, without affecting your production workloads or ongoing replication. Create recovery plans to orchestrate failover and failback of the entire application running on multiple VMs. The recovery plan feature is integrated with Azure automation runbooks.

You can get started by [replicating your virtual machines](#).

Managed snapshots

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 read-only full copy of a managed disk. Snapshots exist independent of the source disk and can be used to create new managed disks for rebuilding a VM. They are billed based on the used portion of the disk. For example, if you create a snapshot of a managed disk with provisioned capacity of 64 GB and actual used data size of 10 GB, snapshot will be billed only for the used data size of 10 GB.

For more information on creating snapshots, see:

- [Create copy of VHD stored as a Managed Disk using Snapshots in Windows](#)
- [Create copy of VHD stored as a Managed Disk using Snapshots in Linux](#)

Next steps

You can try out Azure Backup by following the "Back up Windows virtual machines tutorial" for [Linux](#) or [Windows](#).

Example Azure infrastructure walkthrough for Linux VMs

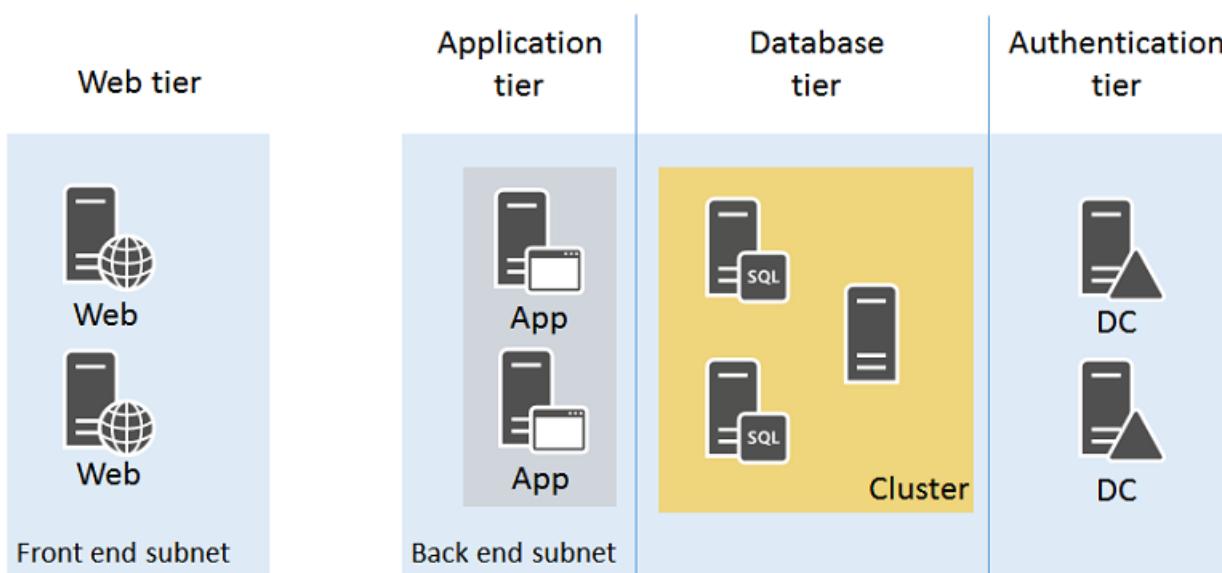
11/13/2019 • 3 minutes to read • [Edit Online](#)

This article walks through building out an example application infrastructure. We detail designing an infrastructure for a simple on-line store that brings together all the guidelines and decisions around naming conventions, availability sets, virtual networks and load balancers, and actually deploying your virtual machines (VMs).

Example workload

Adventure Works Cycles wants to build an on-line store application in Azure that consists of:

- Two nginx servers running the client front-end in a web tier
- Two nginx servers processing data and orders in an application tier
- Two MongoDB servers part of a sharded cluster for storing product data and orders in a database tier
- Two Active Directory domain controllers for customer accounts and suppliers in an authentication tier
- All the servers are located in two subnets:
 - a front-end subnet for the web servers
 - a back-end subnet for the application servers, MongoDB cluster, and domain controllers



Incoming secure web traffic must be load-balanced among the web servers as customers browse the on-line store. Order processing traffic in the form of HTTP requests from the web servers must be load-balanced among the application servers. Additionally, the infrastructure must be designed for high availability.

The resulting design must incorporate:

- An Azure subscription and account
- A single resource group
- Azure Managed Disks
- A virtual network with two subnets
- Availability sets for the VMs with a similar role
- Virtual machines

All the above follow these naming conventions:

- Adventure Works Cycles uses **[IT workload]-[location]-[Azure resource]** as a prefix
 - For this example, "azos" (Azure On-line Store) is the IT workload name and "use" (East US 2) is the location
- Virtual networks use AZOS-USE-VN**[number]**
- Availability sets use azos-use-as-**[role]**
- Virtual machine names use azos-use-vm-**[vmname]**

Azure subscriptions and accounts

Adventure Works Cycles is using their Enterprise subscription, named Adventure Works Enterprise Subscription, to provide billing for this IT workload.

Storage

Adventure Works Cycles determined that they should use Azure Managed Disks. When creating VMs, both storage available storage tiers are used:

- **Standard storage** for the web servers, application servers, and domain controllers and their data disks.
- **Premium storage** for the MongoDB sharded cluster servers and their data disks.

Virtual network and subnets

Because the virtual network does not need ongoing connectivity to the Adventure Work Cycles on-premises network, they decided on a cloud-only virtual network.

They created a cloud-only virtual network with the following settings using the Azure portal:

- Name: AZOS-USE-VN01
- Location: East US 2
- Virtual network address space: 10.0.0.0/8
- First subnet:
 - Name: FrontEnd
 - Address space: 10.0.1.0/24
- Second subnet:
 - Name: BackEnd
 - Address space: 10.0.2.0/24

Availability sets

To maintain high availability of all four tiers of their on-line store, Adventure Works Cycles decided on four availability sets:

- **azos-use-as-web** for the web servers
- **azos-use-as-app** for the application servers
- **azos-use-as-db** for the servers in the MongoDB sharded cluster
- **azos-use-as-dc** for the domain controllers

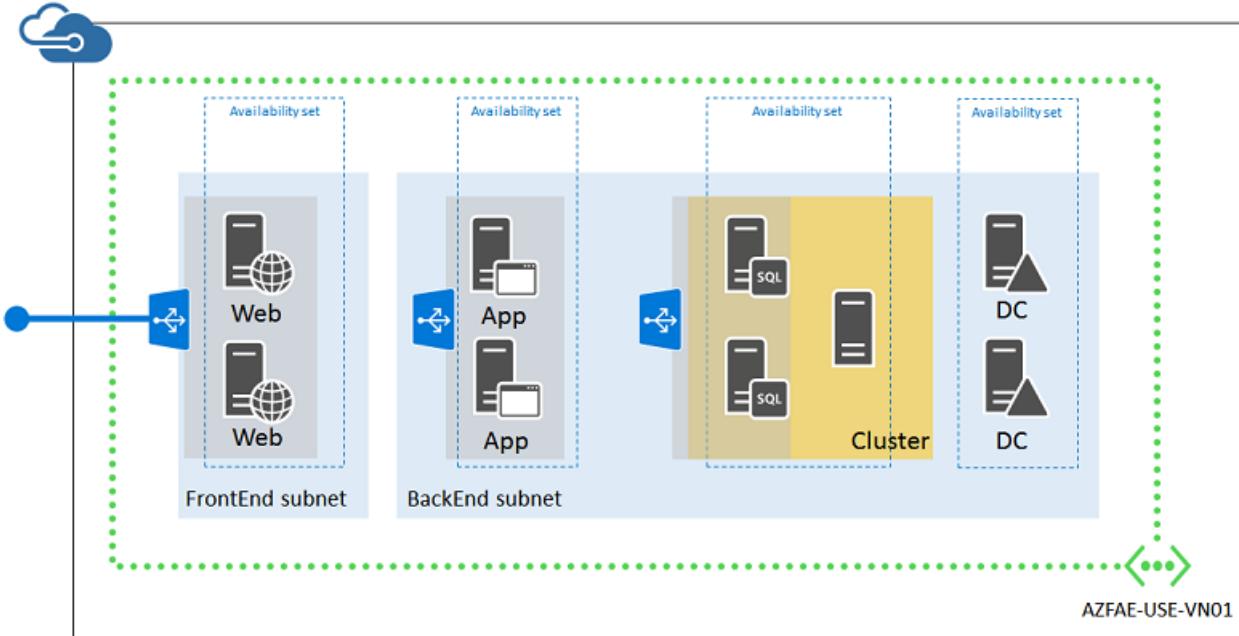
Virtual machines

Adventure Works Cycles decided on the following names for their Azure VMs:

- **azos-use-vm-web01** for the first web server

- **azos-use-vm-web02** for the second web server
- **azos-use-vm-app01** for the first application server
- **azos-use-vm-app02** for the second application server
- **azos-use-vm-db01** for the first MongoDB server in the cluster
- **azos-use-vm-db02** for the second MongoDB server in the cluster
- **azos-use-vm-dc01** for the first domain controller
- **azos-use-vm-dc02** for the second domain controller

Here is the resulting configuration.



This configuration incorporates:

- A cloud-only virtual network with two subnets (FrontEnd and BackEnd)
- Azure Managed Disks using both Standard and Premium disks
- Four availability sets, one for each tier of the on-line store
- The virtual machines for the four tiers
- An external load balanced set for HTTPS-based web traffic from the Internet to the web servers
- An internal load balanced set for unencrypted web traffic from the web servers to the application servers
- A single resource group

Create a complete Linux virtual machine with the Azure CLI

11/13/2019 • 10 minutes to read • [Edit Online](#)

To quickly create a virtual machine (VM) in Azure, you can use a single Azure CLI command that uses default values to create any required supporting resources. Resources such as a virtual network, public IP address, and network security group rules are automatically created. For more control of your environment in production use, you may create these resources ahead of time and then add your VMs to them. This article guides you through how to create a VM and each of the supporting resources one by one.

Make sure that you have installed the latest [Azure CLI](#) and logged to an Azure account in with `az login`.

In the following examples, replace example parameter names with your own values. Example parameter names include `myResourceGroup`, `myVnet`, and `myVM`.

Create resource group

An Azure resource group is a logical container into which Azure resources are deployed and managed. A resource group must be created before a virtual machine and supporting virtual network resources. Create the resource group with [az group create](#). The following example creates a resource group named `myResourceGroup` in the `eastus` location:

```
az group create --name myResourceGroup --location eastus
```

By default, the output of Azure CLI commands is in JSON (JavaScript Object Notation). To change the default output to a list or table, for example, use [az configure --output](#). You can also add `--output` to any command for a one time change in output format. The following example shows the JSON output from the `az group create` command:

```
{
  "id": "/subscriptions/guid/resourceGroups/myResourceGroup",
  "location": "eastus",
  "name": "myResourceGroup",
  "properties": {
    "provisioningState": "Succeeded"
  },
  "tags": null
}
```

Create a virtual network and subnet

Next you create a virtual network in Azure and a subnet in to which you can create your VMs. Use [az network vnet create](#) to create a virtual network named `myVnet` with the `192.168.0.0/16` address prefix. You also add a subnet named `mySubnet` with the address prefix of `192.168.1.0/24`:

```
az network vnet create \
    --resource-group myResourceGroup \
    --name myVnet \
    --address-prefix 192.168.0.0/16 \
    --subnet-name mySubnet \
    --subnet-prefix 192.168.1.0/24
```

The output shows the subnet is logically created inside the virtual network:

```
{
  "addressSpace": {
    "addressPrefixes": [
      "192.168.0.0/16"
    ]
  },
  "dhcpOptions": {
    "dnsServers": []
  },
  "etag": "W/\"e95496fc-f417-426e-a4d8-c9e4d27fc2ee\"",
  "id": "/subscriptions/guid/resourceGroups/myResourceGroup/providers/Microsoft.Network/virtualNetworks/myVnet",
  "location": "eastus",
  "name": "myVnet",
  "provisioningState": "Succeeded",
  "resourceGroup": "myResourceGroup",
  "resourceGuid": "ed62fd03-e9de-430b-84df-8a3b87cacdbb",
  "subnets": [
    {
      "addressPrefix": "192.168.1.0/24",
      "etag": "W/\"e95496fc-f417-426e-a4d8-c9e4d27fc2ee\"",
      "id": "/subscriptions/guid/resourceGroups/myResourceGroup/providers/Microsoft.Network/virtualNetworks/myVnet/subnets/mySubnet",
      "ipConfigurations": null,
      "name": "mySubnet",
      "networkSecurityGroup": null,
      "provisioningState": "Succeeded",
      "resourceGroup": "myResourceGroup",
      "resourceNavigationLinks": null,
      "routeTable": null
    }
  ],
  "tags": {},
  "type": "Microsoft.Network/virtualNetworks",
  "virtualNetworkPeerings": null
}
```

Create a public IP address

Now let's create a public IP address with [az network public-ip create](#). This public IP address enables you to connect to your VMs from the Internet. Because the default address is dynamic, create a named DNS entry with the `--domain-name-label` parameter. The following example creates a public IP named *myPublicIP* with the DNS name of *mypublicdns*. Because the DNS name must be unique, provide your own unique DNS name:

```
az network public-ip create \
    --resource-group myResourceGroup \
    --name myPublicIP \
    --dns-name mypublicdns
```

Output:

```
{  
  "publicIp": {  
    "dnsSettings": {  
      "domainNameLabel": "mypublicdns",  
      "fqdn": "mypublicdns.eastus.cloudapp.azure.com",  
      "reverseFqdn": null  
    },  
    "etag": "W/\"2632aa72-3d2d-4529-b38e-b622b4202925\"",  
    "id":  
      "/subscriptions/guid/resourceGroups/myResourceGroup/providers/Microsoft.Network/publicIPAddresses/myPublicIP",  
      "idleTimeoutInMinutes": 4,  
      "ipAddress": null,  
      "ipConfiguration": null,  
      "location": "eastus",  
      "name": "myPublicIP",  
      "provisioningState": "Succeeded",  
      "publicIpAddressVersion": "IPv4",  
      "publicIpAllocationMethod": "Dynamic",  
      "resourceGroup": "myResourceGroup",  
      "resourceGuid": "4c65de38-71f5-4684-be10-75e605b3e41f",  
      "tags": null,  
      "type": "Microsoft.Network/publicIPAddresses"  
    },  
  },  
}
```

Create a network security group

To control the flow of traffic in and out of your VMs, you apply a network security group to a virtual NIC or subnet.

The following example uses [az network nsg create](#) to create a network security group named *myNetworkSecurityGroup*:

```
az network nsg create \  
  --resource-group myResourceGroup \  
  --name myNetworkSecurityGroup
```

You define rules that allow or deny specific traffic. To allow inbound connections on port 22 (to enable SSH access), create an inbound rule with [az network nsg rule create](#). The following example creates a rule named *myNetworkSecurityGroupRuleSSH*:

```
az network nsg rule create \  
  --resource-group myResourceGroup \  
  --nsg-name myNetworkSecurityGroup \  
  --name myNetworkSecurityGroupRuleSSH \  
  --protocol tcp \  
  --priority 1000 \  
  --destination-port-range 22 \  
  --access allow
```

To allow inbound connections on port 80 (for web traffic), add another network security group rule. The following example creates a rule named *myNetworkSecurityGroupRuleHTTP*:

```
az network nsg rule create \
--resource-group myResourceGroup \
--nsg-name myNetworkSecurityGroup \
--name myNetworkSecurityGroupRuleWeb \
--protocol tcp \
--priority 1001 \
--destination-port-range 80 \
--access allow
```

Examine the network security group and rules with [az network nsg show](#):

```
az network nsg show --resource-group myResourceGroup --name myNetworkSecurityGroup
```

Output:

```
{
  "defaultSecurityRules": [
    {
      "access": "Allow",
      "description": "Allow inbound traffic from all VMs in VNET",
      "destinationAddressPrefix": "VirtualNetwork",
      "destinationPortRange": "*",
      "direction": "Inbound",
      "etag": "W/\"3371b313-ea9f-4687-a336-a8ebdfd80523\"",
      "id": "/subscriptions/guid/resourceGroups/myResourceGroup/providers/Microsoft.Network/networkSecurityGroups/myNetworkSecurityGroup/defaultSecurityRules/AllowVnetInBound",
      "name": "AllowVnetInBound",
      "priority": 65000,
      "protocol": "*",
      "provisioningState": "Succeeded",
      "resourceGroup": "myResourceGroup",
      "sourceAddressPrefix": "VirtualNetwork",
      "sourcePortRange": "*"
    },
    {
      "access": "Allow",
      "description": "Allow inbound traffic from azure load balancer",
      "destinationAddressPrefix": "*",
      "destinationPortRange": "*",
      "direction": "Inbound",
      "etag": "W/\"3371b313-ea9f-4687-a336-a8ebdfd80523\"",
      "id": "/subscriptions/guid/resourceGroups/myResourceGroup/providers/Microsoft.Network/networkSecurityGroups/myNetworkSecurityGroup/defaultSecurityRules/AllowAzureLoadBalancerInBou",
      "name": "AllowAzureLoadBalancerInBound",
      "priority": 65001,
      "protocol": "*",
      "provisioningState": "Succeeded",
      "resourceGroup": "myResourceGroup",
      "sourceAddressPrefix": "AzureLoadBalancer",
      "sourcePortRange": "*"
    },
    {
      "access": "Deny",
      "description": "Deny all inbound traffic",
      "destinationAddressPrefix": "*",
      "destinationPortRange": "*",
      "direction": "Inbound",
      "etag": "W/\"3371b313-ea9f-4687-a336-a8ebdfd80523\"",
      "id": "/subscriptions/guid/resourceGroups/myResourceGroup/providers/Microsoft.Network/networkSecurityGroups/myNetworkSecurityGroup/defaultSecurityRules/DenyAllInBound",
      "name": "DenyAllInBound",
```

```
"priority": 65500,
"protocol": "*",
"provisioningState": "Succeeded",
"resourceGroup": "myResourceGroup",
"sourceAddressPrefix": "*",
"sourcePortRange": "*"
},
{
"access": "Allow",
"description": "Allow outbound traffic from all VMs to all VMs in VNET",
"destinationAddressPrefix": "VirtualNetwork",
"destinationPortRange": "*",
"direction": "Outbound",
"etag": "W/\"3371b313-ea9f-4687-a336-a8ebdfd80523\",
"id":
"/subscriptions/guid/resourceGroups/myResourceGroup/providers/Microsoft.Network/networkSecurityGroups/myNetwor
kSecurityGroup/defaultSecurityRules/AllowVnetOutBound",
"name": "AllowVnetOutBound",
"priority": 65000,
"protocol": "*",
"provisioningState": "Succeeded",
"resourceGroup": "myResourceGroup",
"sourceAddressPrefix": "VirtualNetwork",
"sourcePortRange": "*"
},
{
"access": "Allow",
"description": "Allow outbound traffic from all VMs to Internet",
"destinationAddressPrefix": "Internet",
"destinationPortRange": "*",
"direction": "Outbound",
"etag": "W/\"3371b313-ea9f-4687-a336-a8ebdfd80523\",
"id":
"/subscriptions/guid/resourceGroups/myResourceGroup/providers/Microsoft.Network/networkSecurityGroups/myNetwor
kSecurityGroup/defaultSecurityRules/AllowInternetOutBound",
"name": "AllowInternetOutBound",
"priority": 65001,
"protocol": "*",
"provisioningState": "Succeeded",
"resourceGroup": "myResourceGroup",
"sourceAddressPrefix": "*",
"sourcePortRange": "*"
},
{
"access": "Deny",
"description": "Deny all outbound traffic",
"destinationAddressPrefix": "*",
"destinationPortRange": "*",
"direction": "Outbound",
"etag": "W/\"3371b313-ea9f-4687-a336-a8ebdfd80523\",
"id":
"/subscriptions/guid/resourceGroups/myResourceGroup/providers/Microsoft.Network/networkSecurityGroups/myNetwor
kSecurityGroup/defaultSecurityRules/DenyAllOutBound",
"name": "DenyAllOutBound",
"priority": 65500,
"protocol": "*",
"provisioningState": "Succeeded",
"resourceGroup": "myResourceGroup",
"sourceAddressPrefix": "*",
"sourcePortRange": "*"
}
],
"etag": "W/\"3371b313-ea9f-4687-a336-a8ebdfd80523\",
"id":
"/subscriptions/guid/resourceGroups/myResourceGroup/providers/Microsoft.Network/networkSecurityGroups/myNetwor
kSecurityGroup",
"location": "eastus",
"name": "myNetworkSecurityGroup",
"networkInterfaces": null,
```

```

"provisioningState": "Succeeded",
"resourceGroup": "myResourceGroup",
"resourceGuid": "47a9964e-23a3-438a-a726-8d60ebbb1c3c",
"securityRules": [
  {
    "access": "Allow",
    "description": null,
    "destinationAddressPrefix": "*",
    "destinationPortRange": "22",
    "direction": "Inbound",
    "etag": "W/\"9e344b60-0daa-40a6-84f9-0ebbe4a4b640\"",
    "id": "/subscriptions/guid/resourceGroups/myResourceGroup/providers/Microsoft.Network/networkSecurityGroups/myNetworkSecurityGroup/securityRules/myNetworkSecurityGroupRuleSSH",
    "name": "myNetworkSecurityGroupRuleSSH",
    "priority": 1000,
    "protocol": "Tcp",
    "provisioningState": "Succeeded",
    "resourceGroup": "myResourceGroup",
    "sourceAddressPrefix": "*",
    "sourcePortRange": "*"
  },
  {
    "access": "Allow",
    "description": null,
    "destinationAddressPrefix": "*",
    "destinationPortRange": "80",
    "direction": "Inbound",
    "etag": "W/\"9e344b60-0daa-40a6-84f9-0ebbe4a4b640\"",
    "id": "/subscriptions/guid/resourceGroups/myResourceGroup/providers/Microsoft.Network/networkSecurityGroups/myNetworkSecurityGroup/securityRules/myNetworkSecurityGroupRuleWeb",
    "name": "myNetworkSecurityGroupRuleWeb",
    "priority": 1001,
    "protocol": "Tcp",
    "provisioningState": "Succeeded",
    "resourceGroup": "myResourceGroup",
    "sourceAddressPrefix": "*",
    "sourcePortRange": "*"
  }
],
"subnets": null,
"tags": null,
"type": "Microsoft.Network/networkSecurityGroups"
}

```

Create a virtual NIC

Virtual network interface cards (NICs) are programmatically available because you can apply rules to their use. Depending on the [VM size](#), you can attach multiple virtual NICs to a VM. In the following [az network nic create](#) command, you create a NIC named *myNic* and associate it with your network security group. The public IP address *myPublicIP* is also associated with the virtual NIC.

```

az network nic create \
  --resource-group myResourceGroup \
  --name myNic \
  --vnet-name myVnet \
  --subnet mySubnet \
  --public-ip-address myPublicIP \
  --network-security-group myNetworkSecurityGroup

```

Output:

```
{
  "NewNIC": {
    "dnsSettings": {
      "appliedDnsServers": [],
      "dnsServers": [],
      "internalDnsNameLabel": null,
      "internalDomainNameSuffix": "brqlt10lvoedgkeuomc4pm5tb.bx.internal.cloudapp.net",
      "internalFqdn": null
    },
    "enableAcceleratedNetworking": false,
    "enableIpForwarding": false,
    "etag": "W/\"04b5ab44-d8f4-422a-9541-e5ae7de8466d\"",
    "id": "/subscriptions/guid/resourceGroups/myResourceGroup/providers/Microsoft.Network/networkInterfaces/myNic",
    "ipConfigurations": [
      {
        "applicationGatewayBackendAddressPools": null,
        "etag": "W/\"04b5ab44-d8f4-422a-9541-e5ae7de8466d\"",
        "id": "/subscriptions/guid/resourceGroups/myResourceGroup/providers/Microsoft.Network/networkInterfaces/myNic/ipConfigurations/ipconfig1",
        "loadBalancerBackendAddressPools": null,
        "loadBalancerInboundNatRules": null,
        "name": "ipconfig1",
        "primary": true,
        "privateIpAddress": "192.168.1.4",
        "privateIpAddressVersion": "IPv4",
        "privateIpAllocationMethod": "Dynamic",
        "provisioningState": "Succeeded",
        "publicIpAddress": {
          "dnsSettings": null,
          "etag": null,
          "id": "/subscriptions/guid/resourceGroups/myResourceGroup/providers/Microsoft.Network/publicIPAddresses/myPublicIP",
          "idleTimeoutInMinutes": null,
          "ipAddress": null,
          "ipConfiguration": null,
          "location": null,
          "name": null,
          "provisioningState": null,
          "publicIpAddressVersion": null,
          "publicIpAllocationMethod": null,
          "resourceGroup": "myResourceGroup",
          "resourceGuid": null,
          "tags": null,
          "type": null
        },
        "resourceGroup": "myResourceGroup",
        "subnet": {
          "addressPrefix": null,
          "etag": null,
          "id": "/subscriptions/guid/resourceGroups/myResourceGroup/providers/Microsoft.Network/virtualNetworks/myVnet/subnets/mySubnet",
          "ipConfigurations": null,
          "name": null,
          "networkSecurityGroup": null,
          "provisioningState": null,
          "resourceGroup": "myResourceGroup",
          "resourceNavigationLinks": null,
          "routeTable": null
        }
      }
    ],
    "location": "eastus",
    "macAddress": null,
    "name": "myNic",
    "networkSecurityGroup": {
      "defaultSecurityRules": null,
      "id": "/subscriptions/guid/resourceGroups/myResourceGroup/providers/Microsoft.Network/networkSecurityGroups/myNSG"
    }
  }
}
```

```
        "etag": null,
        "id": "/subscriptions/guid/resourceGroups/myResourceGroup/providers/Microsoft.Network/networkSecurityGroups/myNetworkSecurityGroup",
        "location": null,
        "name": null,
        "networkInterfaces": null,
        "provisioningState": null,
        "resourceGroup": "myResourceGroup",
        "resourceGuid": null,
        "securityRules": null,
        "subnets": null,
        "tags": null,
        "type": null
    },
    "primary": null,
    "provisioningState": "Succeeded",
    "resourceGroup": "myResourceGroup",
    "resourceGuid": "b3dbaa0e-2cf2-43be-a814-5cc49fea3304",
    "tags": null,
    "type": "Microsoft.Network/networkInterfaces",
    "virtualMachine": null
}
}
```

Create an availability set

Availability sets help spread your VMs across fault domains and update domains. Even though you only create one VM right now, it's best practice to use availability sets to make it easier to expand in the future.

Fault domains define a grouping of virtual machines that share a common power source and network switch. By default, the virtual machines that are configured within your availability set are separated across up to three fault domains. A hardware issue in one of these fault domains does not affect every VM that is running your app.

Update domains indicate groups of virtual machines and underlying physical hardware that can be rebooted at the same time. During planned maintenance, the order in which update domains are rebooted might not be sequential, but only one update domain is rebooted at a time.

Azure automatically distributes VMs across the fault and update domains when placing them in an availability set. For more information, see [managing the availability of VMs](#).

Create an availability set for your VM with [az vm availability-set create](#). The following example creates an availability set named *myAvailabilitySet*:

```
az vm availability-set create \
--resource-group myResourceGroup \
--name myAvailabilitySet
```

The output notes fault domains and update domains:

```
{  
  "id":  
    "/subscriptions/guid/resourceGroups/myResourceGroup/providers/Microsoft.Compute/availabilitySets/myAvailabilitySet",  
  "location": "eastus",  
  "managed": null,  
  "name": "myAvailabilitySet",  
  "platformFaultDomainCount": 2,  
  "platformUpdateDomainCount": 5,  
  "resourceGroup": "myResourceGroup",  
  "sku": {  
    "capacity": null,  
    "managed": true,  
    "tier": null  
  },  
  "statuses": null,  
  "tags": {},  
  "type": "Microsoft.Compute/availabilitySets",  
  "virtualMachines": []  
}
```

Create a VM

You've created the network resources to support Internet-accessible VMs. Now create a VM and secure it with an SSH key. In this example, let's create an Ubuntu VM based on the most recent LTS. You can find additional images with [az vm image list](#), as described in [finding Azure VM images](#).

Specify an SSH key to use for authentication. If you do not have an SSH public key pair, you can [create them](#) or use the `--generate-ssh-keys` parameter to create them for you. If you already have a key pair, this parameter uses existing keys in `~/.ssh`.

Create the VM by bringing all the resources and information together with the [az vm create](#) command. The following example creates a VM named *myVM*:

```
az vm create \  
  --resource-group myResourceGroup \  
  --name myVM \  
  --location eastus \  
  --availability-set myAvailabilitySet \  

```

SSH to your VM with the DNS entry you provided when you created the public IP address. This `fqdn` is shown in the output as you create your VM:

```
{  
  "fqdns": "mypublicdns.eastus.cloudapp.azure.com",  
  "id": "/subscriptions/guid/resourceGroups/myResourceGroup/providers/Microsoft.Compute/virtualMachines/myVM",  
  "location": "eastus",  
  "macAddress": "00-0D-3A-13-71-C8",  
  "powerState": "VM running",  
  "privateIpAddress": "192.168.1.5",  
  "publicIpAddress": "13.90.94.252",  
  "resourceGroup": "myResourceGroup"  
}
```

```
ssh azureuser@mypublicdns.eastus.cloudapp.azure.com
```

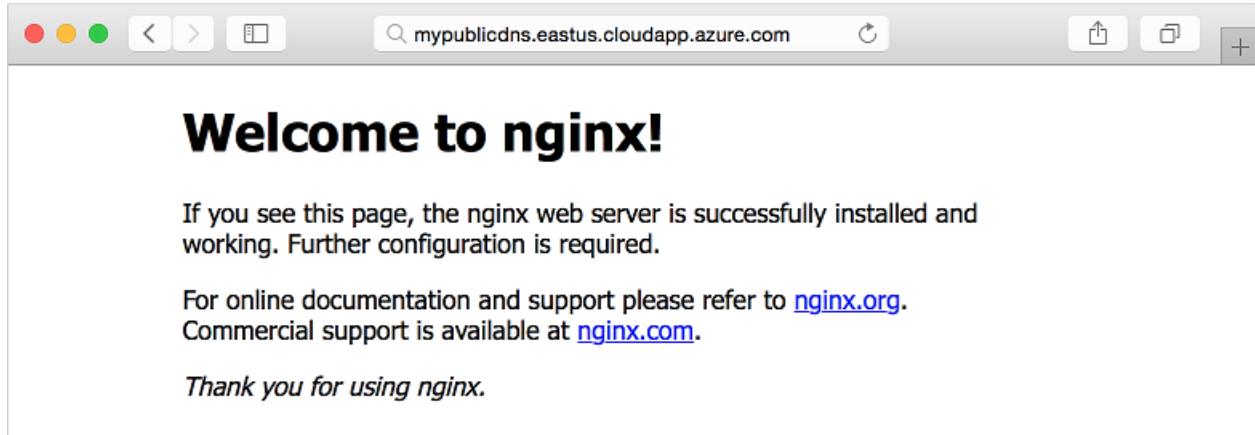
Output:

```
The authenticity of host 'mypublicdns.eastus.cloudapp.azure.com (13.90.94.252)' can't be established.  
ECDSA key fingerprint is SHA256:SyIINP80Um6XRTvWiFaNz+H+1jcrKB1IIiNgCDDJRj6A.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added 'mypublicdns.eastus.cloudapp.azure.com,13.90.94.252' (ECDSA) to the list of known  
hosts.  
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.11.0-1016-azure x86_64)  
  
* Documentation: https://help.ubuntu.com  
* Management: https://landscape.canonical.com  
* Support: https://ubuntu.com/advantage  
  
Get cloud support with Ubuntu Advantage Cloud Guest:  
https://www.ubuntu.com/business/services/cloud  
  
0 packages can be updated.  
0 updates are security updates.  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
azureuser@myVM:~$
```

You can install NGINX and see the traffic flow to the VM. Install NGINX as follows:

```
sudo apt-get install -y nginx
```

To see the default NGINX site in action, open your web browser and enter your FQDN:



Export as a template

What if you now want to create an additional development environment with the same parameters, or a production environment that matches it? Resource Manager uses JSON templates that define all the parameters for your environment. You build out entire environments by referencing this JSON template. You can [build JSON](#)

templates manually or export an existing environment to create the JSON template for you. Use [az group export](#) to export your resource group as follows:

```
az group export --name myResourceGroup > myResourceGroup.json
```

This command creates the `myResourceGroup.json` file in your current working directory. When you create an environment from this template, you are prompted for all the resource names. You can populate these names in your template file by adding the `--include-parameter-default-value` parameter to the `az group export` command. Edit your JSON template to specify the resource names, or [create a parameters.json file](#) that specifies the resource names.

To create an environment from your template, use [az group deployment create](#) as follows:

```
az group deployment create \  
  --resource-group myNewResourceGroup \  
  --template-file myResourceGroup.json
```

You might want to read [more about how to deploy from templates](#). Learn about how to incrementally update environments, use the parameters file, and access templates from a single storage location.

Next steps

Now you're ready to begin working with multiple networking components and VMs. You can use this sample environment to build out your application by using the core components introduced here.

How to create a Linux virtual machine with Azure Resource Manager templates

1/14/2020 • 4 minutes to read • [Edit Online](#)

Learn how to create a Linux virtual machine (VM) by using an Azure Resource Manager template and the Azure CLI from the Azure Cloud shell. To create a Windows virtual machine, see [Create a Windows virtual machine from a Resource Manager template](#).

Templates overview

Azure Resource Manager templates are JSON files that define the infrastructure and configuration of your Azure solution. By using a template, you can repeatedly deploy your solution throughout its lifecycle and have confidence your resources are deployed in a consistent state. To learn more about the format of the template and how you construct it, see [Quickstart: Create and deploy Azure Resource Manager templates by using the Azure portal](#). To view the JSON syntax for resources types, see [Define resources in Azure Resource Manager templates](#).

Create a virtual machine

Creating an Azure virtual machine usually includes two steps:

1. Create a resource group. An Azure resource group is a logical container into which Azure resources are deployed and managed. A resource group must be created before a virtual machine.
2. Create a virtual machine.

The following example creates a VM from an [Azure Quickstart template](#). Only SSH authentication is allowed for this deployment. When prompted, provide the value of your own SSH public key, such as the contents of `~/.ssh/id_rsa.pub`. If you need to create an SSH key pair, see [How to create and use an SSH key pair for Linux VMs in Azure](#). Here is a copy of the template:

```
{  
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json",  
  "contentVersion": "1.0.0.0",  
  "parameters": {  
    "projectName": {  
      "type": "string",  
      "metadata": {  
        "description": "Specifies a name for generating resource names."  
      }  
    },  
    "location": {  
      "type": "string",  
      "defaultValue": "[resourceGroup().location]",  
      "metadata": {  
        "description": "Specifies the location for all resources."  
      }  
    },  
    "adminUsername": {  
      "type": "string",  
      "metadata": {  
        "description": "Specifies a username for the Virtual Machine."  
      }  
    },  
    "adminPublicKey": {  
      "type": "string",  
      "metadata": {  
        "description": "Specifies the public key for SSH authentication."  
      }  
    }  
  },  
  "resources": [  
    {  
      "type": "Microsoft.Compute/virtualMachines",  
      "name": "[parameters('projectName')]",  
      "location": "[parameters('location')]",  
      "properties": {  
        "osProfile": {  
          "computerName": "[parameters('projectName')]",  
          "adminUsername": "[parameters('adminUsername')]",  
          "linuxConfiguration": {  
            "metadata": {  
              "ssh": {  
                "publicKeys": [{  
                  "keyData": "[parameters('adminPublicKey')]"  
                }]  
              }  
            }  
          }  
        }  
      }  
    }  
  ]  
}
```

```

        "description": "Specifies the SSH rsa public key file as a string. Use \"ssh-keygen -t rsa -b 2048\" to generate your SSH key pairs."
    }
},
},
"variables": {
    "vNetName": "[concat(parameters(' projectName'), '-vnet')]",
    "vNetAddressPrefixes": "10.0.0.0/16",
    "vNetSubnetName": "default",
    "vNetSubnetAddressPrefix": "10.0.0.0/24",
    "vmName": "[concat(parameters(' projectName'), '-vm')]",
    "publicIPAddressName": "[concat(parameters(' projectName'), '-ip')]",
    "networkInterfaceName": "[concat(parameters(' projectName'), '-nic')]",
    "networkSecurityGroupName": "[concat(parameters(' projectName'), '-nsg')]"
},
"resources": [
{
    "type": "Microsoft.Network/networkSecurityGroups",
    "apiVersion": "2018-11-01",
    "name": "[variables('networkSecurityGroupName')]",
    "location": "[parameters('location')]",
    "properties": {
        "securityRules": [
            {
                "name": "ssh_rule",
                "properties": {
                    "description": "Locks inbound down to ssh default port 22.",
                    "protocol": "Tcp",
                    "sourcePortRange": "*",
                    "destinationPortRange": "22",
                    "sourceAddressPrefix": "*",
                    "destinationAddressPrefix": "*",
                    "access": "Allow",
                    "priority": 123,
                    "direction": "Inbound"
                }
            }
        ]
    }
},
{
    "type": "Microsoft.Network/publicIPAddresses",
    "apiVersion": "2018-11-01",
    "name": "[variables('publicIPAddressName')]",
    "location": "[parameters('location')]",
    "properties": {
        "publicIPAllocationMethod": "Dynamic"
    },
    "sku": {
        "name": "Basic"
    }
},
{
    "type": "Microsoft.Network/virtualNetworks",
    "apiVersion": "2018-11-01",
    "name": "[variables('vNetName')]",
    "location": "[parameters('location')]",
    "properties": {
        "addressSpace": {
            "addressPrefixes": [
                "[variables('vNetAddressPrefixes')]"
            ]
        },
        "subnets": [
            {
                "name": "[variables('vNetSubnetName')]",
                "properties": {
                    "addressPrefix": "[variables('vNetSubnetAddressPrefix')]"
                }
            }
        ]
    }
}
]
```

```

        }
    ]
}
},
{
    "type": "Microsoft.Network/networkInterfaces",
    "apiVersion": "2018-11-01",
    "name": "[variables('networkInterfaceName')]",
    "location": "[parameters('location')]",
    "dependsOn": [
        "[resourceId('Microsoft.Network/publicIPAddresses', variables('publicIPAddressName'))]",
        "[resourceId('Microsoft.Network/virtualNetworks', variables('vNetName'))]",
        "[resourceId('Microsoft.Network/networkSecurityGroups', variables('networkSecurityGroupName'))]"
    ],
    "properties": {
        "ipConfigurations": [
            {
                "name": "ipconfig1",
                "properties": {
                    "privateIPAllocationMethod": "Dynamic",
                    "publicIPAddress": {
                        "id": "[resourceId('Microsoft.Network/publicIPAddresses', variables('publicIPAddressName'))]"
                    },
                    "subnet": {
                        "id": "[resourceId('Microsoft.Network/virtualNetworks/subnets', variables('vNetName'), variables('vNetSubnetName'))]"
                    }
                }
            }
        ]
    }
},
{
    "type": "Microsoft.Compute/virtualMachines",
    "apiVersion": "2018-10-01",
    "name": "[variables('vmName')]",
    "location": "[parameters('location')]",
    "dependsOn": [
        "[resourceId('Microsoft.Network/networkInterfaces', variables('networkInterfaceName'))]"
    ],
    "properties": {
        "hardwareProfile": {
            "vmSize": "Standard_D2s_v3"
        },
        "osProfile": {
            "computerName": "[variables('vmName')]",
            "adminUsername": "[parameters('adminUsername')]",
            "linuxConfiguration": {
                "disablePasswordAuthentication": true,
                "ssh": {
                    "publicKeys": [
                        {
                            "path": "[concat('/home/', parameters('adminUsername'), '/.ssh/authorized_keys')]",
                            "keyData": "[parameters('adminPublicKey')]"
                        }
                    ]
                }
            }
        },
        "storageProfile": {
            "imageReference": {
                "publisher": "Canonical",
                "offer": "UbuntuServer",
                "sku": "18.04-LTS",
                "version": "latest"
            },
            "osDisk": {
                "createOption": "fromImage"
            }
        }
    }
}

```

```

        },
      "networkProfile": {
        "networkInterfaces": [
          {
            "id": "[resourceId('Microsoft.Network/networkInterfaces', variables('networkInterfaceName'))]"
          }
        ]
      }
    ],
  "outputs": {
    "adminUsername": {
      "type": "string",
      "value": "[parameters('adminUsername')]"
    }
  }
}

```

To run the CLI script, Select **Try it** to open the Azure Cloud shell. To paste the script, right-click the shell, and then select **Paste**:

```

echo "Enter the Resource Group name:" &&
read resourceGroupName &&
echo "Enter the location (i.e. centralus):" &&
read location &&
echo "Enter the project name (used for generating resource names):" &&
read projectName &&
echo "Enter the administrator username:" &&
read username &&
echo "Enter the SSH public key:" &&
read key &&
az group create --name $resourceGroupName --location "$location" &&
az group deployment create --resource-group $resourceGroupName --template-uri
https://raw.githubusercontent.com/azure/azure-quickstart-templates/master/101-vm-sshkey/azuredeploy.json -->
parameters projectName=$projectName adminUsername=$username adminPublicKey="$key" &&
az vm show --resource-group $resourceGroupName --name "$projectName-vm" --show-details --query publicIps -->
output tsv

```

The last Azure CLI command shows the public IP address of the newly created VM. You need the public IP address to connect to the virtual machine. See the next section of this article.

In the previous example, you specified a template stored in GitHub. You can also download or create a template and specify the local path with the `--template-file` parameter.

Here are some additional resources:

- To learn how to develop Resource Manager templates, see [Azure Resource Manager documentation](#).
- To see the Azure virtual machine schemas, see [Azure template reference](#).
- To see more virtual machine template samples, see [Azure Quickstart templates](#).

Connect to virtual machine

You can then SSH to your VM as normal. Provide your own public IP address from the preceding command:

```
ssh <adminUsername>@<ipAddress>
```

Next steps

In this example, you created a basic Linux VM. For more Resource Manager templates that include application frameworks or create more complex environments, browse the [Azure Quickstart templates](#).

To learn more about creating templates, view the JSON syntax and properties for the resources types you deployed:

- [Microsoft.Network/networkSecurityGroups](#)
- [Microsoft.Network/publicIPAddresses](#)
- [Microsoft.Network/virtualNetworks](#)
- [Microsoft.Network/networkInterfaces](#)
- [Microsoft.Compute/virtualMachines](#)

Create a Linux virtual machine that uses SSH authentication with the REST API

11/13/2019 • 3 minutes to read • [Edit Online](#)

A Linux virtual machine (VM) in Azure consists of various resources such as disks and network interfaces and defines parameters such as location, size and operating system image and authentication settings.

You can create a Linux VM via the Azure portal, Azure CLI 2.0, many Azure SDKs, Azure Resource Manager templates and many third-party tools such as Ansible or Terraform. All these tools ultimately use the REST API to create the Linux VM.

This article shows you how to use the REST API to create a Linux VM running Ubuntu 18.04-LTS with managed disks and SSH authentication.

Before you start

Before you create and submit the request, you will need:

- The `{subscription-id}` for your subscription
 - If you have multiple subscriptions, see [Working with multiple subscriptions](#)
- A `{resourceGroupName}` you've created ahead of time
- A [virtual network interface](#) in the same resource group
- An SSH key pair (you can [generate a new one](#) if you don't have one)

Request basics

To create or update a virtual machine, use the following *PUT* operation:

```
PUT https://management.azure.com/subscriptions/{subscription-
id}/resourceGroups/{resourceGroupName}/providers/Microsoft.Compute/virtualMachines/{vmName}?api-version=2017-
12-01
```

In addition to the `{subscription-id}` and `{resourceGroupName}` parameters, you'll need to specify the `{vmName}` (`api-version` is optional, but this article was tested with `api-version=2017-12-01`)

The following headers are required:

REQUEST HEADER	DESCRIPTION
<code>Content-Type:</code>	Required. Set to <code>application/json</code> .
<code>Authorization:</code>	Required. Set to a valid <code>Bearer</code> access token .

For general information about working with REST API requests, see [Components of a REST API request/response](#).

Create the request body

The following common definitions are used to build a request body:

NAME	REQUIRED	TYPE	DESCRIPTION
location	True	string	Resource location.
name		string	Name for the virtual machine.
properties.hardwareProfile		HardwareProfile	Specifies the hardware settings for the virtual machine.
properties.storageProfile		StorageProfile	Specifies the storage settings for the virtual machine disks.
properties.osProfile		OSProfile	Specifies the operating system settings for the virtual machine.
properties.networkProfile		NetworkProfile	Specifies the network interfaces of the virtual machine.

An example request body is below. Make sure you specify the VM name in the `{computerName}` and `{name}` parameters, the name of the network interface you've created under `networkInterfaces`, your username in `adminUsername` and `path`, and the *public* portion of your SSH keypair (located in, for example, `~/.ssh/id_rsa.pub`) in `keyData`. Other parameters you might want to modify include `location` and `vmSize`.

```
{
  "location": "eastus",
  "name": "{vmName}",
  "properties": {
    "hardwareProfile": {
      "vmSize": "Standard_DS1_v2"
    },
    "storageProfile": {
      "imageReference": {
        "sku": "18.04-LTS",
        "publisher": "Canonical",
        "version": "latest",
        "offer": "UbuntuServer"
      },
      "osDisk": {
        "caching": "ReadWrite",
        "managedDisk": {
          "storageAccountType": "Premium_LRS"
        },
        "name": "myVMosdisk",
        "createOption": "FromImage"
      }
    },
    "osProfile": {
      "adminUsername": "{your-username}",
      "computerName": "{vmName}",
      "linuxConfiguration": {
        "ssh": {
          "publicKeys": [
            {
              "path": "/home/{your-username}/.ssh/authorized_keys",
              "keyData": "ssh-rsa AAAAB3NzaC1{snip}mf69/J1"
            }
          ]
        },
        "disablePasswordAuthentication": true
      }
    },
    "networkProfile": {
      "networkInterfaces": [
        {
          "id": "/subscriptions/{subscription-
id}/resourceGroups/{resourceGroupName}/providers/Microsoft.Network/networkInterfaces/{existing-nic-name}",
          "properties": {
            "primary": true
          }
        }
      ]
    }
  }
}
```

For a complete list of the available definitions in the request body, see [Virtual machines create or update request body definitions](#).

Sending the request

You may use the client of your preference for sending this HTTP request. You may also use an [in-browser tool](#) by clicking the **Try it** button.

Responses

There are two successful responses for the operation to create or update a virtual machine:

NAME	TYPE	DESCRIPTION
200 OK	VirtualMachine	OK
201 Created	VirtualMachine	Created

A condensed *201 Created* response from the previous example request body that creates a VM shows a *vmId* has been assigned and the *provisioningState* is *Creating*:

```
{
  "vmId": "e0de9b84-a506-4b95-9623-00a425d05c90",
  "provisioningState": "Creating"
}
```

For more information about REST API responses, see [Process the response message](#).

Next steps

For more information on the Azure REST APIs or other management tools such as Azure CLI or Azure PowerShell, see the following:

- [Azure Compute provider REST API](#)
- [Get started with Azure REST API](#)
- [Azure CLI](#)
- [Azure PowerShell module](#)

Create a copy of a Linux VM by using Azure CLI and Managed Disks

2/10/2020 • 2 minutes to read • [Edit Online](#)

This article shows you how to create a copy of your Azure virtual machine (VM) running Linux by using the Azure CLI and the Azure Resource Manager deployment model.

You can also [upload and create a VM from a VHD](#).

Prerequisites

- Install the [Azure CLI](#).
- Sign in to an Azure account with [az login](#).
- Have an Azure VM to use as the source for your copy.

Stop the source VM

Deallocate the source VM by using [az vm deallocate](#). The following example deallocates the VM named *myVM* in the resource group *myResourceGroup*:

```
az vm deallocate \
    --resource-group myResourceGroup \
    --name myVM
```

Copy the source VM

To copy a VM, you create a copy of the underlying virtual hard disk. This process creates a specialized virtual hard disk (VHD) as a Managed Disk that contains the same configuration and settings as the source VM.

For more information about Azure Managed Disks, see [Azure Managed Disks overview](#).

1. List each VM and the name of its OS disk with [az vm list](#). The following example lists all VMs in the resource group named *myResourceGroup*:

```
az vm list -g myResourceGroup \
    --query '[].{Name:name,DiskName:storageProfile.osDisk.name}' \
    --output table
```

The output is similar to the following example:

Name	DiskName
-----	-----
myVM	myDisk

2. Copy the disk by creating a new managed disk and by using [az disk create](#). The following example creates a disk named *myCopiedDisk* from the managed disk named *myDisk*:

```
az disk create --resource-group myResourceGroup \
--name myCopiedDisk --source myDisk
```

3. Verify the managed disks now in your resource group by using [az disk list](#). The following example lists the managed disks in the resource group named *myResourceGroup*:

```
az disk list --resource-group myResourceGroup --output table
```

Set up a virtual network

The following optional steps create a new virtual network, subnet, public IP address, and virtual network interface card (NIC).

If you are copying a VM for troubleshooting purposes or additional deployments, you might not want to use a VM in an existing virtual network.

If you want to create a virtual network infrastructure for your copied VMs, follow the next few steps. If you don't want to create a virtual network, skip to [Create a VM](#).

1. Create the virtual network by using [az network vnet create](#). The following example creates a virtual network named *myVnet* and a subnet named *mySubnet*:

```
az network vnet create --resource-group myResourceGroup \
--location eastus --name myVnet \
--address-prefix 192.168.0.0/16 \
--subnet-name mySubnet \
--subnet-prefix 192.168.1.0/24
```

2. Create a public IP by using [az network public-ip create](#). The following example creates a public IP named *myPublicIP* with the DNS name of *mypublicdns*. (Because the DNS name must be unique, provide a unique name.)

```
az network public-ip create --resource-group myResourceGroup \
--location eastus --name myPublicIP --dns-name mypublicdns \
--allocation-method static --idle-timeout 4
```

3. Create the NIC by using [az network nic create](#). The following example creates a NIC named *myNic* that's attached to the *mySubnet* subnet:

```
az network nic create --resource-group myResourceGroup \
--location eastus --name myNic \
--vnet-name myVnet --subnet mySubnet \
--public-ip-address myPublicIP
```

Create a VM

Create a VM by using [az vm create](#).

Specify the copied managed disk to use as the OS disk (`--attach-os-disk`), as follows:

```
az vm create --resource-group myResourceGroup \
--name myCopiedVM --nics myNic \
--size Standard_DS1_v2 --os-type Linux \
--attach-os-disk myCopiedDisk
```

Next steps

To learn how to use a [shared image gallery](#) to manage VM images.

Deploy VMs to dedicated hosts using the Azure CLI

2/20/2020 • 5 minutes to read • [Edit Online](#)

This article guides you through how to create an Azure [dedicated host](#) to host your virtual machines (VMs).

Make sure that you have installed Azure CLI version 2.0.70 or later, and signed in to an Azure account using `az login`.

Limitations

- Virtual machine scale sets are not currently supported on dedicated hosts.
- The initial release supports the following VM series: DSv3, ESv3, FSv2, LSv2, and MSv2.

Create resource group

An Azure resource group is a logical container into which Azure resources are deployed and managed. Create the resource group with `az group create`. The following example creates a resource group named `myDHRResourceGroup` in the *East US* location.

```
az group create --name myDHRResourceGroup --location eastus
```

Create a host group

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. When planning for high availability, there are additional options. You can use one or both of the following options with your dedicated hosts:

- Span across multiple availability zones. In this case, you are required to have a host group in each of the zones you wish to use.
- Span across multiple fault domains which are mapped to physical racks.

In either case, you are need to provide the fault domain count for your host group. If you do not want to span fault domains in your group, use a fault domain count of 1.

You can also decide to use both availability zones and fault domains.

In this example, we will use `az vm host group create` to create a host group using both availability zones and fault domains.

```
az vm host group create \
--name myHostGroup \
-g myDHRResourceGroup \
-z 1 \
--platform-fault-domain-count 2
```

Other examples

You can also use `az vm host group create` to create a host group in availability zone 1 (and no fault domains).

```
az vm host group create \
--name myAZHostGroup \
-g myDHRessourceGroup \
-z 1 \
--platform-fault-domain-count 1
```

The following uses [az vm host group create](#) to create a host group by using fault domains only (to be used in regions where availability zones are not supported).

```
az vm host group create \
--name myFDHostGroup \
-g myDHRessourceGroup \
--platform-fault-domain-count 2
```

Create a host

Now let's create a dedicated host in the host group. In addition to a name for the host, you are required to provide the SKU for the host. Host SKU captures the supported VM series as well as the hardware generation for your dedicated host. The following SKU values are supported: DSv3_Type1 and ESv3_Type1.

For more information about the host SKUs and pricing, see [Azure Dedicated Host pricing](#).

Use [az vm host create](#) to create a host. If you set a fault domain count for your host group, you will be asked to specify the fault domain for your host.

```
az vm host create \
--host-group myHostGroup \
--name myHost \
--sku DSv3-Type1 \
--platform-fault-domain 1 \
-g myDHRessourceGroup
```

Create a virtual machine

Create a virtual machine within a dedicated host using [az vm create](#). If you specified an availability zone when creating your host group, you are required to use the same zone when creating the virtual machine.

```
az vm create \
-n myVM \
--image debian \
--generate-ssh-keys \
--host-group myHostGroup \
--host myHost \
--generate-ssh-keys \
--size Standard_D4s_v3 \
-g myDHRessourceGroup \
--zone 1
```

WARNING

If you create a virtual machine on a host which does not have enough resources, the virtual machine will be created in a FAILED state.

Check the status of the host

You can check the host health status and how many virtual machines you can still deploy to the host using [az vm host get-instance-view](#).

```
az vm host get-instance-view \
-g myDHRessourceGroup \
--host-group myHostGroup \
--name myHost
```

The output will look similar to this:

```
{
  "autoReplaceOnFailure": true,
  "hostId": "6de80643-0f45-4e94-9a4c-c49d5c777b62",
  "id": "/subscriptions/10101010-1010-1010-1010-
1010101010/resourceGroups/myDHRessourceGroup/providers/Microsoft.Compute/hostGroups/myHostGroup/hosts/myHost"
,
  "instanceView": {
    "assetId": "12345678-1234-1234-abcd-abc123456789",
    "availableCapacity": {
      "allocatableVms": [
        {
          "count": 31.0,
          "vmSize": "Standard_D2s_v3"
        },
        {
          "count": 15.0,
          "vmSize": "Standard_D4s_v3"
        },
        {
          "count": 7.0,
          "vmSize": "Standard_D8s_v3"
        },
        {
          "count": 3.0,
          "vmSize": "Standard_D16s_v3"
        },
        {
          "count": 1.0,
          "vmSize": "Standard_D32-8s_v3"
        },
        {
          "count": 1.0,
          "vmSize": "Standard_D32-16s_v3"
        },
        {
          "count": 1.0,
          "vmSize": "Standard_D32s_v3"
        },
        {
          "count": 1.0,
          "vmSize": "Standard_D48s_v3"
        },
        {
          "count": 0.0,
          "vmSize": "Standard_D64-16s_v3"
        },
        {
          "count": 0.0,
          "vmSize": "Standard_D64-32s_v3"
        },
        {
          "count": 0.0,
          "vmSize": "Standard_D64s_v3"
        }
      ]
    }
  }
}
```

```
        },
        "statuses": [
            {
                "code": "ProvisioningState/succeeded",
                "displayStatus": "Provisioning succeeded",
                "level": "Info",
                "message": null,
                "time": "2019-07-24T21:22:40.604754+00:00"
            },
            {
                "code": "HealthState/available",
                "displayStatus": "Host available",
                "level": "Info",
                "message": null,
                "time": null
            }
        ]
    },
    "licenseType": null,
    "location": "eastus2",
    "name": "myHost",
    "platformFaultDomain": 1,
    "provisioningState": "Succeeded",
    "provisioningTime": "2019-07-24T21:22:40.604754+00:00",
    "resourceGroup": "myDHResourceGroup",
    "sku": {
        "capacity": null,
        "name": "DSv3-Type1",
        "tier": null
    },
    "tags": null,
    "type": null,
    "virtualMachines": [
        {
            "id": "/subscriptions/10101010-1010-1010-1010-
10101010/resourceGroups/MYDHRESOURCEGROUP/providers/Microsoft.Compute/virtualMachines/MYVM",
            "resourceGroup": "MYDHRESOURCEGROUP"
        }
    ]
}
```

Export as a template

You can export a template if you now want to create an additional development environment with the same parameters, or a production environment that matches it. Resource Manager uses JSON templates that define all the parameters for your environment. You build out entire environments by referencing this JSON template. You can build JSON templates manually or export an existing environment to create the JSON template for you. Use [az group export](#) to export your resource group.

```
az group export --name myDHResourceGroup > myDHResourceGroup.json
```

This command creates the `myDHResourceGroup.json` file in your current working directory. When you create an environment from this template, you are prompted for all the resource names. You can populate these names in your template file by adding the `--include-parameter-default-value` parameter to the `az group export` command. Edit your JSON template to specify the resource names, or create a `parameters.json` file that specifies the resource names.

To create an environment from your template, use [az group deployment create](#).

```
az group deployment create \
--resource-group myNewResourceGroup \
--template-file myDHResourceGroup.json
```

Clean up

You are being charged for your dedicated hosts even when no virtual machines are deployed. You should delete any hosts you are currently not using to save costs.

You can only delete a host when there are no any longer virtual machines using it. Delete the VMs using [az vm delete](#).

```
az vm delete -n myVM -g myDHResourceGroup
```

After deleting the VMs, you can delete the host using [az vm host delete](#).

```
az vm host delete -g myDHResourceGroup --host-group myHostGroup --name myHost
```

Once you have deleted all of your hosts, you may delete the host group using [az vm host group delete](#).

```
az vm host group delete -g myDHResourceGroup --host-group myHostGroup
```

You can also delete the entire resource group in a single command. This will delete all resources created in the group, including all of the VMs, hosts and host groups.

```
az group delete -n myDHResourceGroup
```

Next steps

- For more information, see the [Dedicated hosts](#) overview.
- You can also create dedicated hosts using the [Azure portal](#).
- There is sample template, found [here](#), that uses both zones and fault domains for maximum resiliency in a region.

Deploy VMs to dedicated hosts using the portal

1/9/2020 • 4 minutes to read • [Edit Online](#)

This article guides you through how to create an Azure [dedicated host](#) to host your virtual machines (VMs).

Limitations

- Virtual machine scale sets are not currently supported on dedicated hosts.
- The initial release supports the following VM series: DSv3, ESv3, FSv2, LSv2, and MSv2.

Create a host group

A **host group** is a new 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. When planning for high availability, there are additional options. You can use one or both of the following options with your dedicated hosts:

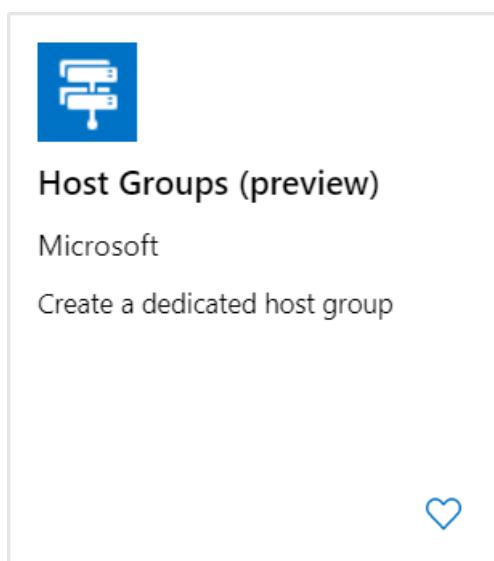
- Span across multiple availability zones. In this case, you are required to have a host group in each of the zones you wish to use.
- Span across multiple fault domains which are mapped to physical racks.

In either case, you are need to provide the fault domain count for your host group. If you do not want to span fault domains in your group, use a fault domain count of 1.

You can also decide to use both availability zones and fault domains.

In this example, we will create a host group using 1 availability zone and 2 fault domains.

1. Open the Azure [portal](#).
2. Select **Create a resource** in the upper left corner.
3. Search for **Host group** and then select **Host Groups** from the results.



4. In the **Host Groups** page, select **Create**.
5. Select the subscription you would like to use, and then select **Create new** to create a new resource group.
6. Type *myDedicatedHostsRG* as the **Name** and then select **OK**.

7. For **Host group name**, type *myHostGroup*.
8. For **Location**, select **East US**.
9. For **Availability Zone**, select **1**.
10. For **Fault domain count**, select **2**.
11. Select **Review + create** and then wait for validation.

Home > New > Marketplace > Host Groups (preview) > Create host group

Create host group

Project details

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

* Subscription <small>i</small>	VMTesting1
└─ * Resource group <small>i</small>	myDedicatedHostRG
	Create new

Instance details

* Host group name <small>i</small>	myHostGroup
* Location <small>i</small>	(US) East US
Availability zone <small>i</small>	1
* Fault domain count <small>i</small>	2

Review + create [< Previous](#) [Next : Tags >](#)

12. Once you see the **Validation passed** message, select **Create** to create the host group.

It should only take a few moments to create the host group.

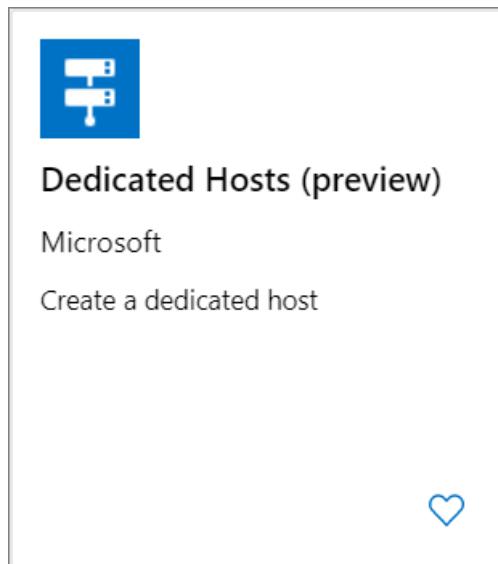
Create a dedicated host

Now create a dedicated host in the host group. In addition to a name for the host, you are required to provide the SKU for the host. Host SKU captures the supported VM series as well as the hardware generation for your dedicated host.

For more information about the host SKUs and pricing, see [Azure Dedicated Host pricing](#).

If you set a fault domain count for your host group, you will be asked to specify the fault domain for your host.

1. Select **Create a resource** in the upper left corner.
2. Search for **Dedicated host** and then select **Dedicated hosts** from the results.



3. In the **Dedicated Hosts** page, select **Create**.
4. Select the subscription you would like to use.
5. Select *myDedicatedHostsRG* as the **Resource group**.
6. In **Instance details**, type *myHost* for the **Name** and select *East US* for the location.
7. In **Hardware profile**, select *Standard Es3 family - Type 1* for the **Size family**, select *myHostGroup* for the **Host group** and then select *1* for the **Fault domain**. Leave the defaults for the rest of the fields.
8. When you are done, select **Review + create** and wait for validation.

Project details

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

* Subscription <small>?</small>	VMTesting1
└─ * Resource group <small>?</small>	myDedicatedHostRG
	Create new

Instance details

* Name <small>?</small>	myHost
* Location <small>?</small>	(US) East US

Hardware profile

* Size family <small>?</small>	Standard Es3 Family - Type 1
* Host group <small>?</small>	myHostGroup
* Fault domain	1
* Automatically replace host on failure <small>?</small>	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

9. Once you see the **Validation passed** message, select **Create** to create the host.

Create a VM

1. Choose **Create a resource** in the upper left corner of the Azure portal.
2. In the search box above the list of Azure Marketplace resources, search for and select **Ubuntu Server 16.04 LTS** by Canonical, then choose **Create**.

3. In the **Basics** tab, under **Project details**, make sure the correct subscription is selected and then select *myDedicatedHostsRG* as the **Resource group**.
4. Under **Instance details**, type *myVM* for the **Virtual machine name** and choose *East US* for your **Location**.
5. In **Availability options** select **Availability zone**, select *1* from the drop-down.
6. For the size, select **Change size**. In the list of available sizes, choose one from the Esv3 series, like **Standard E2s v3**. You may need to clear the filter in order to see all of the available sizes.
7. Under **Administrator account**, select **SSH public key**, type your user name, then paste your public key into the text box. Remove any leading or trailing white space in your public key.

Administrator account

Authentication type Password SSH public key

Username * ✓

SSH public key *

[Learn more about creating and using SSH keys in Azure](#)

8. Under **Inbound port rules > Public inbound ports**, choose **Allow selected ports** and then select **SSH (22)** from the drop-down.
9. At the top of the page, select the **Advanced** tab and in the **Host** section, select *myHostGroup* for **Host group** and *myHost* for the **Host**.

Host

Optionally placing your virtual machine in a host [Learn more](#)

Host group ▼

Host ▼

10. Leave the remaining defaults and then select the **Review + create** button at the bottom of the page.
11. When you see the message that validation has passed, select **Create**.

It will take a few minutes for your VM to be deployed.

Next steps

- For more information, see the [Dedicated hosts](#) overview.
- There is sample template, found [here](#), that uses both zones and fault domains for maximum resiliency in a region.
- You can also deploy a dedicated host using the [Azure CLI](#).

Preview: Deploy Spot VMs using the Azure CLI

2/12/2020 • 2 minutes to read • [Edit Online](#)

Using [Azure Spot VMs](#) 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 Spot VMs. Therefore, Spot VMs are great for workloads that can handle interruptions like batch processing jobs, dev/test environments, large compute workloads, and more.

Pricing for Spot VMs is variable, based on region and SKU. For more information, see VM pricing for [Linux](#) and [Windows](#).

You have option to set a max price you are willing to pay, per hour, for the VM. The max price for a Spot VM can be set in US dollars (USD), using up to 5 decimal places. For example, the value `0.98765` would be a max price of \$0.98765 USD per hour. If you set the max price to be `-1`, the VM won't be evicted based on price. The price for the VM will be the current price for Spot or the price for a standard VM, whichever is less, as long as there is capacity and quota available. For more information about setting the max price, see [Spot VMs - Pricing](#).

The process to create a VM with Spot using the Azure CLI is the same as detailed in the [quickstart article](#). Just add the '--priority Spot' parameter and provide a max price or `-1`.

IMPORTANT

Spot instances are currently in public preview. This preview version is not recommended for production workloads. Certain features might not be supported or might have constrained capabilities. For more information, see [Supplemental Terms of Use for Microsoft Azure Previews](#).

Install Azure CLI

To create Spot VMs, you need to be running the Azure CLI version 2.0.74 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install the Azure CLI](#).

Sign in to Azure using `az login`.

```
az login
```

Create a Spot VM

This example shows how to deploy a Linux Spot VM that will not be evicted based on price.

```
az group create -n mySpotGroup -l eastus
az vm create \
    --resource-group mySpotGroup \
    --name myVM \
    --image UbuntuLTS \
    --admin-username azureuser \
    --generate-ssh-keys \
    --priority Spot \
    --max-price -1
```

After the VM is created, you can query to see the max billing price for all of the VMs in the resource group.

```
az vm list \
-g mySpotGroup \
--query '[].{Name:name, MaxPrice:billingProfile.maxPrice}' \
--output table
```

Next steps

You can also create a Spot VM using [Azure PowerShell](#) or a [template](#).

If you encounter an error, see [Error codes](#).

Preview: Deploy Spot VMs using the Azure portal

2/12/2020 • 2 minutes to read • [Edit Online](#)

Using [Spot VMs](#) 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 Spot VMs. Therefore, Spot VMs are great for workloads that can handle interruptions like batch processing jobs, dev/test environments, large compute workloads, and more.

Pricing for Spot VMs is variable, based on region and SKU. For more information, see VM pricing for [Linux](#) and [Windows](#). For more information about setting the max price, see [Spot VMs - Pricing](#).

You have option to set a max price you are willing to pay, per hour, for the VM. The max price for a Spot VM can be set in US dollars (USD), using up to 5 decimal places. For example, the value would be a max price of \$0.05701 USD per hour. If you set the max price to be , the VM won't be evicted based on price. The price for the VM will be the current price for spot or the price for a standard VM, whichever is less, as long as there is capacity and quota available.

IMPORTANT

Spot instances are currently in public preview. This preview version is not recommended for production workloads. Certain features might not be supported or might have constrained capabilities. For more information, see [Supplemental Terms of Use for Microsoft Azure Previews](#).

Create the VM

The process to create a VM that uses Spot VMs is the same as detailed in the [quickstart](#). When you are deploying a VM, you can choose to use an Azure spot instance.

On the **Basics** tab, in the **Instance details** section, **No** is the default for using an Azure spot instance.

The screenshot shows the 'Instance details' section of the Azure portal's VM creation wizard. It includes fields for Virtual machine name, Region, Availability options, Image, and Azure Spot instance selection. The 'Azure Spot instance' section is highlighted with a red border around the 'Yes' radio button, indicating it is the selected option.

Instance details	
Virtual machine name *	<input type="text"/>
Region *	(US) West US
Availability options	No infrastructure redundancy required
Image *	Ubuntu Server 18.04 LTS
Browse all public and private images	
Azure Spot instance	<input type="radio"/> Yes <input checked="" type="radio"/> No
Size *	Select size

If you select **Yes**, the section expands and you can choose your [eviction type and eviction policy](#).

Azure Spot instance [\(i\)](#)

Yes No

Eviction type [\(i\)](#)

Capacity only: evict virtual machine when Azure needs the capacity for pay as you go workloads. Your max price is set to the pay as you go rate.

Price or capacity: choose a max price and Azure will evict your virtual machine when the cost of the instance is greater than your max price or when Azure needs the capacity for pay as you go workloads.

Eviction policy [\(i\)](#)

Stop / Deallocate Delete (currently not supported)

Size * [\(i\)](#)

Standard D2s v3
2 vcpus, 8 GiB memory (\$0.01900/hour)
[Change size](#)

Maximum price you want to pay per hour
(USD) [\(i\)](#)

0.05701 

[Compare prices in nearby regions](#)

Next steps

You can also create Spot VMs using [PowerShell](#).

Deploy Spot VMs using a Resource Manager template

2/12/2020 • 2 minutes to read • [Edit Online](#)

Using [Spot VMs](#) 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 Spot VMs. Therefore, Spot VMs are great for workloads that can handle interruptions like batch processing jobs, dev/test environments, large compute workloads, and more.

Pricing for Spot VMs is variable, based on region and SKU. For more information, see VM pricing for [Linux](#) and [Windows](#).

You have option to set a max price you are willing to pay, per hour, for the VM. The max price for a Spot VM can be set in US dollars (USD), using up to 5 decimal places. For example, the value `0.98765` would be a max price of \$0.98765 USD per hour. If you set the max price to be `-1`, the VM won't be evicted based on price. The price for the VM will be the current price for Spot or the price for a standard VM, whichever is less, as long as there is capacity and quota available. For more information about setting the max price, see [Spot VMs - Pricing](#).

IMPORTANT

Spot instances are currently in public preview. This preview version is not recommended for production workloads. Certain features might not be supported or might have constrained capabilities. For more information, see [Supplemental Terms of Use for Microsoft Azure Previews](#).

Use a template

For Spot template deployments, use `"apiVersion": "2019-03-01"` or later. Add the `priority`, `evictionPolicy` and `billingProfile` properties to in your template:

```
    "priority": "Spot",
    "evictionPolicy": "Deallocate",
    "billingProfile": {
        "maxPrice": -1
    }
```

Here is a sample template with the added properties for a Spot VM. Replace the resource names with your own and `<password>` with a password for the local administrator account on the VM.

```
{
    "$schema": "http://schema.management.azure.com/schemas/2019-03-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {},
    "variables": {
        "vnetId": "/subscriptions/ec9fc04-e188-48b9-abfc-
abcd515f1836/resourceGroups/spotVM/providers/Microsoft.Network/virtualNetworks/spotVM",
        "subnetName": "default",
        "networkInterfaceName": "spotVMNIC",
        "publicIpAddressName": "spotVM-ip",
        "publicIpAddressType": "Dynamic",
        "publicIpAddressSku": "Basic",
        "virtualMachineName": "spotVM",
```

```

    "osDiskType": "Premium_LRS",
    "virtualMachineSize": "Standard_D2s_v3",
    "adminUsername": "azureuser",
    "adminPassword": "<password>",
    "diagnosticsStorageAccountName": "diagstoragespot2019",
    "diagnosticsStorageAccountId": "Microsoft.Storage/storageAccounts/diagstoragespot2019",
    "diagnosticsStorageAccountType": "Standard_LRS",
    "diagnosticsStorageAccountKind": "Storage",
    "subnetRef": "[concat(variables('vnetId'), '/subnets/', variables('subnetName'))]"
},
"resources": [
{
    "name": "spotVM",
    "type": "Microsoft.Network/networkInterfaces",
    "apiVersion": "2019-03-01",
    "location": "eastus",
    "dependsOn": [
        "[concat('Microsoft.Network/publicIpAddresses/', variables('publicIpAddressName'))]"
    ],
    "properties": {
        "ipConfigurations": [
            {
                "name": "ipconfig1",
                "properties": {
                    "subnet": {
                        "id": "[variables('subnetRef')]"
                    },
                    "privateIPAllocationMethod": "Dynamic",
                    "publicIpAddress": {
                        "id": "[resourceId(resourceGroup().name,
'Microsoft.Network/publicIpAddresses', variables('publicIpAddressName'))]"
                    }
                }
            }
        ]
    }
},
{
    "name": "[variables('publicIpAddressName')]",
    "type": "Microsoft.Network/publicIpAddresses",
    "apiVersion": "2019-02-01",
    "location": "eastus",
    "properties": {
        "publicIpAllocationMethod": "[variables('publicIpAddressType')]"
    },
    "sku": {
        "name": "[variables('publicIpAddressSku')]"
    }
},
{
    "name": "[variables('virtualMachineName')]",
    "type": "Microsoft.Compute/virtualMachines",
    "apiVersion": "2019-03-01",
    "location": "eastus",
    "dependsOn": [
        "[concat('Microsoft.Network/networkInterfaces/', variables('networkInterfaceName'))]",
        "[concat('Microsoft.Storage/storageAccounts/', variables('diagnosticsStorageAccountName'))]"
    ],
    "properties": {
        "hardwareProfile": {
            "vmSize": "[variables('virtualMachineSize')]"
        },
        "storageProfile": {
            "osDisk": {
                "createOption": "fromImage",
                "managedDisk": {
                    "storageAccountType": "[variables('osDiskType')]"
                }
            }
        }
    }
}
]
}

```

```

        "imageReference": {
            "publisher": "Canonical",
            "offer": "UbuntuServer",
            "sku": "18.04-LTS",
            "version": "latest"
        }
    },
    "networkProfile": {
        "networkInterfaces": [
            {
                "id": "[resourceId('Microsoft.Network/networkInterfaces',
variables('networkInterfaceName'))]"
            }
        ]
    },
    "osProfile": {
        "computerName": "[variables('virtualMachineName')]",
        "adminUsername": "[variables('adminUsername')]",
        "adminPassword": "[variables('adminPassword')]"
    },
    "diagnosticsProfile": {
        "bootDiagnostics": {
            "enabled": true,
            "storageUri": "[concat('https://', variables('diagnosticsStorageAccountName'),
'.blob.core.windows.net/'])"
        }
    },
    "priority": "Spot",
    "evictionPolicy": "Deallocate",
    "billingProfile": {
        "maxPrice": -1
    }
},
{
    "name": "[variables('diagnosticsStorageAccountName')]",
    "type": "Microsoft.Storage/storageAccounts",
    "apiVersion": "2019-04-01",
    "location": "eastus",
    "properties": {},
    "kind": "[variables('diagnosticsStorageAccountKind')]",
    "sku": {
        "name": "[variables('diagnosticsStorageAccountType')]"
    }
},
],
"outputs": {
    "adminUsername": {
        "type": "string",
        "value": "[variables('adminUsername')]"
    }
}
}

```

Next steps

You can also create a Spot VM using [Azure PowerShell](#) or the [Azure CLI](#).

If you encounter an error, see [Error codes](#).

Preview: Error messages for Spot VMs and scale sets

2/10/2020 • 2 minutes to read • [Edit Online](#)

IMPORTANT

Spot VMs and virtual machine scale sets are currently in public preview. This preview version is provided without a service level agreement, and it's not recommended for production workloads. Certain features might not be supported or might have constrained capabilities. For more information, see [Supplemental Terms of Use for Microsoft Azure Previews](#).

Here are some possible error codes you could receive when using Spot VMs and scale sets.

KEY	MESSAGE	DESCRIPTION
SkuNotAvailable	The requested tier for resource '<resource>' is currently not available in location '<location>' for subscription '<subscriptionID>'. Please try another tier or deploy to a different location.	There is not enough Azure Spot capacity in this location to create your VM or scale set instance.
EvictionPolicyCanBeSetOnlyOnAzureSpotVirtualMachines	Eviction policy can be set only on Azure Spot Virtual Machines.	This VM is not a Spot VM, so you can't set the eviction policy.
AzureSpotVMNotSupportedInAvailabilitySet	Azure Spot Virtual Machine is not supported in Availability Set.	You need to choose to either use a Spot VM or use a VM in an availability set, you can't choose both.
AzureSpotFeatureNotEnabledForSubscription	Subscription not enabled with Azure Spot feature.	You need to have a subscription that supports Spot VMs.
VMPriorityCannotBeApplied	The specified priority value '{0}' cannot be applied to the Virtual Machine '{1}' since no priority was specified when the Virtual Machine was created.	You need to specify the priority when the VM is created.
SpotPriceGreater ThanProvidedMaxPrice	Unable to perform operation '{0}' since the provided max price '{1} USD' is lower than the current spot price '{2} USD' for Azure Spot VM size '{3}'.	Select a higher max price. For more information, see pricing information for Linux or Windows .
MaxPriceValueInvalid	Invalid max price value. The only supported values for max price are -1 or a decimal greater than zero. Max price value of -1 indicates the Azure Spot virtual machine will not be evicted for price reasons.	Enter a valid max price. For more information, see pricing for Linux or Windows .
MaxPriceChangeNotAllowedForAllocatedVMs	Max price change is not allowed when the VM '{0}' is currently allocated. Please deallocate and try again.	Stop\Deallocate the VM so that you can change the max price.
MaxPriceChangeNotAllowed	Max price change is not allowed.	You cannot change the max price for this VM.

KEY	MESSAGE	DESCRIPTION
AzureSpotIsNotSupportedForThisAPIVersion	Azure Spot is not supported for this API version.	The API version needs to be 2019-03-01.
AzureSpotIsNotSupportedForThisVMSize	Azure Spot is not supported for this VM size {0}.	Select another VM size. For more information, see Spot Virtual Machines .
MaxPriceIsSupportedOnlyForAzureSpotVirtualMachines	Max price is supported only for Azure Spot Virtual Machines.	For more information, see Spot Virtual Machines .
MoveResourcesWithAzureSpotVMNotSupported	The Move resources request contains a Azure Spot virtual machine. This is currently not supported. Please check the error details for virtual machine Ids.	You cannot move Spot VMs.
MoveResourcesWithAzureSpotVmssNotSupported	The Move resources request contains a Azure Spot virtual machine scale set. This is currently not supported. Please check the error details for virtual machine scale set Ids.	You cannot move Spot scale set instances.
EphemeralOSDisksNotSupportedForSpotVMs	Ephemeral OS disks are not supported for Spot VMs.	You need to be using a regular OS disk for your Spot VM.
AzureSpotVMNotSupportedInVmssWithVMOrchestrationMode	Azure Spot Virtual Machine is not supported in Virtual Machine Scale Set with VM Orchestration mode.	Set the orchestration mode to virtual machine scale set in order to use Spot instances.

Next steps For more information, see [spot Virtual Machines](#).

Migrate your IaaS resources to Azure Resource Manager by March 1, 2023

2/28/2020 • 2 minutes to read • [Edit Online](#)

In 2014, we launched IaaS on Azure Resource Manager, and have been enhancing capabilities ever since. Because [Azure Resource Manager](#) now has full IaaS capabilities and other advancements, we deprecated the management of IaaS VMs through Azure Service Manager on February 28, 2020 and this functionality will be fully retired on March 1, 2023.

Today, about 90% of the IaaS VMs are using Azure Resource Manager. If you use IaaS resources through Azure Service Manager (ASM), start planning your migration now and complete it by March 1, 2023 to take advantage of [Azure Resource Manager](#).

Classic VMs will be following the [Modern Lifecycle Policy](#) for deprecation.

How does this affect me?

1. Starting February 28, 2020, customers who did not utilize IaaS VMs through Azure Service Manager (ASM) in the month of February 2020 will no longer be able to create classic VMs.
2. On March 1, 2023, customers will no longer be able to start IaaS VMs using Azure Service Manager and any that are still running or allocated will be stopped and deallocated.
3. On March 1, 2023, subscriptions who have not migrated to Azure Resource Manager will be informed regarding timelines for deleting any remaining Classic VMs.

The following Azure services and functionality will **NOT** be impacted by this retirement:

- Cloud Services
- Storage accounts **not** used by classic VMs
- Virtual networks (VNets) **not** used by classic VMs.
- Other classic resources

What actions should I take?

- Start planning your migration to Azure Resource Manager, today.
- [Learn more](#) about migrating your classic [Linux](#) and [Windows](#) VMs to Azure Resource Manager.
- For more information, refer to the [Frequently asked questions about classic to Azure Resource Manager migration](#)
- For technical questions and issues, [contact support](#).
- For other questions not part of FAQ and feedback, comment below.

Platform-supported migration of IaaS resources from classic to Azure Resource Manager

2/28/2020 • 8 minutes to read • [Edit Online](#)

IMPORTANT

Today, about 90% of IaaS VMs are using [Azure Resource Manager](#). As of February 28, 2020, classic VMs have been deprecated and will be fully retired on March 1, 2023. [Learn more](#) about this deprecation and [how it affects you](#).

This article describes how to migrate infrastructure as a service (IaaS) resources from the Classic to Resource Manager deployment models and details how to connect resources from the two deployment models that coexist in your subscription by using virtual network site-to-site gateways. You can read more about [Azure Resource Manager features and benefits](#).

Goal for migration

Resource Manager enables deploying complex applications through templates, configures virtual machines by using VM extensions, and incorporates access management and tagging. Azure Resource Manager includes scalable, parallel deployment for virtual machines into availability sets. The new deployment model also provides lifecycle management of compute, network, and storage independently. Finally, there's a focus on enabling security by default with the enforcement of virtual machines in a virtual network.

Almost all the features from the classic deployment model are supported for compute, network, and storage under Azure Resource Manager. To benefit from the new capabilities in Azure Resource Manager, you can migrate existing deployments from the Classic deployment model.

Supported resources for migration

These classic IaaS resources are supported during migration

- Virtual Machines
- Availability Sets
- Storage Accounts
- Virtual Networks
- VPN Gateways
- Express Route Gateways (*in the same subscription as Virtual Network only*)
- Network Security Groups
- Route Tables
- Reserved IPs

Supported scopes of migration

There are four different ways to complete migration of compute, network, and storage resources:

- [Migration of virtual machines \(NOT in a virtual network\)](#)
- [Migration of virtual machines \(in a virtual network\)](#)
- [Migration of storage accounts](#)
- [Migration of unattached resources](#)

Migration of virtual machines (NOT in a virtual network)

In the Resource Manager deployment model, security is enforced for your applications by default. All VMs need to be in a virtual network in the Resource Manager model. The Azure platform restarts ([Stop](#) , [Deallocate](#) , and [Start](#)) the VMs as part of the migration. You have two options for the virtual networks that the Virtual Machines will be migrated to:

- You can request the platform to create a new virtual network and migrate the virtual machine into the new virtual network.
- You can migrate the virtual machine into an existing virtual network in Resource Manager.

NOTE

In this migration scope, both the management-plane operations and the data-plane operations may not be allowed for a period of time during the migration.

Migration of virtual machines (in a virtual network)

For most VM configurations, only the metadata is migrating between the Classic and Resource Manager deployment models. The underlying VMs are running on the same hardware, in the same network, and with the same storage. The management-plane operations may not be allowed for a certain period of time during the migration. However, the data plane continues to work. That is, your applications running on top of VMs (classic) do not incur downtime during the migration.

The following configurations are not currently supported. If support is added in the future, some VMs in this configuration might incur downtime (go through stop, deallocate, and restart VM operations).

- You have more than one availability set in a single cloud service.
- You have one or more availability sets and VMs that are not in an availability set in a single cloud service.

NOTE

In this migration scope, the management plane may not be allowed for a period of time during the migration. For certain configurations as described earlier, data-plane downtime occurs.

Migration of storage accounts

To allow seamless migration, you can deploy Resource Manager VMs in a classic storage account. With this capability, compute and network resources can and should be migrated independently of storage accounts. Once you migrate over your Virtual Machines and Virtual Network, you need to migrate over your storage accounts to complete the migration process.

If your storage account does not have any associated disks or Virtual Machines data and only has blobs, files, tables, and queues then the migration to Azure Resource Manager can be done as a standalone migration without dependencies.

NOTE

The Resource Manager deployment model doesn't have the concept of Classic images and disks. When the storage account is migrated, Classic images and disks are not visible in the Resource Manager stack but the backing VHDs remain in the storage account.

The following screenshots show how to upgrade a Classic storage account to an Azure Resource Manager storage account using Azure portal:

1. Sign in to the [Azure portal](#).

2. Navigate to your storage account.
3. In the **Settings** section, click **Migrate to ARM**.
4. Click on **Validate** to determine migration feasibility.
5. If validation passes, click on **Prepare** to create a migrated storage account.
6. Type **yes** to confirm migration and click **Commit** to finish the migration.

Migrate to ARM

testclassicaccount2 - Migrate to ARM
Storage account (classic)

Search (Ctrl+ /) <>

- Overview**
- Activity log**
- Access control (IAM)**
- Diagnose and solve problem...**
- Storage Explorer (preview)**
- Settings**
 - Access keys**
 - CORS**
 - Configuration**
 - Shared access signature**
 - Migrate to ARM**
- Properties**
- Locks**
- Blob service**
 - Blobs**

To benefit from new capabilities in Azure Resource Manager, you can migrate existing deployments from the Classic deployment model. extensions, incorporates role-based access management, and tagging. [Learn more](#)

Take the following steps to complete migration:

1. Validate if the resource is capable of migration **Validate**
2. Prepare
3. Commit or abort

Migrate to ARM

testclassicaccount2 - Migrate to ARM
Storage account (classic)

Search (Ctrl+ /) <>

- Overview**
- Activity log**
- Access control (IAM)**
- Diagnose and solve problem...**
- Storage Explorer (preview)**
- Settings**
 - Access keys**
 - CORS**
 - Configuration**
 - Shared access signature**
 - Migrate to ARM**
- Properties**
- Locks**
- Blob service**
 - Blobs**

Validation passed.

To benefit from new capabilities in Azure Resource Manager, you can migrate existing deployments from the Classic deployment model. extensions, incorporates role-based access management, and tagging. [Learn more](#)

Take the following steps to complete migration:

1. Validate if the resource is capable of migration **Validation passed.**
- 1 storage account will be migrated.
 - View details**
2. Prepare

Simulate the transformation of classic resources into Resource Manager resources.
If you see any issues with the results of 'Prepare', you will be able to abort migration in the next step.

Prepare
3. Commit or abort

Migration of unattached resources

Storage Accounts with no associated disks or Virtual Machines data may be migrated independently.

Network Security Groups, Route Tables & Reserved IPs that are not attached to any Virtual Machines and Virtual Networks can also be migrated independently.

Unsupported features and configurations

Some features and configurations are not currently supported; the following sections describe our recommendations around them.

Unsupported features

The following features are not currently supported. You can optionally remove these settings, migrate the VMs, and then re-enable the settings in the Resource Manager deployment model.

RESOURCE PROVIDER	FEATURE	RECOMMENDATION
Compute	Unassociated virtual machine disks.	The VHD blobs behind these disks will get migrated when the Storage Account is migrated
Compute	Virtual machine images.	The VHD blobs behind these disks will get migrated when the Storage Account is migrated
Network	Endpoint ACLs.	Remove Endpoint ACLs and retry migration.
Network	Application Gateway	Remove the Application Gateway before beginning migration and then recreate the Application Gateway once migration is complete.
Network	Virtual networks using VNet Peering.	Migrate Virtual Network to Resource Manager, then peer. Learn more about VNet Peering .

Unsupported configurations

The following configurations are not currently supported.

Service	Configuration	Recommendation
Resource Manager	Role-Based Access Control (RBAC) for classic resources	Because the URI of the resources is modified after migration, it is recommended that you plan the RBAC policy updates that need to happen after migration.
Compute	Multiple subnets associated with a VM	Update the subnet configuration to reference only one subnet. This may require you to remove a secondary NIC (that is referring to another subnet) from the VM and reattach it after migration has completed.
Compute	Virtual machines that belong to a virtual network but don't have an explicit subnet assigned	You can optionally delete the VM.
Compute	Virtual machines that have alerts, Autoscale policies	The migration goes through and these settings are dropped. It is highly recommended that you evaluate your environment before you do the migration. Alternatively, you can reconfigure the alert settings after migration is complete.
Compute	XML VM extensions (BGInfo 1.* , Visual Studio Debugger, Web Deploy, and Remote Debugging)	This is not supported. It is recommended that you remove these extensions from the virtual machine to continue migration or they will be dropped automatically during the migration process.
Compute	Boot diagnostics with Premium storage	Disable Boot Diagnostics feature for the VMs before continuing with migration. You can re-enable boot diagnostics in the Resource Manager stack after the migration is complete. Additionally, blobs that are being used for screenshot and serial logs should be deleted so you are no longer charged for those blobs.
Compute	Cloud services that contain web/worker roles	This is currently not supported.
Compute	Cloud services that contain more than one availability set or multiple availability sets.	This is currently not supported. Please move the Virtual Machines to the same availability set before migrating.

Service	Configuration	Recommendation
Compute	VM with Azure Security Center extension	Azure Security Center automatically installs extensions on your Virtual Machines to monitor their security and raise alerts. These extensions usually get installed automatically if the Azure Security Center policy is enabled on the subscription. To migrate the Virtual Machines, disable the security center policy on the subscription, which will remove the Security Center monitoring extension from the Virtual Machines.
Compute	VM with backup or snapshot extension	These extensions are installed on a Virtual Machine configured with the Azure Backup service. While the migration of these VMs is not supported, follow the guidance here to keep backups that were taken prior to migration.
Compute	VM with Azure Site Recovery extension	These extensions are installed on a Virtual Machine configured with the Azure Site Recovery service. While the migration of storage used with Site Recovery will work, current replication will be impacted. You need to disable and enable VM replication after storage migration.
Network	Virtual networks that contain virtual machines and web/worker roles	This is currently not supported. Please move the Web/Worker roles to their own Virtual Network before migrating. Once the classic Virtual Network is migrated, the migrated Azure Resource Manager Virtual Network can be peered with the classic Virtual Network to achieve similar configuration as before.
Network	Classic Express Route circuits	This is currently not supported. These circuits need to be migrated to Azure Resource Manager before beginning IaaS migration. To learn more, see Moving ExpressRoute circuits from the classic to the Resource Manager deployment model .
Azure App Service	Virtual networks that contain App Service environments	This is currently not supported.
Azure HDInsight	Virtual networks that contain HDInsight services	This is currently not supported.
Microsoft Dynamics Lifecycle Services	Virtual networks that contain virtual machines that are managed by Dynamics Lifecycle Services	This is currently not supported.

Service	Configuration	Recommendation
Azure AD Domain Services	Virtual networks that contain Azure AD Domain services	This is currently not supported.
Azure API Management	Virtual networks that contain Azure API Management deployments	This is currently not supported. To migrate the IaaS VNET, change the VNET of the API Management deployment, which is a no downtime operation.

Next steps

- [Technical deep dive on platform-supported migration from classic to Azure Resource Manager](#)
- [Planning for migration of IaaS resources from classic to Azure Resource Manager](#)
- [Use PowerShell to migrate IaaS resources from classic to Azure Resource Manager](#)
- [Use CLI to migrate IaaS resources from classic to Azure Resource Manager](#)
- [Community tools for assisting with migration of IaaS resources from classic to Azure Resource Manager](#)
- [Review most common migration errors](#)
- [Review the most frequently asked questions about migrating IaaS resources from classic to Azure Resource Manager](#)

Technical deep dive on platform-supported migration from classic to Azure Resource Manager

2/28/2020 • 13 minutes to read • [Edit Online](#)

IMPORTANT

Today, about 90% of IaaS VMs are using [Azure Resource Manager](#). As of February 28, 2020, classic VMs have been deprecated and will be fully retired on March 1, 2023. [Learn more](#) about this deprecation and [how it affects you](#).

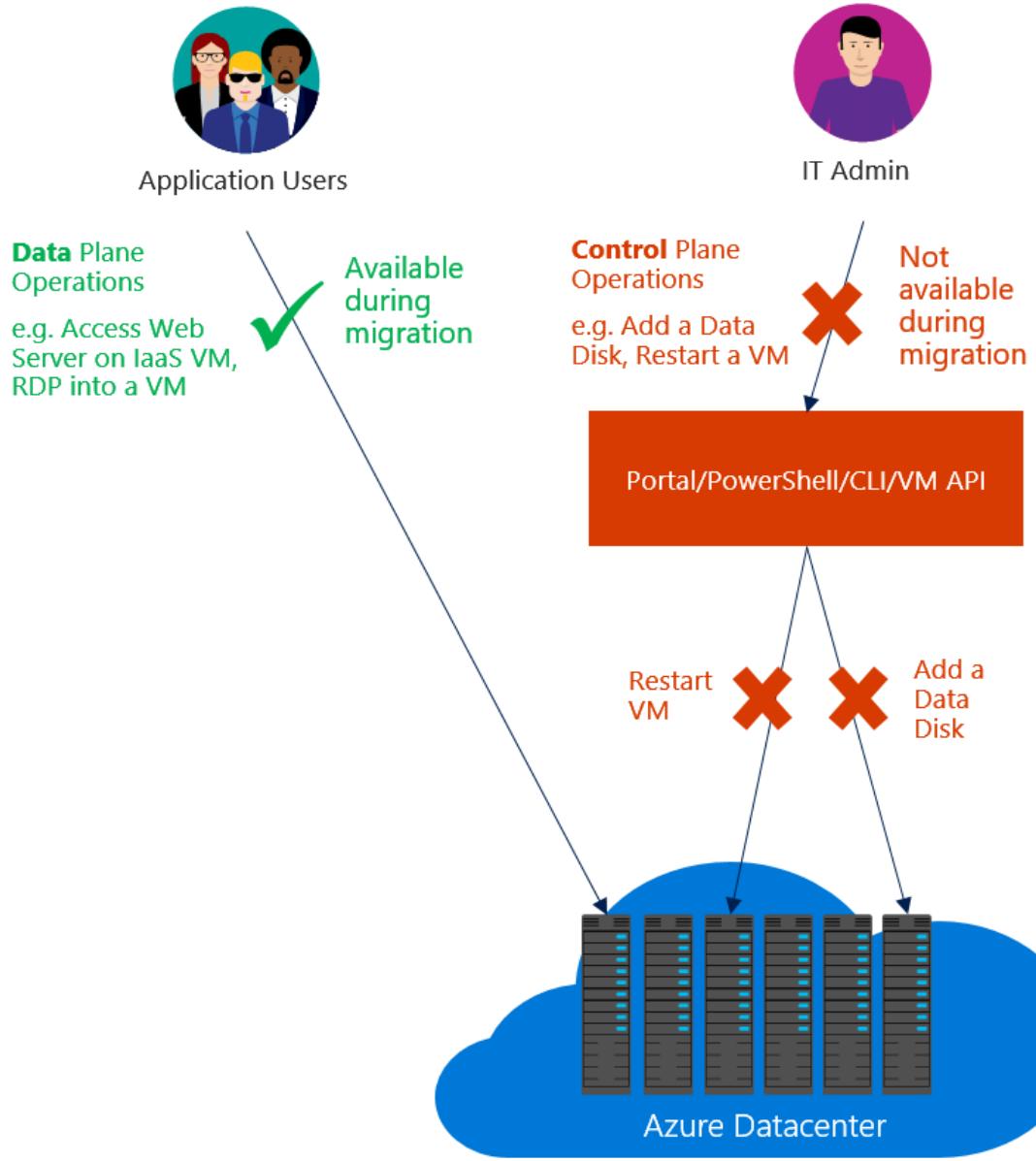
Let's take a deep-dive on migrating from the Azure classic deployment model to the Azure Resource Manager deployment model. We look at resources at a resource and feature level to help you understand how the Azure platform migrates resources between the two deployment models. For more information, please read the service announcement article: [Platform-supported migration of IaaS resources from classic to Azure Resource Manager](#).

Migrate IaaS resources from the classic deployment model to Azure Resource Manager

First, it's important to understand the difference between data-plane and management-plane operations on the infrastructure as a service (IaaS) resources.

- *Management/control plane* describes the calls that come into the management/control plane or the API for modifying resources. For example, operations like creating a VM, restarting a VM, and updating a virtual network with a new subnet manage the running resources. They don't directly affect connecting to the VMs.
- *Data plane* (application) describes the runtime of the application itself, and involves interaction with instances that don't go through the Azure API. For example, accessing your website, or pulling data from a running SQL Server instance or a MongoDB server, are data plane or application interactions. Other examples include copying a blob from a storage account, and accessing a public IP address to use Remote Desktop Protocol (RDP) or Secure Shell (SSH) into the virtual machine. These operations keep the application running across compute, networking, and storage.

The data plane is the same between the classic deployment model and Resource Manager stacks. The difference is that during the migration process, Microsoft translates the representation of the resources from the classic deployment model to that in the Resource Manager stack. As a result, you need to use new tools, APIs, and SDKs to manage your resources in the Resource Manager stack.



NOTE

In some migration scenarios, the Azure platform stops, deallocates, and restarts your virtual machines. This causes a brief data-plane downtime.

The migration experience

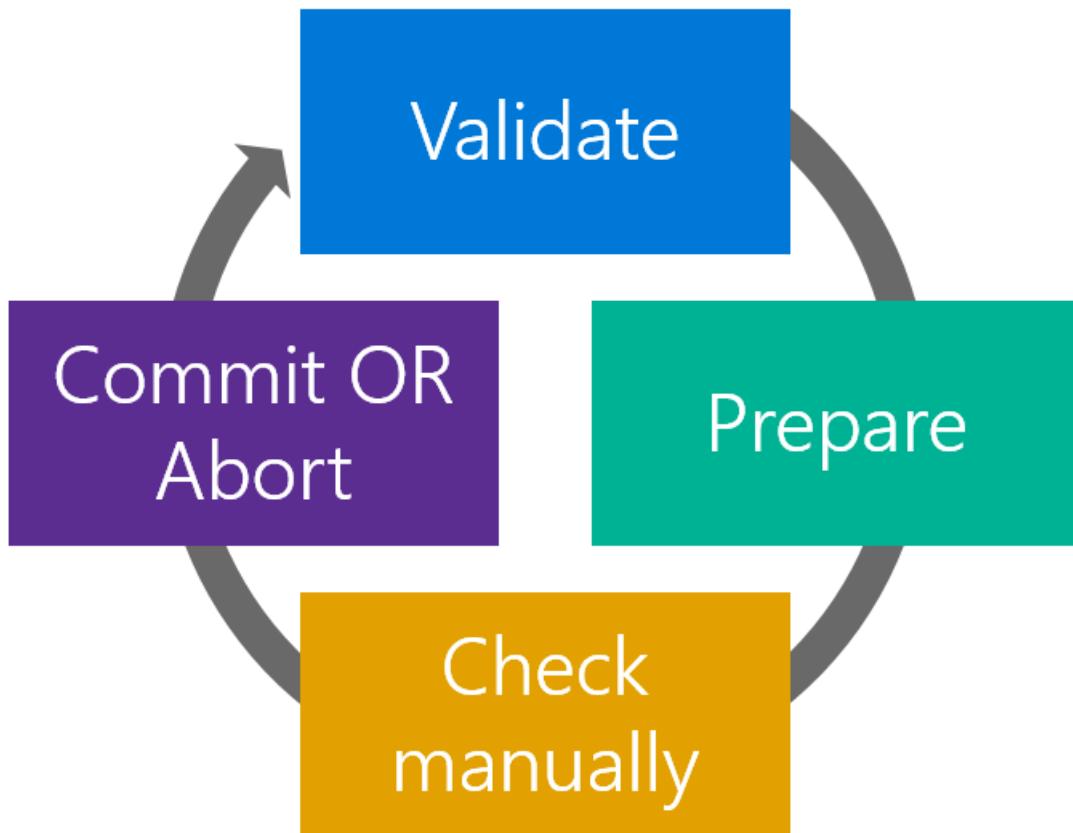
Before you start the migration:

- Ensure that the resources that you want to migrate don't use any unsupported features or configurations. Usually the platform detects these issues and generates an error.
- If you have VMs that are not in a virtual network, they are stopped and deallocated as part of the prepare operation. If you don't want to lose the public IP address, consider reserving the IP address before triggering the prepare operation. If the VMs are in a virtual network, they are not stopped and deallocated.
- Plan your migration during non-business hours to accommodate for any unexpected failures that might happen during migration.
- Download the current configuration of your VMs by using PowerShell, command-line interface (CLI) commands, or REST APIs to make it easier for validation after the prepare step is complete.
- Update your automation and operationalization scripts to handle the Resource Manager deployment model,

before you start the migration. You can optionally do GET operations when the resources are in the prepared state.

- Evaluate the Role-Based Access Control (RBAC) policies that are configured on the IaaS resources in the classic deployment model, and plan for after the migration is complete.

The migration workflow is as follows:



NOTE

The operations described in the following sections are all idempotent. If you have a problem other than an unsupported feature or a configuration error, retry the prepare, abort, or commit operation. Azure tries the action again.

Validate

The validate operation is the first step in the migration process. The goal of this step is to analyze the state of the resources you want to migrate in the classic deployment model. The operation evaluates whether the resources are capable of migration (success or failure).

You select the virtual network or a cloud service (if it's not in a virtual network) that you want to validate for migration. If the resource is not capable of migration, Azure lists the reasons why.

Checks not done in the validate operation

The validate operation only analyzes the state of the resources in the classic deployment model. It can check for all failures and unsupported scenarios due to various configurations in the classic deployment model. It is not possible to check for all issues that the Azure Resource Manager stack might impose on the resources during migration. These issues are only checked when the resources undergo transformation in the next step of migration (the prepare operation). The following table lists all the issues not checked in the validate operation:

NETWORKING CHECKS NOT IN THE VALIDATE OPERATION

A virtual network having both ER and VPN gateways.

A virtual network gateway connection in a disconnected state.

All ER circuits are pre-migrated to Azure Resource Manager stack.

Azure Resource Manager quota checks for networking resources. For example: static public IP, dynamic public IPs, load balancer, network security groups, route tables, and network interfaces.

All load balancer rules are valid across deployment and the virtual network.

Conflicting private IPs between stop-deallocated VMs in the same virtual network.

Prepare

The prepare operation is the second step in the migration process. The goal of this step is to simulate the transformation of the IaaS resources from the classic deployment model to Resource Manager resources. Further, the prepare operation presents this side-by-side for you to visualize.

NOTE

Your resources in the classic deployment model are not modified during this step. It's a safe step to run if you're trying out migration.

You select the virtual network or the cloud service (if it's not a virtual network) that you want to prepare for migration.

- If the resource is not capable of migration, Azure stops the migration process and lists the reason why the prepare operation failed.
- If the resource is capable of migration, Azure locks down the management-plane operations for the resources under migration. For example, you are not able to add a data disk to a VM under migration.

Azure then starts the migration of metadata from the classic deployment model to Resource Manager for the migrating resources.

After the prepare operation is complete, you have the option of visualizing the resources in both the classic deployment model and Resource Manager. For every cloud service in the classic deployment model, the Azure platform creates a resource group name that has the pattern `cloud-service-name>-Migrated`.

NOTE

It is not possible to select the name of a resource group created for migrated resources (that is, "-Migrated"). After migration is complete, however, you can use the move feature of Azure Resource Manager to move resources to any resource group you want. For more information, see [Move resources to new resource group or subscription](#).

The following two screenshots show the result after a successful prepare operation. The first one shows a resource group that contains the original cloud service. The second one shows the new "-Migrated" resource group that contains the equivalent Azure Resource Manager resources.

portalmigrate
Resource group

Search (Ctrl+ /)

Overview

Activity log

Access control (IAM)

Tags

SETTINGS

Quickstart

Resource costs

Deployments

Properties

Locks

Automation script

Essentials

Subscription name (change) Subscription ID

Deployments Location
No deployments East US

Filter by name...

2 items

NAME	TYPE	LOCATION
portalmigrate	Cloud service (class...)	East US
portalmigrate	Virtual machine (cl...)	East US

portalmigrate-Migrated
Resource group

Search (Ctrl+ /)

Overview

Activity log

Access control (IAM)

Tags

SETTINGS

Quickstart

Resource costs

Deployments

Properties

Locks

Automation script

Essentials

Subscription name (change) Subscription ID

Deployments Location
2 Succeeded East US

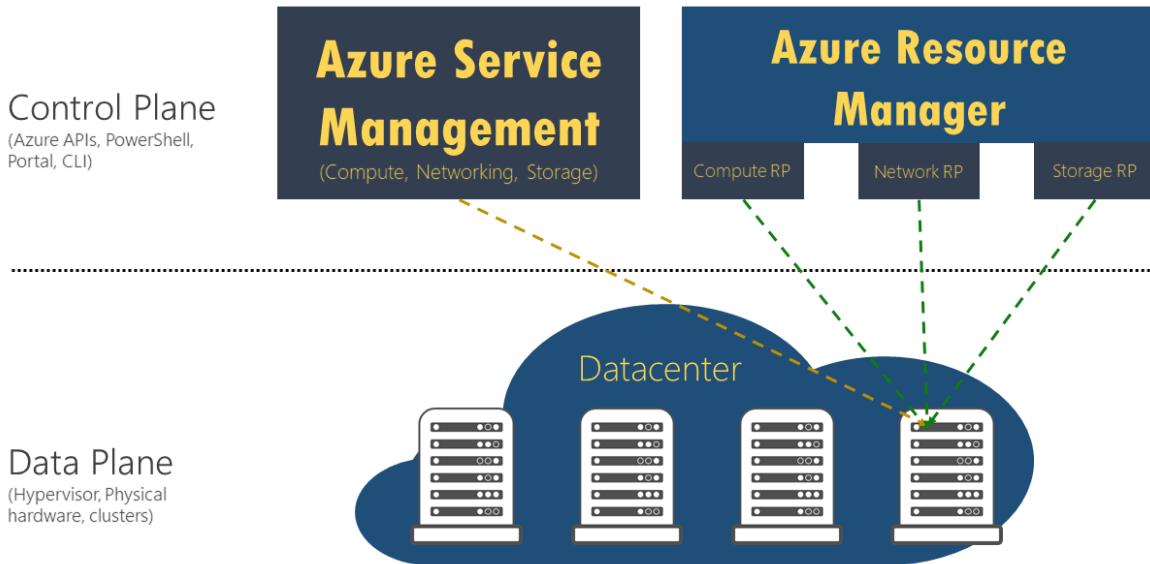
Filter by name...

5 items

NAME	TYPE	LOCATION
portalmigrate	Virtual machine	East US
portalmigrate-PrimaryNic	Network interface	East US
portalmigrate-PrimaryVirtualIP	Public IP address	East US
portalmigrate-PublicLoadBalancer	Load balancer	East US
portalmigrate-VirtualNetwork	Virtual network	East US

Here is a behind-the-scenes look at your resources after the completion of the prepare phase. Note that the resource in the data plane is the same. It's represented in both the management plane (classic deployment model) and the control plane (Resource Manager).

Prepare



NOTE

VMs that are not in a virtual network in the classic deployment model are stopped and deallocated in this phase of migration.

Check (manual or scripted)

In the check step, you have the option to use the configuration that you downloaded earlier to validate that the migration looks correct. Alternatively, you can sign in to the portal, and spot check the properties and resources to validate that metadata migration looks good.

If you are migrating a virtual network, most configuration of virtual machines is not restarted. For applications on those VMs, you can validate that the application is still running.

You can test your monitoring and operational scripts to see if the VMs are working as expected, and if your updated scripts work correctly. Only GET operations are supported when the resources are in the prepared state.

There is no set window of time before which you need to commit the migration. You can take as much time as you want in this state. However, the management plane is locked for these resources until you either abort or commit.

If you see any issues, you can always abort the migration and go back to the classic deployment model. After you go back, Azure opens the management-plane operations on the resources, so that you can resume normal operations on those VMs in the classic deployment model.

Abort

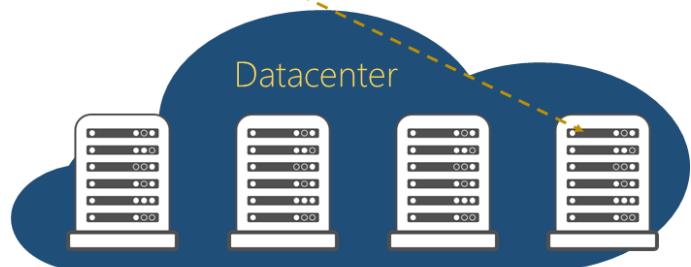
This is an optional step if you want to revert your changes to the classic deployment model and stop the migration. This operation deletes the Resource Manager metadata (created in the prepare step) for your resources.

Abort

Control Plane
(Azure APIs, PowerShell, Portal, CLI)



Data Plane
(Hypervisor, Physical hardware, clusters)



NOTE

This operation can't be done after you have triggered the commit operation.

Commit

After you finish the validation, you can commit the migration. Resources do not appear anymore in the classic deployment model, and are available only in the Resource Manager deployment model. The migrated resources can be managed only in the new portal.

NOTE

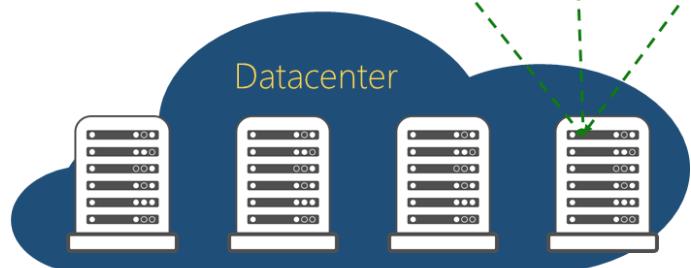
This is an idempotent operation. If it fails, retry the operation. If it continues to fail, create a support ticket or create a forum on [Microsoft Q&A](#)

Commit

Control Plane
(Azure APIs, PowerShell, Portal, CLI)



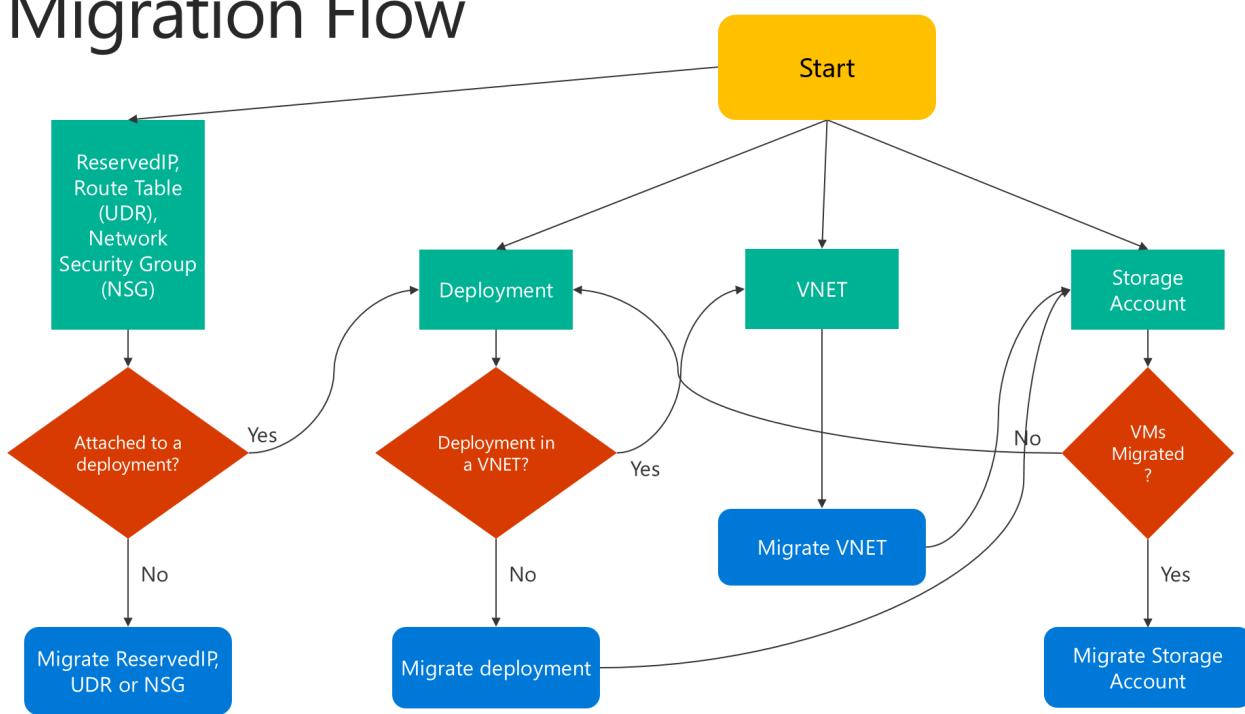
Data Plane
(Hypervisor, Physical hardware, clusters)



Migration flowchart

Here is a flowchart that shows how to proceed with migration:

Migration Flow



Translation of the classic deployment model to Resource Manager resources

You can find the classic deployment model and Resource Manager representations of the resources in the following table. Other features and resources are not currently supported.

CLASSIC REPRESENTATION	RESOURCE MANAGER REPRESENTATION	NOTES
Cloud service name	DNS name	During migration, a new resource group is created for every cloud service with the naming pattern <code><cloudservicename>-migrated</code> . This resource group contains all your resources. The cloud service name becomes a DNS name that is associated with the public IP address.
Virtual machine	Virtual machine	VM-specific properties are migrated unchanged. Certain osProfile information, like computer name, is not stored in the classic deployment model, and remains empty after migration.

CLASSIC REPRESENTATION	RESOURCE MANAGER REPRESENTATION	NOTES
Disk resources attached to VM	Implicit disks attached to VM	Disks are not modeled as top-level resources in the Resource Manager deployment model. They are migrated as implicit disks under the VM. Only disks that are attached to a VM are currently supported. Resource Manager VMs can now use storage accounts in the classic deployment model, which allows the disks to be easily migrated without any updates.
VM extensions	VM extensions	All the resource extensions, except XML extensions, are migrated from the classic deployment model.
Virtual machine certificates	Certificates in Azure Key Vault	If a cloud service contains service certificates, the migration creates a new Azure key vault per cloud service, and moves the certificates into the key vault. The VMs are updated to reference the certificates from the key vault. Do not delete the key vault. This can cause the VM to go into a failed state.
WinRM configuration	WinRM configuration under osProfile	Windows Remote Management configuration is moved unchanged, as part of the migration.
Availability-set property	Availability-set resource	Availability-set specification is a property on the VM in the classic deployment model. Availability sets become a top-level resource as part of the migration. The following configurations are not supported: multiple availability sets per cloud service, or one or more availability sets along with VMs that are not in any availability set in a cloud service.
Network configuration on a VM	Primary network interface	Network configuration on a VM is represented as the primary network interface resource after migration. For VMs that are not in a virtual network, the internal IP address changes during migration.
Multiple network interfaces on a VM	Network interfaces	If a VM has multiple network interfaces associated with it, each network interface becomes a top-level resource as part of the migration, along with all the properties.

CLASSIC REPRESENTATION	RESOURCE MANAGER REPRESENTATION	NOTES
Load-balanced endpoint set	Load balancer	In the classic deployment model, the platform assigned an implicit load balancer for every cloud service. During migration, a new load-balancer resource is created, and the load-balancing endpoint set becomes load-balancer rules.
Inbound NAT rules	Inbound NAT rules	Input endpoints defined on the VM are converted to inbound network address translation rules under the load balancer during the migration.
VIP address	Public IP address with DNS name	The virtual IP address becomes a public IP address, and is associated with the load balancer. A virtual IP can only be migrated if there is an input endpoint assigned to it.
Virtual network	Virtual network	The virtual network is migrated, with all its properties, to the Resource Manager deployment model. A new resource group is created with the name <code>-migrated</code> .
Reserved IPs	Public IP address with static allocation method	Reserved IPs associated with the load balancer are migrated, along with the migration of the cloud service or the virtual machine. Unassociated reserved IP migration is not currently supported.
Public IP address per VM	Public IP address with dynamic allocation method	The public IP address associated with the VM is converted as a public IP address resource, with the allocation method set to static.
NSGs	NSGs	Network security groups associated with a subnet are cloned as part of the migration to the Resource Manager deployment model. The NSG in the classic deployment model is not removed during the migration. However, the management-plane operations for the NSG are blocked when the migration is in progress.
DNS servers	DNS servers	DNS servers associated with a virtual network or the VM are migrated as part of the corresponding resource migration, along with all the properties.

CLASSIC REPRESENTATION	RESOURCE MANAGER REPRESENTATION	NOTES
UDRs	UDRs	User-defined routes associated with a subnet are cloned as part of the migration to the Resource Manager deployment model. The UDR in the classic deployment model is not removed during the migration. The management-plane operations for the UDR are blocked when the migration is in progress.
IP forwarding property on a VM's network configuration	IP forwarding property on the NIC	The IP forwarding property on a VM is converted to a property on the network interface during the migration.
Load balancer with multiple IPs	Load balancer with multiple public IP resources	Every public IP associated with the load balancer is converted to a public IP resource, and associated with the load balancer after migration.
Internal DNS names on the VM	Internal DNS names on the NIC	During migration, the internal DNS suffixes for the VMs are migrated to a read-only property named "InternalDomainNameSuffix" on the NIC. The suffix remains unchanged after migration, and VM resolution should continue to work as previously.
Virtual network gateway	Virtual network gateway	Virtual network gateway properties are migrated unchanged. The VIP associated with the gateway does not change either.
Local network site	Local network gateway	Local network site properties are migrated unchanged to a new resource called a local network gateway. This represents on-premises address prefixes and the remote gateway IP.
Connections references	Connection	Connectivity references between the gateway and the local network site in network configuration is represented by a new resource called Connection. All properties of connectivity reference in network configuration files are copied unchanged to the Connection resource. Connectivity between virtual networks in the classic deployment model is achieved by creating two IPsec tunnels to local network sites representing the virtual networks. This is transformed to the virtual-network-to-virtual-network connection type in the Resource Manager model, without requiring local network gateways.

Changes to your automation and tooling after migration

As part of migrating your resources from the classic deployment model to the Resource Manager deployment

model, you must update your existing automation or tooling to ensure that it continues to work after the migration.

Next steps

- [Overview of platform-supported migration of IaaS resources from classic to Azure Resource Manager](#)
- [Planning for migration of IaaS resources from classic to Azure Resource Manager](#)
- [Use PowerShell to migrate IaaS resources from classic to Azure Resource Manager](#)
- [Use CLI to migrate IaaS resources from classic to Azure Resource Manager](#)
- [Community tools for assisting with migration of IaaS resources from classic to Azure Resource Manager](#)
- [Review most common migration errors](#)
- [Review the most frequently asked questions about migrating IaaS resources from classic to Azure Resource Manager](#)

IMPORTANT

Today, about 90% of IaaS VMs are using [Azure Resource Manager](#). As of February 28, 2020, classic VMs have been deprecated and will be fully retired on March 1, 2023. [Learn more](#) about this deprecation and [how it affects you](#).

Planning for migration of IaaS resources from classic to Azure Resource Manager

While Azure Resource Manager offers a lot of amazing features, it is critical to plan out your migration journey to make sure things go smoothly. Spending time on planning will ensure that you do not encounter issues while executing migration activities.

NOTE

The following guidance was heavily contributed to by the Azure Customer Advisory team and Cloud Solution architects working with customers on migrating large environments. As such this document will continue to get updated as new patterns of success emerge, so check back from time to time to see if there are any new recommendations.

There are four general phases of the migration journey:



Plan

Technical considerations and tradeoffs

Depending on your technical requirements size, geographies and operational practices, you might want to consider:

1. Why is Azure Resource Manager desired for your organization? What are the business reasons for a migration?
2. What are the technical reasons for Azure Resource Manager? What (if any) additional Azure services would you like to leverage?
3. Which application (or sets of virtual machines) is included in the migration?
4. Which scenarios are supported with the migration API? Review the [unsupported features and configurations](#).
5. Will your operational teams now support applications/VMs in both Classic and Azure Resource Manager?
6. How (if at all) does Azure Resource Manager change your VM deployment, management, monitoring, and reporting processes? Do your deployment scripts need to be updated?
7. What is the communications plan to alert stakeholders (end users, application owners, and infrastructure owners)?
8. Depending on the complexity of the environment, should there be a maintenance period where the application is unavailable to end users and to application owners? If so, for how long?

9. What is the training plan to ensure stakeholders are knowledgeable and proficient in Azure Resource Manager?
10. What is the program management or project management plan for the migration?
11. What are the timelines for the Azure Resource Manager migration and other related technology road maps? Are they optimally aligned?

Patterns of success

Successful customers have detailed plans where the preceding questions are discussed, documented and governed. Ensure the migration plans are broadly communicated to sponsors and stakeholders. Equip yourself with knowledge about your migration options; reading through this migration document set below is highly recommended.

- [Overview of platform-supported migration of IaaS resources from classic to Azure Resource Manager](#)
- [Technical deep dive on platform-supported migration from classic to Azure Resource Manager](#)
- [Planning for migration of IaaS resources from classic to Azure Resource Manager](#)
- [Use PowerShell to migrate IaaS resources from classic to Azure Resource Manager](#)
- [Use CLI to migrate IaaS resources from classic to Azure Resource Manager](#)
- [Community tools for assisting with migration of IaaS resources from classic to Azure Resource Manager](#)
- [Review most common migration errors](#)
- [Review the most frequently asked questions about migrating IaaS resources from classic to Azure Resource Manager](#)

Pitfalls to avoid

- Failure to plan. The technology steps of this migration are proven and the outcome is predictable.
- Assumption that the platform supported migration API will account for all scenarios. Read the [unsupported features and configurations](#) to understand what scenarios are supported.
- Not planning potential application outage for end users. Plan enough buffer to adequately warn end users of potentially unavailable application time.

Lab Test

Replicate your environment and do a test migration

NOTE

Exact replication of your existing environment is executed by using a community-contributed tool which is not officially supported by Microsoft Support. Therefore, it is an **optional** step but it is the best way to find out issues without touching your production environments. If using a community-contributed tool is not an option, then read about the Validate/Prepare/Abort Dry Run recommendation below.

Conducting a lab test of your exact scenario (compute, networking, and storage) is the best way to ensure a smooth migration. This will help ensure:

- A wholly separate lab or an existing non-production environment to test. We recommend a wholly separate lab that can be migrated repeatedly and can be destructively modified. Scripts to collect/hydrate metadata from the real subscriptions are listed below.
- It's a good idea to create the lab in a separate subscription. The reason is that the lab will be torn down repeatedly, and having a separate, isolated subscription will reduce the chance that something real will get accidentally deleted.

This can be accomplished by using the AsmMetadataParser tool. [Read more about this tool here](#)

Patterns of success

The following were issues discovered in many of the larger migrations. This is not an exhaustive list and you should refer to the [unsupported features and configurations](#) for more detail. You may or may not encounter these technical issues but if you do solving these before attempting migration will ensure a smoother experience.

- **Do a Validate/Prepare/Abort Dry Run** - This is perhaps the most important step to ensure Classic to Azure Resource Manager migration success. The migration API has three main steps: Validate, Prepare and Commit. Validate will read the state of your classic environment and return a result of all issues. However, because some issues might exist in the Azure Resource Manager stack, Validate will not catch everything. The next step in migration process, Prepare will help expose those issues. Prepare will move the metadata from Classic to Azure Resource Manager, but will not commit the move, and will not remove or change anything on the Classic side. The dry run involves preparing the migration, then aborting (**not committing**) the migration prepare. The goal of validate/prepare/abort dry run is to see all of the metadata in the Azure Resource Manager stack, examine it (*programmatically or in Portal*), and verify that everything migrates correctly, and work through technical issues. It will also give you a sense of migration duration so you can plan for downtime accordingly. A validate/prepare/abort does not cause any user downtime; therefore, it is non-disruptive to application usage.
 - The items below will need to be solved before the dry run, but a dry run test will also safely flush out these preparation steps if they are missed. During enterprise migration, we've found the dry run to be a safe and invaluable way to ensure migration readiness.
 - When prepare is running, the control plane (Azure management operations) will be locked for the whole virtual network, so no changes can be made to VM metadata during validate/prepare/abort. But otherwise any application function (RD, VM usage, etc.) will be unaffected. Users of the VMs will not know that the dry run is being executed.
- **Express Route Circuits and VPN**. Currently Express Route Gateways with authorization links cannot be migrated without downtime. For the workaround, see [Migrate ExpressRoute circuits and associated virtual networks from the classic to the Resource Manager deployment model](#).
- **VM Extensions** - Virtual Machine extensions are potentially one of the biggest roadblocks to migrating running VMs. Remediation of VM Extensions could take upwards of 1-2 days, so plan accordingly. A working Azure agent is needed to report back VM Extension status of running VMs. If the status comes back as bad for a running VM, this will halt migration. The agent itself does not need to be in working order to enable migration, but if extensions exist on the VM, then both a working agent AND outbound internet connectivity (with DNS) will be needed for migration to move forward.
 - If connectivity to a DNS server is lost during migration, all VM Extensions except BGInfo v1.* need to first be removed from every VM before migration prepare, and subsequently re-added back to the VM after Azure Resource Manager migration. **This is only for VMs that are running.** If the VMs are stopped deallocated, VM Extensions do not need to be removed. **Note:** Many extensions like Azure diagnostics and security center monitoring will reinstall themselves after migration, so removing them is not a problem.
 - In addition, make sure Network Security Groups are not restricting outbound internet access. This can happen with some Network Security Groups configurations. Outbound internet access (and DNS) is needed for VM Extensions to be migrated to Azure Resource Manager.
 - There are two versions of the BGInfo extension: v1 and v2. If the VM was created using the Azure portal or PowerShell, the VM will likely have the v1 extension on it. This extension does not need to be removed and will be skipped (not migrated) by the migration API. However, if the Classic VM was created with the new Azure portal, it will likely have the JSON-based v2 version of BGInfo, which can be migrated to Azure Resource Manager provided the agent is working and has outbound internet access (and DNS).
 - **Remediation Option 1.** If you know your VMs will not have outbound internet access, a working DNS service, and working Azure agents on the VMs, then uninstall all VM extensions as part of the

migration before Prepare, then reinstall the VM Extensions after migration.

- **Remediation Option 2.** If VM extensions are too big of a hurdle, another option is to shutdown/deallocate all VMs before migration. Migrate the deallocated VMs, then restart them on the Azure Resource Manager side. The benefit here is that VM extensions will migrate. The downside is that all public facing Virtual IPs will be lost (this may be a non-starter), and obviously the VMs will shut down causing a much greater impact on working applications.

NOTE

If an Azure Security Center policy is configured against the running VMs being migrated, the security policy needs to be stopped before removing extensions, otherwise the security monitoring extension will be reinstalled automatically on the VM after removing it.

- **Availability Sets** - For a virtual network (vNet) to be migrated to Azure Resource Manager, the Classic deployment (i.e. cloud service) contained VMs must all be in one availability set, or the VMs must all not be in any availability set. Having more than one availability set in the cloud service is not compatible with Azure Resource Manager and will halt migration. Additionally, there cannot be some VMs in an availability set, and some VMs not in an availability set. To resolve this, you will need to remediate or reshuffle your cloud service. Plan accordingly as this might be time consuming.
- **Web/Worker Role Deployments** - Cloud Services containing web and worker roles cannot migrate to Azure Resource Manager. The web/worker roles must first be removed from the virtual network before migration can start. A typical solution is to just move web/worker role instances to a separate Classic virtual network that is also linked to an ExpressRoute circuit, or to migrate the code to newer PaaS App Services (this discussion is beyond the scope of this document). In the former redeploy case, create a new Classic virtual network, move/redeploy the web/worker roles to that new virtual network, then delete the deployments from the virtual network being moved. No code changes required. The new [Virtual Network Peering](#) capability can be used to peer together the classic virtual network containing the web/worker roles and other virtual networks in the same Azure region such as the virtual network being migrated (**after virtual network migration is completed as peered virtual networks cannot be migrated**), hence providing the same capabilities with no performance loss and no latency/bandwidth penalties. Given the addition of [Virtual Network Peering](#), web/worker role deployments can now easily be mitigated and not block the migration to Azure Resource Manager.
- **Azure Resource Manager Quotas** - Azure regions have separate quotas/limits for both Classic and Azure Resource Manager. Even though in a migration scenario new hardware isn't being consumed (*we're swapping existing VMs from Classic to Azure Resource Manager*), Azure Resource Manager quotas still need to be in place with enough capacity before migration can start. Listed below are the major limits we've seen cause problems. Open a quota support ticket to raise the limits.

NOTE

These limits need to be raised in the same region as your current environment to be migrated.

- Network Interfaces
- Load Balancers
- Public IPs
- Static Public IPs
- Cores

- Network Security Groups
- Route Tables

You can check your current Azure Resource Manager quotas using the following commands with the latest version of Azure CLI.

Compute (Cores, Availability Sets)

```
az vm list-usage -l <azure-region> -o jsonc
```

Network (Virtual Networks, Static Public IPs, Public IPs, Network Security Groups, Network Interfaces, Load Balancers, Route Tables)

```
az network list-usages -l <azure-region> -o jsonc
```

Storage (Storage Account)

```
az storage account show-usage
```

- **Azure Resource Manager API throttling limits** - If you have a large enough environment (eg. > 400 VMs in a VNET), you might hit the default API throttling limits for writes (currently **1200 writes/hour**) in Azure Resource Manager. Before starting migration, you should raise a support ticket to increase this limit for your subscription.
- **Provisioning Timed Out VM Status** - If any VM has the status of **provisioning timed out**, this needs to be resolved pre-migration. The only way to do this is with downtime by deprovisioning/reprovisioning the VM (delete it, keep the disk, and recreate the VM).
- **RoleStateUnknown VM Status** - If migration halts due to a **role state unknown** error message, inspect the VM using the portal and ensure it is running. This error will typically go away on its own (no remediation required) after a few minutes and is often a transient type often seen during a Virtual Machine **start, stop, restart** operations. **Recommended practice:** re-try migration again after a few minutes.
- **Fabric Cluster does not exist** - In some cases, certain VMs cannot be migrated for various odd reasons. One of these known cases is if the VM was recently created (within the last week or so) and happened to land an Azure cluster that is not yet equipped for Azure Resource Manager workloads. You will get an error that says **fabric cluster does not exist** and the VM cannot be migrated. Waiting a couple of days will usually resolve this particular problem as the cluster will soon get Azure Resource Manager enabled. However, one immediate workaround is to `stop-deallocate` the VM, then continue forward with migration, and start the VM back up in Azure Resource Manager after migrating.

Pitfalls to avoid

- Do not take shortcuts and omit the validate/prepare/abort dry run migrations.
- Most, if not all, of your potential issues will surface during the validate/prepare/abort steps.

Migration

Technical considerations and tradeoffs

Now you are ready because you have worked through the known issues with your environment.

For the real migrations, you might want to consider:

1. Plan and schedule the virtual network (smallest unit of migration) with increasing priority. Do the simple

- virtual networks first, and progress with the more complicated virtual networks.
- 2. Most customers will have non-production and production environments. Schedule production last.
- 3. **(OPTIONAL)** Schedule a maintenance downtime with plenty of buffer in case unexpected issues arise.
- 4. Communicate with and align with your support teams in case issues arise.

Patterns of success

The technical guidance from the Lab Test section above should be considered and mitigated prior to a real migration. With adequate testing, the migration is actually a non-event. For production environments, it might be helpful to have additional support, such as a trusted Microsoft partner or Microsoft Premier services.

Pitfalls to avoid

Not fully testing may cause issues and delay in the migration.

Beyond Migration

Technical considerations and tradeoffs

Now that you are in Azure Resource Manager, maximize the platform. Read the [overview of Azure Resource Manager](#) to find out about additional benefits.

Things to consider:

- Bundling the migration with other activities. Most customers opt for an application maintenance window. If so, you might want to use this downtime to enable other Azure Resource Manager capabilities like encryption and migration to Managed Disks.
- Revisit the technical and business reasons for Azure Resource Manager; enable the additional services available only on Azure Resource Manager that apply to your environment.
- Modernize your environment with PaaS services.

Patterns of success

Be purposeful on what services you now want to enable in Azure Resource Manager. Many customers find the below compelling for their Azure environments:

- [Role Based Access Control](#).
- [Azure Resource Manager templates for easier and more controlled deployment](#).
- [Tags](#).
- [Activity Control](#)
- [Azure Policies](#)

Pitfalls to avoid

Remember why you started this Classic to Azure Resource Manager migration journey. What were the original business reasons? Did you achieve the business reason?

Next steps

- [Overview of platform-supported migration of IaaS resources from classic to Azure Resource Manager](#)
- [Technical deep dive on platform-supported migration from classic to Azure Resource Manager](#)
- [Planning for migration of IaaS resources from classic to Azure Resource Manager](#)
- [Use PowerShell to migrate IaaS resources from classic to Azure Resource Manager](#)
- [Community tools for assisting with migration of IaaS resources from classic to Azure Resource Manager](#)
- [Review most common migration errors](#)
- [Review the most frequently asked questions about migrating IaaS resources from classic to Azure Resource Manager](#)

Migrate IaaS resources from classic to Azure Resource Manager by using Azure CLI

2/28/2020 • 6 minutes to read • [Edit Online](#)

IMPORTANT

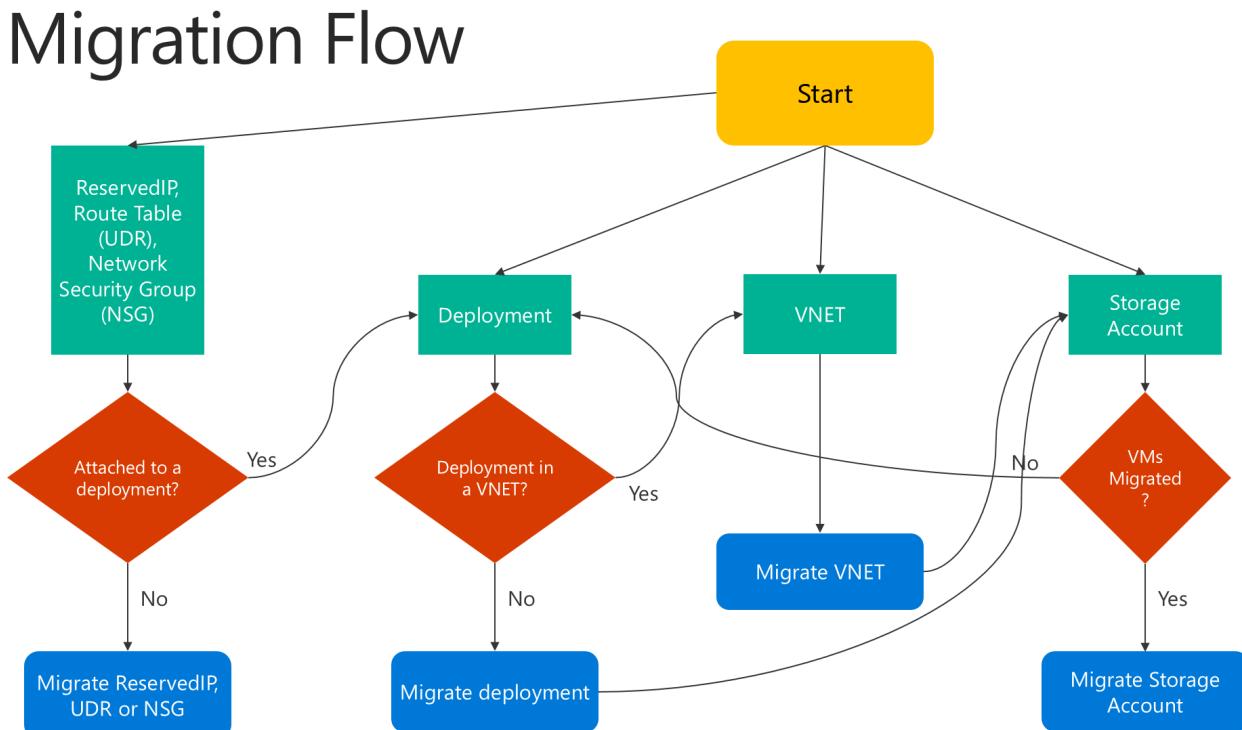
Today, about 90% of IaaS VMs are using [Azure Resource Manager](#). As of February 28, 2020, classic VMs have been deprecated and will be fully retired on March 1, 2023. [Learn more](#) about this deprecation and [how it affects you](#).

These steps show you how to use Azure command-line interface (CLI) commands to migrate infrastructure as a service (IaaS) resources from the classic deployment model to the Azure Resource Manager deployment model. The article requires the [Azure classic CLI](#). Since Azure CLI is only applicable for Azure Resource Manager resources, it cannot be used for this migration.

NOTE

All the operations described here are idempotent. If you have a problem other than an unsupported feature or a configuration error, we recommend that you retry the prepare, abort, or commit operation. The platform will then try the action again.

Here is a flowchart to identify the order in which steps need to be executed during a migration process



Step 1: Prepare for migration

Here are a few best practices that we recommend as you evaluate migrating IaaS resources from classic to Resource Manager:

- Read through the [list of unsupported configurations or features](#). If you have virtual machines that use

unsupported configurations or features, we recommend that you wait for the feature/configuration support to be announced. Alternatively, you can remove that feature or move out of that configuration to enable migration if it suits your needs.

- If you have automated scripts that deploy your infrastructure and applications today, try to create a similar test setup by using those scripts for migration. Alternatively, you can set up sample environments by using the Azure portal.

IMPORTANT

Application Gateways are not currently supported for migration from classic to Resource Manager. To migrate a classic virtual network with an Application gateway, remove the gateway before running a Prepare operation to move the network. After you complete the migration, reconnect the gateway in Azure Resource Manager.

ExpressRoute gateways connecting to ExpressRoute circuits in another subscription cannot be migrated automatically. In such cases, remove the ExpressRoute gateway, migrate the virtual network and recreate the gateway. Please see [Migrate ExpressRoute circuits and associated virtual networks from the classic to the Resource Manager deployment model](#) for more information.

Step 2: Set your subscription and register the provider

For migration scenarios, you need to set up your environment for both classic and Resource Manager. [Install Azure CLI](#) and [select your subscription](#).

Sign-in to your account.

```
azure login
```

Select the Azure subscription by using the following command.

```
azure account set "<azure-subscription-name>"
```

NOTE

Registration is a one time step but it needs to be done once before attempting migration. Without registering you'll see the following error message

BadRequest : Subscription is not registered for migration.

Register with the migration resource provider by using the following command. Note that in some cases, this command times out. However, the registration will be successful.

```
azure provider register Microsoft.ClassicInfrastructureMigrate
```

Please wait five minutes for the registration to finish. You can check the status of the approval by using the following command. Make sure that RegistrationState is `Registered` before you proceed.

```
azure provider show Microsoft.ClassicInfrastructureMigrate
```

Now switch CLI to the `asm` mode.

```
azure config mode asm
```

Step 3: Make sure you have enough Azure Resource Manager Virtual Machine vCPUs in the Azure region of your current deployment or VNET

For this step you'll need to switch to `arm` mode. Do this with the following command.

```
azure config mode arm
```

You can use the following CLI command to check the current number of vCPUs you have in Azure Resource Manager. To learn more about vCPU quotas, see [Limits and the Azure Resource Manager](#).

```
azure vm list-usage -l "<Your VNET or Deployment's Azure region"
```

Once you're done verifying this step, you can switch back to `asm` mode.

```
azure config mode asm
```

Step 4: Option 1 - Migrate virtual machines in a cloud service

Get the list of cloud services by using the following command, and then pick the cloud service that you want to migrate. Note that if the VMs in the cloud service are in a virtual network or if they have web/worker roles, you will get an error message.

```
azure service list
```

Run the following command to get the deployment name for the cloud service from the verbose output. In most cases, the deployment name is the same as the cloud service name.

```
azure service show <serviceName> -vv
```

First, validate if you can migrate the cloud service using the following commands:

```
azure service deployment validate-migration <serviceName> <deploymentName> new "" "" ""
```

Prepare the virtual machines in the cloud service for migration. You have two options to choose from.

If you want to migrate the VMs to a platform-created virtual network, use the following command.

```
azure service deployment prepare-migration <serviceName> <deploymentName> new "" "" ""
```

If you want to migrate to an existing virtual network in the Resource Manager deployment model, use the following command.

```
azure service deployment prepare-migration <serviceName> <deploymentName> existing <destinationVNETResourceGroupName> <subnetName> <vnetName>
```

After the prepare operation is successful, you can look through the verbose output to get the migration state of the VMs and ensure that they are in the `Prepared` state.

```
azure vm show <vmName> -vv
```

Check the configuration for the prepared resources by using either CLI or the Azure portal. If you are not ready for migration and you want to go back to the old state, use the following command.

```
azure service deployment abort-migration <serviceName> <deploymentName>
```

If the prepared configuration looks good, you can move forward and commit the resources by using the following command.

```
azure service deployment commit-migration <serviceName> <deploymentName>
```

Step 4: Option 2 - Migrate virtual machines in a virtual network

Pick the virtual network that you want to migrate. Note that if the virtual network contains web/worker roles or VMs with unsupported configurations, you will get a validation error message.

Get all the virtual networks in the subscription by using the following command.

```
azure network vnet list
```

The output will look something like this:

```
info: Executing command network vnet list
+ Looking up the virtual network sites
data:   Name                           Location  Affinity gr
data:   -----
data:   Group classicubuntu16 classicubuntu16  East US
data:   Group Group LinuxHost          East US
data:   Group LinuxRG LinuxRG         East US
data:   Group SUSEClassicRG SUSEClassicRG  East US
info: network vnet list command OK
```

In the above example, the **virtualNetworkName** is the entire name "**Group classicubuntu16 classicubuntu16**".

First, validate if you can migrate the virtual network using the following command:

```
azure network vnet validate-migration <virtualNetworkName>
```

Prepare the virtual network of your choice for migration by using the following command.

```
azure network vnet prepare-migration <virtualNetworkName>
```

Check the configuration for the prepared virtual machines by using either CLI or the Azure portal. If you are not ready for migration and you want to go back to the old state, use the following command.

```
azure network vnet abort-migration <virtualNetworkName>
```

If the prepared configuration looks good, you can move forward and commit the resources by using the following

command.

```
azure network vnet commit-migration <virtualNetworkName>
```

Step 5: Migrate a storage account

Once you're done migrating the virtual machines, we recommend you migrate the storage account.

Prepare the storage account for migration by using the following command

```
azure storage account prepare-migration <storageAccountName>
```

Check the configuration for the prepared storage account by using either CLI or the Azure portal. If you are not ready for migration and you want to go back to the old state, use the following command.

```
azure storage account abort-migration <storageAccountName>
```

If the prepared configuration looks good, you can move forward and commit the resources by using the following command.

```
azure storage account commit-migration <storageAccountName>
```

Next steps

- [Overview of platform-supported migration of IaaS resources from classic to Azure Resource Manager](#)
- [Technical deep dive on platform-supported migration from classic to Azure Resource Manager](#)
- [Planning for migration of IaaS resources from classic to Azure Resource Manager](#)
- [Use PowerShell to migrate IaaS resources from classic to Azure Resource Manager](#)
- [Community tools for assisting with migration of IaaS resources from classic to Azure Resource Manager](#)
- [Review most common migration errors](#)
- [Review the most frequently asked questions about migrating IaaS resources from classic to Azure Resource Manager](#)

Common errors during Classic to Azure Resource Manager migration

2/28/2020 • 9 minutes to read • [Edit Online](#)

IMPORTANT

Today, about 90% of IaaS VMs are using [Azure Resource Manager](#). As of February 28, 2020, classic VMs have been deprecated and will be fully retired on March 1, 2023. [Learn more](#) about this deprecation and [how it affects you](#).

This article catalogs the most common errors and mitigations during the migration of IaaS resources from Azure classic deployment model to the Azure Resource Manager stack.

NOTE

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

List of errors

ERROR STRING	MITIGATION
Internal server error	In some cases, this is a transient error that goes away with a retry. If it continues to persist, contact Azure support as it needs investigation of platform logs. NOTE: Once the incident is tracked by the support team, please do not attempt any self-mitigation as this might have unintended consequences on your environment.
Migration is not supported for Deployment {deployment-name} in HostedService {hosted-service-name} because it is a PaaS deployment (Web/Worker).	This happens when a deployment contains a web/worker role. Since migration is only supported for Virtual Machines, please remove the web/worker role from the deployment and try migration again.
Template {template-name} deployment failed. CorrelationId= {guid}	In the backend of migration service, we use Azure Resource Manager templates to create resources in the Azure Resource Manager stack. Since templates are idempotent, usually you can safely retry the migration operation to get past this error. If this error continues to persist, please contact Azure support and give them the CorrelationId. NOTE: Once the incident is tracked by the support team, please do not attempt any self-mitigation as this might have unintended consequences on your environment.
The virtual network {virtual-network-name} does not exist.	This can happen if you created the Virtual Network in the new Azure portal. The actual Virtual Network name follows the pattern "Group * < VNET name >"

ERROR STRING	MITIGATION
VM {vm-name} in HostedService {hosted-service-name} contains Extension {extension-name} which is not supported in Azure Resource Manager. It is recommended to uninstall it from the VM before continuing with migration.	XML extensions such as BGInfo 1.* are not supported in Azure Resource Manager. Therefore, these extensions cannot be migrated. If these extensions are left installed on the virtual machine, they are automatically uninstalled before completing the migration.
VM {vm-name} in HostedService {hosted-service-name} contains Extension VMSnapshot/VMSnapshotLinux, which is currently not supported for Migration. Uninstall it from the VM and add it back using Azure Resource Manager after the Migration is Complete	This is the scenario where the virtual machine is configured for Azure Backup. Since this is currently an unsupported scenario, please follow the workaround at https://aka.ms/vmbakcupmigration
VM {vm-name} in HostedService {hosted-service-name} contains Extension {extension-name} whose Status is not being reported from the VM. Hence, this VM cannot be migrated. Ensure that the Extension status is being reported or uninstall the extension from the VM and retry migration.	Azure guest agent & VM Extensions need outbound internet access to the VM storage account to populate their status. Common causes of status failure include <ul style="list-style-type: none"> • a Network Security Group that blocks outbound access to the internet • If the VNET has on premises DNS servers and DNS connectivity is lost
VM {vm-name} in HostedService {hosted-service-name} contains Extension {extension-name} reporting Handler Status: {handler-status}. Hence, the VM cannot be migrated. Ensure that the Extension handler status being reported is {handler-status} or uninstall it from the VM and retry migration.	If you continue to see an unsupported status, you can uninstall the extensions to skip this check and move forward with migration.
VM Agent for VM {vm-name} in HostedService {hosted-service-name} is reporting the overall agent status as Not Ready. Hence, the VM may not be migrated, if it has a migratable extension. Ensure that the VM Agent is reporting overall agent status as Ready. Refer to https://aka.ms/classiciaasmigrationfaqs .	
Migration is not supported for Deployment {deployment-name} in HostedService {hosted-service-name} because it has multiple Availability Sets.	Currently, only hosted services that have 1 or less Availability sets can be migrated. To work around this problem, please move the additional Availability sets and Virtual machines in those Availability sets to a different hosted service.
Migration is not supported for Deployment {deployment-name} in HostedService {hosted-service-name} because it has VMs that are not part of the Availability Set even though the HostedService contains one.	The workaround for this scenario is to either move all the virtual machines into a single Availability set or remove all Virtual machines from the Availability set in the hosted service.
Storage account/HostedService/Virtual Network {virtual-network-name} is in the process of being migrated and hence cannot be changed	This error happens when the "Prepare" migration operation has been completed on the resource and an operation that would make a change to the resource is triggered. Because of the lock on the management plane after "Prepare" operation, any changes to the resource are blocked. To unlock the management plane, you can run the "Commit" migration operation to complete migration or the "Abort" migration operation to roll back the "Prepare" operation.
Migration is not allowed for HostedService {hosted-service-name} because it has VM {vm-name} in State: RoleStateUnknown. Migration is allowed only when the VM is in one of the following states - Running, Stopped, Stopped Deallocated.	The VM might be undergoing through a state transition, which usually happens when during an update operation on the HostedService such as a reboot, extension installation etc. It is recommended for the update operation to complete on the HostedService before trying migration.

ERROR STRING	MITIGATION
Deployment {deployment-name} in HostedService {hosted-service-name} contains a VM {vm-name} with Data Disk {data-disk-name} whose physical blob size {size-of-the-vhd-blob-backing-the-data-disk} bytes does not match the VM Data Disk logical size {size-of-the-data-disk-specified-in-the-vm-api} bytes. Migration will proceed without specifying a size for the data disk for the Azure Resource Manager VM.	This error happens if you've resized the VHD blob without updating the size in the VM API model. Detailed mitigation steps are outlined below .
A storage exception occurred while validating data disk {data-disk-name} with media link {data-disk-uri} for VM {VM name} in Cloud Service {Cloud Service name}. Please ensure that the VHD media link is accessible for this virtual machine	This error can happen if the disks of the VM have been deleted or are not accessible anymore. Please make sure the disks for the VM exist.
VM {vm-name} in HostedService {cloud-service-name} contains Disk with MediaLink {vhd-uri} which has blob name {vhd-blob-name} that is not supported in Azure Resource Manager.	This error occurs when the name of the blob has a "/" in it which is not supported in Compute Resource Provider currently.
Migration is not allowed for Deployment {deployment-name} in HostedService {cloud-service-name} as it is not in the regional scope. Please refer to https://aka.ms/regionscope for moving this deployment to regional scope.	In 2014, Azure announced that networking resources will move from a cluster level scope to regional scope. See https://aka.ms/regionscope for more details . This error happens when the deployment being migrated has not had an update operation, which automatically moves it to a regional scope. Best workaround is to either add an endpoint to a VM or a data disk to the VM and then retry migration. See How to set up endpoints on a classic Windows virtual machine in Azure or Attach a data disk to a Windows virtual machine created with the classic deployment model
Migration is not supported for Virtual Network {vnet-name} because it has non-gateway PaaS deployments.	This error occurs when you have non-gateway PaaS deployments such as Application Gateway or API Management services that are connected to the Virtual Network.

Detailed mitigations

VM with Data Disk whose physical blob size bytes does not match the VM Data Disk logical size bytes.

This happens when the Data disk logical size can get out of sync with the actual VHD blob size. This can be easily verified using the following commands:

Verifying the issue

```

# Store the VM details in the VM object
$vm = Get-AzureVM -ServiceName $servicename -Name $vmname

# Display the data disk properties
# NOTE the data disk LogicalDiskSizeInGB below which is 11GB. Also note the MediaLink Uri of the VHD blob as
we'll use this in the next step
$vm.VM.DataVirtualHardDisks


HostCaching      : None
DiskLabel        :
DiskName         : coreosvm-coreosvm-0-201611230636240687
Lun              : 0
LogicalDiskSizeInGB : 11
MediaLink        : https://contosostorage.blob.core.windows.net/vhds/coreosvm-dd1.vhd
SourceMediaLink   :
IOType           : Standard
ExtensionData    :

# Now get the properties of the blob backing the data disk above
# NOTE the size of the blob is about 15 GB which is different from LogicalDiskSizeInGB above
blob = Get-AzStorageblob -Blob "coreosvm-dd1.vhd" -Container vhds

blob

ICloudBlob      : Microsoft.WindowsAzure.Storage.Blob.CloudPageBlob
BlobType        : PageBlob
Length          : 16106127872
ContentType     : application/octet-stream
LastModified    : 11/23/2016 7:16:22 AM +00:00
SnapshotTime    :
ContinuationToken :
Context          : Microsoft.WindowsAzure.Commands.Common.Storage.AzureStorageContext
Name            : coreosvm-dd1.vhd

```

Mitigating the issue

```

# Convert the blob size in bytes to GB into a variable which we'll use later
$newSize = [int]($blob.Length / 1GB)

# See the calculated size in GB
$newSize

15

# Store the disk name of the data disk as we'll use this to identify the disk to be updated
$diskName = $vm.VM.DataVirtualHardDisks[0].DiskName

# Identify the LUN of the data disk to remove
$lunToRemove = $vm.VM.DataVirtualHardDisks[0].Lun

# Now remove the data disk from the VM so that the disk isn't leased by the VM and it's size can be updated
Remove-AzureDataDisk -LUN $lunToRemove -VM $vm | Update-AzureVm -Name $vmname -ServiceName $servicename

OperationDescription OperationId          OperationStatus
----- ----- -----
Update-AzureVM      213xx1-b44b-1v6n-23gg-591f2a13cd16 Succeeded

# Verify we have the right disk that's going to be updated
Get-AzureDisk -DiskName $diskName

AffinityGroup      :
AttachedTo        :
IsCorrupted       : False
Label             :
Location          : East US
DiskSizeInGB      : 11

```

```

DISKSIZEINGB          : 11
MediaLink             : https://contosostorage.blob.core.windows.net/vhds/coreosvm-dd1.vhd
DiskName              : coreosvm-coreosvm-0-201611230636240687
SourceImageName       :
OS                   :
IOType                : Standard
OperationDescription  : Get-AzureDisk
OperationId           : 0c56a2b7-a325-123b-7043-74c27d5a61fd
OperationStatus        : Succeeded

# Now update the disk to the new size
Update-AzureDisk -DiskName $diskName -ResizedSizeInGB $newSize -Label $diskName

OperationDescription OperationId          OperationStatus
-----  -----  -----
Update-AzureDisk      cv134b65-1b6n-8908-abuo-ce9e395ac3e7 Succeeded

# Now verify that the "DiskSizeInGB" property of the disk matches the size of the blob
Get-AzureDisk -DiskName $diskName

AffinityGroup         :
AttachedTo            :
IsCorrupted          : False
Label                : coreosvm-coreosvm-0-201611230636240687
Location              : East US
DiskSizeInGB          : 15
MediaLink             : https://contosostorage.blob.core.windows.net/vhds/coreosvm-dd1.vhd
DiskName              : coreosvm-coreosvm-0-201611230636240687
SourceImageName       :
OS                   :
IOType                : Standard
OperationDescription  : Get-AzureDisk
OperationId           : 1v53bde5-cv56-5621-9078-16b9c8a0bad2
OperationStatus        : Succeeded

# Now we'll add the disk back to the VM as a data disk. First we need to get an updated VM object
$vm = Get-AzureVM -ServiceName $servicename -Name $vmname

Add-AzureDataDisk -Import -DiskName $diskName -LUN 0 -VM $vm -HostCaching ReadWrite | Update-AzureVm -Name
$vmname -ServiceName $servicename

OperationDescription OperationId          OperationStatus
-----  -----  -----
Update-AzureVM       b0ad3d4c-4v68-45vb-xxc1-134fd010d0f8 Succeeded

```

Moving a VM to a different subscription after completing migration

After you complete the migration process, you may want to move the VM to another subscription. However, if you have a secret/certificate on the VM that references a Key Vault resource, the move is currently not supported. The below instructions will allow you to workaround the issue.

PowerShell

```

$vm = Get-AzVM -ResourceGroupName "MyRG" -Name "MyVM"
Remove-AzVMSecret -VM $vm
Update-AzVM -ResourceGroupName "MyRG" -VM $vm

```

Azure CLI

```
az vm update -g "myrg" -n "myvm" --set osProfile.Secrets=[]
```

Next steps

- Overview of platform-supported migration of IaaS resources from classic to Azure Resource Manager
- Technical deep dive on platform-supported migration from classic to Azure Resource Manager
- Planning for migration of IaaS resources from classic to Azure Resource Manager
- Use PowerShell to migrate IaaS resources from classic to Azure Resource Manager
- Use CLI to migrate IaaS resources from classic to Azure Resource Manager
- Community tools for assisting with migration of IaaS resources from classic to Azure Resource Manager
- Review the most frequently asked questions about migrating IaaS resources from classic to Azure Resource Manager

Community tools to migrate IaaS resources from classic to Azure Resource Manager

2/28/2020 • 2 minutes to read • [Edit Online](#)

IMPORTANT

Today, about 90% of IaaS VMs are using [Azure Resource Manager](#). As of February 28, 2020, classic VMs have been deprecated and will be fully retired on March 1, 2023. [Learn more](#) about this deprecation and [how it affects you](#).

This article catalogs the tools that have been provided by the community to assist with migration of IaaS resources from classic to the Azure Resource Manager deployment model.

NOTE

These tools are not officially supported by Microsoft Support. Therefore they are open sourced on GitHub and we're happy to accept PRs for fixes or additional scenarios. To report an issue, use the GitHub issues feature.

Migrating with these tools will cause downtime for your classic Virtual Machine. If you're looking for platform supported migration, visit

- [Platform supported migration of IaaS resources from Classic to Azure Resource Manager stack](#)
- [Technical Deep Dive on Platform supported migration from Classic to Azure Resource Manager](#)
- [Migrate IaaS resources from Classic to Azure Resource Manager using Azure PowerShell](#)

AsmMetadataParser

This is a collection of helper tools created as part of enterprise migrations from Azure Service Management to Azure Resource Manager. This tool allows you to replicate your infrastructure into another subscription which can be used for testing migration and iron out any issues before running the migration on your Production subscription.

[Link to the tool documentation](#)

migAz

migAz is an additional option to migrate a complete set of classic IaaS resources to Azure Resource Manager IaaS resources. The migration can occur within the same subscription or between different subscriptions and subscription types (ex: CSP subscriptions).

[Link to the tool documentation](#)

Next Steps

- [Overview of platform-supported migration of IaaS resources from classic to Azure Resource Manager](#)
- [Technical deep dive on platform-supported migration from classic to Azure Resource Manager](#)
- [Planning for migration of IaaS resources from classic to Azure Resource Manager](#)
- [Use PowerShell to migrate IaaS resources from classic to Azure Resource Manager](#)
- [Use CLI to migrate IaaS resources from classic to Azure Resource Manager](#)
- [Review most common migration errors](#)

- Review the most frequently asked questions about migrating IaaS resources from classic to Azure Resource Manager

Frequently asked questions about classic to Azure Resource Manager migration

2/28/2020 • 6 minutes to read • [Edit Online](#)

IMPORTANT

Today, about 90% of IaaS VMs are using [Azure Resource Manager](#). As of February 28, 2020, classic VMs have been deprecated and will be fully retired on March 1, 2023. [Learn more](#) about this deprecation and [how it affects you](#).

What is the time required for migration?

Planning and execution of migration greatly depends on the complexity of the architecture and could take couple of months.

What is the definition of a new customer on IaaS VMs (classic)?

Customers who did not have IaaS VMs (classic) in their subscriptions in the month of February 2020 (a month before deprecation started) are considered as new customers.

Does this migration plan affect any of my existing services or applications that run on Azure virtual machines?

Not until March 1st, 2023 for IaaS VMs (classic). The IaaS VMs (classic) are fully supported services in general availability. You can continue to use these resources to expand your footprint on Microsoft Azure. On March 1st, 2023, these VMs will be fully retired and any active or allocated VMs will be stopped & deallocated. There will be no impact to other classic resources like Cloud Services (Classic), Storage Accounts (Classic), etc.

What happens to my VMs if I don't plan on migrating in the near future?

On March 1st, 2023, the IaaS VMs (Classic) will be fully retired and any active or allocated VMs will be stopped & deallocated. To prevent business impact, we highly recommend to start planning your migration today and complete it before March 1st, 2023. We are not deprecating the existing classic APIs, Cloud Services and resource model. We want to make migration easy, considering the advanced features that are available in the Resource Manager deployment model. We recommend that you start planning to migrate these resources to Azure Resource Manager.

What does this migration plan mean for my existing tooling?

Updating your tooling to the Resource Manager deployment model is one of the most important changes that you have to account for in your migration plans.

How long will the management-plane downtime be?

It depends on the number of resources that are being migrated. For smaller deployments (a few tens of VMs), the whole migration should take less than an hour. For large-scale deployments (hundreds of VMs), the migration can take a few hours.

Can I roll back after my migrating resources are committed in Resource Manager?

You can abort your migration as long as the resources are in the prepared state. Rollback is not supported after the resources have been successfully migrated through the commit operation.

Can I roll back my migration if the commit operation fails?

You cannot abort migration if the commit operation fails. All migration operations, including the commit operation, are idempotent. So we recommend that you retry the operation after a short time. If you still face an error, create a support ticket.

Do I have to buy another express route circuit if I have to use IaaS under Resource Manager?

No. We recently enabled [moving ExpressRoute circuits from the classic to the Resource Manager deployment model](#). You don't have to buy a new ExpressRoute circuit if you already have one.

What if I had configured Role-Based Access Control policies for my classic IaaS resources?

During migration, the resources transform from classic to Resource Manager. So we recommend that you plan the RBAC policy updates that need to happen after migration.

I backed up my classic VMs in a vault. Can I migrate my VMs from classic mode to Resource Manager mode and protect them in a Recovery Services vault?

When you move a VM from classic to Resource Manager mode, backups taken prior to migration will not migrate to newly migrated Resource Manager VM. However, if you wish to keep your backups of classic VMs, follow these steps before the migration.

1. In the Recovery Services vault, go to the **Protected Items** tab and select the VM.
2. Click Stop Protection. Leave *Delete associated backup data* option **unchecked**.

NOTE

You will be charged backup instance cost till you retain data. Backup copies will be pruned as per retention range. However, last backup copy is always kept until you explicitly delete backup data. It is advised to check your retention range of the Virtual machine and trigger "Delete Backup Data" on the protected item in the vault once the retention range is over.

To migrate the virtual machine to Resource Manager mode,

1. Delete the backup/snapshot extension from the VM.
2. Migrate the virtual machine from classic mode to Resource Manager mode. Make sure the storage and network information corresponding to the virtual machine is also migrated to Resource Manager mode.

Additionally, if you want to back up the migrated VM, go to Virtual Machine management blade to [enable backup](#).

Can I validate my subscription or resources to see if they're capable of

migration?

Yes. In the platform-supported migration option, the first step in preparing for migration is to validate that the resources are capable of migration. In case the validate operation fails, you receive messages for all the reasons the migration cannot be completed.

What happens if I run into a quota error while preparing the IaaS resources for migration?

We recommend that you abort your migration and then log a support request to increase the quotas in the region where you are migrating the VMs. After the quota request is approved, you can start executing the migration steps again.

How do I report an issue?

Post your issues and questions about migration to our [VM forum](#), with the keyword ClassicIaaSMigration. We recommend posting all your questions on this forum. If you have a support contract, you're welcome to log a support ticket as well.

What if I don't like the names of the resources that the platform chose during migration?

All the resources that you explicitly provide names for in the classic deployment model are retained during migration. In some cases, new resources are created. For example: a network interface is created for every VM. We currently don't support the ability to control the names of these new resources created during migration. Log your votes for this feature on the [Azure feedback forum](#).

Can I migrate ExpressRoute circuits used across subscriptions with authorization links?

ExpressRoute circuits which use cross-subscription authorization links cannot be migrated automatically without downtime. We have guidance on how these can be migrated using manual steps. See [Migrate ExpressRoute circuits and associated virtual networks from the classic to the Resource Manager deployment model](#) for steps and more information.

I got the message "VM is reporting the overall agent status as Not Ready. Hence, the VM cannot be migrated. Ensure that the VM Agent is reporting overall agent status as Ready" or "VM contains Extension whose Status is not being reported from the VM. Hence, this VM cannot be migrated."

This message is received when the VM does not have outbound connectivity to the internet. The VM agent uses outbound connectivity to reach the Azure storage account for updating the agent status every five minutes.

Next steps

- [Overview of platform-supported migration of IaaS resources from classic to Azure Resource Manager](#)
- [Technical deep dive on platform-supported migration from classic to Azure Resource Manager](#)
- [Planning for migration of IaaS resources from classic to Azure Resource Manager](#)
- [Use PowerShell to migrate IaaS resources from classic to Azure Resource Manager](#)
- [Use CLI to migrate IaaS resources from classic to Azure Resource Manager](#)

- Community tools for assisting with migration of IaaS resources from classic to Azure Resource Manager
- Review most common migration errors

Security recommendations for Linux virtual machines in Azure

11/13/2019 • 3 minutes to read • [Edit Online](#)

This article contains security recommendations for Azure Virtual Machines. Follow these recommendations to help fulfill the security obligations described in our model for shared responsibility. The recommendations will also help you improve overall security for your web app solutions. For more information about what Microsoft does to fulfill service-provider responsibilities, see [Shared responsibilities for cloud computing](#).

Some of this article's recommendations can be automatically addressed by Azure Security Center. Azure Security Center is the first line of defense for your resources in Azure. It periodically analyzes the security state of your Azure resources to identify potential security vulnerabilities. It then recommends how to address the vulnerabilities. For more information, see [Security recommendations in Azure Security Center](#).

For general information about Azure Security Center, see [What is Azure Security Center?](#).

General

RECOMMENDATION	COMMENTS	SECURITY CENTER
When you build custom VM images, apply the latest updates.	Before you create images, install the latest updates for the operating system and for all applications that will be part of your image.	-
Keep your VMs current.	You can use the Update Management solution in Azure Automation to manage operating system updates for your Windows and Linux computers in Azure.	Yes
Back up your VMs.	Azure Backup helps protect your application data and has minimal operating costs. Application errors can corrupt your data, and human errors can introduce bugs into your applications. Azure Backup protects your VMs that run Windows and Linux.	-
Use multiple VMs for greater resilience and availability.	If your VM runs applications that must be highly available, use multiple VMs or availability sets .	-
Adopt a business continuity and disaster recovery (BCDR) strategy.	Azure Site Recovery allows you to choose from different options designed to support business continuity. It supports different replication and failover scenarios. For more information, see About Site Recovery .	-

Data security

RECOMMENDATION	COMMENTS	SECURITY CENTER
Encrypt operating system disks.	Azure Disk Encryption helps you encrypt your Windows and Linux IaaS VM disks. Without the necessary keys, the contents of encrypted disks are unreadable. Disk encryption protects stored data from unauthorized access that would otherwise be possible if the disk were copied.	Yes
Encrypt data disks.	Azure Disk Encryption helps you encrypt your Windows and Linux IaaS VM disks. Without the necessary keys, the contents of encrypted disks are unreadable. Disk encryption protects stored data from unauthorized access that would otherwise be possible if the disk were copied.	-
Limit installed software.	Limit installed software to what is required to successfully apply your solution. This guideline helps reduce your solution's attack surface.	-
Use antivirus or antimalware.	In Azure, you can use antimalware software from security vendors such as Microsoft, Symantec, Trend Micro, and Kaspersky. This software helps protect your VMs from malicious files, adware, and other threats. You can deploy Microsoft Antimalware based on your application workloads. Use either basic secure-by-default or advanced custom configuration. For more information, see Microsoft Antimalware for Azure Cloud Services and Virtual Machines .	-
Securely store keys and secrets.	Simplify the management of your secrets and keys by providing your application owners with a secure, centrally managed option. This management reduces the risk of an accidental compromise or leak. Azure Key Vault can securely store your keys in hardware security modules (HSMs) that are certified to FIPS 140-2 Level 2. If you need to use FIPs 140.2 Level 3 to store your keys and secrets, you can use Azure Dedicated HSM .	-

Identity and access management

RECOMMENDATION	COMMENTS	SECURITY CENTER
Centralize VM authentication.	You can centralize the authentication of your Windows and Linux VMs by using Azure Active Directory authentication .	-

Monitoring

RECOMMENDATION	COMMENTS	SECURITY CENTER
Monitor your VMs.	You can use Azure Monitor for VMs to monitor the state of your Azure VMs and virtual machine scale sets. Performance issues with a VM can lead to service disruption, which violates the security principle of availability.	-

Networking

RECOMMENDATION	COMMENTS	SECURITY CENTER
Restrict access to management ports.	Attackers scan public cloud IP ranges for open management ports and attempt "easy" attacks like common passwords and known unpatched vulnerabilities. You can use just-in-time (JIT) VM access to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy connections to VMs when they're needed.	-
Limit network access.	Network security groups allow you to restrict network access and control the number of exposed endpoints. For more information, see Create, change, or delete a network security group .	-

Next steps

Check with your application provider to learn about additional security requirements. For more information about developing secure applications, see [Secure-development documentation](#).

Secure your management ports with just-in-time access

2/25/2020 • 11 minutes to read • [Edit Online](#)

If you're on Security Center's standard pricing tier (see [pricing](#)), you can lock down inbound traffic to your Azure VMs with just-in-time (JIT) virtual machine (VM) access. This reduces exposure to attacks while providing easy access to connect to VMs when needed.

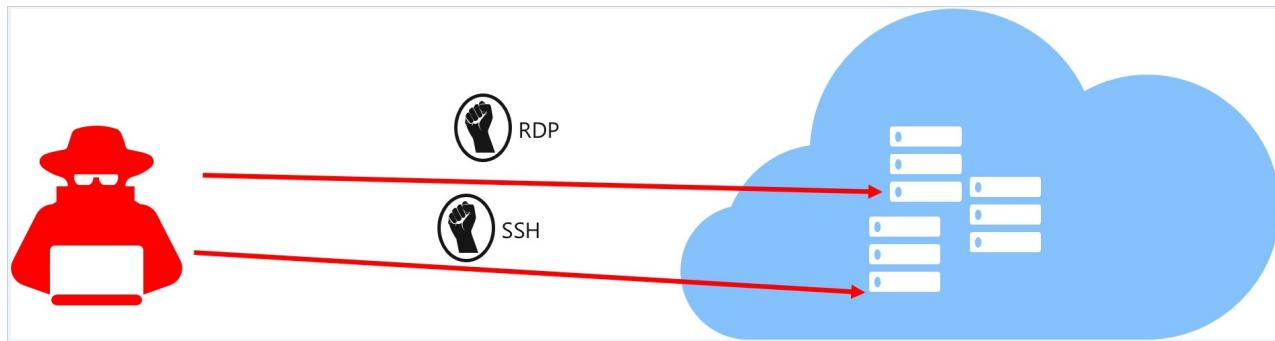
NOTE

Security Center just-in-time VM access currently supports only VMs deployed through Azure Resource Manager. To learn more about the classic and Resource Manager deployment models see [Azure Resource Manager vs. classic deployment](#).

Attack scenario

Brute force attacks commonly target management ports as a means to gain access to a VM. If successful, an attacker can take control over the VM and establish a foothold into your environment.

One way to reduce exposure to a brute force attack is to limit the amount of time that a port is open. Management ports don't need to be open at all times. They only need to be open while you're connected to the VM, for example to perform management or maintenance tasks. When just-in-time is enabled, Security Center uses [network security group](#) (NSG) and Azure Firewall rules, which restrict access to management ports so they cannot be targeted by attackers.



How does JIT access work?

When just-in-time is enabled, Security Center locks down inbound traffic to your Azure VMs by creating an NSG rule. You select the ports on the VM to which inbound traffic will be locked down. These ports are controlled by the just-in-time solution.

When a user requests access to a VM, Security Center checks that the user has [Role-Based Access Control \(RBAC\)](#) permissions for that VM. If the request is approved, Security Center automatically configures the Network Security Groups (NSGs) and Azure Firewall to allow inbound traffic to the selected ports and requested source IP addresses or ranges, for the amount of time that was specified. After the time has expired, Security Center restores the NSGs to their previous states. Those connections that are already established are not being interrupted, however.

NOTE

If a JIT access request is approved for a VM behind an Azure Firewall, then Security Center automatically changes both the NSG and firewall policy rules. For the amount of time that was specified, the rules allow inbound traffic to the selected ports and requested source IP addresses or ranges. After the time is over, Security Center restores the firewall and NSG rules to their previous states.

Permissions needed to configure and use JIT

TO ENABLE A USER TO:	PERMISSIONS TO SET
Configure or edit a JIT policy for a VM	<p><i>Assign these actions to the role:</i></p> <ul style="list-style-type: none"> On the scope of a subscription or resource group that is associated with the VM: <code>Microsoft.Security/locations/jitNetworkAccessPolicies/write</code> On the scope of a subscription or resource group of VM: <code>Microsoft.Compute/virtualMachines/write</code>
Request JIT access to a VM	<p><i>Assign these actions to the user:</i></p> <ul style="list-style-type: none"> On the scope of a subscription or resource group that is associated with the VM: <code>Microsoft.Security/locations/jitNetworkAccessPolicies/initiate/*/read</code> On the scope of a subscription or resource group that is associated with the VM: <code>Microsoft.Security/locations/jitNetworkAccessPolicies/*/read</code> On the scope of a subscription or resource group or VM: <code>Microsoft.Compute/virtualMachines/read</code> On the scope of a subscription or resource group or VM: <code>Microsoft.Network/networkInterfaces/*/read</code>

Configure JIT on a VM

There are three ways to configure a JIT policy on a VM:

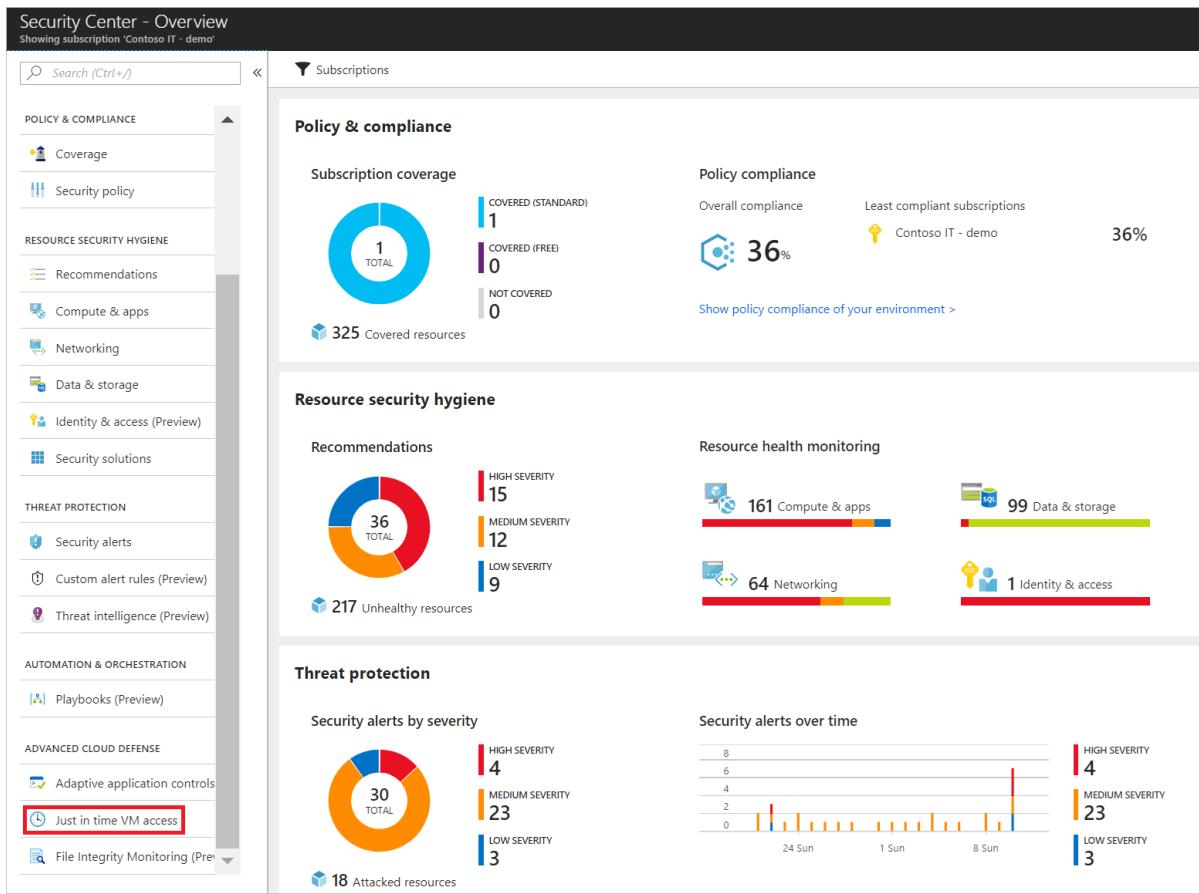
- Configure JIT access in Azure Security Center
- Configure JIT access in an Azure VM page
- Configure a JIT policy on a VM programmatically

Configure JIT in Azure Security Center

From Security Center, you can configure a JIT policy and request access to a VM using a JIT policy

Configure JIT access on a VM in Security Center

- Open the **Security Center** dashboard.
- In the left pane, select **Just-in-time VM access**.



The **Just-in-time VM access** window opens and shows information on the state of your VMs:

- **Configured** - VMs that have been configured to support just-in-time VM access. The data presented is for the last week and includes for each VM the number of approved requests, last access date and time, and last user.
- **Recommended** - VMs that can support just-in-time VM access but haven't been configured to. We recommend that you enable just-in-time VM access control for these VMs.
- **No recommendation** - Reasons that can cause a VM not to be recommended are:
 - Missing NSG - The just-in-time solution requires an NSG to be in place.
 - Classic VM - Security Center just-in-time VM access currently supports only VMs deployed through Azure Resource Manager. A classic deployment is not supported by the just-in-time solution.
 - Other - A VM is in this category if the just-in-time solution is turned off in the security policy of the subscription or the resource group, or if the VM is missing a public IP and doesn't have an NSG in place.

3. Select the **Recommended** tab.
4. Under **VIRTUAL MACHINE**, click the VMs that you want to enable. This puts a checkmark next to a VM.

Virtual machines

Configured Recommended No recommendation

VMs for which we recommend you to apply the just in time VM access control.

61 VMs

[Enable JIT on 2 VMs](#)

Search to filter items...

VIRTUAL MACHINE	STATE	SEVERITY
AA-Contoso-01	Open	! High
<input checked="" type="checkbox"/> App01	Open	! High
App03	Open	! High
App04	Open	! High
App05	Open	! High
App06	Open	! High
<input checked="" type="checkbox"/> App07	Open	! High
App08	Open	! High
App09	Open	! High

5. Click **Enable JIT on VMs**. A pane opens displaying the default ports recommended by Azure Security Center:

- 22 - SSH
- 3389 - RDP
- 5985 - WinRM
- 5986 - WinRM

6. Optionally, you can add custom ports to the list:

- a. Click **Add**. The **Add port configuration** window opens.
- b. For each port you choose to configure, both default and custom, you can customize the following settings:
 - **Protocol type**- The protocol that is allowed on this port when a request is approved.
 - **Allowed source IP addresses**- The IP ranges that are allowed on this port when a request is approved.
 - **Maximum request time**- The maximum time window during which a specific port can be opened.
- c. Click **OK**.

7. Click **Save**.

NOTE

When JIT VM Access is enabled for a VM, Azure Security Center creates "deny all inbound traffic" rules for the selected ports in the network security groups associated and Azure Firewall with it. If other rules had been created for the selected ports, then the existing rules take priority over the new "deny all inbound traffic" rules. If there are no existing rules on the selected ports, then the new "deny all inbound traffic" rules take top priority in the Network Security Groups and Azure Firewall.

Request JIT access via Security Center

To request access to a VM via Security Center:

1. Under **Just-in-time VM access**, select the **Configured** tab.

2. Under **Virtual Machine**, click the VMs that you want to request access for. This puts a checkmark next to the VM.

- The icon in the **Connection Details** column indicates whether JIT is enabled on the NSG or FW. If it's enabled on both, only the Firewall icon appears.
- The **Connection Details** column provides the information required to connect the VM, and its open ports.

Virtual machines						
Configured Recommended No recommendation						
VMs for which the just in time VM access control is already in place. Presented data is for the last week.						
92 VMs						Request access
<input type="checkbox"/> Search to filter items...						
VIRTUAL MACHINE	APPROVED	LAST ACCESS	CONNECTION DETAILS	LAST USER		
 af-vm	1 Requests	5/7/19, 11:05 AM	 13.64.24.215:13389	user@contoso.com	...	
 srvworkload2	1 Requests	5/7/19, 11:30 AM	 20.185.107.87:10022	user@contoso.com	...	
 sc2019	2 Requests	5/7/19, 11:39 AM	 3 Ports	user@contoso.com	...	
 bengr-jit-mul-1	1 Requests	Active now	 Ports: 5986, 22, 3389	user@contoso.com	...	
 LBWeb0	0 Requests	N/A	 -	N/A	...	
 LBWeb1	0 Requests	N/A	 -	N/A	...	
 muliport1	0 Requests	N/A	 -	N/A	...	
<input checked="" type="checkbox"/>  muliport0	0 Requests	N/A	 -	N/A	...	
 WebApp1	0 Requests	N/A	 -	N/A	...	
 WinVM	0 Requests	N/A	 -	N/A	...	
 vm2	0 Requests	N/A	 -	N/A	...	
 BarWafT2Jun3	0 Requests	N/A	 -	N/A	...	
 bengr-jit-mul-2	0 Requests	N/A	 -	N/A	...	
 ChkplJun3	0 Requests	N/A	 -	N/A	...	

3. Click **Request access**. The **Request access** window opens.

Request access

Please select the ports that you would like to open per virtual machine.

PORT	TOGGLE	ALLOWED SOURCE IP	IP RANGE	TIMERANGE
▼ vm1				
22	<input checked="" type="button"/> On <input type="button"/> Off	<input type="button"/> My IP <input type="button"/> IP Range	<input type="button"/> No range	<div style="width: 100%;"><div style="width: 100%; background-color: #0072bc; height: 10px;"></div><div style="width: 10px; background-color: white; height: 10px; float: right;">3</div></div>
3389	<input checked="" type="button"/> On <input type="button"/> Off	<input type="button"/> My IP <input type="button"/> IP Range	<input type="button"/> No range	<div style="width: 100%;"><div style="width: 100%; background-color: #0072bc; height: 10px;"></div><div style="width: 10px; background-color: white; height: 10px; float: right;">3</div></div>
5985	<input type="button"/> On <input checked="" type="button"/> Off	<input type="button"/> My IP <input type="button"/> IP Range	<input type="button"/> No range	<div style="width: 100%;"><div style="width: 100%; background-color: #0072bc; height: 10px;"></div><div style="width: 10px; background-color: white; height: 10px; float: right;">3</div></div>
5986	<input type="button"/> On <input checked="" type="button"/> Off	<input type="button"/> My IP <input type="button"/> IP Range	<input type="button"/> No range	<div style="width: 100%;"><div style="width: 100%; background-color: #0072bc; height: 10px;"></div><div style="width: 10px; background-color: white; height: 10px; float: right;">3</div></div>
▼ vm2				
22	<input type="button"/> On <input checked="" type="button"/> Off	<input type="button"/> My IP <input type="button"/> IP Range	<input type="button"/> No range	<div style="width: 100%;"><div style="width: 100%; background-color: #0072bc; height: 10px;"></div><div style="width: 10px; background-color: white; height: 10px; float: right;">3</div></div>
3389	<input type="button"/> On <input checked="" type="button"/> Off	<input type="button"/> My IP <input type="button"/> IP Range	<input type="button"/> No range	<div style="width: 100%;"><div style="width: 100%; background-color: #0072bc; height: 10px;"></div><div style="width: 10px; background-color: white; height: 10px; float: right;">2</div></div>
5985	<input type="button"/> On <input checked="" type="button"/> Off	<input type="button"/> My IP <input type="button"/> IP Range	<input type="button"/> No range	<div style="width: 100%;"><div style="width: 100%; background-color: #0072bc; height: 10px;"></div><div style="width: 10px; background-color: white; height: 10px; float: right;">3</div></div>
5986	<input type="button"/> On <input checked="" type="button"/> Off	<input type="button"/> My IP <input type="button"/> IP Range	<input type="button"/> No range	<div style="width: 100%;"><div style="width: 100%; background-color: #0072bc; height: 10px;"></div><div style="width: 10px; background-color: white; height: 10px; float: right;">3</div></div>

Open ports

4. Under **Request access**, for each VM, configure the ports that you want to open and the source IP addresses that the port is opened on and the time window for which the port will be open. It will only be possible to request access to the ports that are configured in the just-in-time policy. Each port has a maximum allowed time derived from the just-in-time policy.

5. Click **Open ports**.

NOTE

If a user who is requesting access is behind a proxy, the option **My IP** may not work. You may need to define the full IP address range of the organization.

Edit a JIT access policy via Security Center

You can change a VM's existing just-in-time policy by adding and configuring a new port to protect for that VM, or by changing any other setting related to an already protected port.

To edit an existing just-in-time policy of a VM:

1. In the **Configured** tab, under **VMs**, select a VM to which to add a port by clicking on the three dots within the row for that VM.
2. Select **Edit**.
3. Under **JIT VM access configuration**, you can either edit the existing settings of an already protected port or add a new custom port.

The screenshot shows two side-by-side interface panels. The left panel is titled 'Just in time VM access' and displays information about JIT VM access, including its definition and how it works. It also lists 'Virtual machines' with a 'Configured' tab selected (highlighted with a red box). The right panel is titled 'JIT VM access configuration' and shows a table of ports configured for JIT access. A context menu is open over the first row of the table, with the 'Edit' option highlighted (also highlighted with a red box).

PORT	PROT...	ALLOWED SOU...	IP RANGE	TIME RANGE	...
22	Any	Per request	N/A	3 hours	...
3389	Any	Per request	N/A	3 hours	...

Audit JIT access activity in Security Center

You can gain insights into VM activities using log search. To view logs:

1. Under **Just-in-time VM access**, select the **Configured** tab.
2. Under **VMs**, select a VM to view information about by clicking on the three dots within the row for that VM and select **Activity Log** from the menu. The **Activity log** opens.

Just in time VM access

Last week

What is just in time VM access?

Just in time VM access enables you to lock down your VMs in the network level by blocking inbound traffic to specific ports. It enables you to control the access and reduce the attack surface to your VMs, by allowing access only upon a specific need.

How does it work?

Upon a user request, based on Azure RBAC, Security Center will decide whether to grant access. If a request is approved, Security Center automatically configures the NSGs to allow inbound traffic to these ports, for only 3 hours, after which it restores the NSGs to their previous states.

For more information go to the documentation >

Virtual machines

Configured Recommended No recommendation

VMs for which the just in time VM access control is already in place. Presented data is for the last week.

5 VMs

Request access

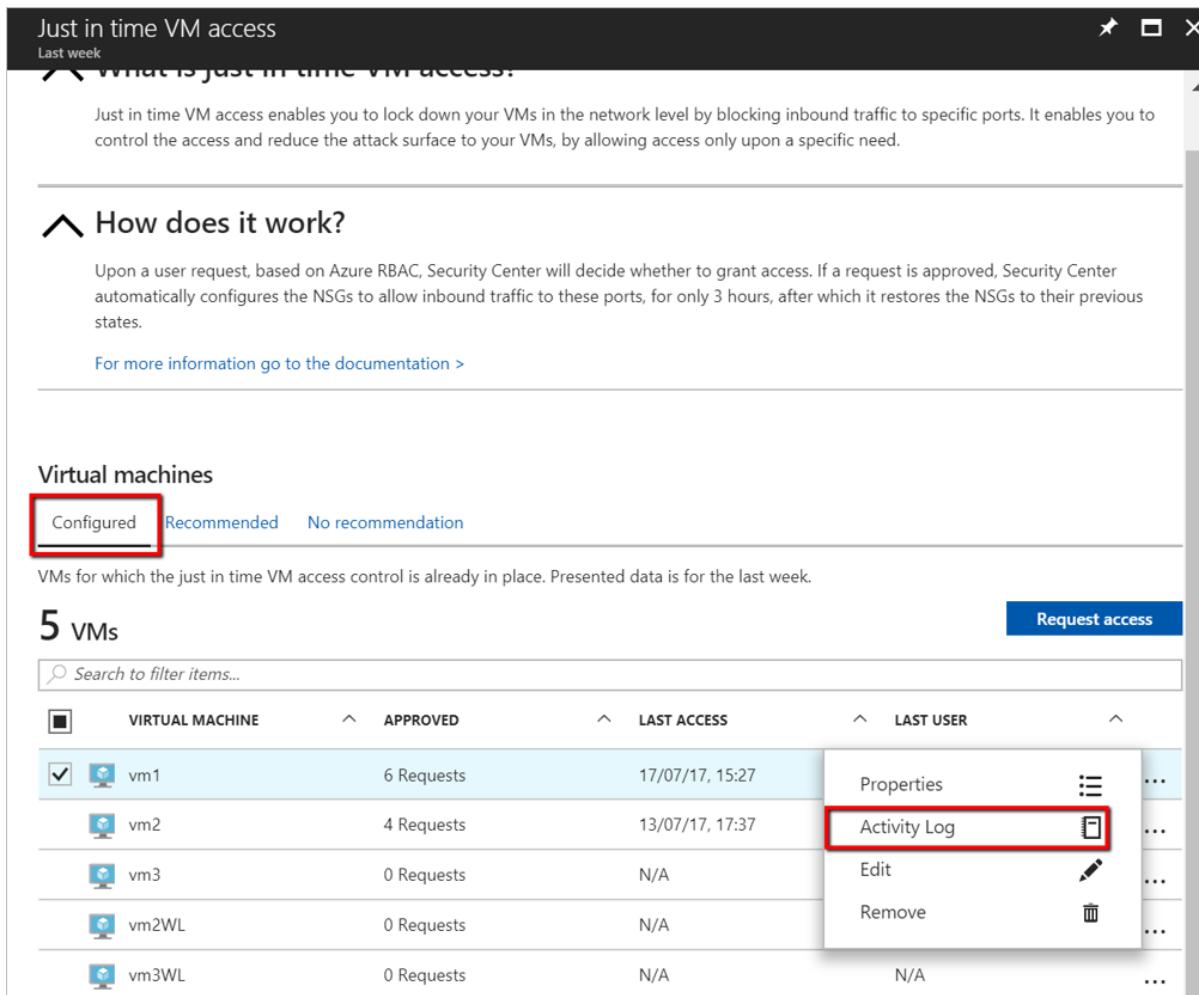
Search to filter items...

	VIRTUAL MACHINE	APPROVED	LAST ACCESS	LAST USER	
<input checked="" type="checkbox"/>	vm1	6 Requests	17/07/17, 15:27		Properties
<input type="checkbox"/>	vm2	4 Requests	13/07/17, 17:37		Activity Log
<input type="checkbox"/>	vm3	0 Requests	N/A		Edit
<input type="checkbox"/>	vm2WL	0 Requests	N/A		Remove
<input type="checkbox"/>	vm3WL	0 Requests	N/A		...

Activity log provides a filtered view of previous operations for that VM along with time, date, and subscription.

You can download the log information by selecting [Click here to download all the items as CSV](#).

Modify the filters and click **Apply** to create a search and log.



Configure JIT access from an Azure VM's page

For your convenience, you can connect to a VM using JIT directly from within the VM's page in Security Center.

Configure JIT access on a VM via the Azure VM page

To make it easy to roll out just-in-time access across your VMs, you can set a VM to allow only just-in-time access directly from within the VM.

1. From the [Azure portal](#), search for and select **Virtual machines**.
2. Select the virtual machine you want to limit to just-in-time access.
3. In the menu, select **Configuration**.
4. Under **Just-in-time access**, select **Enable just-in-time**.

This enables just-in-time access for the VM using the following settings:

- Windows servers:
 - RDP port 3389
 - Three hours of maximum allowed access
 - Allowed source IP addresses is set to Any
- Linux servers:
 - SSH port 22
 - Three hours of maximum allowed access
 - Allowed source IP addresses is set to Any

If a VM already has just-in-time enabled, when you go to its configuration page you will be able to see that just-in-time is

enabled and you can use the link to open the policy in Azure Security Center to view and change the settings.

The screenshot shows the Azure portal interface for managing virtual machines. On the left, a sidebar lists several VMs: vm-usa, vm-contoso-us (selected and highlighted with a red box), vm-europe, vm-contoso1, vm-contoso2, vmcontoso-3, vm-contoso4, vm-london, vm-marketing, vm-hr, vm-uni, vm-contoso-hr, and vm-contoso. The main pane is titled "vm-contoso-us - Configuration". It includes a search bar, save and discard buttons, and a "Just-in-time access" section with a call-to-action button "Enable just-in-time policy" (also highlighted with a red box). Below this are sections for "Azure hybrid benefit" (with "Use existing Windows license" options) and "Settings" (Networking, Disks, Size, Security, Extensions, Continuous delivery (Preview), Availability set, Configuration, and Identity (Preview)).

Request JIT access to a VM via an Azure VM's page

In the Azure portal, when you try to connect to a VM, Azure checks to see if you have a just-in-time access policy configured on that VM.

- If you have a JIT policy configured on the VM, you can click **Request access** to grant access in accordance with the JIT policy set for the VM.

Connect to virtual machine

X

vm1



This VM has a just-in-time access policy. Select "Request access" before connecting.

RDP

SSH

You need to request access to connect to your virtual machine. Select an IP address, optionally change the port number, and select "Request access". [Learn more](#)

o

* IP address

Public IP address (52.161.18.9)



* Port number

3389

Request access

[Download RDP file anyway](#)

Having trouble connecting to this VM?

- [Diagnose and solve problems](#)
- [Troubleshoot connection](#)
- [Serial console](#)

Access is requested with the following default parameters:

- o **source IP:** 'Any' (*) (cannot be changed)
- o **time range:** Three hours (cannot be changed)
- o **port number** RDP port 3389 for Windows / port 22 for Linux (can be changed)

NOTE

After a request is approved for a VM protected by Azure Firewall, Security Center provides the user with the proper connection details (the port mapping from the DNAT table) to use to connect to the VM.

- If you do not have JIT configured on a VM, you will be prompted to configure a JIT policy on it.

Connect to virtual machine

ContosoAppSrv2

To improve security, enable just-in-time access on this VM.

RDP **SSH**

To connect to your virtual machine via RDP, select an IP address, optionally change the port number, and download the RDP file.

* IP address
Public IP address (40.124.37.238)

* Port number
3389

Download RDP File

i Inbound traffic to the Public IP address may be blocked. You can update inbound port rules in the **VM Networking** page.

wrench You can troubleshoot VM connection issues by opening the **Diagnose and solve problems** page.

Configure a JIT policy on a VM programmatically

You can set up and use just-in-time via REST APIs and via PowerShell.

JIT VM access via REST APIs

The just-in-time VM access feature can be used via the Azure Security Center API. You can get information about configured VMs, add new ones, request access to a VM, and more, via this API. See [Jit Network Access Policies](#), to learn more about the just-in-time REST API.

JIT VM access via PowerShell

To use the just-in-time VM access solution via PowerShell, use the official Azure Security Center PowerShell cmdlets, and specifically `Set-AzJitNetworkAccessPolicy`.

The following example sets a just-in-time VM access policy on a specific VM, and sets the following:

1. Close ports 22 and 3389.
2. Set a maximum time window of 3 hours for each so they can be opened per approved request.
3. Allows the user who is requesting access to control the source IP addresses and allows the user to establish a successful session upon an approved just-in-time access request.

Run the following in PowerShell to accomplish this:

1. Assign a variable that holds the just-in-time VM access policy for a VM:

```
$JitPolicy = (@{
    id="/subscriptions/SUBSCRIPTIONID/resourceGroups/RESOURCEGROUP/providers/Microsoft.Compute/virtualMachines/VMNAME"
    "
    ports=@{
        number=22;
        protocol="*";
        allowedSourceAddressPrefix=@("*.");
        maxRequestAccessDuration="PT3H"},

        @{
            number=3389;
            protocol="*";
            allowedSourceAddressPrefix=@("*.");
            maxRequestAccessDuration="PT3H"})})
```

2. Insert the VM just-in-time VM access policy to an array:

```
$JitPolicyArr=@($JitPolicy)
```

3. Configure the just-in-time VM access policy on the selected VM:

```
Set-AzJitNetworkAccessPolicy -Kind "Basic" -Location "LOCATION" -Name "default" -ResourceGroupName "RESOURCEGROUP"
-VirtualMachine $JitPolicyArr
```

Request access to a VM via PowerShell

In the following example, you can see a just-in-time VM access request to a specific VM in which port 22 is requested to be opened for a specific IP address and for a specific amount of time:

Run the following in PowerShell:

1. Configure the VM request access properties

```
$JitPolicyVm1 = (@{
    id="/SUBSCRIPTIONID/resourceGroups/RESOURCEGROUP/providers/Microsoft.Compute/virtualMachines/VMNAME"
    ports=@{
        number=22;
        endTimeUtc="2018-09-17T17:00:00.3658798Z";
        allowedSourceAddressPrefix=@("IPV4ADDRESS"))})
```

2. Insert the VM access request parameters in an array:

```
$JitPolicyArr=@($JitPolicyVm1)
```

3. Send the request access (use the resource ID you got in step 1)

```
Start-AzJitNetworkAccessPolicy -ResourceId
"/subscriptions/SUBSCRIPTIONID/resourceGroups/RESOURCEGROUP/providers/Microsoft.Security/locations/LOCATION/jitNet
workAccessPolicies/default" -VirtualMachine $JitPolicyArr
```

For more information, see the [PowerShell cmdlet documentation](#).

Automatic cleanup of redundant JIT rules

Whenever you update a JIT policy, a cleanup tool automatically runs to check the validity of your entire ruleset. The tool looks for mismatches between rules in your policy and rules in the NSG. If the cleanup tool finds a mismatch, it determines the cause and, when it's safe to do so, removes built-in rules that aren't needed any more. The cleaner never deletes rules that you've created.

Examples scenarios when the cleaner might remove a built-in rule:

- When two rules with identical definitions exist and one has a higher priority than the other (meaning, the lower priority

rule will never be used)

- When a rule description includes the name of a VM which doesn't match the destination IP in the rule

Next steps

In this article, you learned how just-in-time VM access in Security Center helps you control access to your Azure virtual machines.

To learn more about Security Center, see the following:

- [Setting security policies](#) — Learn how to configure security policies for your Azure subscriptions and resource groups.
- [Managing security recommendations](#) — Learn how recommendations help you protect your Azure resources.
- [Security health monitoring](#) — Learn how to monitor the health of your Azure resources.

Azure Disk Encryption scenarios on Linux VMs

12/23/2019 • 16 minutes to read • [Edit Online](#)

Azure Disk Encryption uses the DM-Crypt feature of Linux to provide volume encryption for the OS and data disks of Azure virtual machines (VMs), and is integrated with Azure Key Vault to help you control and manage the disk encryption keys and secrets. For an overview of the service, see [Azure Disk Encryption for Linux VMs](#).

There are many disk encryption scenarios, and the steps may vary according to the scenario. The following sections cover the scenarios in greater detail for Linux VMs.

You can only apply disk encryption to virtual machines of [supported VM sizes and operating systems](#). You must also meet the following prerequisites:

- [Additional requirements for VMs](#)
- [Networking requirements](#)
- [Encryption key storage requirements](#)

In all cases, you should [take a snapshot](#) and/or create a backup before disks are encrypted. Backups ensure that a recovery option is possible if an unexpected failure occurs during encryption. VMs with managed disks require a backup before encryption occurs. Once a backup is made, you can use the [Set-AzVMDiskEncryptionExtension cmdlet](#) to encrypt managed disks by specifying the `-skipVmBackup` parameter. For more information about how to back up and restore encrypted VMs, see the [Azure Backup](#) article.

WARNING

- If you have previously used Azure Disk Encryption with Azure AD to encrypt a VM, you must continue use this option to encrypt your VM. See [Azure Disk Encryption with Azure AD \(previous release\)](#) for details.
- When encrypting Linux OS volumes, the VM should be considered unavailable. We strongly recommend to avoid SSH logins while the encryption is in progress to avoid issues blocking any open files that will need to be accessed during the encryption process. To check progress, use the [Get-AzVMDiskEncryptionStatus](#) PowerShell cmdlet or the [vm encryption show](#) CLI command. This process can be expected to take a few hours for a 30GB OS volume, plus additional time for encrypting data volumes. Data volume encryption time will be proportional to the size and quantity of the data volumes unless the `encrypt format all` option is used.
- Disabling encryption on Linux VMs is only supported for data volumes. It is not supported on data or OS volumes if the OS volume has been encrypted.

Install tools and connect to Azure

Azure Disk Encryption can be enabled and managed through the [Azure CLI](#) and [Azure PowerShell](#). To do so you must install the tools locally and connect to your Azure subscription.

Azure CLI

The [Azure CLI 2.0](#) is a command-line tool for managing Azure resources. The CLI is designed to flexibly query data, support long-running operations as non-blocking processes, and make scripting easy. You can install it locally by following the steps in [Install the Azure CLI](#).

To [Sign in to your Azure account with the Azure CLI](#), use the `az login` command.

```
az login
```

If you would like to select a tenant to sign in under, use:

```
az login --tenant <tenant>
```

If you have multiple subscriptions and want to specify a specific one, get your subscription list with [az account list](#) and specify with [az account set](#).

```
az account list  
az account set --subscription "<subscription name or ID>"
```

For more information, see [Get started with Azure CLI 2.0](#).

Azure PowerShell

The [Azure PowerShell az module](#) provides a set of cmdlets that uses the [Azure Resource Manager](#) model for managing your Azure resources. You can use it in your browser with [Azure Cloud Shell](#), or you can install it on your local machine using the instructions in [Install the Azure PowerShell module](#).

If you already have it installed locally, make sure you use the latest version of Azure PowerShell SDK version to configure Azure Disk Encryption. Download the latest version of [Azure PowerShell release](#).

To [Sign in to your Azure account with Azure PowerShell](#), use the `Connect-AzAccount` cmdlet.

```
Connect-AzAccount
```

If you have multiple subscriptions and want to specify one, use the [Get-AzSubscription](#) cmdlet to list them, followed by the [Set-AzContext](#) cmdlet:

```
Set-AzContext -Subscription -Subscription <SubscriptionId>
```

Running the [Get-AzContext](#) cmdlet will verify that the correct subscription has been selected.

To confirm the Azure Disk Encryption cmdlets are installed, use the [Get-command](#) cmdlet:

```
Get-command *diskencryption*
```

For more information, see [Getting started with Azure PowerShell](#).

Enable encryption on an existing or running Linux VM

In this scenario, you can enable encryption by using the Resource Manager template, PowerShell cmdlets, or CLI commands. If you need schema information for the virtual machine extension, see the [Azure Disk Encryption for Linux extension](#) article.

IMPORTANT

It is mandatory to snapshot and/or backup a managed disk based VM instance outside of, and prior to enabling Azure Disk Encryption. A snapshot of the managed disk can be taken from the portal, or through [Azure Backup](#). Backups ensure that a recovery option is possible in the case of any unexpected failure during encryption. Once a backup is made, the `Set-AzVMDiskEncryptionExtension` cmdlet can be used to encrypt managed disks by specifying the `-skipVmBackup` parameter. The `Set-AzVMDiskEncryptionExtension` command will fail against managed disk based VMs until a backup has been made and this parameter has been specified.

Encrypting or disabling encryption may cause the VM to reboot.

Enable encryption on an existing or running Linux VM using Azure CLI

You can enable disk encryption on your encrypted VHD by installing and using the [Azure CLI](#) command-line tool. You can use it in your browser with [Azure Cloud Shell](#), or you can install it on your local machine and use it in any PowerShell session. To enable encryption on existing or running Linux VMs in Azure, use the following CLI commands:

Use the `az vm encryption enable` command to enable encryption on a running virtual machine in Azure.

- **Encrypt a running VM:**

```
az vm encryption enable --resource-group "MyVirtualMachineResourceGroup" --name "MySecureVM" --disk-encryption-keyvault "MySecureVault" --volume-type [All|OS|Data]
```

- **Encrypt a running VM using KEK:**

```
az vm encryption enable --resource-group "MyVirtualMachineResourceGroup" --name "MySecureVM" --disk-encryption-keyvault "MySecureVault" --key-encryption-key "MyKEK_URI" --key-encryption-keyvault "MySecureVaultContainingTheKEK" --volume-type [All|OS|Data]
```

NOTE

The syntax for the value of `disk-encryption-keyvault` parameter is the full identifier string:

/subscriptions/[subscription-id-guid]/resourceGroups/[resource-group-name]/providers/Microsoft.KeyVault/vaults/[keyvault-name]

The syntax for the value of the `key-encryption-key` parameter is the full URI to the KEK as in: [https://\[keyvault-name\].vault.azure.net/keys/\[kekname\]/\[kek-unique-id\]](https://[keyvault-name].vault.azure.net/keys/[kekname]/[kek-unique-id])

- **Verify the disks are encrypted:** To check on the encryption status of a VM, use the `az vm encryption show` command.

```
az vm encryption show --name "MySecureVM" --resource-group "MyVirtualMachineResourceGroup"
```

- **Disable encryption:** To disable encryption, use the `az vm encryption disable` command. Disabling encryption is only allowed on data volumes for Linux VMs.

```
az vm encryption disable --name "MySecureVM" --resource-group "MyVirtualMachineResourceGroup" --volume-type DATA
```

Enable encryption on an existing or running Linux VM using PowerShell

Use the `Set-AzVMDiskEncryptionExtension` cmdlet to enable encryption on a running virtual machine in Azure. Take a [snapshot](#) and/or back up the VM with [Azure Backup](#) before disks are encrypted. The `-skipVmBackup`

parameter is already specified in the PowerShell scripts to encrypt a running Linux VM.

- **Encrypt a running VM:** The script below initializes your variables and runs the Set-AzVMDiskEncryptionExtension cmdlet. The resource group, VM, and key vault, were created as prerequisites. Replace MyVirtualMachineResourceGroup, MySecureVM, and MySecureVault with your values. Modify the -VolumeType parameter to specify which disks you're encrypting.

```
$KVRGname = 'MyKeyVaultResourceGroup';
$VMRGName = 'MyVirtualMachineResourceGroup';
$vmName = 'MySecureVM';
$keyVaultName = 'MySecureVault';
$keyVault = Get-AzKeyVault -VaultName $keyVaultName -ResourceGroupName $KVRGname;
$diskEncryptionKeyVaultUrl = $keyVault.VaultUri;
$keyVaultResourceId = $keyVault.ResourceId;
$sequenceVersion = [Guid]::NewGuid();

Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGName -VMName $vmName -
DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl -DiskEncryptionKeyVaultId $keyVaultResourceId -
VolumeType '[All|OS|Data]' -SequenceVersion $sequenceVersion -skipVmBackup;
```

- **Encrypt a running VM using KEK:** You may need to add the -VolumeType parameter if you're encrypting data disks and not the OS disk.

```
$KVRGname = 'MyKeyVaultResourceGroup';
$VMRGName = 'MyVirtualMachineResourceGroup';
$vmName = 'MyExtraSecureVM';
$keyVaultName = 'MySecureVault';
$keyEncryptionKeyName = 'MyKeyEncryptionKey';
$keyVault = Get-AzKeyVault -VaultName $keyVaultName -ResourceGroupName $KVRGname;
$diskEncryptionKeyVaultUrl = $keyVault.VaultUri;
$keyVaultResourceId = $keyVault.ResourceId;
$keyEncryptionKeyUrl = (Get-AzKeyVaultKey -VaultName $keyVaultName -Name
$keyEncryptionKeyName).Key.kid;
$sequenceVersion = [Guid]::NewGuid();

Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGName -VMName $vmName -
DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl -DiskEncryptionKeyVaultId $keyVaultResourceId -
KeyEncryptionKeyUrl $keyEncryptionKeyUrl -KeyEncryptionKeyVaultId $keyVaultResourceId -VolumeType
'[All|OS|Data]' -SequenceVersion $sequenceVersion -skipVmBackup;
```

NOTE

The syntax for the value of disk-encryption-keyvault parameter is the full identifier string:

/subscriptions/[subscription-id-guid]/resourceGroups/[resource-group-name]/providers/Microsoft.KeyVault/vaults/[keyvault-name]

The syntax for the value of the key-encryption-key parameter is the full URI to the KEK as in: https://[keyvault-name].vault.azure.net/keys/[kekname]/[kek-unique-id]

- **Verify the disks are encrypted:** To check on the encryption status of a VM, use the [Get-AzVmDiskEncryptionStatus](#) cmdlet.

```
Get-AzVmDiskEncryptionStatus -ResourceGroupName 'MyVirtualMachineResourceGroup' -VMName 'MySecureVM'
```

- **Disable disk encryption:** To disable the encryption, use the [Disable-AzVMDiskEncryption](#) cmdlet. Disabling encryption is only allowed on data volumes for Linux VMs.

```
Disable-AzVMDiskEncryption -ResourceGroupName 'MyVirtualMachineResourceGroup' -VMName 'MySecureVM'
```

Enable encryption on an existing or running Linux VM with a template

You can enable disk encryption on an existing or running Linux VM in Azure by using the [Resource Manager template](#).

1. Click **Deploy to Azure** on the Azure quickstart template.
2. Select the subscription, resource group, resource group location, parameters, legal terms, and agreement. Click **Create** to enable encryption on the existing or running VM.

The following table lists Resource Manager template parameters for existing or running VMs:

PARAMETER	DESCRIPTION
vmName	Name of the VM to run the encryption operation.
keyVaultName	Name of the key vault that the encryption key should be uploaded to. You can get it by using the cmdlet <code>(Get-AzKeyVault -ResourceGroupName <MyKeyVaultResourceGroupName>). Vaultname</code> or the Azure CLI command <code>az keyvault list --resource-group "MyKeyVaultResourceGroupName"</code>
keyVaultResourceGroup	Name of the resource group that contains the key vault.
keyEncryptionKeyURL	URL of the key encryption key that's used to encrypt the encryption key. This parameter is optional if you select nokek in the UseExistingKek drop-down list. If you select kek in the UseExistingKek drop-down list, you must enter the <i>keyEncryptionKeyURL</i> value.
volumeType	Type of volume that the encryption operation is performed on. Valid values are <i>OS</i> , <i>Data</i> , and <i>All</i> .
forceUpdateTag	Pass in a unique value like a GUID every time the operation needs to be force run.
resizeOSDisk	Should the OS partition be resized to occupy full OS VHD before splitting system volume.
location	Location for all resources.

Use EncryptFormatAll feature for data disks on Linux VMs

The **EncryptFormatAll** parameter reduces the time for Linux data disks to be encrypted. Partitions meeting certain criteria will be formatted (with its current file system), then remounted back to where it was before command execution. If you wish to exclude a data disk that meets the criteria, you can unmount it before running the command.

After running this command, any drives that were mounted previously will be reformatted, and the encryption layer will be started on top of the now empty drive. When this option is selected, the ephemeral resource disk attached to the VM will also be encrypted. If the ephemeral drive is reset, it will be reformatted and re-encrypted for the VM by the Azure Disk Encryption solution at the next opportunity. Once the resource disk gets encrypted, the

Microsoft Azure Linux Agent will not be able to manage the resource disk and enable the swap file, but you may manually configure the swap file.

WARNING

EncryptFormatAll shouldn't be used when there is needed data on a VM's data volumes. You may exclude disks from encryption by unmounting them. You should first try out the EncryptFormatAll first on a test VM, understand the feature parameter and its implication before trying it on the production VM. The EncryptFormatAll option formats the data disk and all the data on it will be lost. Before proceeding, verify that disks you wish to exclude are properly unmounted.

If you're setting this parameter while updating encryption settings, it might lead to a reboot before the actual encryption. In this case, you will also want to remove the disk you don't want formatted from the fstab file. Similarly, you should add the partition you want encrypt-formatted to the fstab file before initiating the encryption operation.

EncryptFormatAll criteria

The parameter goes through all partitions and encrypts them as long as they meet **all** of the criteria below:

- Is not a root/OS/boot partition
- Is not already encrypted
- Is not a BEK volume
- Is not a RAID volume
- Is not an LVM volume
- Is mounted

Encrypt the disks that compose the RAID or LVM volume rather than the RAID or LVM volume.

Use the EncryptFormatAll parameter with Azure CLI

Use the [az vm encryption enable](#) command to enable encryption on a running virtual machine in Azure.

- **Encrypt a running VM using EncryptFormatAll:**

```
az vm encryption enable --resource-group "MyVirtualMachineResourceGroup" --name "MySecureVM" --disk-  
encryption-keyvault "MySecureVault" --encrypt-format-all
```

Use the EncryptFormatAll parameter with a PowerShell cmdlet

Use the [Set-AzVMDiskEncryptionExtension](#) cmdlet with the EncryptFormatAll parameter.

Encrypt a running VM using EncryptFormatAll: As an example, the script below initializes your variables and runs the Set-AzVMDiskEncryptionExtension cmdlet with the EncryptFormatAll parameter. The resource group, VM, and key vault were created as prerequisites. Replace MyVirtualMachineResourceGroup, MySecureVM, and MySecureVault with your values.

```
$KVRGname = 'MyKeyVaultResourceGroup';  
$VMRGName = 'MyVirtualMachineResourceGroup';  
$vmName = 'MySecureVM';  
$KeyVaultName = 'MySecureVault';  
$KeyVault = Get-AzKeyVault -VaultName $KeyVaultName -ResourceGroupName $KVRGname;  
$diskEncryptionKeyVaultUrl = $KeyVault.VaultUri;  
$KeyVaultResourceId = $KeyVault.ResourceId;  
  
Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGName -VMName $vmName -DiskEncryptionKeyVaultUrl  
$diskEncryptionKeyVaultUrl -DiskEncryptionKeyId $KeyVaultResourceId -EncryptFormatAll
```

Use the EncryptFormatAll parameter with Logical Volume Manager (LVM)

We recommend an LVM-on-crypt setup. For all the following examples, replace the device-path and mountpoints with whatever suits your use-case. This setup can be done as follows:

- Add the data disks that will compose the VM.
- Format, mount, and add these disks to the fstab file.
 1. Format the newly added disk. We use symlinks generated by Azure here. Using symlinks avoids problems related to device names changing. For more information, see the [Troubleshoot Device Names problems](#) article.

```
mkfs -t ext4 /dev/disk/azure/scsi1/lun0
```

2. Mount the disks.

```
mount /dev/disk/azure/scsi1/lun0 /mnt/mountpoint
```

3. Add to fstab.

```
echo "/dev/disk/azure/scsi1/lun0 /mnt/mountpoint ext4 defaults,nofail 1 2" >> /etc/fstab
```

4. Run the Set-AzVMDiskEncryptionExtension PowerShell cmdlet with -EncryptFormatAll to encrypt these disks.

```
$KeyVault = Get-AzKeyVault -VaultName "MySecureVault" -ResourceGroupName "MySecureGroup"

Set-AzVMDiskEncryptionExtension -ResourceGroupName "MySecureGroup" -VMName "MySecureVM" -
DiskEncryptionKeyVaultUrl $KeyVault.VaultUri -DiskEncryptionKeyId $KeyVault.ResourceId -
EncryptFormatAll -SkipVmBackup -VolumeType Data
```

5. Set up LVM on top of these new disks. Note the encrypted drives are unlocked after the VM has finished booting. So, the LVM mounting will also have to be subsequently delayed.

New VMs created from customer-encrypted VHD and encryption keys

In this scenario, you can enable encrypting by using PowerShell cmdlets or CLI commands.

Use the instructions in the Azure Disk encryption same scripts for preparing pre-encrypted images that can be used in Azure. After the image is created, you can use the steps in the next section to create an encrypted Azure VM.

- [Prepare a pre-encrypted Linux VHD](#)

IMPORTANT

It is mandatory to snapshot and/or backup a managed disk based VM instance outside of, and prior to enabling Azure Disk Encryption. A snapshot of the managed disk can be taken from the portal, or [Azure Backup](#) can be used. Backups ensure that a recovery option is possible in the case of any unexpected failure during encryption. Once a backup is made, the Set-AzVMDiskEncryptionExtension cmdlet can be used to encrypt managed disks by specifying the -skipVmBackup parameter. The Set-AzVMDiskEncryptionExtension command will fail against managed disk based VMs until a backup has been made and this parameter has been specified.

Encrypting or disabling encryption may cause the VM to reboot.

Use Azure PowerShell to encrypt VMs with pre-encrypted VHDS

You can enable disk encryption on your encrypted VHD by using the PowerShell cmdlet [Set-AzVMOSDisk](#). The example below gives you some common parameters.

```
$VirtualMachine = New-AzVMConfig -VMName "MySecureVM" -VMSize "Standard_A1"
$VirtualMachine = Set-AzVMOSDisk -VM $VirtualMachine -Name "SecureOSDisk" -VhdUri "os.vhd" Caching ReadWrite -
Linux -CreateOption "Attach" -DiskEncryptionKeyUrl
"https://mytestvault.vault.azure.net/secrets/Test1/514ceb769c984379a7e0230bddaaaaaa" -DiskEncryptionKeyVaultId
"/subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/myresourcegroup/providers/Microsoft.KeyVault/vaults/mytestvault"
New-AzVM -VM $VirtualMachine -ResourceGroupName "MyVirtualMachineResourceGroup"
```

Enable encryption on a newly added data disk

You can add a new data disk using [az vm disk attach](#), or [through the Azure portal](#). Before you can encrypt, you need to mount the newly attached data disk first. You must request encryption of the data drive since the drive will be unusable while encryption is in progress.

Enable encryption on a newly added disk with Azure CLI

If the VM was previously encrypted with "All" then the --volume-type parameter should remain "All". All includes both OS and data disks. If the VM was previously encrypted with a volume type of "OS", then the --volume-type parameter should be changed to "All" so that both the OS and the new data disk will be included. If the VM was encrypted with only the volume type of "Data", then it can remain "Data" as demonstrated below. Adding and attaching a new data disk to a VM is not sufficient preparation for encryption. The newly attached disk must also be formatted and properly mounted within the VM prior to enabling encryption. On Linux the disk must be mounted in /etc/fstab with a [persistent block device name](#).

In contrast to Powershell syntax, the CLI does not require the user to provide a unique sequence version when enabling encryption. The CLI automatically generates and uses its own unique sequence version value.

- Encrypt data volumes of a running VM:**

```
az vm encryption enable --resource-group "MyVirtualMachineResourceGroup" --name "MySecureVM" --disk-
encryption-keyvault "MySecureVault" --volume-type "Data"
```

- Encrypt data volumes of a running VM using KEK:**

```
az vm encryption enable --resource-group "MyVirtualMachineResourceGroup" --name "MySecureVM" --disk-
encryption-keyvault "MySecureVault" --key-encryption-key "MyKEK_URI" --key-encryption-keyvault
"MySecureVaultContainingTheKEK" --volume-type "Data"
```

Enable encryption on a newly added disk with Azure PowerShell

When using Powershell to encrypt a new disk for Linux, a new sequence version needs to be specified. The sequence version has to be unique. The script below generates a GUID for the sequence version. Take a [snapshot](#) and/or back up the VM with [Azure Backup](#) before disks are encrypted. The -skipVmBackup parameter is already specified in the PowerShell scripts to encrypt a newly added data disk.

- Encrypt data volumes of a running VM:** The script below initializes your variables and runs the Set-AzVMDiskEncryptionExtension cmdlet. The resource group, VM, and key vault should have already been created as prerequisites. Replace MyVirtualMachineResourceGroup, MySecureVM, and MySecureVault with your values. Acceptable values for the -VolumeType parameter are All, OS, and Data. If the VM was previously encrypted with a volume type of "OS" or "All", then the -VolumeType parameter should be changed to "All" so that both the OS and the new data disk will be included.

```

$KVRGname = 'MyKeyVaultResourceGroup';
$VMRGName = 'MyVirtualMachineResourceGroup';
$vmName = 'MySecureVM';
$keyVaultName = 'MySecureVault';
$keyVault = Get-AzKeyVault -VaultName $keyVaultName -ResourceGroupName $KVRGname;
$diskEncryptionKeyVaultUrl = $keyVault.VaultUri;
$keyVaultResourceId = $keyVault.ResourceId;
$sequenceVersion = [Guid]::.NewGuid();

Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGName -VMName $vmName -DiskEncryptionKeyVaultUrl
$diskEncryptionKeyVaultUrl -DiskEncryptionKeyId $keyVaultResourceId -VolumeType 'data' -
SequenceVersion $sequenceVersion -skipVmBackup;

```

- **Encrypt data volumes of a running VM using KEK:** Acceptable values for the -VolumeType parameter are All, OS, and Data. If the VM was previously encrypted with a volume type of "OS" or "All", then the -VolumeType parameter should be changed to All so that both the OS and the new data disk will be included.

```

$KVRGname = 'MyKeyVaultResourceGroup';
$VMRGName = 'MyVirtualMachineResourceGroup';
$vmName = 'MyExtraSecureVM';
$keyVaultName = 'MySecureVault';
$keyEncryptionKeyName = 'MyKeyEncryptionKey';
$keyVault = Get-AzKeyVault -VaultName $keyVaultName -ResourceGroupName $KVRGname;
$diskEncryptionKeyVaultUrl = $keyVault.VaultUri;
$keyVaultResourceId = $keyVault.ResourceId;
$keyEncryptionKeyUrl = (Get-AzKeyVaultKey -VaultName $keyVaultName -Name
$keyEncryptionKeyName).Key.kid;
$sequenceVersion = [Guid]::.NewGuid();

Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGName -VMName $vmName -
DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl -DiskEncryptionKeyId $keyVaultResourceId -
KeyEncryptionKeyUrl $keyEncryptionKeyUrl -KeyEncryptionKeyId $keyVaultResourceId -VolumeType
'data' -SequenceVersion $sequenceVersion -skipVmBackup;

```

NOTE

The syntax for the value of disk-encryption-keyvault parameter is the full identifier string:

/subscriptions/[subscription-id-guid]/resourceGroups/[KVresource-group-name]/providers/Microsoft.KeyVault/vaults/[keyvault-name]

The syntax for the value of the key-encryption-key parameter is the full URI to the KEK as in: https://[keyvault-name].vault.azure.net/keys/[kekname]/[kek-unique-id]

Disable encryption for Linux VMs

You can disable encryption using Azure PowerShell, the Azure CLI, or with a Resource Manager template.

IMPORTANT

Disabling encryption with Azure Disk Encryption on Linux VMs is only supported for data volumes. It is not supported on data or OS volumes if the OS volume has been encrypted.

- **Disable disk encryption with Azure PowerShell:** To disable the encryption, use the [Disable-AzVMDiskEncryption](#) cmdlet.

```
Disable-AzVMDiskEncryption -ResourceGroupName 'MyVirtualMachineResourceGroup' -VMName 'MySecureVM' [-VolumeType {ALL, DATA, OS}]
```

- **Disable encryption with the Azure CLI:** To disable encryption, use the [az vm encryption disable](#) command.

```
az vm encryption disable --name "MySecureVM" --resource-group "MyVirtualMachineResourceGroup" --volume-type [ALL, DATA, OS]
```

- **Disable encryption with a Resource Manager template:** Use the [Disable encryption on a running Linux VM](#) template to disable encryption.

1. Click **Deploy to Azure**.
2. Select the subscription, resource group, location, VM, legal terms, and agreement.

Unsupported scenarios

Azure Disk Encryption does not work for the following Linux scenarios, features, and technology:

- Encrypting basic tier VM or VMs created through the classic VM creation method.
- Disabling encryption on an OS drive or data drive of a Linux VM when the OS drive is encrypted.
- Encrypting OS drive for Linux virtual machine scale sets.
- Encrypting custom images on Linux VMs.
- Integration with an on-premises key management system.
- Azure Files (shared file system).
- Network File System (NFS).
- Dynamic volumes.
- Ephemeral OS disks.
- Encryption of shared/distributed file systems like (but not limited to): DFS, GFS, DRDB, and CephFS.
- Kernel Crash Dump (kdump).

Next steps

- [Azure Disk Encryption overview](#)
- [Azure Disk Encryption sample scripts](#)
- [Azure Disk Encryption troubleshooting](#)

Quickstart: Create and encrypt a Linux VM with the Azure CLI

1/8/2020 • 2 minutes to read • [Edit Online](#)

The Azure CLI is used to create and manage Azure resources from the command line or in scripts. This quickstart shows you how to use the Azure CLI to create and encrypt a Linux virtual machine (VM).

If you don't have an Azure subscription, create a [free account](#) before you begin.

If you choose to install and use the CLI locally, this quickstart requires that you are running the Azure CLI version 2.0.30 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Create a resource group

Create a resource group with the [az group create](#) command. An Azure resource group is a logical container into which Azure resources are deployed and managed. The following example creates a resource group named *myResourceGroup* in the *eastus* location:

```
az group create --name "myResourceGroup" --location "eastus"
```

Create a virtual machine

Create a VM with [az vm create](#). The following example creates a VM named *myVM*.

```
az vm create \
--resource-group "myResourceGroup" \
--name "myVM" \
--image "Canonical:UbuntuServer:16.04-LTS:latest" \
--size "Standard_D2S_V3" \
--generate-ssh-keys
```

It takes a few minutes to create the VM and supporting resources. The following example output shows the VM create operation was successful.

```
{
  "fqdns": "",
  "id": "/subscriptions/<guid>/resourceGroups/myResourceGroup/providers/Microsoft.Compute/virtualMachines/myVM",
  "location": "eastus",
  "macAddress": "00-0D-3A-23-9A-49",
  "powerState": "VM running",
  "privateIpAddress": "10.0.0.4",
  "publicIpAddress": "52.174.34.95",
  "resourceGroup": "myResourceGroup"
}
```

Create a Key Vault configured for encryption keys

Azure disk encryption stores its encryption key in an Azure Key Vault. Create a Key Vault with [az keyvault create](#). To enable the Key Vault to store encryption keys, use the `--enabled-for-disk-encryption` parameter.

IMPORTANT

Every key vault must have a name that is unique across Azure. In the examples below, replace with the name you choose.

```
az keyvault create --name "<your-unique-keyvault-name>" --resource-group "myResourceGroup" --location "eastus"  
--enabled-for-disk-encryption
```

Encrypt the virtual machine

Encrypt your VM with [az vm encryption](#), providing your unique Key Vault name to the --disk-encryption-keyvault parameter.

```
az vm encryption enable -g "MyResourceGroup" --name "myVM" --disk-encryption-keyvault "<your-unique-keyvault-name>"
```

After a moment the process will return, "The encryption request was accepted. Please use 'show' command to monitor the progress.". The "show" command is [az vm show](#).

```
az vm show --name "myVM" -g "MyResourceGroup"
```

When encryption is enabled, you will see the following in the returned output:

```
"EncryptionOperation": "EnableEncryption"
```

Clean up resources

When no longer needed, you can use the [az group delete](#) command to remove the resource group, VM, and Key Vault.

```
az group delete --name "myResourceGroup"
```

Next steps

In this quickstart, you created a virtual machine, created a Key Vault that was enable for encryption keys, and encrypted the VM. Advance to the next article to learn more about more Azure Disk Encryption for Linux VMs.

[Azure Disk Encryption overview](#)

Quickstart: Create and encrypt a Linux VM in Azure with Azure PowerShell

10/2/2019 • 2 minutes to read • [Edit Online](#)

The Azure PowerShell module is used to create and manage Azure resources from the PowerShell command line or in scripts. This quickstart shows you how to use the Azure PowerShell module to create a Linux virtual machine (VM), create a Key Vault for the storage of encryption keys, and encrypt the VM. This quickstart uses the Ubuntu 16.04 LTS marketplace image from Canonical and a VM Standard_D2S_V3 size.

If you don't have an Azure subscription, create a [free account](#) before you begin.

Create a resource group

Create an Azure resource group with [New-AzResourceGroup](#). A resource group is a logical container into which Azure resources are deployed and managed:

```
New-AzResourceGroup -Name "myResourceGroup" -Location "EastUS"
```

Create a virtual machine

Create an Azure virtual machine with [New-AzVM](#), passing to it the VM configuration object you created above.

```
$cred = Get-Credential  
  
New-AzVM -Name MyVm -Credential $cred -ResourceGroupName MyResourceGroup -Image Canonical:UbuntuServer:16.04-LTS:latest -Size Standard_D2S_V3
```

It will take a few minutes for your VM to be deployed.

Create a Key Vault configured for encryption keys

Azure disk encryption stores its encryption key in an Azure Key Vault. Create a Key Vault with [New-AzKeyVault](#). To enable the Key Vault to store encryption keys, use the `-EnabledForDiskEncryption` parameter.

IMPORTANT

Every key vault must have a name that is unique across Azure. In the examples below, replace with the name you choose.

```
New-AzKeyVault -name "<your-unique-keyvault-name>" -ResourceGroupName "myResourceGroup" -Location EastUS -EnabledForDiskEncryption
```

Encrypt the virtual machine

Encrypt your VM with [Set-AzVmDiskEncryptionExtension](#).

`Set-AzVmDiskEncryptionExtension` requires some values from your Key Vault object. You can obtain these values by passing the unique name of your key vault to [Get-AzKeyVault](#).

```
$KeyVault = Get-AzKeyVault -VaultName "<your-unique-keyvault-name>" -ResourceGroupName "MyResourceGroup"

Set-AzVMDiskEncryptionExtension -ResourceGroupName MyResourceGroup -VMName "MyVM" -DiskEncryptionKeyVaultUrl
$KeyVault.VaultUri -DiskEncryptionKeyId $KeyVault.ResourceId -SkipVmBackup -VolumeType All
```

After a few minutes the process will return the following:

RequestId	IsSuccess	Status	StatusCode	ReasonPhrase
	True	OK	OK	

You can verify the encryption process by running [Get-AzVmDiskEncryptionStatus](#).

```
Get-AzVmDiskEncryptionStatus -VMName MyVM -ResourceGroupName MyResourceGroup
```

When encryption is enabled, you will see the following in the returned output:

```
OsVolumeEncrypted      : EncryptionInProgress
DataVolumesEncrypted   : NotMounted
OsVolumeEncryptionSettings : Microsoft.Azure.Management.Compute.Models.DiskEncryptionSettings
ProgressMessage        : OS disk encryption started
```

Clean up resources

When no longer needed, you can use the [Remove-AzResourceGroup](#) cmdlet to remove the resource group, VM, and all related resources:

```
Remove-AzResourceGroup -Name "myResourceGroup"
```

Next steps

In this quickstart, you created a virtual machine, created a Key Vault that was enable for encryption keys, and encrypted the VM. Advance to the next article to learn more about Azure Disk Encryption for Linux VMs.

[Azure Disk Encryption overview](#)

Quickstart: Create and encrypt a virtual machine with the Azure portal

1/8/2020 • 2 minutes to read • [Edit Online](#)

Azure virtual machines (VMs) can be created through the Azure portal. The Azure portal is a browser-based user interface to create VMs and their associated resources. In this quickstart you will use the Azure portal to deploy a Linux virtual machine (VM) running Ubuntu 18.04 LTS, create a key vault for the storage of encryption keys, and encrypt the VM.

If you don't have an Azure subscription, create a [free account](#) before you begin.

Sign in to Azure

Sign in to the [Azure portal](#).

Create a virtual machine

1. Choose **Create a resource** in the upper left corner of the Azure portal.
2. In the New page, under Popular, select **Ubuntu Server 18.04 LTS**.
3. In the **Basics** tab, under **Project details**, make sure the correct subscription is selected.
4. For **Resource group**, select the resource group you created when making your key vault above (e.g., **myResourceGroup**).
5. For **Virtual machine name**, enter **MyVM**.
6. For **Region**, select the same region you used when making your key vault above (e.g., **East US**).
7. Make sure the **Size** is *Standard D2s v3*.
8. Under **Administrator account**, select **Password**. Enter a user name and a password.

Create a virtual machine

Looking for classic VMs? [Create VM from Azure Marketplace](#)

Project details

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

* Subscription [i](#)

Free Trial

 └ * Resource group [i](#)

myResourceGroup

[Create new](#)

Instance details

* Virtual machine name [i](#)

myVM

* Region [i](#)

(US) East US

Availability options [i](#)

No infrastructure redundancy required

* Image [i](#)

Ubuntu Server 18.04 LTS

[Browse all public and private images](#)

* Size [i](#)

Standard D2s v3

2 vcpus, 8 GiB memory

[Change size](#)

Administrator account

Authentication type [i](#)

Password SSH public key

* Username [i](#)

azureUser

* Password [i](#)

.....

* Confirm password [i](#)

.....

Review + create

[< Previous](#)

[Next : Disks >](#)

9. Select the "Management" tab and verify that you have a Diagnostics Storage Account. If you have no storage accounts, select "Create New", give your new account a name, and select "Ok"

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. [Learn more](#)

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

Monitoring

Enable detailed monitoring (preview) [?](#) On Off

Boot diagnostics [?](#) On Off

OS guest diagnostics [?](#) On Off

* Diagnostics storage account [?](#) No existing storage accounts in current subscription. [Create new](#) The value must not be empty.

Create storage account

* Name

.core.windows.net

Account kind [?](#) Storage (general purpose v1)

Performance [?](#) Standard Premium

Replication [?](#) Locally-redundant storage (LRS)

10. Click "Review + Create".

11. On the **Create a virtual machine** page, you can see the details about the VM you are about to create. When you are ready, select **Create**.

It will take a few minutes for your VM to be deployed. When the deployment is finished, move on to the next section.

Encrypt the virtual machine

1. When the VM deployment is complete, select **Go to resource**.

2. On the left-hand sidebar, select **Disks**.

3. On the Disks screen, select **Encryption**.

myVM - Disks
Virtual machine

Search (Ctrl+ /)

Edit Refresh Encryption Swap OS Disk

Managed disks created since June 10, 2017 are encrypted at rest with Storage Service Encryption (SSE). You may also want to enable Azure Disk Encryption.

Ultra Disk compatibility is not available for this location.

Disk settings

Enable Ultra Disk compatibility Yes No

OS disk

Name	Size	Storage account type	Encryption
myVM_OsDisk_1_8df8426fc5464c6d8cb2b26f8658e9b0	30 GiB	Premium SSD	Not enabled

Data disks

None

+ Add data disk

4. On the encryption screen, under **Disks to encrypt**, choose **OS and data disks**.

5. Under **Encryption settings**, choose **Select a key vault and key for encryption**.

6. On the **Select key from Azure Key Vault** screen, select **Create New**.

The screenshot shows the 'Select key from Azure Key Vault' interface. At the top, there's a breadcrumb navigation: Home > myVM - Disks > Encryption > Select key from Azure Key Vault. Below this is a title 'Select key from Azure Key Vault'. There are three main sections: 'Key vault *', 'Key', and 'Version'. The 'Key vault *' section has a dropdown menu with 'Select the key vault.' and a 'Create new' button, which is highlighted with a red circle. The 'Key' section has a dropdown menu with 'Select the key.' and a 'Create new' button. The 'Version' section has a dropdown menu with 'Select the version.' and a 'Create new' button.

7. On the **Create key vault** screen, ensure that the Resource Group is the same as the one you used to create the VM.
8. Give your key vault a name. Every key vault across Azure must have an unique name.
9. On the **Access Policies** tab, check the **Azure Disk Encryption for volume encryption** box.

The screenshot shows the 'Create key vault' interface. At the top, there's a breadcrumb navigation: Home > myVM - Disks > Encryption > Select key from Azure Key Vault > Create key vault. Below this is a title 'Create key vault'. There are four tabs at the top: 'Basics' (highlighted), 'Access policy' (circled in red), 'Virtual network', and 'Tags'. Under the 'Access policy' tab, there's a section 'Enable Access to:' with three checkboxes: 'Azure Virtual Machines for deployment' (unchecked), 'Azure Resource Manager for template deployment' (unchecked), and 'Azure Disk Encryption for volume encryption' (checked and circled in red).

10. Select **Review + create**.
11. After the key vault has passed validation, select **Create**. This will return you to the **Select key from Azure Key Vault** screen.
12. Leave the **Key** field blank and choose **Select**.
13. At the top of the encryption screen, click **Save**. A popup will warn you that the VM will reboot. Click **Yes**.

Clean up resources

When no longer needed, you can delete the resource group, virtual machine, and all related resources. To do so, select the resource group for the virtual machine, select Delete, then confirm the name of the resource group to delete.

Next steps

In this quickstart, you created a Key Vault that was enabled for encryption keys, created a virtual machine, and enabled the virtual machine for encryption.

[Azure Disk Encryption overview](#)

Creating and configuring a key vault for Azure Disk Encryption

10/2/2019 • 6 minutes to read • [Edit Online](#)

Azure Disk Encryption uses Azure Key Vault to control and manage disk encryption keys and secrets. For more information about key vaults, see [Get started with Azure Key Vault](#) and [Secure your key vault](#).

WARNING

- If you have previously used Azure Disk Encryption with Azure AD to encrypt a VM, you must continue use this option to encrypt your VM. See [Creating and configuring a key vault for Azure Disk Encryption with Azure AD \(previous release\)](#) for details.

Creating and configuring a key vault for use with Azure Disk Encryption involves three steps:

1. Creating a resource group, if needed.
2. Creating a key vault.
3. Setting key vault advanced access policies.

These steps are illustrated in the following quickstarts:

- [Create and encrypt a Linux VM with Azure CLI](#)
- [Create and encrypt a Linux VM with Azure PowerShell](#)

You may also, if you wish, generate or import a key encryption key (KEK).

NOTE

The steps in this article are automated in the [Azure Disk Encryption prerequisites CLI script](#) and [Azure Disk Encryption prerequisites PowerShell script](#).

Install tools and connect to Azure

The steps in this article can be completed with the [Azure CLI](#), the [Azure PowerShell Az module](#), or the [Azure portal](#).

While the portal is accessible through your browser, Azure CLI and Azure PowerShell require local installation; see [Azure Disk Encryption for Linux: Install tools](#) for details.

Connect to your Azure account

Before using the Azure CLI or Azure PowerShell, you must first connect to your Azure subscription. You do so by [Signing in with Azure CLI](#), [Signing in with Azure Powershell](#), or supplying your credentials to the Azure portal when prompted.

```
az login
```

```
Connect-AzAccount
```

Create a resource group

If you already have a resource group, you can skip to [Create a key vault](#).

A resource group is a logical container into which Azure resources are deployed and managed.

Create a resource group using the `az group create` Azure CLI command, the `New-AzResourceGroup` Azure PowerShell command, or from the [Azure portal](#).

Azure CLI

```
az group create --name "myResourceGroup" --location eastus
```

Azure PowerShell

```
New-AzResourceGroup -Name "myResourceGroup" -Location "EastUS"
```

Create a key vault

If you already have a key vault, you can skip to [Set key vault advanced access policies](#).

Create a key vault using the `az keyvault create` Azure CLI command, the `New-AzKeyvault` Azure Powershell command, the [Azure portal](#), or a [Resource Manager template](#).

WARNING

To ensure that encryption secrets don't cross regional boundaries, Azure Disk Encryption requires the Key Vault and the VMs to be co-located in the same region. Create and use a Key Vault that is in the same region as the VMs to be encrypted.

Each Key Vault must have a unique name. Replace with the name of your key vault in the following examples.

Azure CLI

When creating a key vault using Azure CLI, add the "--enabled-for-disk-encryption" flag.

```
az keyvault create --name "<your-unique-keyvault-name>" --resource-group "myResourceGroup" --location "eastus" --enabled-for-disk-encryption
```

Azure PowerShell

When creating a key vault using Azure PowerShell, add the "-EnabledForDiskEncryption" flag.

```
New-AzKeyvault -name "<your-unique-keyvault-name>" -ResourceGroupName "myResourceGroup" -Location "eastus" -EnabledForDiskEncryption
```

Resource Manager template

You can also create a key vault by using the [Resource Manager template](#).

1. On the Azure quickstart template, click **Deploy to Azure**.
2. Select the subscription, resource group, resource group location, Key Vault name, Object ID, legal terms, and agreement, and then click **Purchase**.

Set key vault advanced access policies

The Azure platform needs access to the encryption keys or secrets in your key vault to make them available to the VM for booting and decrypting the volumes.

If you did not enable your key vault for disk encryption, deployment, or template deployment at the time of creation (as demonstrated in the previous step), you must update its advanced access policies.

Azure CLI

Use [az keyvault update](#) to enable disk encryption for the key vault.

- **Enable Key Vault for disk encryption:** Enabled-for-disk-encryption is required.

```
az keyvault update --name "<your-unique-keyvault-name>" --resource-group "MyResourceGroup" --enabled-for-disk-encryption "true"
```

- **Enable Key Vault for deployment, if needed:** Enables the Microsoft.Compute resource provider to retrieve secrets from this key vault when this key vault is referenced in resource creation, for example when creating a virtual machine.

```
az keyvault update --name "<your-unique-keyvault-name>" --resource-group "MyResourceGroup" --enabled-for-deployment "true"
```

- **Enable Key Vault for template deployment, if needed:** Allow Resource Manager to retrieve secrets from the vault.

```
az keyvault update --name "<your-unique-keyvault-name>" --resource-group "MyResourceGroup" --enabled-for-template-deployment "true"
```

Azure PowerShell

Use the key vault PowerShell cmdlet [Set-AzKeyVaultAccessPolicy](#) to enable disk encryption for the key vault.

- **Enable Key Vault for disk encryption:** EnabledForDiskEncryption is required for Azure Disk encryption.

```
Set-AzKeyVaultAccessPolicy -VaultName "<your-unique-keyvault-name>" -ResourceGroupName "MyResourceGroup" -EnabledForDiskEncryption
```

- **Enable Key Vault for deployment, if needed:** Enables the Microsoft.Compute resource provider to retrieve secrets from this key vault when this key vault is referenced in resource creation, for example when creating a virtual machine.

```
Set-AzKeyVaultAccessPolicy -VaultName "<your-unique-keyvault-name>" -ResourceGroupName "MyResourceGroup" -EnabledForDeployment
```

- **Enable Key Vault for template deployment, if needed:** Enables Azure Resource Manager to get secrets from this key vault when this key vault is referenced in a template deployment.

```
Set-AzKeyVaultAccessPolicy -VaultName "<your-unique-keyvault-name>" -ResourceGroupName "MyResourceGroup" -EnabledForTemplateDeployment
```

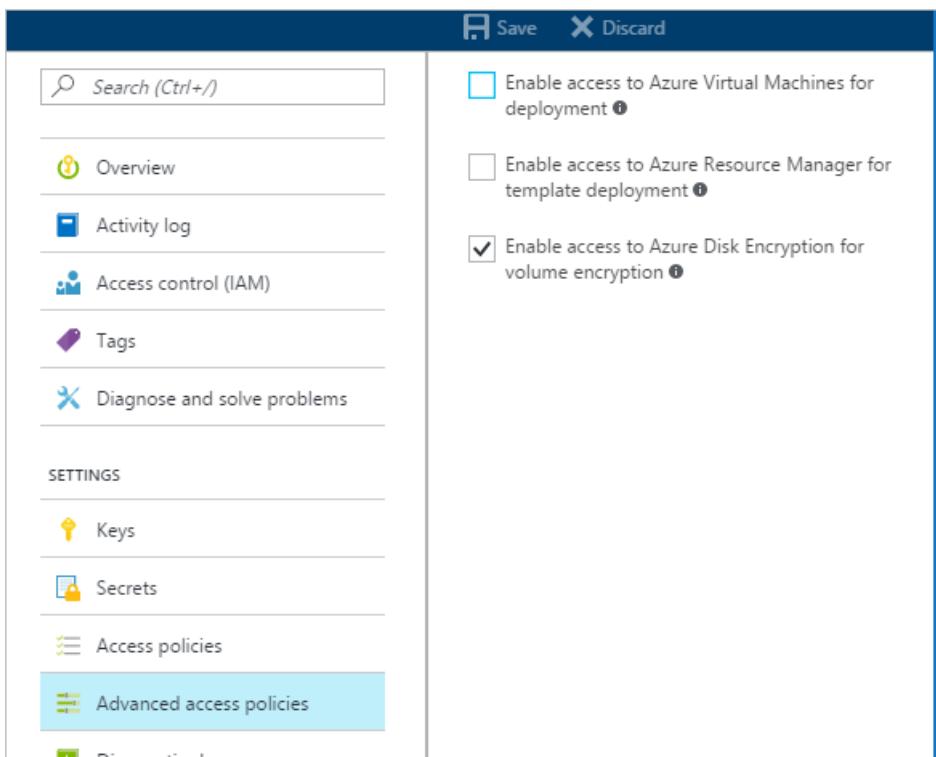
Azure portal

1. Select your key vault, go to **Access Policies**, and [Click to show advanced access policies](#).

2. Select the box labeled **Enable access to Azure Disk Encryption for volume encryption**.

3. Select **Enable access to Azure Virtual Machines for deployment** and/or **Enable Access to Azure Resource Manager for template deployment**, if needed.

4. Click **Save**.



Set up a key encryption key (KEK)

If you want to use a key encryption key (KEK) for an additional layer of security for encryption keys, add a KEK to your key vault. When a key encryption key is specified, Azure Disk Encryption uses that key to wrap the encryption secrets before writing to Key Vault.

You can generate a new KEK using the Azure CLI [az keyvault key create](#) command, the Azure PowerShell [Add-AzKeyVaultKey](#) cmdlet, or the [Azure portal](#). You must generate an RSA key type; Azure Disk Encryption does not yet support using Elliptic Curve keys.

You can instead import a KEK from your on-premises key management HSM. For more information, see [Key Vault Documentation](#).

Your key vault KEK URLs must be versioned. Azure enforces this restriction of versioning. For valid secret and KEK URLs, see the following examples:

- Example of a valid secret URL:

<https://contosovault.vault.azure.net/secrets/EncryptionSecretWithKek/xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

- Example of a valid KEK URL:

<https://contosovault.vault.azure.net/keys/diskencryptionkek/xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Azure Disk Encryption doesn't support specifying port numbers as part of key vault secrets and KEK URLs. For examples of non-supported and supported key vault URLs, see the following examples:

- Acceptable key vault URL:

<https://contosovault.vault.azure.net/secrets/contososecret/xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

- Unacceptable key vault URL:

<https://contosovault.vault.azure.net:443/secrets/contososecret/xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Azure CLI

Use the Azure CLI [az keyvault key create](#) command to generate a new KEK and store it in your key vault.

```
az keyvault key create --name "myKEK" --vault-name "<your-unique-keyvault-name>" --kty RSA-HSM
```

You may instead import a private key using the Azure CLI [az keyvault key import](#) command:

In either case, you will supply the name of your KEK to the Azure CLI [az vm encryption enable](#) --key-encryption-key parameter.

```
az vm encryption enable -g "MyResourceGroup" --name "myVM" --disk-encryption-keyvault "<your-unique-keyvault-name>" --key-encryption-key "myKEK"
```

Azure PowerShell

Use the Azure PowerShell [Add-AzKeyVaultKey](#) cmdlet to generate a new KEK and store it in your key vault.

```
Add-AzKeyVaultKey -Name "myKEK" -VaultName "<your-unique-keyvault-name>" -Destination "HSM"
```

You may instead import a private key using the Azure PowerShell [az keyvault key import](#) command.

In either case, you will supply the ID of your KEK key Vault and the URL of your KEK to the Azure PowerShell [Set-AzVMDiskEncryptionExtension](#) -KeyEncryptionKeyVaultId and -KeyEncryptionKeyUrl parameters. Note that this example assumes that you are using the same key vault for both the disk encryption key and the KEK.

```
$KeyVault = Get-AzKeyVault -VaultName "<your-unique-keyvault-name>" -ResourceGroupName "myResourceGroup"  
$KEK = Get-AzKeyVaultKey -VaultName "<your-unique-keyvault-name>" -Name "myKEK"  
  
Set-AzVMDiskEncryptionExtension -ResourceGroupName MyResourceGroup -VMName "MyVM" -DiskEncryptionKeyVaultUrl  
$KeyVault.VaultUri -DiskEncryptionKeyId $KeyVault.ResourceId -KeyEncryptionKeyVaultId  
$KeyVault.ResourceId -KeyEncryptionKeyUrl $KEK.Id -SkipVmBackup -VolumeType All
```

Next steps

- [Azure Disk Encryption prerequisites CLI script](#)
- [Azure Disk Encryption prerequisites PowerShell script](#)
- Learn [Azure Disk Encryption scenarios on Linux VMs](#)
- Learn how to [troubleshoot Azure Disk Encryption](#)
- Read the [Azure Disk Encryption sample scripts](#)

Azure Disk Encryption sample scripts

11/21/2019 • 13 minutes to read • [Edit Online](#)

This article provides sample scripts for preparing pre-encrypted VHDs and other tasks.

Sample PowerShell scripts for Azure Disk Encryption

- **List all encrypted VMs in your subscription**

```
$osVolEncrypted = {(Get-AzVMDiskEncryptionStatus -ResourceGroupName $_.ResourceGroupName -VMName
$_.Name).OsVolumeEncrypted}
$dataVolEncrypted= {(Get-AzVMDiskEncryptionStatus -ResourceGroupName $_.ResourceGroupName -VMName
$_.Name).DataVolumesEncrypted}
Get-AzVm | Format-Table @{Label="MachineName"; Expression={$.Name}}, @{Label="OsVolumeEncrypted";
Expression=$osVolEncrypted}, @{Label="DataVolumesEncrypted"; Expression=$dataVolEncrypted}
```

- **List all disk encryption secrets used for encrypting VMs in a key vault**

```
Get-AzKeyVaultSecret -VaultName $KeyVaultName | where
{$_.Tags.ContainsKey('DiskEncryptionKeyFileName')} | format-table @{Label="MachineName"; Expression=
{$_.Tags['MachineName']}}, @{Label="VolumeLetter"; Expression={$_.Tags['VolumeLetter']}},
@{Label="EncryptionKeyURL"; Expression={$.Id}}
```

Using the Azure Disk Encryption prerequisites PowerShell script

If you're already familiar with the prerequisites for Azure Disk Encryption, you can use the [Azure Disk Encryption prerequisites PowerShell script](#). For an example of using this PowerShell script, see the [Encrypt a VM Quickstart](#). You can remove the comments from a section of the script, starting at line 211, to encrypt all disks for existing VMs in an existing resource group.

The following table shows which parameters can be used in the PowerShell script:

PARAMETER	DESCRIPTION	MANDATORY?
\$resourceGroupName	Name of the resource group to which the KeyVault belongs to. A new resource group with this name will be created if one doesn't exist.	True
\$keyVaultName	Name of the KeyVault in which encryption keys are to be placed. A new vault with this name will be created if one doesn't exist.	True
\$location	Location of the KeyVault. Make sure the KeyVault and VMs to be encrypted are in the same location. Get a location list with <code>Get-AzLocation</code> .	True
\$subscriptionId	Identifier of the Azure subscription to be used. You can get your Subscription ID with <code>Get-AzSubscription</code> .	True

PARAMETER	DESCRIPTION	MANDATORY?
\$aadAppName	Name of the Azure AD application that will be used to write secrets to KeyVault. A new application with this name will be created if one doesn't exist. If this app already exists, pass aadClientSecret parameter to the script.	False
\$aadClientSecret	Client secret of the Azure AD application that was created earlier.	False
\$keyEncryptionKeyName	Name of optional key encryption key in KeyVault. A new key with this name will be created if one doesn't exist.	False

Encrypt or decrypt VMs without an Azure AD app

- [Enable disk encryption on an existing or running Linux VM](#)
- [Disable encryption on a running Linux VM](#)
 - Disabling encryption is only allowed on Data volumes for Linux VMs.

Encrypt or decrypt VMs with an Azure AD app (previous release)

- [Enable disk encryption on an existing or running Linux VM](#)
- [Disable encryption on a running Linux VM](#)
 - Disabling encryption is only allowed on Data volumes for Linux VMs.
- [Create a new encrypted managed disk from a pre-encrypted VHD/storage blob](#)
 - Creates a new encrypted managed disk provided a pre-encrypted VHD and its corresponding encryption settings

Encrypting an OS drive on a running Linux VM

Prerequisites for OS disk encryption

- The VM must be using a distribution compatible with OS disk encryption as listed in the [Azure Disk Encryption supported operating systems](#)
- The VM must be created from the Marketplace image in Azure Resource Manager.
- Azure VM with at least 4 GB of RAM (recommended size is 7 GB).
- (For RHEL and CentOS) Disable SELinux. To disable SELinux, see "4.4.2. Disabling SELinux" in the [SELinux User's and Administrator's Guide](#) on the VM.
- After you disable SELinux, reboot the VM at least once.

Steps

1. Create a VM by using one of the distributions specified previously.

For CentOS 7.2, OS disk encryption is supported via a special image. To use this image, specify "7.2n" as the SKU when you create the VM:

```
Set-AzVMSourceImage -VM $VirtualMachine -PublisherName "OpenLogic" -Offer "CentOS" -Skus "7.2n" -Version "latest"
```

2. Configure the VM according to your needs. If you're going to encrypt all the (OS + data) drives, the data drives need to be specified and mountable from /etc/fstab.

NOTE

Use `UUID=...` to specify data drives in `/etc/fstab` instead of specifying the block device name (for example, `/dev/sdb1`). During encryption, the order of drives changes on the VM. If your VM relies on a specific order of block devices, it will fail to mount them after encryption.

3. Sign out of the SSH sessions.
4. To encrypt the OS, specify `volumeType` as **All** or **OS** when you enable encryption.

NOTE

All user-space processes that are not running as `systemd` services should be killed with a `SIGKILL`. Reboot the VM. When you enable OS disk encryption on a running VM, plan on VM downtime.

5. Periodically monitor the progress of encryption by using the instructions in the [next section](#).
6. After `Get-AzVmDiskEncryptionStatus` shows "VMRestartPending", restart your VM either by signing in to it or by using the portal, PowerShell, or CLI.

```
C:\> Get-AzVmDiskEncryptionStatus -ResourceGroupName $ResourceGroupName -VMName $VMName  
-ExtensionName $ExtensionName  
  
OsVolumeEncrypted : VMRestartPending  
DataVolumesEncrypted : NotMounted  
OsVolumeEncryptionSettings : Microsoft.Azure.Management.Compute.Models.DiskEncryptionSettings  
ProgressMessage : OS disk successfully encrypted, reboot the VM
```

Before you reboot, we recommend that you save [boot diagnostics](#) of the VM.

Monitoring OS encryption progress

You can monitor OS encryption progress in three ways:

- Use the `Get-AzVmDiskEncryptionStatus` cmdlet and inspect the `ProgressMessage` field:

```
OsVolumeEncrypted : EncryptionInProgress  
DataVolumesEncrypted : NotMounted  
OsVolumeEncryptionSettings : Microsoft.Azure.Management.Compute.Models.DiskEncryptionSettings  
ProgressMessage : OS disk encryption started
```

After the VM reaches "OS disk encryption started", it takes about 40 to 50 minutes on a Premium-storage backed VM.

Because of [issue #388](#) in WALinuxAgent, `OsVolumeEncrypted` and `DataVolumesEncrypted` show up as `Unknown` in some distributions. With WALinuxAgent version 2.1.5 and later, this issue is fixed automatically. If you see `Unknown` in the output, you can verify disk-encryption status by using the Azure Resource Explorer.

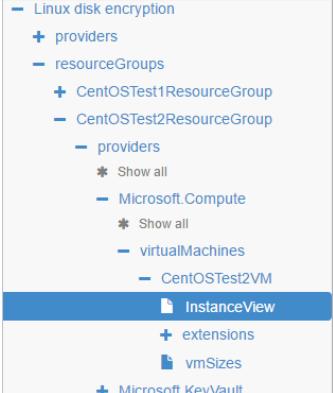
Go to [Azure Resource Explorer](#), and then expand this hierarchy in the selection panel on left:

```

|-- subscriptions
  |-- [Your subscription]
    |-- resourceGroups
      |-- [Your resource group]
        |-- providers
          |-- Microsoft.Compute
            |-- virtualMachines
              |-- [Your virtual machine]
                |-- InstanceView

```

In the InstanceView, scroll down to see the encryption status of your drives.



```

- Linux disk encryption
+ providers
- resourceGroups
  + CentOSTest1ResourceGroup
  - CentOSTest2ResourceGroup
    - providers
      * Show all
    - Microsoft.Compute
      * Show all
    - virtualMachines
      - CentOSTest2VM
        - InstanceView
        + extensions
        + vmSizes
        + Microsoft.KeyVault

```

```

60-
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80

```

```

{
  "code": "ProvisioningState/succeeded",
  "level": "Info",
  "displayStatus": "Provisioning succeeded",
  "time": "2016-09-22T02:19:41.4646766+00:00"
}
],
"extensions": [
  {
    "name": "AzureDiskEncryptionForLinux",
    "type": "Microsoft.Azure.Security.AzureDiskEncryptionForLinux",
    "typeHandlerVersion": "0.1.0.999190",
    "substatuses": [
      {
        "code": "ComponentStatus/Microsoft.Azure.Security.AzureDiskEncryptionForLinux",
        "level": "Info",
        "displayStatus": "Provisioning succeeded",
        "message": "{\"os\": \"NotEncrypted\", \"data\": \"EncryptionInProgress\"}"
      }
    ]
  }
]
}

```

- Look at [boot diagnostics](#). Messages from the ADE extension should be prefixed with [\[AzureDiskEncryption\]](#)
- Sign in to the VM via SSH, and get the extension log from:

/var/log/azure/Microsoft.Azure.Security.AzureDiskEncryptionForLinux

We recommend that you don't sign-in to the VM while OS encryption is in progress. Copy the logs only when the other two methods have failed.

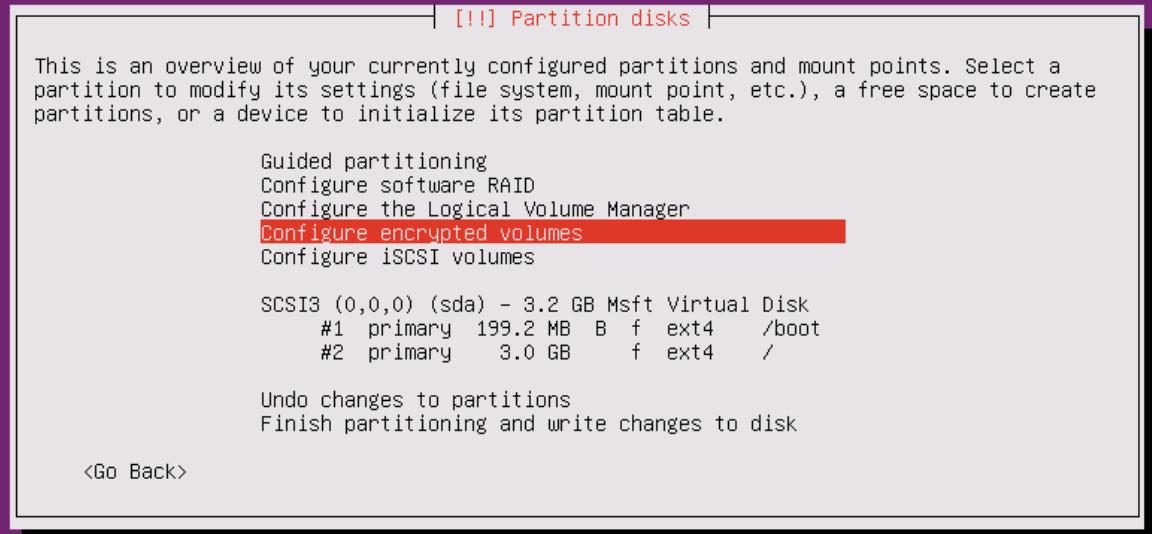
Prepare a pre-encrypted Linux VHD

The preparation for pre-encrypted VHDs can vary depending on the distribution. Examples on preparing Ubuntu 16, openSUSE 13.2, and CentOS 7 are available.

Ubuntu 16

Configure encryption during the distribution installation by doing the following steps:

1. Select **Configure encrypted volumes** when you partition the disks.



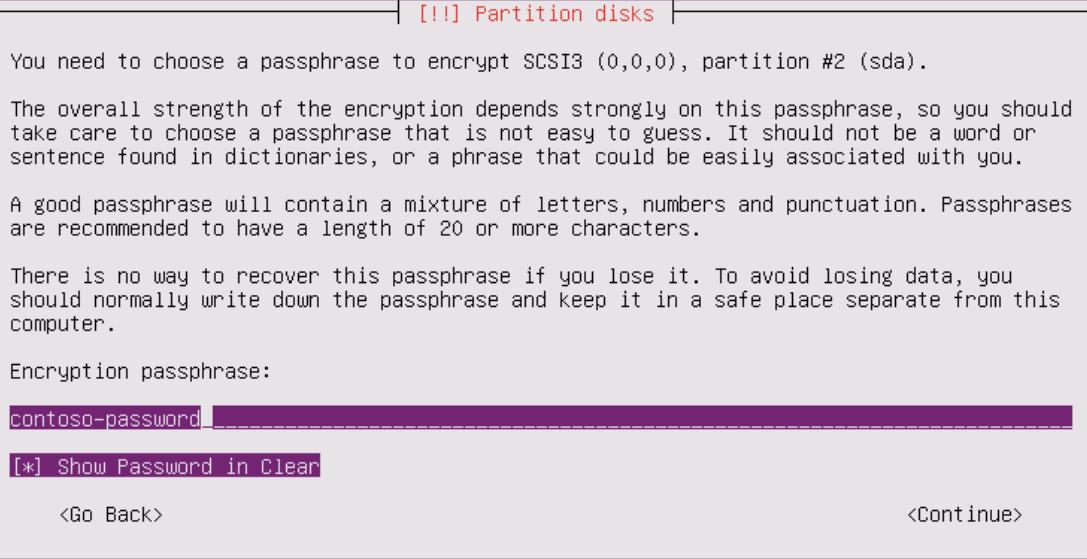
<F1> for help; <Tab> moves; <Space> selects; <Enter> activates buttons

2. Create a separate boot drive, which must not be encrypted. Encrypt your root drive.



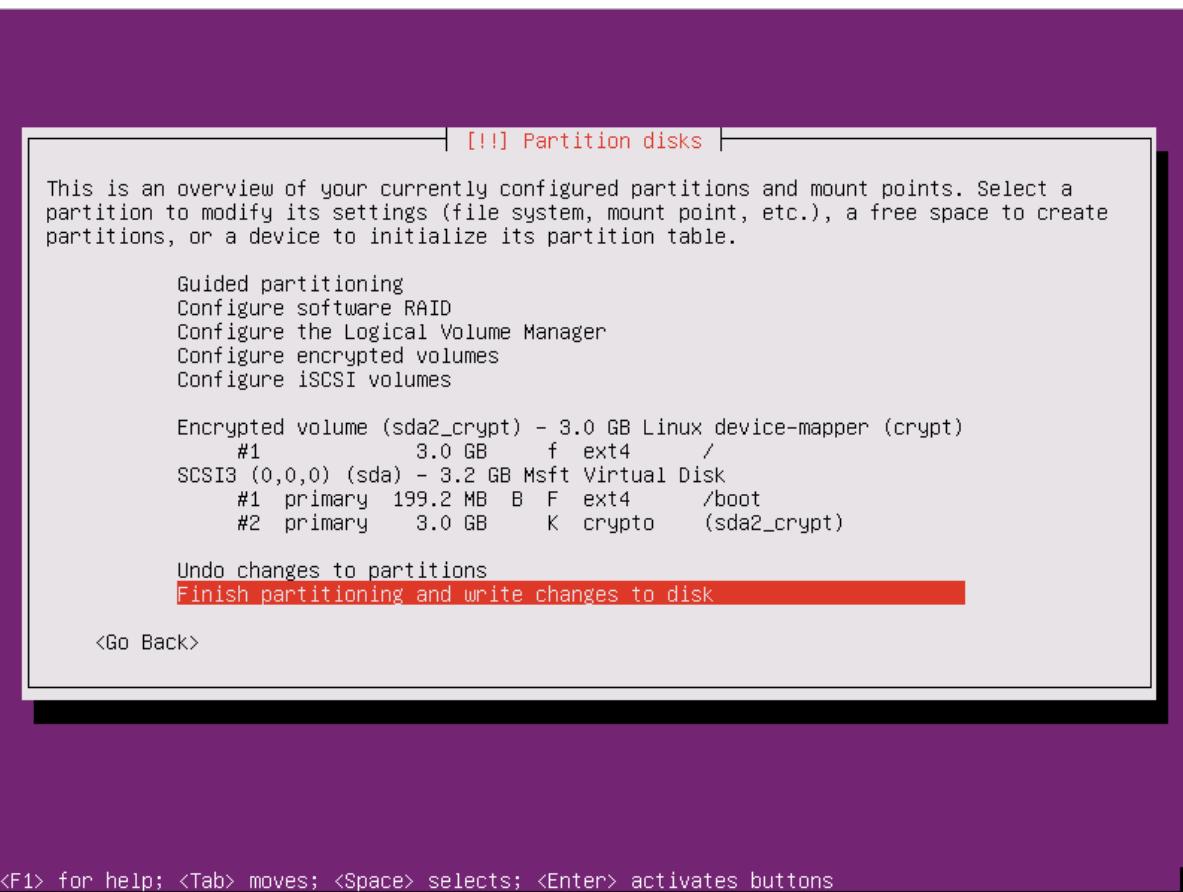
<Tab> moves; <Space> selects; <Enter> activates buttons

3. Provide a passphrase. This is the passphrase that you uploaded to the key vault.



<Tab> moves; <Space> selects; <Enter> activates buttons

4. Finish partitioning.



<F1> for help; <Tab> moves; <Space> selects; <Enter> activates buttons

5. When you boot the VM and are asked for a passphrase, use the passphrase you provided in step 3.

```

[ 1.129797] input: Microsoft Vmbus HID-compliant Mouse as /devices/0006:045E:0621.0001/input/input4
[ 1.132206] sda: sda1 sda2
[ 1.133217] hid 0006:045E:0621.0001: input: <UNKNOWN> HID v0.01 Mouse [Microsoft Vmbus HID-compliant Mouse] on
[ 1.134340] hv_netvsc: hv_netvsc channel opened successfully
[ 1.138418] sd 2:0:0:0: [sdal] Attached SCSI disk
[ 1.265049] hv_netvsc vmbus_15: Send section size: 6144, Section count:2560
[ 1.266137] hv_netvsc vmbus_15: Device MAC 00:15:5d:05:34:01 link state up
[ 1.272596] scsi host3: storvsc_host_t
[ 1.436076] psmouse serio1: trackpoint: failed to get extended button data
Begin: Loading essential drivers ... [ 2.401782] md: linear personality registered for level -1
[ 2.404316] md: multipath personality registered for level -4
[ 2.407122] md: raid0 personality registered for level 0
[ 2.410610] md: raid1 personality registered for level 1
[ 2.480009] raid6: sse2x1 gen() 10995 MB/s
[ 2.548012] raid6: sse2x1 xor() 8467 MB/s
[ 2.616010] raid6: sse2x2 gen() 14312 MB/s
[ 2.684013] raid6: sse2x2 xor() 9555 MB/s
[ 2.752011] raid6: sse2x4 gen() 16205 MB/s
[ 2.820010] raid6: sse2x4 xor() 11594 MB/s
[ 2.888007] raid6: avx2x1 gen() 21995 MB/s
[ 2.956007] raid6: avx2x2 gen() 25959 MB/s
[ 3.024011] raid6: avx2x4 gen() 29505 MB/s
[ 3.024735] raid6: using algorithm avx2x4 gen() 29505 MB/s
[ 3.025038] raid6: using avx2x2 recovery algorithm
[ 3.027102] xor: automatically using best checksumming function:
[ 3.064003]   avx      : 35013.000 MB/sec
[ 3.065688] async_tx: api initialized (async)
[ 3.074685] md: raid6 personality registered for level 6
[ 3.075435] md: raid5 personality registered for level 5
[ 3.075746] md: raid4 personality registered for level 4
[ 3.079565] md: raid10 personality registered for level 10
done.
Begin: Running /scripts/init-premount ... done.
Begin: Mounting root file system ... Begin: Running /scripts/local-top ... Please unlock disk sda2_crypt: -

```

6. Prepare the VM for uploading into Azure using [these instructions](#). Don't run the last step (deprovisioning the VM) yet.

Configure encryption to work with Azure by doing the following steps:

1. Create a file under /usr/local/sbin/azure_crypt_key.sh, with the content in the following script. Pay attention to the KeyFileName, because it's the passphrase file name used by Azure.

```

#!/bin/sh
MountPoint=/tmp-keydisk-mount
KeyFileName=LinuxPassPhraseFileName
echo "Trying to get the key from disks ..." >&2
mkdir -p $MountPoint
modprobe vfat >/dev/null 2>&1
modprobe ntfs >/dev/null 2>&1
sleep 2
OPENED=0
cd /sys/block
for DEV in sd*; do

    echo "> Trying device: $DEV ..." >&2
    mount -t vfat -r /dev/${DEV}1 $MountPoint >/dev/null ||
    mount -t ntfs -r /dev/${DEV}1 $MountPoint >/dev/null
    if [ -f $MountPoint/$KeyFileName ]; then
        cat $MountPoint/$KeyFileName
        umount $MountPoint 2>/dev/null
        OPENED=1
        break
    fi
    umount $MountPoint 2>/dev/null
done

if [ $OPENED -eq 0 ]; then
    echo "FAILED to find suitable passphrase file ..." >&2
    echo -n "Try to enter your password: " >&2
    read -s -r A </dev/console
    echo -n "$A"
else
    echo "Success loading keyfile!" >&2
fi

```

2. Change the crypt config in */etc/crypttab*. It should look like this:

```
xxx_crypt  uuid=xxxxxxxxxxxxxxxxxxxxxx none luks,discard,keyscript=/usr/local/sbin/azure_crypt_key.sh
```

3. Add executable permissions to the script:

```
chmod +x /usr/local/sbin/azure_crypt_key.sh
```

4. Edit */etc/initramfs-tools/modules* by appending lines:

```
vfat
ntfs
nls_cp437
nls_utf8
nls_iso8859-1
```

5. Run `update-initramfs -u -k all` to update the initramfs to make the `keyscript` take effect.

6. Now you can deprovision the VM.

```

root@ubuntu-preencrypted:~# ls -l /usr/local/sbin/azure_crypt_key.sh
-rwxr-xr-x 1 root root 860 Sep 18 16:57 /usr/local/sbin/azure_crypt_key.sh
root@ubuntu-preencrypted:~# cat /etc/crypttab
sda2_crypt UUID=b0dee704-1f2a-4f02-9a13-289c6c99dbb8 none luks,discard,keyscheme=/usr/local/sbin/azure_crypt_key.sh
root@ubuntu-preencrypted:~# cat /etc/initramfs-tools/modules
# List of modules that you want to include in your initramfs.
# They will be loaded at boot time in the order below.
#
# Syntax: module_name [args ...]
#
# You must run update-initramfs(8) to effect this change.
#
# Examples:
#
# raid1
# sd_mod
# ofat
# ntfs
# nls_cp437
# nls_utf8
# nls_iso8859-1
root@ubuntu-preencrypted:~# update-initramfs -u -k all
update-initramfs: Generating /boot/initrd.img-4.4.0-36-generic
W: plymouth: The plugin label.so is missing, the selected theme might not work as expected.
W: plymouth: You might want to install the plymouth-themes and plymouth-label package to fix this.
W: mdadm: /etc/mdadm/mdadm.conf defines no arrays.
[ 6289.960173] blk update_request: I/O error, dev fd0, sector 0
update-initramfs: Generating /boot/initrd.img-4.4.0-21-generic
W: plymouth: The plugin label.so is missing, the selected theme might not work as expected.
W: plymouth: You might want to install the plymouth-themes and plymouth-label package to fix this.
W: mdadm: /etc/mdadm/mdadm.conf defines no arrays.
[ 6297.592236] blk update_request: I/O error, dev fd0, sector 0
root@ubuntu-preencrypted:~# waagent -force -deprovision
WARNING! The waagent service will be stopped.
WARNING! Cached DHCP leases will be deleted.
WARNING! root password will be disabled. You will not be able to login as root.
WARNING! Nameserver configuration in /etc/resolvconf/resolv.conf.d/tail,original will be deleted.
2016/09/18 17:06:38.572398 INFO resoluconf is enabled: leaving /etc/resolv.conf intact
2016/09/18 17:06:38.572398 INFO resoluconf is enabled: leaving /etc/resolv.conf intact
root@ubuntu-preencrypted:~# export HISTSIZE=0
root@ubuntu-preencrypted:~# logout

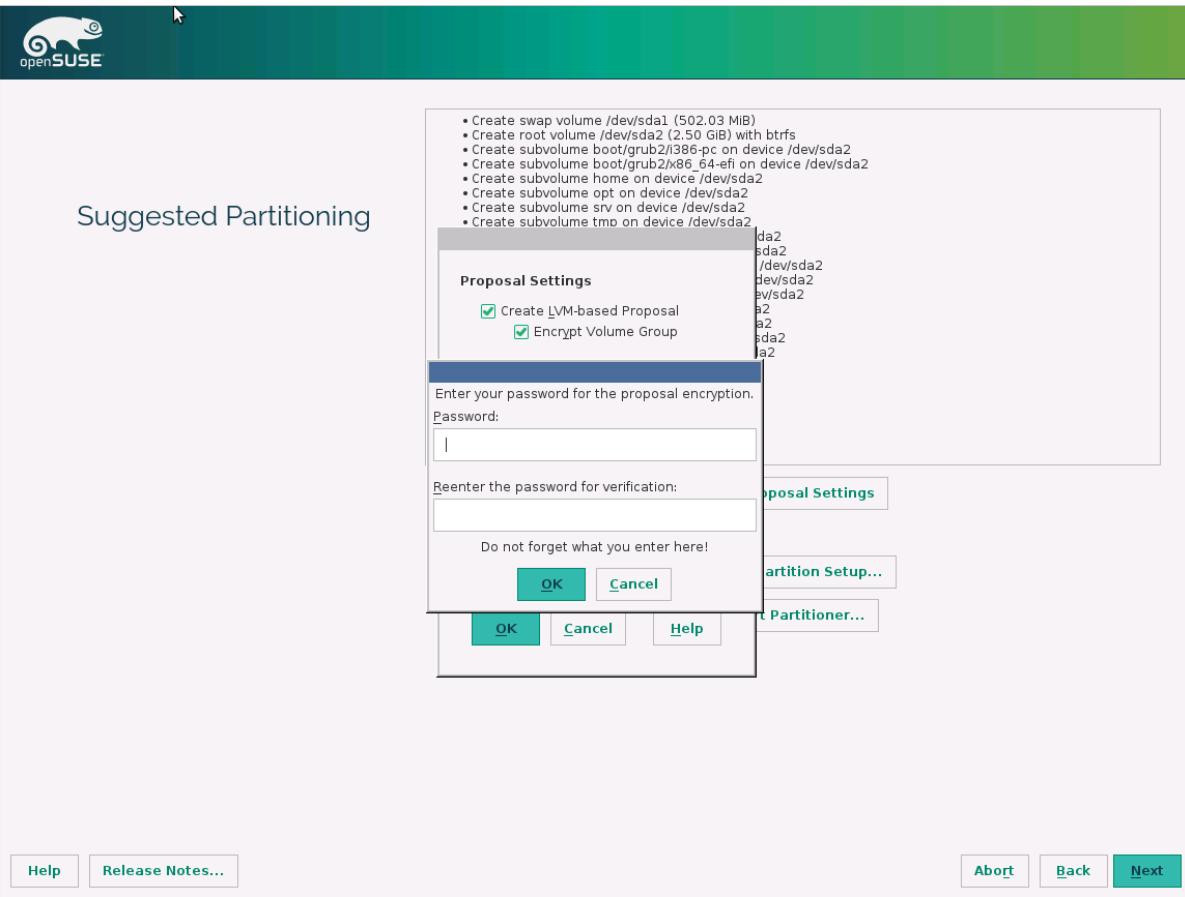
```

7. Continue to the next step and upload your VHD into Azure.

openSUSE 13.2

To configure encryption during the distribution installation, do the following steps:

1. When you partition the disks, select **Encrypt Volume Group**, and then enter a password. This is the password that you'll upload to your key vault.



2. Boot the VM using your password.

```
[ 0.000000] tsc: Fast TSC calibration failed
[ OK ] Found device Virtual_Disk.
[ OK ] Found device Virtual_Disk.
      Starting Cryptography Setup for cr_scsi-14d534654202020fd10f64360...278fd6327ec-part2...
      Starting Setup Virtual Console...
[ OK ] Started Setup Virtual Console.
      Starting Dispatch Password Requests to Console...
[ OK ] Started Dispatch Password Requests to Console.
Please enter passphrase for disk Virtual_Disk (cr_scsi-14d534654202020fd10f64360f5f14797052278fd6327ec-part2)! *****
```

3. Prepare the VM for uploading to Azure by following the instructions in [Prepare a SLES or openSUSE virtual machine for Azure](#). Don't run the last step (deprovisioning the VM) yet.

To configure encryption to work with Azure, do the following steps:

1. Edit the /etc/dracut.conf, and add the following line:

```
add_drivers+=" vfat ntfs nls_cp437 nls_iso8859-1"
```

2. Comment out these lines by the end of the file /usr/lib/dracut/modules.d/90crypt/module-setup.sh:

```
#      inst_multiple -o \
#      $systemdutildir/system-generators/systemd-cryptsetup-generator \
#      $systemdutildir/systemd-cryptsetup \
#      $systemdsystemunitdir/systemd-ask-password-console.path \
#      $systemdsystemunitdir/systemd-ask-password-console.service \
#      $systemdsystemunitdir/cryptsetup.target \
#      $systemdsystemunitdir/sysinit.target.wants/cryptsetup.target \
#      systemd-ask-password systemd-tty-ask-password-agent
#      inst_script "$moddir"/crypt-run-generator.sh /sbin/crypt-run-generator
```

3. Append the following line at the beginning of the file /usr/lib/dracut/modules.d/90crypt/parse-crypt.sh:

```
DRACUT_SYSTEMD=0
```

And change all occurrences of:

```
if [ -z "$DRACUT_SYSTEMD" ]; then
```

to:

```
if [ 1 ]; then
```

4. Edit /usr/lib/dracut/modules.d/90crypt/cryptroot-ask.sh and append it to "# Open LUKS device":

```
MountPoint=/tmp-keydisk-mount
KeyFileName=LinuxPassPhraseFileName
echo "Trying to get the key from disks ..." >&2
mkdir -p $MountPoint >&2
modprobe vfat >/dev/null >&2
modprobe ntfs >/dev/null >&2
for SFS in /dev/sd*; do
    echo "> Trying device:$SFS..." >&2
    mount ${SFS}1 $MountPoint -t vfat -r >&2 ||
    mount ${SFS}1 $MountPoint -t ntfs -r >&2
    if [ -f $MountPoint/$KeyFileName ]; then
        echo "> keyfile got..." >&2
        cp $MountPoint/$KeyFileName /tmp-keyfile >&2
        luksfile=/tmp-keyfile
        umount $MountPoint >&2
        break
    fi
done
```

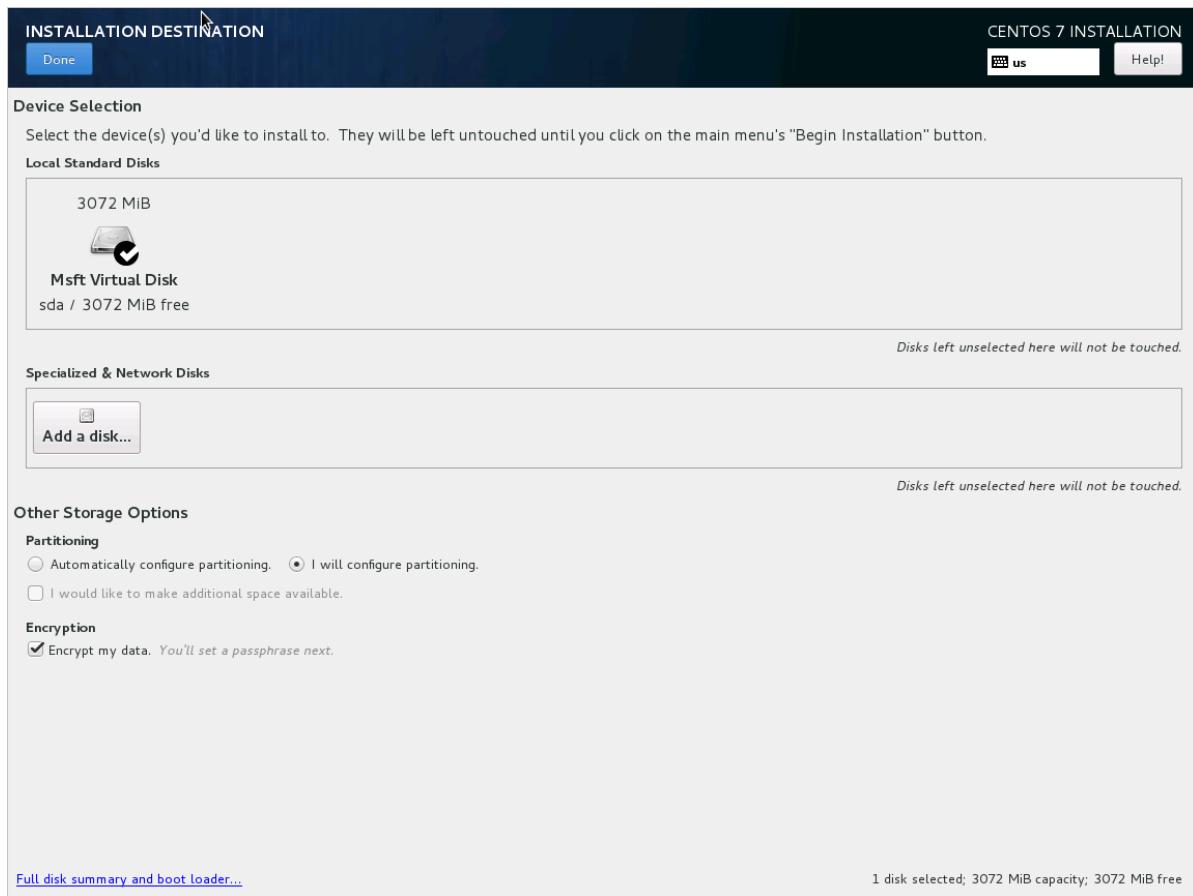
5. Run `/usr/sbin/dracut -f -v` to update the initrd.

6. Now you can deprovision the VM and upload your VHD into Azure.

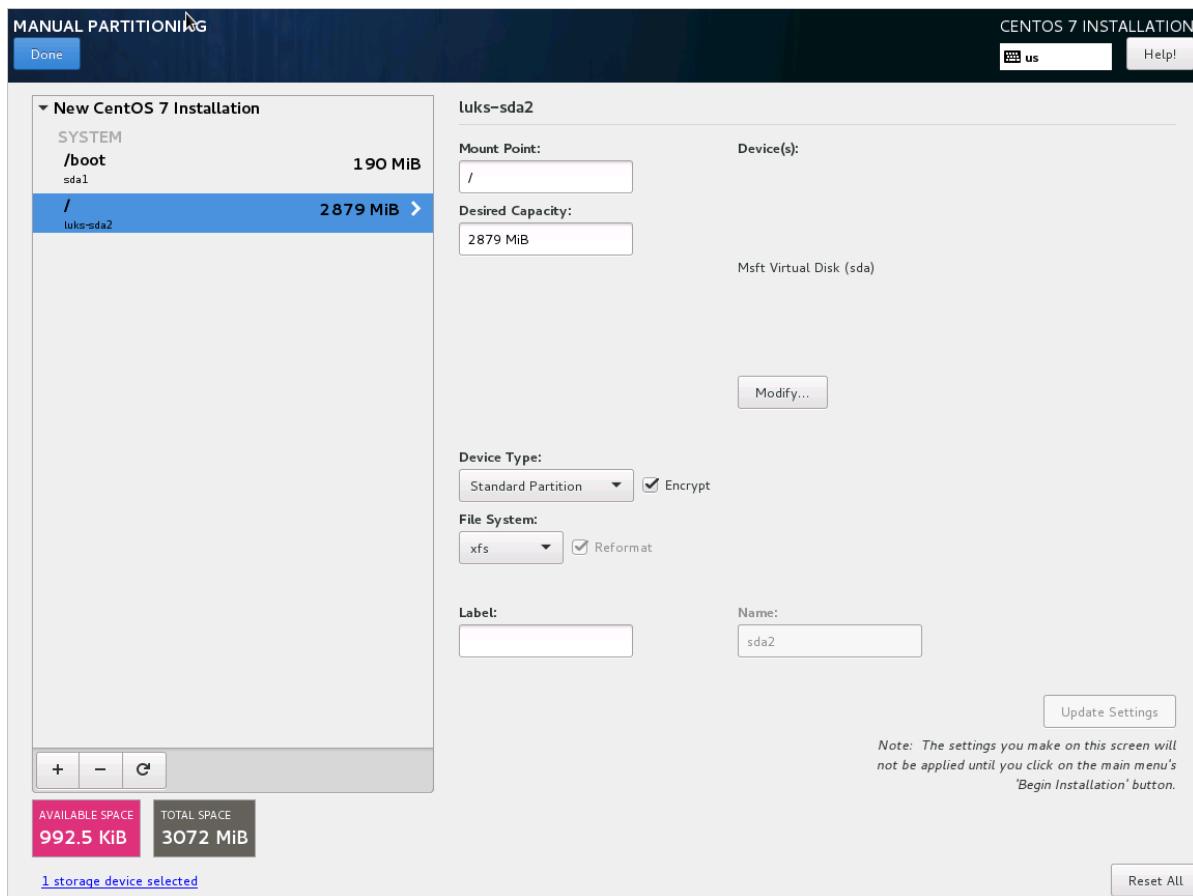
CentOS 7 and RHEL 8.1

To configure encryption during the distribution installation, do the following steps:

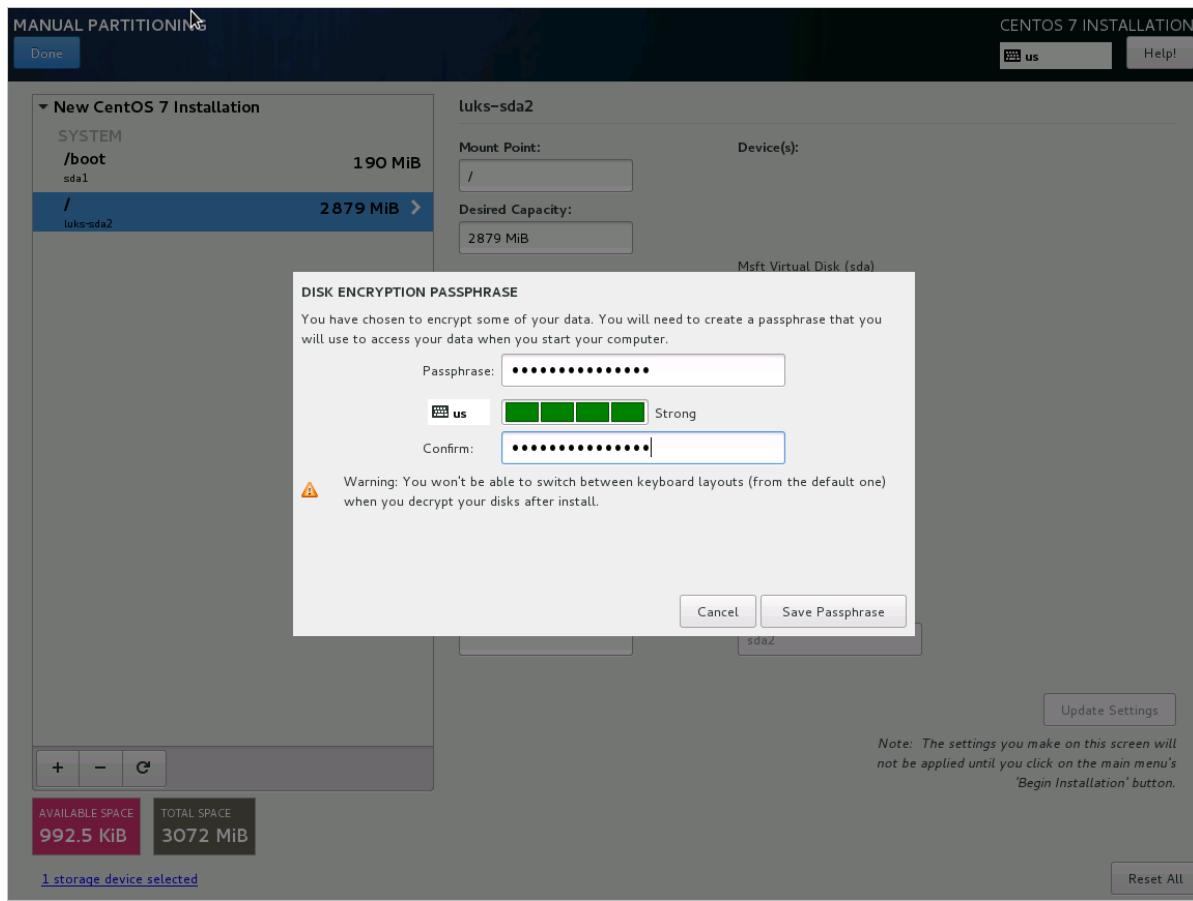
1. Select **Encrypt my data** when you partition disks.



2. Make sure **Encrypt** is selected for root partition.



3. Provide a passphrase. This is the passphrase that you'll upload to your key vault.



- When you boot the VM and are asked for a passphrase, use the passphrase you provided in step 3.



- Prepare the VM for uploading into Azure by using the "CentOS 7.0+" instructions in [Prepare a CentOS-based virtual machine for Azure](#). Don't run the last step (deprovisioning the VM) yet.
- Now you can deprovision the VM and upload your VHD into Azure.

To configure encryption to work with Azure, do the following steps:

1. Edit the /etc/dracut.conf, and add the following line:

```
add_drivers+=" vfat ntfs nls_cp437 nls_iso8859-1"
```

2. Comment out these lines by the end of the file /usr/lib/dracut/modules.d/90crypt/module-setup.sh:

```
#      inst_multiple -o \
#      $systemdutildir/system-generators/systemd-cryptsetup-generator \
#      $systemdutildir/systemd-cryptsetup \
#      $systemdsystemunitdir/systemd-ask-password-console.path \
#      $systemdsystemunitdir/systemd-ask-password-console.service \
#      $systemdsystemunitdir/cryptsetup.target \
#      $systemdsystemunitdir/sysinit.target.wants/cryptsetup.target \
#      systemd-ask-password systemd-tty-ask-password-agent
#      inst_script "$moddir"/crypt-run-generator.sh /sbin/crypt-run-generator
```

3. Append the following line at the beginning of the file /usr/lib/dracut/modules.d/90crypt/parse-crypt.sh:

```
DRACUT_SYSTEMD=0
```

And change all occurrences of:

```
if [ -z "$DRACUT_SYSTEMD" ]; then
```

to

```
if [ 1 ]; then
```

4. Edit /usr/lib/dracut/modules.d/90crypt/cryptroot-ask.sh and append the following after the "# Open LUKS device":

```
MountPoint=/tmp-keydisk-mount
KeyFileName=LinuxPassPhraseFileName
echo "Trying to get the key from disks ..." >&2
mkdir -p $MountPoint >&2
modprobe vfat >/dev/null >&2
modprobe ntfs >/dev/null >&2
for SFS in /dev/sd*; do
echo "> Trying device:$SFS..." >&2
mount ${SFS}1 $MountPoint -t vfat -r >&2 ||
mount ${SFS}1 $MountPoint -t ntfs -r >&2
if [ -f $MountPoint/$KeyFileName ]; then
    echo "> keyfile got..." >&2
    cp $MountPoint/$KeyFileName /tmp-keyfile >&2
    luksfile=/tmp-keyfile
    umount $MountPoint >&2
    break
fi
done
```

5. Run the "/usr/sbin/dracut -f -v" to update the initrd.

```
[root@centos-preencrypted ~]# cat /etc/dracut.conf | grep add_drivers
add_drivers+="vfat ntfs nls_cp437 nls_iso8859-1"
[root@centos-preencrypted ~]# cat /usr/lib/dracut/modules.d/90crypt/cryptroot-ask.sh | grep LinuxPassPhraseFileName -A 15 -B 1
MountPoint=/tmp-keydisk-mount
KeyFileName=LinuxPassPhraseFileName
echo "Trying to get the key from disks ..." >&2
mkdir -p $MountPoint >&2
modprobe vfat >/dev/null >&2
modprobe ntfs >/dev/null >&2
for SFS in /dev/sd*; do
echo "> Trying device:$SFS..." >&2
mount ${SFS}1 $MountPoint -t vfat -r >&2 ||
mount ${SFS}1 $MountPoint -t ntfs -r >&2
if [ ! -f $MountPoint/$KeyFileName ]; then
    echo "> keyfile got..." >&2
    cp $MountPoint/$KeyFileName /tmp-keyfile >&2
    luksfile=/tmp-keyfile
    umount $MountPoint >&2
    break
fi
[root@centos-preencrypted ~]# dracut -f -v_
```

Upload encrypted VHD to an Azure storage account

After DM-Crypt encryption is enabled, the local encrypted VHD needs to be uploaded to your storage account.

```
Add-AzVhd [-Destination] <Uri> [-LocalFilePath] <FileInfo> [[-NumberOfUploaderThreads] <Int32> ] [[-BaseImageUriToPatch] <Uri> ] [[-OverWrite]] [ <CommonParameters>]
```

Upload the secret for the pre-encrypted VM to your key vault

When encrypting using an Azure AD app (previous release), the disk-encryption secret that you obtained previously must be uploaded as a secret in your key vault. The key vault needs to have disk encryption and permissions enabled for your Azure AD client.

```
$AadClientId = "My-AAD-Client-Id"
$AadClientSecret = "My-AAD-Client-Secret"

$keyVault = New-AzKeyVault -VaultName $KeyVaultName -ResourceGroupName $ResourceGroupName -Location
$Location

Set-AzKeyVaultAccessPolicy -VaultName $KeyVaultName -ResourceGroupName $ResourceGroupName -
ServicePrincipalName $AadClientId -PermissionsToKeys all -PermissionsToSecrets all
Set-AzKeyVaultAccessPolicy -VaultName $KeyVaultName -ResourceGroupName $ResourceGroupName -
EnabledForDiskEncryption
```

Disk encryption secret not encrypted with a KEK

To set up the secret in your key vault, use [Set-AzKeyVaultSecret](#). The passphrase is encoded as a base64 string and then uploaded to the key vault. In addition, make sure that the following tags are set when you create the secret in the key vault.

```

# This is the passphrase that was provided for encryption during the distribution installation
$passphrase = "contoso-password"

$tags = @{"DiskEncryptionKeyEncryptionAlgorithm" = "RSA-OAEP"; "DiskEncryptionKeyFileName" =
"LinuxPassPhraseFileName"}
$secretName = [guid]::NewGuid().ToString()
$secretValue = [Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($passphrase))
$secureSecretValue = ConvertTo-SecureString $secretValue -AsPlainText -Force

$secret = Set-AzKeyVaultSecret -VaultName $KeyVaultName -Name $secretName -SecretValue $secureSecretValue -
tags $tags
$secretUrl = $secret.Id

```

Use the `$secretUrl` in the next step for [attaching the OS disk without using KEK](#).

Disk encryption secret encrypted with a KEK

Before you upload the secret to the key vault, you can optionally encrypt it by using a key encryption key. Use the [wrap API](#) to first encrypt the secret using the key encryption key. The output of this wrap operation is a base64 URL encoded string, which you can then upload as a secret by using the `Set-AzKeyVaultSecret` cmdlet.

```

# This is the passphrase that was provided for encryption during the distribution installation
$passphrase = "contoso-password"

Add-AzKeyVaultKey -VaultName $KeyVaultName -Name "keyencryptionkey" -Destination Software
$keyEncryptionKey = Get-AzKeyVaultKey -VaultName $KeyVault.OriginalVault.Name -Name "keyencryptionkey"

$apiversion = "2015-06-01"

#####
# Get Auth URI
#####

$uri = $KeyVault.VaultUri + "/keys"
$headers = @{}

$response = try { Invoke-RestMethod -Method GET -Uri $uri -Headers $headers } catch {
$_._Exception.Response }

$authHeader = $response.Headers["www-authenticate"]
$authUri = [regex]::match($authHeader, 'authorization="(.*)"').Groups[1].Value

Write-Host "Got Auth URI successfully"

#####
# Get Auth Token
#####

$uri = $authUri + "/oauth2/token"
$body = "grant_type=client_credentials"
$body += "&client_id=" + $AadClientId
$body += "&client_secret=" + [Uri]::EscapeDataString($AadClientSecret)
$body += "&resource=" + [Uri]::EscapeDataString("https://vault.azure.net")
$headers = @{}

$response = Invoke-RestMethod -Method POST -Uri $uri -Headers $headers -Body $body

$access_token = $response.access_token

Write-Host "Got Auth Token successfully"

#####
# Get KEK info
#####

```

```

$uri = $KeyEncryptionKey.Id + "?api-version=" + $apiversion
$headers = @{"Authorization" = "Bearer " + $access_token}

$response = Invoke-RestMethod -Method GET -Uri $uri -Headers $headers

$keyid = $response.key.kid

Write-Host "Got KEK info successfully"

#####
# Encrypt passphrase using KEK
#####

$passphraseB64 = [Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($Passphrase))
$uri = $keyid + "/encrypt?api-version=" + $apiversion
$headers = @{"Authorization" = "Bearer " + $access_token; "Content-Type" = "application/json"}
$bodyObj = @{"alg" = "RSA-OAEP"; "value" = $passphraseB64}
$body = $bodyObj | ConvertTo-Json

$response = Invoke-RestMethod -Method POST -Uri $uri -Headers $headers -Body $body

$wrappedSecret = $response.value

Write-Host "Encrypted passphrase successfully"

#####
# Store secret
#####

$secretName = [guid]::NewGuid().ToString()
$uri = $KeyVault.VaultUri + "/secrets/" + $secretName + "?api-version=" + $apiversion
$secretAttributes = @{"enabled" = $true}
$secretTags = @{"DiskEncryptionKeyEncryptionAlgorithm" = "RSA-OAEP"; "DiskEncryptionKeyFileName" =
"LinuxPassPhraseFileName"}
$headers = @{"Authorization" = "Bearer " + $access_token; "Content-Type" = "application/json"}
$bodyObj = @{"value" = $wrappedSecret; "attributes" = $secretAttributes; "tags" = $secretTags}
$body = $bodyObj | ConvertTo-Json

$response = Invoke-RestMethod -Method PUT -Uri $uri -Headers $headers -Body $body

Write-Host "Stored secret successfully"

$secretUrl = $response.id

```

Use `$keyEncryptionKey` and `$secreturl` in the next step for [attaching the OS disk using KEK](#).

Specify a secret URL when you attach an OS disk

Without using a KEK

While you're attaching the OS disk, you need to pass `$secretUrl`. The URL was generated in the "Disk-encryption secret not encrypted with a KEK" section.

```

Set-AzVMOSDisk ` 
    -VM $VirtualMachine ` 
    -Name $OSDiskName ` 
    -SourceImageUri $VhdUri ` 
    -VhdUri $OSDiskUri ` 
    -Linux ` 
    -CreateOption FromImage ` 
    -DiskEncryptionKeyVaultId $KeyVault.ResourceId ` 
    -DiskEncryptionKeyUrl $SecretUrl

```

Using a KEK

When you attach the OS disk, pass `$KeyEncryptionKey` and `$secretUrl`. The URL was generated in the "Disk encryption secret encrypted with a KEK" section.

```
Set-AzVMOSDisk ` 
    -VM $VirtualMachine ` 
    -Name $OSDiskName ` 
    -SourceImageUri $CopiedTemplateBlobUri ` 
    -VhdUri $OSDiskUri ` 
    -Linux ` 
    -CreateOption FromImage ` 
    -DiskEncryptionKeyVaultId $KeyVault.ResourceId ` 
    -DiskEncryptionKeyUrl $SecretUrl ` 
    -KeyEncryptionKeyVaultId $KeyVault.ResourceId ` 
    -KeyEncryptionKeyURL $KeyEncryptionKey.Id
```

Azure Disk Encryption troubleshooting guide

11/7/2019 • 7 minutes to read • [Edit Online](#)

This guide is for IT professionals, information security analysts, and cloud administrators whose organizations use Azure Disk Encryption. This article is to help with troubleshooting disk-encryption-related problems.

Before taking any of the steps below, first ensure that the VMs you are attempting to encrypt are among the [supported VM sizes and operating systems](#), and that you have met all the prerequisites:

- [Additional requirements for VMs](#)
- [Networking requirements](#)
- [Encryption key storage requirements](#)

Troubleshooting Linux OS disk encryption

Linux operating system (OS) disk encryption must unmount the OS drive before running it through the full disk encryption process. If it can't unmount the drive, an error message of "failed to unmount after ..." is likely to occur.

This error can occur when OS disk encryption is attempted on a VM with an environment that has been changed from the supported stock gallery image. Deviations from the supported image can interfere with the extension's ability to unmount the OS drive. Examples of deviations can include the following items:

- Customized images no longer match a supported file system or partitioning scheme.
- Large applications such as SAP, MongoDB, Apache Cassandra, and Docker aren't supported when they're installed and running in the OS before encryption. Azure Disk Encryption is unable to shut down these processes safely as required in preparation of the OS drive for disk encryption. If there are still active processes holding open file handles to the OS drive, the OS drive can't be unmounted, resulting in a failure to encrypt the OS drive.
- Custom scripts that run in close time proximity to the encryption being enabled, or if any other changes are being made on the VM during the encryption process. This conflict can happen when an Azure Resource Manager template defines multiple extensions to execute simultaneously, or when a custom script extension or other action runs simultaneously to disk encryption. Serializing and isolating such steps might resolve the issue.
- Security Enhanced Linux (SELinux) hasn't been disabled before enabling encryption, so the unmount step fails. SELinux can be reenabled after encryption is complete.
- The OS disk uses a Logical Volume Manager (LVM) scheme. Although limited LVM data disk support is available, an LVM OS disk isn't.
- Minimum memory requirements aren't met (7 GB is suggested for OS disk encryption).
- Data drives are recursively mounted under the /mnt/ directory, or each other (for example, /mnt/data1, /mnt/data2, /data3 + /data3/data4).

Update the default kernel for Ubuntu 14.04 LTS

The Ubuntu 14.04 LTS image ships with a default kernel version of 4.4. This kernel version has a known issue in which Out of Memory Killer improperly terminates the dd command during the OS encryption process. This bug has been fixed in the most recent Azure tuned Linux kernel. To avoid this error, prior to enabling encryption on the image, update to the [Azure tuned kernel 4.15](#) or later using the following commands:

```
sudo apt-get update
sudo apt-get install linux-azure
sudo reboot
```

After the VM has restarted into the new kernel, the new kernel version can be confirmed using:

```
uname -a
```

Update the Azure Virtual Machine Agent and extension versions

Azure Disk Encryption operations may fail on virtual machine images using unsupported versions of the Azure Virtual Machine Agent. Linux images with agent versions earlier than 2.2.38 should be updated prior to enabling encryption. For more information, see [How to update the Azure Linux Agent on a VM](#) and [Minimum version support for virtual machine agents in Azure](#).

The correct version of the Microsoft.Azure.Security.AzureDiskEncryption or Microsoft.Azure.Security.AzureDiskEncryptionForLinux guest agent extension is also required. Extension versions are maintained and updated automatically by the platform when Azure Virtual Machine agent prerequisites are satisfied and a supported version of the virtual machine agent is used.

The Microsoft.OSTCExtensions.AzureDiskEncryptionForLinux extension has been deprecated and is no longer supported.

Unable to encrypt Linux disks

In some cases, the Linux disk encryption appears to be stuck at "OS disk encryption started" and SSH is disabled. The encryption process can take between 3-16 hours to finish on a stock gallery image. If multi-terabyte-sized data disks are added, the process might take days.

The Linux OS disk encryption sequence unmounts the OS drive temporarily. It then performs block-by-block encryption of the entire OS disk, before it remounts it in its encrypted state. Linux Disk Encryption doesn't allow for concurrent use of the VM while the encryption is in progress. The performance characteristics of the VM can make a significant difference in the time required to complete encryption. These characteristics include the size of the disk and whether the storage account is standard or premium (SSD) storage.

To check the encryption status, poll the **ProgressMessage** field returned from the [Get-AzVmDiskEncryptionStatus](#) command. While the OS drive is being encrypted, the VM enters a servicing state, and disables SSH to prevent any disruption to the ongoing process. The **EncryptionInProgress** message reports for the majority of the time while the encryption is in progress. Several hours later, a **VMRestartPending** message prompts you to restart the VM. For example:

```
PS > Get-AzVmDiskEncryptionStatus -ResourceGroupName "MyVirtualMachineResourceGroup" -VMName
"VirtualMachineName"
OsVolumeEncrypted      : EncryptionInProgress
DataVolumesEncrypted   : EncryptionInProgress
OsVolumeEncryptionSettings : Microsoft.Azure.Management.Compute.Models.DiskEncryptionSettings
ProgressMessage         : OS disk encryption started

PS > Get-AzVmDiskEncryptionStatus -ResourceGroupName "MyVirtualMachineResourceGroup" -VMName
"VirtualMachineName"
OsVolumeEncrypted      : VMRestartPending
DataVolumesEncrypted   : Encrypted
OsVolumeEncryptionSettings : Microsoft.Azure.Management.Compute.Models.DiskEncryptionSettings
ProgressMessage         : OS disk successfully encrypted, please reboot the VM
```

After you're prompted to reboot the VM, and after the VM restarts, you must wait 2-3 minutes for the reboot and for the final steps to be performed on the target. The status message changes when the encryption is finally complete. After this message is available, the encrypted OS drive is expected to be ready for use and the VM is ready to be used again.

In the following cases, we recommend that you restore the VM back to the snapshot or backup taken immediately before encryption:

- If the reboot sequence, described previously, doesn't happen.
- If the boot information, progress message, or other error indicators report that OS encryption has failed in the middle of this process. An example of a message is the "failed to unmount" error that is described in this guide.

Before the next attempt, reevaluate the characteristics of the VM and make sure that all of the prerequisites are satisfied.

Troubleshooting Azure Disk Encryption behind a firewall

When connectivity is restricted by a firewall, proxy requirement, or network security group (NSG) settings, the ability of the extension to perform needed tasks might be disrupted. This disruption can result in status messages such as "Extension status not available on the VM." In expected scenarios, the encryption fails to finish. The sections that follow have some common firewall problems that you might investigate.

Network security groups

Any network security group settings that are applied must still allow the endpoint to meet the documented network configuration [prerequisites](#) for disk encryption.

Azure Key Vault behind a firewall

When encryption is being enabled with [Azure AD credentials](#), the target VM must allow connectivity to both Azure Active Directory endpoints and Key Vault endpoints. Current Azure Active Directory authentication endpoints are maintained in sections 56 and 59 of the [Office 365 URLs and IP address ranges](#) documentation. Key Vault instructions are provided in the documentation on how to [Access Azure Key Vault behind a firewall](#).

Azure Instance Metadata Service

The VM must be able to access the [Azure Instance Metadata service](#) endpoint which uses a well-known non-routable IP address (`169.254.169.254`) that can be accessed only from within the VM. Proxy configurations that alter local HTTP traffic to this address (for example, adding an X-Forwarded-For header) are not supported.

Linux package management behind a firewall

At runtime, Azure Disk Encryption for Linux relies on the target distribution's package management system to install needed prerequisite components before enabling encryption. If the firewall settings prevent the VM from being able to download and install these components, then subsequent failures are expected. The steps to configure this package management system can vary by distribution. On Red Hat, when a proxy is required, you must make sure that the subscription-manager and yum are set up properly. For more information, see [How to troubleshoot subscription-manager and yum problems](#).

Troubleshooting encryption status

The portal may display a disk as encrypted even after it has been unencrypted within the VM. This can occur when low-level commands are used to directly unencrypt the disk from within the VM, instead of using the higher level Azure Disk Encryption management commands. The higher level commands not only unencrypt the disk from within the VM, but outside of the VM they also update important platform level encryption settings and extension settings associated with the VM. If these are not kept in alignment, the platform will not be able to report encryption status or provision the VM properly.

To disable Azure Disk Encryption with PowerShell, use [Disable-AzVMDiskEncryption](#) followed by [Remove-](#)

[AzVMDiskEncryptionExtension](#). Running Remove-AzVMDiskEncryptionExtension before the encryption is disabled will fail.

To disable Azure Disk Encryption with CLI, use `az vm encryption disable`.

Next steps

In this document, you learned more about some common problems in Azure Disk Encryption and how to troubleshoot those problems. For more information about this service and its capabilities, see the following articles:

- [Apply disk encryption in Azure Security Center](#)
- [Azure data encryption at rest](#)

Azure Disk Encryption for IaaS VMs FAQ

11/13/2019 • 7 minutes to read • [Edit Online](#)

This article provides answers to frequently asked questions (FAQ) about Azure Disk Encryption for Linux VMs. For more information about this service, see [Azure Disk Encryption overview](#).

Where is Azure Disk Encryption in general availability (GA)?

Azure Disk Encryption for Linux VMs is in general availability in all Azure public regions.

What user experiences are available with Azure Disk Encryption?

Azure Disk Encryption GA supports Azure Resource Manager templates, Azure PowerShell, and Azure CLI. The different user experiences give you flexibility. You have three different options for enabling disk encryption for your VMs. For more information on the user experience and step-by-step guidance available in Azure Disk Encryption, see [Azure Disk Encryption scenarios for Linux](#).

How much does Azure Disk Encryption cost?

There's no charge for encrypting VM disks with Azure Disk Encryption, but there are charges associated with the use of Azure Key Vault. For more information on Azure Key Vault costs, see the [Key Vault pricing](#) page.

How can I start using Azure Disk Encryption?

To get started, read the [Azure Disk Encryption overview](#).

What VM sizes and operating systems support Azure Disk Encryption?

The [Azure Disk Encryption overview](#) article lists the [VM sizes](#) and [VM operating systems](#) that support Azure Disk Encryption.

Can I encrypt both boot and data volumes with Azure Disk Encryption?

Yes, you can encrypt both boot and data volumes, or you can encrypt the data volume without having to encrypt the OS volume first.

After you've encrypted the OS volume, disabling encryption on the OS volume isn't supported. For Linux VMs in a scale set, only the data volume can be encrypted.

Can I encrypt an unmounted volume with Azure Disk Encryption?

No, Azure Disk Encryption only encrypts mounted volumes.

How do I rotate secrets or encryption keys?

To rotate secrets, just call the same command you used originally to enable disk encryption, specifying a different Key Vault. To rotate the key encryption key, call the same command you used originally to enable disk encryption, specifying the new key encryption.

WARNING

- If you have previously used [Azure Disk Encryption with Azure AD app](#) by specifying Azure AD credentials to encrypt this VM, you will have to continue use this option to encrypt your VM. You can't use Azure Disk Encryption on this encrypted VM as this isn't a supported scenario, meaning switching away from AAD application for this encrypted VM isn't supported yet.

How do I add or remove a key encryption key if I didn't originally use one?

To add a key encryption key, call the enable command again passing the key encryption key parameter. To remove a key encryption key, call the enable command again without the key encryption key parameter.

Does Azure Disk Encryption allow you to bring your own key (BYOK)?

Yes, you can supply your own key encryption keys. These keys are safeguarded in Azure Key Vault, which is the key store for Azure Disk Encryption. For more information on the key encryption keys support scenarios, see [Creating and configuring a key vault for Azure Disk Encryption](#).

Can I use an Azure-created key encryption key?

Yes, you can use Azure Key Vault to generate a key encryption key for Azure disk encryption use. These keys are safeguarded in Azure Key Vault, which is the key store for Azure Disk Encryption. For more information on the key encryption key, see [Creating and configuring a key vault for Azure Disk Encryption](#).

Can I use an on-premises key management service or HSM to safeguard the encryption keys?

You can't use the on-premises key management service or HSM to safeguard the encryption keys with Azure Disk Encryption. You can only use the Azure Key Vault service to safeguard the encryption keys. For more information on the key encryption key support scenarios, see [Creating and configuring a key vault for Azure Disk Encryption](#).

What are the prerequisites to configure Azure Disk Encryption?

There are prerequisites for Azure Disk Encryption. See the [Creating and configuring a key vault for Azure Disk Encryption](#) article to create a new key vault, or set up an existing key vault for disk encryption access to enable encryption, and safeguard secrets and keys. For more information on the key encryption key support scenarios, see [Creating and configuring a key vault for Azure Disk Encryption](#).

What are the prerequisites to configure Azure Disk Encryption with an Azure AD app (previous release)?

There are prerequisites for Azure Disk Encryption. See the [Azure Disk Encryption with Azure AD](#) content to create an Azure Active Directory application, create a new key vault, or set up an existing key vault for disk encryption access to enable encryption, and safeguard secrets and keys. For more information on the key encryption key support scenarios, see [Creating and configuring a key vault for Azure Disk Encryption with Azure AD](#).

Is Azure Disk Encryption using an Azure AD app (previous release) still supported?

Yes. Disk encryption using an Azure AD app is still supported. However, when encrypting new VMs it's

recommended that you use the new method rather than encrypting with an Azure AD app.

Can I migrate VMs that were encrypted with an Azure AD app to encryption without an Azure AD app?

Currently, there isn't a direct migration path for machines that were encrypted with an Azure AD app to encryption without an Azure AD app. Additionally, there isn't a direct path from encryption without an Azure AD app to encryption with an AD app.

What version of Azure PowerShell does Azure Disk Encryption support?

Use the latest version of the Azure PowerShell SDK to configure Azure Disk Encryption. Download the latest version of [Azure PowerShell](#). Azure Disk Encryption is *not* supported by Azure SDK version 1.1.0.

NOTE

The Linux Azure disk encryption preview extension "Microsoft.OSTCExtension.AzureDiskEncryptionForLinux" is deprecated. This extension was published for Azure disk encryption preview release. You should not use the preview version of the extension in your testing or production deployment.

For deployment scenarios like Azure Resource Manager (ARM), where you have a need to deploy Azure disk encryption extension for Linux VM to enable encryption on your Linux IaaS VM, you must use the Azure disk encryption production supported extension "Microsoft.Azure.Security.AzureDiskEncryptionForLinux".

Can I apply Azure Disk Encryption on my custom Linux image?

You can't apply Azure Disk Encryption on your custom Linux image. Only the gallery Linux images for the supported distributions called out previously are supported. Custom Linux images aren't currently supported.

Can I apply updates to a Linux Red Hat VM that uses the yum update?

Yes, you can perform a yum update on a Red Hat Linux VM. For more information, see [Linux package management behind a firewall](#).

What is the recommended Azure disk encryption workflow for Linux?

The following workflow is recommended to have the best results on Linux:

- Start from the unmodified stock gallery image corresponding to the needed OS distro and version
- Back up any mounted drives that will be encrypted. This back up allows for recovery if there's a failure, for example if the VM is rebooted before encryption has completed.
- Encrypt (can take several hours or even days depending on VM characteristics and size of any attached data disks)
- Customize, and add software to the image as needed.

If this workflow isn't possible, relying on [Storage Service Encryption](#) (SSE) at the platform storage account layer may be an alternative to full disk encryption using dm-crypt.

What is the disk "Bek Volume" or "/mnt/azure_bek_disk"?

The "Bek volume" is a local data volume that securely stores the encryption keys for Encrypted Azure VMs.

NOTE

Do not delete or edit any contents in this disk. Do not unmount the disk since the encryption key presence is needed for any encryption operations on the IaaS VM.

What encryption method does Azure Disk Encryption use?

Azure Disk Encryption uses the decrypt default of aes-xts-plain64 with a 256-bit volume master key.

If I use EncryptFormatAll and specify all volume types, will it erase the data on the data drives that we already encrypted?

No, data won't be erased from data drives that are already encrypted using Azure Disk Encryption. Similar to how EncryptFormatAll didn't re-encrypt the OS drive, it won't re-encrypt the already encrypted data drive. For more information, see the [EncryptFormatAll criteria](#).

Is XFS filesystem supported?

XFS volumes are supported for data disk encryption only with the EncryptFormatAll. This will reformat the volume, erasing any data previously there. For more information, see the [EncryptFormatAll criteria](#).

Can I backup and restore an encrypted VM?

Azure Backup provides a mechanism to backup and restore encrypted VM's within the same subscription and region. For instructions, please see [Back up and restore encrypted virtual machines with Azure Backup](#). Restoring an encrypted VM to a different region is not currently supported.

Where can I go to ask questions or provide feedback?

You can ask questions or provide feedback on the [Azure Disk Encryption forum](#).

Next steps

In this document, you learned more about the most frequent questions related to Azure Disk Encryption. For more information about this service, see the following articles:

- [Azure Disk Encryption Overview](#)
- [Apply disk encryption in Azure Security Center](#)
- [Azure data encryption at rest](#)

Azure Disk Encryption with Azure AD (previous release)

11/24/2019 • 2 minutes to read • [Edit Online](#)

The new release of Azure Disk Encryption eliminates the requirement for providing an Azure Active Directory (Azure AD) application parameter to enable VM disk encryption. With the new release, you're no longer required to provide Azure AD credentials during the enable encryption step. All new VMs must be encrypted without the Azure AD application parameters by using the new release. For instructions on how to enable VM disk encryption by using the new release, see [Azure Disk Encryption for Linux VMs](#). VMs that were already encrypted with Azure AD application parameters are still supported and should continue to be maintained with the AAD syntax.

This article provides supplements to [Azure Disk Encryption for Linux VMs](#) with additional requirements and prerequisites for Azure Disk Encryption with Azure AD (previous release).

The information in these sections remains the same:

- [Supported VMs and operating systems](#)
- [Additional VM requirements](#)

Networking and Group Policy

To enable the Azure Disk Encryption feature by using the older AAD parameter syntax, the infrastructure as a service (IaaS) VMs must meet the following network endpoint configuration requirements:

- To get a token to connect to your key vault, the IaaS VM must be able to connect to an Azure AD endpoint, [login.microsoftonline.com].
- To write the encryption keys to your key vault, the IaaS VM must be able to connect to the key vault endpoint.
- The IaaS VM must be able to connect to an Azure storage endpoint that hosts the Azure extension repository and an Azure storage account that hosts the VHD files.
- If your security policy limits access from Azure VMs to the internet, you can resolve the preceding URI and configure a specific rule to allow outbound connectivity to the IPs. For more information, see [Azure Key Vault behind a firewall](#).
- On Windows, if TLS 1.0 is explicitly disabled and the .NET version isn't updated to 4.6 or higher, the following registry change enables Azure Disk Encryption to select the more recent TLS version:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
"SystemDefaultTlsVersions"=dword:00000001
"SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v4.0.30319]
"SystemDefaultTlsVersions"=dword:00000001
"SchUseStrongCrypto"=dword:00000001`
```

Group Policy

- The Azure Disk Encryption solution uses the BitLocker external key protector for Windows IaaS VMs. For domain-joined VMs, don't push any Group Policies that enforce TPM protectors. For information about the Group Policy for the option **Allow BitLocker without a compatible TPM**, see [BitLocker Group Policy](#)

reference.

- BitLocker policy on domain-joined virtual machines with a custom Group Policy must include the following setting: [Configure user storage of BitLocker recovery information -> Allow 256-bit recovery key](#). Azure Disk Encryption fails when custom Group Policy settings for BitLocker are incompatible. On machines that don't have the correct policy setting, apply the new policy, force the new policy to update (gpupdate.exe /force), and then restart if it's required.

Encryption key storage requirements

Azure Disk Encryption requires Azure Key Vault to control and manage disk encryption keys and secrets. Your key vault and VMs must reside in the same Azure region and subscription.

For more information, see [Creating and configuring a key vault for Azure Disk Encryption with Azure AD \(previous release\)](#).

Next steps

- [Creating and configuring a key vault for Azure Disk Encryption with Azure AD \(previous release\)](#)
- [Enable Azure Disk Encryption with Azure AD on Linux VMs \(previous release\)](#)
- [Azure Disk Encryption prerequisites CLI script](#)
- [Azure Disk Encryption prerequisites PowerShell script](#)

Creating and configuring a key vault for Azure Disk Encryption with Azure AD (previous release)

10/2/2019 • 15 minutes to read • [Edit Online](#)

The new release of Azure Disk Encryption eliminates the requirement for providing an Azure AD application parameter to enable VM disk encryption. With the new release, you are no longer required to provide Azure AD credentials during the enable encryption step. All new VMs must be encrypted without the Azure AD application parameters using the new release. To view instructions to enable VM disk encryption using the new release, see [Azure Disk Encryption](#). VMs that were already encrypted with Azure AD application parameters are still supported and should continue to be maintained with the AAD syntax.

Azure Disk Encryption uses Azure Key Vault to control and manage disk encryption keys and secrets. For more information about key vaults, see [Get started with Azure Key Vault](#) and [Secure your key vault](#).

Creating and configuring a key vault for use with Azure Disk Encryption with Azure AD (previous release) involves three steps:

1. Create a key vault.
2. Set up an Azure AD application and service principal.
3. Set the key vault access policy for the Azure AD app.
4. Set key vault advanced access policies.

You may also, if you wish, generate or import a key encryption key (KEK).

See the main [Creating and configuring a key vault for Azure Disk Encryption](#) article for steps on how to [Install tools and connect to Azure](#).

NOTE

The steps in this article are automated in the [Azure Disk Encryption prerequisites CLI script](#) and [Azure Disk Encryption prerequisites PowerShell script](#).

Create a key vault

Azure Disk Encryption is integrated with [Azure Key Vault](#) to help you control and manage the disk-encryption keys and secrets in your key vault subscription. You can create a key vault or use an existing one for Azure Disk Encryption. For more information about key vaults, see [Get started with Azure Key Vault](#) and [Secure your key vault](#). You can use a Resource Manager template, Azure PowerShell, or the Azure CLI to create a key vault.

WARNING

In order to make sure the encryption secrets don't cross regional boundaries, Azure Disk Encryption needs the Key Vault and the VMs to be co-located in the same region. Create and use a Key Vault that is in the same region as the VM to be encrypted.

Create a key vault with PowerShell

You can create a key vault with Azure PowerShell using the [New-AzKeyVault](#) cmdlet. For additional cmdlets for Key Vault, see [Az.KeyVault](#).

1. Create a new resource group, if needed, with [New-AzResourceGroup](#). To list data center locations, use [Get-AzLocation](#).

```
# Get-AzLocation  
New-AzResourceGroup -Name 'MyKeyVaultResourceGroup' -Location 'East US'
```

2. Create a new key vault using [New-AzKeyVault](#)

```
New-AzKeyVault -VaultName 'MySecureVault' -ResourceGroupName 'MyKeyVaultResourceGroup' -Location 'East US'
```

3. Note the **Vault Name**, **Resource Group Name**, **Resource ID**, **Vault URI**, and the **Object ID** that are returned for later use when you encrypt the disks.

Create a key vault with Azure CLI

You can manage your key vault with Azure CLI using the [az keyvault](#) commands. To create a key vault, use [az keyvault create](#).

1. Create a new resource group, if needed, with [az group create](#). To list locations, use [az account list-locations](#)

```
# To list locations: az account list-locations --output table  
az group create -n "MyKeyVaultResourceGroup" -l "East US"
```

2. Create a new key vault using [az keyvault create](#).

```
az keyvault create --name "MySecureVault" --resource-group "MyKeyVaultResourceGroup" --location "East US"
```

3. Note the **Vault Name** (name), **Resource Group Name**, **Resource ID** (ID), **Vault URI**, and the **Object ID** that are returned for use later.

Create a key vault with a Resource Manager template

You can create a key vault by using the [Resource Manager template](#).

1. On the Azure quickstart template, click **Deploy to Azure**.
2. Select the subscription, resource group, resource group location, Key Vault name, Object ID, legal terms, and agreement, and then click **Purchase**.

Set up an Azure AD app and service principal

When you need encryption to be enabled on a running VM in Azure, Azure Disk Encryption generates and writes the encryption keys to your key vault. Managing encryption keys in your key vault requires Azure AD authentication. Create an Azure AD application for this purpose. For authentication purposes, you can use either client secret-based authentication or [client certificate-based Azure AD authentication](#).

Set up an Azure AD app and service principal with Azure PowerShell

To execute the following commands, get and use the [Azure AD PowerShell module](#).

1. Use the [New-AzADApplication](#) PowerShell cmdlet to create an Azure AD application.
MyApplicationHomePage and the MyApplicationUri can be any values you wish.

```

$aadClientSecret = "My AAD client secret"
$aadClientSecretSec = ConvertTo-SecureString -String $aadClientSecret -AsPlainText -Force
$azureAdApplication = New-AzADApplication -DisplayName "My Application Display Name" -HomePage
"https://MyApplicationHomePage" -IdentifierUris "https://MyApplicationUri" -Password
$aadClientSecretSec
$servicePrincipal = New-AzADServicePrincipal -ApplicationId $azureAdApplication.ApplicationId

```

2. The \$azureAdApplication.ApplicationId is the Azure AD ClientID and the \$aadClientSecret is the client secret that you will use later to enable Azure Disk Encryption. Safeguard the Azure AD client secret appropriately. Running `$azureAdApplication.ApplicationId` will show you the ApplicationID.

Set up an Azure AD app and service principal with Azure CLI

You can manage your service principals with Azure CLI using the `az ad sp` commands. For more information, see [Create an Azure service principal](#).

1. Create a new service principal.

```

az ad sp create-for-rbac --name "ServicePrincipalName" --password "My-AAD-client-secret" --skip-
assignment

```

2. The appId returned is the Azure AD ClientID used in other commands. It's also the SPN you'll use for az keyvault set-policy. The password is the client secret that you should use later to enable Azure Disk Encryption. Safeguard the Azure AD client secret appropriately.

Set up an Azure AD app and service principal though the Azure portal

Use the steps from the [Use portal to create an Azure Active Directory application and service principal that can access resources](#) article to create an Azure AD application. Each step listed below will take you directly to the article section to complete.

1. [Verify required permissions](#)
2. [Create an Azure Active Directory application](#)
 - You can use any name and sign-on URL you would like when creating the application.
3. [Get the application ID and the authentication key](#).
 - The authentication key is the client secret and is used as the AadClientSecret for Set-AzVMDiskEncryptionExtension.
 - The authentication key is used by the application as a credential to sign in to Azure AD. In the Azure portal, this secret is called keys, but has no relation to key vaults. Secure this secret appropriately.
 - The application ID will be used later as the AadClientId for Set-AzVMDiskEncryptionExtension and as the ServicePrincipalName for Set-AzKeyVaultAccessPolicy.

Set the key vault access policy for the Azure AD app

To write encryption secrets to a specified Key Vault, Azure Disk Encryption needs the Client ID and the Client Secret of the Azure Active Directory application that has permissions to write secrets to the Key Vault.

NOTE

Azure Disk Encryption requires you to configure the following access policies to your Azure AD client application: *WrapKey* and *Set* permissions.

Set the key vault access policy for the Azure AD app with Azure PowerShell

Your Azure AD application needs rights to access the keys or secrets in the vault. Use the [Set-](#)

[AzKeyVaultAccessPolicy](#) cmdlet to grant permissions to the application, using the client ID (which was generated when the application was registered) as the `-ServicePrincipalName` parameter value. To learn more, see the blog post [Azure Key Vault - Step by Step](#).

1. Set the key vault access policy for the AD application with PowerShell.

```
$keyVaultName = 'MySecureVault'  
$aadClientID = 'MyAadAppClientID'  
$KVRGname = 'MyKeyVaultResourceGroup'  
Set-AzKeyVaultAccessPolicy -VaultName $keyVaultName -ServicePrincipalName $aadClientID -  
PermissionsToKeys 'WrapKey' -PermissionsToSecrets 'Set' -ResourceGroupName $KVRGname
```

Set the key vault access policy for the Azure AD app with Azure CLI

Use `az keyvault set-policy` to set the access policy. For more information, see [Manage Key Vault using CLI 2.0](#).

Give the service principal you created via the Azure CLI access to get secrets and wrap keys with the following command:

```
```azurecli-interactive  
az keyvault set-policy --name "MySecureVault" --spn "<spn created with CLI/the Azure AD ClientID>" --key-
permissions wrapKey --secret-permissions set
```
```

Set the key vault access policy for the Azure AD app with the portal

1. Open the resource group with your key vault.
2. Select your key vault, go to **Access Policies**, then click **Add new**.
3. Under **Select principal**, search for the Azure AD application you created and select it.
4. For **Key permissions**, check **Wrap Key** under **Cryptographic Operations**.
5. For **Secret permissions**, check **Set** under **Secret Management Operations**.
6. Click **OK** to save the access policy.

Add new permissions - □ X

Add a new access policy - PREVIEW

★ Select principal
vmencrypt >

Configure from template (optional)

Key permissions
1 selected >

Secret permissions
1 selected >

Authorized application ⓘ
None selected

Key permissions

All Key Operations

All

Key Management Operations

Get

List

Update

Create

Import

Delete

Backup

Restore

Cryptographic Operations

Decrypt

Encrypt

UnwrapKey

WrapKey

Verify

Sign

Add new permissions - □ X

Add a new access policy - PREVIEW

★ Select principal
vmencrypt >

Configure from template (optional)

Key permissions
1 selected >

Secret permissions
1 selected >

Authorized application ⓘ
None selected

Secret permissions

All Secret Operations

All

Secret Management Operations

Get

List

Set

Delete

Set key vault advanced access policies

The Azure platform needs access to the encryption keys or secrets in your key vault to make them available to the VM for booting and decrypting the volumes. Enable disk encryption on the key vault or deployments will fail.

Set key vault advanced access policies with Azure PowerShell

Use the key vault PowerShell cmdlet [Set-AzKeyVaultAccessPolicy](#) to enable disk encryption for the key vault.

- **Enable Key Vault for disk encryption:** EnabledForDiskEncryption is required for Azure Disk encryption.

```
Set-AzKeyVaultAccessPolicy -VaultName 'MySecureVault' -ResourceGroupName 'MyKeyVaultResourceGroup' -  
EnabledForDiskEncryption
```

- **Enable Key Vault for deployment, if needed:** Enables the Microsoft.Compute resource provider to retrieve secrets from this key vault when this key vault is referenced in resource creation, for example when creating a virtual machine.

```
Set-AzKeyVaultAccessPolicy -VaultName 'MySecureVault' -ResourceGroupName 'MyKeyVaultResourceGroup' -  
EnabledForDeployment
```

- **Enable Key Vault for template deployment, if needed:** Enables Azure Resource Manager to get secrets from this key vault when this key vault is referenced in a template deployment.

```
Set-AzKeyVaultAccessPolicy -VaultName 'MySecureVault' -ResourceGroupName 'MyKeyVaultResourceGroup' -  
EnabledForTemplateDeployment
```

Set key vault advanced access policies using the Azure CLI

Use [az keyvault update](#) to enable disk encryption for the key vault.

- **Enable Key Vault for disk encryption:** Enabled-for-disk-encryption is required.

```
az keyvault update --name "MySecureVault" --resource-group "MyKeyVaultResourceGroup" --enabled-for-  
disk-encryption "true"
```

- **Enable Key Vault for deployment, if needed:** Allow Virtual Machines to retrieve certificates stored as secrets from the vault.

```
az keyvault update --name "MySecureVault" --resource-group "MyKeyVaultResourceGroup" --enabled-for-  
deployment "true"
```

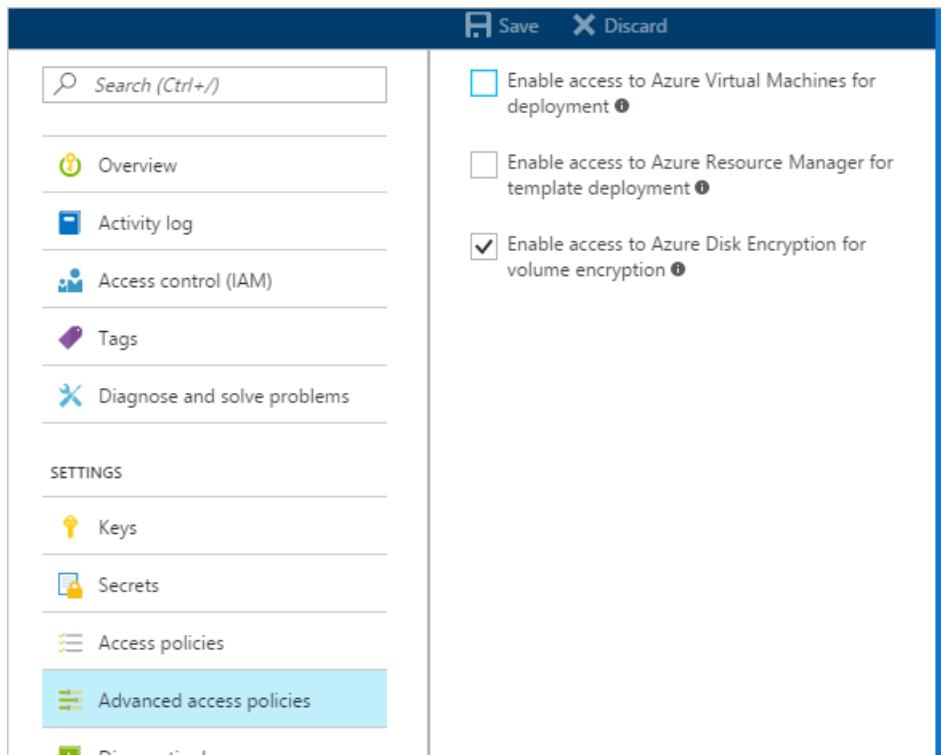
- **Enable Key Vault for template deployment, if needed:** Allow Resource Manager to retrieve secrets from the vault.

```
az keyvault update --name "MySecureVault" --resource-group "MyKeyVaultResourceGroup" --enabled-for-  
template-deployment "true"
```

Set key vault advanced access policies through the Azure portal

1. Select your keyvault, go to **Access Policies**, and [Click to show advanced access policies](#).
2. Select the box labeled **Enable access to Azure Disk Encryption for volume encryption**.
3. Select **Enable access to Azure Virtual Machines for deployment** and/or **Enable Access to Azure Resource Manager for template deployment**, if needed.

4. Click **Save**.



Set up a key encryption key (optional)

If you want to use a key encryption key (KEK) for an additional layer of security for encryption keys, add a KEK to your key vault. Use the [Add-AzKeyVaultKey](#) cmdlet to create a key encryption key in the key vault. You can also import a KEK from your on-premises key management HSM. For more information, see [Key Vault Documentation](#). When a key encryption key is specified, Azure Disk Encryption uses that key to wrap the encryption secrets before writing to Key Vault.

- When generating keys, use an RSA key type. Azure Disk Encryption does not yet support using Elliptic Curve keys.
- Your key vault secret and KEK URLs must be versioned. Azure enforces this restriction of versioning. For valid secret and KEK URLs, see the following examples:
 - Example of a valid secret URL:
<https://contosovault.vault.azure.net/secrets/EncryptionSecretWithKek/xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - Example of a valid KEK URL:
<https://contosovault.vault.azure.net/keys/diskencryptionkek/xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
- Azure Disk Encryption doesn't support specifying port numbers as part of key vault secrets and KEK URLs. For examples of non-supported and supported key vault URLs, see the following examples:
 - Unacceptable key vault URL
<https://contosovault.vault.azure.net:443/secrets/contososecret/xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - Acceptable key vault URL:
<https://contosovault.vault.azure.net/secrets/contososecret/xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Set up a key encryption key with Azure PowerShell

Before using the PowerShell script, you should be familiar with the Azure Disk Encryption prerequisites to understand the steps in the script. The sample script might need changes for your environment. This script creates all Azure Disk Encryption prerequisites and encrypts an existing IaaS VM, wrapping the disk encryption key by using a key encryption key.

```

# Step 1: Create a new resource group and key vault in the same location.
# Fill in 'MyLocation', 'MyKeyVaultResourceGroup', and 'MySecureVault' with your values.
# Use Get-AzLocation to get available locations and use the DisplayName.
# To use an existing resource group, comment out the line for New-AzResourceGroup

$Loc = 'MyLocation';
$KVRGname = 'MyKeyVaultResourceGroup';
$keyVaultName = 'MySecureVault';
New-AzResourceGroup -Name $KVRGname -Location $Loc;
New-AzKeyVault -VaultName $keyVaultName -ResourceGroupName $KVRGname -Location $Loc;
$keyVault = Get-AzKeyVault -VaultName $keyVaultName -ResourceGroupName $KVRGname;
$keyVaultResourceId = (Get-AzKeyVault -VaultName $keyVaultName -ResourceGroupName $KVRGname).ResourceId;
$diskEncryptionKeyVaultUrl = (Get-AzKeyVault -VaultName $keyVaultName -ResourceGroupName $KVRGname).VaultUri;

# Step 2: Create the AD application and service principal.
# Fill in 'MyAADClientSecret', "<My Application Display Name>", "<https://MyApplicationHomePage>", and "<https://MyApplicationUri>" with your values.
# MyApplicationHomePage and the MyApplicationUri can be any values you wish.

$aadClientSecret = 'MyAADClientSecret';
$aadClientSecretSec = ConvertTo-SecureString -String $aadClientSecret -AsPlainText -Force;
$azureAdApplication = New-AzADApplication -DisplayName "<My Application Display Name>" -HomePage "<https://MyApplicationHomePage>" -IdentifierUris "<https://MyApplicationUri>" -Password $aadClientSecretSec
$servicePrincipal = New-AzADServicePrincipal -ApplicationId $azureAdApplication.ApplicationId;
$aadClientID = $azureAdApplication.ApplicationId;

#Step 3: Enable the vault for disk encryption and set the access policy for the Azure AD application.

Set-AzKeyVaultAccessPolicy -VaultName $keyVaultName -ResourceGroupName $KVRGname -EnabledForDiskEncryption;
Set-AzKeyVaultAccessPolicy -VaultName $keyVaultName -ServicePrincipalName $aadClientID -PermissionsToKeys 'WrapKey' -PermissionsToSecrets 'Set' -ResourceGroupName $KVRGname;

#Step 4: Create a new key in the key vault with the Add-AzKeyVaultKey cmdlet.
# Fill in 'MyKeyEncryptionKey' with your value.

$keyEncryptionKeyName = 'MyKeyEncryptionKey';
Add-AzKeyVaultKey -VaultName $keyVaultName -Name $keyEncryptionKeyName -Destination 'Software';
$keyEncryptionKeyUrl = (Get-AzKeyVaultKey -VaultName $keyVaultName -Name $keyEncryptionKeyName).Key.kid;

#Step 5: Encrypt the disks of an existing IaaS VM
# Fill in 'MySecureVM' and 'MyVirtualMachineResourceGroup' with your values.

$VMName = 'MySecureVM';
$VMRGName = 'MyVirtualMachineResourceGroup';
Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGName -VMName $vmName -AadClientID $aadClientID -AadClientSecret $aadClientSecret -DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl -DiskEncryptionKeyId $keyVaultResourceId -KeyEncryptionKeyUrl $keyEncryptionKeyUrl -KeyEncryptionKeyId $keyVaultResourceId;

```

Certificate-based authentication (optional)

If you would like to use certificate authentication, you can upload one to your key vault and deploy it to the client. Before using the PowerShell script, you should be familiar with the Azure Disk Encryption prerequisites to understand the steps in the script. The sample script might need changes for your environment.

```

# Fill in "MyKeyVaultResourceGroup", "MySecureVault", and 'MyLocation' ('My location' only if needed)

$KVRGname = 'MyKeyVaultResourceGroup'
$keyVaultName= 'MySecureVault'

# Create a key vault and set enabledForDiskEncryption property on it.
# Comment out the next three lines if you already have an existing key vault enabled for encryption. No need

```

to set 'My location' in this case.

```
$Loc = 'MyLocation'
New-AzKeyVault -VaultName $KeyVaultName -ResourceGroupName $KVRGname -Location $Loc
Set-AzKeyVaultAccessPolicy -VaultName $KeyVaultName -ResourceGroupName $KVRGname -EnabledForDiskEncryption

#Setting some variables with the key vault information
$keyVault = Get-AzKeyVault -VaultName $KeyVaultName -ResourceGroupName $KVRGname
$DiskEncryptionKeyVaultUrl = $keyVault.VaultUri
$keyVaultResourceId = $keyVault.ResourceId

# Create the Azure AD application and associate the certificate with it.
# Fill in "C:\certificates\mycert.pfx", "Password", "<My Application Display Name>", "
<https://MyApplicationHomePage>", and "<https://MyApplicationUri>" with your values.
# MyApplicationHomePage and the MyApplicationUri can be any values you wish

$CertPath = "C:\certificates\mycert.pfx"
$CertPassword = "Password"
$Cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2($CertPath, $CertPassword)
$CertValue = [System.Convert]::ToBase64String($cert.GetRawCertData())

$AzureAdApplication = New-AzADApplication -DisplayName "<My Application Display Name>" -HomePage "
<https://MyApplicationHomePage>" -IdentifierUris "<https://MyApplicationUri>" -CertValue $CertValue
$ServicePrincipal = New-AzADServicePrincipal -ApplicationId $AzureAdApplication.ApplicationId

$AADClientID = $AzureAdApplication.ApplicationId
$aadClientCertThumbprint= $cert.Thumbprint

Set-AzKeyVaultAccessPolicy -VaultName $keyVaultName -ServicePrincipalName $aadClientID -PermissionsToKeys
'WrapKey' -PermissionsToSecrets 'Set' -ResourceGroupName $KVRGname

# Upload the pfx file to the key vault.
# Fill in "MyAADCert".

$keyVaultSecretName = "MyAADCert"
$fileContentBytes = get-content $CertPath -Encoding Byte
$fileContentEncoded = [System.Convert]::ToBase64String($fileContentBytes)
$jsonObject = @"
{
    "data" : "$fileContentEncoded",
    "dataType" : "pfx",
    "password" : "$CertPassword"
}
"@

$jsonObjectBytes = [System.Text.Encoding]::UTF8.GetBytes($jsonObject)
$jsonEncoded = [System.Convert]::ToBase64String($jsonObjectBytes)

#Set the secret and set the key vault policy for -EnabledForDeployment

$secret = ConvertTo-SecureString -String $jsonEncoded -AsPlainText -Force
Set-AzKeyVaultSecret -VaultName $keyVaultName -Name $keyVaultSecretName -SecretValue $secret
Set-AzKeyVaultAccessPolicy -VaultName $keyVaultName -ResourceGroupName $KVRGname -EnabledForDeployment

# Deploy the certificate to the VM
# Fill in 'MySecureVM' and 'MyVirtualMachineResourceGroup' with your values.

$vmName = 'MySecureVM'
$vmrgName = 'MyVirtualMachineResourceGroup'
$certUrl = (Get-AzKeyVaultSecret -VaultName $keyVaultName -Name $keyVaultSecretName).Id
$sourceVaultId = (Get-AzKeyVault -VaultName $keyVaultName -ResourceGroupName $KVRGname).ResourceId
$vm = Get-AzVM -ResourceGroupName $vmrgName -Name $vmName
$vm = Add-AzVMSecret -VM $vm -SourceVaultId $sourceVaultId -CertificateStore "My" -CertificateUrl $certUrl
Update-AzVM -VM $vm -ResourceGroupName $vmrgName

#Enable encryption on the VM using Azure AD client ID and the client certificate thumbprint

Set-AzVMDiskEncryptionExtension -ResourceGroupName $vmrgName -VMName $vmName -AadClientID $AADClientID -
AadClientCertThumbprint $AADClientCertThumbprint -DiskEncryptionKeyVaultUrl $DiskEncryptionKeyVaultUrl -
```

```
DiskEncryptionKeyVaultId $KeyVaultResourceId
```

Certificate-based authentication and a KEK (optional)

If you would like to use certificate authentication and wrap the encryption key with a KEK, you can use the below script as an example. Before using the PowerShell script, you should be familiar with all of the previous Azure Disk Encryption prerequisites to understand the steps in the script. The sample script might need changes for your environment.

IMPORTANT

Azure AD certificate-based authentication is currently not supported on Linux VMs.

```
# Fill in 'MyKeyVaultResourceGroup', 'MySecureVault', and 'MyLocation' (if needed)

$KVRGname = 'MyKeyVaultResourceGroup'
$keyVaultName= 'MySecureVault'

# Create a key vault and set enabledForDiskEncryption property on it.
# Comment out the next three lines if you already have an existing key vault enabled for encryption.

$Loc = 'MyLocation'
New-AzKeyVault -VaultName $keyVaultName -ResourceGroupName $KVRGname -Location $Loc
Set-AzKeyVaultAccessPolicy -VaultName $keyVaultName -ResourceGroupName $KVRGname -EnabledForDiskEncryption

# Create the Azure AD application and associate the certificate with it.
# Fill in "C:\certificates\mycert.pfx", "Password", "<My Application Display Name>", "
<https://MyApplicationHomePage>", and "<https://MyApplicationUri>" with your values.
# MyApplicationHomePage and the MyApplicationUri can be any values you wish

$CertPath = "C:\certificates\mycert.pfx"
$CertPassword = "Password"
$Cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2($CertPath, $CertPassword)
$CertValue = [System.Convert]::ToBase64String($cert.GetRawCertData())

$AzureAdApplication = New-AzADApplication -DisplayName "<My Application Display Name>" -HomePage "
<https://MyApplicationHomePage>" -IdentifierUris "<https://MyApplicationUri>" -CertValue $CertValue
$ServicePrincipal = New-AzADServicePrincipal -ApplicationId $AzureAdApplication.ApplicationId

$AADClientID = $AzureAdApplication.ApplicationId
$aadClientCertThumbprint= $cert.Thumbprint

## Give access for setting secrets and wrapping keys
Set-AzKeyVaultAccessPolicy -VaultName $keyVaultName -ServicePrincipalName $aadClientID -PermissionsToKeys
'WrapKey' -PermissionsToSecrets 'Set' -ResourceGroupName $KVRGname

# Upload the pfx file to the key vault.
# Fill in "MyAADCert".

$keyVaultSecretName = "MyAADCert"
$FileContentBytes = get-content $CertPath -Encoding Byte
$FileContentEncoded = [System.Convert]::ToBase64String($fileContentBytes)
$jsonObject = @"
{
    "data" : "$filecontentencoded",
    "dataType" : "pfx",
    "password" : "$CertPassword"
}
"@

$jsonObjectBytes = [System.Text.Encoding]::UTF8.GetBytes($jsonObject)
$jsonEncoded = [System.Convert]::ToBase64String($jsonObjectBytes)
```

```

#Set the secret and set the key vault policy for deployment

$Secret = ConvertTo-SecureString -String $JSONEncoded -AsPlainText -Force
Set-AzKeyVaultSecret -VaultName $KeyVaultName -Name $KeyVaultSecretName -SecretValue $Secret
Set-AzKeyVaultAccessPolicy -VaultName $KeyVaultName -ResourceGroupName $KVRGname -EnabledForDeployment

#Setting some variables with the key vault information and generating a KEK
# Fill in 'KEKName'

$KEKName = 'KEKName'
$keyVault = Get-AzKeyVault -VaultName $KeyVaultName -ResourceGroupName $KVRGname
$DiskEncryptionKeyVaultUrl = $keyVault.VaultUri
$keyVaultResourceId = $keyVault.ResourceId
$KEK = Add-AzKeyVaultKey -VaultName $KeyVaultName -Name $KEKName -Destination "Software"
$keyEncryptionKeyUrl = $KEK.Key.kid


# Deploy the certificate to the VM
# Fill in 'MySecureVM' and 'MyVirtualMachineResourceGroup' with your values.

$VMName = 'MySecureVM';
$VMRGName = 'MyVirtualMachineResourceGroup';
$CertUrl = (Get-AzKeyVaultSecret -VaultName $KeyVaultName -Name $KeyVaultSecretName).Id
$SourceVaultId = (Get-AzKeyVault -VaultName $KeyVaultName -ResourceGroupName $KVRGName).ResourceId
$VM = Get-AzVM -ResourceGroupName $VMRGName -Name $VMName
$VM = Add-AzVMSecret -VM $VM -SourceVaultId $SourceVaultId -CertificateStore "My" -CertificateUrl $CertUrl
Update-AzVM -VM $VM -ResourceGroupName $VMRGName

#Enable encryption on the VM using Azure AD client ID and the client certificate thumbprint

Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGName -VMName $VMName -AadClientID $AADClientID -
AadClientCertThumbprint $AADClientCertThumbprint -DiskEncryptionKeyVaultUrl $DiskEncryptionKeyVaultUrl -
DiskEncryptionKeyId $KeyVaultResourceId -KeyEncryptionKeyUrl $keyEncryptionKeyUrl -
KeyEncryptionKeyId $KeyVaultResourceId

```

Next steps

[Enable Azure Disk Encryption with Azure AD on Linux VMs \(previous release\)](#)

Enable Azure Disk Encryption with Azure AD on Linux VMs (previous release)

11/24/2019 • 17 minutes to read • [Edit Online](#)

The new release of Azure Disk Encryption eliminates the requirement for providing an Azure Active Directory (Azure AD) application parameter to enable VM disk encryption. With the new release, you're no longer required to provide Azure AD credentials during the enable encryption step. All new VMs must be encrypted without the Azure AD application parameters by using the new release. For instructions on how to enable VM disk encryption by using the new release, see [Azure Disk Encryption for Linux VMs](#). VMs that were already encrypted with Azure AD application parameters are still supported and should continue to be maintained with the AAD syntax.

You can enable many disk-encryption scenarios, and the steps might vary according to the scenario. The following sections cover the scenarios in greater detail for Linux infrastructure as a service (IaaS) VMs. You can only apply disk encryption to virtual machines of [supported VM sizes and operating systems](#). You must also meet the following prerequisites:

- [Additional requirements for VMs](#)
- [Networking and Group Policy](#)
- [Encryption key storage requirements](#)

Take a [snapshot](#), make a backup, or both before you encrypt the disks. Backups ensure that a recovery option is possible if an unexpected failure occurs during encryption. VMs with managed disks require a backup before encryption occurs. After a backup is made, you can use the `Set-AzVMDiskEncryptionExtension` cmdlet to encrypt managed disks by specifying the `-skipVmBackup` parameter. For more information about how to back up and restore encrypted VMs, see [Azure Backup](#).

WARNING

- If you previously used [Azure Disk Encryption with the Azure AD app](#) to encrypt this VM, you must continue to use this option to encrypt your VM. You can't use [Azure Disk Encryption](#) on this encrypted VM because this isn't a supported scenario, which means switching away from the Azure AD application for this encrypted VM isn't supported yet.
- To make sure the encryption secrets don't cross regional boundaries, Azure Disk Encryption needs the key vault and the VMs to be co-located in the same region. Create and use a key vault that's in the same region as the VM to be encrypted.
- When you encrypt Linux OS volumes, the process can take a few hours. It's normal for Linux OS volumes to take longer than data volumes to encrypt.
- When you encrypt Linux OS volumes, the VM should be considered unavailable. We strongly recommend that you avoid SSH logins while the encryption is in progress to avoid blocking any open files that need to be accessed during the encryption process. To check progress, use the `Get-AzVMDiskEncryptionStatus` or `vm encryption show` commands. You can expect this process to take a few hours for a 30-GB OS volume, plus additional time for encrypting data volumes. Data volume encryption time is proportional to the size and quantity of the data volumes unless the **encrypt format all** option is used.
- Disabling encryption on Linux VMs is only supported for data volumes. It's not supported on data or OS volumes if the OS volume has been encrypted.

Enable encryption on an existing or running IaaS Linux VM

In this scenario, you can enable encryption by using the Azure Resource Manager template, PowerShell cmdlets, or Azure CLI commands.

IMPORTANT

It's mandatory to take a snapshot or back up a managed disk-based VM instance outside of and prior to enabling Azure Disk Encryption. You can take a snapshot of the managed disk from the Azure portal, or you can use [Azure Backup](#). Backups ensure that a recovery option is possible in the case of any unexpected failure during encryption. After a backup is made, use the Set-AzVMDiskEncryptionExtension cmdlet to encrypt managed disks by specifying the -skipVmBackup parameter. The Set-AzVMDiskEncryptionExtension command fails against managed disk-based VMs until a backup is made and this parameter is specified.

Encrypting or disabling encryption might cause the VM to reboot.

Enable encryption on an existing or running Linux VM by using the Azure CLI

You can enable disk encryption on your encrypted VHD by installing and using the [Azure CLI 2.0](#) command-line tool. You can use it in your browser with [Azure Cloud Shell](#), or you can install it on your local machine and use it in any PowerShell session. To enable encryption on existing or running IaaS Linux VMs in Azure, use the following CLI commands:

Use the [az vm encryption enable](#) command to enable encryption on a running IaaS virtual machine in Azure.

- **Encrypt a running VM by using a client secret:**

```
az vm encryption enable --resource-group "MyVirtualMachineResourceGroup" --name "MySecureVM" --aad-client-id "<my spn created with CLI/my Azure AD ClientID>" --aad-client-secret "My-AAD-client-secret" --disk-encryption-keyvault "MySecureVault" --volume-type [All|OS|Data]
```

- **Encrypt a running VM by using KEK to wrap the client secret:**

```
az vm encryption enable --resource-group "MyVirtualMachineResourceGroup" --name "MySecureVM" --aad-client-id "<my spn created with CLI which is the Azure AD ClientID>" --aad-client-secret "My-AAD-client-secret" --disk-encryption-keyvault "MySecureVault" --key-encryption-key "MyKEK_URI" --key-encryption-keyvault "MySecureVaultContainingTheKEK" --volume-type [All|OS|Data]
```

NOTE

The syntax for the value of the disk-encryption-keyvault parameter is the full identifier string:
/subscriptions/[subscription-id-guid]/resourceGroups/[resource-group-name]/providers/Microsoft.KeyVault/vaults/[keyvault-name].

The syntax for the value of the key-encryption-key parameter is the full URI to the KEK as in: https://[keyvault-name].vault.azure.net/keys/[kekname]/[kek-unique-id].

- **Verify that the disks are encrypted:** To check on the encryption status of an IaaS VM, use the [az vm encryption show](#) command.

```
az vm encryption show --name "MySecureVM" --resource-group "MyVirtualMachineResourceGroup"
```

- **Disable encryption:** To disable encryption, use the [az vm encryption disable](#) command. Disabling encryption is only allowed on data volumes for Linux VMs.

```
az vm encryption disable --name "MySecureVM" --resource-group "MyVirtualMachineResourceGroup" --volume-type DATA
```

Enable encryption on an existing or running Linux VM by using PowerShell

Use the [Set-AzVMDiskEncryptionExtension](#) cmdlet to enable encryption on a running IaaS virtual machine in Azure. Take a [snapshot](#) or make a backup of the VM with [Azure Backup](#) before the disks are encrypted. The `-skipVmBackup` parameter is already specified in the PowerShell scripts to encrypt a running Linux VM.

- **Encrypt a running VM by using a client secret:** The following script initializes your variables and runs the Set-AzVMDiskEncryptionExtension cmdlet. The resource group, VM, key vault, Azure AD app, and client secret should have already been created as prerequisites. Replace MyVirtualMachineResourceGroup, MyKeyVaultResourceGroup, MySecureVM, MySecureVault, My-AAD-client-ID, and My-AAD-client-secret with your values. Modify the `-VolumeType` parameter to specify which disks you're encrypting.

```
$VMRGName = 'MyVirtualMachineResourceGroup';
$KVRGname = 'MyKeyVaultResourceGroup';
$vmName = 'MySecureVM';
$aadClientID = 'My-AAD-client-ID';
$aadClientSecret = 'My-AAD-client-secret';
$keyVaultName = 'MySecureVault';
$keyVault = Get-AzKeyVault -VaultName $keyVaultName -ResourceGroupName $KVRGname;
$diskEncryptionKeyVaultUrl = $keyVault.VaultUri;
$keyVaultResourceId = $keyVault.ResourceId;
$sequenceVersion = [Guid]::NewGuid();

Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGName -VMName $vmName -AadClientID
$aadClientID -AadClientSecret $aadClientSecret -DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl -
DiskEncryptionKeyVaultId $keyVaultResourceId -VolumeType '[All|OS|Data]' -SequenceVersion
$sequenceVersion -skipVmBackup;
```

- **Encrypt a running VM by using KEK to wrap the client secret:** Azure Disk Encryption lets you specify an existing key in your key vault to wrap disk encryption secrets that were generated while enabling encryption. When a key encryption key is specified, Azure Disk Encryption uses that key to wrap the encryption secrets before writing to the key vault. Modify the `-VolumeType` parameter to specify which disks you're encrypting.

```
$KVRGname = 'MyKeyVaultResourceGroup';
$VMRGName = 'MyVirtualMachineResourceGroup';
$aadClientID = 'My-AAD-client-ID';
$aadClientSecret = 'My-AAD-client-secret';
$keyVaultName = 'MySecureVault';
$keyEncryptionKeyName = 'MyKeyEncryptionKey';
$keyVault = Get-AzKeyVault -VaultName $keyVaultName -ResourceGroupName $KVRGname;
$diskEncryptionKeyVaultUrl = $keyVault.VaultUri;
$keyVaultResourceId = $keyVault.ResourceId;
$keyEncryptionKeyUrl = (Get-AzKeyVaultKey -VaultName $keyVaultName -Name
$keyEncryptionKeyName).Key.kid;
$sequenceVersion = [Guid]::NewGuid();

Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGName -VMName $vmName -AadClientID
$aadClientID -AadClientSecret $aadClientSecret -DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl -
DiskEncryptionKeyVaultId $keyVaultResourceId -KeyEncryptionKeyUrl $keyEncryptionKeyUrl -
KeyEncryptionKeyVaultId $keyVaultResourceId -VolumeType '[All|OS|Data]' -SequenceVersion
$sequenceVersion -skipVmBackup;
```

NOTE

The syntax for the value of the disk-encryption-keyvault parameter is the full identifier string:
/subscriptions/[subscription-id-guid]/resourceGroups/[KVresource-group-name]/providers/Microsoft.KeyVault/vaults/[keyvault-name].

The syntax for the value of the key-encryption-key parameter is the full URI to the KEK as in: https://[keyvault-name].vault.azure.net/keys/[kekname]/[kek-unique-id].

- **Verify that the disks are encrypted:** To check on the encryption status of an IaaS VM, use the [Get-AzVmDiskEncryptionStatus](#) cmdlet.

```
Get-AzVmDiskEncryptionStatus -ResourceGroupName MyVirtualMachineResourceGroup -VMName MySecureVM
```

- **Disable disk encryption:** To disable the encryption, use the [Disable-AzureRmVMDiskEncryption](#) cmdlet. Disabling encryption is only allowed on data volumes for Linux VMs.

```
Disable-AzVMDiskEncryption -ResourceGroupName 'MyVirtualMachineResourceGroup' -VMName 'MySecureVM'
```

Enable encryption on an existing or running IaaS Linux VM with a template

You can enable disk encryption on an existing or running IaaS Linux VM in Azure by using the [Resource Manager template](#).

1. Select **Deploy to Azure** on the Azure quickstart template.
2. Select the subscription, resource group, resource group location, parameters, legal terms, and agreement. Select **Create** to enable encryption on the existing or running IaaS VM.

The following table lists Resource Manager template parameters for existing or running VMs that use an Azure AD client ID:

| PARAMETER | DESCRIPTION |
|---------------------|---|
| AADClientID | Client ID of the Azure AD application that has permissions to write secrets to the key vault. |
| AADClientSecret | Client secret of the Azure AD application that has permissions to write secrets to your key vault. |
| keyVaultName | Name of the key vault that the key should be uploaded to. You can get it by using the Azure CLI command
<pre>az keyvault show --name "MySecureVault" --query KVresourceGroup</pre> |
| keyEncryptionKeyURL | URL of the key encryption key that's used to encrypt the generated key. This parameter is optional if you select nokek in the UseExistingKek drop-down list. If you select kek in the UseExistingKek drop-down list, you must enter the <i>keyEncryptionKeyURL</i> value. |

| PARAMETER | DESCRIPTION |
|-----------------|---|
| volumeType | Type of volume that the encryption operation is performed on. Valid supported values are <i>OS</i> or <i>All</i> . (See supported Linux distributions and their versions for OS and data disks in the prerequisites section earlier.) |
| sequenceVersion | Sequence version of the BitLocker operation. Increment this version number every time a disk-encryption operation is performed on the same VM. |
| vmName | Name of the VM that the encryption operation is to be performed on. |
| passphrase | Type a strong passphrase as the data encryption key. |

Use the EncryptFormatAll feature for data disks on Linux IaaS VMs

The `EncryptFormatAll` parameter reduces the time for Linux data disks to be encrypted. Partitions that meet certain criteria are formatted (with their current file system). Then they're remounted back to where they were before command execution. If you want to exclude a data disk that meets the criteria, you can unmount it before you run the command.

After you run this command, any drives that were mounted previously are reformatted. Then the encryption layer starts on top of the now empty drive. When this option is selected, the ephemeral resource disk attached to the VM is also encrypted. If the ephemeral drive is reset, it's reformatted and re-encrypted for the VM by the Azure Disk Encryption solution at the next opportunity.

WARNING

`EncryptFormatAll` shouldn't be used when there's needed data on a VM's data volumes. You can exclude disks from encryption by unmounting them. Try out the `EncryptFormatAll` parameter on a test VM first to understand the feature parameter and its implication before you try it on the production VM. The `EncryptFormatAll` option formats the data disk, so all the data on it will be lost. Before you proceed, verify that any disks you want to exclude are properly unmounted. If you set this parameter while you update encryption settings, it might lead to a reboot before the actual encryption. In this case, you also want to remove the disk you don't want formatted from the `fstab` file. Similarly, you should add the partition you want encrypt-formatted to the `fstab` file before you initiate the encryption operation.

EncryptFormatAll criteria

The parameter goes through all partitions and encrypts them as long as they meet *all* of the following criteria:

- Is not a root/OS/boot partition
- Is not already encrypted
- Is not a BEK volume
- Is not a RAID volume
- Is not an LVM volume
- Is mounted

Encrypt the disks that compose the RAID or LVM volume rather than the RAID or LVM volume.

Use the EncryptFormatAll parameter with a template

To use the `EncryptFormatAll` option, use any preexisting Azure Resource Manager template that encrypts a Linux VM and change the **EncryptionOperation** field for the `AzureDiskEncryption` resource.

1. As an example, use the [Resource Manager template to encrypt a running Linux IaaS VM](#).
2. Select **Deploy to Azure** on the Azure quickstart template.
3. Change the **EncryptionOperation** field from **EnableEncryption** to **EnableEncryptionFormatAll**.
4. Select the subscription, resource group, resource group location, other parameters, legal terms, and agreement. Select **Create** to enable encryption on the existing or running IaaS VM.

Use the EncryptFormatAll parameter with a PowerShell cmdlet

Use the [Set-AzVMDiskEncryptionExtension](#) cmdlet with the EncryptFormatAll parameter.

Encrypt a running VM by using a client secret and EncryptFormatAll: As an example, the following script initializes your variables and runs the Set-AzVMDiskEncryptionExtension cmdlet with the EncryptFormatAll parameter. The resource group, VM, key vault, Azure AD app, and client secret should have already been created as prerequisites. Replace MyKeyVaultResourceGroup, MyVirtualMachineResourceGroup, MySecureVM, MySecureVault, My-AAD-client-ID, and My-AAD-client-secret with your values.

```
$KVRGname = 'MyKeyVaultResourceGroup';
$VMRGName = 'MyVirtualMachineResourceGroup';
$aadClientID = 'My-AAD-client-ID';
$aadClientSecret = 'My-AAD-client-secret';
$keyVaultName = 'MySecureVault';
$keyVault = Get-AzKeyVault -VaultName $keyVaultName -ResourceGroupName $KVRGname;
$diskEncryptionKeyVaultUrl = $keyVault.VaultUri;
$keyVaultResourceId = $keyVault.ResourceId;

Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGName -VMName $vmName -AadClientID $aadClientID -
AadClientSecret $aadClientSecret -DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl -
DiskEncryptionKeyVaultId $keyVaultResourceId -EncryptFormatAll
```

Use the EncryptFormatAll parameter with Logical Volume Manager (LVM)

We recommend an LVM-on-crypt setup. For all the following examples, replace the device-path and mountpoints with whatever suits your use case. This setup can be done as follows:

- Add the data disks that will compose the VM.
 - Format, mount, and add these disks to the fstab file.
1. Format the newly added disk. We use symlinks generated by Azure here. Using symlinks avoids problems related to device names changing. For more information, see [Troubleshoot device names problems](#).

```
`mkfs -t ext4 /dev/disk/azure/scsi1/lun0`
```

2. Mount the disks.

```
`mount /dev/disk/azure/scsi1/lun0 /mnt/mountpoint`
```

3. Add to fstab.

```
`echo "/dev/disk/azure/scsi1/lun0 /mnt/mountpoint ext4 defaults,nofail 1 2" >> /etc/fstab`
```

4. Run the Set-AzVMDiskEncryptionExtension PowerShell cmdlet with -EncryptFormatAll to encrypt these disks.

```
azurerepowershell-interactive Set-AzVMDiskEncryptionExtension -ResourceGroupName "MySecureGroup" -
VMName "MySecureVM" -DiskEncryptionKeyVaultUrl "https://mykeyvault.vault.azure.net/" -
EncryptFormatAll
```

- Set up LVM on top of these new disks. Note the encrypted drives are unlocked after the VM has finished booting. So, the LVM mounting will also have to be subsequently delayed.

New IaaS VMs created from customer-encrypted VHD and encryption keys

In this scenario, you can enable encrypting by using the Resource Manager template, PowerShell cmdlets, or CLI commands. The following sections explain in greater detail the Resource Manager template and CLI commands.

Use the instructions in the appendix for preparing pre-encrypted images that can be used in Azure. After the image is created, you can use the steps in the next section to create an encrypted Azure VM.

- [Prepare a pre-encrypted Linux VHD](#)

IMPORTANT

It's mandatory to take a snapshot or back up a managed disk-based VM instance outside of and prior to enabling Azure Disk Encryption. You can take a snapshot of the managed disk from the portal, or you can use [Azure Backup](#). Backups ensure that a recovery option is possible in the case of any unexpected failure during encryption. After a backup is made, use the `Set-AzVMDiskEncryptionExtension` cmdlet to encrypt managed disks by specifying the `-skipVmBackup` parameter. The `Set-AzVMDiskEncryptionExtension` command fails against managed disk-based VMs until a backup is made and this parameter is specified.

Encrypting or disabling encryption might cause the VM to reboot.

Use Azure PowerShell to encrypt IaaS VMs with pre-encrypted VHDS

You can enable disk encryption on your encrypted VHD by using the PowerShell cmdlet [Set-AzVMDisk](#). The following example gives you some common parameters.

```
$VirtualMachine = New-AzVMConfig -VMName "MySecureVM" -VMSize "Standard_A1"
$VirtualMachine = Set-AzVMDisk -VM $VirtualMachine -Name "SecureOSDisk" -VhdUri "os.vhd" Caching ReadWrite -
Windows -CreateOption "Attach" -DiskEncryptionKeyUrl
"https://mytestvault.vault.azure.net/secrets/Test1/514ceb769c984379a7e0230bddaaaaaa" -DiskEncryptionKeyVaultId
"/subscriptions/00000000-0000-0000-0000-
00000000/resourceGroups/myresourcegroup/providers/Microsoft.KeyVault/vaults/mytestvault"
New-AzVM -VM $VirtualMachine -ResourceGroupName "MyVirtualMachineResourceGroup"
```

Enable encryption on a newly added data disk

You can add a new data disk by using [az vm disk attach](#) or [through the Azure portal](#). Before you can encrypt, you need to mount the newly attached data disk first. You must request encryption of the data drive because the drive will be unusable while encryption is in progress.

Enable encryption on a newly added disk with the Azure CLI

If the VM was previously encrypted with "All," then the `--volume-type` parameter should remain All. All includes both OS and data disks. If the VM was previously encrypted with a volume type of "OS," then the `--volume-type` parameter should be changed to All so that both the OS and the new data disk will be included. If the VM was encrypted with only the volume type of "Data," then it can remain Data as demonstrated here. Adding and attaching a new data disk to a VM isn't sufficient preparation for encryption. The newly attached disk must also be formatted and properly mounted within the VM before you enable encryption. On Linux, the disk must be mounted in `/etc/fstab` with a [persistent block device name](#).

In contrast to Powershell syntax, the CLI doesn't require you to provide a unique sequence version when you enable encryption. The CLI automatically generates and uses its own unique sequence version value.

- **Encrypt a running VM by using a client secret:**

```
az vm encryption enable --resource-group "MyVirtualMachineResourceGroup" --name "MySecureVM" --aad-client-id "<my spn created with CLI/my Azure AD ClientID>" --aad-client-secret "My-AAD-client-secret" --disk-encryption-keyvault "MySecureVault" --volume-type "Data"
```

- **Encrypt a running VM by using KEK to wrap the client secret:**

```
az vm encryption enable --resource-group "MyVirtualMachineResourceGroup" --name "MySecureVM" --aad-client-id "<my spn created with CLI which is the Azure AD ClientID>" --aad-client-secret "My-AAD-client-secret" --disk-encryption-keyvault "MySecureVault" --key-encryption-key "MyKEK_URI" --key-encryption-keyvault "MySecureVaultContainingTheKEK" --volume-type "Data"
```

Enable encryption on a newly added disk with Azure PowerShell

When you use Powershell to encrypt a new disk for Linux, a new sequence version needs to be specified. The sequence version has to be unique. The following script generates a GUID for the sequence version.

- **Encrypt a running VM by using a client secret:** The following script initializes your variables and runs the Set-AzVMDiskEncryptionExtension cmdlet. The resource group, VM, key vault, Azure AD app, and client secret should have already been created as prerequisites. Replace MyVirtualMachineResourceGroup, MyKeyVaultResourceGroup, MySecureVM, MySecureVault, My-AAD-client-ID, and My-AAD-client-secret with your values. The -VolumeType parameter is set to data disks and not the OS disk. If the VM was previously encrypted with a volume type of "OS" or "All," then the -VolumeType parameter should be changed to All so that both the OS and the new data disk will be included.

```
$KVRGname = 'MyKeyVaultResourceGroup';
$VMRGName = 'MyVirtualMachineResourceGroup';
$vmName = 'MySecureVM';
$aadClientID = 'My-AAD-client-ID';
$aadClientSecret = 'My-AAD-client-secret';
$keyVaultName = 'MySecureVault';
$keyVault = Get-AzKeyVault -VaultName $keyVaultName -ResourceGroupName $KVRGname;
$diskEncryptionKeyVaultUrl = $keyVault.VaultUri;
$keyVaultResourceId = $keyVault.ResourceId;
$sequenceVersion = [Guid]::NewGuid();

Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGName -VMName $vmName -AadClientID
$aadClientID -AadClientSecret $aadClientSecret -DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl -
DiskEncryptionKeyId $keyVaultResourceId -VolumeType 'data' -SequenceVersion $sequenceVersion;
```

- **Encrypt a running VM by using KEK to wrap the client secret:** Azure Disk Encryption lets you specify an existing key in your key vault to wrap disk encryption secrets that were generated while enabling encryption. When a key encryption key is specified, Azure Disk Encryption uses that key to wrap the encryption secrets before writing to the key vault. The -VolumeType parameter is set to data disks and not the OS disk. If the VM was previously encrypted with a volume type of "OS" or "All," then the -VolumeType parameter should be changed to All so that both the OS and the new data disk will be included.

```

$KVRGname = 'MyKeyVaultResourceGroup';
$VMRGName = 'MyVirtualMachineResourceGroup';
$vmName = 'MyExtraSecureVM';
$aadClientID = 'My-AAD-client-ID';
$aadClientSecret = 'My-AAD-client-secret';
$keyVaultName = 'MySecureVault';
$keyEncryptionKeyName = 'MyKeyEncryptionKey';
$keyVault = Get-AzKeyVault -VaultName $keyVaultName -ResourceGroupName $KVRGname;
$diskEncryptionKeyVaultUrl = $keyVault.VaultUri;
$keyVaultResourceId = $keyVault.ResourceId;
$keyEncryptionKeyUrl = (Get-AzKeyVaultKey -VaultName $keyVaultName -Name
$keyEncryptionKeyName).Key.kid;
$sequenceVersion = [Guid]::NewGuid();

Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGName -VMName $vmName -AadClientID
$aadClientID -AadClientSecret $aadClientSecret -DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl -
DiskEncryptionKeyVaultId $keyVaultResourceId -KeyEncryptionKeyUrl $keyEncryptionKeyUrl -
KeyEncryptionKeyVaultId $keyVaultResourceId -VolumeType 'data' -SequenceVersion $sequenceVersion;

```

NOTE

The syntax for the value of the disk-encryption-keyvault parameter is the full identifier string: /subscriptions/[subscription-id-guid]/resourceGroups/[resource-group-name]/providers/Microsoft.KeyVault/vaults/[keyvault-name].

The syntax for the value of the key-encryption-key parameter is the full URI to the KEK as in: https://[keyvault-name].vault.azure.net/keys/[kekname]/[kek-unique-id].

Disable encryption for Linux VMs

You can disable encryption by using Azure PowerShell, the Azure CLI, or a Resource Manager template.

IMPORTANT

Disabling encryption with Azure Disk Encryption on Linux VMs is only supported for data volumes. It's not supported on data or OS volumes if the OS volume has been encrypted.

- Disable disk encryption with Azure PowerShell:** To disable encryption, use the [Disable-AzureRmVMDiskEncryption](#) cmdlet.

```
Disable-AzVMDiskEncryption -ResourceGroupName 'MyVirtualMachineResourceGroup' -VMName 'MySecureVM'
[--volume-type {ALL, DATA, OS}]
```

- Disable encryption with the Azure CLI:** To disable encryption, use the [az vm encryption disable](#) command.

```
az vm encryption disable --name "MySecureVM" --resource-group "MyVirtualMachineResourceGroup" --
volume-type [ALL, DATA, OS]
```

- Disable encryption with a Resource Manager template:** To disable encryption, use the [Disable encryption on a running Linux VM](#) template.

- Select **Deploy to Azure**.
- Select the subscription, resource group, location, VM, legal terms, and agreement.
- Select **Purchase** to disable disk encryption on a running Windows VM.

Next steps

- [Azure Disk Encryption for Linux overview](#)
- [Creating and configuring a key vault for Azure Disk Encryption with Azure AD \(previous release\)](#)

What is role-based access control (RBAC) for Azure resources?

12/23/2019 • 7 minutes to read • [Edit Online](#)

Access management for cloud resources is a critical function for any organization that is using the cloud. Role-based access control (RBAC) helps you manage who has access to Azure resources, what they can do with those resources, and what areas they have access to.

RBAC is an authorization system built on [Azure Resource Manager](#) that provides fine-grained access management of Azure resources.

What can I do with RBAC?

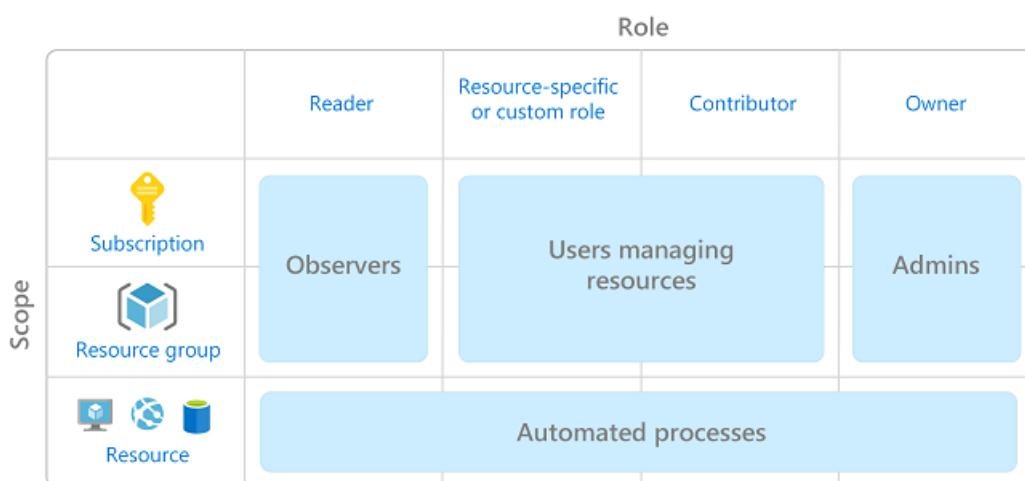
Here are some examples of what you can do with RBAC:

- Allow one user to manage virtual machines in a subscription and another user to manage virtual networks
- Allow a DBA group to manage SQL databases in a subscription
- Allow a user to manage all resources in a resource group, such as virtual machines, websites, and subnets
- Allow an application to access all resources in a resource group

Best practice for using RBAC

Using RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs. Instead of giving everybody unrestricted permissions in your Azure subscription or resources, you can allow only certain actions at a particular scope.

When planning your access control strategy, it's a best practice to grant users the least privilege to get their work done. The following diagram shows a suggested pattern for using RBAC.



How RBAC works

The way you control access to resources using RBAC is to create role assignments. This is a key concept to understand – it's how permissions are enforced. A role assignment consists of three elements: security principal, role definition, and scope.

Security principal

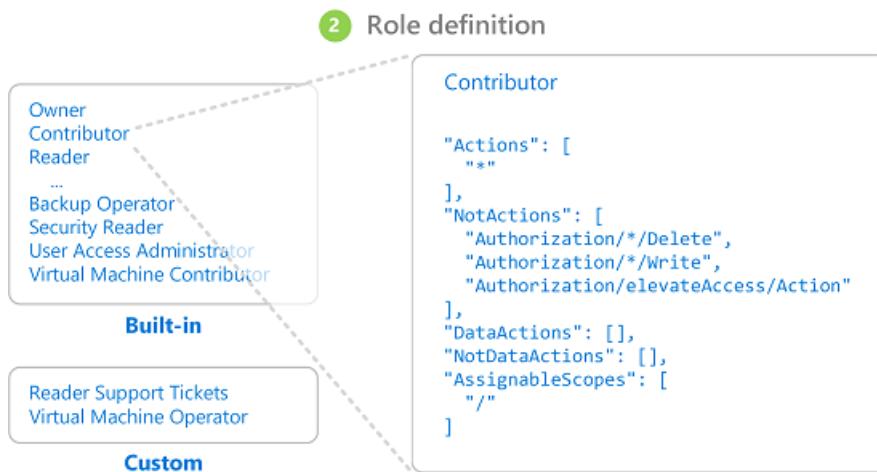
A *security principal* is an object that represents a user, group, service principal, or managed identity that is requesting access to Azure resources.



- **User** - An individual who has a profile in Azure Active Directory. You can also assign roles to users in other tenants. For information about users in other organizations, see [Azure Active Directory B2B](#).
- **Group** - A set of users created in Azure Active Directory. When you assign a role to a group, all users within that group have that role.
- **Service principal** - A security identity used by applications or services to access specific Azure resources. You can think of it as a *user identity* (username and password or certificate) for an application.
- **Managed identity** - An identity in Azure Active Directory that is automatically managed by Azure. You typically use [managed identities](#) when developing cloud applications to manage the credentials for authenticating to Azure services.

Role definition

A *role definition* is a collection of permissions. It's typically just called a *role*. A role definition lists the operations that can be performed, such as read, write, and delete. Roles can be high-level, like owner, or specific, like virtual machine reader.



Azure includes several [built-in roles](#) that you can use. The following lists four fundamental built-in roles. The first three apply to all resource types.

- **Owner** - Has full access to all resources including the right to delegate access to others.
- **Contributor** - Can create and manage all types of Azure resources but can't grant access to others.
- **Reader** - Can view existing Azure resources.
- **User Access Administrator** - Lets you manage user access to Azure resources.

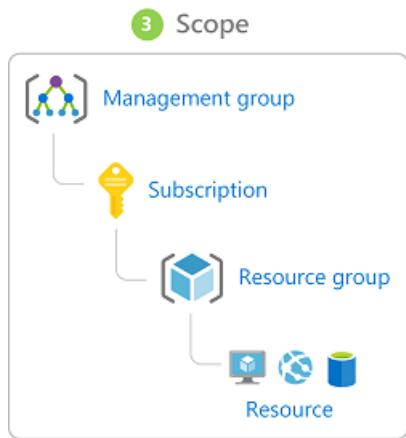
The rest of the built-in roles allow management of specific Azure resources. For example, the [Virtual Machine Contributor](#) role allows a user to create and manage virtual machines. If the built-in roles don't meet the specific needs of your organization, you can create your own [custom roles for Azure resources](#).

Azure has data operations that enable you to grant access to data within an object. For example, if a user has read data access to a storage account, then they can read the blobs or messages within that storage account. For more information, see [Understand role definitions for Azure resources](#).

Scope

Scope is the set of resources that the access applies to. When you assign a role, you can further limit the actions allowed by defining a scope. This is helpful if you want to make someone a [Website Contributor](#), but only for one resource group.

In Azure, you can specify a scope at multiple levels: [management group](#), subscription, resource group, or resource. Scopes are structured in a parent-child relationship.



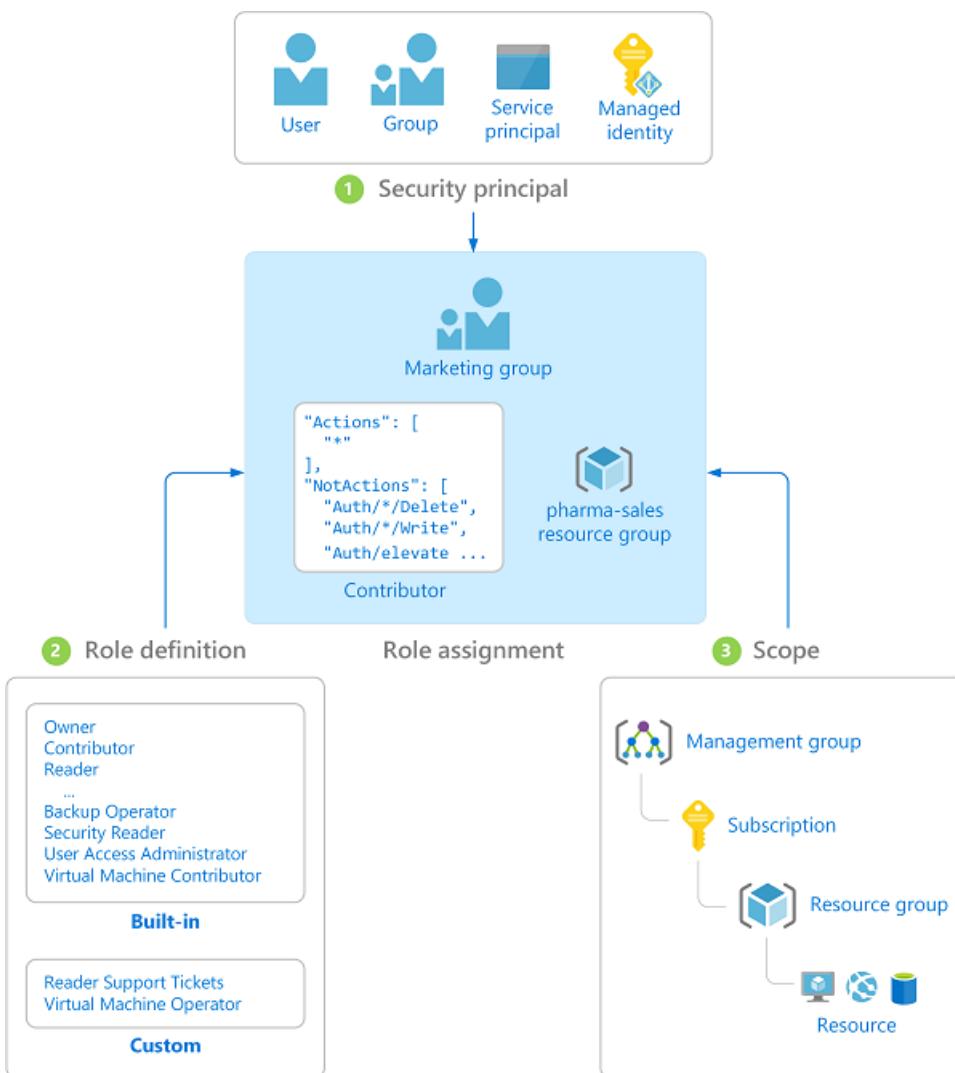
When you grant access at a parent scope, those permissions are inherited to the child scopes. For example:

- If you assign the [Owner](#) role to a user at the management group scope, that user can manage everything in all subscriptions in the management group.
- If you assign the [Reader](#) role to a group at the subscription scope, the members of that group can view every resource group and resource in the subscription.
- If you assign the [Contributor](#) role to an application at the resource group scope, it can manage resources of all types in that resource group, but not other resource groups in the subscription.

Role assignments

A *role assignment* is the process of attaching a role definition to a user, group, service principal, or managed identity at a particular scope for the purpose of granting access. Access is granted by creating a role assignment, and access is revoked by removing a role assignment.

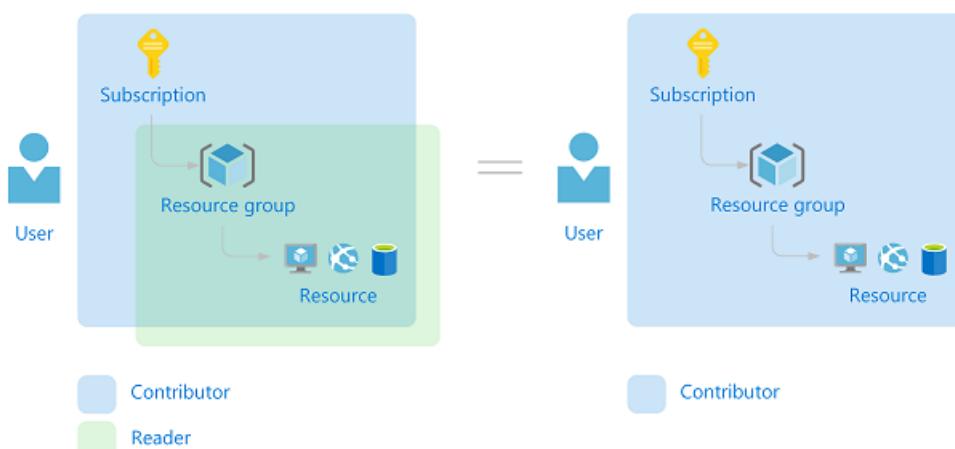
The following diagram shows an example of a role assignment. In this example, the Marketing group has been assigned the [Contributor](#) role for the pharma-sales resource group. This means that users in the Marketing group can create or manage any Azure resource in the pharma-sales resource group. Marketing users do not have access to resources outside the pharma-sales resource group, unless they are part of another role assignment.



You can create role assignments using the Azure portal, Azure CLI, Azure PowerShell, Azure SDKs, or REST APIs. You can have up to **2000** role assignments in each subscription and **500** role assignments in each management group. To create and remove role assignments, you must have `Microsoft.Authorization/roleAssignments/*` permission. This permission is granted through the [Owner](#) or [User Access Administrator](#) roles.

Multiple role assignments

So what happens if you have multiple overlapping role assignments? RBAC is an additive model, so your effective permissions are the addition of your role assignments. Consider the following example where a user is granted the Contributor role at the subscription scope and the Reader role on a resource group. The addition of the Contributor permissions and the Reader permissions is effectively the Contributor role for the resource group. Therefore, in this case, the Reader role assignment has no impact.



Deny assignments

Previously, RBAC was an allow-only model with no deny, but now RBAC supports deny assignments in a limited way. Similar to a role assignment, a *deny assignment* attaches a set of deny actions to a user, group, service principal, or managed identity at a particular scope for the purpose of denying access. A role assignment defines a set of actions that are *allowed*, while a deny assignment defines a set of actions that are *not allowed*. In other words, deny assignments block users from performing specified actions even if a role assignment grants them access. Deny assignments take precedence over role assignments. For more information, see [Understand deny assignments for Azure resources](#).

How RBAC determines if a user has access to a resource

The following are the high-level steps that RBAC uses to determine if you have access to a resource on the management plane. This is helpful to understand if you are trying to troubleshoot an access issue.

1. A user (or service principal) acquires a token for Azure Resource Manager.

The token includes the user's group memberships (including transitive group memberships).

2. The user makes a REST API call to Azure Resource Manager with the token attached.
3. Azure Resource Manager retrieves all the role assignments and deny assignments that apply to the resource upon which the action is being taken.
4. Azure Resource Manager narrows the role assignments that apply to this user or their group and determines what roles the user has for this resource.
5. Azure Resource Manager determines if the action in the API call is included in the roles the user has for this resource.
6. If the user doesn't have a role with the action at the requested scope, access is not granted. Otherwise, Azure Resource Manager checks if a deny assignment applies.
7. If a deny assignment applies, access is blocked. Otherwise access is granted.

License requirements

Using this feature is free and included in your Azure subscription.

Next steps

- [Quickstart: View the access a user has to Azure resources using the Azure portal](#)
- [Manage access to Azure resources using RBAC and the Azure portal](#)
- [Understand the different roles in Azure](#)
- [Enterprise Cloud Adoption: Resource access management in Azure](#)

Apply policies to Linux VMs with Azure Resource Manager

11/13/2019 • 2 minutes to read • [Edit Online](#)

By using policies, an organization can enforce various conventions and rules throughout the enterprise. Enforcement of the desired behavior can help mitigate risk while contributing to the success of the organization. In this article, we describe how you can use Azure Resource Manager policies to define the desired behavior for your organization's Virtual Machines.

For an introduction to policies, see [What is Azure Policy?](#).

Permitted Virtual Machines

To ensure that virtual machines for your organization are compatible with an application, you can restrict the permitted operating systems. In the following policy example, you allow only Ubuntu 14.04.2-LTS Virtual Machines to be created.

```
{
  "if": {
    "allOf": [
      {
        "field": "type",
        "in": [
          "Microsoft.Compute/disks",
          "Microsoft.Compute/virtualMachines",
          "Microsoft.Compute/VirtualMachineScaleSets"
        ]
      },
      {
        "not": {
          "allOf": [
            {
              "field": "Microsoft.Compute/imagePublisher",
              "in": [
                "Canonical"
              ]
            },
            {
              "field": "Microsoft.Compute/imageOffer",
              "in": [
                "UbuntuServer"
              ]
            },
            {
              "field": "Microsoft.Compute/imageSku",
              "in": [
                "14.04.2-LTS"
              ]
            },
            {
              "field": "Microsoft.Compute/imageVersion",
              "in": [
                "latest"
              ]
            }
          ]
        }
      }
    ],
    "then": {
      "effect": "deny"
    }
  }
}
```

Use a wild card to modify the preceding policy to allow any Ubuntu LTS image:

```
{
  "field": "Microsoft.Compute/virtualMachines/imageSku",
  "like": "*LTS"
}
```

For information about policy fields, see [Policy aliases](#).

Managed disks

To require the use of managed disks, use the following policy:

```
{
  "if": {
    "anyOf": [
      {
        "allOf": [
          {
            "field": "type",
            "equals": "Microsoft.Compute/virtualMachines"
          },
          {
            "field": "Microsoft.Compute/virtualMachines/osDisk.uri",
            "exists": true
          }
        ]
      },
      {
        "allOf": [
          {
            "field": "type",
            "equals": "Microsoft.Compute/VirtualMachineScaleSets"
          },
          {
            "anyOf": [
              {
                "field": "Microsoft.Compute/VirtualMachineScaleSets/osDisk.vhdContainers",
                "exists": true
              },
              {
                "field": "Microsoft.Compute/VirtualMachineScaleSets/osdisk.imageUrl",
                "exists": true
              }
            ]
          }
        ]
      }
    ],
    "then": {
      "effect": "deny"
    }
  }
}
```

Images for Virtual Machines

For security reasons, you can require that only approved custom images are deployed in your environment. You can specify either the resource group that contains the approved images, or the specific approved images.

The following example requires images from an approved resource group:

```
{
  "if": {
    "allOf": [
      {
        "field": "type",
        "in": [
          "Microsoft.Compute/virtualMachines",
          "Microsoft.Compute/VirtualMachineScaleSets"
        ]
      },
      {
        "not": {
          "field": "Microsoft.Compute/imageId",
          "contains": "resourceGroups/CustomImage"
        }
      }
    ],
    "then": {
      "effect": "deny"
    }
  }
}
```

The following example specifies the approved image IDs:

```
{
  "field": "Microsoft.Compute/imageId",
  "in": ["{imageId1}","{imageId2}"]
}
```

Virtual Machine extensions

You may want to forbid usage of certain types of extensions. For example, an extension may not be compatible with certain custom virtual machine images. The following example shows how to block a specific extension. It uses publisher and type to determine which extension to block.

```
{
  "if": {
    "allOf": [
      {
        "field": "type",
        "equals": "Microsoft.Compute/virtualMachines/extensions"
      },
      {
        "field": "Microsoft.Compute/virtualMachines/extensions/publisher",
        "equals": "Microsoft.Compute"
      },
      {
        "field": "Microsoft.Compute/virtualMachines/extensions/type",
        "equals": "{extension-type}"
      }
    ],
    "then": {
      "effect": "deny"
    }
  }
}
```

Next steps

- After defining a policy rule (as shown in the preceding examples), you need to create the policy definition and assign it to a scope. The scope can be a subscription, resource group, or resource. To assign policies, see [Use Azure portal to assign and manage resource policies](#), [Use PowerShell to assign policies](#), or [Use Azure CLI to assign policies](#).
- For an introduction to resource policies, see [What is Azure Policy?](#).
- For guidance on how enterprises can use Resource Manager to effectively manage subscriptions, see [Azure enterprise scaffold - prescriptive subscription governance](#).

How to set up Key Vault for virtual machines with the Azure CLI

11/13/2019 • 2 minutes to read • [Edit Online](#)

In the Azure Resource Manager stack, secrets/certificates are modeled as resources that are provided by Key Vault. To learn more about Azure Key Vault, see [What is Azure Key Vault?](#) In order for Key Vault to be used with Azure Resource Manager VMs, the *EnabledForDeployment* property on Key Vault must be set to true. This article shows you how to set up Key Vault for use with Azure virtual machines (VMs) using the Azure CLI.

To perform these steps, you need the latest [Azure CLI](#) installed and logged in to an Azure account using [az login](#).

Create a Key Vault

Create a key vault and assign the deployment policy with [az keyvault create](#). The following example creates a key vault named `myKeyVault` in the `myResourceGroup` resource group:

```
az keyvault create -l westus -n myKeyVault -g myResourceGroup --enabled-for-deployment true
```

Update a Key Vault for use with VMs

Set the deployment policy on an existing key vault with [az keyvault update](#). The following updates the key vault named `myKeyVault` in the `myResourceGroup` resource group:

```
az keyvault update -n myKeyVault -g myResourceGroup --set properties.enabledForDeployment=true
```

Use templates to set up Key Vault

When you use a template, you need to set the `enabledForDeployment` property to `true` for the Key Vault resource as follows:

```
{
  "type": "Microsoft.KeyVault/vaults",
  "name": "ContosoKeyVault",
  "apiVersion": "2015-06-01",
  "location": "<location-of-key-vault>",
  "properties": {
    "enabledForDeployment": "true",
    ....
    ....
  }
}
```

Next steps

For other options that you can configure when you create a Key Vault by using templates, see [Create a key vault](#).

Quick steps: Create and use an SSH public-private key pair for Linux VMs in Azure

1/29/2020 • 4 minutes to read • [Edit Online](#)

With a secure shell (SSH) key pair, you can create virtual machines (VMs) in Azure that use SSH keys for authentication, eliminating the need for passwords to sign in. This article shows you how to quickly generate and use an SSH public-private key file pair for Linux VMs. You can complete these steps with the Azure Cloud Shell, a macOS or Linux host, the Windows Subsystem for Linux, and other tools that support OpenSSH.

NOTE

VMs created using SSH keys are by default configured with passwords disabled, which greatly increases the difficulty of brute-force guessing attacks.

For more background and examples, see [Detailed steps to create SSH key pairs](#).

For additional ways to generate and use SSH keys on a Windows computer, see [How to use SSH keys with Windows on Azure](#).

Supported SSH key formats

Azure currently supports SSH protocol 2 (SSH-2) RSA public-private key pairs with a minimum length of 2048 bits. Other key formats such as ED25519 and ECDSA are not supported.

Create an SSH key pair

Use the `ssh-keygen` command to generate SSH public and private key files. By default, these files are created in the `~/.ssh` directory. You can specify a different location, and an optional password (*passphrase*) to access the private key file. If an SSH key pair with the same name exists in the given location, those files are overwritten.

The following command creates an SSH key pair using RSA encryption and a bit length of 4096:

```
ssh-keygen -m PEM -t rsa -b 4096
```

If you use the [Azure CLI](#) to create your VM with the `az vm create` command, you can optionally generate SSH public and private key files using the `--generate-ssh-keys` option. The key files are stored in the `~/.ssh` directory unless specified otherwise with the `--ssh-dest-key-path` option. The `--generate-ssh-keys` option will not overwrite existing key files, instead returning an error. In the following command, replace *VMname* and *RGname* with your own values:

```
az vm create --name VMname --resource-group RGname --generate-ssh-keys
```

Provide an SSH public key when deploying a VM

To create a Linux VM that uses SSH keys for authentication, specify your SSH public key when creating the VM using the Azure portal, Azure CLI, Azure Resource Manager templates, or other methods:

- [Create a Linux virtual machine with the Azure portal](#)

- [Create a Linux virtual machine with the Azure CLI](#)
- [Create a Linux VM using an Azure template](#)

If you're not familiar with the format of an SSH public key, you can display your public key with the following `cat` command, replacing `~/.ssh/id_rsa.pub` with the path and filename of your own public key file if needed:

```
cat ~/.ssh/id_rsa.pub
```

A typical public key value looks like this example:

```
ssh-rsa
AAAAB3NzaC1yc2EAAQABAAQACQ1/KanayNr+Q7ogR5mKnGpKWRBQU7F3Jjh7utdf7Z2iUFykaYx+MINsnT3XdnBRS8KhC0IP8ptbng
IaNOWd6zM8hB6UrcRT1Tpwl/SuGMw1Vb40x1EFphBkVEUgBo1oANIEXriAMv1DMZsgvnMF1Q12tD/u14cxy1WNEMAftey/vX3Fgp2vEq4zH
Xe1iY/sFZLJUJzcRUI0MOFXAuCjg/qyqzbIuTDFyfg8k0JTtyGFEMQhbXKcuP2yGx1uw0ice62LRzr8w0mszftXyMik1PnshRXbmE2xgINY
g5xo/ra3mq2imwtOKJpfdtFoMiKhJmSNHBSkK7vFTeYgg0v2cQ2+vL381cIFX40h+QCzvNF/Ax0Dv1QtVtSqfQxRVG79Zqio5p12ghFkt1fV
7reCBvVlhyxc2L1YUkrq4DHzkxNY5c90GSHXSle9Ys03F1J5ip18f6gPq4xFmo6dVoJodZm9N0YMKCkZ4k1qJDEssJBk2ujDPmQ0eMjJX3Fn
DXYYB182ZCGQzXfz1PDC29cWVgDZEXNHuYrOLmJTmYtLZ4WkdUhLL1t5XsdoKwqlWpbegyYtGZgeZNRt00dN6ybOPJqmYFd2qRtb4sYPniGJ
DOGhx4VodXAjT09omhQJpE6w1ZbRWdVkc55R2d/CSPHJscEiuudb+1SG2uA/oik/WQ== username@domainname
```

If you copy and paste the contents of the public key file to use in the Azure portal or a Resource Manager template, make sure you don't copy any trailing whitespace. To copy a public key in macOS, you can pipe the public key file to `pbcopy`. Similarly in Linux, you can pipe the public key file to programs such as `xclip`.

The public key that you place on your Linux VM in Azure is by default stored in `~/.ssh/id_rsa.pub`, unless you specified a different location when you created the key pair. To use the [Azure CLI 2.0](#) to create your VM with an existing public key, specify the value and optionally the location of this public key using the `az vm create` command with the `--ssh-key-value` option. In the following command, replace `VMname`, `RGname`, and `keyFile` with your own values:

```
az vm create --name VMname --resource-group RGname --ssh-key-values mysshkey.pub
```

If you want to use multiple SSH keys with your VM, you can enter them in a space-separated list, like this

```
--ssh-key-values sshkey-desktop.pub sshkey-laptop.pub
```

SSH into your VM

With the public key deployed on your Azure VM, and the private key on your local system, SSH into your VM using the IP address or DNS name of your VM. In the following command, replace `azureuser` and `myvm.westus.cloudapp.azure.com` with the administrator user name and the fully qualified domain name (or IP address):

```
ssh azureuser@myvm.westus.cloudapp.azure.com
```

If you specified a passphrase when you created your key pair, enter that passphrase when prompted during the login process. The VM is added to your `~/.ssh/known_hosts` file, and you won't be asked to connect again until either the public key on your Azure VM changes or the server name is removed from `~/.ssh/known_hosts`.

If the VM is using the just-in-time access policy, you need to request access before you can connect to the VM. For more information about the just-in-time policy, see [Manage virtual machine access using the just in time policy](#).

Next steps

- For more information on working with SSH key pairs, see [Detailed steps to create and manage SSH key pairs](#).
- If you have difficulties with SSH connections to Azure VMs, see [Troubleshoot SSH connections to an Azure Linux VM](#).

How to use SSH keys with Windows on Azure

11/13/2019 • 6 minutes to read • [Edit Online](#)

This article describes ways to generate and use *secure shell* (SSH) keys on a Windows computer to create and connect to a Linux virtual machine (VM) in Azure. To use SSH keys from a Linux or macOS client, see the [quick](#) or [detailed](#) guidance.

Overview of SSH and keys

SSH is an encrypted connection protocol that allows secure sign-ins over unsecured connections. SSH is the default connection protocol for Linux VMs hosted in Azure. Although SSH itself provides an encrypted connection, using passwords with SSH connections still leaves the VM vulnerable to brute-force attacks or guessing of passwords. A more secure and preferred method of connecting to a VM using SSH is by using a public-private key pair, also known as *SSH keys*.

- The *public key* is placed on your Linux VM, or any other service that you wish to use with public-key cryptography.
- The *private key* remains on your local system. Protect this private key. Do not share it.

When you use an SSH client to connect to your Linux VM (which has the public key), the remote VM tests the client to make sure it possesses the private key. If the client has the private key, it's granted access to the VM.

Depending on your organization's security policies, you can reuse a single public-private key pair to access multiple Azure VMs and services. You do not need a separate pair of keys for each VM or service you wish to access.

Your public key can be shared with anyone, but only you (or your local security infrastructure) should possess your private key.

Supported SSH key formats

Azure currently supports SSH protocol 2 (SSH-2) RSA public-private key pairs with a minimum length of 2048 bits. Other key formats such as ED25519 and ECDSA are not supported.

Windows packages and SSH clients

You connect to and manage Linux VMs in Azure using an *SSH client*. Computers running Linux or macOS usually have a suite of SSH commands to generate and manage SSH keys and to make SSH connections.

Windows computers do not always have comparable SSH commands installed. Recent versions of Windows 10 provide [OpenSSH client commands](#) to create and manage SSH keys and make SSH connections from a command prompt. Recent Windows 10 versions also include the [Windows Subsystem for Linux](#) to run and access utilities such as an SSH client natively within a Bash shell.

Other common Windows SSH clients you can install locally are included in the following packages:

- [PuTTY](#)
- [Git For Windows](#)
- [MobaXterm](#)
- [Cygwin](#)

You can also use the SSH utilities available in Bash in the [Azure Cloud Shell](#).

- Access Cloud Shell in your web browser at <https://shell.azure.com> or in the [Azure portal](#).
- Access Cloud Shell as a terminal from within Visual Studio Code by installing the [Azure Account extension](#).

Create an SSH key pair

The following sections describe two options to create an SSH key pair on Windows. You can use a shell command (`ssh-keygen`) or a GUI tool (PuTTYgen). Also note, when using Powershell to create a key, upload the public key as ssh.com(SECSh) format. When using CLI, convert the key into OpenSSH format prior to uploading.

Create SSH keys with `ssh-keygen`

If you run a command shell on Windows that supports SSH client tools (or you use Azure Cloud Shell), create an SSH key pair using the `ssh-keygen` command. Type the following command, and answer the prompts. If an SSH key pair exists in the chosen location, those files are overwritten.

```
ssh-keygen -t rsa -b 2048
```

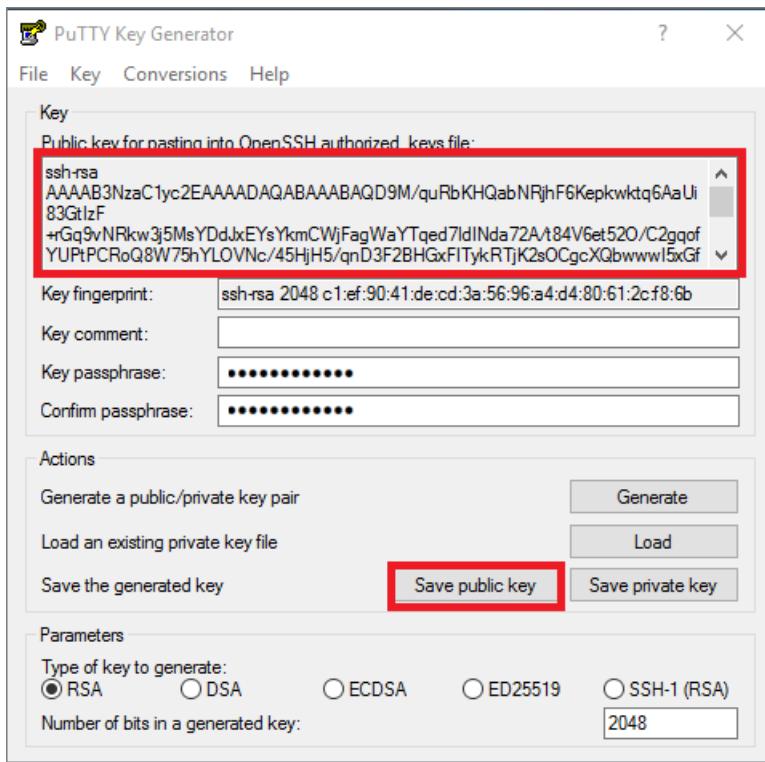
For more background and information, see the [quick](#) or [detailed](#) steps to create SSH keys using `ssh-keygen`.

Create SSH keys with PuTTYgen

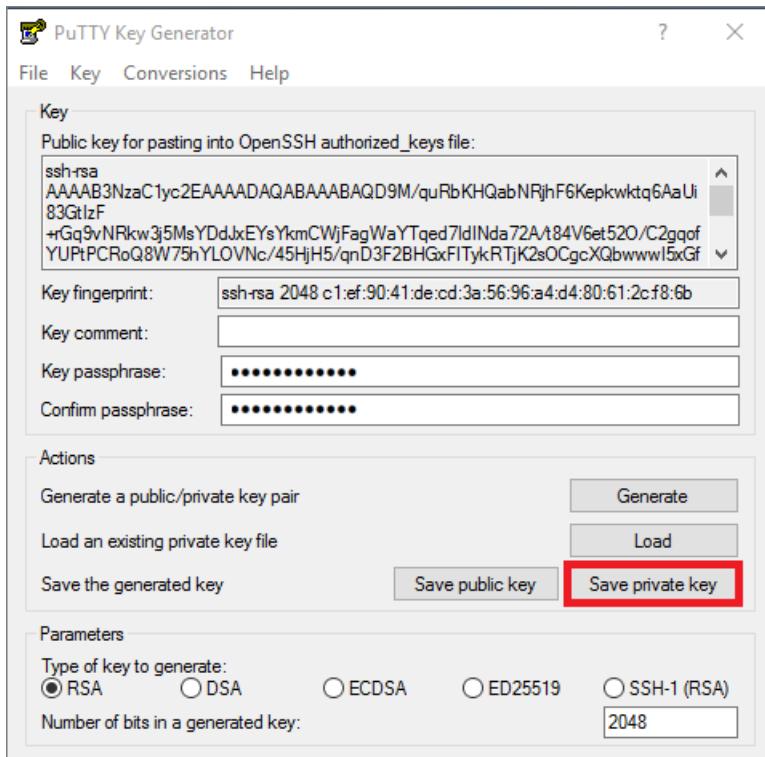
If you prefer to use a GUI-based tool to create SSH keys, you can use the PuTTYgen key generator, included with the [PuTTY download package](#).

To create an SSH RSA key pair with PuTTYgen:

1. Start PuTTYgen.
2. Click **Generate**. By default PuTTYgen generates a 2048-bit SSH-2 RSA key.
3. Move the mouse around in the blank area to provide randomness for the key.
4. After the public key is generated, optionally enter and confirm a passphrase. You will be prompted for the passphrase when you authenticate to the VM with your private SSH key. Without a passphrase, if someone obtains your private key, they can sign in to any VM or service that uses that key. We recommend you create a passphrase. However, if you forget the passphrase, there is no way to recover it.
5. The public key is displayed at the top of the window. You can copy this entire public key and then paste it into the Azure portal or an Azure Resource Manager template when you create a Linux VM. You can also select **Save public key** to save a copy to your computer:



6. Optionally, to save the private key in PuTTY private key format (.ppk file), select **Save private key**. You will need the .ppk file later to use PuTTY to make an SSH connection to the VM.

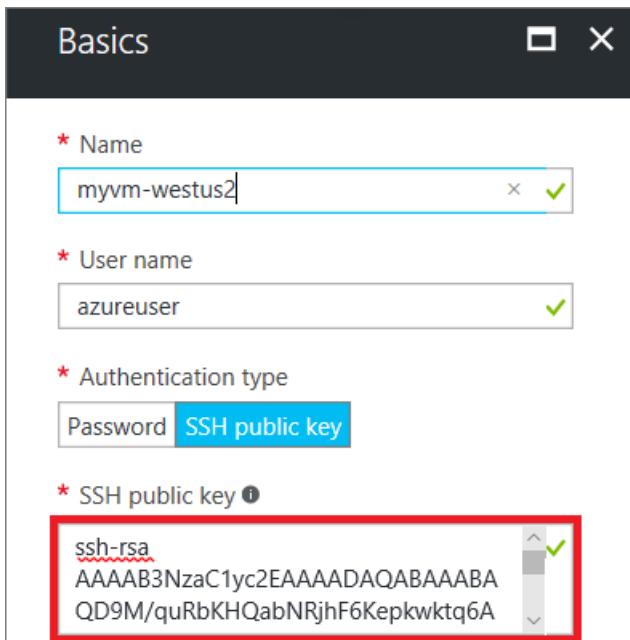


If you want to save the private key in the OpenSSH format, the private key format used by many SSH clients, select **Conversions > Export OpenSSH key**.

Provide an SSH public key when deploying a VM

To create a Linux VM that uses SSH keys for authentication, provide your SSH public key when creating the VM using the Azure portal or other methods.

The following example shows how you would copy and paste this public key into the Azure portal when you create a Linux VM. The public key is typically then stored in the `~/.ssh/authorized_key` directory on your new VM.



Connect to your VM

One way to make an SSH connection to your Linux VM from Windows is to use an SSH client. This is the preferred method if you have an SSH client installed on your Windows system, or if you use the SSH tools in Bash in Azure Cloud Shell. If you prefer a GUI-based tool, you can connect with PuTTY.

Use an SSH client

With the public key deployed on your Azure VM, and the private key on your local system, SSH to your VM using the IP address or DNS name of your VM. Replace `azureuser` and `myvm.westus.cloudapp.azure.com` in the following command with the administrator user name and the fully qualified domain name (or IP address):

```
ssh azureuser@myvm.westus.cloudapp.azure.com
```

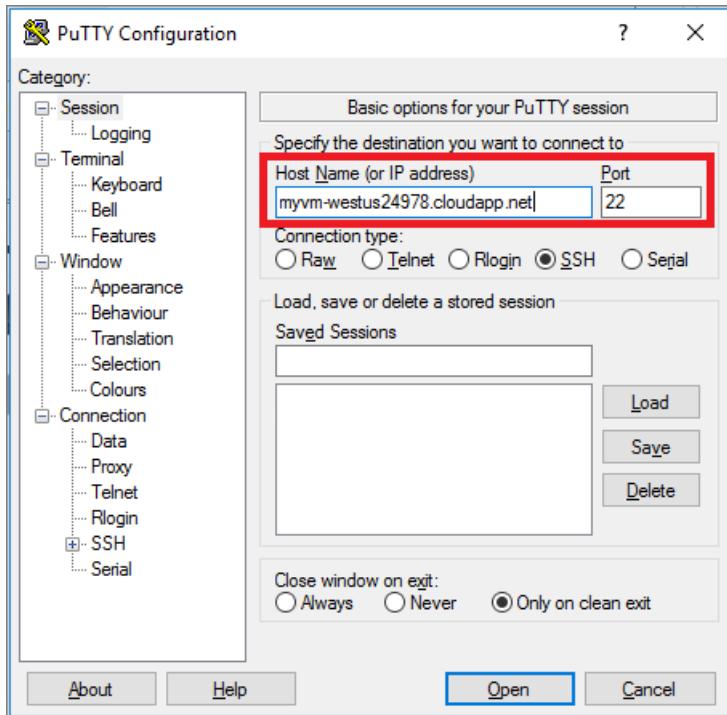
If you configured a passphrase when you created your key pair, enter the passphrase when prompted during the sign-in process.

If the VM is using the just-in-time access policy, you need to request access before you can connect to the VM. For more information about the just-in-time policy, see [Manage virtual machine access using the just in time policy](#).

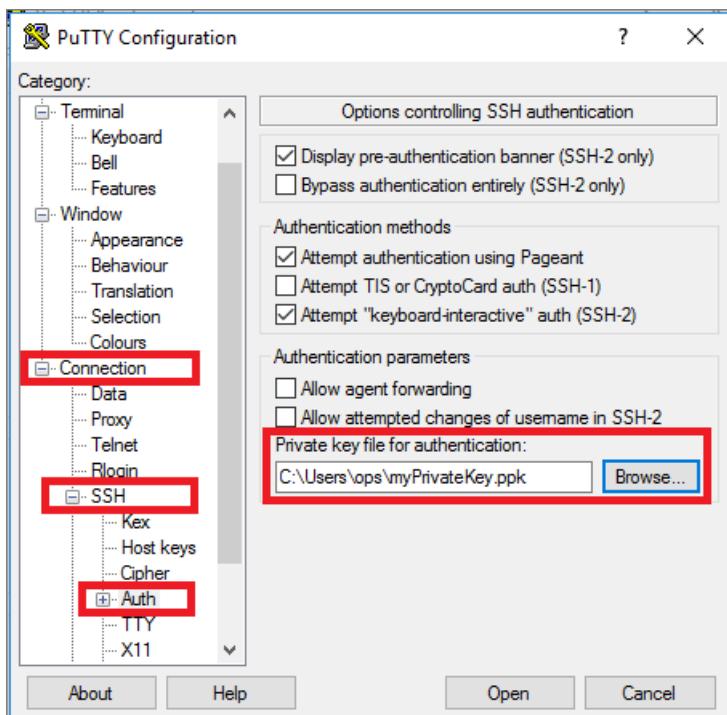
Connect with PuTTY

If you installed the [PuTTY download package](#) and previously generated a PuTTY private key (.ppk) file, you can connect to a Linux VM with PuTTY.

1. Start PuTTy.
2. Fill in the host name or IP address of your VM from the Azure portal:



3. Select the **Connection > SSH > Auth** category. Browse to and select your PuTTY private key (.ppk file):



4. Click **Open** to connect to your VM.

Next steps

- For detailed steps, options, and advanced examples of working with SSH keys, see [Detailed steps to create SSH key pairs](#).
- You can also use PowerShell in Azure Cloud Shell to generate SSH keys and make SSH connections to Linux VMs. See the [PowerShell quickstart](#).
- If you have difficulty using SSH to connect to your Linux VMs, see [Troubleshoot SSH connections to an Azure Linux VM](#).

Detailed steps: Create and manage SSH keys for authentication to a Linux VM in Azure

12/6/2019 • 10 minutes to read • [Edit Online](#)

With a secure shell (SSH) key pair, you can create a Linux virtual machine on Azure that defaults to using SSH keys for authentication, eliminating the need for passwords to sign in. VMs created with the Azure portal, Azure CLI, Resource Manager templates, or other tools can include your SSH public key as part of the deployment, which sets up SSH key authentication for SSH connections.

This article provides detailed background and steps to create and manage an SSH RSA public-private key file pair for SSH client connections. If you want quick commands, see [How to create an SSH public-private key pair for Linux VMs in Azure](#).

For additional ways to generate and use SSH keys on a Windows computer, see [How to use SSH keys with Windows on Azure](#).

Overview of SSH and keys

SSH is an encrypted connection protocol that allows secure sign-ins over unsecured connections. SSH is the default connection protocol for Linux VMs hosted in Azure. Although SSH itself provides an encrypted connection, using passwords with SSH connections still leaves the VM vulnerable to brute-force attacks or guessing of passwords. A more secure and preferred method of connecting to a VM using SSH is by using a public-private key pair, also known as *SSH keys*.

- The *public key* is placed on your Linux VM, or any other service that you wish to use with public-key cryptography.
- The *private key* remains on your local system. Protect this private key. Do not share it.

When you use an SSH client to connect to your Linux VM (which has the public key), the remote VM tests the client to make sure it possesses the private key. If the client has the private key, it's granted access to the VM.

Depending on your organization's security policies, you can reuse a single public-private key pair to access multiple Azure VMs and services. You do not need a separate pair of keys for each VM or service you wish to access.

Your public key can be shared with anyone, but only you (or your local security infrastructure) should possess your private key.

Private key passphrase

The SSH private key should have a very secure passphrase to safeguard it. This passphrase is just to access the private SSH key file and *is not* the user account password. When you add a passphrase to your SSH key, it encrypts the private key using 128-bit AES, so that the private key is useless without the passphrase to decrypt it. If an attacker stole your private key and that key did not have a passphrase, they would be able to use that private key to sign in to any servers that have the corresponding public key. If a private key is protected by a passphrase, it cannot be used by that attacker, providing an additional layer of security for your infrastructure on Azure.

Supported SSH key formats

Azure currently supports SSH protocol 2 (SSH-2) RSA public-private key pairs with a minimum length of 2048 bits. Other key formats such as ED25519 and ECDSA are not supported.

SSH keys use and benefits

When you create an Azure VM by specifying the public key, Azure copies the public key (in the `.pub` format) to the `~/.ssh/authorized_keys` folder on the VM. SSH keys in `~/.ssh/authorized_keys` are used to challenge the client to match the corresponding private key on an SSH connection. In an Azure Linux VM that uses SSH keys for authentication, Azure configures the SSHD server to not allow password sign-in, only SSH keys. Therefore, by creating an Azure Linux VM with SSH keys, you can help secure the VM deployment and save yourself the typical post-deployment configuration step of disabling passwords in the `sshd_config` file.

If you do not wish to use SSH keys, you can set up your Linux VM to use password authentication. If your VM is not exposed to the Internet, using passwords may be sufficient. However, you still need to manage your passwords for each Linux VM and maintain healthy password policies and practices, such as minimum password length and regular updates. Using SSH keys reduces the complexity of managing individual credentials across multiple VMs.

Generate keys with ssh-keygen

To create the keys, a preferred command is `ssh-keygen`, which is available with OpenSSH utilities in the Azure Cloud Shell, a macOS or Linux host, the [Windows Subsystem for Linux](#), and other tools. `ssh-keygen` asks a series of questions and then writes a private key and a matching public key.

SSH keys are by default kept in the `~/.ssh` directory. If you do not have a `~/.ssh` directory, the `ssh-keygen` command creates it for you with the correct permissions.

Basic example

The following `ssh-keygen` command generates 2048-bit SSH RSA public and private key files by default in the `~/.ssh` directory. If an SSH key pair exists in the current location, those files are overwritten.

```
ssh-keygen -m PEM -t rsa -b 4096
```

Detailed example

The following example shows additional command options to create an SSH RSA key pair. If an SSH key pair exists in the current location, those files are overwritten.

```
ssh-keygen \
-m PEM \
-t rsa \
-b 4096 \
-C "azureuser@myserver" \
-f ~/.ssh/mykeys/myprivatekey \
-N mypassphrase
```

Command explained

`ssh-keygen` = the program used to create the keys

`-m PEM` = format the key as PEM

`-t rsa` = type of key to create, in this case in the RSA format

`-b 4096` = the number of bits in the key, in this case 4096

`-C "azureuser@myserver"` = a comment appended to the end of the public key file to easily identify it. Normally an email address is used as the comment, but use whatever works best for your infrastructure.

`-f ~/.ssh/mykeys/myprivatekey` = the filename of the private key file, if you choose not to use the default name. A

corresponding public key file appended with `.pub` is generated in the same directory. The directory must exist.

`-N mypassphrase` = an additional passphrase used to access the private key file.

Example of ssh-keygen

```
ssh-keygen -t -m PEM rsa -b 4096 -C "azureuser@myserver"
Generating public/private rsa key pair.
Enter file in which to save the key (/home/azureuser/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/azureuser/.ssh/id_rsa.
Your public key has been saved in /home/azureuser/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:vFfHHrpSGQBd/oNdvNiX0sG9Vh+wR0lZBktNZw9AUjA azureuser@myserver
The key's randomart image is:
+---[RSA 4096]---+
|       .oE=*B*+ |
|       o+o.*++|
|       .oo++*|
|       .B+.0|
|       S   o=B0.|
|       . .o++o |
|       . .... .|
|       .. . . |
|       .. |
+---[SHA256]---+
```

Saved key files

Enter file in which to save the key (/home/azureuser/.ssh/id_rsa): `~/.ssh/id_rsa`

The key pair name for this article. Having a key pair named `id_rsa` is the default; some tools might expect the `id_rsa` private key file name, so having one is a good idea. The directory `~/ssh/` is the default location for SSH key pairs and the SSH config file. If not specified with a full path, `ssh-keygen` creates the keys in the current working directory, not the default `~/ssh`.

List of the `~/ssh` directory

```
ls -al ~/ssh
-rw----- 1 azureuser staff 1675 Aug 25 18:04 id_rsa
-rw-r--r-- 1 azureuser staff 410 Aug 25 18:04 id_rsa.pub
```

Key passphrase

Enter passphrase (empty for no passphrase):

It is *strongly* recommended to add a passphrase to your private key. Without a passphrase to protect the key file, anyone with the file can use it to sign in to any server that has the corresponding public key. Adding a passphrase offers more protection in case someone is able to gain access to your private key file, giving you time to change the keys.

Generate keys automatically during deployment

If you use the [Azure CLI](#) to create your VM, you can optionally generate SSH public and private key files by running the `az vm create` command with the `--generate-ssh-keys` option. The keys are stored in the `~/ssh` directory. Note that this command option does not overwrite keys if they already exist in that location.

Provide SSH public key when deploying a VM

To create a Linux VM that uses SSH keys for authentication, provide your SSH public key when creating the VM

using the Azure portal, CLI, Resource Manager templates, or other methods. When using the portal, you enter the public key itself. If you use the [Azure CLI](#) to create your VM with an existing public key, specify the value or location of this public key by running the `az vm create` command with the `--ssh-key-value` option.

If you're not familiar with the format of an SSH public key, you can see your public key by running `cat` as follows, replacing `~/.ssh/id_rsa.pub` with your own public key file location:

```
cat ~/.ssh/id_rsa.pub
```

Output is similar to the following (here redacted):

```
ssh-rsa  
XXXXXXXXXXc2EAAAADAXABAAABAXC5Am7+fGZ+5zXBGgXS6GUvmsXCLGc7tX7/rViXk3+eShZzaXnt75gUmT1I2f75zFn2h1AIDGKwf4g12KW  
cZxy81TniUOTjUsV1wPymXUXxESL/UfJKfbdstBhT0dy5EG9rYWA0K43SJmwPhH28BpoLfXXXXXG+/ilsXXXXXgRLiJ2W19MzXHp8z3Lxw7r  
9wx3HaV1P4XiFv9U4hGcp8RMI1MP1nNesF1oBpG4pV2bJRBTXNXeY416F8WZ3C4kuF8Xx0o08mxaTpVZ3T1841altnTZCcPkXuMrBjYSjbA8  
npoXAXNwiivyo3X2KMXXXXdXXXXXXXXXXXX/ azureuser@myserver
```

If you copy and paste the contents of the public key file into the Azure portal or a Resource Manager template, make sure you don't copy any additional whitespace or introduce additional line breaks. For example, if you use macOS, you can pipe the public key file (by default, `~/.ssh/id_rsa.pub`) to **pbcopy** to copy the contents (there are other Linux programs that do the same thing, such as `xclip`).

If you prefer to use a public key that is in a multiline format, you can generate an RFC4716 formatted key in a pem container from the public key you previously created.

To create a RFC4716 formatted key from an existing SSH public key:

```
ssh-keygen \  
-f ~/.ssh/id_rsa.pub \  
-e \  
-m RFC4716 > ~/.ssh/id_ssh2.pem
```

SSH to your VM with an SSH client

With the public key deployed on your Azure VM, and the private key on your local system, SSH to your VM using the IP address or DNS name of your VM. Replace `azureuser` and `myvm.westus.cloudapp.azure.com` in the following command with the administrator user name and the fully qualified domain name (or IP address):

```
ssh azureuser@myvm.westus.cloudapp.azure.com
```

If you provided a passphrase when you created your key pair, enter the passphrase when prompted during the sign-in process. (The server is added to your `~/.ssh/known_hosts` folder, and you won't be asked to connect again until the public key on your Azure VM changes or the server name is removed from `~/.ssh/known_hosts`.)

If the VM is using the just-in-time access policy, you need to request access before you can connect to the VM. For more information about the just-in-time policy, see [Manage virtual machine access using the just in time policy](#).

Use ssh-agent to store your private key passphrase

To avoid typing your private key file passphrase with every SSH sign-in, you can use `ssh-agent` to cache your private key file passphrase. If you are using a Mac, the macOS Keychain securely stores the private key passphrase when you invoke `ssh-agent`.

Verify and use `ssh-agent` and `ssh-add` to inform the SSH system about the key files so that you do not need to use the passphrase interactively.

```
eval "$(ssh-agent -s)"
```

Now add the private key to `ssh-agent` using the command `ssh-add`.

```
ssh-add ~/.ssh/id_rsa
```

The private key passphrase is now stored in `ssh-agent`.

Use `ssh-copy-id` to copy the key to an existing VM

If you have already created a VM, you can install the new SSH public key to your Linux VM with a command similar to the following:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub azureuser@myserver
```

Create and configure an SSH config file

You can create and configure an SSH config file (`~/.ssh/config`) to speed up log-ins and to optimize your SSH client behavior.

The following example shows a simple configuration that you can use to quickly sign in as a user to a specific VM using the default SSH private key.

Create the file

```
touch ~/.ssh/config
```

Edit the file to add the new SSH configuration

```
vim ~/.ssh/config
```

Example configuration

Add configuration settings appropriate for your host VM.

```
# Azure Keys
Host myvm
  Hostname 102.160.203.241
  User azureuser
# ./Azure Keys
```

You can add configurations for additional hosts to enable each to use its own dedicated key pair. See [SSH config file](#) for more advanced configuration options.

Now that you have an SSH key pair and a configured SSH config file, you are able to sign in to your Linux VM quickly and securely. When you run the following command, SSH locates and loads any settings from the `Host myvm` block in the SSH config file.

```
ssh myvm
```

The first time you sign in to a server using an SSH key, the command prompts you for the passphrase for that key file.

Next steps

Next up is to create Azure Linux VMs using the new SSH public key. Azure VMs that are created with an SSH public key as the sign-in are better secured than VMs created with the default sign-in method, passwords.

- [Create a Linux virtual machine with the Azure portal](#)
- [Create a Linux virtual machine with the Azure CLI](#)
- [Create a Linux VM using an Azure template](#)

What if an Azure service disruption impacts Azure VMs

2/10/2020 • 3 minutes to read • [Edit Online](#)

At Microsoft, we work hard to make sure that our services are always available to you when you need them. Forces beyond our control sometimes impact us in ways that cause unplanned service disruptions.

Microsoft provides a Service Level Agreement (SLA) for its services as a commitment for uptime and connectivity. The SLA for individual Azure services can be found at [Azure Service Level Agreements](#).

Azure already has many built-in platform features that support highly available applications. For more about these services, read [Disaster recovery and high availability for Azure applications](#).

This article covers a true disaster recovery scenario, when a whole region experiences an outage due to major natural disaster or widespread service interruption. These are rare occurrences, but you must prepare for the possibility that there is an outage of an entire region. If an entire region experiences a service disruption, the locally redundant copies of your data would temporarily be unavailable. If you have enabled geo-replication, three additional copies of your Azure Storage blobs and tables are stored in a different region. In the event of a complete regional outage or a disaster in which the primary region is not recoverable, Azure remaps all of the DNS entries to the geo-replicated region.

To help you handle these rare occurrences, we provide the following guidance for Azure virtual machines in the case of a service disruption of the entire region where your Azure virtual machine application is deployed.

Option 1: Initiate a failover by using Azure Site Recovery

You can configure Azure Site Recovery for your VMs so that you can recover your application with a single click in matter of minutes. You can replicate to Azure region of your choice and not restricted to paired regions. You can get started by [replicating your virtual machines](#). You can [create a recovery plan](#) so that you can automate the entire failover process for your application. You can [test your failovers](#) beforehand without impacting production application or the ongoing replication. In the event of a primary region disruption, you just [initiate a failover](#) and bring your application in target region.

Option 2: Wait for recovery

In this case, no action on your part is required. Know that we are working diligently to restore service availability. You can see the current service status on our [Azure Service Health Dashboard](#).

This is the best option if you have not set up Azure Site Recovery, read-access geo-redundant storage, or geo-redundant storage prior to the disruption. If you have set up geo-redundant storage or read-access geo-redundant storage for the storage account where your VM virtual hard drives (VHDs) are stored, you can look to recover the base image VHD and try to provision a new VM from it. This is not a preferred option because there are no guarantees of synchronization of data. Consequently, this option is not guaranteed to work.

NOTE

Be aware that you do not have any control over this process, and it will only occur for region-wide service disruptions. Because of this, you must also rely on other application-specific backup strategies to achieve the highest level of availability. For more information, see the section on [Data strategies for disaster recovery](#).

Next steps

- Start protecting your applications running on [Azure virtual machines](#) using Azure Site Recovery
- To learn more about how to implement a disaster recovery and high availability strategy, see [Disaster recovery and high availability for Azure applications](#).
- To develop a detailed technical understanding of a cloud platform's capabilities, see [Azure resiliency technical guidance](#).
- If the instructions are not clear, or if you would like Microsoft to do the operations on your behalf, contact [Customer Support](#).

2 minutes to read

Back up a virtual machine in Azure with the CLI

11/18/2019 • 5 minutes to read • [Edit Online](#)

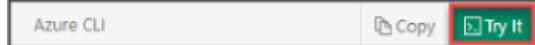
The Azure CLI is used to create and manage Azure resources from the command line or in scripts. You can protect your data by taking backups at regular intervals. Azure Backup creates recovery points that can be stored in geo-redundant recovery vaults. This article details how to back up a virtual machine (VM) in Azure with the Azure CLI. You can also perform these steps with [Azure PowerShell](#) or in the [Azure portal](#).

This quickstart enables backup on an existing Azure VM. If you need to create a VM, you can [create a VM with the Azure CLI](#).

Use Azure Cloud Shell

Azure hosts Azure Cloud Shell, an interactive shell environment that you can use through your browser. You can use either Bash or PowerShell with Cloud Shell to work with Azure services. You can use the Cloud Shell preinstalled commands to run the code in this article without having to install anything on your local environment.

To start Azure Cloud Shell:

| OPTION | EXAMPLE/LINK |
|---|--|
| Select Try It in the upper-right corner of a code block. Selecting Try It doesn't automatically copy the code to Cloud Shell. |  |
| Go to https://shell.azure.com , or select the Launch Cloud Shell button to open Cloud Shell in your browser. |  |
| Select the Cloud Shell button on the menu bar at the upper right in the Azure portal . |  |

To run the code in this article in Azure Cloud Shell:

1. Start Cloud Shell.
2. Select the **Copy** button on a code block to copy the code.
3. Paste the code into the Cloud Shell session by selecting **Ctrl+Shift+V** on Windows and Linux or by selecting **Cmd+Shift+V** on macOS.
4. Select **Enter** to run the code.

To install and use the CLI locally, you must run Azure CLI version 2.0.18 or later. To find the CLI version, run `az --version`. If you need to install or upgrade, see [Install the Azure CLI](#).

Create a recovery services vault

A Recovery Services vault is a logical container that stores the backup data for each protected resource, such as Azure VMs. When the backup job for a protected resource runs, it creates a recovery point inside the Recovery Services vault. You can then use one of these recovery points to restore data to a given point in time.

Create a Recovery Services vault with `az backup vault create`. Specify the same resource group and location as the VM you wish to protect. If you used the [VM quickstart](#), then you created:

- a resource group named *myResourceGroup*,
- a VM named *myVM*,
- resources in the *eastus* location.

```
az backup vault create --resource-group myResourceGroup \
--name myRecoveryServicesVault \
--location eastus
```

By default, the Recovery Services vault is set for Geo-Redundant storage. Geo-Redundant storage ensures your backup data is replicated to a secondary Azure region that is hundreds of miles away from the primary region. If the storage redundancy setting needs to be modified, use [az backup vault backup-properties set](#) cmdlet.

```
az backup vault backup-properties set \
--name myRecoveryServicesVault \
--resource-group myResourceGroup \
--backup-storage-redundancy "LocallyRedundant/GeoRedundant"
```

Enable backup for an Azure VM

Create a protection policy to define: when a backup job runs, and how long the recovery points are stored. The default protection policy runs a backup job each day and retains recovery points for 30 days. You can use these default policy values to quickly protect your VM. To enable backup protection for a VM, use [az backup protection enable-for-vm](#). Specify the resource group and VM to protect, then the policy to use:

```
az backup protection enable-for-vm \
--resource-group myResourceGroup \
--vault-name myRecoveryServicesVault \
--vm myVM \
--policy-name DefaultPolicy
```

NOTE

If the VM is not in the same resource group as that of vault, then myResourceGroup refers to the resource group where vault was created. Instead of VM name, provide the VM ID as indicated below.

```
az backup protection enable-for-vm \
--resource-group myResourceGroup \
--vault-name myRecoveryServicesVault \
--vm $(az vm show -g VMResourceGroup -n MyVm --query id | tr -d '') \
--policy-name DefaultPolicy
```

IMPORTANT

While using CLI to enable backup for multiple VMs at once, ensure that a single policy doesn't have more than 100 VMs associated with it. This is a [recommended best practice](#). Currently, the PS client doesn't explicitly block if there are more than 100 VMs but the check is planned to be added in the future.

Start a backup job

To start a backup now rather than wait for the default policy to run the job at the scheduled time, use [az backup protection backup-now](#). This first backup job creates a full recovery point. Each backup job after this initial backup

creates incremental recovery points. Incremental recovery points are storage and time-efficient, as they only transfer changes made since the last backup.

The following parameters are used to back up the VM:

- `--container-name` is the name of your VM
- `--item-name` is the name of your VM
- `--retain-until` value should be set to the last available date, in UTC time format (**dd-mm-yyyy**), that you wish the recovery point to be available

The following example backs up the VM named *myVM* and sets the expiration of the recovery point to October 18, 2017:

```
az backup protection backup-now \
    --resource-group myResourceGroup \
    --vault-name myRecoveryServicesVault \
    --container-name myVM \
    --item-name myVM \
    --retain-until 18-10-2017
```

Monitor the backup job

To monitor the status of backup jobs, use [az backup job list](#):

```
az backup job list \
    --resource-group myResourceGroup \
    --vault-name myRecoveryServicesVault \
    --output table
```

The output is similar to the following example, which shows the backup job is *InProgress*:

| Name | Operation | Status | Item Name | Start Time UTC | Duration |
|----------|-----------------|------------|-----------|---------------------|----------------|
| a0a8e5e6 | Backup | InProgress | myvm | 2017-09-19T03:09:21 | 0:00:48.718366 |
| fe5d0414 | ConfigureBackup | Completed | myvm | 2017-09-19T03:03:57 | 0:00:31.191807 |

When the *Status* of the backup job reports *Completed*, your VM is protected with Recovery Services and has a full recovery point stored.

Clean up deployment

When no longer needed, you can disable protection on the VM, remove the restore points and Recovery Services vault, then delete the resource group and associated VM resources. If you used an existing VM, you can skip the final [az group delete](#) command to leave the resource group and VM in place.

If you want to try a Backup tutorial that explains how to restore data for your VM, go to [Next steps](#).

```
az backup protection disable \
--resource-group myResourceGroup \
--vault-name myRecoveryServicesVault \
--container-name myVM \
--item-name myVM \
--delete-backup-data true
az backup vault delete \
--resource-group myResourceGroup \
--name myRecoveryServicesVault \
az group delete --name myResourceGroup
```

Next steps

In this quickstart, you created a Recovery Services vault, enabled protection on a VM, and created the initial recovery point. To learn more about Azure Backup and Recovery Services, continue to the tutorials.

[Back up multiple Azure VMs](#)

Use Azure portal to back up multiple virtual machines

11/18/2019 • 6 minutes to read • [Edit Online](#)

When you back up data in Azure, you store that data in an Azure resource called a Recovery Services vault. The Recovery Services vault resource is available from the Settings menu of most Azure services. The benefit of having the Recovery Services vault integrated into the Settings menu of most Azure services makes it easy to back up data. However, individually working with each database or virtual machine in your business is tedious. What if you want to back up the data for all virtual machines in one department, or in one location? It is easy to back up multiple virtual machines by creating a backup policy and applying that policy to the desired virtual machines. This tutorial explains how to:

- Create a Recovery Services vault
- Define a backup policy
- Apply the backup policy to protect multiple virtual machines
- Trigger an on-demand backup job for the protected virtual machines

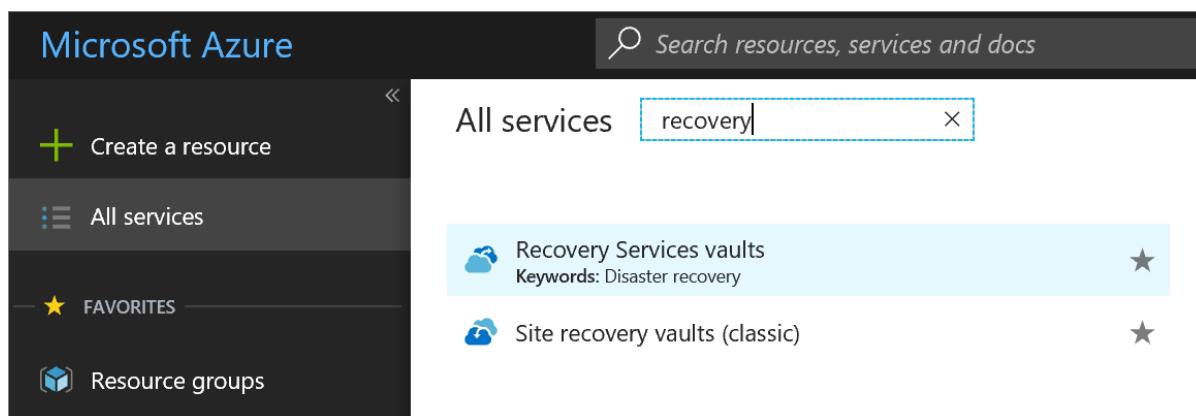
Sign in to the Azure portal

Sign in to the [Azure portal](#).

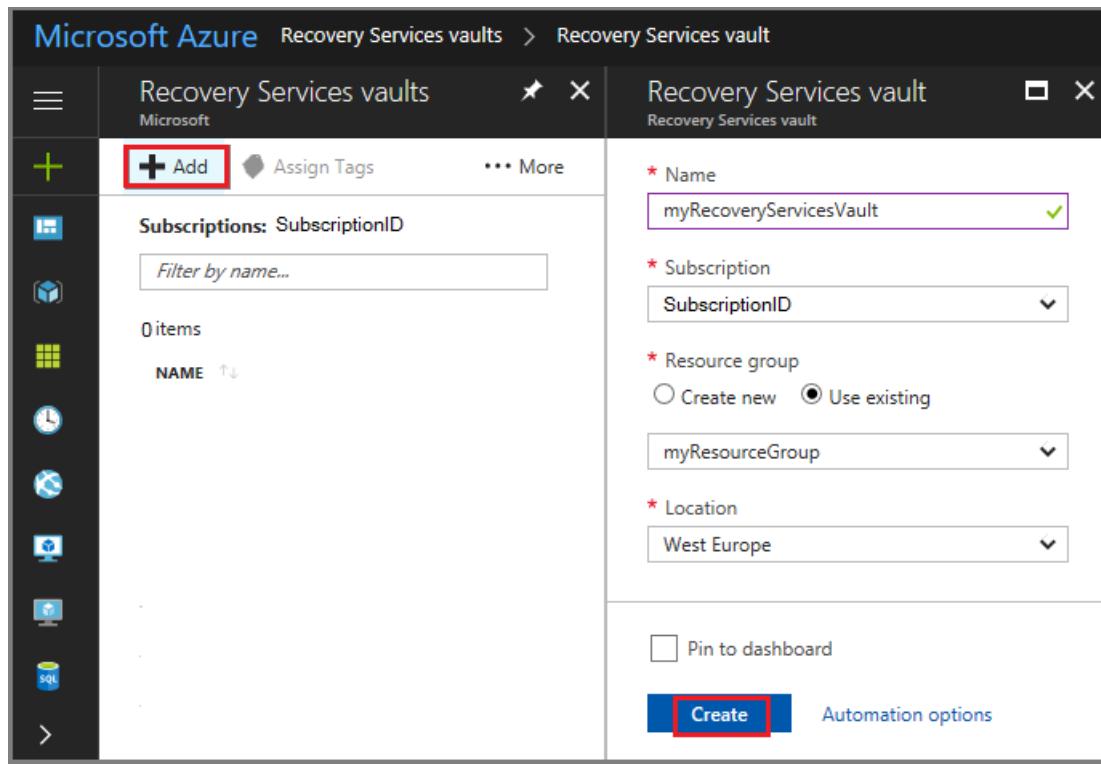
Create a Recovery Services vault

The Recovery Services vault contains the backup data, and the backup policy applied to the protected virtual machines. Backing up virtual machines is a local process. You cannot back up a virtual machine from one location to a Recovery Services vault in another location. So, for each Azure location that has virtual machines to be backed up, at least one Recovery Services vault must exist in that location.

1. On the left-hand menu, select **All services** and in the services list, type *Recovery Services*. As you type, the list of resources filters. When you see Recovery Services vaults in the list, select it to open the Recovery Services vaults menu.



2. In the **Recovery Services vaults** menu, click **Add** to open the Recovery Services vault menu.



3. In the Recovery Services vault menu,

- Type *myRecoveryServicesVault* in **Name**.
- The current subscription ID appears in **Subscription**. If you have additional subscriptions, you could choose another subscription for the new vault.
- For **Resource group**, select **Use existing** and choose *myResourceGroup*. If *myResourceGroup* doesn't exist, select **Create new** and type *myResourceGroup*.
- From the **Location** drop-down menu, choose *West Europe*.
- Click **Create** to create your Recovery Services vault.

A Recovery Services vault must be in the same location as the virtual machines being protected. If you have virtual machines in multiple regions, create a Recovery Services vault in each region. This tutorial creates a Recovery Services vault in *West Europe* because that is where *myVM* (the virtual machine created with the quickstart) was created.

It can take several minutes for the Recovery Services vault to be created. Monitor the status notifications in the upper right-hand area of the portal. Once your vault is created, it appears in the list of Recovery Services vaults.

When you create a Recovery Services vault, by default the vault has geo-redundant storage. To provide data resiliency, geo-redundant storage replicates the data multiple times across two Azure regions.

Set backup policy to protect VMs

After creating the Recovery Services vault, the next step is to configure the vault for the type of data, and to set the backup policy. Backup policy is the schedule for how often and when recovery points are taken. Policy also includes the retention range for the recovery points. For this tutorial, let's assume your business is a sports complex with a hotel, stadium, and restaurants and concessions, and you are protecting the data on the virtual machines. The following steps create a backup policy for the financial data.

1. From the list of Recovery Services vaults, select **myRecoveryServicesVault** to open its dashboard.

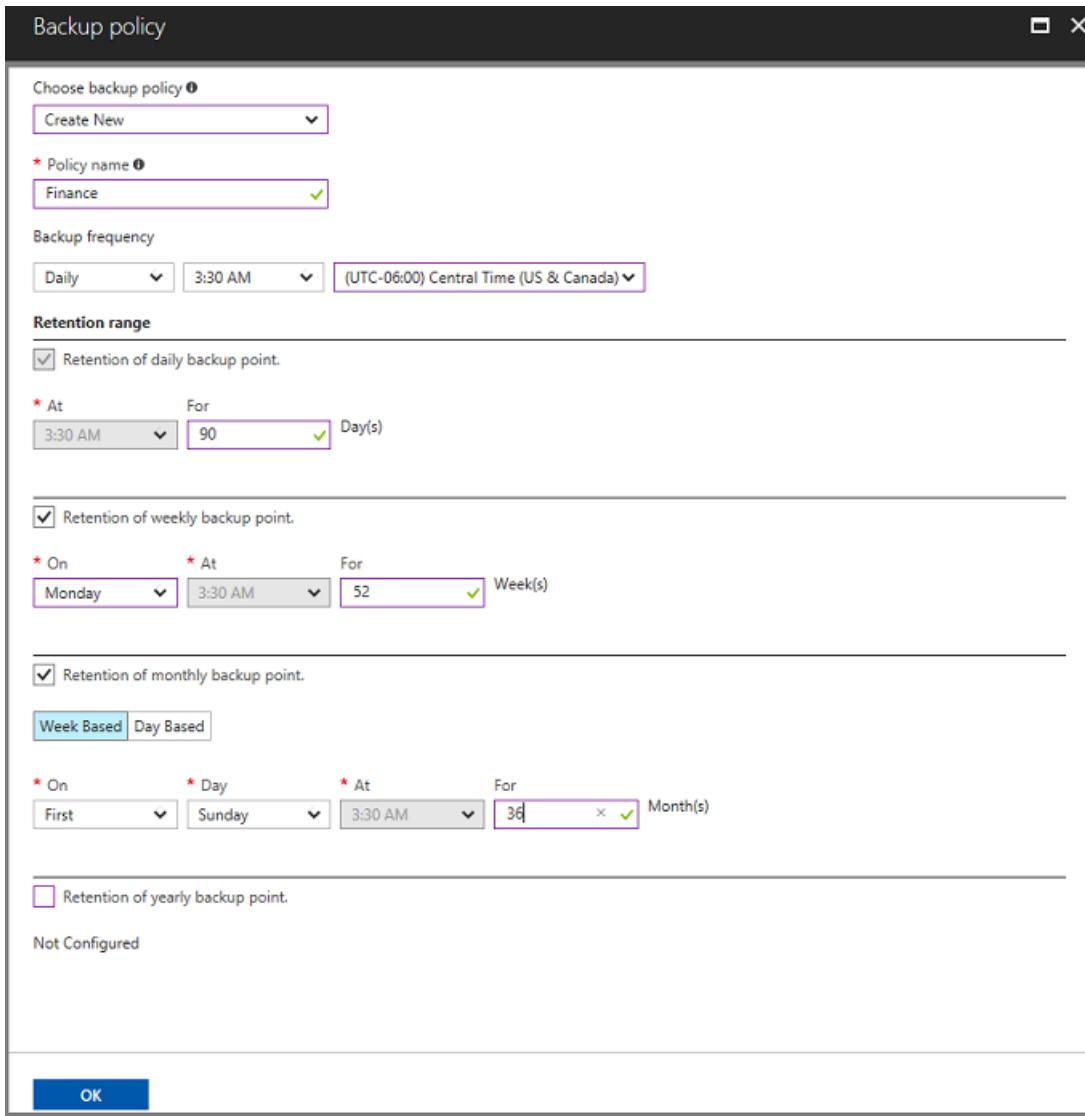
2. On the vault dashboard menu, click **Backup** to open the Backup menu.
3. On the Backup Goal menu, in the **Where is your workload running?** drop-down menu, choose *Azure*. From the **What do you want to backup?** drop-down, choose *Virtual machine*, and click **Backup**.

These actions prepare the Recovery Services vault for interacting with a virtual machine. Recovery Services vaults have a default policy that creates a restore point each day, and retains the restore points for 30 days.

4. To create a new policy, on the Backup policy menu, from the **Choose backup policy** drop-down menu, select *Create New*.

5. In the **Backup policy** menu, for **Policy Name** type *Finance*. Enter the following changes for the Backup policy:

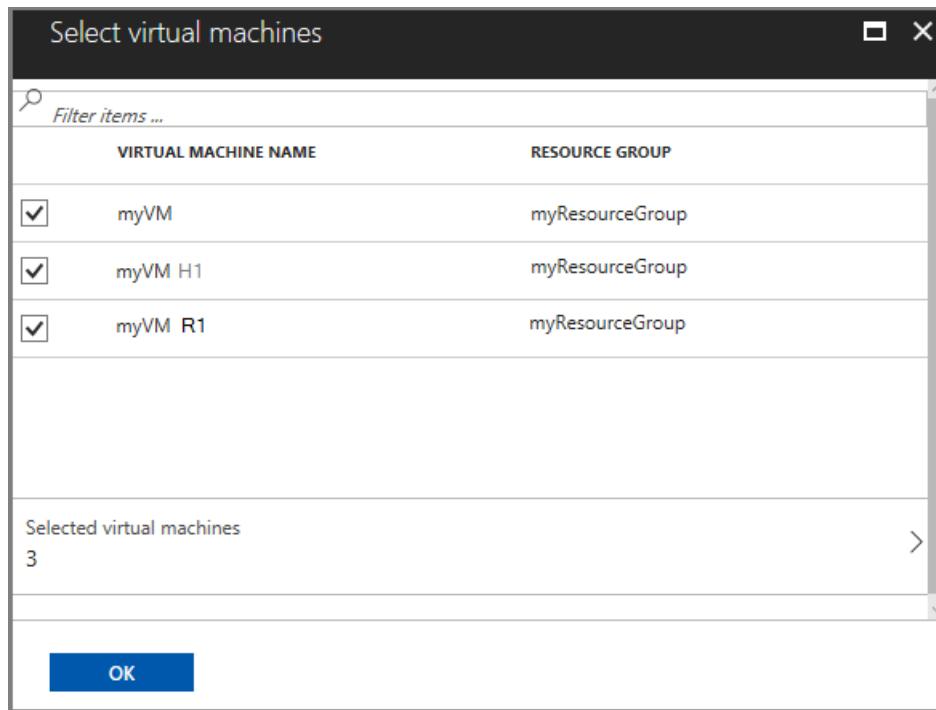
- For **Backup frequency** set the timezone for *Central Time*. Since the sports complex is in Texas, the owner wants the timing to be local. Leave the backup frequency set to Daily at 3:30AM.
- For **Retention of daily backup point**, set the period to 90 days.
- For **Retention of weekly backup point**, use the *Monday* restore point and retain it for 52 weeks.
- For **Retention of monthly backup point**, use the restore point from First Sunday of the month, and retain it for 36 months.
- Deselect the **Retention of yearly backup point** option. The leader of Finance doesn't want to keep data longer than 36 months.
- Click **OK** to create the backup policy.



After creating the backup policy, associate the policy with the virtual machines.

6. In the **Select virtual machines** dialog, select *myVM* and click **OK** to deploy the backup policy to the virtual machines.

All virtual machines that are in the same location, and are not already associated with a backup policy, appear. *myVMH1* and *myVMR1* are selected to be associated with the *Finance* policy.



When the deployment completes, you receive a notification that deployment successfully completed.

Initial backup

You have enabled backup for the Recovery Services vaults, but an initial backup has not been created. It is a disaster recovery best practice to trigger the first backup, so that your data is protected.

To run an on-demand backup job:

1. On the vault dashboard, click **3** under **Backup Items**, to open the Backup Items menu.

The **Backup Items** menu opens.

2. On the **Backup Items** menu, click **Azure Virtual Machine** to open the list of virtual machines associated with the vault.

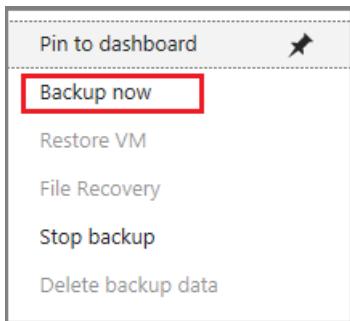
| NAME | RESOURCE GROUP | BACKUP PRE-CHECK | LAST BACKUP STATUS | LATEST RESTORE POI | Context menu |
|-------|-------------------|------------------|----------------------------|--------------------|--------------|
| myVM | myResourceGroup | Passed | Warning(Initial backup...) | | ... |
| buntu | rasquill-security | Passed | Warning(Initial backup...) | | ... |
| ops | rhelpfiles | Passed | Warning(Initial backup...) | | ... |

The **Backup Items** list opens.

| NAME | RESOURCE GROUP | BACKUP PRE-CHECK | LAST BACKUP STATUS | LATEST RESTORE POI | Context menu |
|-------|-------------------|------------------|----------------------------|--------------------|--------------|
| myVM | myResourceGroup | Passed | Warning(Initial backup...) | | ... |
| buntu | rasquill-security | Passed | Warning(Initial backup...) | | ... |
| ops | rhelpfiles | Passed | Warning(Initial backup...) | | ... |

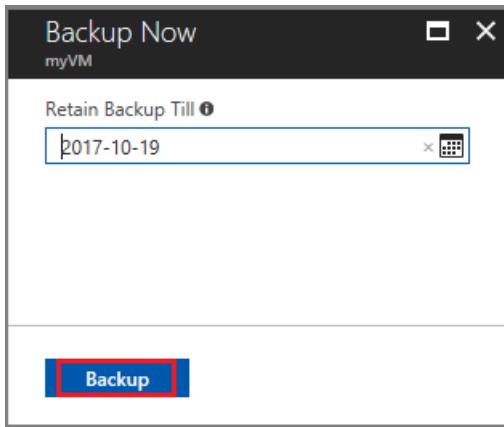
3. On the **Backup Items** list, click the ellipses ... to open the Context menu.

4. On the Context menu, select **Backup now**.



The Backup Now menu opens.

5. On the Backup Now menu, enter the last day to retain the recovery point, and click **Backup**.



Deployment notifications let you know the backup job has been triggered, and that you can monitor the progress of the job on the Backup jobs page. Depending on the size of your virtual machine, creating the initial backup may take a while.

When the initial backup job completes, you can see its status in the Backup job menu. The on-demand backup job created the initial restore point for *myVM*. If you want to back up other virtual machines, repeat these steps for each virtual machine.

| NAME | RESOURCE GROUP | BACKUP PRE-CHECK | LAST BACKUP STATUS | LATEST RESTORE POINT | ... |
|------|-----------------|------------------|--------------------|----------------------|-----|
| myVM | myResourceGroup | Passed | Success | 9/19/2017 6:52:32 PM | ... |

Clean up resources

If you plan to continue on to work with subsequent tutorials, do not clean up the resources created in this tutorial. If you do not plan to continue, use the following steps to delete all resources created by this tutorial in the Azure portal.

1. On the **myRecoveryServicesVault** dashboard, click **3** under **Backup Items**, to open the Backup Items menu.

myRecoveryServicesVault

Recovery Services vault

Search (Ctrl+ /)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

SETTINGS

Properties

Locks

Automation script

GETTING STARTED

Backup

Site Recovery

MONITORING AND REPORTS

Jobs

Alerts and Events

Backup Reports

Backup items

3

Status

Active

Location

West Europe

Subscription name

subscriptionID

Subscription ID

subscription number

Backup management servers

0

Replicated items

0

Monitoring

Backup Alerts (last 24...)

Critical 0

Warning 0

Backup Pre-Check Status (Azure VMs)

CRITICAL 0

TOTAL 0

WARNING 0

Site Recovery Health

Unhealthy serv... 0

Events 0

Updates availa... 0

2. On the **Backup Items** menu, click **Azure Virtual Machine** to open the list of virtual machines associated with the vault.

| BACKUP MANAGEMENT TYPE | BACKUP ITEM COUNT |
|------------------------|-------------------|
| Azure Virtual Machine | 3 |
| Azure Backup Agent | 0 |
| Azure Backup Server | 0 |

The **Backup Items** list opens.

3. In the **Backup Items** menu, click the ellipsis to open the Context menu.

Backup Items (Azure Virtual Machine)

myRecoveryServicesVault

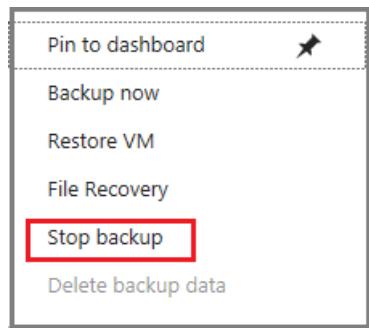
Refresh Add Filter

Fetching data from service completed.

Filter items ...

| NAME | RESOURCE GROUP | BACKUP PRE-CHECK | LAST BACKUP STATUS | LATEST RESTORE POINT | ... |
|---------|-----------------|------------------|--------------------|----------------------|---|
| myVM | myResourceGroup | Passed | Success | 9/19/2017 6:22:37 PM | ... |
| myVM H1 | myResourceGroup | Passed | Success | 9/19/2017 6:32:35 PM | ... |
| myVM R1 | myResourceGroup | Passed | Success | 9/19/2017 6:56:17 PM | ... |

4. On the context menu, select **Stop backup** to open Stop Backup menu.



5. In the **Stop Backup** menu, select the upper drop-down menu and choose **Delete Backup Data**.
6. In the **Type the name of the Backup item** dialog, type **myVM**.
7. Once the backup item is verified (a check mark appears), **Stop backup** button is enabled. Click **Stop Backup** to stop the policy and delete the restore points.

Stop Backup

myVM

Delete Backup Data

i This option will stop all scheduled backup jobs, deletes backup data and can't be undone.

* Type the name of Backup Item
myVM

Reason (optional)
Others

Comments

Stop backup

8. In the **myRecoveryServicesVault** menu, click **Delete**.

The screenshot shows the Azure portal interface for a Recovery Services vault named 'myRecoveryServicesVault'. The left sidebar includes options like 'Overview', 'Activity log', 'Access control (IAM)', and 'Tags'. The main content area has tabs for 'Backup', 'Replicate', and 'Delete', with 'Delete' being the active tab and highlighted with a red box. A survey prompt at the top right encourages users to take a survey about their experience with Azure Backup and Site Recovery. Below the prompt, the 'Essentials' section displays resource group information: 'Resource group (change) myResourceGroup', 'Status Active', 'Backup items 0', and 'Backup management servers 0'.

Once the vault is deleted, you return to the list of Recovery Services vaults.

Next steps

In this tutorial, you used the Azure portal to:

- Create a Recovery Services vault
- Set the vault to protect virtual machines
- Create a custom backup and retention policy
- Assign the policy to protect multiple virtual machines
- Trigger an on-demand back up for virtual machines

Continue to the next tutorial to restore an Azure virtual machine from disk.

[Restore VMs using CLI](#)

Restore a disk and create a recovered VM in Azure

2/10/2020 • 8 minutes to read • [Edit Online](#)

Azure Backup creates recovery points that are stored in geo-redundant recovery vaults. When you restore from a recovery point, you can restore the whole VM or individual files. This article explains how to restore a complete VM using CLI. In this tutorial you learn how to:

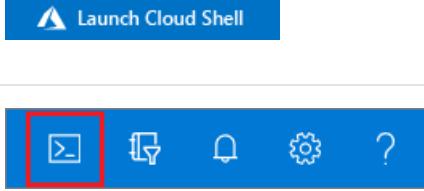
- List and select recovery points
- Restore a disk from a recovery point
- Create a VM from the restored disk

For information on using PowerShell to restore a disk and create a recovered VM, see [Back up and restore Azure VMs with PowerShell](#).

Use Azure Cloud Shell

Azure hosts Azure Cloud Shell, an interactive shell environment that you can use through your browser. You can use either Bash or PowerShell with Cloud Shell to work with Azure services. You can use the Cloud Shell preinstalled commands to run the code in this article without having to install anything on your local environment.

To start Azure Cloud Shell:

| OPTION | EXAMPLE/LINK |
|---|--|
| Select Try It in the upper-right corner of a code block. Selecting Try It doesn't automatically copy the code to Cloud Shell. |  |
| Go to https://shell.azure.com , or select the Launch Cloud Shell button to open Cloud Shell in your browser. |  |
| Select the Cloud Shell button on the menu bar at the upper right in the Azure portal . | |

To run the code in this article in Azure Cloud Shell:

1. Start Cloud Shell.
2. Select the **Copy** button on a code block to copy the code.
3. Paste the code into the Cloud Shell session by selecting **Ctrl+Shift+V** on Windows and Linux or by selecting **Cmd+Shift+V** on macOS.
4. Select **Enter** to run the code.

If you choose to install and use the CLI locally, this tutorial requires that you are running the Azure CLI version 2.0.18 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install the Azure CLI](#).

Prerequisites

This tutorial requires a Linux VM that has been protected with Azure Backup. To simulate an accidental VM deletion and recovery process, you create a VM from a disk in a recovery point. If you need a Linux VM that has

been protected with Azure Backup, see [Back up a virtual machine in Azure with the CLI](#).

Backup overview

When Azure initiates a backup, the backup extension on the VM takes a point-in-time snapshot. The backup extension is installed on the VM when the first backup is requested. Azure Backup can also take a snapshot of the underlying storage if the VM is not running when the backup takes place.

By default, Azure Backup takes a file system consistent backup. Once Azure Backup takes the snapshot, the data is transferred to the Recovery Services vault. To maximize efficiency, Azure Backup identifies and transfers only the blocks of data that have changed since the previous backup.

When the data transfer is complete, the snapshot is removed and a recovery point is created.

List available recovery points

To restore a disk, you select a recovery point as the source for the recovery data. As the default policy creates a recovery point each day and retains them for 30 days, you can keep a set of recovery points that allows you to select a particular point in time for recovery.

To see a list of available recovery points, use `az backup recoverypoint list`. The recovery point **name** is used to recover disks. In this tutorial, we want the most recent recovery point available. The `--query [0].name` parameter selects the most recent recovery point name as follows:

```
az backup recoverypoint list \
--resource-group myResourceGroup \
--vault-name myRecoveryServicesVault \
--backup-management-type AzureIaaSVM \
--container-name myVM \
--item-name myVM \
--query [0].name \
--output tsv
```

Restore a VM disk

IMPORTANT

It is very strongly recommended to use Az CLI version 2.0.74 or later to get all the benefits of a quick restore including managed disk restore. It is best if user always uses the latest version.

Managed disk restore

If the backed up VM has managed disks and if the intent is to restore managed disks from the recovery point, you first provide an Azure storage account. This storage account is used to store the VM configuration and the deployment template that can be later used to deploy the VM from the restored disks. Then, you also provide a target resource group for the managed disks to be restored into.

1. To create a storage account, use `az storage account create`. The storage account name must be all lowercase, and be globally unique. Replace *mystorageaccount* with your own unique name:

```
az storage account create \
--resource-group myResourceGroup \
--name mystorageaccount \
--sku Standard_LRS
```

2. Restore the disk from your recovery point with `az backup restore restore-disks`. Replace *mystorageaccount*

with the name of the storage account you created in the preceding command. Replace *myRecoveryPointName* with the recovery point name you obtained in the output from the previous [az backup recoverypoint list](#) command. **Also provide the target resource group to which the managed disks are restored into.**

```
az backup restore restore-disks \
--resource-group myResourceGroup \
--vault-name myRecoveryServicesVault \
--container-name myVM \
--item-name myVM \
--storage-account mystorageaccount \
--rp-name myRecoveryPointName \
--target-resource-group targetRG
```

WARNING

If *target-resource-group* is not provided then the managed disks will be restored as unmanaged disks to the given storage account. This will have significant consequences to the restore time since the time taken to restore the disks entirely depends on the given storage account.

Unmanaged disks restore

If the backed up VM has unmanaged disks and if the intent is to restore disks from the recovery point, you first provide an Azure storage account. This storage account is used to store the VM configuration and the deployment template that can be later used to deploy the VM from the restored disks. By default, the unmanaged disks will be restored to their original storage accounts. If user wishes to restore all unmanaged disks to one single place, then the given storage account can also be used as a staging location for those disks too.

In additional steps, the restored disk is used to create a VM.

1. To create a storage account, use [az storage account create](#). The storage account name must be all lowercase, and be globally unique. Replace *mystorageaccount* with your own unique name:

```
az storage account create \
--resource-group myResourceGroup \
--name mystorageaccount \
--sku Standard_LRS
```

2. Restore the disk from your recovery point with [az backup restore restore-disks](#). Replace *mystorageaccount* with the name of the storage account you created in the preceding command. Replace *myRecoveryPointName* with the recovery point name you obtained in the output from the previous [az backup recoverypoint list](#) command:

```
az backup restore restore-disks \
--resource-group myResourceGroup \
--vault-name myRecoveryServicesVault \
--container-name myVM \
--item-name myVM \
--storage-account mystorageaccount \
--rp-name myRecoveryPointName
```

As mentioned above, the unmanaged disks will be restored to their original storage account. This provides the best restore performance. But if all unmanaged disks need to be restored to given storage account, then use the relevant flag as shown below.

```

az backup restore restore-disks \
--resource-group myResourceGroup \
--vault-name myRecoveryServicesVault \
--container-name myVM \
--item-name myVM \
--storage-account mystorageaccount \
--rp-name myRecoveryPointName
--restore-to-staging-storage-account
```
Monitor the restore job

To monitor the status of restore job, use [az backup job list](https://docs.microsoft.com/cli/azure/backup/job?view=azure-cli-latest#az-backup-job-list):

```azurecli-interactive
az backup job list \
--resource-group myResourceGroup \
--vault-name myRecoveryServicesVault \
--output table
```

```

The output is similar to the following example, which shows the restore job is *InProgress*:

| Name     | Operation       | Status     | Item Name | Start Time UTC      | Duration       |
|----------|-----------------|------------|-----------|---------------------|----------------|
| 7f2ad916 | Restore         | InProgress | myvm      | 2017-09-19T19:39:52 | 0:00:34.520850 |
| a0a8e5e6 | Backup          | Completed  | myvm      | 2017-09-19T03:09:21 | 0:15:26.155212 |
| fe5d0414 | ConfigureBackup | Completed  | myvm      | 2017-09-19T03:03:57 | 0:00:31.191807 |

When the *Status* of the restore job reports *Completed*, the necessary information (VM configuration and the deployment template) has been restored to the storage account.

## Create a VM from the restored disk

The final step is to create a VM from the restored disks. You can use the deployment template downloaded to the given storage account to create the VM.

### Fetch the Job details

The resultant job details give the template URI that can be queried and deployed. Use the job show command to get more details for the triggered restored job.

```

az backup job show \
-v myRecoveryServicesVault \
-g myResourceGroup \
-n 1fc2d55d-f0dc-4ca6-ad48-aca0fe5d0414

```

The output of this query will give all details but we are interested only in the storage account contents. We can use the [query capability](#) of Azure CLI to fetch the relevant details

```

az backup job show \
-v myRecoveryServicesVault \
-g myResourceGroup \
-n 1fc2d55d-f0dc-4ca6-ad48-aca0fe5d0414 \
--query properties.extendedInfo.propertyBag

{
 "Config Blob Container Name": "myVM-daa1931199fd4a22ae601f46d8812276",
 "Config Blob Name": "config-myVM-1fc2d55d-f0dc-4ca6-ad48-aca0fe5d0414.json",
 "Config Blob Uri": "https://mystorageaccount.blob.core.windows.net/myVM-
daa1931199fd4a22ae601f46d8812276/config-appvm8-1fc2d55d-f0dc-4ca6-ad48-aca0519c0232.json",
 "Job Type": "Recover disks",
 "Recovery point time": "12/25/2019 10:07:11 PM",
 "Target Storage Account Name": "mystorageaccount",
 "Target resource group": "mystorageaccountRG",
 "Template Blob Uri": "https://mystorageaccount.blob.core.windows.net/myVM-
daa1931199fd4a22ae601f46d8812276/azuredeploy1fc2d55d-f0dc-4ca6-ad48-aca0519c0232.json"
}

```

## Fetch the deployment template

The template is not directly accessible since it is under a customer's storage account and the given container. We need the complete URL (along with a temporary SAS token) to access this template.

First, extract the template blob Uri from job details

```

az backup job show \
-v myRecoveryServicesVault \
-g myResourceGroup \
-n 1fc2d55d-f0dc-4ca6-ad48-aca0fe5d0414 \
--query properties.extendedInfo.propertyBag."Template Blob Uri"

"https://mystorageaccount.blob.core.windows.net/myVM-daa1931199fd4a22ae601f46d8812276/azuredeploy1fc2d55d-f0dc-
4ca6-ad48-aca0519c0232.json"

```

The template blob Uri will be of this format and extract the template name

```
https://<storageAccountName.blob.core.windows.net>/<containerName>/<templateName>
```

So, the template name from the above example will be `azuredeploy1fc2d55d-f0dc-4ca6-ad48-aca0519c0232.json` and the container name is `myVM-daa1931199fd4a22ae601f46d8812276`

Now get the SAS token for this container and template as detailed [here](#)

```
expiretime=$(date -u -d '30 minutes' +%Y-%m-%dT%H:%MZ)
connection=$(az storage account show-connection-string \
 --resource-group mystorageaccountRG \
 --name mystorageaccount \
 --query connectionString)
token=$(az storage blob generate-sas \
 --container-name myVM-daa1931199fd4a22ae601f46d8812276 \
 --name azuredeploy1fc2d55d-f0dc-4ca6-ad48-aca0519c0232.json \
 --expiry $expiretime \
 --permissions r \
 --output tsv \
 --connection-string $connection)
url=$(az storage blob url \
 --container-name myVM-daa1931199fd4a22ae601f46d8812276 \
 --name azuredeploy1fc2d55d-f0dc-4ca6-ad48-aca0519c0232.json \
 --output tsv \
 --connection-string $connection)
```

## Deploy the template to create the VM

Now deploy the template to create the VM as explained [here](#).

```
az group deployment create \
 --resource-group ExampleGroup \
 --template-uri $url?$token
```

To confirm that your VM has been created from your recovered disk, list the VMs in your resource group with [az vm list](#) as follows:

```
az vm list --resource-group myResourceGroup --output table
```

## Next steps

In this tutorial, you restored a disk from a recovery point and then created a VM from the disk. You learned how to:

- List and select recovery points
- Restore a disk from a recovery point
- Create a VM from the restored disk

Advance to the next tutorial to learn about restoring individual files from a recovery point.

[Restore files to a virtual machine in Azure](#)

# Restore files to a virtual machine in Azure

11/18/2019 • 6 minutes to read • [Edit Online](#)

Azure Backup creates recovery points that are stored in geo-redundant recovery vaults. When you restore from a recovery point, you can restore the whole VM or individual files. This article details how to restore individual files. In this tutorial you learn how to:

- List and select recovery points
- Connect a recovery point to a VM
- Restore files from a recovery point

## Use Azure Cloud Shell

Azure hosts Azure Cloud Shell, an interactive shell environment that you can use through your browser. You can use either Bash or PowerShell with Cloud Shell to work with Azure services. You can use the Cloud Shell preinstalled commands to run the code in this article without having to install anything on your local environment.

To start Azure Cloud Shell:

| OPTION                                                                                                                                                    | EXAMPLE/LINK                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Select <b>Try It</b> in the upper-right corner of a code block.<br>Selecting <b>Try It</b> doesn't automatically copy the code to Cloud Shell.            |  |
| Go to <a href="https://shell.azure.com">https://shell.azure.com</a> , or select the <b>Launch Cloud Shell</b> button to open Cloud Shell in your browser. |  |
| Select the <b>Cloud Shell</b> button on the menu bar at the upper right in the <a href="#">Azure portal</a> .                                             |  |

To run the code in this article in Azure Cloud Shell:

1. Start Cloud Shell.
2. Select the **Copy** button on a code block to copy the code.
3. Paste the code into the Cloud Shell session by selecting **Ctrl+Shift+V** on Windows and Linux or by selecting **Cmd+Shift+V** on macOS.
4. Select **Enter** to run the code.

If you choose to install and use the CLI locally, this tutorial requires that you are running the Azure CLI version 2.0.18 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install the Azure CLI](#).

## Prerequisites

This tutorial requires a Linux VM that has been protected with Azure Backup. To simulate an accidental file deletion and recovery process, you delete a page from a web server. If you need a Linux VM that runs a webserver and has been protected with Azure Backup, see [Back up a virtual machine in Azure with the CLI](#).

## Backup overview

When Azure initiates a backup, the backup extension on the VM takes a point-in-time snapshot. The backup extension is installed on the VM when the first backup is requested. Azure Backup can also take a snapshot of the underlying storage if the VM is not running when the backup takes place.

By default, Azure Backup takes a file system consistent backup. Once Azure Backup takes the snapshot, the data is transferred to the Recovery Services vault. To maximize efficiency, Azure Backup identifies and transfers only the blocks of data that have changed since the previous backup.

When the data transfer is complete, the snapshot is removed and a recovery point is created.

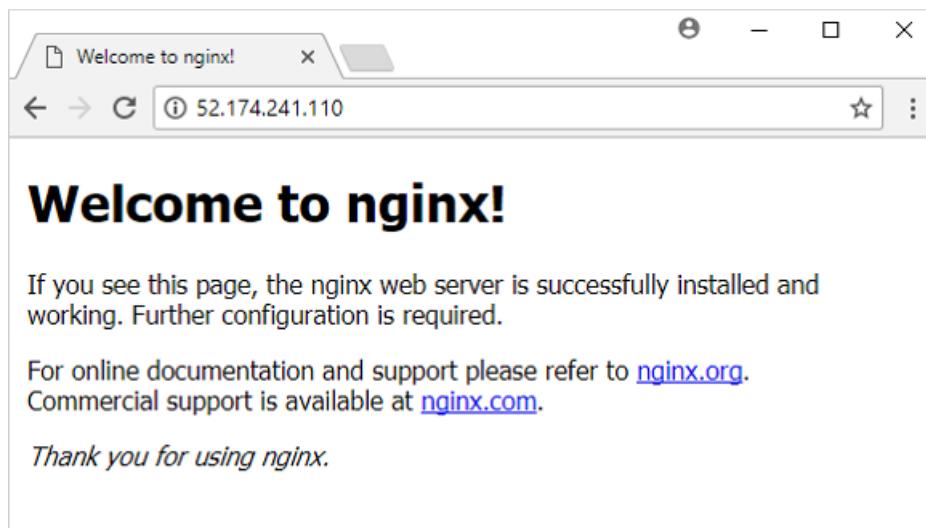
## Delete a file from a VM

If you accidentally delete or make changes to a file, you can restore individual files from a recovery point. This process allows you to browse the files backed up in a recovery point and restore only the files you need. In this example, we delete a file from a web server to demonstrate the file-level recovery process.

1. To connect to your VM, obtain the IP address of your VM with [az vm show](#):

```
az vm show --resource-group myResourceGroup --name myVM -d --query [publicIps] --o tsv
```

2. To confirm that your web site currently works, open a web browser to the public IP address of your VM. Leave the web browser window open.



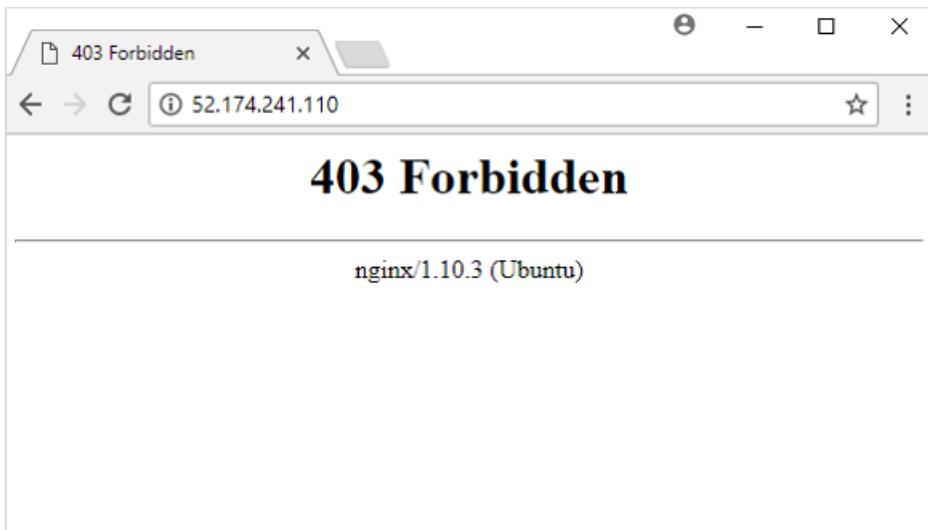
3. Connect to your VM with SSH. Replace *publicIpAddress* with the public IP address that you obtained in a previous command:

```
ssh publicIpAddress
```

4. Delete the default page from the web server at */var/www/html/index.nginx-debian.html* as follows:

```
sudo rm /var/www/html/index.nginx-debian.html
```

5. In your web browser, refresh the web page. The web site no longer loads the page, as shown in the following example:



6. Close the SSH session to your VM as follows:

```
exit
```

## Generate file recovery script

To restore your files, Azure Backup provides a script to run on your VM that connects your recovery point as a local drive. You can browse this local drive, restore files to the VM itself, then disconnect the recovery point. Azure Backup continues to back up your data based on the assigned policy for schedule and retention.

1. To list recovery points for your VM, use [az backup recoverypoint list](#). In this example, we select the most recent recovery point for the VM named *myVM* that is protected in *myRecoveryServicesVault*:

```
az backup recoverypoint list \
--resource-group myResourceGroup \
--vault-name myRecoveryServicesVault \
--container-name myVM \
--item-name myVM \
--query [0].name \
--output tsv
```

2. To obtain the script that connects, or mounts, the recovery point to your VM, use [az backup restore files mount-rp](#). The following example obtains the script for the VM named *myVM* that is protected in *myRecoveryServicesVault*.

Replace *myRecoveryPointName* with the name of the recovery point that you obtained in the preceding command:

```
az backup restore files mount-rp \
--resource-group myResourceGroup \
--vault-name myRecoveryServicesVault \
--container-name myVM \
--item-name myVM \
--rp-name myRecoveryPointName
```

The script is downloaded and a password is displayed, as in the following example:

```
File downloaded: myVM_we_1571974050985163527.sh. Use password c068a041ce12465
```

3. To transfer the script to your VM, use Secure Copy (SCP). Provide the name of your downloaded script, and

replace *publicIpAddress* with the public IP address of your VM. Make sure you include the trailing `:` at the end of the SCP command as follows:

```
scp myVM_we_1571974050985163527.sh 52.174.241.110:
```

## Restore file to your VM

With the recovery script copied to your VM, you can now connect the recovery point and restore files.

1. Connect to your VM with SSH. Replace *publicIpAddress* with the public IP address of your VM as follows:

```
ssh publicIpAddress
```

2. To allow your script to run correctly, add execute permissions with **chmod**. Enter the name of your own script:

```
chmod +x myVM_we_1571974050985163527.sh
```

3. To mount the recovery point, run the script. Enter the name of your own script:

```
./myVM_we_1571974050985163527.sh
```

As the script runs, you are prompted to enter a password to access the recovery point. Enter the password shown in the output from the previous [az backup restore files mount-rp](#) command that generated the recovery script.

The output from the script gives you the path for the recovery point. The following example output shows that the recovery point is mounted at `/home/azureuser/myVM-20170919213536/Volume1`:

```
Microsoft Azure VM Backup - File Recovery

Please enter the password as shown on the portal to securely connect to the recovery point. :
c068a041ce12465

Connecting to recovery point using ISCSI service...

Connection succeeded!

Please wait while we attach volumes of the recovery point to this machine...

***** Volumes of the recovery point and their mount paths on this machine *****

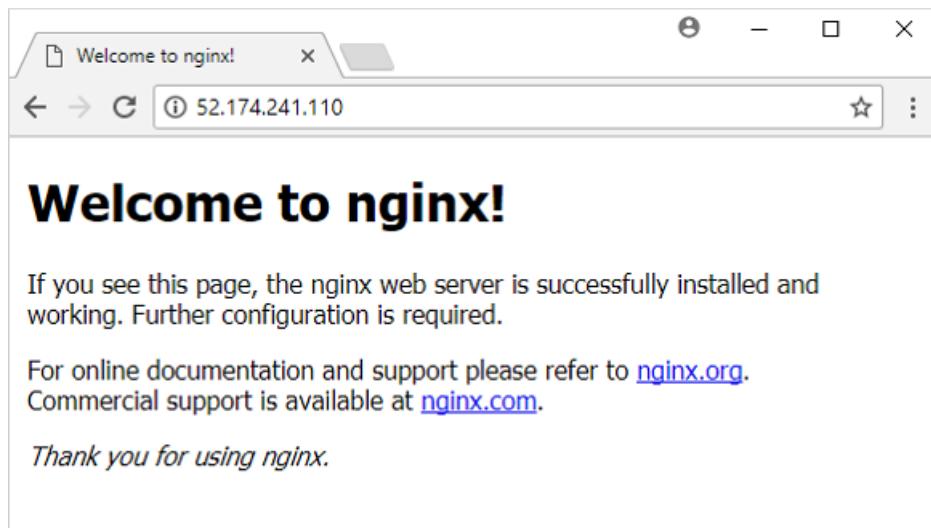
Sr.No. | Disk | Volume | MountPath
1) | /dev/sdc | /dev/sdc1 | /home/azureuser/myVM-20170919213536/Volume1

***** Open File Explorer to browse for files. *****
```

4. Use **cp** to copy the NGINX default web page from the mounted recovery point back to the original file location. Replace the `/home/azureuser/myVM-20170919213536/Volume1` mount point with your own location:

```
sudo cp /home/azureuser/myVM-20170919213536/Volume1/var/www/html/index.nginx-debian.html /var/www/html/
```

5. In your web browser, refresh the web page. The web site now loads correctly again, as shown in the following example:



6. Close the SSH session to your VM as follows:

```
exit
```

7. Unmount the recovery point from your VM with `az backup restore files unmount-rp`. The following example unmounts the recovery point from the VM named *myVM* in *myRecoveryServicesVault*.

Replace *myRecoveryPointName* with the name of your recovery point that you obtained in the previous commands:

```
az backup restore files unmount-rp \
--resource-group myResourceGroup \
--vault-name myRecoveryServicesVault \
--container-name myVM \
--item-name myVM \
--rp-name myRecoveryPointName
```

## Next steps

In this tutorial, you connected a recovery point to a VM and restored files for a web server. You learned how to:

- List and select recovery points
- Connect a recovery point to a VM
- Restore files from a recovery point

Advance to the next tutorial to learn about how to back up Windows Server to Azure.

[Back up Windows Server to Azure](#)

# About Site Recovery

9/9/2019 • 3 minutes to read • [Edit Online](#)

Welcome to the Azure Site Recovery service! This article provides a quick service overview.

As an organization you need to adopt a business continuity and disaster recovery (BCDR) strategy that keeps your data safe, and your apps and workloads up and running, when planned and unplanned outages occur.

Azure Recovery Services contribute to your BCDR strategy:

- **Site Recovery service:** Site Recovery helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. When an outage occurs at your primary site, you fail over to secondary location, and access apps from there. After the primary location is running again, you can fail back to it.
- **Backup service:** The [Azure Backup](#) service keeps your data safe and recoverable by backing it up to Azure.

Site Recovery can manage replication for:

- Azure VMs replicating between Azure regions.
- On-premises VMs, Azure Stack VMs and physical servers.

## What does Site Recovery provide?

| FEATURE                           | DETAILS                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Simple BCDR solution</b>       | Using Site Recovery, you can set up and manage replication, failover, and fallback from a single location in the Azure portal.                                                                                                                                                                                                       |
| <b>Azure VM replication</b>       | You can set up disaster recovery of Azure VMs from a primary region to a secondary region.                                                                                                                                                                                                                                           |
| <b>On-premises VM replication</b> | You can replicate on-premises VMs and physical servers to Azure, or to a secondary on-premises datacenter. Replication to Azure eliminates the cost and complexity of maintaining a secondary datacenter.                                                                                                                            |
| <b>Workload replication</b>       | Replicate any workload running on supported Azure VMs, on-premises Hyper-V and VMware VMs, and Windows/Linux physical servers.                                                                                                                                                                                                       |
| <b>Data resilience</b>            | Site Recovery orchestrates replication without intercepting application data. When you replicate to Azure, data is stored in Azure storage, with the resilience that provides. When failover occurs, Azure VMs are created, based on the replicated data.                                                                            |
| <b>RTO and RPO targets</b>        | Keep recovery time objectives (RTO) and recovery point objectives (RPO) within organizational limits. Site Recovery provides continuous replication for Azure VMs and VMware VMs, and replication frequency as low as 30 seconds for Hyper-V. You can reduce RTO further by integrating with <a href="#">Azure Traffic Manager</a> . |

| FEATURE                                   | DETAILS                                                                                                                                                                                                                                                                                        |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Keep apps consistent over failover</b> | You can replicate using recovery points with application-consistent snapshots. These snapshots capture disk data, all data in memory, and all transactions in process.                                                                                                                         |
| <b>Testing without disruption</b>         | You can easily run disaster recovery drills, without affecting ongoing replication.                                                                                                                                                                                                            |
| <b>Flexible failovers</b>                 | You can run planned failovers for expected outages with zero-data loss, or unplanned failovers with minimal data loss (depending on replication frequency) for unexpected disasters. You can easily fail back to your primary site when it's available again.                                  |
| <b>Customized recovery plans</b>          | Using recovery plans, can customize and sequence the failover and recovery of multi-tier applications running on multiple VMs. You group machines together in a recovery plan, and optionally add scripts and manual actions. Recovery plans can be integrated with Azure automation runbooks. |
| <b>BCDR integration</b>                   | Site Recovery integrates with other BCDR technologies. For example, you can use Site Recovery to protect the SQL Server backend of corporate workloads, with native support for SQL Server AlwaysOn, to manage the failover of availability groups.                                            |
| <b>Azure automation integration</b>       | A rich Azure Automation library provides production-ready, application-specific scripts that can be downloaded and integrated with Site Recovery.                                                                                                                                              |
| <b>Network integration</b>                | Site Recovery integrates with Azure for simple application network management, including reserving IP addresses, configuring load-balancers, and integrating Azure Traffic Manager for efficient network switchovers.                                                                          |

## What can I replicate?

| SUPPORTED                    | DETAILS                                                                                                                                                                                   |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Replication scenarios</b> | <p>Replicate Azure VMs from one Azure region to another.</p> <p>Replicate on-premises VMware VMs, Hyper-V VMs, physical servers (Windows and Linux), Azure Stack VMs to Azure.</p>        |
|                              | <p>Replicate AWS Windows instances to Azure.</p> <p>Replicate on-premises VMware VMs, Hyper-V VMs managed by System Center VMM, and physical servers to a secondary site.</p>             |
| <b>Regions</b>               | Review <a href="#">supported regions</a> for Site Recovery.                                                                                                                               |
| <b>Replicated machines</b>   | Review the replication requirements for <a href="#">Azure VM</a> replication, <a href="#">on-premises VMware VMs and physical servers</a> , and <a href="#">on-premises Hyper-V VMs</a> . |

| SUPPORTED        | DETAILS                                                                                                                                                                                              |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Workloads</b> | You can replicate any workload running on a machine that's supported for replication. In addition, the Site Recovery team have performed app-specific testing for a <a href="#">number of apps</a> . |

## Next steps

- Read more about [workload support](#).
- Get started with [Azure VM replication between regions](#).

# Set up disaster recovery for Azure VMs

1/24/2020 • 9 minutes to read • [Edit Online](#)

The [Azure Site Recovery](#) service contributes to your disaster recovery strategy by managing and orchestrating replication, failover, and failback of on-premises machines and Azure virtual machines (VMs).

This tutorial shows you how to set up disaster recovery for Azure VMs by replicating them from one Azure region to another. In this tutorial, you learn how to:

- Create a Recovery Services vault
- Verify target resource settings
- Set up outbound network connectivity for VMs
- Enable replication for a VM

## NOTE

This article provides instructions for deploying disaster recovery with the simplest settings. If you want to learn about customized settings, review the articles in the [How To section](#).

## Prerequisites

To complete this tutorial:

- Review the [scenario architecture and components](#).
- Review the [support requirements](#) before you start.

## Create a Recovery Services vault

Create the vault in any region, except the source region.

1. Sign in to the [Azure portal](#).
2. On the Azure portal menu or from the **Home** page, select **Create a resource**. Then, select **IT & Management Tools > Backup and Site Recovery**.
3. In **Name**, specify a friendly name to identify the vault. If you have more than one subscription, select the appropriate one.
4. Create a resource group or select an existing one. Specify an Azure region. To check supported regions, see geographic availability in [Azure Site Recovery Pricing Details](#).
5. To access the vault from the dashboard, select **Pin to dashboard** and then select **Create**.

The screenshot shows the Azure portal interface for creating a new Recovery Services vault. On the left, there's a list of existing vaults: contosoassessment-Migr..., ContosoCorporation-Rec..., ContosoDemo, ContosoEmpty, ContosoScale, ContosoVMVault, ContosoVMVault, and Demo. On the right, the 'Recovery Services vault' creation form is open. It includes fields for Name (Vault1), Subscription (<subscription-name>), Resource group (RG1), and Location (West Central US). A note at the top right suggests trying a new preview experience.

The new vault is added to the **Dashboard** under **All resources**, and on the main **Recovery Services vaults** page.

## Verify target resource settings

Check your Azure subscription for the target region.

- Verify that your Azure subscription allows you to create VMs in the target region. Contact support to enable the required quota.
- Make sure your subscription has enough resources to support VM sizes that match your source VMs. Site Recovery picks the same size, or the closest possible size, for the target VM.

## Set up outbound network connectivity for VMs

For Site Recovery to work as expected, you need to modify outbound network connectivity from the VMs that you want to replicate.

### NOTE

Site Recovery doesn't support using an authentication proxy to control network connectivity.

### Outbound connectivity for URLs

If you're using a URL-based firewall proxy to control outbound connectivity, allow access to these URLs:

| URL                       | DETAILS                                                                                  |
|---------------------------|------------------------------------------------------------------------------------------|
| *.blob.core.windows.net   | Allows data to be written from the VM to the cache storage account in the source region. |
| login.microsoftonline.com | Provides authorization and authentication to Site Recovery service URLs.                 |

| URL                                      | DETAILS                                                               |
|------------------------------------------|-----------------------------------------------------------------------|
| *.hypervrecoverymanager.windowsazure.com | Allows the VM to communicate with the Site Recovery service.          |
| *.servicebus.windows.net                 | Allows the VM to write Site Recovery monitoring and diagnostics data. |

## Outbound connectivity for IP address ranges

If you're using a network security group (NSG), create service-tag based NSG rules for access to Azure Storage, Azure Active Directory, Site Recovery service, and Site Recovery monitoring. [Learn more](#).

## Verify Azure VM certificates

Check that the VMs you want to replicate have the latest root certificates. If they don't, the VM can't be registered to Site Recovery because of security constraints.

- For Windows VMs, install all the latest Windows updates on the VM, so that all the trusted root certificates are on the machine. In a disconnected environment, follow the standard Windows Update and certificate update processes for your organization.
- For Linux VMs, follow the guidance provided by your Linux distributor, to get the latest trusted root certificates and certificate revocation list on the VM.

## Set permissions on the account

Azure Site Recovery provides three built-in roles to control Site Recovery management operations.

- Site Recovery Contributor** - This role has all permissions required to manage Azure Site Recovery operations in a Recovery Services vault. A user with this role, however, can't create or delete a Recovery Services vault or assign access rights to other users. This role is best suited for disaster recovery administrators who can enable and manage disaster recovery for applications or entire organizations.
- Site Recovery Operator** - This role has permissions to execute and manage Failover and Failback operations. A user with this role can't enable or disable replication, create or delete vaults, register new infrastructure, or assign access rights to other users. This role is best suited for a disaster recovery operator who can fail over virtual machines or applications when instructed by application owners and IT administrators. Post resolution of the disaster, the disaster recovery operator can reprotect and failback the virtual machines.
- Site Recovery Reader** - This role has permissions to view all Site Recovery management operations. This role is best suited for an IT monitoring executive who can monitor the current state of protection and raise support tickets.

Learn more about [Azure RBAC built-in roles](#).

## Enable replication for a VM

The following sections describe how to enable replication.

### Select the source

To begin the replication set up, choose the source where your Azure VMs are running.

- Go to **Recovery Services vaults**, select the vault name, then select **+Replicate**.
- For the **Source**, select **Azure**.
- In **Source location**, select the source Azure region where your VMs are currently running.

- Select the **Source subscription** where the virtual machines are running. This can be any subscription within the same Azure Active Directory tenant where your recovery services vault exists.
- Select the **Source resource group**, and select **OK** to save the settings.

The image shows two overlapping windows. On the left is the 'Enable replication' wizard with three steps: 1. Source Configure, 2. Virtual machines Select, and 3. Replication settings Configure replication settings. Step 1 is highlighted. On the right is the 'Source' configuration dialog, which has a dropdown for 'Source' set to 'Azure'. It also contains fields for 'Source location' (West US), 'Azure virtual machine deployment model' (Resource Manager), 'Source subscription' (<subscription-ID>), and 'Source resource group' (123). Both windows have a header bar with a close button.

### Select the VMs

Site Recovery retrieves a list of the VMs associated with the subscription and resource group/cloud service.

- In **Virtual Machines**, select the VMs you want to replicate.
- Select **OK**.

### Configure replication settings

Site Recovery creates default settings and replication policy for the target region. You can change these settings as required.

- Select **Settings** to view the target and replication settings.
- To override the default target settings, select **Customize** next to **Resource group, Network, Storage and Availability**.

The image shows the 'Configure settings' dialog. It includes a 'Target location' dropdown set to 'East US 2', a 'Target subscription' section with a 'Customize' link, and a note about customizing resource groups, network, storage, and availability sets. Below this is a table for customizing target settings.

| SETTING | DETAILS |
|---------|---------|
|         |         |

| SETTING                                                           | DETAILS                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Target subscription</b>                                        | By default, the target subscription is the same as the source subscription. Select <b>Customize</b> to select a different target subscription within the same Azure Active Directory tenant.                                                                                                                                                                                                              |
| <b>Target location</b>                                            | <p>The target region used for disaster recovery.</p> <p>We recommend that the target location matches the location of the Site Recovery vault.</p>                                                                                                                                                                                                                                                        |
| <b>Target resource group</b>                                      | <p>The resource group in the target region that holds Azure VMs after failover.</p> <p>By default, Site Recovery creates a new resource group in the target region with an <code>asr</code> suffix. The location of the target resource group can be any region except the region in which your source virtual machines are hosted.</p>                                                                   |
| <b>Target virtual network</b>                                     | <p>The network in the target region that VMs are located after failover.</p> <p>By default, Site Recovery creates a new virtual network (and subnets) in the target region with an <code>asr</code> suffix.</p>                                                                                                                                                                                           |
| <b>Cache storage accounts</b>                                     | <p>Site Recovery uses a storage account in the source region. Changes to source VMs are sent to this account before replication to the target location.</p> <p>If you're using a firewall-enabled cache storage account, make sure that you enable <b>Allow trusted Microsoft services</b>. <a href="#">Learn more</a>. Also, ensure that you allow access to at least one subnet of the source Vnet.</p> |
| <b>Target storage accounts (source VM uses non-managed disks)</b> | <p>By default, Site Recovery creates a new storage account in the target region to mirror the source VM storage account.</p> <p>Enable <b>Allow trusted Microsoft services</b> if you're using a firewall-enabled cache storage account.</p>                                                                                                                                                              |
| <b>Replica managed disks (If source VM uses managed disks)</b>    | By default, Site Recovery creates replica managed disks in the target region to mirror the source VM's managed disks with the same storage type (standard or premium) as the source VM's managed disk. You can only customize Disk type.                                                                                                                                                                  |
| <b>Target availability sets</b>                                   | By default, Azure Site Recovery creates a new availability set in the target region with name having <code>asr</code> suffix for the VMs part of an availability set in source region. In case availability set created by Azure Site Recovery already exists, it's reused.                                                                                                                               |

| SETTING                          | DETAILS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Target availability zones</b> | <p>By default, Site Recovery assigns the same zone number as the source region in target region if the target region supports availability zones.</p> <p>If the target region doesn't support availability zones, the target VMs are configured as single instances by default.</p> <p>Select <b>Customize</b> to configure VMs as part of an availability set in the target region.</p> <p>You can't change the availability type (single instance, availability set, or availability zone) after you enable replication. To change the availability type, disable and enable replication.</p> |

- To customize replication policy settings, select **Customize** next to **Replication policy**, and modify the settings as needed.

| SETTING                                  | DETAILS                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Replication policy name</b>           | Policy name.                                                                                                                                                                                                                                                                                                                                                |
| <b>Recovery point retention</b>          | By default, Site Recovery keeps recovery points for 24 hours. You can configure a value between 1 and 72 hours.                                                                                                                                                                                                                                             |
| <b>App-consistent snapshot frequency</b> | <p>By default, Site Recovery takes an app-consistent snapshot every 4 hours. You can configure any value between 1 and 12 hours.</p> <p>An app-consistent snapshot is a point-in-time snapshot of the application data inside the VM. Volume Shadow Copy Service (VSS) ensures that app on the VM are in a consistent state when the snapshot is taken.</p> |
| <b>Replication group</b>                 | If your application needs multi-VM consistency across VMs, you can create a replication group for those VMs. By default, the selected VMs are not part of any replication group.                                                                                                                                                                            |

- In **Customize**, select **Yes** for multi-VM consistency if you want to add VMs to a new or existing replication group. Then select **OK**.

#### NOTE

- All the machines in a replication group have shared crash consistent and app-consistent recovery points when failed over.
- Enabling multi-VM consistency can impact workload performance (it's CPU intensive). It should be used only if machines are running the same workload, and you need consistency across multiple machines.
- You can have a maximum of 16 VMs in a replication group.
- If you enable multi-VM consistency, machines in the replication group communicate with each other over port 20004. Make sure there's no firewall blocking the internal communication between the VMs over this port.
- For Linux VMs in a replication group, ensure the outbound traffic on port 20004 is manually opened in accordance with guidance for the Linux version.

## Configure encryption settings

If the source VM has Azure disk encryption (ADE) enabled, review the settings.

1. Verify the settings:
  - a. **Disk encryption key vaults:** By default, Site Recovery creates a new key vault on the source VM disk encryption keys, with an `asr` suffix. If the key vault already exists, it's reused.
  - b. **Key encryption key vaults:** By default, Site Recovery creates a new key vault in the target region. The name has an `asr` suffix, and is based on the source VM key encryption keys. If the key vault created by Site Recovery already exists, it's reused.
2. Select **Customize** to select custom key vaults.

#### NOTE

Only Azure VMs running Windows operating systems and [enabled for encryption with Azure AD app](#) are currently supported by Azure Site Recovery.

## Track replication status

After replication is enabled, you can track the job's status.

1. In **Settings**, select **Refresh** to get the latest status.
2. Track progress and status as follows:
  - a. Track progress of the **Enable protection** job in **Settings > Jobs > Site Recovery Jobs**.
  - b. In **Settings > Replicated Items**, you can view the status of VMs and the initial replication progress.  
Select the VM to drill down into its settings.

## Next steps

In this tutorial, you configured disaster recovery for an Azure VM. Now you can run a disaster recovery drill to check that failover works as expected.

[Run a disaster recovery drill](#)

# Run a disaster recovery drill to a secondary region for Azure VMs

1/17/2020 • 2 minutes to read • [Edit Online](#)

The [Azure Site Recovery](#) service contributes to your business continuity and disaster recovery (BCDR) strategy by keeping your business apps up and running available during planned and unplanned outages. Site Recovery manages and orchestrates disaster recovery of on-premises machines and Azure virtual machines (VMs), including replication, failover, and recovery.

This tutorial shows you how to run a disaster recovery drill for an Azure VM, from one Azure region to another, with a test failover. A drill validates your replication strategy without data loss or downtime, and doesn't affect your production environment. In this tutorial, you learn how to:

- Check the prerequisites
- Run a test failover for a single VM

## NOTE

This tutorial helps you to perform a disaster recovery drill with minimal steps. To learn more about the various functions related to doing a disaster recovery drill, see the documentation for Azure VMs [replication](#), [networking](#), [automation](#), or [troubleshooting](#).

## Prerequisites

Check the following items before you do this tutorial:

- Before you run a test failover, we recommend that you check the VM's properties to make sure it's configured for disaster recovery. Go to the VM's **Operations > Disaster Recovery > Properties** to view the replication and failover properties.
- **We recommend you use a separate Azure VM network for the test failover**, and not the default network that was set up when you enabled replication.
- Depending on your source networking configurations for each NIC, you can specify **Subnet**, **Private IP address**, **Public IP**, **Network security group**, or **Load balancer** to attach to each NIC under test failover settings in **Compute and Network** before doing a disaster recovery drill.

## Run a test failover

This example shows how to use a Recovery Services vault to do a VM test failover.

1. Select a vault and go to **Protected items > Replicated items** and select a VM.
2. In **Test Failover**, select a recovery point to use for the failover:
  - **Latest**: Processes all the data in Site Recovery and provides the lowest RTO (Recovery Time Objective).
  - **Latest processed**: Fails the VM over to the latest recovery point that was processed by Site Recovery. The time stamp is shown. With this option, no time is spent processing data, so it provides a low RTO.
  - **Latest app-consistent**: This option fails over all VMs to the latest app-consistent recovery point. The time stamp is shown.
  - **Custom**: Fail over to particular recovery point. Custom is only available when you fail over a single VM, and not for failover with a recovery plan.

3. Select the target Azure virtual network that Azure VMs in the secondary region will connect to after the failover.

**NOTE**

If the test failover settings are pre-configured for the replicated item, the dropdown menu to select an Azure virtual network isn't visible.

4. To start the failover, select **OK**. To track the progress from the vault, go to **Monitoring > Site Recovery jobs** and select the **Test Failover** job.
5. After the failover finishes, the replica Azure VM appears in the Azure portal's **Virtual Machines**. Make sure that the VM is running, sized appropriately, and connected to the appropriate network.
6. To delete the VMs that were created during the test failover, select **Cleanup test failover** on the replicated item or the recovery plan. In **Notes**, record and save any observations associated with the test failover.

## Next steps

[Run a production failover](#)

# Fail over and reprotect Azure VMs between regions

8/5/2019 • 2 minutes to read • [Edit Online](#)

This tutorial describes how to fail over an Azure virtual machine (VM) to a secondary Azure region with the [Azure Site Recovery](#) service. After you've failed over, you reprotect the VM. In this tutorial, you learn how to:

- Fail over the Azure VM
- Reprotect the secondary Azure VM, so that it replicates to the primary region.

## NOTE

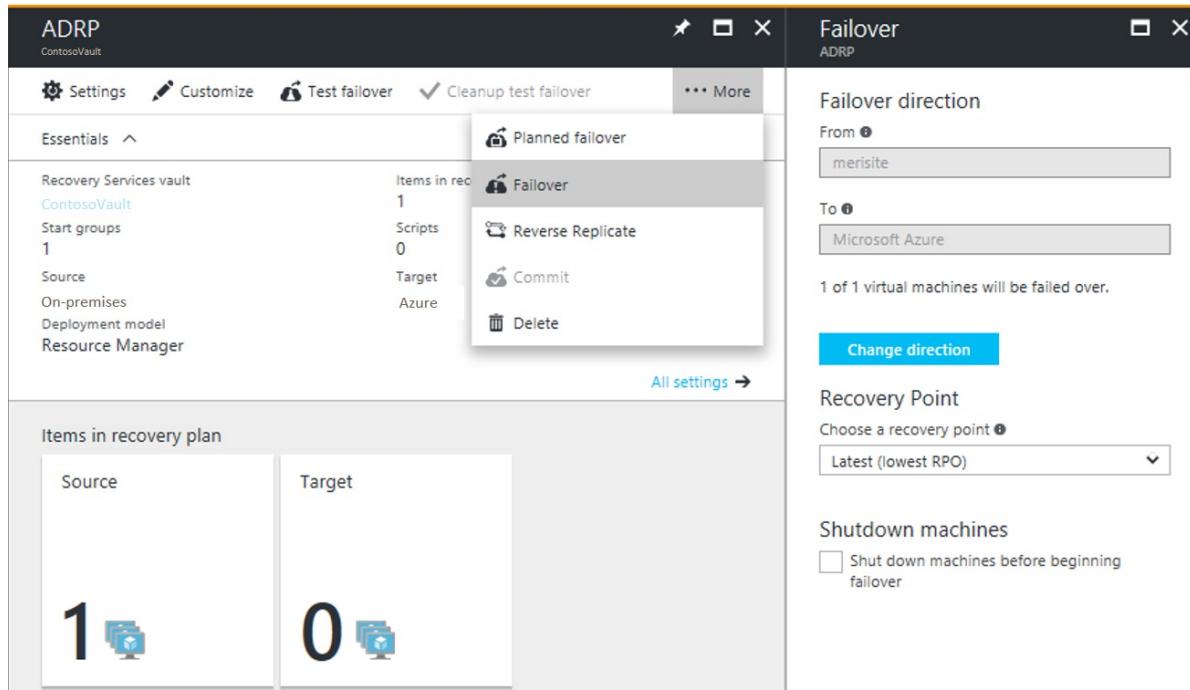
This tutorial contains the simplest path with default settings and minimum customization. For more complex scenarios, use the articles under 'How To' for Azure VMs.

## Prerequisites

- Before you start, review [frequently asked questions](#) about failover.
- Make sure that you've completed a [disaster recovery drill](#) to check everything is working as expected.
- Verify the VM properties before you run the test failover. The VM must comply with [Azure requirements](#).

## Run a failover to the secondary region

1. In **Replicated items**, select the VM that you want to fail over > **Failover**



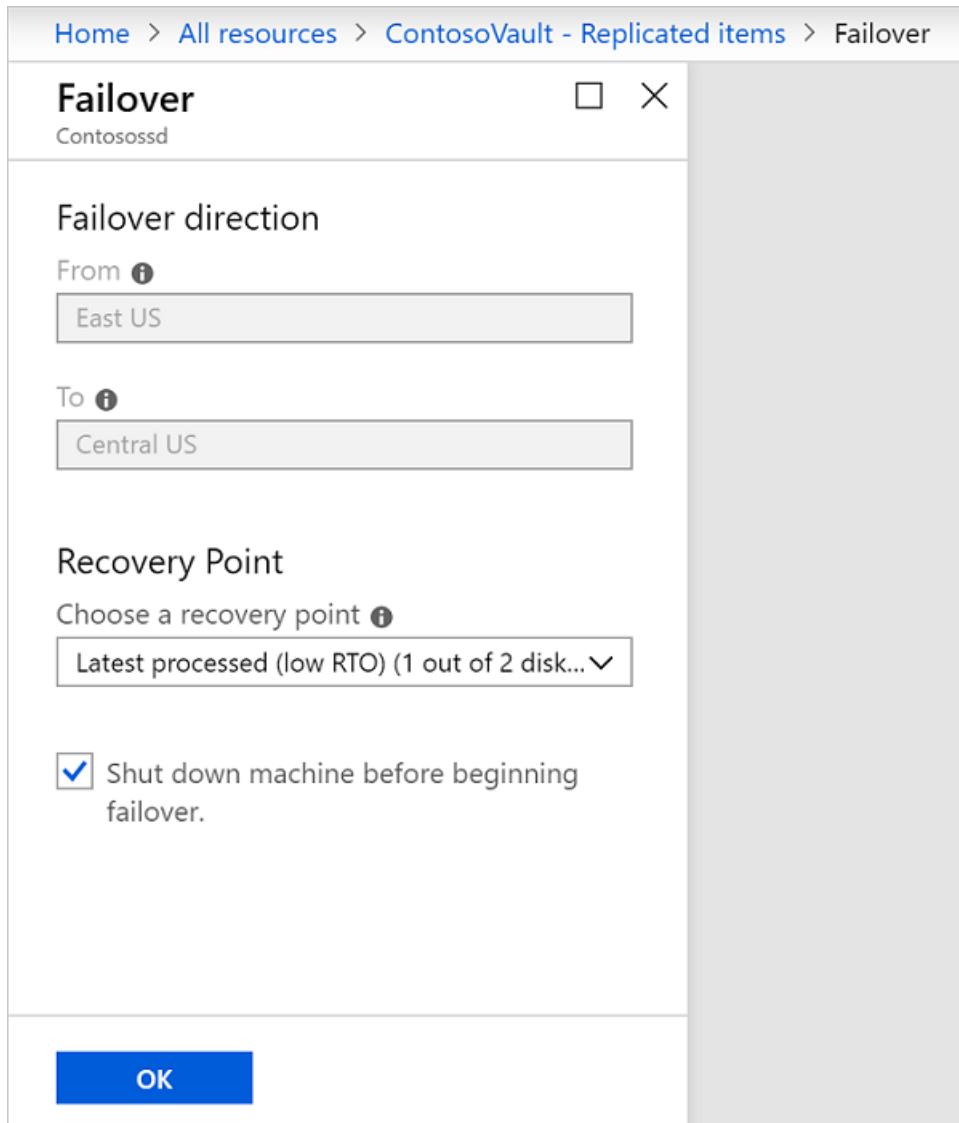
2. In **Failover**, select a **Recovery Point** to fail over to. You can use one of the following options:

- **Latest** (default): Processes all the data in the Site Recovery service and provides the lowest Recovery Point Objective (RPO).
- **Latest processed**: Reverts the virtual machine to the latest recovery point that has been processed by Site Recovery service.
- **Custom**: Fails over to a particular recovery point. This option is useful for performing a test failover.

3. Select **Shut down machine before beginning failover** if you want Site Recovery to attempt to do a shutdown of source VMs before triggering the failover. Shutdown helps to ensure no data loss. Failover continues even if shutdown fails. Site Recovery does not clean up the source after failover.
4. Follow the failover progress on the **Jobs** page.
5. After the failover, validate the virtual machine by logging in to it. If you want to go another recovery point for the virtual machine, then you can use **Change recovery point** option.
6. Once you are satisfied with the failed over virtual machine, you can **Commit** the failover. Committing deletes all the recovery points available with the service. You won't now be able to change the recovery point.

#### **NOTE**

When you fail over a VM to which you add a disk after you enabled replication for the VM, replication points will show the disks that are available for recovery. For example, if a VM has a single disk and you add a new one, replication points that were created before you added the disk will show that the replication point consists of "1 of 2 disks".

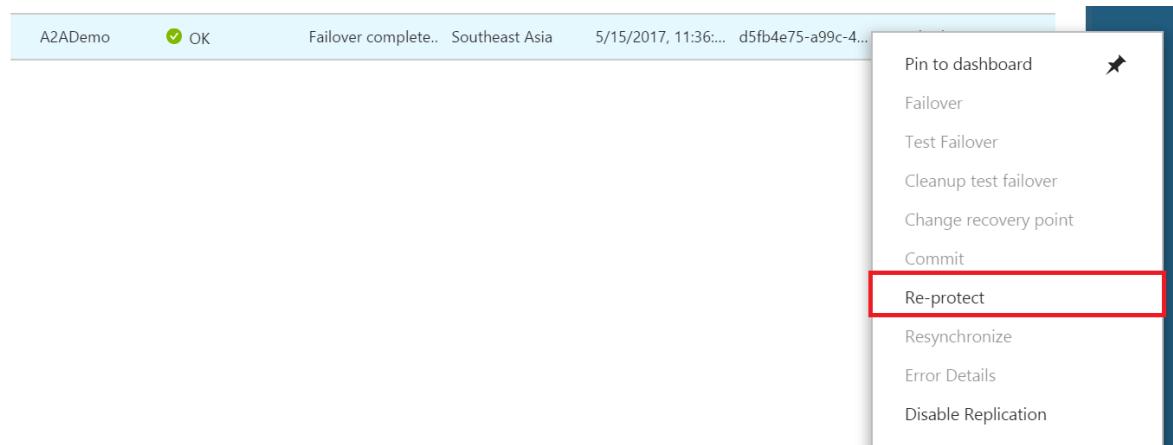


## Reprotect the secondary VM

After failover of the VM, you need to reprotect it so that it replicates back to the primary region.

1. Make sure that the VM is in the **Failover committed** state, and check that the primary region is available, and you're able to create and access new resources in it.

2. In **Vault > Replicated items**, right-click the VM that's been failed over, and then select **Re-Protect**.



3. Verify that the direction of protection, secondary to primary region, is already selected.
4. Review the **Resource group, Network, Storage, and Availability sets** information. Any resources marked as new are created as part of the reprotect operation.
5. Click **OK** to trigger a reprotect job. This job seeds the target site with the latest data. Then, it replicates the deltas to the primary region. The VM is now in a protected state.

## Next steps

- After reprotecting, [learn how to](#) fail back to the primary region when it's available.
- [Learn more](#) about the reprotection flow.

# Understanding Azure virtual machine usage

11/13/2019 • 7 minutes to read • [Edit Online](#)

By analyzing your Azure usage data, powerful consumption insights can be gained – insights that can enable better cost management and allocation throughout your organization. This document provides a deep dive into your Azure Compute consumption details. For more details on general Azure usage, navigate to [Understanding your bill](#).

## Download your usage details

To begin, [download your usage details](#). The table below provides the definition and example values of usage for Virtual Machines deployed via the Azure Resource Manager. This document does not contain detailed information for VMs deployed via our classic model.

| FIELDS             | MEANING                                                                                                                                                                                                                                                                                                                                                                                                | EXAMPLE VALUES                         |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|
| Usage Date         | The date when the resource was used.                                                                                                                                                                                                                                                                                                                                                                   | "11/23/2017"                           |
| Meter ID           | Identifies the top-level service for which this usage belongs to.                                                                                                                                                                                                                                                                                                                                      | "Virtual Machines"                     |
| Meter Sub-Category | The billed meter identifier. <ul style="list-style-type: none"><li>For Compute Hour usage, there is a meter for each VM Size + OS (Windows, Non-Windows) + Region.</li><li>For Premium software usage, there is a meter for each software type. Most premium software images have different meters for each core size. For more information, visit the <a href="#">Compute Pricing Page</a>.</li></ul> | "2005544f-659d-49c9-9094-8e0aea1be3a5" |
| Meter Name         | This is specific for each service in Azure. For compute, it is always "Compute Hours".                                                                                                                                                                                                                                                                                                                 | "Compute Hours"                        |
| Meter Region       | Identifies the location of the datacenter for certain services that are priced based on datacenter location.                                                                                                                                                                                                                                                                                           | "JA East"                              |
| Unit               | Identifies the unit that the service is charged in. Compute resources are billed per hour.                                                                                                                                                                                                                                                                                                             | "Hours"                                |
| Consumed           | The amount of the resource that has been consumed for that day. For Compute, we bill for each minute the VM ran for a given hour (up to 6 decimals of accuracy).                                                                                                                                                                                                                                       | "1", "0.5"                             |

| FIELDS            | MEANING                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | EXAMPLE VALUES                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Resource Location | Identifies the datacenter where the resource is running.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | "JA East"                                                                                                                                                                                                                                                                                                                                                                                                   |
| Consumed Service  | The Azure platform service that you used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | "Microsoft.Compute"                                                                                                                                                                                                                                                                                                                                                                                         |
| Resource Group    | The resource group in which the deployed resource is running in. For more information, see <a href="#">Azure Resource Manager overview</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | "MyRG"                                                                                                                                                                                                                                                                                                                                                                                                      |
| Instance ID       | The identifier for the resource. The identifier contains the name you specify for the resource when it was created. For VMs, the Instance ID will contain the SubscriptionId, ResourceGroupName, and VMName (or scale set name for scale set usage).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <pre>"/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx/ resourceGroups/MyRG/providers/Microsoft.Compute/virtualMachines/MyVM1"</pre> <p>or</p> <pre>"/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx/ resourceGroups/MyRG/providers/Microsoft.Compute/virtualMachineScaleSets/MyVMSS1"</pre>                                                                                                             |
| Tags              | Tag you assign to the resource. Use tags to group billing records. Learn how to <a href="#">tag your Virtual Machines</a> . This is available for Resource Manager VMs only.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <pre>"</pre> <pre>{"myDepartment":"RD","myUser":"myName"}</pre>                                                                                                                                                                                                                                                                                                                                             |
| Additional Info   | <p>Service-specific metadata. For VMs, we populate the following data in the additional info field:</p> <ul style="list-style-type: none"> <li>• Image Type- specific image that you ran. Find the full list of supported strings below under Image Types.</li> <li>• Service Type: the size that you deployed.</li> <li>• VMName: name of your VM. This field is only populated for scale set VMs. If you need your VM Name for scale set VMs, you can find that in the Instance ID string above.</li> <li>• UsageType: This specifies the type of usage this represents. <ul style="list-style-type: none"> <li>◦ ComputeHR is the Compute Hour usage for the underlying VM, like Standard_D1_v2.</li> <li>◦ ComputeHR_SW is the premium software charge if the VM is using premium software, like Microsoft R Server.</li> </ul> </li> </ul> | <p>Virtual Machines</p> <pre>{"ImageType":"Canonical","ServiceType":"Standard_DS1_v2","VMName":"","UsageType":"ComputeHR"}</pre> <p>Virtual Machine Scale Sets</p> <pre>{"ImageType":"Canonical","ServiceType":"Standard_DS1_v2","VMName":"myVM1","UsageType":"ComputeHR"}</pre> <p>Premium Software</p> <pre>{"ImageType":"","ServiceType":"Standard_DS1_v2","VMName":"","UsageType":"ComputeHR_SW"}</pre> |

## Image Type

For some images in the Azure gallery, the image type is populated in the Additional Info field. This enables users to understand and track what they have deployed on their Virtual Machine. The following values that are populated in this field based on the image you have deployed:

- BitRock
- Canonical
- FreeBSD
- Open Logic
- Oracle
- SLES for SAP
- SQL Server 14 Preview on Windows Server 2012 R2 Preview
- SUSE
- SUSE Premium
- StorSimple Cloud Appliance
- Red Hat
- Red Hat for SAP Business Applications
- Red Hat for SAP HANA
- Windows Client BYOL
- Windows Server BYOL
- Windows Server Preview

## Service Type

The service type field in the Additional Info field corresponds to the exact VM size you deployed. Premium storage VMs (SSD-based) and non-premium storage VMs (HDD-based) are priced the same. If you deploy an SSD-based size, like Standard\_DS2\_v2, you see the non-SSD size ('Standard\_D2\_v2 VM') in the Meter Sub-Category column and the SSD-size ('Standard\_DS2\_v2') in the Additional Info field.

## Region Names

The region name populated in the Resource Location field in the usage details varies from the region name used in the Azure Resource Manager. Here is a mapping between the region values:

| RESOURCE MANAGER REGION NAME | RESOURCE LOCATION IN USAGE DETAILS |
|------------------------------|------------------------------------|
| australiaeast                | AU East                            |
| australiasoutheast           | AU Southeast                       |
| brazilsouth                  | BR South                           |
| CanadaCentral                | CA Central                         |
| CanadaEast                   | CA East                            |
| CentralIndia                 | IN Central                         |
| centralus                    | Central US                         |

| RESOURCE MANAGER REGION NAME | RESOURCE LOCATION IN USAGE DETAILS |
|------------------------------|------------------------------------|
| chinaeast                    | China East                         |
| chinanorth                   | China North                        |
| eastasia                     | East Asia                          |
| eastus                       | East US                            |
| eastus2                      | East US 2                          |
| GermanyCentral               | DE Central                         |
| GermanyNortheast             | DE Northeast                       |
| japaneast                    | JA East                            |
| japanwest                    | JA West                            |
| KoreaCentral                 | KR Central                         |
| KoreaSouth                   | KR South                           |
| northcentralus               | North Central US                   |
| northeurope                  | North Europe                       |
| southcentralus               | South Central US                   |
| southeastasia                | Southeast Asia                     |
| SouthIndia                   | IN South                           |
| UKNorth                      | US North                           |
| uksouth                      | UK South                           |
| UKSouth2                     | UK South 2                         |
| ukwest                       | UK West                            |
| USDoDCentral                 | US DoD Central                     |
| USDoDEast                    | US DoD East                        |
| USGovArizona                 | USGov Arizona                      |
| usgoviowa                    | USGov Iowa                         |
| USGovTexas                   | USGov Texas                        |

| RESOURCE MANAGER REGION NAME | RESOURCE LOCATION IN USAGE DETAILS |
|------------------------------|------------------------------------|
| usgovvirginia                | USGov Virginia                     |
| westcentralus                | US West Central                    |
| westeurope                   | West Europe                        |
| WestIndia                    | IN West                            |
| westus                       | West US                            |
| westus2                      | US West 2                          |

## Virtual machine usage FAQ

### What resources are charged when deploying a VM?

VMs acquire costs for the VM itself, any premium software running on the VM, the storage account\managed disk associated with the VM, and the networking bandwidth transfers from the VM.

### How can I tell if a VM is using Azure Hybrid Benefit in the Usage CSV?

If you deploy using the [Azure Hybrid Benefit](#), you are charged the Non-Windows VM rate since you are bringing your own license to the cloud. In your bill, you can distinguish which Resource Manager VMs are running Azure Hybrid Benefit because they have either "Windows\_Server BYOL" or "Windows\_Client BYOL" in the ImageType column.

### How are Basic vs. Standard VM Types differentiated in the Usage CSV?

Both Basic and Standard A-Series VMs are offered. If you deploy a Basic VM, in the Meter Sub Category, it has the string "Basic." If you deploy a Standard A-Series VM, then the VM size appears as "A1 VM" since Standard is the default. To learn more about the differences between Basic and Standard, see the [Pricing Page](#).

### What are ExtraSmall, Small, Medium, Large, and ExtraLarge sizes?

ExtraSmall - ExtraLarge are the legacy names for Standard\_A0 – Standard\_A4. In classic VM usage records, you might see this convention used if you have deployed these sizes.

### What is the difference between Meter Region and Resource Location?

The Meter Region is associated with the meter. For some Azure services who use one price for all regions, the Meter Region field could be blank. However, since VMs have dedicated prices per region for Virtual Machines, this field is populated. Similarly, the Resource Location for Virtual Machines is the location where the VM is deployed. The Azure regions in both fields are the same, although they might have a different string convention for the region name.

### Why is the ImageType value blank in the Additional Info field?

The ImageType field is only populated for a subset of images. If you did not deploy one of the images above, the ImageType is blank.

### Why is the VMName blank in the Additional Info?

The VMName is only populated in the Additional Info field for VMs in a scale set. The InstanceID field contains the VM name for non-scale set VMs.

### What does ComputeHR mean in the UsageType field in the Additional Info?

ComputeHR stands for Compute Hour which represents the usage event for the underlying infrastructure cost. If the UsageType is ComputeHR\_SW, the usage event represents the premium software charge for the VM.

## **How do I know if I am charged for premium software?**

When exploring which VM Image best fits your needs, be sure to check out the [Azure Marketplace](#). The image has the software plan rate. If you see "Free" for the rate, there is no additional cost for the software.

## **What is the difference between Microsoft.ClassicCompute and Microsoft.Compute in the Consumed service?**

Microsoft.ClassicCompute represents classic resources deployed via the Azure Service Manager. If you deploy via the Resource Manager, then Microsoft.Compute is populated in the consumed service. Learn more about the [Azure Deployment models](#).

## **Why is the InstanceID field blank for my Virtual Machine usage?**

If you deploy via the classic deployment model, the InstanceID string is not available.

## **Why are the tags for my VMs not flowing to the usage details?**

Tags only flow to you the Usage CSV for Resource Manager VMs only. Classic resource tags are not available in the usage details.

## **How can the consumed quantity be more than 24 hours one day?**

In the Classic model, billing for resources is aggregated at the Cloud Service level. If you have more than one VM in a Cloud Service that uses the same billing meter, your usage is aggregated together. VMs deployed via Resource Manager are billed at the VM level, so this aggregation will not apply.

## **Why is pricing not available for DS/FS/GS/LS sizes on the pricing page?**

Premium storage capable VMs are billed at the same rate as non-premium storage capable VMs. Only your storage costs differ. Visit the [storage pricing page](#) for more information.

## **Next steps**

To learn more about your usage details, see [Understand your bill for Microsoft Azure](#).

# Common Azure CLI commands for managing Azure resources

11/13/2019 • 2 minutes to read • [Edit Online](#)

The Azure CLI allows you to create and manage your Azure resources on macOS, Linux, and Windows. This article details some of the most common commands to create and manage virtual machines (VMs).

This article requires the Azure CLI version 2.0.4 or later. Run `az --version` to find the version. If you need to upgrade, see [Install Azure CLI](#). You can also use [Cloud Shell](#) from your browser.

## Basic Azure Resource Manager commands in Azure CLI

For more detailed help with specific command line switches and options, you can use the online command help and options by typing `az <command> <subcommand> --help`.

### Create VMs

| TASK                    | AZURE CLI COMMANDS                                                                               |
|-------------------------|--------------------------------------------------------------------------------------------------|
| Create a resource group | <code>az group create --name myResourceGroup --location eastus</code>                            |
| Create a Linux VM       | <code>az vm create --resource-group myResourceGroup --name myVM --image ubuntults</code>         |
| Create a Windows VM     | <code>az vm create --resource-group myResourceGroup --name myVM --image win2016datacenter</code> |

### Manage VM state

| TASK            | AZURE CLI COMMANDS                                                         |
|-----------------|----------------------------------------------------------------------------|
| Start a VM      | <code>az vm start --resource-group myResourceGroup --name myVM</code>      |
| Stop a VM       | <code>az vm stop --resource-group myResourceGroup --name myVM</code>       |
| Deallocate a VM | <code>az vm deallocate --resource-group myResourceGroup --name myVM</code> |
| Restart a VM    | <code>az vm restart --resource-group myResourceGroup --name myVM</code>    |
| Redeploy a VM   | <code>az vm redeploy --resource-group myResourceGroup --name myVM</code>   |
| Delete a VM     | <code>az vm delete --resource-group myResourceGroup --name myVM</code>     |

### Get VM info

| TASK                       | AZURE CLI COMMANDS                                                   |
|----------------------------|----------------------------------------------------------------------|
| List VMs                   | <code>az vm list</code>                                              |
| Get information about a VM | <code>az vm show --resource-group myResourceGroup --name myVM</code> |
| Get usage of VM resources  | <code>az vm list-usage --location eastus</code>                      |
| Get all available VM sizes | <code>az vm list-sizes --location eastus</code>                      |

## Disks and images

| TASK                         | AZURE CLI COMMANDS                                                                                                   |
|------------------------------|----------------------------------------------------------------------------------------------------------------------|
| Add a data disk to a VM      | <code>az vm disk attach --resource-group myResourceGroup --vm-name myVM --disk myDataDisk --size-gb 128 --new</code> |
| Remove a data disk from a VM | <code>az vm disk detach --resource-group myResourceGroup --vm-name myVM --disk myDataDisk</code>                     |
| Resize a disk                | <code>az disk update --resource-group myResourceGroup --name myDataDisk --size-gb 256</code>                         |
| Snapshot a disk              | <code>az snapshot create --resource-group myResourceGroup --name mySnapshot --source myDataDisk</code>               |
| Create image of a VM         | <code>az image create --resource-group myResourceGroup --source myVM --name myImage</code>                           |
| Create VM from image         | <code>az vm create --resource-group myResourceGroup --name myNewVM --image myImage</code>                            |

## Next steps

For additional examples of the CLI commands, see the [Create and Manage Linux VMs with the Azure CLI](#) tutorial.

# Resize a Linux virtual machine using Azure CLI

11/13/2019 • 2 minutes to read • [Edit Online](#)

After you provision a virtual machine (VM), you can scale the VM up or down by changing the [VM size](#). In some cases, you must deallocate the VM first. You need to deallocate the VM if the desired size is not available on the hardware cluster that is hosting the VM. This article details how to resize a Linux VM with the Azure CLI.

## Resize a VM

To resize a VM, you need the latest [Azure CLI](#) installed and logged in to an Azure account using [az login](#).

1. View the list of available VM sizes on the hardware cluster where the VM is hosted with [az vm list-vm-resize-options](#). The following example lists VM sizes for the VM named `myVM` in the resource group `myResourceGroup` region:

```
az vm list-vm-resize-options --resource-group myResourceGroup --name myVM --output table
```

2. If the desired VM size is listed, resize the VM with [az vm resize](#). The following example resizes the VM named `myVM` to the `Standard_DS3_v2` size:

```
az vm resize --resource-group myResourceGroup --name myVM --size Standard_DS3_v2
```

The VM restarts during this process. After the restart, your existing OS and data disks are remapped. Anything on the temporary disk is lost.

3. If the desired VM size is not listed, you need to first deallocate the VM with [az vm deallocate](#). This process allows the VM to then be resized to any size available that the region supports and then started. The following steps deallocate, resize, and then start the VM named `myVM` in the resource group named `myResourceGroup`:

```
az vm deallocate --resource-group myResourceGroup --name myVM
az vm resize --resource-group myResourceGroup --name myVM --size Standard_DS3_v2
az vm start --resource-group myResourceGroup --name myVM
```

### WARNING

Deallocating the VM also releases any dynamic IP addresses assigned to the VM. The OS and data disks are not affected.

## Next steps

For additional scalability, run multiple VM instances and scale out. For more information, see [Automatically scale Linux machines in a Virtual Machine Scale Set](#).

# Change the OS disk used by an Azure VM using the CLI

11/13/2019 • 2 minutes to read • [Edit Online](#)

If you have an existing VM, but you want to swap the disk for a backup disk or another OS disk, you can use the Azure CLI to swap the OS disks. You don't have to delete and recreate the VM. You can even use a managed disk in another resource group, as long as it isn't already in use.

The VM does need to be stopped\deallocated, then the resource ID of the managed disk can be replaced with the resource ID of a different managed disk.

Make sure that the VM size and storage type are compatible with the disk you want to attach. For example, if the disk you want to use is in Premium Storage, then the VM needs to be capable of Premium Storage (like a DS-series size).

This article requires Azure CLI version 2.0.25 or greater. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Use [az disk list](#) to get a list of the disks in your resource group.

```
az disk list \
 -g myResourceGroupDisk \
 --query '[*].{diskId:id}' \
 --output table
```

Use [az vm stop](#) to stop\deallocate the VM before swapping the disks.

```
az vm stop \
 -n myVM \
 -g myResourceGroup
```

Use [az vm update](#) with the full resource ID of the new disk for the `--osdisk` parameter

```
az vm update \
 -g myResourceGroup \
 -n myVM \
 --os-disk /subscriptions/<subscription ID>/resourceGroups/swap/providers/Microsoft.Compute/disks/myDisk
```

Restart the VM using [az vm start](#).

```
az vm start \
 -n myVM \
 -g myResourceGroup
```

## Next steps

To create a copy of a disk, see [Snapshot a disk](#).

# Time sync for Linux VMs in Azure

11/26/2019 • 6 minutes to read • [Edit Online](#)

Time sync is important for security and event correlation. Sometimes it is used for distributed transactions implementation. Time accuracy between multiple computer systems is achieved through synchronization. Synchronization can be affected by multiple things, including reboots and network traffic between the time source and the computer fetching the time.

Azure is backed by infrastructure running Windows Server 2016. Windows Server 2016 has improved algorithms used to correct time and condition the local clock to synchronize with UTC. The Windows Server 2016 Accurate Time feature greatly improved how the VMCTimeSync service that governs VMs with the host for accurate time. Improvements include more accurate initial time on VM start or VM restore and interrupt latency correction.

## NOTE

For a quick overview of Windows Time service, take a look at this [high-level overview video](#).

For more information, see [Accurate time for Windows Server 2016](#).

## Overview

Accuracy for a computer clock is gauged on how close the computer clock is to the Coordinated Universal Time (UTC) time standard. UTC is defined by a multinational sample of precise atomic clocks that can only be off by one second in 300 years. But, reading UTC directly requires specialized hardware. Instead, time servers are synced to UTC and are accessed from other computers to provide scalability and robustness. Every computer has time synchronization service running that knows what time servers to use and periodically checks if computer clock needs to be corrected and adjusts time if needed.

Azure hosts are synchronized to internal Microsoft time servers that take their time from Microsoft-owned Stratum 1 devices, with GPS antennas. Virtual machines in Azure can either depend on their host to pass the accurate time (*host time*) on to the VM or the VM can directly get time from a time server, or a combination of both.

On stand-alone hardware, the Linux OS only reads the host hardware clock on boot. After that, the clock is maintained using the interrupt timer in the Linux kernel. In this configuration, the clock will drift over time. In newer Linux distributions on Azure, VMs can use the VMCTimeSync provider, included in the Linux integration services (LIS), to query for clock updates from the host more frequently.

Virtual machine interactions with the host can also affect the clock. During [memory preserving maintenance](#), VMs are paused for up to 30 seconds. For example, before maintenance begins the VM clock shows 10:00:00 AM and lasts 28 seconds. After the VM resumes, the clock on the VM would still show 10:00:00 AM, which would be 28 seconds off. To correct for this, the VMCTimeSync service monitors what is happening on the host and prompts for changes to happen on the VMs to compensate.

Without time synchronization working, the clock on the VM would accumulate errors. When there is only one VM, the effect might not be significant unless the workload requires highly accurate timekeeping. But in most cases, we have multiple, interconnected VMs that use time to track transactions and the time needs to be consistent throughout the entire deployment. When time between VMs is different, you could see the following effects:

- Authentication will fail. Security protocols like Kerberos or certificate-dependent technology rely on time being consistent across the systems.
- It's very hard to figure out what has happened in a system if logs (or other data) don't agree on time. The same

event would look like it occurred at different times, making correlation difficult.

- If clock is off, the billing could be calculated incorrectly.

## Configuration options

There are generally three ways to configure time sync for your Linux VMs hosted in Azure:

- The default configuration for Azure Marketplace images uses both NTP time and VMICTimeSync host-time.
- Host-only using VMICTimeSync.
- Use another, external time server with or without using VMICTimeSync host-time.

### Use the default

By default, most Azure Marketplace images for Linux are configured to sync from two sources:

- NTP as primary, which gets time from an NTP server. For example, Ubuntu 16.04 LTS Marketplace images use [ntp.ubuntu.com](http://ntp.ubuntu.com).
- The VMICTimeSync service as secondary, used to communicate the host time to the VMs and make corrections after the VM is paused for maintenance. Azure hosts use Microsoft-owned Stratum 1 devices to keep accurate time.

In newer Linux distributions, the VMICTimeSync service uses the precision time protocol (PTP), but earlier distributions may not support PTP and will fall-back to NTP for getting time from the host.

To confirm NTP is synchronizing correctly, run the `ntpq -p` command.

### Host-only

Because NTP servers like time.windows.com and ntp.ubuntu.com are public, syncing time with them requires sending traffic over the internet. Varying packet delays can negatively affect quality of the time sync. Removing NTP by switching to host-only sync can sometimes improve your time sync results.

Switching to host-only time sync makes sense if you experience time sync issues using the default configuration. Try out the host-only sync to see if that would improve the time sync on your VM.

### External time server

If you have specific time sync requirements, there is also an option of using external time servers. External time servers can provide specific time, which can be useful for test scenarios, ensuring time uniformity with machines hosted in non-Microsoft datacenters, or handling leap seconds in a special way.

You can combine an external time server with the VMICTimeSync service to provide results similar to the default configuration. Combining an external time server with VMICTimeSync is the best option for dealing with issues that can be caused when VMs are paused for maintenance.

## Tools and resources

There are some basic commands for checking your time synchronization configuration. Documentation for Linux distribution will have more details on the best way to configure time synchronization for that distribution.

### Integration services

Check to see if the integration service (hv\_utils) is loaded.

```
lsmod | grep hv_utils
```

You should see something similar to this:

```
hv_utils 24418 0
hv_vmbus 397185 7 hv_balloon,hyperv_keyboard,hv_netvsc,hid_hyperv,hv_utils,hyperv_fb,hv_storvsc
```

See if the Hyper-V integration services daemon is running.

```
ps -ef | grep hv
```

You should see something similar to this:

```
root 229 2 0 17:52 ? 00:00:00 [hv_vmbus_con]
root 391 2 0 17:52 ? 00:00:00 [hv_balloon]
```

## Check for PTP

With newer versions of Linux, a Precision Time Protocol (PTP) clock source is available as part of the VMICTimeSync provider. On older versions of Red Hat Enterprise Linux or CentOS 7.x the [Linux Integration Services](#) can be downloaded and used to install the updated driver. When using PTP, the Linux device will be of the form /dev/ptpx.

See which PTP clock sources are available.

```
ls /sys/class/ptp
```

In this example, the value returned is *ptp0*, so we use that to check the clock name. To verify the device, check the clock name.

```
cat /sys/class/ptp/ptp0/clock_name
```

This should return **hyperv**.

## chrony

On Red Hat Enterprise Linux and CentOS 7.x, [chrony](#) configured to use a PTP source clock. The Network Time Protocol daemon (*ntpd*) doesn't support PTP sources, so using **chrony** is recommended. To enable PTP, update **chrony.conf**.

```
refclock PHC /dev/ptp0 poll 3 dpoll -2 offset 0
```

For more information on Red Hat and NTP, see [Configure NTP](#).

For more information on chrony, see [Using chrony](#).

If both chrony and TimeSync sources are enabled simultaneously, you can mark one as **prefer** which sets the other source as a backup. Because NTP services do not update the clock for large skews except after a long period, the VMICTimeSync will recover the clock from paused VM events far more quickly than NTP-based tools alone.

By default chrony accelerates or slows the system clock to fix any time drift. If the drift becomes too big, chrony will fail to fix the drift. To overcome this the `makestep` parameter in **/etc/chrony.conf** can be changed to force a timesync if the drift exceeds the threshold specified.

```
makestep 1.0 -1
```

Here, chrony will force a time update if the drift is greater than 1 second. To apply the changes restart the chronyd

service.

```
systemctl restart chronyd
```

## systemd

On Ubuntu and SUSE time sync is configured using [systemd](#). For more information on Ubuntu, see [Time Synchronization](#). For more information on SUSE, see Section 4.5.8 in [SUSE Linux Enterprise Server 12 SP3 Release Notes](#).

## Next steps

For more information, see [Accurate time for Windows Server 2016](#).

# How to tag a Linux virtual machine in Azure

2/25/2020 • 2 minutes to read • [Edit Online](#)

This article describes different ways to tag a Linux virtual machine in Azure through the Resource Manager deployment model. Tags are user-defined key/value pairs which can be placed directly on a resource or a resource group. Azure currently supports up to 50 tags per resource and resource group. Tags may be placed on a resource at the time of creation or added to an existing resource. Please note, tags are supported for resources created via the Resource Manager deployment model only.

## Tagging a Virtual Machine through Templates

First, let's look at tagging through templates. [This template](#) places tags on the following resources: Compute (Virtual Machine), Storage (Storage Account), and Network (Public IP Address, Virtual Network, and Network Interface). This template is for a Windows VM but can be adapted for Linux VMs.

Click the **Deploy to Azure** button from the [template link](#). This will navigate to the [Azure portal](#) where you can deploy this template.

### Simple deployment of a VM with Tags

 Deploy to Azure

 Visualize

This template includes the following tags: *Department*, *Application*, and *Created By*. You can add/edit these tags directly in the template if you would like different tag names.

```
"apiVersion": "2015-05-01-preview",
"type": "Microsoft.Compute/virtualMachines",
"name": "[variables('vmName')]",
"location": "[variables('location')]",
"tags": {
 "Department": "[parameters('departmentName')]",
 "Application": "[parameters('applicationName')]",
 "Created By": "[parameters('createdBy')]"
},
```

As you can see, the tags are defined as key/value pairs, separated by a colon (:). The tags must be defined in this format:

```
"tags": {
 "Key1" : "Value1",
 "Key2" : "Value2"
}
```

Save the template file after you finish editing it with the tags of your choice.

Next, in the **Edit Parameters** section, you can fill out the values for your tags.

DEPARTMENTNAME (string) ⓘ

APPLICATIONNAME (string) ⓘ

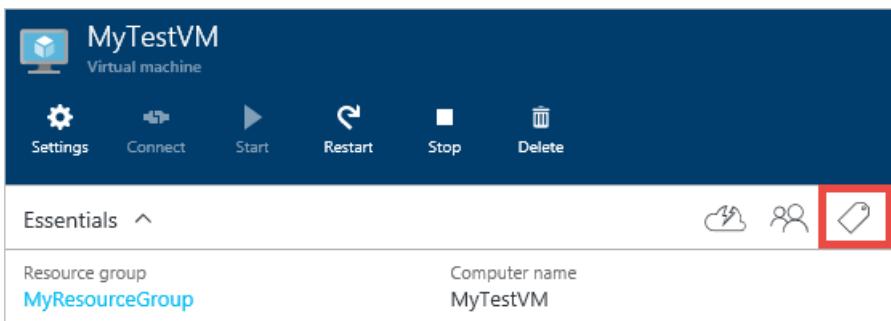
CREATEDBY (string) ⓘ

Click **Create** to deploy this template with your tag values.

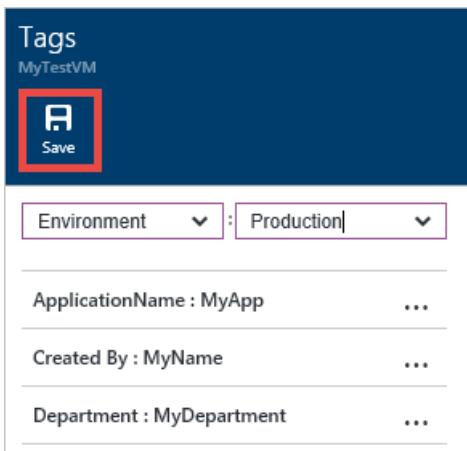
## Tagging through the Portal

After creating your resources with tags, you can view, add, and delete tags in the portal.

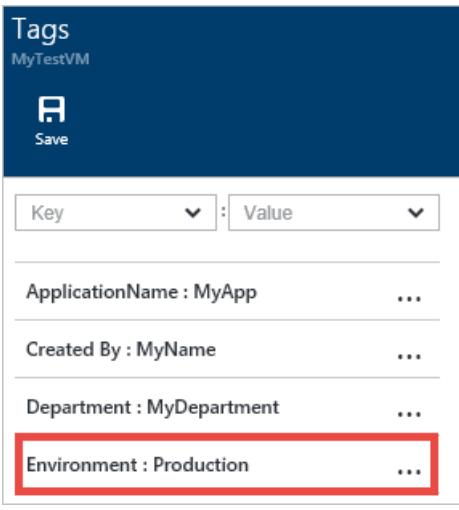
Select the tags icon to view your tags:



Add a new tag through the portal by defining your own Key/Value pair, and save it.



Your new tag should now appear in the list of tags for your resource.



## Tagging with Azure CLI

To begin, you need the latest [Azure CLI](#) installed and logged in to an Azure account using `az login`.

You can view all properties for a given Virtual Machine, including the tags, using this command:

```
az vm show --resource-group MyResourceGroup --name MyTestVM
```

To add a new VM tag through the Azure CLI, you can use the `azure vm update` command along with the tag parameter `--set`:

```
az vm update \
--resource-group MyResourceGroup \
--name MyTestVM \
--set tags.myNewTagName1=myNewTagValue1 tags.myNewTagName2=myNewTagValue2
```

To remove tags, you can use the `--remove` parameter in the `azure vm update` command.

```
az vm update --resource-group MyResourceGroup --name MyTestVM --remove tags.myNewTagName1
```

Now that we have applied tags to our resources Azure CLI and the Portal, let's take a look at the usage details to see the tags in the billing portal.

## Viewing your tags in the usage details

Tags placed on Compute, Network, and Storage resources in the Resource Manager deployment model will be populated in your usage details in the [billing portal](#).

Click on **Download usage details** to view the usage details in your subscription.

**NEXT BILL (ESTIMATED):**

# \$0.00

**DATE PURCHASED**  
6/24/2014

**CURRENT BILLING PERIOD**  
5/24/2015 - 6/23/2015

[!\[\]\(718e209524af206d6883fab35359a964\_img.jpg\) Download usage details](#)

- [!\[\]\(3802c207154fa8dca052af9a57e4891b\_img.jpg\) Contact Microsoft Support](#)
- [!\[\]\(e2dbd002128049de21b5a4dae925a8b9\_img.jpg\) Edit subscription details](#)
- [!\[\]\(c23b2f74bc8235fd52569f8978628283\_img.jpg\) Change subscription address](#)
- [!\[\]\(8b644050a5a3087fdbd23ff97b6ffe20\_img.jpg\) Partner Information](#)
- [!\[\]\(ca58b3d1bbc08fc4324e731e28f6e611\_img.jpg\) Cancel Subscription](#)

Select your billing statement and the **Version 2** usage details:

Click here to [Understand Your Bill](#).

| Current period        | <a href="#">View Current Statement</a> | <a href="#">Download Usage</a>      | ▼                         |
|-----------------------|----------------------------------------|-------------------------------------|---------------------------|
| 7/24/2014 - 8/23/2014 |                                        | <a href="#">Version 2 - Preview</a> |                           |
|                       |                                        | <a href="#">Download Usage</a>      | <a href="#">Version 1</a> |

From the usage details, you can see all of the tags in the **Tags** column:

| Consumed Service    | Resource Group    | Instance Id                                                                                                                                       | Tags                                                                                                                                                       |
|---------------------|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| "Microsoft.Compute" | "MYRESOURCEGROUP" | "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/MYRESOURCEGROUP/providers/Microsoft.Compute/virtualMachines/MyWindowsVM"      | "[{"Department":"MyDepartment","Application":"MyApp1","Created By":"MyName","Type":"Virtual Machine","Environment":"Production","Location":"MyLocation"}]" |
| "Microsoft.Storage" | "myresourcegroup" | "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/myresourcegroup/providers/Microsoft.Storage/storageAccounts/mystorageaccount" | "[{"Application":"MyApp1","Created By":"MyName","Department":"MyDepartment","Type":"Storage Account"}]"                                                    |
| "Microsoft.Network" | "MyResourceGroup" | "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/MyResourceGroup/providers/Microsoft.Network/publicIPAddresses/myPublicIP"     | "[{"Department":"MyDepartment","Application":"MyApp1","Created By":"MyName","Type":"Public IP"}]"                                                          |

By analyzing these tags along with usage, organizations will be able to gain new insights into their consumption data.

## Next steps

- To learn more about tagging your Azure resources, see [Azure Resource Manager Overview](#) and [Using Tags to organize your Azure Resources](#).
- To see how tags can help you manage your use of Azure resources, see [Understanding your Azure Bill](#) and [Gain insights into your Microsoft Azure resource consumption](#).

# Run scripts in your Linux VM

6/28/2019 • 2 minutes to read • [Edit Online](#)

To automate tasks or troubleshoot issues, you may need to run commands in a VM. The following article gives a brief overview of the features that are available to run scripts and commands within your VMs.

## Custom Script Extension

The [Custom Script Extension](#) is primarily used for post deployment configuration and software installation.

- Download and run scripts in Azure virtual machines.
- Can be run using Azure Resource Manager templates, Azure CLI, REST API, PowerShell, or Azure portal.
- Script files can be downloaded from Azure storage or GitHub, or provided from your PC when run from the Azure portal.
- Run PowerShell script in Windows machines and Bash script in Linux machines.
- Useful for post deployment configuration, software installation, and other configuration or management tasks.

## Run command

The [Run Command](#) feature enables virtual machine and application management and troubleshooting using scripts, and is available even when the machine is not reachable, for example if the guest firewall doesn't have the RDP or SSH port open.

- Run scripts in Azure virtual machines.
- Can be run using [Azure portal](#), [REST API](#), [Azure CLI](#), or [PowerShell](#)
- Quickly run a script and view output and repeat as needed in the Azure portal.
- Script can be typed directly or you can run one of the built-in scripts.
- Run PowerShell script in Windows machines and Bash script in Linux machines.
- Useful for virtual machine and application management and for running scripts in virtual machines that are unreachable.

## Hybrid Runbook Worker

The [Hybrid Runbook Worker](#) provides general machine, application, and environment management with user's custom scripts stored in an Automation account.

- Run scripts in Azure and non-Azure machines.
- Can be run using Azure portal, Azure CLI, REST API, PowerShell, webhook.
- Scripts stored and managed in an Automation Account.
- Run PowerShell, PowerShell Workflow, Python, or Graphical runbooks
- No time limit on script run time.
- Multiple scripts can run concurrently.
- Full script output is returned and stored.
- Job history available for 90 days.
- Scripts can run as Local System or with user-supplied credentials.
- Requires [manual installation](#)

## Serial console

The [Serial console](#) provides direct access to a VM, similar to having a keyboard connected to the VM.

- Run commands in Azure virtual machines.
- Can be run using a text-based console to the machine in the Azure portal.
- Login to the machine with a local user account.
- Useful when access to the virtual machine is needed regardless of the machine's network or operating system state.

## Next steps

Learn more about the different features that are available to run scripts and commands within your VMs.

- [Custom Script Extension](#)
- [Run Command](#)
- [Hybrid Runbook Worker](#)
- [Serial console](#)

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

1/16/2020 • 12 minutes to read • [Edit Online](#)

The Custom Script Extension Version 2 downloads and runs scripts on Azure virtual machines. This extension is useful for post-deployment configuration, software installation, or any other configuration/management task. You can download scripts from Azure Storage or another accessible internet location, or you can provide them to the extension runtime.

The Custom Script Extension integrates with Azure Resource Manager templates. You can also run it by using Azure CLI, PowerShell, or the Azure Virtual Machines REST API.

This article details how to use the Custom Script Extension from Azure CLI, and how to run the extension by using an Azure Resource Manager template. This article also provides troubleshooting steps for Linux systems.

There are two Linux Custom Script Extensions:

- Version 1 - Microsoft.OSTCExtensions.CustomScriptForLinux
- Version 2 - Microsoft.Azure.Extensions.CustomScript

Please switch new and existing deployments to use the new version 2 instead. The new version is intended to be a drop-in replacement. Therefore, the migration is as easy as changing the name and version, you do not need to change your extension configuration.

## Operating System

The Custom Script Extension for Linux will run on the extension supported extension OS's, for more information, see this [article](#).

## Script Location

You can use the extension to use your Azure Blob storage credentials, to access Azure Blob storage. Alternatively, the script location can be any where, as long as the VM can route to that end point, such as GitHub, internal file server etc.

## Internet Connectivity

If you need to download a script externally such as GitHub or Azure Storage, then additional firewall/Network Security Group ports need to be opened. For example if your script is located in Azure Storage, you can allow access using Azure NSG Service Tags for [Storage](#).

If your script is on a local server, then you may still need additional firewall/Network Security Group ports need to be opened.

## Tips and Tricks

- The highest failure rate for this extension is due to syntax errors in the script, test the script runs without error, and also put in additional logging into the script to make it easier to find where it failed.
- Write scripts that are idempotent, so if they get run again more than once accidentally, it will not cause system changes.
- Ensure the scripts do not require user input when they run.
- There is 90 mins allowed for the script to run, anything longer will result in a failed provision of the extension.
- Do not put reboots inside the script, this will cause issues with other extensions that are being installed, and post reboot, the extension will not continue after the restart.

- If you have a script that will cause a reboot, then install applications and run scripts etc. You should schedule the reboot using a Cron job, or using tools such as DSC, or Chef, Puppet extensions.
- The extension will only run a script once, if you want to run a script on every boot, then you can use [cloud-init image](#) and use a [Scripts Per Boot](#) module. Alternatively, you can use the script to create a SystemD service unit.
- If you want to schedule when a script will run, you should use the extension to create a Cron job.
- When the script is running, you will only see a 'transitioning' extension status from the Azure portal or CLI. If you want more frequent status updates of a running script, you will need to create your own solution.
- Custom Script extension does not natively support proxy servers, however you can use a file transfer tool that supports proxy servers within your script, such as *Curl*.
- Be aware of non default directory locations that your scripts or commands may rely on, have logic to handle this.
- When deploying custom script to production VMSS instances it is suggested to deploy via json template and store your script storage account where you have control over the SAS token.

## Extension schema

The Custom Script Extension configuration specifies things like script location and the command to be run. You can store this configuration in configuration files, specify it on the command line, or specify it in an Azure Resource Manager template.

You can store sensitive data in a protected configuration, which is encrypted and only decrypted inside the virtual machine. The protected configuration is useful when the execution command includes secrets such as a password.

These items should be treated as sensitive data and specified in the extensions protected setting configuration. Azure VM extension protected setting data is encrypted, and only decrypted on the target virtual machine.

```
{
 "name": "config-app",
 "type": "Extensions",
 "location": "[resourceGroup().location]",
 "apiVersion": "2019-03-01",
 "dependsOn": [
 "[concat('Microsoft.Compute/virtualMachines/', concat(variables('vmName'),copyindex()))]"
],
 "tags": {
 "displayName": "config-app"
 },
 "properties": {
 "publisher": "Microsoft.Azure.Extensions",
 "type": "CustomScript",
 "typeHandlerVersion": "2.1",
 "autoUpgradeMinorVersion": true,
 "settings": {
 "skipDOS2Unix":false,
 "timestamp":123456789
 },
 "protectedSettings": {
 "commandToExecute": "<command-to-execute>",
 "script": "<base64-script-to-execute>",
 "storageAccountName": "<storage-account-name>",
 "storageAccountKey": "<storage-account-key>",
 "fileUris": ["https://.."],
 "managedIdentity" : "<managed-identity-identifier>"
 }
 }
}
```

**NOTE**

managedIdentity property **must not** be used in conjunction with storageAccountName or storageAccountKey properties

**Property values**

| NAME                      | VALUE / EXAMPLE                                                                                                             | DATA TYPE      |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------|----------------|
| apiVersion                | 2019-03-01                                                                                                                  | date           |
| publisher                 | Microsoft.Compute.Extensions                                                                                                | string         |
| type                      | CustomScript                                                                                                                | string         |
| typeHandlerVersion        | 2.1                                                                                                                         | int            |
| fileUris (e.g.)           | <a href="https://github.com/MyProject/Archive/MyPythonScript.py">https://github.com/MyProject/Archive/MyPythonScript.py</a> | array          |
| commandToExecute (e.g.)   | python MyPythonScript.py <my-param1>                                                                                        | string         |
| script                    | lyEvYmluL3NoCmVjaG8gIlVwZGF0aW5nIHBlY2thZ2VzIC4uLiKYXB0IHVwZGF0ZQphcHQgdXBncmFkZSAteQo=                                     | string         |
| skipDos2Unix (e.g.)       | false                                                                                                                       | boolean        |
| timestamp (e.g.)          | 123456789                                                                                                                   | 32-bit integer |
| storageAccountName (e.g.) | examplestorageacct                                                                                                          | string         |
| storageAccountKey (e.g.)  | TmJK/1N3AbAZ3q/+hOXoi/I73zOqsaxX Dhqa9Y83/v5UpXQp2DQIBuv2Tifp60cE /OaHsJzmQZ7teQfczQj8hg==                                  | string         |
| managedIdentity (e.g.)    | { } or { "clientId": "31b403aa-c364-4240-a7ff-d85fb6cd7232" } or { "objectId": "12dd289c-0583-46e5-b9b4-115d5c19ef4b" }     | json object    |

**Property value details**

- `apiVersion` : The most up to date apiVersion can be found using [Resource Explorer](#) or from Azure CLI using the following command `az provider list -o json`
- `skipDos2Unix` : (optional, boolean) skip dos2unix conversion of script-based file URLs or script.
- `timestamp` (optional, 32-bit integer) use this field only to trigger a re-run of the script by changing value of this field. Any integer value is acceptable; it must only be different than the previous value.
  - `commandToExecute` : (**required** if script not set, string) the entry point script to execute. Use this field instead if your command contains secrets such as passwords.
- `script` : (**required** if commandToExecute not set, string)a base64 encoded (and optionally gzip'ed) script executed by /bin/sh.
- `fileUris` : (optional, string array) the URLs for file(s) to be downloaded.
- `storageAccountName` : (optional, string) the name of storage account. If you specify storage credentials, all

- `fileUris` must be URLs for Azure Blobs.
- `storageAccountKey` : (optional, string) the access key of storage account
- `managedIdentity` : (optional, json object) the [managed identity](#) for downloading file(s)
  - `clientId` : (optional, string) the client ID of the managed identity
  - `objectId` : (optional, string) the object ID of the managed identity

The following values can be set in either public or protected settings, the extension will reject any configuration where the values below are set in both public and protected settings.

- `commandToExecute`
- `script`
- `fileUris`

Using public settings maybe useful for debugging, but it is strongly recommended that you use protected settings.

Public settings are sent in clear text to the VM where the script will be executed. Protected settings are encrypted using a key known only to the Azure and the VM. The settings are saved to the VM as they were sent, i.e. if the settings were encrypted they are saved encrypted on the VM. The certificate used to decrypt the encrypted values is stored on the VM, and used to decrypt settings (if necessary) at runtime.

#### **Property: skipDos2Unix**

The default value is false, which means dos2unix conversion **is** executed.

The previous version of CustomScript, Microsoft.OSTCExtensions.CustomScriptForLinux, would automatically convert DOS files to UNIX files by translating `\r\n` to `\n`. This translation still exists, and is on by default. This conversion is applied to all files downloaded from `fileUris` or the `script` setting based on any of the following criteria.

- If the extension is one of `.sh`, `.txt`, `.py`, or `.pl` it will be converted. The `script` setting will always match this criteria because it is assumed to be a script executed with `/bin/sh`, and is saved as `script.sh` on the VM.
- If the file starts with `#!`.

The dos2unix conversion can be skipped by setting the `skipDos2Unix` to true.

```
{
 "fileUris": ["<url>"],
 "commandToExecute": "<command-to-execute>",
 "skipDos2Unix": true
}
```

#### **Property: script**

CustomScript supports execution of a user-defined script. The script settings to combine `commandToExecute` and `fileUris` into a single setting. Instead of the having to setup a file for download from Azure storage or GitHub gist, you can simply encode the script as a setting. Script can be used to replaced `commandToExecute` and `fileUris`.

The script **must** be base64 encoded. The script can **optionally** be gzip'ed. The script setting can be used in public or protected settings. The maximum size of the script parameter's data is 256 KB. If the script exceeds this size it will not be executed.

For example, given the following script saved to the file `/script.sh`.

```
#!/bin/sh
echo "Updating packages ..."
apt update
apt upgrade -y
```

The correct CustomScript script setting would be constructed by taking the output of the following command.

```
cat script.sh | base64 -w0
```

```
{
 "script": "IyEvYmluL3NoCmVjaG8gIlVwZGF0aW5nIHBhY2thZ2VzIC4uLiIKYXB0IHVwZGF0ZQphcHQgdXBncmFkZSAtE0o="
}
```

The script can optionally be gzip'ed to further reduce size (in most cases). (CustomScript auto-detects the use of gzip compression.)

```
cat script | gzip -9 | base64 -w 0
```

CustomScript uses the following algorithm to execute a script.

1. assert the length of the script's value does not exceed 256 KB.
2. base64 decode the script's value
3. *attempt* to gunzip the base64 decoded value
4. write the decoded (and optionally decompressed) value to disk (/var/lib/waagent/custom-script/#/script.sh)
5. execute the script using \_/bin/sh -c /var/lib/waagent/custom-script/#/script.sh.

#### Property: managedIdentity

CustomScript (version 2.1 onwards) supports [managed identity](#) for downloading file(s) from URLs provided in the "fileUris" setting. It allows CustomScript to access Azure Storage private blobs or containers without the user having to pass secrets like SAS tokens or storage account keys.

To use this feature, the user must add a [system-assigned](#) or [user-assigned](#) identity to the VM or VMSS where CustomScript is expected to run, and [grant the managed identity access to the Azure Storage container or blob](#).

To use the system-assigned identity on the target VM/VMSS, set "managedidentity" field to an empty json object.

Example:

```
{
 "fileUris": ["https://mystorage.blob.core.windows.net/privatecontainer/script1.sh"],
 "commandToExecute": "sh script1.sh",
 "managedIdentity" : {}
}
```

To use the user-assigned identity on the target VM/VMSS, configure "managedidentity" field with the client ID or the object ID of the managed identity.

Examples:

```
{
 "fileUris": ["https://mystorage.blob.core.windows.net/privatecontainer/script1.sh"],
 "commandToExecute": "sh script1.sh",
 "managedIdentity" : { "clientId": "31b403aa-c364-4240-a7ff-d85fb6cd7232" }
}
```

```
{
 "fileUris": ["https://mystorage.blob.core.windows.net/privatecontainer/script1.sh"],
 "commandToExecute": "sh script1.sh",
 "managedIdentity" : { "objectId": "12dd289c-0583-46e5-b9b4-115d5c19ef4b" }
}
```

#### NOTE

managedIdentity property **must not** be used in conjunction with storageAccountName or storageAccountKey properties

## Template deployment

Azure VM extensions can be deployed with Azure Resource Manager templates. The JSON schema detailed in the previous section can be used in an Azure Resource Manager template to run the Custom Script Extension during an Azure Resource Manager template deployment. A sample template that includes the Custom Script Extension can be found here, [GitHub](#).

```
{
 "name": "config-app",
 "type": "extensions",
 "location": "[resourceGroup().location]",
 "apiVersion": "2019-03-01",
 "dependsOn": [
 "[concat('Microsoft.Compute/virtualMachines/', concat(variables('vmName'),copyindex()))]"
],
 "tags": {
 "displayName": "config-app"
 },
 "properties": {
 "publisher": "Microsoft.Azure.Extensions",
 "type": "CustomScript",
 "typeHandlerVersion": "2.1",
 "autoUpgradeMinorVersion": true,
 "settings": {
 },
 "protectedSettings": {
 "commandToExecute": "sh hello.sh <param2>",
 "fileUris": ["https://github.com/MyProject/Archive/hello.sh"]
 }
 }
}
```

#### NOTE

These property names are case-sensitive. To avoid deployment problems, use the names as shown here.

## Azure CLI

When you're using Azure CLI to run the Custom Script Extension, create a configuration file or files. At a minimum, you must have 'commandToExecute'.

```
az vm extension set \
--resource-group myResourceGroup \
--vm-name myVM --name customScript \
--publisher Microsoft.Azure.Extensions \
--protected-settings ./script-config.json
```

Optionally, you can specify the settings in the command as a JSON formatted string. This allows the configuration to be specified during execution and without a separate configuration file.

```
az vm extension set \
--resource-group exttest \
--vm-name exttest \
--name customScript \
--publisher Microsoft.Azure.Extensions \
--protected-settings '{"fileUris": ["https://raw.githubusercontent.com/Microsoft/dotnet-core-sample-templates/master/dotnet-core-music-linux/scripts/config-music.sh"], "commandToExecute": "./config-music.sh"}'
```

## Azure CLI examples

### Public configuration with script file

```
{
 "fileUris": ["https://raw.githubusercontent.com/Microsoft/dotnet-core-sample-templates/master/dotnet-core-music-linux/scripts/config-music.sh"],
 "commandToExecute": "./config-music.sh"
}
```

Azure CLI command:

```
az vm extension set \
--resource-group myResourceGroup \
--vm-name myVM --name customScript \
--publisher Microsoft.Azure.Extensions \
--settings ./script-config.json
```

### Public configuration with no script file

```
{
 "commandToExecute": "apt-get -y update && apt-get install -y apache2"
}
```

Azure CLI command:

```
az vm extension set \
--resource-group myResourceGroup \
--vm-name myVM --name customScript \
--publisher Microsoft.Azure.Extensions \
--settings ./script-config.json
```

### Public and protected configuration files

You use a public configuration file to specify the script file URI. You use a protected configuration file to specify the command to be run.

Public configuration file:

```
{
 "fileUris": ["https://raw.githubusercontent.com/Microsoft/dotnet-core-sample-templates/master/dotnet-core-music-linux/scripts/config-music.sh"]
}
```

Protected configuration file:

```
{
 "commandToExecute": "./config-music.sh <param1>"
}
```

Azure CLI command:

```
az vm extension set \
 --resource-group myResourceGroup \
 --vm-name myVM \
 --name customScript \
 --publisher Microsoft.Azure.Extensions \
 --settings ./script-config.json \
 --protected-settings ./protected-config.json
```

## Troubleshooting

When the Custom Script Extension runs, the script is created or downloaded into a directory that's similar to the following example. The command output is also saved into this directory in `stdout` and `stderr` files.

```
/var/lib/waagent/custom-script/download/0/
```

To troubleshoot, first check the Linux Agent Log, ensure the extension ran, check:

```
/var/log/waagent.log
```

You should look for the extension execution, it will look something like:

```
2018/04/26 17:47:22.110231 INFO [Microsoft.Azure.Extensions.customScript-2.0.6] [Enable] current handler state
is: notinstalled
2018/04/26 17:47:22.306407 INFO Event: name=Microsoft.Azure.Extensions.customScript, op=Download,
message=Download succeeded, duration=167
2018/04/26 17:47:22.339958 INFO [Microsoft.Azure.Extensions.customScript-2.0.6] Initialize extension directory
2018/04/26 17:47:22.368293 INFO [Microsoft.Azure.Extensions.customScript-2.0.6] Update settings file:
0.settings
2018/04/26 17:47:22.394482 INFO [Microsoft.Azure.Extensions.customScript-2.0.6] Install extension [bin/custom-
script-shim install]
2018/04/26 17:47:23.432774 INFO Event: name=Microsoft.Azure.Extensions.customScript, op=Install,
message=Launch command succeeded: bin/custom-script-shim install, duration=1007
2018/04/26 17:47:23.476151 INFO [Microsoft.Azure.Extensions.customScript-2.0.6] Enable extension [bin/custom-
script-shim enable]
2018/04/26 17:47:24.516444 INFO Event: name=Microsoft.Azure.Extensions.customScript, op=Enable, message=Launch
command succeeded: bin/custom-sc
```

Some points to note:

1. Enable is when the command starts running.
2. Download relates to the downloading of the CustomScript extension package from Azure, not the script files specified in fileUris.

The Azure Script Extension produces a log, which you can find here:

```
/var/log/azure/custom-script/handler.log
```

You should look for the individual execution, it will look something like:

```
time=2018-04-26T17:47:23Z version=v2.0.6/git@1008306-clean operation=enable seq=0 event=start
time=2018-04-26T17:47:23Z version=v2.0.6/git@1008306-clean operation=enable seq=0 event=pre-check
time=2018-04-26T17:47:23Z version=v2.0.6/git@1008306-clean operation=enable seq=0 event="comparing seqnum"
path=mrseq
time=2018-04-26T17:47:23Z version=v2.0.6/git@1008306-clean operation=enable seq=0 event="seqnum saved"
path=mrseq
time=2018-04-26T17:47:23Z version=v2.0.6/git@1008306-clean operation=enable seq=0 event="reading configuration"
time=2018-04-26T17:47:23Z version=v2.0.6/git@1008306-clean operation=enable seq=0 event="read configuration"
time=2018-04-26T17:47:23Z version=v2.0.6/git@1008306-clean operation=enable seq=0 event="validating json schema"
time=2018-04-26T17:47:23Z version=v2.0.6/git@1008306-clean operation=enable seq=0 event="json schema valid"
time=2018-04-26T17:47:23Z version=v2.0.6/git@1008306-clean operation=enable seq=0 event="parsing configuration json"
time=2018-04-26T17:47:23Z version=v2.0.6/git@1008306-clean operation=enable seq=0 event="parsed configuration json"
time=2018-04-26T17:47:23Z version=v2.0.6/git@1008306-clean operation=enable seq=0 event="validating configuration logically"
time=2018-04-26T17:47:23Z version=v2.0.6/git@1008306-clean operation=enable seq=0 event="validated configuration"
time=2018-04-26T17:47:23Z version=v2.0.6/git@1008306-clean operation=enable seq=0 event="creating output directory" path=/var/lib/waagent/custom-script/download/0
time=2018-04-26T17:47:23Z version=v2.0.6/git@1008306-clean operation=enable seq=0 event="created output directory"
time=2018-04-26T17:47:23Z version=v2.0.6/git@1008306-clean operation=enable seq=0 files=1
time=2018-04-26T17:47:23Z version=v2.0.6/git@1008306-clean operation=enable seq=0 file=0 event="download start"
time=2018-04-26T17:47:23Z version=v2.0.6/git@1008306-clean operation=enable seq=0 file=0 event="download complete" output=/var/lib/waagent/custom-script/download/0
time=2018-04-26T17:47:23Z version=v2.0.6/git@1008306-clean operation=enable seq=0 event="executing command" output=/var/lib/waagent/custom-script/download/0
time=2018-04-26T17:47:23Z version=v2.0.6/git@1008306-clean operation=enable seq=0 event="executing protected commandToExecute" output=/var/lib/waagent/custom-script/download/0
time=2018-04-26T17:47:23Z version=v2.0.6/git@1008306-clean operation=enable seq=0 event="executed command" output=/var/lib/waagent/custom-script/download/0
time=2018-04-26T17:47:23Z version=v2.0.6/git@1008306-clean operation=enable seq=0 event=enabled
time=2018-04-26T17:47:23Z version=v2.0.6/git@1008306-clean operation=enable seq=0 event=end
```

Here you can see:

- The Enable command starting is this log
- The settings passed to the extension
- The extension downloading file and the result of that.
- The command being run and the result.

You can also retrieve the execution state of the Custom Script Extension by using Azure CLI:

```
az vm extension list -g myResourceGroup --vm-name myVM
```

The output looks like the following text:

```
info: Executing command vm extension get
+ Looking up the VM "scripttst001"
data: Publisher Name Version State
data: ----- -----
data: Microsoft.Azure.Extensions CustomScript 2.0 Succeeded
data: Microsoft.OSTCExtensions Microsoft.Insights.VMDiagnosticsSettings 2.3 Succeeded
info: vm extension get command OK
```

## Next steps

To see the code, current issues and versions, see [custom-script-extension-linux repo](#).

# Run shell scripts in your Linux VM by using Run Command

10/18/2019 • 3 minutes to read • [Edit Online](#)

The Run Command feature uses the virtual machine (VM) agent to run shell scripts within an Azure Linux VM. You can use these scripts for general machine or application management. They can help you to quickly diagnose and remediate VM access and network issues and get the VM back to a good state.

## Benefits

You can access your virtual machines in multiple ways. Run Command can run scripts on your virtual machines remotely by using the VM agent. You use Run Command through the Azure portal, [REST API](#), or [Azure CLI](#) for Linux VMs.

This capability is useful in all scenarios where you want to run a script within a virtual machine. It's one of the only ways to troubleshoot and remediate a virtual machine that doesn't have the RDP or SSH port open because of improper network or administrative user configuration.

## Restrictions

The following restrictions apply when you're using Run Command:

- Output is limited to the last 4,096 bytes.
- The minimum time to run a script is about 20 seconds.
- Scripts run by default as an elevated user on Linux.
- You can run one script at a time.
- Scripts that prompt for information (interactive mode) are not supported.
- You can't cancel a running script.
- The maximum time a script can run is 90 minutes. After that, the script will time out.
- Outbound connectivity from the VM is required to return the results of the script.

### NOTE

To function correctly, Run Command requires connectivity (port 443) to Azure public IP addresses. If the extension doesn't have access to these endpoints, the scripts might run successfully but not return the results. If you're blocking traffic on the virtual machine, you can use [service tags](#) to allow traffic to Azure public IP addresses by using the `AzureCloud` tag.

## Available commands

This table shows the list of commands available for Linux VMs. You can use the **RunShellScript** command to run any custom script that you want. When you're using the Azure CLI or PowerShell to run a command, the value that you provide for the `--command-id` or `-CommandId` parameter must be one of the following listed values. When you specify a value that is not an available command, you receive this error:

The entity was not found in this Azure location

| NAME           | DESCRIPTION                                       |
|----------------|---------------------------------------------------|
| RunShellScript | Runs a Linux shell script.                        |
| ifconfig       | Gets the configuration of all network interfaces. |

## Azure CLI

The following example uses the `az vm run-command` command to run a shell script on an Azure Linux VM.

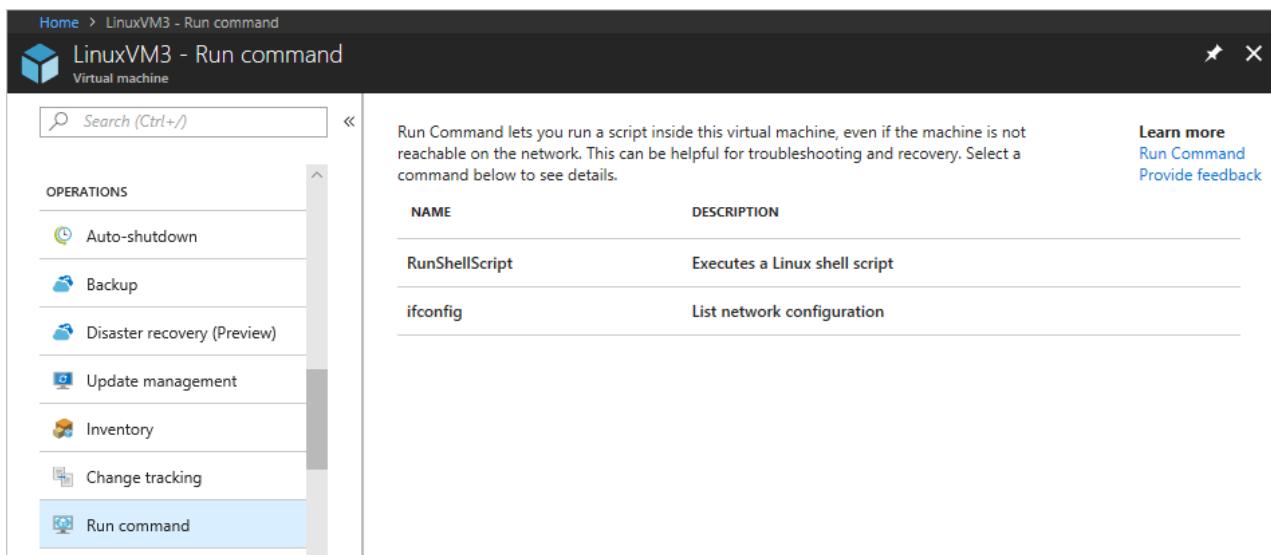
```
az vm run-command invoke -g myResourceGroup -n myVm --command-id RunShellScript --scripts "sudo apt-get update && sudo apt-get install -y nginx"
```

### NOTE

To run commands as a different user, enter `sudo -u` to specify a user account.

## Azure portal

Go to a VM in the [Azure portal](#) and select **Run command** under **OPERATIONS**. You see a list of the available commands to run on the VM.



The screenshot shows the Azure portal interface for a virtual machine named "LinuxVM3". The left sidebar has a "Run command" item selected under the "OPERATIONS" section. The main content area displays a list of commands:

| NAME           | DESCRIPTION                   |
|----------------|-------------------------------|
| RunShellScript | Executes a Linux shell script |
| ifconfig       | List network configuration    |

At the top right of the content area, there are links for "Learn more", "Run Command", and "Provide feedback".

Choose a command to run. Some of the commands might have optional or required input parameters. For those commands, the parameters are presented as text fields for you to provide the input values. For each command, you can view the script that's being run by expanding **View script**. **RunShellScript** is different from the other commands, because it allows you to provide your own custom script.

### NOTE

The built-in commands are not editable.

After you choose the command, select **Run** to run the script. After the script finishes, it returns the output and any errors in the output window. The following screenshot shows an example output from running the **ifconfig** command.

Run Command Script  
ifconfig

Script execution complete

Details  
Get the configuration of all network interfaces.

View script

Parameters

ARGUMENTS ⓘ  
Default will be used

Run

Output

```
Enable succeeded:
[stdout]
eth0 Link encap:Ethernet HWaddr 00:0d:3a:12:81:d1
 inet addr:10.0.0.7 Bcast:10.0.0.255 Mask:255.255.255.0
 inet6 addr: fe80::20d:3aff:fe12:81d1/64 Scope:Link
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:2134524 errors:0 dropped:0 overruns:0 frame:0
 TX packets:1438287 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:2208675468 (2.2 GB) TX bytes:400069292 (400.0 MB)

lo Link encap:Local Loopback
 inet addr:127.0.0.1 Mask:255.0.0.0
 inet6 addr: ::1/128 Scope:Host
 UP LOOPBACK RUNNING MTU:65536 Metric:1
 RX packets:160 errors:0 dropped:0 overruns:0 frame:0
 TX packets:160 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:11840 (11.8 KB) TX bytes:11840 (11.8 KB)

[stderr]
```

## PowerShell

The following example uses the [Invoke-AzVMRunCommand](#) cmdlet to run a PowerShell script on an Azure VM. The cmdlet expects the script referenced in the `-ScriptPath` parameter to be local to where the cmdlet is being run.

```
Invoke-AzVMRunCommand -ResourceGroupName '<myResourceGroup>' -Name '<myVMName>' -CommandId 'RunPowerShellScript' -ScriptPath '<pathToScript>' -Parameter @{"arg1" = "var1";"arg2" = "var2"}
```

## Limiting access to Run Command

Listing the run commands or showing the details of a command requires the `Microsoft.Compute/locations/runCommands/read` permission at the subscription level. The built-in [Reader](#) role and higher levels have this permission.

Running a command requires the `Microsoft.Compute/virtualMachines/runCommand/action` permission at the subscription level. The [Virtual Machine Contributor](#) role and higher levels have this permission.

You can use one of the [built-in roles](#) or create a [custom role](#) to use Run Command.

## Next steps

To learn about other ways to run scripts and commands remotely in your VM, see [Run scripts in your Linux VM](#).



# Install and configure Remote Desktop to connect to a Linux VM in Azure

11/13/2019 • 4 minutes to read • [Edit Online](#)

Linux virtual machines (VMs) in Azure are usually managed from the command line using a secure shell (SSH) connection. When new to Linux, or for quick troubleshooting scenarios, the use of remote desktop may be easier. This article details how to install and configure a desktop environment ([xfce](#)) and remote desktop ([xrdp](#)) for your Linux VM using the Resource Manager deployment model.

## Prerequisites

This article requires an existing Ubuntu 18.04 LTS VM in Azure. If you need to create a VM, use one of the following methods:

- The [Azure CLI](#)
- The [Azure portal](#)

## Install a desktop environment on your Linux VM

Most Linux VMs in Azure do not have a desktop environment installed by default. Linux VMs are commonly managed using SSH connections rather than a desktop environment. There are various desktop environments in Linux that you can choose. Depending on your choice of desktop environment, it may consume one to 2 GB of disk space, and take 5 to 10 minutes to install and configure all the required packages.

The following example installs the lightweight [xfce4](#) desktop environment on an Ubuntu 18.04 LTS VM. Commands for other distributions vary slightly (use [yum](#) to install on Red Hat Enterprise Linux and configure appropriate [selinux](#) rules, or use [zypper](#) to install on SUSE, for example).

First, SSH to your VM. The following example connects to the VM named *myvm.westus.cloudapp.azure.com* with the username of *azureuser*. Use your own values:

```
ssh azureuser@myvm.westus.cloudapp.azure.com
```

If you are using Windows and need more information on using SSH, see [How to use SSH keys with Windows](#).

Next, install xfce using [apt](#) as follows:

```
sudo apt-get update
sudo apt-get install xfce4
```

## Install and configure a remote desktop server

Now that you have a desktop environment installed, configure a remote desktop service to listen for incoming connections. [xrdp](#) is an open source Remote Desktop Protocol (RDP) server that is available on most Linux distributions, and works well with xfce. Install xrdp on your Ubuntu VM as follows:

```
sudo apt-get -y install xrdp
sudo systemctl enable xrdp
```

Tell xrdp what desktop environment to use when you start your session. Configure xrdp to use xfce as your desktop environment as follows:

```
echo xfce4-session >~/xsession
```

Restart the xrdp service for the changes to take effect as follows:

```
sudo service xrdp restart
```

## Set a local user account password

If you created a password for your user account when you created your VM, skip this step. If you only use SSH key authentication and do not have a local account password set, specify a password before you use xrdp to log in to your VM. xrdp cannot accept SSH keys for authentication. The following example specifies a password for the user account *azureuser*:

```
sudo passwd azureuser
```

### NOTE

Specifying a password does not update your SSHD configuration to permit password logins if it currently does not. From a security perspective, you may wish to connect to your VM with an SSH tunnel using key-based authentication and then connect to xrdp. If so, skip the following step on creating a network security group rule to allow remote desktop traffic.

## Create a Network Security Group rule for Remote Desktop traffic

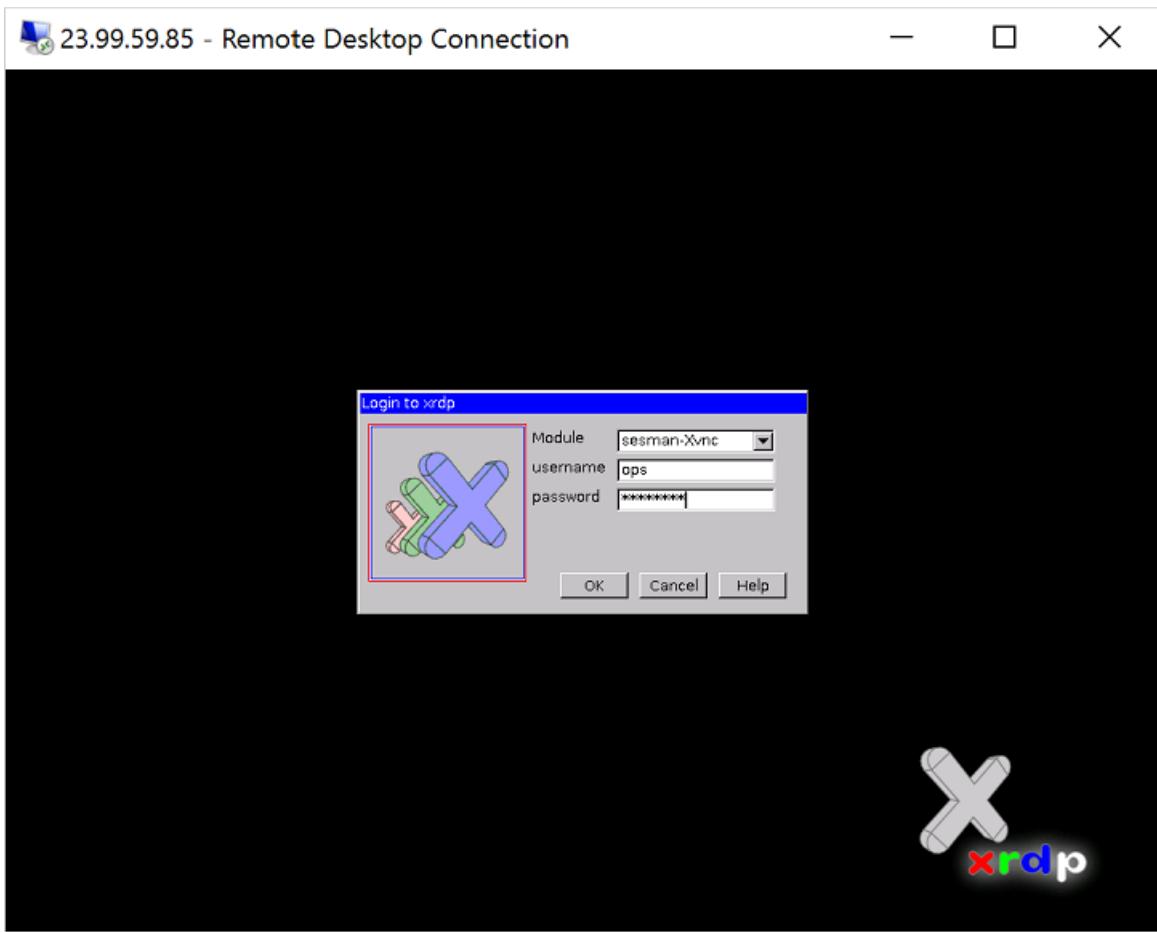
To allow Remote Desktop traffic to reach your Linux VM, a network security group rule needs to be created that allows TCP on port 3389 to reach your VM. For more information about network security group rules, see [What is a network security group?](#) You can also [use the Azure portal to create a network security group rule](#).

The following example creates a network security group rule with [az vm open-port](#) on port 3389. From the Azure CLI, not the SSH session to your VM, open the following network security group rule:

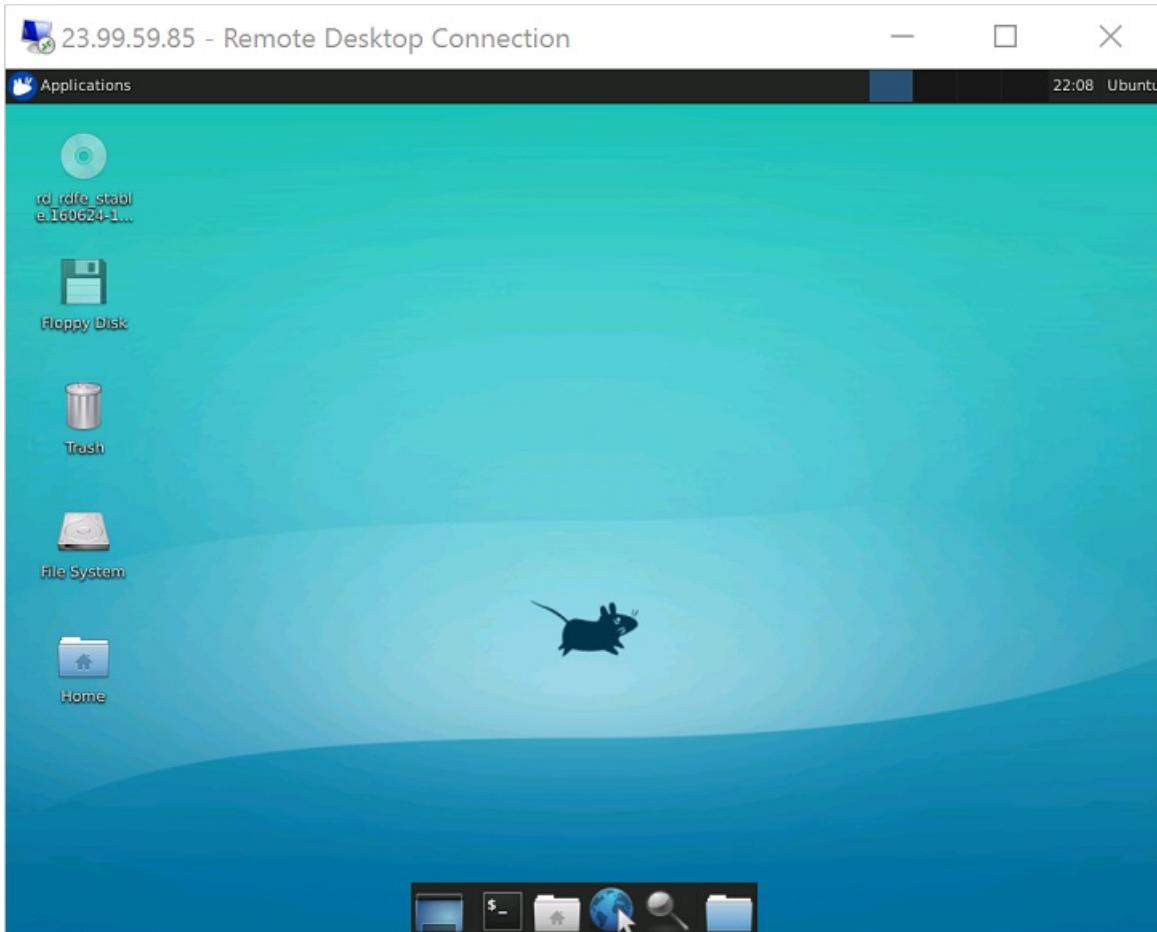
```
az vm open-port --resource-group myResourceGroup --name myVM --port 3389
```

## Connect your Linux VM with a Remote Desktop client

Open your local remote desktop client and connect to the IP address or DNS name of your Linux VM. Enter the username and password for the user account on your VM as follows:



After authenticating, the xfce desktop environment will load and look similar to the following example:



If your local RDP client uses network level authentication (NLA), you may need to disable that connection setting. XRDp does not currently support NLA. You can also look at alternative RDP solutions that do support NLA, such

as [FreeRDP](#).

## Troubleshoot

If you cannot connect to your Linux VM using a Remote Desktop client, use `netstat` on your Linux VM to verify that your VM is listening for RDP connections as follows:

```
sudo netstat -plnt | grep rdp
```

The following example shows the VM listening on TCP port 3389 as expected:

```
tcp 0 0 127.0.0.1:3350 0.0.0.0:* LISTEN 53192/xrdp-sesman
tcp 0 0 0.0.0.0:3389 0.0.0.0:* LISTEN 53188/xrdp
```

If the *xrdp-sesman* service is not listening, on an Ubuntu VM restart the service as follows:

```
sudo service xrdp restart
```

Review logs in `/var/log` on your Ubuntu VM for indications as to why the service may not be responding. You can also monitor the syslog during a remote desktop connection attempt to view any errors:

```
tail -f /var/log/syslog
```

Other Linux distributions such as Red Hat Enterprise Linux and SUSE may have different ways to restart services and alternate log file locations to review.

If you do not receive any response in your remote desktop client and do not see any events in the system log, this behavior indicates that remote desktop traffic cannot reach the VM. Review your network security group rules to ensure that you have a rule to permit TCP on port 3389. For more information, see [Troubleshoot application connectivity issues](#).

## Next steps

For more information about creating and using SSH keys with Linux VMs, see [Create SSH keys for Linux VMs in Azure](#).

For information on using SSH from Windows, see [How to use SSH keys with Windows](#).

# Join a Red Hat Enterprise Linux virtual machine to an Azure AD Domain Services managed domain

2/25/2020 • 8 minutes to read • [Edit Online](#)

To let users sign in to virtual machines (VMs) in Azure using a single set of credentials, you can join VMs to an Azure Active Directory Domain Services (AD DS) managed domain. When you join a VM to an Azure AD DS managed domain, user accounts and credentials from the domain can be used to sign in and manage servers. Group memberships from the Azure AD DS managed domain are also applied to let you control access to files or services on the VM.

This article shows you how to join a Red Hat Enterprise Linux (RHEL) VM to an Azure AD DS managed domain.

## Prerequisites

To complete this tutorial, you need the following resources and privileges:

- An active Azure subscription.
  - If you don't have an Azure subscription, [create an account](#).
- An Azure Active Directory tenant associated with your subscription, either synchronized with an on-premises directory or a cloud-only directory.
  - If needed, [create an Azure Active Directory tenant](#) or [associate an Azure subscription with your account](#).
- An Azure Active Directory Domain Services managed domain enabled and configured in your Azure AD tenant.
  - If needed, the first tutorial [creates and configures an Azure Active Directory Domain Services instance](#).
- A user account that's a member of the *Azure AD DC administrators* group in your Azure AD tenant.

## Create and connect to a RHEL Linux VM

If you have an existing RHEL Linux VM in Azure, connect to it using SSH, then continue on to the next step to [start configuring the VM](#).

If you need to create a RHEL Linux VM, or want to create a test VM for use with this article, you can use one of the following methods:

- [Azure portal](#)
- [Azure CLI](#)
- [Azure PowerShell](#)

When you create the VM, pay attention to the virtual network settings to make sure that the VM can communicate with the Azure AD DS managed domain:

- Deploy the VM into the same, or a peered, virtual network in which you have enabled Azure AD Domain Services.
- Deploy the VM into a different subnet than your Azure AD Domain Services instance.

Once the VM is deployed, follow the steps to connect to the VM using SSH.

## Configure the hosts file

To make sure that the VM host name is correctly configured for the managed domain, edit the `/etc/hosts` file and set the hostname:

```
sudo vi /etc/hosts
```

In the *hosts* file, update the *localhost* address. In the following example:

- *aaddscontoso.com* is the DNS domain name of your Azure AD DS managed domain.
- *rhel* is the hostname of your RHEL VM that you're joining to the managed domain.

Update these names with your own values:

```
127.0.0.1 rhel rhel.aaddscontoso.com
```

When done, save and exit the *hosts* file using the `:wq` command of the editor.

## Install required packages

The VM needs some additional packages to join the VM to the Azure AD DS managed domain. To install and configure these packages, update and install the domain-join tools using `yum`. There are some differences between RHEL 7.x and RHEL 6.x, so use the appropriate commands for your distro version in the remaining sections of this article.

### RHEL 7

```
sudo yum install realmd sssd krb5-workstation krb5-libs oddjob oddjob-mkhomedir samba-common-tools
```

### RHEL 6

```
sudo yum install adcli sssd authconfig krb5-workstation
```

## Join VM to the managed domain

Now that the required packages are installed on the VM, join the VM to the Azure AD DS managed domain. Again, use the appropriate steps for your RHEL distro version.

### RHEL 7

1. Use the `realm discover` command to discover the Azure AD DS managed domain. The following example discovers the realm *AADDSCONTOSO.COM*. Specify your own Azure AD DS managed domain name in ALL UPPERCASE:

```
sudo realm discover AADDSCONTOSO.COM
```

If the `realm discover` command can't find your Azure AD DS managed domain, review the following troubleshooting steps:

- Make sure that the domain is reachable from the VM. Try `ping aaddscontoso.com` to see if a positive reply is returned.
  - Check that the VM is deployed to the same, or a peered, virtual network in which the Azure AD DS managed domain is available.
  - Confirm that the DNS server settings for the virtual network have been updated to point to the domain controllers of the Azure AD DS managed domain.
2. Now initialize Kerberos using the `kinit` command. Specify a user that belongs to the *AAD DC*

*Administrators* group. If needed, [add a user account to a group in Azure AD](#).

Again, the Azure AD DS managed domain name must be entered in ALL UPPERCASE. In the following example, the account named `contosoadmin@aaddscontoso.com` is used to initialize Kerberos. Enter your own user account that's a member of the *AAD DC Administrators* group:

```
kinit contosoadmin@AADDSCONTOSO.COM
```

- Finally, join the machine to the Azure AD DS managed domain using the `realm join` command. Use the same user account that's a member of the *AAD DC Administrators* group that you specified in the previous `kinit` command, such as `contosoadmin@AADDSCONTOSO.COM`:

```
sudo realm join --verbose AADDSCONTOSO.COM -U 'contosoadmin@AADDSCONTOSO.COM'
```

It takes a few moments to join the VM to the Azure AD DS managed domain. The following example output shows the VM has successfully joined to the Azure AD DS managed domain:

```
Successfully enrolled machine in realm
```

## RHEL 6

- Use the `adcli info` command to discover the Azure AD DS managed domain. The following example discovers the realm `AADDSCONTOSO.COM`. Specify your own Azure AD DS managed domain name in ALL UPPERCASE:

```
sudo adcli info aaddscontoso.com
```

If the `adcli info` command can't find your Azure AD DS managed domain, review the following troubleshooting steps:

- Make sure that the domain is reachable from the VM. Try `ping aaddscontoso.com` to see if a positive reply is returned.
  - Check that the VM is deployed to the same, or a peered, virtual network in which the Azure AD DS managed domain is available.
  - Confirm that the DNS server settings for the virtual network have been updated to point to the domain controllers of the Azure AD DS managed domain.
- First, join the domain using the `adcli join` command, this command will also creates the keytab to authenticate the machine. Use a user account that's a member of the *AAD DC Administrators* group.

```
sudo adcli join aaddscontoso.com -U contosoadmin
```

- Now configure the `/etc/krb5.conf` and create the `/etc/sssd/sssd.conf` files to use the `aaddscontoso.com` Active Directory domain. Make sure that `AADDSCONTOSO.COM` is replaced by your own domain name:

Open the `/etc/krb5.conf` file with an editor:

```
sudo vi /etc/krb5.conf
```

Update the `krb5.conf` file to match the following sample:

```

[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log

[libdefaults]
default_realm = AADDSCONTOSO.COM
dns_lookup_realm = true
dns_lookup_kdc = true
ticket_lifetime = 24h
renew_lifetime = 7d
forwardable = true

[realms]
AADDSCONTOSO.COM = {
kdc = AADDSCONTOSO.COM
admin_server = AADDSCONTOSO.COM
}

[domain_realm]
.AADDSCONTOSO.COM = AADDSCONTOSO.COM
AADDSCONTOSO.COM = AADDSCONTOSO.COM

```

Create the `/etc/sssd/sssd.conf` file:

```
sudo vi /etc/sssd/sssd.conf
```

Update the `sssd.conf` file to match the following sample:

```

[sssd]
services = nss, pam, ssh, autofs
config_file_version = 2
domains = AADDSCONTOSO.COM

[domain/AADDSCONTOSO.COM]

id_provider = ad

```

4. Make sure `/etc/sssd/sssd.conf` permissions are 600 and is owned by root user:

```
sudo chmod 600 /etc/sssd/sssd.conf
sudo chown root:root /etc/sssd/sssd.conf
```

5. Use `authconfig` to instruct the VM about the AD Linux integration:

```
sudo authconfig --enablerssd --enablesssdauth --update
```

6. Start and enable the sssd service:

```
sudo service sssd start
sudo chkconfig sssd on
```

If your VM can't successfully complete the domain-join process, make sure that the VM's network security group allows outbound Kerberos traffic on TCP + UDP port 464 to the virtual network subnet for your Azure AD DS managed domain.

Now check if you can query user AD information using `getent`

```
sudo getent passwd contosoadmin
```

## Allow password authentication for SSH

By default, users can only sign in to a VM using SSH public key-based authentication. Password-based authentication fails. When you join the VM to an Azure AD DS managed domain, those domain accounts need to use password-based authentication. Update the SSH configuration to allow password-based authentication as follows.

1. Open the `sshd_config` file with an editor:

```
sudo vi /etc/ssh/sshd_config
```

2. Update the line for `PasswordAuthentication` to `yes`:

```
PasswordAuthentication yes
```

When done, save and exit the `sshd_config` file using the `:wq` command of the editor.

3. To apply the changes and let users sign in using a password, restart the SSH service for your RHEL distro version:

### RHEL 7

```
sudo systemctl restart sshd
```

### RHEL 6

```
sudo service sshd restart
```

## Grant the 'AAD DC Administrators' group sudo privileges

To grant members of the *AAD DC Administrators* group administrative privileges on the RHEL VM, you add an entry to the `/etc/sudoers`. Once added, members of the *AAD DC Administrators* group can use the `sudo` command on the RHEL VM.

1. Open the `sudoers` file for editing:

```
sudo visudo
```

2. Add the following entry to the end of `/etc/sudoers` file. The *AAD DC Administrators* group contains whitespace in the name, so include the backslash escape character in the group name. Add your own domain name, such as `aaddscontoso.com`:

```
Add 'AAD DC Administrators' group members as admins.
%AAD\ DC\ Administrators@aaddscontoso.com ALL=(ALL) NOPASSWD:ALL
```

When done, save and exit the editor using the `:wq` command of the editor.

## Sign in to the VM using a domain account

To verify that the VM has been successfully joined to the Azure AD DS managed domain, start a new SSH connection using a domain user account. Confirm that a home directory has been created, and that group membership from the domain is applied.

1. Create a new SSH connection from your console. Use a domain account that belongs to the managed domain using the `ssh -l` command, such as `contosoadmin@aaddscontoso.com` and then enter the address of your VM, such as `rhel.aaddscontoso.com`. If you use the Azure Cloud Shell, use the public IP address of the VM rather than the internal DNS name.

```
ssh -l contosoadmin@AADDSCONTOSO.com rhel.aaddscontoso.com
```

2. When you've successfully connected to the VM, verify that the home directory was initialized correctly:

```
pwd
```

You should be in the `/home` directory with your own directory that matches the user account.

3. Now check that the group memberships are being resolved correctly:

```
id
```

You should see your group memberships from the Azure AD DS managed domain.

4. If you signed in to the VM as a member of the *AAD DC Administrators* group, check that you can correctly use the `sudo` command:

```
sudo yum update
```

## Next steps

If you have problems connecting the VM to the Azure AD DS managed domain or signing in with a domain account, see [Troubleshooting domain join issues](#).

# Join a CentOS Linux virtual machine to an Azure AD Domain Services managed domain

2/25/2020 • 6 minutes to read • [Edit Online](#)

To let users sign in to virtual machines (VMs) in Azure using a single set of credentials, you can join VMs to an Azure Active Directory Domain Services (AD DS) managed domain. When you join a VM to an Azure AD DS managed domain, user accounts and credentials from the domain can be used to sign in and manage servers. Group memberships from the Azure AD DS managed domain are also applied to let you control access to files or services on the VM.

This article shows you how to join a CentOS Linux VM to an Azure AD DS managed domain.

## Prerequisites

To complete this tutorial, you need the following resources and privileges:

- An active Azure subscription.
  - If you don't have an Azure subscription, [create an account](#).
- An Azure Active Directory tenant associated with your subscription, either synchronized with an on-premises directory or a cloud-only directory.
  - If needed, [create an Azure Active Directory tenant](#) or [associate an Azure subscription with your account](#).
- An Azure Active Directory Domain Services managed domain enabled and configured in your Azure AD tenant.
  - If needed, the first tutorial [creates and configures an Azure Active Directory Domain Services instance](#).
- A user account that's a member of the *Azure AD DC administrators* group in your Azure AD tenant.

## Create and connect to a CentOS Linux VM

If you have an existing CentOS Linux VM in Azure, connect to it using SSH, then continue on to the next step to [start configuring the VM](#).

If you need to create a CentOS Linux VM, or want to create a test VM for use with this article, you can use one of the following methods:

- [Azure portal](#)
- [Azure CLI](#)
- [Azure PowerShell](#)

When you create the VM, pay attention to the virtual network settings to make sure that the VM can communicate with the Azure AD DS managed domain:

- Deploy the VM into the same, or a peered, virtual network in which you have enabled Azure AD Domain Services.
- Deploy the VM into a different subnet than your Azure AD Domain Services instance.

Once the VM is deployed, follow the steps to connect to the VM using SSH.

## Configure the hosts file

To make sure that the VM host name is correctly configured for the managed domain, edit the `/etc/hosts` file and set the hostname:

```
sudo vi /etc/hosts
```

In the *hosts* file, update the *localhost* address. In the following example:

- *aaddscontoso.com* is the DNS domain name of your Azure AD DS managed domain.
- *centos* is the hostname of your CentOS VM that you're joining to the managed domain.

Update these names with your own values:

```
127.0.0.1 centos.aaddscontoso.com centos
```

When done, save and exit the *hosts* file using the `:wq` command of the editor.

## Install required packages

The VM needs some additional packages to join the VM to the Azure AD DS managed domain. To install and configure these packages, update and install the domain-join tools using `yum`:

```
sudo yum install realmd sssd krb5-workstation krb5-libs oddjob oddjob-mkhomedir samba-common-tools
```

## Join VM to the managed domain

Now that the required packages are installed on the VM, join the VM to the Azure AD DS managed domain.

1. Use the `realm discover` command to discover the Azure AD DS managed domain. The following example discovers the realm *AADDSCONTOSO.COM*. Specify your own Azure AD DS managed domain name in ALL UPPERCASE:

```
sudo realm discover AADDSCONTOSO.COM
```

If the `realm discover` command can't find your Azure AD DS managed domain, review the following troubleshooting steps:

- Make sure that the domain is reachable from the VM. Try `ping aaddscontoso.com` to see if a positive reply is returned.
  - Check that the VM is deployed to the same, or a peered, virtual network in which the Azure AD DS managed domain is available.
  - Confirm that the DNS server settings for the virtual network have been updated to point to the domain controllers of the Azure AD DS managed domain.
2. Now initialize Kerberos using the `kinit` command. Specify a user that belongs to the *AAD DC Administrators* group. If needed, [add a user account to a group in Azure AD](#).

Again, the Azure AD DS managed domain name must be entered in ALL UPPERCASE. In the following example, the account named `contosoadmin@aaddscontoso.com` is used to initialize Kerberos. Enter your own user account that's a member of the *AAD DC Administrators* group:

```
kinit contosoadmin@AADDSCONTOSO.COM
```

3. Finally, join the machine to the Azure AD DS managed domain using the `realm join` command. Use the same user account that's a member of the *AAD DC Administrators* group that you specified in the previous `kinit` command, such as `contosoadmin@AADDSCONTOSO.COM`:

```
sudo realm join --verbose ADDSCONTOSO.COM -U 'contosoadmin@ADDSCONTOSO.COM'
```

It takes a few moments to join the VM to the Azure AD DS managed domain. The following example output shows the VM has successfully joined to the Azure AD DS managed domain:

```
Successfully enrolled machine in realm
```

If your VM can't successfully complete the domain-join process, make sure that the VM's network security group allows outbound Kerberos traffic on TCP + UDP port 464 to the virtual network subnet for your Azure AD DS managed domain.

## Allow password authentication for SSH

By default, users can only sign in to a VM using SSH public key-based authentication. Password-based authentication fails. When you join the VM to an Azure AD DS managed domain, those domain accounts need to use password-based authentication. Update the SSH configuration to allow password-based authentication as follows.

1. Open the `sshd_config` file with an editor:

```
sudo vi /etc/ssh/sshd_config
```

2. Update the line for `PasswordAuthentication` to `yes`:

```
PasswordAuthentication yes
```

When done, save and exit the `sshd_config` file using the `:wq` command of the editor.

3. To apply the changes and let users sign in using a password, restart the SSH service:

```
sudo systemctl restart sshd
```

## Grant the 'AAD DC Administrators' group sudo privileges

To grant members of the `AAD DC Administrators` group administrative privileges on the CentOS VM, you add an entry to the `/etc/sudoers`. Once added, members of the `AAD DC Administrators` group can use the `sudo` command on the CentOS VM.

1. Open the `sudoers` file for editing:

```
sudo visudo
```

2. Add the following entry to the end of `/etc/sudoers` file. The `AAD DC Administrators` group contains whitespace in the name, so include the backslash escape character in the group name. Add your own domain name, such as `aaddscontoso.com`:

```
Add 'AAD DC Administrators' group members as admins.
%AAD\ DC\ Administrators@aaddscontoso.com ALL=(ALL) NOPASSWD:ALL
```

When done, save and exit the editor using the `:wq` command of the editor.

## Sign in to the VM using a domain account

To verify that the VM has been successfully joined to the Azure AD DS managed domain, start a new SSH connection using a domain user account. Confirm that a home directory has been created, and that group membership from the domain is applied.

1. Create a new SSH connection from your console. Use a domain account that belongs to the managed domain using the `ssh -l` command, such as `contosoadmin@aaddscontoso.com` and then enter the address of your VM, such as `centos.aaddscontoso.com`. If you use the Azure Cloud Shell, use the public IP address of the VM rather than the internal DNS name.

```
ssh -l contosoadmin@AADDSCONTOSO.com centos.aaddscontoso.com
```

2. When you've successfully connected to the VM, verify that the home directory was initialized correctly:

```
pwd
```

You should be in the `/home` directory with your own directory that matches the user account.

3. Now check that the group memberships are being resolved correctly:

```
id
```

You should see your group memberships from the Azure AD DS managed domain.

4. If you signed in to the VM as a member of the *AAD DC Administrators* group, check that you can correctly use the `sudo` command:

```
sudo yum update
```

## Next steps

If you have problems connecting the VM to the Azure AD DS managed domain or signing in with a domain account, see [Troubleshooting domain join issues](#).

# Join an Ubuntu Linux virtual machine to an Azure AD Domain Services managed domain

2/25/2020 • 8 minutes to read • [Edit Online](#)

To let users sign in to virtual machines (VMs) in Azure using a single set of credentials, you can join VMs to an Azure Active Directory Domain Services (AD DS) managed domain. When you join a VM to an Azure AD DS managed domain, user accounts and credentials from the domain can be used to sign in and manage servers. Group memberships from the Azure AD DS managed domain are also applied to let you control access to files or services on the VM.

This article shows you how to join an Ubuntu Linux VM to an Azure AD DS managed domain.

## Prerequisites

To complete this tutorial, you need the following resources and privileges:

- An active Azure subscription.
  - If you don't have an Azure subscription, [create an account](#).
- An Azure Active Directory tenant associated with your subscription, either synchronized with an on-premises directory or a cloud-only directory.
  - If needed, [create an Azure Active Directory tenant](#) or [associate an Azure subscription with your account](#).
- An Azure Active Directory Domain Services managed domain enabled and configured in your Azure AD tenant.
  - If needed, the first tutorial [creates and configures an Azure Active Directory Domain Services instance](#).
- A user account that's a member of the *Azure AD DC administrators* group in your Azure AD tenant.

## Create and connect to an Ubuntu Linux VM

If you have an existing Ubuntu Linux VM in Azure, connect to it using SSH, then continue on to the next step to [start configuring the VM](#).

If you need to create an Ubuntu Linux VM, or want to create a test VM for use with this article, you can use one of the following methods:

- [Azure portal](#)
- [Azure CLI](#)
- [Azure PowerShell](#)

When you create the VM, pay attention to the virtual network settings to make sure that the VM can communicate with the Azure AD DS managed domain:

- Deploy the VM into the same, or a peered, virtual network in which you have enabled Azure AD Domain Services.
- Deploy the VM into a different subnet than your Azure AD Domain Services instance.

Once the VM is deployed, follow the steps to connect to the VM using SSH.

## Configure the hosts file

To make sure that the VM host name is correctly configured for the managed domain, edit the `/etc/hosts` file and set the hostname:

```
sudo vi /etc/hosts
```

In the *hosts* file, update the *localhost* address. In the following example:

- *aaddscontoso.com* is the DNS domain name of your Azure AD DS managed domain.
- *ubuntu* is the hostname of your Ubuntu VM that you're joining to the managed domain.

Update these names with your own values:

```
127.0.0.1 ubuntu.aaddscontoso.com ubuntu
```

When done, save and exit the *hosts* file using the `:wq` command of the editor.

## Install required packages

The VM needs some additional packages to join the VM to the Azure AD DS managed domain. To install and configure these packages, update and install the domain-join tools using `apt-get`

During the Kerberos installation, the *krb5-user* package prompts for the realm name in ALL UPPERCASE. For example, if the name of your Azure AD DS managed domain is *aaddscontoso.com*, enter *AADDSCONTOSO.COM* as the realm. The installation writes the `[realm]` and `[domain_realm]` sections in */etc krb5.conf* configuration file. Make sure that you specify the realm an ALL UPPERCASE:

```
sudo apt-get update
sudo apt-get install krb5-user samba sssd sssd-tools libnss-sss libpam-sss ntp ntpdate realmd adcli
```

## Configure Network Time Protocol (NTP)

For domain communication to work correctly, the date and time of your Ubuntu VM must synchronize with the Azure AD DS managed domain. Add your Azure AD DS managed domain's NTP hostname to the */etc/ntp.conf* file.

1. Open the *ntp.conf* file with an editor:

```
sudo vi /etc/ntp.conf
```

2. In the *ntp.conf* file, create a line to add your Azure AD DS managed domain's DNS name. In the following example, an entry for *aaddscontoso.com* is added. Use your own DNS name:

```
server aaddscontoso.com
```

When done, save and exit the *ntp.conf* file using the `:wq` command of the editor.

3. To make sure that the VM is synchronized with the Azure AD DS managed domain, the following steps are needed:

- Stop the NTP server
- Update the date and time from the managed domain
- Start the NTP service

Run the following commands to complete these steps. Use your own DNS name with the `ntpdate` command:

```
sudo systemctl stop ntp
sudo ntpdate aaddscontoso.com
sudo systemctl start ntp
```

## Join VM to the managed domain

Now that the required packages are installed on the VM and NTP is configured, join the VM to the Azure AD DS managed domain.

1. Use the `realm discover` command to discover the Azure AD DS managed domain. The following example discovers the realm `AADDSCONTOSO.COM`. Specify your own Azure AD DS managed domain name in ALL UPPERCASE:

```
sudo realm discover AADDSCONTOSO.COM
```

If the `realm discover` command can't find your Azure AD DS managed domain, review the following troubleshooting steps:

- Make sure that the domain is reachable from the VM. Try `ping aaddscontoso.com` to see if a positive reply is returned.
  - Check that the VM is deployed to the same, or a peered, virtual network in which the Azure AD DS managed domain is available.
  - Confirm that the DNS server settings for the virtual network have been updated to point to the domain controllers of the Azure AD DS managed domain.
2. Now initialize Kerberos using the `kinit` command. Specify a user that belongs to the *AAD DC Administrators* group. If needed, [add a user account to a group in Azure AD](#).

Again, the Azure AD DS managed domain name must be entered in ALL UPPERCASE. In the following example, the account named `contosoadmin@aaddscontoso.com` is used to initialize Kerberos. Enter your own user account that's a member of the *AAD DC Administrators* group:

```
kinit contosoadmin@AADDSCONTOSO.COM
```

3. Finally, join the machine to the Azure AD DS managed domain using the `realm join` command. Use the same user account that's a member of the *AAD DC Administrators* group that you specified in the previous `kinit` command, such as `contosoadmin@AADDSCONTOSO.COM`:

```
sudo realm join --verbose AADDSCONTOSO.COM -U 'contosoadmin@AADDSCONTOSO.COM' --install=/
```

It takes a few moments to join the VM to the Azure AD DS managed domain. The following example output shows the VM has successfully joined to the Azure AD DS managed domain:

```
Successfully enrolled machine in realm
```

If your VM can't successfully complete the domain-join process, make sure that the VM's network security group allows outbound Kerberos traffic on TCP + UDP port 464 to the virtual network subnet for your Azure AD DS managed domain.

## Update the SSSD configuration

One of the packages installed in a previous step was for System Security Services Daemon (SSSD). When a user tries to sign in to a VM using domain credentials, SSSD relays the request to an authentication provider. In this scenario, SSSD uses Azure AD DS to authenticate the request.

1. Open the `sssd.conf` file with an editor:

```
sudo vi /etc/sssd/sssd.conf
```

2. Comment out the line for `use_fully_qualified_names` as follows:

```
use_fully_qualified_names = True
```

When done, save and exit the `sssd.conf` file using the `:wq` command of the editor.

3. To apply the change, restart the SSSD service:

```
sudo service sssd restart
```

## Configure user account and group settings

With the VM joined to the Azure AD DS managed domain and configured for authentication, there are a few user configuration options to complete. These configuration changes include allowing password-based authentication, and automatically creating home directories on the local VM when domain users first sign in.

### Allow password authentication for SSH

By default, users can only sign in to a VM using SSH public key-based authentication. Password-based authentication fails. When you join the VM to an Azure AD DS managed domain, those domain accounts need to use password-based authentication. Update the SSH configuration to allow password-based authentication as follows.

1. Open the `sshd_config` file with an editor:

```
sudo vi /etc/ssh/sshd_config
```

2. Update the line for `PasswordAuthentication` to `yes`:

```
PasswordAuthentication yes
```

When done, save and exit the `sshd_config` file using the `:wq` command of the editor.

3. To apply the changes and let users sign in using a password, restart the SSH service:

```
sudo systemctl restart ssh
```

### Configure automatic home directory creation

To enable automatic creation of the home directory when a user first signs in, complete the following steps:

1. Open the `/etc/pam.d/common-session` file in an editor:

```
sudo vi /etc/pam.d/common-session
```

2. Add the following line in this file below the line `session optional pam_sss.so`:

```
session required pam_mkhomedir.so skel=/etc/skel/ umask=0077
```

When done, save and exit the *common-session* file using the `:wq` command of the editor.

### Grant the 'AAD DC Administrators' group sudo privileges

To grant members of the *AAD DC Administrators* group administrative privileges on the Ubuntu VM, you add an entry to the */etc/sudoers*. Once added, members of the *AAD DC Administrators* group can use the `sudo` command on the Ubuntu VM.

1. Open the *sudoers* file for editing:

```
sudo visudo
```

2. Add the following entry to the end of */etc/sudoers* file:

```
Add 'AAD DC Administrators' group members as admins.
%AAD\ DC\ Administrators ALL=(ALL) NOPASSWD:ALL
```

When done, save and exit the editor using the `Ctrl-X` command.

## Sign in to the VM using a domain account

To verify that the VM has been successfully joined to the Azure AD DS managed domain, start a new SSH connection using a domain user account. Confirm that a home directory has been created, and that group membership from the domain is applied.

1. Create a new SSH connection from your console. Use a domain account that belongs to the managed domain using the `ssh -l` command, such as `contosoadmin@aaddscontoso.com` and then enter the address of your VM, such as `ubuntu.aaddscontoso.com`. If you use the Azure Cloud Shell, use the public IP address of the VM rather than the internal DNS name.

```
ssh -l contosoadmin@AADDSCONTOSO.com ubuntu.aaddscontoso.com
```

2. When you've successfully connected to the VM, verify that the home directory was initialized correctly:

```
pwd
```

You should be in the */home* directory with your own directory that matches the user account.

3. Now check that the group memberships are being resolved correctly:

```
id
```

You should see your group memberships from the Azure AD DS managed domain.

4. If you signed in to the VM as a member of the *AAD DC Administrators* group, check that you can correctly use the `sudo` command:

```
sudo apt-get update
```

## Next steps

If you have problems connecting the VM to the Azure AD DS managed domain or signing in with a domain account, see [Troubleshooting domain join issues](#).

# Preview: Log in to a Linux virtual machine in Azure using Azure Active Directory authentication

1/23/2020 • 8 minutes to read • [Edit Online](#)

To improve the security of Linux virtual machines (VMs) in Azure, you can integrate with Azure Active Directory (AD) authentication. When you use Azure AD authentication for Linux VMs, you centrally control and enforce policies that allow or deny access to the VMs. This article shows you how to create and configure a Linux VM to use Azure AD authentication.

## IMPORTANT

Azure Active Directory authentication is currently in public preview. This preview version is provided without a service level agreement, and it's not recommended for production workloads. Certain features might not be supported or might have constrained capabilities. For more information, see [Supplemental Terms of Use for Microsoft Azure Previews](#). Use this feature on a test virtual machine that you expect to discard after testing.

There are many benefits of using Azure AD authentication to log in to Linux VMs in Azure, including:

- **Improved security:**

- You can use your corporate AD credentials to log in to Azure Linux VMs. There is no need to create local administrator accounts and manage credential lifetime.
- By reducing your reliance on local administrator accounts, you do not need to worry about credential loss/theft, users configuring weak credentials etc.
- The password complexity and password lifetime policies configured for your Azure AD directory help secure Linux VMs as well.
- To further secure login to Azure virtual machines, you can configure multi-factor authentication.
- The ability to log in to Linux VMs with Azure Active Directory also works for customers that use [Federation Services](#).

- **Seamless collaboration:** With Role-Based Access Control (RBAC), you can specify who can sign in to a given VM as a regular user or with administrator privileges. When users join or leave your team, you can update the RBAC policy for the VM to grant access as appropriate. This experience is much simpler than having to scrub VMs to remove unnecessary SSH public keys. When employees leave your organization and their user account is disabled or removed from Azure AD, they no longer have access to your resources.

## Supported Azure regions and Linux distributions

The following Linux distributions are currently supported during the preview of this feature:

| DISTRIBUTION            | VERSION            |
|-------------------------|--------------------|
| CentOS                  | CentOS 6, CentOS 7 |
| Debian                  | Debian 9           |
| openSUSE                | openSUSE Leap 42.3 |
| RedHat Enterprise Linux | RHEL 6, RHEL 7     |

| DISTRIBUTION                 | VERSION                                                        |
|------------------------------|----------------------------------------------------------------|
| SUSE Linux Enterprise Server | SLES 12                                                        |
| Ubuntu Server                | Ubuntu 14.04 LTS, Ubuntu Server 16.04, and Ubuntu Server 18.04 |

The following Azure regions are currently supported during the preview of this feature:

- All global Azure regions

#### IMPORTANT

To use this preview feature, only deploy a supported Linux distro and in a supported Azure region. The feature is not supported in Azure Government or sovereign clouds.

If you choose to install and use the CLI locally, this tutorial requires that you are running the Azure CLI version 2.0.31 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

## Network requirements

To enable Azure AD authentication for your Linux VMs in Azure, you need to ensure your VMs network configuration permits outbound access to the following endpoints over TCP port 443:

- <https://login.microsoftonline.com>
- <https://device.login.microsoftonline.com>
- <https://pas.windows.net>
- <https://management.azure.com>
- <https://packages.microsoft.com>

#### NOTE

Currently, Azure network security groups can't be configured for VMs enabled with Azure AD authentication.

## Create a Linux virtual machine

Create a resource group with [az group create](#), then create a VM with [az vm create](#) using a supported distro and in a supported region. The following example deploys a VM named *myVM* that uses *Ubuntu 16.04 LTS* into a resource group named *myResourceGroup* in the *southcentralus* region. In the following examples, you can provide your own resource group and VM names as needed.

```
az group create --name myResourceGroup --location southcentralus

az vm create \
 --resource-group myResourceGroup \
 --name myVM \
 --image UbuntuLTS \
 --admin-username azureuser \
 --generate-ssh-keys
```

It takes a few minutes to create the VM and supporting resources.

## Install the Azure AD login VM extension

#### NOTE

If deploying this extension to a previously created VM ensure the machine has at least 1GB of memory allocated else the extension will fail to install

To log in to a Linux VM with Azure AD credentials, install the Azure Active Directory login VM extension. VM extensions are small applications that provide post-deployment configuration and automation tasks on Azure virtual machines. Use [az vm extension set](#) to install the *AADLoginForLinux* extension on the VM named *myVM* in the *myResourceGroup* resource group:

```
az vm extension set \
 --publisher Microsoft.Azure.ActiveDirectory.LinuxSSH \
 --name AADLoginForLinux \
 --resource-group myResourceGroup \
 --vm-name myVM
```

The *provisioningState* of *Succeeded* is shown once the extension is successfully installed on the VM.

## Configure role assignments for the VM

Azure Role-Based Access Control (RBAC) policy determines who can log in to the VM. Two RBAC roles are used to authorize VM login:

- **Virtual Machine Administrator Login:** Users with this role assigned can log in to an Azure virtual machine with Windows Administrator or Linux root user privileges.
- **Virtual Machine User Login:** Users with this role assigned can log in to an Azure virtual machine with regular user privileges.

#### NOTE

To allow a user to log in to the VM over SSH, you must assign either the *Virtual Machine Administrator Login* or *Virtual Machine User Login* role. An Azure user with the *Owner* or *Contributor* roles assigned for a VM do not automatically have privileges to log in to the VM over SSH.

The following example uses [az role assignment create](#) to assign the *Virtual Machine Administrator Login* role to the VM for your current Azure user. The username of your active Azure account is obtained with [az account show](#), and the *scope* is set to the VM created in a previous step with [az vm show](#). The scope could also be assigned at a resource group or subscription level, and normal RBAC inheritance permissions apply. For more information, see [Role-Based Access Controls](#)

```
username=$(az account show --query user.name --output tsv)
vm=$(az vm show --resource-group myResourceGroup --name myVM --query id -o tsv)

az role assignment create \
 --role "Virtual Machine Administrator Login" \
 --assignee $username \
 --scope $vm
```

#### NOTE

If your AAD domain and logon username domain do not match, you must specify the object ID of your user account with the *--assignee-object-id*, not just the username for *--assignee*. You can obtain the object ID for your user account with [az ad user list](#).

For more information on how to use RBAC to manage access to your Azure subscription resources, see using the [Azure CLI](#), [Azure portal](#), or [Azure PowerShell](#).

You can also configure Azure AD to require multi-factor authentication for a specific user to sign in to the Linux virtual machine. For more information, see [Get started with Azure Multi-Factor Authentication in the cloud](#).

## Log in to the Linux virtual machine

First, view the public IP address of your VM with `az vm show`:

```
az vm show --resource-group myResourceGroup --name myVM -d --query publicIps -o tsv
```

Log in to the Azure Linux virtual machine using your Azure AD credentials. The `-1` parameter lets you specify your own Azure AD account address. Replace the example account with your own. Account addresses should be entered in all lowercase. Replace the example IP address with the public IP address of your VM from the previous command.

```
ssh -1 azureuser@contoso.onmicrosoft.com 10.11.123.456
```

You are prompted to sign in to Azure AD with a one-time use code at <https://microsoft.com/devicelogin>. Copy and paste the one-time use code into the device login page.

When prompted, enter your Azure AD login credentials at the login page.

The following message is shown in the web browser when you have successfully authenticated:

```
You have signed in to the Microsoft Azure Linux Virtual Machine Sign-In application on your device.
```

Close the browser window, return to the SSH prompt, and press the **Enter** key.

You are now signed in to the Azure Linux virtual machine with the role permissions as assigned, such as *VM User* or *VM Administrator*. If your user account is assigned the *Virtual Machine Administrator Login* role, you can use `sudo` to run commands that require root privileges.

## Sudo and AAD login

The first time that you run sudo, you will be asked to authenticate a second time. If you don't want to have to authenticate again to run sudo, you can edit your sudoers file `/etc/sudoers.d/aad_admins` and replace this line:

```
%aad_admins ALL=(ALL) ALL
```

With this line:

```
%aad_admins ALL=(ALL) NOPASSWD:ALL
```

## Troubleshoot sign-in issues

Some common errors when you try to SSH with Azure AD credentials include no RBAC roles assigned, and repeated prompts to sign in. Use the following sections to correct these issues.

### Access denied: RBAC role not assigned

If you see the following error on your SSH prompt, verify that you have configured RBAC policies for the VM that grants the user either the *Virtual Machine Administrator Login* or *Virtual Machine User Login* role:

```
login as: azureuser@contoso.onmicrosoft.com
Using keyboard-interactive authentication.
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code FJX327AXD
to authenticate. Press ENTER when ready.
Using keyboard-interactive authentication.
Access denied: to sign-in you be assigned a role with action 'Microsoft.Compute/virtualMachines/login/action',
for example 'Virtual Machine User Login'
Access denied
```

## Continued SSH sign-in prompts

If you successfully complete the authentication step in a web browser, you may be immediately prompted to sign in again with a fresh code. This error is typically caused by a mismatch between the sign-in name you specified at the SSH prompt and the account you signed in to Azure AD with. To correct this issue:

- Verify that the sign-in name you specified at the SSH prompt is correct. A typo in the sign-in name could cause a mismatch between the sign-in name you specified at the SSH prompt and the account you signed in to Azure AD with. For example, you typed *azuresuer@contoso.onmicrosoft.com* instead of *azureuser@contoso.onmicrosoft.com*.
- If you have multiple user accounts, make sure you don't provide a different user account in the browser window when signing in to Azure AD.
- Linux is a case-sensitive operating system. There is a difference between 'Azureuser@contoso.onmicrosoft.com' and 'azureuser@contoso.onmicrosoft.com', which can cause a mismatch. Make sure that you specify the UPN with the correct case-sensitivity at the SSH prompt.

## Other limitations

Users that inherit access rights through nested groups or role assignments aren't currently supported. The user or group must be directly assigned the [required role assignments](#). For example, the use of management groups or nested group role assignments won't grant the correct permissions to allow the user to sign in.

## Preview feedback

Share your feedback about this preview feature or report issues using it on the [Azure AD feedback forum](#)

## Next steps

For more information on Azure Active Directory, see [What is Azure Active Directory](#)

# Red Hat Update Infrastructure for on-demand Red Hat Enterprise Linux VMs in Azure

2/21/2020 • 8 minutes to read • [Edit Online](#)

Red Hat Update Infrastructure (RHUI) allows cloud providers, such as Azure, to mirror Red Hat-hosted repository content, create custom repositories with Azure-specific content, and make it available to end-user VMs.

Red Hat Enterprise Linux (RHEL) Pay-As-You-Go (PAYG) images come preconfigured to access Azure RHUI. No additional configuration is needed. To get the latest updates, run `sudo yum update` after your RHEL instance is ready. This service is included as part of the RHEL PAYG software fees.

Additional information on RHEL images in Azure, including publishing and retention policies, is available [here](#).

Information on Red Hat support policies for all versions of RHEL can be found on the [Red Hat Enterprise Linux Life Cycle](#) page.

## IMPORTANT

RHUI is intended only for pay-as-you-go (PAYG) images. For custom and golden images, also known as bring-your-own-subscription (BYOS), the system needs to be attached to RHSM or Satellite in order to receive updates. See [Red Hat article](#) for more details.

## Important information about Azure RHUI

- Azure RHUI is the update infrastructure that supports all RHEL PAYG VMs created in Azure. This does not preclude you from registering your PAYG RHEL VMs with Subscription Manager or Satellite or other source of updates, but doing so with a PAYG VM will result in indirect double-billing. See the following point for details.
- Access to the Azure-hosted RHUI is included in the RHEL PAYG image price. If you unregister a PAYG RHEL VM from the Azure-hosted RHUI that does not convert the virtual machine into a bring-your-own-license (BYOL) type of VM. If you register the same VM with another source of updates, you might incur *indirect* double charges. You're charged the first time for the Azure RHEL software fee. You're charged the second time for Red Hat subscriptions that were purchased previously. If you consistently need to use an update infrastructure other than Azure-hosted RHUI, consider registering to use the [RHEL BYOS images](#).
- RHEL SAP PAYG images in Azure (RHEL for SAP, RHEL for SAP HANA, and RHEL for SAP Business Applications) are connected to dedicated RHUI channels that remain on the specific RHEL minor version as required for SAP certification.
- Access to Azure-hosted RHUI is limited to the VMs within the [Azure datacenter IP ranges](#). If you're proxying all VM traffic via an on-premises network infrastructure, you might need to set up user-defined routes for the RHEL PAYG VMs to access the Azure RHUI. If that is the case, user-defined routes will need to be added for *all* RHUI IP addresses.

## Image update behavior

As of April 2019, Azure offers RHEL images that are connected to Extended Update Support (EUS) repositories by default and RHEL images that come connected to the regular (non-EUS) repositories by default. More details on RHEL EUS are available in Red Hat's [version lifecycle documentation](#) and [EUS documentation](#). The default

behavior of `sudo yum update` will vary depending which RHEL image you provisioned from, as different images are connected to different repositories.

For a full image list, run `az vm image list --publisher redhat --all` using the Azure CLI.

### Images connected to non-EUS repositories

If you provision a VM from a RHEL image that is connected to non-EUS repositories, you will be upgraded to the latest RHEL minor version when you run `sudo yum update`. For example, if you provision a VM from an RHEL 7.4 PAYG image and run `sudo yum update`, you end up with an RHEL 7.7 VM (the latest minor version in the RHEL7 family).

Images that are connected to non-EUS repositories will not contain a minor version number in the SKU. The SKU is the third element in the URN (full name of the image). For example, all of the following images come attached to non-EUS repositories:

```
RedHat:RHEL:7-LVM:7.4.2018010506
RedHat:RHEL:7-LVM:7.5.2018081518
RedHat:RHEL:7-LVM:7.6.2019062414
RedHat:RHEL:7-RAW:7.4.2018010506
RedHat:RHEL:7-RAW:7.5.2018081518
RedHat:RHEL:7-RAW:7.6.2019062120
```

Note that the SKUs are either 7-LVM or 7-RAW. The minor version is indicated in the version (fourth element in the URN) of these images.

### Images connected to EUS repositories

If you provision a VM from a RHEL image that is connected to EUS repositories, you will not be upgraded to the latest RHEL minor version when you run `sudo yum update`. This is because the images connected to EUS repositories are also version-locked to their specific minor version.

Images connected to EUS repositories will contain a minor version number in the SKU. For example, all of the following images come attached to EUS repositories:

```
RedHat:RHEL:7.4:7.4.2019062107
RedHat:RHEL:7.5:7.5.2019062018
RedHat:RHEL:7.6:7.6.2019062116
```

## RHEL EUS and version-locking RHEL VMs

Extended Update Support (EUS) repositories are available to customers who may want to lock their RHEL VMs to a certain RHEL minor release after provisioning the VM. You can version-lock your RHEL VM to a specific minor version by updating the repositories to point to the Extended Update Support repositories. You can also undo the EUS version-locking operation.

#### NOTE

EUS is not supported on RHEL Extras. This means that if you are installing a package that is usually available from the RHEL Extras channel, you will not be able to do so while on EUS. The Red Hat Extras Product Life Cycle is detailed [here](#).

At the time of this writing, EUS support has ended for RHEL <= 7.4. See the "Red Hat Enterprise Linux Longer Support Add-Ons" section in the [Red Hat documentation](#) for more details.

- RHEL 7.4 EUS support ends August 31, 2019
- RHEL 7.5 EUS support ends April 30, 2020

- RHEL 7.6 EUS support ends October 31, 2020
- RHEL 7.7 EUS support ends August 30, 2021

## Switch a RHEL VM to EUS (version-lock to a specific minor version)

Use the following instructions to lock a RHEL VM to a particular minor release (run as root):

### NOTE

This only applies for RHEL versions for which EUS is available. At the time of this writing, this includes RHEL 7.2-7.7. More details are available at the [Red Hat Enterprise Linux Life Cycle](#) page.

1. Disable non-EUS repos:

```
yum --disablerepo='*' remove 'rhui-azure-rhel7'
```

2. Add EUS repos:

```
yum --config='https://rhelimage.blob.core.windows.net/repositories/rhui-microsoft-azure-rhel7-eus.config' install 'rhui-azure-rhel7-eus'
```

3. Lock the `releasever` variable (run as root):

```
echo $(. /etc/os-release && echo $VERSION_ID) > /etc/yum/vars/releasever
```

### NOTE

The above instruction will lock the RHEL minor release to the current minor release. Enter a specific minor release if you are looking to upgrade and lock to a later minor release that is not the latest. For example,

`echo 7.5 > /etc/yum/vars/releasever` will lock your RHEL version to RHEL 7.5

4. Update your RHEL VM

```
sudo yum update
```

## Switch a RHEL VM back to non-EUS (remove a version lock)

Run the following as root:

1. Remove the `releasever` file:

```
rm /etc/yum/vars/releasever
```

2. Disable EUS repos:

```
yum --disablerepo='*' remove 'rhui-azure-rhel7-eus'
```

3. Configure RHEL VM

```
yum --config='https://rhelimage.blob.core.windows.net/repositories/rhui-microsoft-azure-rhel7.config' install 'rhui-azure-rhel7'
```

#### 4. Update your RHEL VM

```
sudo yum update
```

## The IPs for the RHUI content delivery servers

RHUI is available in all regions where RHEL on-demand images are available. It currently includes all public regions listed on the [Azure status dashboard](#) page, Azure US Government, and Microsoft Azure Germany regions.

If you're using a network configuration to further restrict access from RHEL PAYG VMs, make sure the following IPs are allowed for `yum update` to work depending on the environment you're in:

```
Azure Global
13.91.47.76
40.85.190.91
52.187.75.218
52.174.163.213
52.237.203.198

Azure US Government
13.72.186.193
13.72.14.155
52.244.249.194

Azure Germany
51.5.243.77
51.4.228.145
```

## Azure RHUI Infrastructure

### Update expired RHUI client certificate on a VM

If you are using an older RHEL VM image, for example, RHEL 7.4 (image URN: `RedHat:RHEL:7.4:7.4.2018010506`), you will experience connectivity issues to RHUI due to a now-expired SSL client certificate. The error you see may look like "SSL peer rejected your certificate as expired" or "Error: Cannot retrieve repository metadata (repomd.xml) for repository: ... Please verify its path and try again". To overcome this problem, please update the RHUI client package on the VM using the following command:

```
sudo yum update -y --disablerepo='*' --enablerepo='*microsoft*'
```

Alternatively, running `sudo yum update` may also update the client certificate package (depending on your RHEL version), despite "expired SSL certificate" errors you will see for other repositories. If this update is successful, normal connectivity to other RHUI repositories should be restored, so you will be able to run `sudo yum update` successfully.

If you run into a 404 error while running a `yum update`, try the following to refresh your yum cache:

```
sudo yum clean all;
sudo yum makecache
```

### Troubleshoot connection problems to Azure RHUI

If you experience problems connecting to Azure RHUI from your Azure RHEL PAYG VM, follow these steps:

1. Inspect the VM configuration for the Azure RHUI endpoint:

- a. Check if the `/etc/yum.repos.d/rh-cloud.repo` file contains a reference to `rhui-[1-3].microsoft.com` in the `baseurl` of the `[rhui-microsoft-azure-rhel*]` section of the file. If it does, you're using the new Azure RHUI.
  - b. If it points to a location with the following pattern, `mirrorlist.*cds[1-4].cloudapp.net`, a configuration update is required. You're using the old VM snapshot, and you need to update it to point to the new Azure RHUI.
2. Access to Azure-hosted RHUI is limited to VMs within the [Azure datacenter IP ranges](#).
  3. If you're using the new configuration, have verified that the VM connects from the Azure IP range, and still can't connect to Azure RHUI, file a support case with Microsoft or Red Hat.

## Infrastructure update

In September 2016, we deployed an updated Azure RHUI. In April 2017, we shut down the old Azure RHUI. If you have been using the RHEL PAYG images (or their snapshots) from September 2016 or later, you're automatically connecting to the new Azure RHUI. If, however, you have older snapshots on your VMs, you need to manually update their configuration to access the Azure RHUI as described in a following section.

The new Azure RHUI servers are deployed with [Azure Traffic Manager](#). In Traffic Manager, a single endpoint (`rhui-1.microsoft.com`) can be used by any VM, regardless of region.

## Manual update procedure to use the Azure RHUI servers

This procedure is provided for reference only. RHEL PAYG images already have the correct configuration to connect to Azure RHUI. To manually update the configuration to use the Azure RHUI servers, complete the following steps:

- For RHEL 6:

```
yum --config='https://rhelimage.blob.core.windows.net/repositories/rhui-microsoft-azure-rhel6.config'
install 'rhui-azure-rhel6'
```

- For RHEL 7:

```
yum --config='https://rhelimage.blob.core.windows.net/repositories/rhui-microsoft-azure-rhel7.config'
install 'rhui-azure-rhel7'
```

- For RHEL 8:

1. Create a config file:

```
vi rhel8.config
```

2. Add the following content into the config file:

```
[rhui-microsoft-azure-rhel8]
name=Microsoft Azure RPMs for Red Hat Enterprise Linux 8
baseurl=https://rhui-1.microsoft.com/pulp/repos/microsoft-azure-rhel8 https://rhui-
2.microsoft.com/pulp/repos/microsoft-azure-rhel8 https://rhui-
3.microsoft.com/pulp/repos/microsoft-azure-rhel8
enabled=1
gpgcheck=1
gpgkey=https://rhelimage.blob.core.windows.net/repositories/RPM-GPG-KEY-microsoft-azure-release
sslverify=1
```

3. Save the file and run the following command:

```
dnf --config rhel8.config install 'rhui-azure-rhel8'
```

#### 4. Update your VM

```
sudo dnf update
```

## Next steps

- To create a Red Hat Enterprise Linux VM from an Azure Marketplace PAYG image and to use Azure-hosted RHUI, go to the [Azure Marketplace](#).
- To learn more about the Red Hat images in Azure, go to the [documentation page](#).
- Information on Red Hat support policies for all versions of RHEL can be found on the [Red Hat Enterprise Linux Life Cycle](#) page.

# Understanding and using the Azure Linux Agent

11/13/2019 • 7 minutes to read • [Edit Online](#)

The Microsoft Azure Linux Agent (waagent) manages Linux & FreeBSD provisioning, and VM interaction with the Azure Fabric Controller. In addition to the Linux Agent providing provisioning functionality, Azure also provides the option of using cloud-init for some Linux OSes. The Linux Agent provides the following functionality for Linux and FreeBSD IaaS deployments:

## NOTE

For more information, see the [README](#).

- **Image Provisioning**

- Creation of a user account
- Configuring SSH authentication types
- Deployment of SSH public keys and key pairs
- Setting the host name
- Publishing the host name to the platform DNS
- Reporting SSH host key fingerprint to the platform
- Resource Disk Management
- Formatting and mounting the resource disk
- Configuring swap space

- **Networking**

- Manages routes to improve compatibility with platform DHCP servers
- Ensures the stability of the network interface name

- **Kernel**

- Configures virtual NUMA (disable for kernel < 2.6.37 )
- Consumes Hyper-V entropy for /dev/random
- Configures SCSI timeouts for the root device (which could be remote)

- **Diagnostics**

- Console redirection to the serial port

- **SCVMM Deployments**

- Detects and bootstraps the VMM agent for Linux when running in a System Center Virtual Machine Manager 2012 R2 environment

- **VM Extension**

- Inject component authored by Microsoft and Partners into Linux VM (IaaS) to enable software and configuration automation
- VM Extension reference implementation on <https://github.com/Azure/azure-linux-extensions>

## Communication

The information flow from the platform to the agent occurs via two channels:

- A boot-time attached DVD for IaaS deployments. This DVD includes an OVF-compliant configuration file that includes all provisioning information other than the actual SSH keypairs.
- A TCP endpoint exposing a REST API used to obtain deployment and topology configuration.

## Requirements

The following systems have been tested and are known to work with the Azure Linux Agent:

### NOTE

This list may differ from the official list of supported systems on the Microsoft Azure Platform, as described here:

<https://support.microsoft.com/kb/2805216>

- CoreOS
- CentOS 6.3+
- Red Hat Enterprise Linux 6.7+
- Debian 7.0+
- Ubuntu 12.04+
- openSUSE 12.3+
- SLES 11 SP3+
- Oracle Linux 6.4+

Other Supported Systems:

- FreeBSD 10+ (Azure Linux Agent v2.0.10+)

The Linux agent depends on some system packages in order to function properly:

- Python 2.6+
- OpenSSL 1.0+
- OpenSSH 5.3+
- Filesystem utilities: sfdisk, fdisk, mkfs, parted
- Password tools: chpasswd, sudo
- Text processing tools: sed, grep
- Network tools: ip-route
- Kernel support for mounting UDF filesystems.

## Installation

Installation using an RPM or a DEB package from your distribution's package repository is the preferred method of installing and upgrading the Azure Linux Agent. All the [endorsed distribution providers](#) integrate the Azure Linux agent package into their images and repositories.

Refer to the documentation in the [Azure Linux Agent repo on GitHub](#) for advanced installation options, such as installing from source or to custom locations or prefixes.

## Command-Line Options

### Flags

- verbose: Increase verbosity of specified command
- force: Skip interactive confirmation for some commands

### Commands

- help: Lists the supported commands and flags.
- deprovision: Attempt to clean the system and make it suitable for reprovisioning. The following operation deletes:
  - All SSH host keys (if Provisioning.RegenerateSshHostKeyPair is 'y' in the configuration file)
  - Nameserver configuration in /etc/resolv.conf
  - Root password from /etc/shadow (if Provisioning.DeleteRootPassword is 'y' in the configuration file)
  - Cached DHCP client leases
  - Resets host name to localhost.localdomain

**WARNING**

Deprovisioning does not guarantee that the image is cleared of all sensitive information and suitable for redistribution.

- deprovision+user: Performs everything in -deprovision (above) and also deletes the last provisioned user account (obtained from /var/lib/waagent) and associated data. This parameter is when de-provisioning an image that was previously provisioning on Azure so it may be captured and reused.
- version: Displays the version of waagent
- serialconsole: Configures GRUB to mark ttyS0 (the first serial port) as the boot console. This ensures that kernel bootup logs are sent to the serial port and made available for debugging.
- daemon: Run waagent as a daemon to manage interaction with the platform. This argument is specified to waagent in the waagent init script.
- start: Run waagent as a background process

## Configuration

A configuration file (/etc/waagent.conf) controls the actions of waagent. The following shows a sample configuration file:

```
...
Provisioning.Enabled=y
Provisioning.DeleteRootPassword=
Provisioning.RegenerateSshHostKeyPair=y
Provisioning.SshHostKeyPairType=rsa
Provisioning.MonitorHostName=y
Provisioning.DecodeCustomData=n
Provisioning.ExecuteCustomData=
Provisioning.AllowResetSysUser=n
Provisioning.PasswordCryptId=6
Provisioning.PasswordCryptSaltLength=10
ResourceDisk.Format=y
ResourceDisk.Filesystem=ext4
ResourceDisk.MountPoint=/mnt/resource
ResourceDisk.MountOptions=None
ResourceDisk.EnableSwap=n
ResourceDisk.SwapSizeMB=0
LBProbeResponder=y
Logs.Verbose=n
OS.RootDeviceScsiTimeout=300
OS.OpensslPath=None
HttpProxy.Host=None
HttpProxy.Port=None
AutoUpdate.Enabled=y
...
```

The following various configuration options are described. Configuration options are of three types; Boolean,

String, or Integer. The Boolean configuration options can be specified as "y" or "n". The special keyword "None" may be used for some string type configuration entries as the following details:

#### **Provisioning.Enabled:**

Type: Boolean  
Default: y

This allows the user to enable or disable the provisioning functionality in the agent. Valid values are "y" or "n". If provisioning is disabled, SSH host and user keys in the image are preserved and any configuration specified in the Azure provisioning API is ignored.

#### **NOTE**

The `Provisioning.Enabled` parameter defaults to "n" on Ubuntu Cloud Images that use cloud-init for provisioning.

#### **Provisioning.DeleteRootPassword:**

Type: Boolean  
Default: n

If set, the root password in the /etc/shadow file is erased during the provisioning process.

#### **Provisioning.RegenerateSshHostKeyPair:**

Type: Boolean  
Default: y

If set, all SSH host key pairs (ecdsa, dsa, and rsa) are deleted during the provisioning process from /etc/ssh/. And a single fresh key pair is generated.

The encryption type for the fresh key pair is configurable by the `Provisioning.SshHostKeyPairType` entry. Some distributions re-create SSH key pairs for any missing encryption types when the SSH daemon is restarted (for example, upon a reboot).

#### **Provisioning.SshHostKeyPairType:**

Type: String  
Default: rsa

This can be set to an encryption algorithm type that is supported by the SSH daemon on the virtual machine. The typically supported values are "rsa", "dsa" and "ecdsa". "putty.exe" on Windows does not support "ecdsa". So, if you intend to use putty.exe on Windows to connect to a Linux deployment, use "rsa" or "dsa".

#### **Provisioning.MonitorHostName:**

Type: Boolean  
Default: y

If set, waagent monitors the Linux virtual machine for hostname changes (as returned by the "hostname" command) and automatically update the networking configuration in the image to reflect the change. In order to push the name change to the DNS servers, networking is restarted in the virtual machine. This results in brief loss of Internet connectivity.

## **Provisioning.DecodeCustomData**

Type: Boolean  
Default: n

If set, waagent decodes CustomData from Base64.

## **Provisioning.ExecuteCustomData**

Type: Boolean  
Default: n

If set, waagent executes CustomData after provisioning.

## **Provisioning.AllowResetSysUser**

Type: Boolean  
Default: n

This option allows the password for the sys user to be reset; default is disabled.

## **Provisioning.PasswordCryptId**

Type: String  
Default: 6

Algorithm used by crypt when generating password hash.

- 1 - MD5
- 2a - Blowfish
- 5 - SHA-256
- 6 - SHA-512

## **Provisioning.PasswordCryptSaltLength**

Type: String  
Default: 10

Length of random salt used when generating password hash.

## **ResourceDisk.Format:**

Type: Boolean  
Default: y

If set, the resource disk provided by the platform is formatted and mounted by waagent if the filesystem type requested by the user in "ResourceDisk.Filesystem" is anything other than "ntfs". A single partition of type Linux (83) is made available on the disk. This partition is not formatted if it can be successfully mounted.

## **ResourceDisk.Filesystem:**

Type: String  
Default: ext4

This specifies the filesystem type for the resource disk. Supported values vary by Linux distribution. If the string is X, then mkfs.X should be present on the Linux image. SLES 11 images should typically use 'ext3'. FreeBSD images should use 'ufs2' here.

#### **ResourceDisk.MountPoint:**

```
Type: String
Default: /mnt/resource
```

This specifies the path at which the resource disk is mounted. The resource disk is a *temporary* disk, and might be emptied when the VM is deprovisioned.

#### **ResourceDisk.MountOptions**

```
Type: String
Default: None
```

Specifies disk mount options to be passed to the mount -o command. This is a comma-separated list of values, ex. 'nodev,nosuid'. See mount(8) for details.

#### **ResourceDisk.EnableSwap:**

```
Type: Boolean
Default: n
```

If set, a swap file (/swapfile) is created on the resource disk and added to the system swap space.

#### **ResourceDisk.SwapSizeMB:**

```
Type: Integer
Default: 0
```

The size of the swap file in megabytes.

#### **Logs.Verbose:**

```
Type: Boolean
Default: n
```

If set, log verbosity is boosted. Waagent logs to /var/log/waagent.log and utilizes the system logrotate functionality to rotate logs.

#### **OS.EnableRDMA**

```
Type: Boolean
Default: n
```

If set, the agent attempts to install and then load an RDMA kernel driver that matches the version of the firmware on the underlying hardware.

#### **OS.RootDeviceScsiTimeout:**

Type: Integer  
Default: 300

This setting configures the SCSI timeout in seconds on the OS disk and data drives. If not set, the system defaults are used.

#### **OS.OpensslPath:**

Type: String  
Default: None

This setting can be used to specify an alternate path for the openssl binary to use for cryptographic operations.

#### **HttpProxy.Host, HttpProxy.Port**

Type: String  
Default: None

If set, the agent uses this proxy server to access the internet.

#### **AutoUpdate.Enabled**

Type: Boolean  
Default: y

Enable or disable auto-update for goal state processing; default is enabled.

## Ubuntu Cloud Images

Ubuntu Cloud Images utilize [cloud-init](#) to perform many configuration tasks that would otherwise be managed by the Azure Linux Agent. The following differences apply:

- **Provisioning.Enabled** defaults to "n" on Ubuntu Cloud Images that use cloud-init to perform provisioning tasks.
- The following configuration parameters have no effect on Ubuntu Cloud Images that use cloud-init to manage the resource disk and swap space:
  - **ResourceDisk.Format**
  - **ResourceDisk.Filesystem**
  - **ResourceDisk.MountPoint**
  - **ResourceDisk.EnableSwap**
  - **ResourceDisk.SwapSizeMB**
- For more information, see the following resources to configure the resource disk mount point and swap space on Ubuntu Cloud Images during provisioning:
  - [Ubuntu Wiki: Configure Swap Partitions](#)
  - [Injecting Custom Data into an Azure Virtual Machine](#)

2 minutes to read

# Guidance for mitigating speculative execution side-channel vulnerabilities in Azure

11/13/2019 • 7 minutes to read • [Edit Online](#)

**Last document update:** 12 November 2019 10:00 AM PST.

The disclosure of a [new class of CPU vulnerabilities](#) known as speculative execution side-channel attacks has resulted in questions from customers seeking more clarity.

Microsoft has deployed mitigations across all our cloud services. The infrastructure that runs Azure and isolates customer workloads from each other is protected. This means that a potential attacker using the same infrastructure can't attack your application using these vulnerabilities.

Azure is using [memory preserving maintenance](#) whenever possible, to minimize customer impact and eliminate the need for reboots. Azure will continue utilizing these methods when making systemwide updates to the host and protect our customers.

More information about how security is integrated into every aspect of Azure is available on the [Azure Security Documentation](#) site.

## NOTE

Since this document was first published, multiple variants of this vulnerability class have been disclosed. Microsoft continues to be heavily invested in protecting our customers and providing guidance. This page will be updated as we continue to release further fixes.

On November 12, 2019, [Intel published](#) a technical advisory around Intel® Transactional Synchronization Extensions (Intel® TSX) Transaction Asynchronous Abort (TAA) vulnerability that is assigned [CVE-2019-11135](#). This vulnerability affects Intel® Core® processors and Intel® Xeon® processors. Microsoft Azure has released operating system updates and is deploying new microcode, as it is made available by Intel, throughout our fleet to protect our customers against these new vulnerabilities. Azure is closely working with Intel to test and validate the new microcode prior to its official release on the platform.

**Customers that are running untrusted code within their VM** need to take action to protect against these vulnerabilities by reading below for additional guidance on all speculative execution side-channel vulnerabilities (Microsoft Advisories ADV 180002, 180018, and 190013).

Other customers should evaluate these vulnerabilities from a Defense in Depth perspective and consider the security and performance implications of their chosen configuration.

## Keeping your operating systems up-to-date

While an OS update is not required to isolate your applications running on Azure from other Azure customers, it is always a best practice to keep your software up-to-date. The latest Security Rollups for Windows contain mitigations for several speculative execution side channel vulnerabilities. Similarly, Linux distributions have released multiple updates to address these vulnerabilities. Here are our recommended actions to update your operating system:

| OFFERING             | RECOMMENDED ACTION                                                                |
|----------------------|-----------------------------------------------------------------------------------|
| Azure Cloud Services | Enable <a href="#">auto update</a> or ensure you are running the newest Guest OS. |

| OFFERING                       | RECOMMENDED ACTION                                                                                                           |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Azure Linux Virtual Machines   | Install updates from your operating system provider. For more information, see <a href="#">Linux</a> later in this document. |
| Azure Windows Virtual Machines | Install the latest security rollup.                                                                                          |
| Other Azure PaaS Services      | There is no action needed for customers using these services. Azure automatically keeps your OS versions up-to-date.         |

## Additional guidance if you are running untrusted code

Customers who allow untrusted users to execute arbitrary code may wish to implement some additional security features inside their Azure Virtual Machines or Cloud Services. These features protect against the intra-process disclosure vectors that several speculative execution vulnerabilities describe.

Example scenarios where additional security features are recommended:

- You allow code that you do not trust to run inside your VM.
  - *For example, you allow one of your customers to upload a binary or script that you then execute within your application.*
- You allow users that you do not trust to log into your VM using low privileged accounts.
  - *For example, you allow a low-privileged user to log into one of your VMs using remote desktop or SSH.*
- You allow untrusted users access to virtual machines implemented via nested virtualization.
  - *For example, you control the Hyper-V host, but allocate the VMs to untrusted users.*

Customers who do not implement a scenario involving untrusted code do not need to enable these additional security features.

## Enabling additional security

You can enable additional security features inside your VM or Cloud Service if you are running untrusted code. In parallel, ensure your operating system is up-to-date to enable security features inside your VM or Cloud Service

### Windows

Your target operating system must be up-to-date to enable these additional security features. While numerous speculative execution side channel mitigations are enabled by default, the additional features described here must be enabled manually and may cause a performance impact.

**Step 1: Disable hyper-threading on the VM** - Customers running untrusted code on a hyper-threaded VM will need to disable hyper-threading or move to a non-hyper-threaded VM size. Reference [this doc](#) for a list of hyper-threaded VM sizes (where ratio of vCPU to Core is 2:1). To check if your VM has hyper-threading enabled, please refer to the below script using the Windows command line from within the VM.

Type `wmic` to enter the interactive interface. Then type the below to view the amount of physical and logical processors on the VM.

```
CPU Get NumberOfCores,NumberOfLogicalProcessors /Format:List
```

If the number of logical processors is greater than physical processors (cores), then hyper-threading is enabled. If you are running a hyper-threaded VM, please [contact Azure Support](#) to get hyper-threading disabled. Once hyper-

threading is disabled, **support will require a full VM reboot**. Please refer to [Core count](#) to understand why your VM core count decreased.

**Step 2:** In parallel to Step 1, follow the instructions in [KB4072698](#) to verify protections are enabled using the [SpeculationControl](#) PowerShell module.

**NOTE**

If you previously downloaded this module, you will need to install the newest version.

The output of the PowerShell script should have the below values to validate enabled protections against these vulnerabilities:

```
Windows OS support for branch target injection mitigation is enabled: True
Windows OS support for kernel VA shadow is enabled: True
Windows OS support for speculative store bypass disable is enabled system-wide: False
Windows OS support for L1 terminal fault mitigation is enabled: True
Windows OS support for MDS mitigation is enabled: True
Windows OS support for TAA mitigation is enabled: True
```

If the output shows `MDS mitigation is enabled: False`, please [contact Azure Support](#) for available mitigation options.

**Step 3:** To enable Kernel Virtual Address Shadowing (KVAS) and Branch Target Injection (BTI) OS support, follow the instructions in [KB4072698](#) to enable protections using the [Session Manager](#) registry keys. A reboot is required.

**Step 4:** For deployments that are using [nested virtualization](#) (D3 and E3 only): These instructions apply inside the VM you are using as a Hyper-V host.

1. Follow the instructions in [KB4072698](#) to enable protections using the [MinVmVersionForCpuBasedMitigations](#) registry keys.
2. Set the hypervisor scheduler type to `Core` by following the instructions [here](#).

## Linux

Enabling the set of additional security features inside requires that the target operating system be fully up-to-date. Some mitigations will be enabled by default. The following section describes the features which are off by default and/or reliant on hardware support (microcode). Enabling these features may cause a performance impact. Reference your operating system provider's documentation for further instructions

**Step 1: Disable hyper-threading on the VM** - Customers running untrusted code on a hyper-threaded VM will need to disable hyper-threading or move to a non-hyper-threaded VM. Reference [this doc](#) for a list of hyper-threaded VM sizes (where ratio of vCPU to Core is 2:1). To check if you are running a hyper-threaded VM, run the `lscpu` command in the Linux VM.

If `Thread(s) per core = 2`, then hyper-threading has been enabled.

If `Thread(s) per core = 1`, then hyper-threading has been disabled.

Sample output for a VM with hyper-threading enabled:

|                      |                |
|----------------------|----------------|
| CPU Architecture:    | x86_64         |
| CPU op-mode(s):      | 32-bit, 64-bit |
| Byte Order:          | Little Endian  |
| CPU(s):              | 8              |
| On-line CPU(s) list: | 0-7            |
| Thread(s) per core:  | 2              |
| Core(s) per socket:  | 4              |
| Socket(s):           | 1              |
| NUMA node(s):        | 1              |

If you are running a hyper-threaded VM, please [contact Azure Support](#) to get hyper-threading disabled. Once hyper-threading is disabled, **support will require a full VM reboot**. Please refer to [Core count](#) to understand why your VM core count decreased.

**Step 2:** To mitigate against any of the below speculative execution side-channel vulnerabilities, refer to your operating system provider's documentation:

- [Redhat and CentOS](#)
- [SUSE](#)
- [Ubuntu](#)

#### Core count

When a hyper-threaded VM is created, Azure allocates 2 threads per core - these are called vCPUs. When hyper-threading is disabled, Azure removes a thread and surfaces up single threaded cores (physical cores). The ratio of vCPU to CPU is 2:1, so once hyper-threading is disabled, the CPU count in the VM will appear to have decreased by half. For example, a D8\_v3 VM is a hyper-threaded VM running on 8 vCPUs (2 threads per core x 4 cores).

When hyper-threading is disabled, CPUs will drop to 4 physical cores with 1 thread per core.

## Next steps

This article provides guidance to the below speculative execution side-channel attacks that affect many modern processors:

#### Spectre Meltdown:

- CVE-2017-5715 - Branch Target Injection (BTI)
- CVE-2017-5754 - Kernel Page Table Isolation (KPTI)
- CVE-2018-3639 – Speculative Store Bypass (KPTI)
- [CVE-2019-1125](#) – Windows Kernel Information – variant of Spectre Variant 1

#### L1 Terminal Fault (L1TF):

- CVE-2018-3615 - Intel Software Guard Extensions (Intel SGX)
- CVE-2018-3620 - Operating Systems (OS) and System Management Mode (SMM)
- CVE-2018-3646 – impacts Virtual Machine Manager (VMM)

#### Microarchitectural Data Sampling:

- CVE-2019-11091 - Microarchitectural Data Sampling Uncacheable Memory (MDSUM)
- CVE-2018-12126 - Microarchitectural Store Buffer Data Sampling (MSBDS)
- CVE-2018-12127 - Microarchitectural Load Port Data Sampling (MLPDS)
- CVE-2018-12130 - Microarchitectural Fill Buffer Data Sampling (MFBDS)

Transactional Synchronization Extensions (Intel® TSX) Transaction Asynchronous Abort:

- [CVE-2019-11135](#) – TSX Transaction Asynchronous Abort (TAA)



# Azure Instance Metadata service

2/25/2020 • 20 minutes to read • [Edit Online](#)

The Azure Instance Metadata Service (IMDS) provides information about currently running virtual machine instances and can be used to manage and configure your virtual machines. Information provided includes the SKU, network configuration, and upcoming maintenance events. For a complete list of the data that is available, see [metadata APIs](#).

Azure's Instance Metadata Service is a REST Endpoint accessible to all IaaS VMs created via the [Azure Resource Manager](#). The endpoint is available at a well-known non-routable IP address ( 169.254.169.254 ) that can be accessed only from within the VM.

## IMPORTANT

This service is **generally available** in all Azure Regions. It regularly receives updates to expose new information about virtual machine instances. This page reflects the up-to-date [metadata APIs](#) available.

## Service availability

The service is available in generally available Azure regions. Not all API version may be available in all Azure Regions.

| REGIONS                                      | AVAILABILITY?       | SUPPORTED VERSIONS                                                                                                                                         |
|----------------------------------------------|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All Generally Available Global Azure Regions | Generally Available | 2017-04-02, 2017-08-01, 2017-12-01, 2018-02-01, 2018-04-02, 2018-10-01, 2019-02-01, 2019-03-11, 2019-04-30, 2019-06-01, 2019-06-04, 2019-08-01, 2019-08-15 |
| Azure Government                             | Generally Available | 2017-04-02, 2017-08-01, 2017-12-01, 2018-02-01, 2018-04-02, 2018-10-01, 2019-02-01, 2019-03-11, 2019-04-30, 2019-06-01, 2019-06-04, 2019-08-01, 2019-08-15 |
| Azure China 21Vianet                         | Generally Available | 2017-04-02, 2017-08-01, 2017-12-01, 2018-02-01, 2018-04-02, 2018-10-01, 2019-02-01, 2019-03-11, 2019-04-30, 2019-06-01, 2019-06-04, 2019-08-01, 2019-08-15 |
| Azure Germany                                | Generally Available | 2017-04-02, 2017-08-01, 2017-12-01, 2018-02-01, 2018-04-02, 2018-10-01, 2019-02-01, 2019-03-11, 2019-04-30, 2019-06-01, 2019-06-04, 2019-08-01, 2019-08-15 |

The version 2019-11-01 is currently getting deployed and may not be available in all regions.

This table is updated when there are service updates and/or new supported versions are available.

To try out the Instance Metadata Service, create a VM from [Azure Resource Manager](#) or the [Azure portal](#) in the

above regions and follow the examples below. Further examples of how to query IMDS can be found at [Azure Instance Metadata Samples](#)

## Usage

### Versioning

The Instance Metadata Service is versioned, and specifying the API version in the HTTP request is mandatory.

You can see the newest versions listed in this [availability table](#).

As newer versions are added, older versions can still be accessed for compatibility if your scripts have dependencies on specific data formats.

When no version is specified, an error is returned with a list of the newest supported versions.

#### NOTE

The response is a JSON string. The following example response is pretty-printed for readability.

### Request

```
curl -H Metadata:true "http://169.254.169.254/metadata/instance"
```

### Response

```
{
 "error": "Bad request. api-version was not specified in the request. For more information refer to
aka.ms/azureimds",
 "newest-versions": [
 "2018-10-01",
 "2018-04-02",
 "2018-02-01"
]
}
```

### Using headers

When you query the Instance Metadata Service, you must provide the header `Metadata: true` to ensure the request was not unintentionally redirected.

### Retrieving metadata

Instance metadata is available for running VMs created/managed using [Azure Resource Manager](#). Access all data categories for a virtual machine instance using the following request:

```
curl -H Metadata:true "http://169.254.169.254/metadata/instance?api-version=2017-08-01"
```

#### NOTE

All instance metadata queries are case-sensitive.

### Data output

By default, the Instance Metadata Service returns data in JSON format (`Content-Type: application/json`).

However, different APIs return data in different formats if requested. The following table is a reference of other data formats APIs may support.

| API              | DEFAULT DATA FORMAT | OTHER FORMATS |
|------------------|---------------------|---------------|
| /instance        | json                | text          |
| /scheduledevents | json                | none          |
| /attested        | json                | none          |

To access a non-default response format, specify the requested format as a query string parameter in the request. For example:

```
curl -H Metadata:true "http://169.254.169.254/metadata/instance?api-version=2017-08-01&format=text"
```

#### NOTE

For leaf nodes the `format=json` doesn't work. For these queries `format=text` needs to be explicitly specified if the default format is json.

## Security

The Instance Metadata Service endpoint is accessible only from within the running virtual machine instance on a non-routable IP address. In addition, any request with a `X-Forwarded-For` header is rejected by the service.

Requests must also contain a `Metadata: true` header to ensure that the actual request was directly intended and not a part of unintentional redirection.

## Error

If there is a data element not found or a malformed request, the Instance Metadata Service returns standard HTTP errors. For example:

| HTTP STATUS CODE       | REASON                                                                                     |
|------------------------|--------------------------------------------------------------------------------------------|
| 200 OK                 |                                                                                            |
| 400 Bad Request        | Missing <code>Metadata: true</code> header or missing the format when querying a leaf node |
| 404 Not Found          | The requested element doesn't exist                                                        |
| 405 Method Not Allowed | Only <code>GET</code> requests are supported                                               |
| 410 Gone               | Retry after some time for a max of 70 seconds                                              |
| 429 Too Many Requests  | The API currently supports a maximum of 5 queries per second                               |
| 500 Service Error      | Retry after some time                                                                      |

## Examples

#### NOTE

All API responses are JSON strings. All following example responses are pretty-printed for readability.

## Retrieving network information

### Request

```
curl -H Metadata:true "http://169.254.169.254/metadata/instance/network?api-version=2017-08-01"
```

### Response

#### NOTE

The response is a JSON string. The following example response is pretty-printed for readability.

```
{
 "interface": [
 {
 "ipv4": {
 "ipAddress": [
 {
 "privateIpAddress": "10.1.0.4",
 "publicIpAddress": "X.X.X.X"
 }
],
 "subnet": [
 {
 "address": "10.1.0.0",
 "prefix": "24"
 }
]
 },
 "ipv6": {
 "ipAddress": []
 },
 "macAddress": "000D3AF806EC"
 }
]
}
```

## Retrieving public IP address

```
curl -H Metadata:true "http://169.254.169.254/metadata/instance/network/interface/0/ipv4/ipAddress/0/publicIpAddress?api-version=2017-08-01&format=text"
```

## Retrieving all metadata for an instance

### Request

```
curl -H Metadata:true "http://169.254.169.254/metadata/instance?api-version=2019-06-01"
```

### Response

#### NOTE

The response is a JSON string. The following example response is pretty-printed for readability.

```
{
 "compute": {
 "azEnvironment": "AzurePublicCloud",
```

```
"customData": "",
"location": "centralus",
"name": "negasonic",
"offer": "lampstack",
"osType": "Linux",
"placementGroupId": "",
"plan": {
 "name": "5-6",
 "product": "lampstack",
 "publisher": "bitnami"
},
"platformFaultDomain": "0",
"platformUpdateDomain": "0",
"provider": "Microsoft.Compute",
"publicKeys": [],
"publisher": "bitnami",
"resourceGroupName": "myrg",
"resourceId": "/subscriptions/xxxxx-xxxx-xxxx-xxxx-xxxx-
xxxxxxxxxx/resourceGroups/myrg/providers/Microsoft.Compute/virtualMachines/negasonic",
"sku": "5-6",
"storageProfile": {
 "dataDisks": [
 {
 "caching": "None",
 "createOption": "Empty",
 "diskSizeGB": "1024",
 "image": {
 "uri": ""
 },
 "lun": "0",
 "managedDisk": {
 "id": "/subscriptions/xxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx/resourceGroups/macikgo-test-may-
23/providers/Microsoft.Compute/disks/exampledataldiskname",
 "storageAccountType": "Standard_LRS"
 },
 "name": "exampledataldiskname",
 "vhd": {
 "uri": ""
 },
 "writeAcceleratorEnabled": "false"
 }
],
 "imageReference": {
 "id": "",
 "offer": "UbuntuServer",
 "publisher": "Canonical",
 "sku": "16.04.0-LTS",
 "version": "latest"
 },
 "osDisk": {
 "caching": "ReadWrite",
 "createOption": "FromImage",
 "diskSizeGB": "30",
 "diffDiskSettings": {
 "option": "Local"
 },
 "encryptionSettings": {
 "enabled": "false"
 },
 "image": {
 "uri": ""
 },
 "managedDisk": {
 "id": "/subscriptions/xxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx/resourceGroups/macikgo-test-may-
23/providers/Microsoft.Compute/disks/exampleosdiskname",
 "storageAccountType": "Standard_LRS"
 },
 "name": "exampleosdiskname",
 "osType": "Linux"
 }
}
```

```

 "osType": "Linux",
 "vhd": {
 "uri": ""
 },
 "writeAcceleratorEnabled": "false"
}
},
"subscriptionId": "xxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx",
"tags": "Department:IT;Environment:Prod;Role:WorkerRole",
"version": "7.1.1902271506",
"vmId": "13f56399-bd52-4150-9748-7190aae1ff21",
"vmScaleSetName": "",
"vmSize": "Standard_A1_v2",
"zone": "1"
},
"network": {
 "interface": [
 {
 "ipv4": {
 "ipAddress": [
 {
 "privateIpAddress": "10.1.2.5",
 "publicIpAddress": "X.X.X.X"
 }
],
 "subnet": [
 {
 "address": "10.1.2.0",
 "prefix": "24"
 }
]
 },
 "ipv6": {
 "ipAddress": []
 },
 "macAddress": "000D3A36DDED"
 }
]
}
}

```

## Retrieving metadata in Windows Virtual Machine

### Request

Instance metadata can be retrieved in Windows via the PowerShell utility `curl`:

```
curl -H @{'Metadata'='true'} http://169.254.169.254/metadata/instance?api-version=2019-06-01 | select -ExpandProperty Content
```

Or through the `Invoke-RestMethod` cmdlet:

```
Invoke-RestMethod -Headers @{"Metadata"="true"} -URI http://169.254.169.254/metadata/instance?api-version=2019-06-01 -Method get
```

### Response

#### NOTE

The response is a JSON string. The following example response is pretty-printed for readability.

```
{
```

```
"compute": {
 "azEnvironment": "AzurePublicCloud",
 "customData": "",
 "location": "centralus",
 "name": "negasonic",
 "offer": "lampstack",
 "osType": "Linux",
 "placementGroupId": "",
 "plan": {
 "name": "5-6",
 "product": "lampstack",
 "publisher": "bitnami"
 },
 "platformFaultDomain": "0",
 "platformUpdateDomain": "0",
 "provider": "Microsoft.Compute",
 "publicKeys": [],
 "publisher": "bitnami",
 "resourceGroupName": "myrg",
 "resourceId": "/subscriptions/xxxxx-xxxx-xxxx-xxxx-xxxx-
xxxxxxxx/resourceGroups/myrg/providers/Microsoft.Compute/virtualMachines/negasonic",
 "sku": "5-6",
 "storageProfile": {
 "dataDisks": [
 {
 "caching": "None",
 "createOption": "Empty",
 "diskSizeGB": "1024",
 "image": {
 "uri": ""
 },
 "lun": "0",
 "managedDisk": {
 "id": "/subscriptions/xxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx/resourceGroups/macikgo-test-may-
23/providers/Microsoft.Compute/disks/exampledatadiskname",
 "storageAccountType": "Standard_LRS"
 },
 "name": "exampledatadiskname",
 "vhd": {
 "uri": ""
 },
 "writeAcceleratorEnabled": "false"
 }
],
 "imageReference": {
 "id": "",
 "offer": "UbuntuServer",
 "publisher": "Canonical",
 "sku": "16.04.0-LTS",
 "version": "latest"
 },
 "osDisk": {
 "caching": "ReadWrite",
 "createOption": "FromImage",
 "diskSizeGB": "30",
 "diffDiskSettings": {
 "option": "Local"
 },
 "encryptionSettings": {
 "enabled": "false"
 },
 "image": {
 "uri": ""
 },
 "managedDisk": {
 "id": "/subscriptions/xxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx/resourceGroups/macikgo-test-may-
23/providers/Microsoft.Compute/disks/exampleosdiskname",
 "storageAccountType": "Standard_LRS"
 }
 }
 }
}
```

```

 },
 "name": "exampleosdiskname",
 "osType": "Linux",
 "vhd": {
 "uri": ""
 },
 "writeAcceleratorEnabled": "false"
 }
},
"subscriptionId": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx",
"tags": "Department:IT;Environment:Test;Role:WebRole",
"version": "7.1.1902271506",
"vmId": "13f56399-bd52-4150-9748-7190aae1ff21",
"vmScaleSetName": "",
"vmSize": "Standard_A1_v2",
"zone": "1"
},
"network": {
 "interface": [
 {
 "ipv4": {
 "ipAddress": [
 {
 "privateIpAddress": "10.0.1.4",
 "publicIpAddress": "X.X.X.X"
 }
],
 "subnet": [
 {
 "address": "10.0.1.0",
 "prefix": "24"
 }
]
 },
 "ipv6": {
 "ipAddress": []
 },
 "macAddress": "002248020E1E"
 }
]
}
}

```

## Metadata APIs

The following APIs are available through the metadata endpoint:

| DATA            | DESCRIPTION                                                                            | VERSION INTRODUCED |
|-----------------|----------------------------------------------------------------------------------------|--------------------|
| attested        | See <a href="#">Attested Data</a>                                                      | 2018-10-01         |
| identity        | Managed identities for Azure resources.<br>See <a href="#">acquire an access token</a> | 2018-02-01         |
| instance        | See <a href="#">Instance API</a>                                                       | 2017-04-02         |
| scheduledevents | See <a href="#">Scheduled Events</a>                                                   | 2017-08-01         |

### Instance API

The following Compute categories are available through the Instance API:

**NOTE**

Through the metadata endpoint, the following categories are accessed through instance/compute

| DATA                 | DESCRIPTION                                                                                               | VERSION INTRODUCED |
|----------------------|-----------------------------------------------------------------------------------------------------------|--------------------|
| azEnvironment        | Azure Environment where the VM is running in                                                              | 2018-10-01         |
| customData           | This feature is currently disabled, and we will update this documentation when it becomes available       | 2019-02-01         |
| location             | Azure Region the VM is running in                                                                         | 2017-04-02         |
| name                 | Name of the VM                                                                                            | 2017-04-02         |
| offer                | Offer information for the VM image and is only present for images deployed from Azure image gallery       | 2017-04-02         |
| osType               | Linux or Windows                                                                                          | 2017-04-02         |
| placementGroupId     | <a href="#">Placement Group</a> of your virtual machine scale set                                         | 2017-08-01         |
| plan                 | <a href="#">Plan</a> containing name, product, and publisher for a VM if it is an Azure Marketplace Image | 2018-04-02         |
| platformUpdateDomain | <a href="#">Update domain</a> the VM is running in                                                        | 2017-04-02         |
| platformFaultDomain  | <a href="#">Fault domain</a> the VM is running in                                                         | 2017-04-02         |
| provider             | Provider of the VM                                                                                        | 2018-10-01         |
| publicKeys           | <a href="#">Collection of Public Keys</a> assigned to the VM and paths                                    | 2018-04-02         |
| publisher            | Publisher of the VM image                                                                                 | 2017-04-02         |
| resourceGroupName    | <a href="#">Resource group</a> for your Virtual Machine                                                   | 2017-08-01         |
| resourceId           | The <a href="#">fully qualified</a> ID of the resource                                                    | 2019-03-11         |
| sku                  | Specific SKU for the VM image                                                                             | 2017-04-02         |
| storageProfile       | See <a href="#">Storage Profile</a>                                                                       | 2019-06-01         |
| subscriptionId       | Azure subscription for the Virtual Machine                                                                | 2017-08-01         |

| DATA           | DESCRIPTION                                                      | VERSION INTRODUCED |
|----------------|------------------------------------------------------------------|--------------------|
| tags           | Tags for your Virtual Machine                                    | 2017-08-01         |
| tagsList       | Tags formatted as a JSON array for easier programmatic parsing   | 2019-06-04         |
| version        | Version of the VM image                                          | 2017-04-02         |
| vmId           | Unique identifier for the VM                                     | 2017-04-02         |
| vmScaleSetName | Virtual machine scale set Name of your virtual machine scale set | 2017-12-01         |
| vmSize         | VM size                                                          | 2017-04-02         |
| zone           | Availability Zone of your virtual machine                        | 2017-12-01         |

The following Network categories are available through the Instance API:

#### NOTE

Through the metadata endpoint, the following categories are accessed through instance/network/interface

| DATA                  | DESCRIPTION                   | VERSION INTRODUCED |
|-----------------------|-------------------------------|--------------------|
| ipv4/privateIpAddress | Local IPv4 address of the VM  | 2017-04-02         |
| ipv4/publicIpAddress  | Public IPv4 address of the VM | 2017-04-02         |
| subnet/address        | Subnet address of the VM      | 2017-04-02         |
| subnet/prefix         | Subnet prefix, example 24     | 2017-04-02         |
| ipv6/ipAddress        | Local IPv6 address of the VM  | 2017-04-02         |
| macAddress            | VM mac address                | 2017-04-02         |

## Attested Data

Part of the scenario served by Instance Metadata Service is to provide guarantees that the data provided is coming from Azure. We sign part of this information so that marketplace images can be sure that it's their image running on Azure.

#### Example Attested Data

#### NOTE

All API responses are JSON strings. The following example responses are pretty-printed for readability.

#### Request

```
curl -H Metadata:true "http://169.254.169.254/metadata/attested/document?api-version=2018-10-01&nonce=1234567890"
```

Api-version is a mandatory field. Refer to the [service availability section](#) for supported API versions.Nonce is an optional 10-digit string. If not provided, IMDS returns the current UTC timestamp in its place. Due to IMDS's caching mechanism, a previously cached nonce value may be returned.

## Response

### NOTE

The response is a JSON string. The following example response is pretty-printed for readability.

```
{
 "encoding": "pkcs7", "signature": "MIIEEgYJKoZIhvcNAQcCoIIIEAzCCA/8CAQExDzANBqkqhkiG9w0BAQsFADCBugYJKoZIhvcNAQcBoIG
sBIGpeyJub25jZSI6IjEyMzQ1NjY3NjYiLCJwbGFuIjp7Im5hbWUiOiiIiLCJwcm9kdWN0IjoiIiwicHVibGlzaGVyIjoiIn0sInRpWVtGftC
I6eyJcmVhdGVkT24i0iIxMS8yMC8xOCAYMjowNzozOSAtMDAwMCIsImV4cGlyZXNPbiI6IjExLzIwLzE4IDIy0jA40jI0IC0wMDAwIn0sInZts
WQioiIifaCCAj8wggi7MIIIBpKADAgECAhBnxW5Kh8ds1eBA0E2mIBJ0MA0GCSqGSiB3DQEBAUAMCsxKTAnBgNVBAMTIHr1c3RzdWJkb21haW4u
bWV0YWRhdGEuYXp1cmUuY29tMB4XDTE4MTExMDIxNTc1N1oXDTE4MTIyMDIxNTc1NlowKzEpMCCGA1UEAxMgdGVzdHN1YmRvbWFpb15tZXrhZGF
0Y55henVyZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAML/tBo86ENWPzmXZ0kPkX5dY5QZ150mA8lommszE71x2sCLonzv4/UWk4
H+jMMWRRwIea2CuQ5RhdWAhvKq6if4okKnt66fxm+YTVz9z0CTfClmLT+nsdf0ASG1xZppEapC0Cd9vD6NCKyE8aYI1pliaeOnFjG0WvMY04uWz
2MdAgMBAAGjYDBeMFwGA1UdAQRMFOAENnYkHLa04Ut4Mpt7TkJFfyhLTArMSkwJwYDVQQDEyB0ZXM0c3ViZG9tYWluLm1ldGfkYXRhLmF6dXJ1
LmNvbYIQZ8VuSoFhbJRAQNBnpiASdDANBqkqhkiG9w0BAQQFAAOBgQCLSM6aX5Bs1KHCJp4VQtzXF71rVKCocHy3N9PTJQ9Fpnd+bYw2vSpQ
Hg/Aig82WuDFpReJvr7Pa938mZqW9HUOGjQKK2FYDTg6fXD8pkPdygh1X5boGWAMMr7bfkup+lsT+n2tRw2wbNkn01tQ0wICtqy2VqzWwLi45
RBwTGB6DCB5QIBATA/MCsxKTAnBgNVBAMTIHr1c3RzdWJkb21haW4ubW0YWRhdGEuYXp1cmUuY29tAhBnxW5Kh8ds1eBA0E2mIBJ0MA0GCSqGS
Ib3DQEBCwUAMA0GCSqGSiB3DQEBAQUABIGA1d1BM/yYIqqv8SDE4kjQo3U1/IKAVR8ETKcve5BAdGSNkTUooUGVniTXeuvDj5Nkmaz0aKZp9fEt
ByqqPOyw/n1XaZg0044HDGiPUJ90xVYmfeK6p9RpJBu6kiKhnnYTelUk5u75phe5ZbMZfBhuPhXmYAdjc7Nmw97nx8NnprQ="}
}
```

The signature blob is a [pkcs7](#) signed version of document. It contains the certificate used for signing along with the VM details like vmId, sku, nonce, subscriptionId, timeStamp for creation and expiry of the document and the plan information about the image. The plan information is only populated for Azure Market place images. The certificate can be extracted from the response and used to validate that the response is valid and is coming from Azure.

## Retrieving attested metadata in Windows Virtual Machine

### Request

Instance metadata can be retrieved in Windows via the PowerShell utility `curl`:

```
curl -H @{"Metadata"='true'} "http://169.254.169.254/metadata/attested/document?api-version=2018-10-01&nonce=1234567890" | select -ExpandProperty Content
```

Or through the `Invoke-RestMethod` cmdlet:

```
Invoke-RestMethod -Headers @{"Metadata"="true"} -URI "http://169.254.169.254/metadata/attested/document?api-version=2018-10-01&nonce=1234567890" -Method get
```

Api-version is a mandatory field. Refer to the service availability section for supported API versions.Nonce is an optional 10-digit string. If not provided, IMDS returns the current UTC timestamp in its place. Due to IMDS's caching mechanism, a previously cached nonce value may be returned.

## Response

## NOTE

The response is a JSON string. The following example response is pretty-printed for readability.

```
{
 "encoding": "pkcs7", "signature": "MIIEGyJkoZihvcNAQcCoIEAzCCA/8CAQExDzANBgkqhkiG9w0BAQsFADCBugYJKoZihvcNAQcBoIG
sBIGpeyJub25jZSI6IjEyMzQ1NjY3NjYiLCJwbGFuIjp7Im5hbWUiOiiLCJwcm9kdWN0IjoiIiwicHvibGlzaGVyIjoiIn0sInRpbwTdgFtcC
I6eyJjcmVhdGVkT24i0iIxMS8yMC8xOCAYMjowNzozOSAtMDAwMCIsImV4cGlyZXNPbiI6IjExLzIwLzE4IDIyOjA40jI0IC0wMDAwIn0sInZts
WQiOiiifaCCAj8wggI7MIIIBpKADAgECAhBnxW5Kh8ds1EB0E2mIBJ0MA0GCSqGSib3DQEBAUAMCsxKTAnBgNVBAMTIHRlc3RzdWJkb21halW4u
bwV0YWRhdGEuYXp1cmUuY29tMB4XDTE4MTIyMDIxNTc1NlowKzEpMCCGA1UEAxMgdGVzdHN1YmRvbWFpb5tZXrhZGF
0YS5henVyzS5jb20wgZ8wDQYJKoZihvcNAQEBBQADgY0AMIGJAoGBAML/tBo86ENWPzmXZ0kPKx5dY5QZ150mA8lommszE71x2sCLonzv4/UWk4
H+jMMWRwIea2CuQ5RhdWAhvKq6if4okKnt66fxm+YTVz9z0CTfCLmLT+nsdf0AsG1xZppEapC0Cd9vD6NCKyE8aYI1pliaeOnFjG0WvMY04uWz
2MdAgMBAAGjYDBeMFwGA1UdAQRMFOAEnnYkHLa04Ut4Mp7TkJFfyhLTArMSkwJwYDVQQDEyB0ZXN0c3ViZG9tYWluLm1ldGFkYXRhLmF6dXJ1
LmNvbYIQZ8VuSoFhbJRAQNBnpiaSdDANBgkqhkiG9w0BAQQFAAOBqQCLSM6aX5Bs1KHCJp4VQtzXPzXF71rVKCocHy3N9PTJQ9Fpnd+bYw2vSpQ
Hg/Aig82WuDFpReJvr7Pa938mZqW9HUOGjQKK2FYDTg6fXD8pkPdygh1X5boGWAMMr7bFkup+lsT+n2tRw2wbNkn01tQ0wICtqy2VqzWwLi45
RBwTGB6DCB5QIBATA/MCsxKTAnBgNVBAMTIHRlc3RzdWJkb21halW4ubW0YWRhdGEuYXp1cmUuY29tAhBnxW5Kh8ds1EB0E2mIBJ0MA0GCSqGS
Ib3DQEBCwUAMA0GCSqGSib3DQEBAQUABIGAl1BM/yYIqqv8SDE4kjQo3U1/IKAVR8ETKve5BAdGSNkTUooUGVniTXeuvDj5Nkmaz0aKzp9fEt
ByqqPOyw/n1xaZg0044HDGiPUJ90xYmfeK6p9RpJBu6kiKhnnYTelUk5u75phe5ZbMZfBhuPhXmYAdjc7Nmww97nx8NnprQ="}
}
```

The signature blob is a [pkcs7](#) signed version of document. It contains the certificate used for signing along with the VM details like vmId, sku, nonce, subscriptionId, timeStamp for creation and expiry of the document and the plan information about the image. The plan information is only populated for Azure Market place images. The certificate can be extracted from the response and used to validate that the response is valid and is coming from Azure.

## Example scenarios for usage

### Tracking VM running on Azure

As a service provider, you may require to track the number of VMs running your software or have agents that need to track uniqueness of the VM. To be able to get a unique ID for a VM, use the `vmId` field from Instance Metadata Service.

### Request

```
curl -H Metadata:true "http://169.254.169.254/metadata/instance/compute/vmId?api-version=2017-08-01&format=text"
```

### Response

```
5c08b38e-4d57-4c23-ac45-aca61037f084
```

### Placement of containers, data-partitions based fault/update domain

For certain scenarios, placement of different data replicas is of prime importance. For example, [HDFS replica placement](#) or container placement via an [orchestrator](#) may you require to know the `platformFaultDomain` and `platformUpdateDomain` the VM is running on. You can also use [Availability Zones](#) for the instances to make these decisions. You can query this data directly via the Instance Metadata Service.

### Request

```
curl -H Metadata:true "http://169.254.169.254/metadata/instance/compute/platformFaultDomain?api-version=2017-08-01&format=text"
```

### Response

## Getting more information about the VM during support case

As a service provider, you may get a support call where you would like to know more information about the VM. Asking the customer to share the compute metadata can provide basic information for the support professional to know about the kind of VM on Azure.

### Request

```
curl -H Metadata:true "http://169.254.169.254/metadata/instance/compute?api-version=2019-06-01"
```

### Response

#### NOTE

The response is a JSON string. The following example response is pretty-printed for readability.

```
{
 "azEnvironment": "AzurePublicCloud",
 "customData": "",
 "location": "centralus",
 "name": "negasonic",
 "offer": "lampstack",
 "osType": "Linux",
 "placementGroupId": "",
 "plan": {
 "name": "5-6",
 "product": "lampstack",
 "publisher": "bitnami"
 },
 "platformFaultDomain": "0",
 "platformUpdateDomain": "0",
 "provider": "Microsoft.Compute",
 "publicKeys": [],
 "publisher": "bitnami",
 "resourceGroupName": "myrg",
 "resourceId": "/subscriptions/xxxxx-xxxx-xxxx-xxxx-xxxx-
xxxxxxxx/resourceGroups/myrg/providers/Microsoft.Compute/virtualMachines/negasonic",
 "sku": "5-6",
 "storageProfile": {
 "dataDisks": [
 {
 "caching": "None",
 "createOption": "Empty",
 "diskSizeGB": "1024",
 "image": {
 "uri": ""
 },
 "lun": "0",
 "managedDisk": {
 "id": "/subscriptions/xxxxx-xxxx-xxxx-xxxx-xxxxxxxx/resourceGroups/macikgo-test-may-
23/providers/Microsoft.Compute/disks/exampledatadiskname",
 "storageAccountType": "Standard_LRS"
 },
 "name": "exampledatadiskname",
 "vhd": {
 "uri": ""
 },
 "writeAcceleratorEnabled": "false"
 }
]
 }
}
```

```

],
 "imageReference": {
 "id": "",
 "offer": "UbuntuServer",
 "publisher": "Canonical",
 "sku": "16.04.0-LTS",
 "version": "latest"
 },
 "osDisk": {
 "caching": "ReadWrite",
 "createOption": "FromImage",
 "diskSizeGB": "30",
 "diffDiskSettings": {
 "option": "Local"
 },
 "encryptionSettings": {
 "enabled": "false"
 },
 "image": {
 "uri": ""
 },
 "managedDisk": {
 "id": "/subscriptions/xxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx/resourceGroups/macikgo-test-may-23/providers/Microsoft.Compute/disks/exampleosdiskname",
 "storageAccountType": "Standard_LRS"
 },
 "name": "exampleosdiskname",
 "osType": "Linux",
 "vhd": {
 "uri": ""
 },
 "writeAcceleratorEnabled": "false"
 }
 },
 "subscriptionId": "xxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx",
 "tags": "Department:IT;Environment:Test;Role:WebRole",
 "version": "7.1.1902271506",
 "vmId": "13f56399-bd52-4150-9748-7190aae1ff21",
 "vmScaleSetName": "",
 "vmSize": "Standard_A1_v2",
 "zone": "1"
}

```

## Getting Azure Environment where the VM is running

Azure has various sovereign clouds like [Azure Government](#). Sometimes you need the Azure Environment to make some runtime decisions. The following sample shows you how you can achieve this behavior.

### Request

```
curl -H Metadata:true "http://169.254.169.254/metadata/instance/compute/azEnvironment?api-version=2018-10-01&format=text"
```

### Response

```
AzurePublicCloud
```

The cloud and the values of the Azure Environment are listed below.

| CLOUD                                        | AZURE ENVIRONMENT |
|----------------------------------------------|-------------------|
| All Generally Available Global Azure Regions | AzurePublicCloud  |

| CLOUD                | AZURE ENVIRONMENT      |
|----------------------|------------------------|
| Azure Government     | AzureUSGovernmentCloud |
| Azure China 21Vianet | AzureChinaCloud        |
| Azure Germany        | AzureGermanCloud       |

## Getting the tags for the VM

Tags may have been applied to your Azure VM to logically organize them into a taxonomy. The tags assigned to a VM can be retrieved by using the request below.

### Request

```
curl -H Metadata:true "http://169.254.169.254/metadata/instance/compute/tags?api-version=2018-10-01&format=text"
```

### Response

```
Department:IT;Environment:Test;Role:WebRole
```

The `tags` field is a string with the tags delimited by semicolons. This can be a problem if semicolons are used in the tags themselves. If a parser is written to programmatically extract the tags, you should rely on the `tagsList` field which is a JSON array with no delimiters, and consequently, easier to parse.

### Request

```
curl -H Metadata:true "http://169.254.169.254/metadata/instance/compute/tagsList?api-version=2019-06-04&format=json"
```

### Response

```
[
 {
 "name": "Department",
 "value": "IT"
 },
 {
 "name": "Environment",
 "value": "Test"
 },
 {
 "name": "Role",
 "value": "WebRole"
 }
]
```

## Validating that the VM is running in Azure

Marketplace vendors want to ensure that their software is licensed to run only in Azure. If someone copies the VHD out to on-premises, then they should have the ability to detect that. By calling into Instance Metadata Service, Marketplace vendors can get signed data that guarantees response only from Azure.

## NOTE

Requires jq to be installed.

## Request

```
Get the signature
curl --silent -H Metadata:True http://169.254.169.254/metadata/attested/document?api-version=2019-04-30 | jq
-r '[."signature"]' > signature
Decode the signature
base64 -d signature > decodedsignature
#Get PKCS7 format
openssl pkcs7 -in decodedsignature -inform DER -out sign.pk7
Get Public key out of pkc7
openssl pkcs7 -in decodedsignature -inform DER -print_certs -out signer.pem
#Get the intermediate certificate
wget -q -O intermediate.cer "$(openssl x509 -in signer.pem -text -noout | grep " CA Issuers -" | awk -FURI:
'{print $2}')"
openssl x509 -inform der -in intermediate.cer -out intermediate.pem
#Verify the contents
openssl smime -verify -in sign.pk7 -inform pem -noverify
```

## Response

```
Verification successful
{
 "nonce": "20181128-001617",
 "plan": {
 "name": "",
 "product": "",
 "publisher": ""
 },
 "timeStamp": {
 "createdOn": "11/28/18 00:16:17 -0000",
 "expiresOn": "11/28/18 06:16:17 -0000"
 },
 "vmId": "d3e0e374-fda6-4649-bbc9-7f20dc379f34",
 "subscriptionId": "xxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx",
 "sku": "RS3-Pro"
}
```

| DATA                | DESCRIPTION                                                                                                                    |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------|
| nonce               | User supplied optional string with the request. If no nonce was supplied in the request, the current UTC timestamp is returned |
| plan                | <a href="#">Plan</a> for a VM in it's an Azure Marketplace Image, contains name, product, and publisher                        |
| timestamp/createdOn | The UTC timestamp at which the first signed document was created                                                               |
| timestamp/expiresOn | The UTC timestamp at which the signed document expires                                                                         |
| vmId                | <a href="#">Unique identifier</a> for the VM                                                                                   |

| DATA           | DESCRIPTION                                                             |
|----------------|-------------------------------------------------------------------------|
| subscriptionId | Azure subscription for the Virtual Machine, introduced in<br>2019-04-30 |
| sku            | Specific SKU for the VM image, introduced in 2019-11-01                 |

#### Verifying the signature

Once you get the signature above, you can verify that the signature is from Microsoft. Also you can verify the intermediate certificate and the certificate chain. Lastly, you can verify the subscription ID is correct.

#### NOTE

The certificate for Public cloud and sovereign cloud will be different.

| CLOUD                                        | CERTIFICATE                  |
|----------------------------------------------|------------------------------|
| All Generally Available Global Azure Regions | *.metadata.azure.com         |
| Azure Government                             | *.metadata.azure.us          |
| Azure China 21Vianet                         | *.metadata.azure.cn          |
| Azure Germany                                | *.metadata.microsoftazure.de |

There is a known issue around the certificate used for signing. The certificates may not have an exact match of `metadata.azure.com` for public cloud. Hence the certification validation should allow a common name from any `.metadata.azure.com` subdomain.

```
Verify the subject name for the main certificate
openssl x509 -noout -subject -in signer.pem
Verify the issuer for the main certificate
openssl x509 -noout -issuer -in signer.pem
#Validate the subject name for intermediate certificate
openssl x509 -noout -subject -in intermediate.pem
Verify the issuer for the intermediate certificate
openssl x509 -noout -issuer -in intermediate.pem
Verify the certificate chain
openssl verify -verbose -CAfile /etc/ssl/certs/Baltimore_CyberTrust_Root.pem -untrusted intermediate.pem
signer.pem
```

In cases where the intermediate certificate cannot be downloaded due to network constraints during validation, the intermediate certificate can be pinned. However, Azure will roll over the certificates as per standard PKI practice. The pinned certificates would need to be updated when roll over happens. Whenever a change to update the intermediate certificate is planned, the Azure blog will be updated and Azure customers will be notified. The intermediate certificates can be found [here](#). The intermediate certificates for each of the regions can be different.

#### Failover Clustering in Windows Server

For certain scenarios, when querying Instance Metadata Service with Failover Clustering, it is necessary to add a route to the routing table.

1. Open command prompt with administrator privileges.
2. Run the following command and note the address of the Interface for Network Destination (`0.0.0.0`) in the

## IPv4 Route Table.

```
route print
```

### NOTE

The following example output from a Windows Server VM with Failover Cluster enabled contains only the IPv4 Route Table for simplicity.

### IPv4 Route Table

```
=====
Active Routes:
Network Destination Netmask Gateway Interface Metric
 0.0.0.0 0.0.0.0 10.0.1.1 10.0.1.10 266
 10.0.1.0 255.255.255.192 On-link 10.0.1.10 266
 10.0.1.10 255.255.255.255 On-link 10.0.1.10 266
 10.0.1.15 255.255.255.255 On-link 10.0.1.10 266
 10.0.1.63 255.255.255.255 On-link 10.0.1.10 266
 127.0.0.0 255.0.0.0 127.0.0.1 127.0.0.1 331
 127.0.0.1 255.255.255.255 On-link 127.0.0.1 331
127.255.255.255 255.255.255.255 On-link 127.0.0.1 331
 169.254.0.0 255.255.0.0 169.254.1.156 169.254.1.156 271
 169.254.1.156 255.255.255.255 On-link 169.254.1.156 271
 169.254.255.255 255.255.255.255 On-link 169.254.1.156 271
 224.0.0.0 240.0.0.0 127.0.0.1 127.0.0.1 331
 224.0.0.0 240.0.0.0 169.254.1.156 169.254.1.156 271
 224.0.0.0 240.0.0.0 10.0.1.10 10.0.1.10 266
 255.255.255.255 255.255.255.255 On-link 127.0.0.1 331
 255.255.255.255 255.255.255.255 On-link 169.254.1.156 271
 255.255.255.255 255.255.255.255 On-link 10.0.1.10 266
```

1. Run the following command and use the address of the Interface for Network Destination ( `0.0.0.0` ) which is ( `10.0.1.10` ) in this example.

```
route add 169.254.169.254/32 10.0.1.10 metric 1 -p
```

### Storage profile

Instance Metadata Service can provide details about the storage disks associated with the VM. This data can be found at the instance/compute/storageProfile endpoint.

The storage profile of a VM is divided into three categories - image reference, OS disk, and data disks.

The image reference object contains the following information about the OS image:

| DATA      | DESCRIPTION                                  |
|-----------|----------------------------------------------|
| id        | Resource ID                                  |
| offer     | Offer of the platform or marketplace image   |
| publisher | Image publisher                              |
| sku       | Image sku                                    |
| version   | Version of the platform or marketplace image |

The OS disk object contains the following information about the OS disk used by the VM:

| DATA                    | DESCRIPTION                                            |
|-------------------------|--------------------------------------------------------|
| caching                 | Caching requirements                                   |
| createOption            | Information about how the VM was created               |
| diffDiskSettings        | Ephemeral disk settings                                |
| diskSizeGB              | Size of the disk in GB                                 |
| image                   | Source user image virtual hard disk                    |
| lun                     | Logical unit number of the disk                        |
| managedDisk             | Managed disk parameters                                |
| name                    | Disk name                                              |
| vhd                     | Virtual hard disk                                      |
| writeAcceleratorEnabled | Whether or not writeAccelerator is enabled on the disk |

The data disks array contains a list of data disks attached to the VM. Each data disk object contains the following information:

| DATA                    | DESCRIPTION                                            |
|-------------------------|--------------------------------------------------------|
| caching                 | Caching requirements                                   |
| createOption            | Information about how the VM was created               |
| diffDiskSettings        | Ephemeral disk settings                                |
| diskSizeGB              | Size of the disk in GB                                 |
| encryptionSettings      | Encryption settings for the disk                       |
| image                   | Source user image virtual hard disk                    |
| managedDisk             | Managed disk parameters                                |
| name                    | Disk name                                              |
| osType                  | Type of OS included in the disk                        |
| vhd                     | Virtual hard disk                                      |
| writeAcceleratorEnabled | Whether or not writeAccelerator is enabled on the disk |

The following is an example of how to query the VM's storage information.

## Request

```
curl -H Metadata:true "http://169.254.169.254/metadata/instance/compute/storageProfile?api-version=2019-06-01"
```

## Response

### NOTE

The response is a JSON string. The following example response is pretty-printed for readability.

```
{
 "dataDisks": [
 {
 "caching": "None",
 "createOption": "Empty",
 "diskSizeGB": "1024",
 "image": {
 "uri": ""
 },
 "lun": "0",
 "managedDisk": {
 "id": "/subscriptions/xxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx/resourceGroups/macikgo-test-may-23/providers/Microsoft.Compute/disks/exampledatadiskname",
 "storageAccountType": "Standard_LRS"
 },
 "name": "exampledatadiskname",
 "vhd": {
 "uri": ""
 },
 "writeAcceleratorEnabled": "false"
 }
],
 "imageReference": {
 "id": "",
 "offer": "UbuntuServer",
 "publisher": "Canonical",
 "sku": "16.04.0-LTS",
 "version": "latest"
 },
 "osDisk": {
 "caching": "ReadWrite",
 "createOption": "FromImage",
 "diskSizeGB": "30",
 "diffDiskSettings": {
 "option": "Local"
 },
 "encryptionSettings": {
 "enabled": "false"
 },
 "image": {
 "uri": ""
 },
 "managedDisk": {
 "id": "/subscriptions/xxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx/resourceGroups/macikgo-test-may-23/providers/Microsoft.Compute/disks/exampleosdiskname",
 "storageAccountType": "Standard_LRS"
 },
 "name": "exampleosdiskname",
 "osType": "Linux",
 "vhd": {
 "uri": ""
 },
 "writeAcceleratorEnabled": "false"
 }
}
}
```

## Examples of calling metadata service using different languages inside the VM

| LANGUAGE | EXAMPLE                                                                                                                                         |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Ruby     | <a href="https://github.com/Microsoft/azureimds/blob/master/IMDSSample.rb">https://github.com/Microsoft/azureimds/blob/master/IMDSSample.rb</a> |

| LANGUAGE     | EXAMPLE                                                                                                                                                           |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Go           | <a href="https://github.com/Microsoft/azureimds/blob/master/imdssample.go">https://github.com/Microsoft/azureimds/blob/master/imdssample.go</a>                   |
| Python       | <a href="https://github.com/Microsoft/azureimds/blob/master/IMDSSample.py">https://github.com/Microsoft/azureimds/blob/master/IMDSSample.py</a>                   |
| C++          | <a href="https://github.com/Microsoft/azureimds/blob/master/IMDSSample-windows.cpp">https://github.com/Microsoft/azureimds/blob/master/IMDSSample-windows.cpp</a> |
| C#           | <a href="https://github.com/Microsoft/azureimds/blob/master/IMDSSample.cs">https://github.com/Microsoft/azureimds/blob/master/IMDSSample.cs</a>                   |
| JavaScript   | <a href="https://github.com/Microsoft/azureimds/blob/master/IMDSSample.js">https://github.com/Microsoft/azureimds/blob/master/IMDSSample.js</a>                   |
| PowerShell   | <a href="https://github.com/Microsoft/azureimds/blob/master/IMDSSample.ps1">https://github.com/Microsoft/azureimds/blob/master/IMDSSample.ps1</a>                 |
| Bash         | <a href="https://github.com/Microsoft/azureimds/blob/master/IMDSSample.sh">https://github.com/Microsoft/azureimds/blob/master/IMDSSample.sh</a>                   |
| Perl         | <a href="https://github.com/Microsoft/azureimds/blob/master/IMDSSample.pl">https://github.com/Microsoft/azureimds/blob/master/IMDSSample.pl</a>                   |
| Java         | <a href="https://github.com/Microsoft/azureimds/blob/master/imdssample.java">https://github.com/Microsoft/azureimds/blob/master/imdssample.java</a>               |
| Visual Basic | <a href="https://github.com/Microsoft/azureimds/blob/master/IMDSSample.vb">https://github.com/Microsoft/azureimds/blob/master/IMDSSample.vb</a>                   |
| Puppet       | <a href="https://github.com/keirans/azurometadata">https://github.com/keirans/azurometadata</a>                                                                   |

## FAQ

- I am getting the error `400 Bad Request, Required metadata header not specified`. What does this mean?
  - The Instance Metadata Service requires the header `Metadata: true` to be passed in the request. Passing this header in the REST call allows access to the Instance Metadata Service.
- Why am I not getting compute information for my VM?
  - Currently the Instance Metadata Service only supports instances created with Azure Resource Manager. In the future, support for Cloud Service VMs might be added.
- I created my Virtual Machine through Azure Resource Manager a while back. Why am I not see compute metadata information?
  - For any VMs created after Sep 2016, add a [Tag](#) to start seeing compute metadata. For older VMs (created before Sep 2016), add/remove extensions or data disks to the VM to refresh metadata.
- I am not seeing all data populated for new version
  - For any VMs created after Sep 2016, add a [Tag](#) to start seeing compute metadata. For older VMs (created before Sep 2016), add/remove extensions or data disks to the VM to refresh metadata.
- Why am I getting the error `500 Internal Server Error`?

- Retry your request based on exponential back off system. If the issue persists contact Azure support.
6. Where do I share additional questions/comments?
    - Send your comments on <https://feedback.azure.com>.
  7. Would this work for Virtual Machine Scale Set Instance?
    - Yes Metadata service is available for Scale Set Instances.
  8. How do I get support for the service?
    - To get support for the service, create a support issue in Azure portal for the VM where you are not able to get metadata response after long retries.
  9. I get request timed out for my call to the service?
    - Metadata calls must be made from the primary IP address assigned to the primary network card of the VM, in addition in case you have changed your routes there must be a route for 169.254.0.0/16 address out of your network card.
  10. I updated my tags in virtual machine scale set but they don't appear in the instances unlike VMs?
    - Currently for ScaleSets tags only show to the VM on a reboot/reimage/or a disk change to the instance.

# Problem

NEW SUPPORT REQUEST



\* Severity ⓘ

C - Minimal impact



\* Problem type

Management



\* Category

✓ Choose a category

Backup

Cannot stop, start, or restart a VM

Capacity issues that are related to SAP HANA large instances

Instance Metadata Service

Manage an Exchange Server

Manage an instance of SQL Server

Manage encrypted disks, keys or secrets, or permissions

Manage or use RDS in Azure

Manage or use a VPN

Manage or use a cluster in Azure

Manage or use a virtual network

Manage or use endpoints

Unable to delete a virtual machine

Virtual machine restarts

When did the problem start?

Choose a date



Enter a local time

File upload ⓘ

Select a file



Share diagnostic information ⓘ

[Learn more about the information we collect](#)

**Next**

## Next steps

- Learn more about [Scheduled Events](#)

# Get Virtual Machine usage metrics using the REST API

11/13/2019 • 2 minutes to read • [Edit Online](#)

This example shows how to retrieve the CPU usage for a [Linux Virtual Machine](#) using the [Azure REST API](#).

Complete reference documentation and additional samples for the REST API are available in the [Azure Monitor REST reference](#).

## Build the request

Use the following GET request to collect the [Percentage CPU](#) metric from a Virtual Machine

```
GET
https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.Compute/virtualMachines/{vmname}/providers/microsoft.insights/metrics?api-version=2018-01-01&metricnames=Percentage%20CPU×pan=2018-06-05T03:00:00Z/2018-06-07T03:00:00Z
```

### Request headers

The following headers are required:

| REQUEST HEADER         | DESCRIPTION                                                                 |
|------------------------|-----------------------------------------------------------------------------|
| <i>Content-Type</i> :  | Required. Set to <code>application/json</code> .                            |
| <i>Authorization</i> : | Required. Set to a valid <code>Bearer</code> <a href="#">access token</a> . |

### URI parameters

| NAME                     | DESCRIPTION                                                                                                                                              |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>subscriptionId</i>    | The subscription ID that identifies an Azure subscription. If you have multiple subscriptions, see <a href="#">Working with multiple subscriptions</a> . |
| <i>resourceGroupName</i> | The name of the Azure resource group associated with the resource. You can get this value from the Azure Resource Manager API, CLI, or the portal.       |
| <i>vmname</i>            | The name of the Azure Virtual Machine.                                                                                                                   |
| <i>metricnames</i>       | Comma-separated list of valid <a href="#">Load Balancer metrics</a> .                                                                                    |
| <i>api-version</i>       | The API version to use for the request.<br><br>This document covers <i>api-version</i> <code>2018-01-01</code> , included in the above URL.              |

| NAME     | DESCRIPTION                                                                                                                                                                                                         |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| timespan | String with the following format <code>startDateTime_ISO/endDateTime_ISO</code> that defines the time range of the returned metrics. This optional parameter is set to return a day's worth of data in the example. |
|          |                                                                                                                                                                                                                     |

## Request body

No request body is needed for this operation.

## Handle the response

Status code 200 is returned when the list of metric values is returned successfully. A full list of error codes is available in the [reference documentation](#).

## Example response

```
{
 "cost": 0,
 "timespan": "2018-06-08T23:48:10Z/2018-06-09T00:48:10Z",
 "interval": "PT1M",
 "value": [
 {
 "id": "/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.Compute/virtualMachines/{vmname}/providers/microsoft.insights/metrics?api-version=2018-01-01&metricnames=Percentage%20CPU",
 "type": "Microsoft.Insights/metrics",
 "name": {
 "value": "Percentage CPU",
 "localizedValue": "Percentage CPU"
 },
 "unit": "Percent",
 "timeseries": [
 {
 "metadatavalues": [],
 "data": [
 {
 "timeStamp": "2018-06-08T23:48:00Z",
 "average": 0.44
 },
 {
 "timeStamp": "2018-06-08T23:49:00Z",
 "average": 0.31
 },
 {
 "timeStamp": "2018-06-08T23:50:00Z",
 "average": 0.29
 },
 {
 "timeStamp": "2018-06-08T23:51:00Z",
 "average": 0.29
 },
 {
 "timeStamp": "2018-06-08T23:52:00Z",
 "average": 0.285
 }
]
 }
]
 }
]
}
```



# Handling planned maintenance notifications

2/10/2020 • 7 minutes to read • [Edit Online](#)

Azure periodically performs updates to improve the reliability, performance, and security of the host infrastructure for virtual machines. Updates are changes like patching the hosting environment or upgrading and decommissioning hardware. A majority of these updates are completed without any impact to the hosted virtual machines. However, there are cases where updates do have an impact:

- If the maintenance does not require a reboot, Azure uses in-place migration to pause the VM while the host is updated. These types maintenance operations are applied fault domain by fault domain. Progress is stopped if any warning health signals are received.
- If maintenance requires a reboot, you get a notice of when the maintenance is planned. You are given a time window of about 35 days where you can start the maintenance yourself, when it works for you.

Planned maintenance that requires a reboot is scheduled in waves. Each wave has different scope (regions).

- A wave starts with a notification to customers. By default, notification is sent to the Service Administrator and Co-Administrators. You can add more recipients and messaging options like email, SMS, and webhooks, using [Activity Log Alerts](#).
- Once a notification goes out, a *self-service window* is made available. During this window, you can query which of your virtual machines are affected and start maintenance based on your own scheduling needs. The self-service window is typically about 35 days.
- After the self-service window, a *scheduled maintenance window* begins. At some point during this window, Azure schedules and applies the required maintenance to your virtual machine.

The goal in having two windows is to give you enough time to start maintenance and reboot your virtual machine while knowing when Azure will automatically start maintenance.

You can use the Azure portal, PowerShell, REST API, and CLI to query for the maintenance windows for your VMs and start self-service maintenance.

## Should you start maintenance using during the self-service window?

The following guidelines should help you decide whether to use this capability and start maintenance at your own time.

### NOTE

Self-service maintenance might not be available for all of your VMs. To determine if proactive redeploy is available for your VM, look for the **Start now** in the maintenance status. Self-service maintenance is currently not available for Cloud Services (Web/Worker Role) and Service Fabric.

Self-service maintenance is not recommended for deployments using **availability sets**. Availability sets are already only updated one update domain at a time.

- Let Azure trigger the maintenance. For maintenance that requires reboot, maintenance will be done update domain by update domain. The update domains do not necessarily receive the maintenance sequentially, and that there is a 30-minute pause between update domains.
- If a temporary loss of some capacity (1 update domain) is a concern, you can add instances during the maintenance period.

- For maintenance that does not require reboot, updates are applied at the fault domain level.

**Don't** use self-service maintenance in the following scenarios:

- If you shut down your VMs frequently, either manually, using DevTest Labs, using auto-shutdown, or following a schedule, it could revert the maintenance status and therefore cause additional downtime.
- On short-lived VMs that you know will be deleted before the end of the maintenance wave.
- For workloads with a large state stored in the local (ephemeral) disk that is desired to be maintained upon update.
- For cases where you resize your VM often, as it could revert the maintenance status.
- If you have adopted scheduled events that enable proactive failover or graceful shutdown of your workload, 15 minutes before start of maintenance shutdown

**Use** self-service maintenance, if you are planning to run your VM uninterrupted during the scheduled maintenance phase and none of the counter-indications mentioned above are applicable.

It is best to use self-service maintenance in the following cases:

- You need to communicate an exact maintenance window to your management or end-customer.
- You need to complete the maintenance by a given date.
- You need to control the sequence of maintenance, for example, multi-tier application to guarantee safe recovery.
- More than 30 minutes of VM recovery time is needed between two update domains (UDs). To control the time between update domains, you must trigger maintenance on your VMs one update domain (UD) at a time.

## FAQ

### **Q: Why do you need to reboot my virtual machines now?**

**A:** While the majority of updates and upgrades to the Azure platform do not impact virtual machine's availability, there are cases where we can't avoid rebooting virtual machines hosted in Azure. We have accumulated several changes that require us to restart our servers that will result in virtual machines reboot.

### **Q: If I follow your recommendations for High Availability by using an Availability Set, am I safe?**

**A:** Virtual machines deployed in an availability set or virtual machine scale sets have the notion of Update Domains (UD). When performing maintenance, Azure honors the UD constraint and will not reboot virtual machines from different UD (within the same availability set). Azure also waits for at least 30 minutes before moving to the next group of virtual machines.

For more information about high availability, see [Availability for virtual machines in Azure](#).

### **Q: How do I get notified about planned maintenance?**

**A:** A planned maintenance wave starts by setting a schedule to one or more Azure regions. Soon after, an email notification is sent to the subscription Admins (one email per subscription). Additional channels and recipients for this notification could be configured using Activity Log Alerts. In case you deploy a virtual machine to a region where planned maintenance is already scheduled, you will not receive the notification but rather need to check the maintenance state of the VM.

### **Q: I don't see any indication of planned maintenance in the portal, Powershell, or CLI. What is wrong?**

**A:** Information related to planned maintenance is available during a planned maintenance wave only for the VMs that are going to be impacted by it. In other words, if you see no data, it could be that the maintenance wave has already completed (or not started) or that your virtual machine is already hosted in an updated server.

### **Q: Is there a way to know exactly when my virtual machine will be impacted?**

**A:** When setting the schedule, we define a time window of several days. However, the exact sequencing of servers (and VMs) within this window is unknown. Customers who would like to know the exact time for their VMs can use [scheduled events](#) and query from within the virtual machine and receive a 15-minute notification before a VM reboot.

**Q: How long will it take you to reboot my virtual machine?**

**A:** Depending on the size of your VM, reboot may take up to several minutes during the self-service maintenance window. During the Azure initiated reboots in the scheduled maintenance window, the reboot will typically take about 25 minutes. Note that in case you use Cloud Services (Web/Worker Role), Virtual Machine Scale Sets, or availability sets, you will be given 30 minutes between each group of VMs (UD) during the scheduled maintenance window.

**Q: What is the experience in the case of Virtual Machine Scale Sets?**

**A:** Planned maintenance is now available for Virtual Machine Scale Sets. For instructions on how to initiate self-service maintenance refer [planned maintenance for virtual machine scale sets](#) document.

**Q: What is the experience in the case of Cloud Services (Web/Worker Role) and Service Fabric?**

**A:** While these platforms are impacted by planned maintenance, customers using these platforms are considered safe given that only VMs in a single Upgrade Domain (UD) will be impacted at any given time. Self-service maintenance is currently not available for Cloud Services (Web/Worker Role) and Service Fabric.

**Q: I don't see any maintenance information on my VMs. What went wrong?**

**A:** There are several reasons why you're not seeing any maintenance information on your VMs:

1. You are using a subscription marked as Microsoft internal.
2. Your VMs are not scheduled for maintenance. It could be that the maintenance wave has ended, canceled, or modified so that your VMs are no longer impacted by it.
3. You don't have the **Maintenance** column added to your VM list view. While we have added this column to the default view, customers who configured to see non-default columns must manually add the **Maintenance** column to their VM list view.

**Q: My VM is scheduled for maintenance for the second time. Why?**

**A:** There are several use cases where you will see your VM scheduled for maintenance after you have already completed your maintenance-redeploy:

1. We have canceled the maintenance wave and restarted it with a different payload. It could be that we've detected faulted payload and we simply need to deploy an additional payload.
2. Your VM was *service healed* to another node due to a hardware fault.
3. You have selected to stop (deallocate) and restart the VM.
4. You have **auto shutdown** turned on for the VM.

## Next steps

You can handle planned maintenance using the [Azure CLI](#), [Azure PowerShell](#) or [portal](#).

# Handling planned maintenance notifications using the Azure CLI

2/28/2020 • 2 minutes to read • [Edit Online](#)

**This article applies to virtual machines running both Linux and Windows.**

You can use the CLI to see when VMs are scheduled for [maintenance](#). Planned maintenance information is available from `az vm get-instance-view`.

Maintenance information is returned only if there is maintenance planned.

```
az vm get-instance-view -n myVM -g myResourceGroup --query instanceView.maintenanceRedeployStatus
```

## Start maintenance

The following call will start maintenance on a VM if `IsCustomerInitiatedMaintenanceAllowed` is set to true.

```
az vm perform-maintenance -g myResourceGroup -n myVM
```

## Classic deployments

### IMPORTANT

Classic VMs will be retired on March 1, 2023.

If you use IaaS resources from ASM, please complete your migration by March 1, 2023. We encourage you to make the switch sooner to take advantage of the many feature enhancements in Azure Resource Manager.

For more information, see [Migrate your IaaS resources to Azure Resource Manager by March 1, 2023](#).

If you still have legacy VMs that were deployed using the classic deployment model, you can use the Azure classic CLI to query for VMs and initiate maintenance.

Make sure you are in the correct mode to work with classic VM by typing:

```
azure config mode asm
```

To get the maintenance status of a VM named *myVM*, type:

```
azure vm show myVM
```

To start maintenance on your classic VM named *myVM* in the *myService* service and *myDeployment* deployment, type:

```
azure compute virtual-machine initiate-maintenance --service-name myService --name myDeployment --virtual-machine-name myVM
```

## Next steps

You can also handle planned maintenance using the [Azure PowerShell](#) or [portal](#).

# Handling planned maintenance notifications using the portal

2/10/2020 • 2 minutes to read • [Edit Online](#)

**This article applies to virtual machines running both Linux and Windows.**

Once a [planned maintenance](#) wave is scheduled, you can check for a list of virtual machines that are impacted.

You can use the Azure portal and look for VMs scheduled for maintenance.

1. Sign in to the [Azure portal](#).
2. In the left navigation, click **Virtual Machines**.
3. In the Virtual Machines pane, select **Edit columns** button to open the list of available columns.
4. Select and add the following columns:

**Maintenance status:** Shows the maintenance status for the VM. The following are the potential values:

| VALUE           | DESCRIPTION                                                                                                                                                                                                        |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Start now       | The VM is in the self-service maintenance window that lets you initiate the maintenance yourself. See below on how to start maintenance on your VM.                                                                |
| Scheduled       | The VM is scheduled for maintenance with no option for you to initiate maintenance. You can learn of the maintenance window by selecting the Maintenance - Scheduled window in this view or by clicking on the VM. |
| Already updated | Your VM is already updated and no further action is required at this time.                                                                                                                                         |
| Retry later     | You have initiated maintenance with no success. You will be able to use the self-service maintenance option at a later time.                                                                                       |
| Retry now       | You can retry a previously unsuccessful self-initiated maintenance.                                                                                                                                                |
| -               | Your VM is not part of a planned maintenance wave.                                                                                                                                                                 |

**Maintenance - Self-service window:** Shows the time window when you can self-start maintenance on your VMs.

**Maintenance - Scheduled window:** Shows the time window when Azure will maintain your VM in order to complete maintenance.

## Notification and alerts in the portal

Azure communicates a schedule for planned maintenance by sending an email to the subscription owner and co-owners group. You can add additional recipients and channels to this communication by creating Azure activity log alerts. For more information, see [Create activity log alerts on service notifications](#).

Make sure you set the **Event type** as **Planned maintenance**, and **Services** as **Virtual Machine Scale Sets** and/or **Virtual Machines**.

## Start Maintenance on your VM from the portal

While looking at the VM details, you will be able to see more maintenance-related details.

At the top of the VM details view, a new notification ribbon will be added if your VM is included in a planned maintenance wave. In addition, a new option is added to start maintenance when possible.

Click on the maintenance notification to see the maintenance page with more details on the planned maintenance. From there, you will be able to **start maintenance** on your VM.

Once you start maintenance, your virtual machine will be maintained and the maintenance status will be updated to reflect the result within few minutes.

If you missed the self-service window, you will still be able to see the window when your VM will be maintained by Azure.

## Next steps

You can also handle planned maintenance using the [Azure CLI](#) or [PowerShell](#).

# Handling planned maintenance using PowerShell

2/28/2020 • 2 minutes to read • [Edit Online](#)

**This article applies to virtual machines running both Linux and Windows.**

You can use Azure PowerShell to see when VMs are scheduled for [maintenance](#). Planned maintenance information is available from the [Get-AzVM](#) cmdlet when you use the `-Status` parameter.

Maintenance information is returned only if there is maintenance planned. If no maintenance is scheduled that impacts the VM, the cmdlet does not return any maintenance information.

```
Get-AzVM -ResourceGroupName myResourceGroup -Name myVM -Status
```

The following properties are returned under MaintenanceRedeployStatus:

| VALUE                                 | DESCRIPTION                                                                                       |
|---------------------------------------|---------------------------------------------------------------------------------------------------|
| IsCustomerInitiatedMaintenanceAllowed | Indicates whether you can start maintenance on the VM at this time                                |
| PreMaintenanceWindowStartTime         | The beginning of the maintenance self-service window when you can initiate maintenance on your VM |
| PreMaintenanceWindowEndTime           | The end of the maintenance self-service window when you can initiate maintenance on your VM       |
| MaintenanceWindowStartTime            | The beginning of the maintenance scheduled in which Azure initiates maintenance on your VM        |
| MaintenanceWindowEndTime              | The end of the maintenance scheduled window in which Azure initiates maintenance on your VM       |
| LastOperationResultCode               | The result of the last attempt to initiate maintenance on the VM                                  |

You can also get the maintenance status for all VMs in a resource group by using [Get-AzVM](#) and not specifying a VM.

```
Get-AzVM -ResourceGroupName myResourceGroup -Status
```

The following PowerShell example takes your subscription ID and returns a list of VMs that are scheduled for maintenance.

```

function MaintenanceIterator
{
 Select-AzSubscription -SubscriptionId $args[0]

 $rgList= Get-AzResourceGroup

 for ($rgIdx=0; $rgIdx -lt $rgList.Length ; $rgIdx++)
 {
 $rg = $rgList[$rgIdx]
 $vmList = Get-AzVM -ResourceGroupName $rg.ResourceGroupName
 for ($vmIdx=0; $vmIdx -lt $vmList.Length ; $vmIdx++)
 {
 $vm = $vmList[$vmIdx]
 $vmDetails = Get-AzVM -ResourceGroupName $rg.ResourceGroupName -Name $vm.Name -Status
 if ($vmDetails.MaintenanceRedeployStatus)
 {
 Write-Output "VM: $($vmDetails.Name) IsCustomerInitiatedMaintenanceAllowed:
$($vmDetails.MaintenanceRedeployStatus.IsCustomerInitiatedMaintenanceAllowed)
 $($vmDetails.MaintenanceRedeployStatus.LastOperationMessage)"
 }
 }
 }
}

```

## Start maintenance on your VM using PowerShell

Using information from the function in the previous section, the following starts maintenance on a VM if **IsCustomerInitiatedMaintenanceAllowed** is set to true.

```
Restart-AzVM -PerformMaintenance -name $vm.Name -ResourceGroupName $rg.ResourceGroupName
```

## Classic deployments

### IMPORTANT

Classic VMs will be retired on March 1, 2023.

If you use IaaS resources from ASM, please complete your migration by March 1, 2023. We encourage you to make the switch sooner to take advantage of the many feature enhancements in Azure Resource Manager.

For more information, see [Migrate your IaaS resources to Azure Resource Manager by March 1, 2023](#).

If you still have legacy VMs that were deployed using the classic deployment model, you can use PowerShell to query for VMs and initiate maintenance.

To get the maintenance status of a VM, type:

```
Get-AzureVM -ServiceName <Service name> -Name <VM name>
```

To start maintenance on your classic VM, type:

```
Restart-AzureVM -InitiateMaintenance -ServiceName <service name> -Name <VM name>
```

## Next steps

You can also handle planned maintenance using the [Azure CLI](#) or [portal](#).

# Preview: Control updates with Maintenance Control and the Azure CLI

2/14/2020 • 5 minutes to read • [Edit Online](#)

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 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.

Maintenance control lets you decide when to apply updates to your isolated VMs and Azure Dedicated Hosts.

With maintenance control, you can:

- Batch updates into one update package.
- Wait up to 35 days to apply updates.
- Automate platform updates for your maintenance window using Azure Functions.
- Maintenance configurations work across subscriptions and resource groups.

## IMPORTANT

Maintenance Control is currently in public preview. This preview version is provided without a service level agreement, and it's not recommended for production workloads. Certain features might not be supported or might have constrained capabilities. For more information, see [Supplemental Terms of Use for Microsoft Azure Previews](#).

## Limitations

- VMs must be on a [dedicated host](#), or be created using an [isolated VM size](#).
- After 35 days, an update will automatically be applied.
- User must have **Resource Contributor** access.

## Install the maintenance extension

If you choose to install the [Azure CLI](#) locally, you need version 2.0.76 or later.

Install the `maintenance` preview CLI extension locally or in Cloud Shell.

```
az extension add -n maintenance
```

## Create a maintenance configuration

Use `az maintenance configuration create` to create a maintenance configuration. This example creates a maintenance configuration named *myConfig* scoped to the host.

```
az group create \
--location eastus \
--name myMaintenanceRG
az maintenance configuration create \
-g myMaintenanceRG \
--name myConfig \
--maintenanceScope host \
--location eastus
```

Copy the configuration ID from the output to use later.

Using `--maintenanceScope host` ensures that the maintenance config is used for controlling updates to the host.

If you try to create a configuration with the same name, but in a different location, you will get an error.

Configuration names must be unique to your subscription.

You can query for available maintenance configurations using `az maintenance configuration list`.

```
az maintenance configuration list --query "[].{Name:name, ID:id}" -o table
```

## Assign the configuration

Use `az maintenance assignment create` to assign the configuration to your isolated VM or Azure Dedicated Host.

### Isolated VM

Apply the configuration to a VM using the ID of the configuration. Specify `--resource-type virtualMachines` and supply the name of the VM for `--resource-name`, and the resource group for the VM in `--resource-group`, and the location of the VM for `--location`.

```
az maintenance assignment create \
--resource-group myMaintenanceRG \
--location eastus \
--resource-name myVM \
--resource-type virtualMachines \
--provider-name Microsoft.Compute \
--configuration-assignment-name myConfig \
--maintenance-configuration-id "/subscriptions/1111abcd-1a11-1a2b-1a12-123456789abc/resourcegroups/myMaintenanceRG/providers/Microsoft.Maintenance/maintenanceConfigurations/myConfig"
```

### Dedicated host

To apply a configuration to a dedicated host, you need to include `--resource-type hosts`, `--resource-parent-name` with the name of the host group, and `--resource-parent-type hostGroups`.

The parameter `--resource-id` is the ID of the host. You can use [az vm host get-instance-view](#) to get the ID of your dedicated host.

```
az maintenance assignment create \
-g myDHRG \
--resource-name myHost \
--resource-type hosts \
--provider-name Microsoft.Compute \
--configuration-assignment-name myConfig \
--maintenance-configuration-id "/subscriptions/1111abcd-1a11-1a2b-1a12-
123456789abc/resourcegroups/myDHRG/providers/Microsoft.Maintenance/maintenanceConfigurations/myConf
ig" \
-l eastus \
--resource-parent-name myHostGroup \
--resource-parent-type hostGroups
```

## Check configuration

You can verify that the configuration was applied correctly, or check to see what configuration is currently applied using `az maintenance assignment list`.

### Isolated VM

```
az maintenance assignment list \
--provider-name Microsoft.Compute \
--resource-group myMaintenanceRG \
--resource-name myVM \
--resource-type virtualMachines \
--query "[].{resource:resourceGroup, configName:name}" \
--output table
```

### Dedicated host

```
az maintenance assignment list \
--resource-group myDHRG \
--resource-name myHost \
--resource-type hosts \
--provider-name Microsoft.Compute \
--resource-parent-name myHostGroup \
--resource-parent-type hostGroups \
--query "[].{ResourceGroup:resourceGroup,configName:name}" \
-o table
```

## Check for pending updates

Use `az maintenance update list` to see if there are pending updates. Update --subscription to be the ID for the subscription that contains the VM.

If there are no updates, the command will return an error message, which will contain the text:

```
Resource not found...StatusCode: 404
```

If there are updates, only one will be returned, even if there are multiple updates pending. The data for this update will be returned in an object:

```
[
 {
 "impactDurationInSec": 9,
 "impactType": "Freeze",
 "maintenanceScope": "Host",
 "notBefore": "2020-03-03T07:23:04.905538+00:00",
 "resourceId": "/subscriptions/9120c5ff-e78e-4bd0-b29f-
75c19cadd078/resourcegroups/DemoRG/providers/Microsoft.Compute/hostGroups/demoHostGroup/hosts/myHost",
 "status": "Pending"
 }
]
```

## Isolated VM

Check for pending updates for an isolated VM. In this example, the output is formatted as a table for readability.

```
az maintenance update list \
-g myMaintenanceRg \
--resource-name myVM \
--resource-type virtualMachines \
--provider-name Microsoft.Compute \
-o table
```

## Dedicated host

To check for pending updates for a dedicated host. In this example, the output is formatted as a table for readability. Replace the values for the resources with your own.

```
az maintenance update list \
--subscription 1111abcd-1a11-1a2b-1a12-123456789abc \
-g myHostResourceGroup \
--resource-name myHost \
--resource-type hosts \
--provider-name Microsoft.Compute \
--resource-parentname myHostGroup \
--resource-parent-type hostGroups \
-o table
```

# Apply updates

Use `az maintenance apply update` to apply pending updates. On success, this command will return JSON containing the details of the update.

## Isolated VM

Create a request to apply updates to an isolated VM.

```
az maintenance applyupdate create \
--subscription 1111abcd-1a11-1a2b-1a12-123456789abc \
--resource-group myMaintenanceRG \
--resource-name myVM \
--resource-type virtualMachines \
--provider-name Microsoft.Compute
```

## Dedicated host

Apply updates to a dedicated host.

```
az maintenance applyupdate create \
--subscription 1111abcd-1a11-1a2b-1a12-123456789abc \
--resource-group myHostResourceGroup \
--resource-name myHost \
--resource-type hosts \
--provider-name Microsoft.Compute \
--resource-parent-name myHostGroup \
--resource-parent-type hostGroups
```

## Check the status of applying updates

You can check on the progress of the updates using `az maintenance applyupdate get`.

You can use `default` as the update name to see results for the last update, or replace `myUpdateName` with the name of the update that was returned when you ran `az maintenance applyupdate create`.

```
Status : Completed
ResourceId : /subscriptions/12ae7457-4a34-465c-94c1-
 17c058c2bd25/resourcegroups/TestShants/providers/Microsoft.Com-
 pute/virtualMachines/DXT-test-04-iso
LastUpdateTime : 1/1/2020 12:00:00 AM
Id : /subscriptions/12ae7457-4a34-465c-94c1-
 17c058c2bd25/resourcegroups/TestShants/providers/Microsoft.Com-
 pute/virtualMachines/DXT-test-04-iso/providers/Microsoft.Mainten-
 ance/applyUpdates/default
Name : default
Type : Microsoft.Maintenance/applyUpdates
```

`LastUpdateTime` will be the time when the update got complete, either initiated by you or by the platform in case self-maintenance window was not used. If there has never been an update applied through maintenance control it will show default value.

### Isolated VM

```
az maintenance applyupdate get \
--resource-group myMaintenanceRG \
--resource-name myVM \
--resource-type virtualMachines \
--provider-name Microsoft.Compute \
--apply-update-name default
```

### Dedicated host

```
az maintenance applyupdate get \
--subscription 1111abcd-1a11-1a2b-1a12-123456789abc \
--resource-group myMaintenanceRG \
--resource-name myHost \
--resource-type hosts \
--provider-name Microsoft.Compute \
--resource-parent-name myHostGroup \
--resource-parent-type hostGroups \
--apply-update-name myUpdateName \
--query "{LastUpdate:lastUpdateTime, Name:name, ResourceGroup:resourceGroup, Status:status}" \
--output table
```

## Delete a maintenance configuration

Use `az maintenance configuration delete` to delete a maintenance configuration. Deleting the configuration removes the maintenance control from the associated resources.

```
az maintenance configuration delete \
--subscription 1111abcd-1a11-1a2b-1a12-123456789abc \
-g myResourceGroup \
--name myConfig
```

## Next steps

To learn more, see [Maintenance and updates](#).

# Preview: Control updates with Maintenance Control and Azure PowerShell

2/14/2020 • 5 minutes to read • [Edit Online](#)

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 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.

Maintenance control lets you decide when to apply updates to your isolated VMs.

With maintenance control, you can:

- Batch updates into one update package.
- Wait up to 35 days to apply updates.
- Automate platform updates for your maintenance window using Azure Functions.
- Maintenance configurations work across subscriptions and resource groups.

## IMPORTANT

Maintenance Control is currently in public preview. This preview version is provided without a service level agreement, and it's not recommended for production workloads. Certain features might not be supported or might have constrained capabilities. For more information, see [Supplemental Terms of Use for Microsoft Azure Previews](#).

## Limitations

- VMs must be on a [dedicated host](#), or be created using an [isolated VM size](#).
- After 35 days, an update will automatically be applied.
- User must have **Resource Contributor** access.

## Enable the PowerShell module

Make sure `PowerShellGet` is up to date.

```
Install-Module -Name PowerShellGet -Repository PSGallery -Force
```

The Az.Maintenance PowerShell cmdlets are in preview, so you need to install the module with the `AllowPrerelease` parameter in Cloud Shell or your local PowerShell installation.

```
Install-Module -Name Az.Maintenance -AllowPrerelease
```

If you are installing locally, make sure you open your PowerShell prompt as an administrator.

You may also be asked to confirm that you want to install from an *untrusted repository*. Type `y` or select **Yes to All** to install the module.

## Create a maintenance configuration

Create a resource group as a container for your configuration. In this example, a resource group named *myMaintenanceRG* is created in *eastus*. If you already have a resource group that you want to use, you can skip this part and replace the resource group name with your own in the rest of the examples.

```
New-AzResourceGroup `
 -Location eastus `
 -Name myMaintenanceRG
```

Use [New-AzMaintenanceConfiguration](#) to create a maintenance configuration. This example creates a maintenance configuration named *myConfig* scoped to the host.

```
$config = New-AzMaintenanceConfiguration `
 -ResourceGroup myMaintenanceRG `
 -Name myConfig `
 -MaintenanceScope host `
 -Location eastus
```

Using `-MaintenanceScope host` ensures that the maintenance configuration is used for controlling updates to the host.

If you try to create a configuration with the same name, but in a different location, you will get an error. Configuration names must be unique to your subscription.

You can query for available maintenance configurations using [Get-AzMaintenanceConfiguration](#).

```
Get-AzMaintenanceConfiguration | Format-Table -Property Name,Id
```

## Assign the configuration

Use [New-AzConfigurationAssignment](#) to assign the configuration to your isolated VM or Azure Dedicated Host.

### Isolated VM

Apply the configuration to a VM using the ID of the configuration. Specify `-ResourceType VirtualMachines` and supply the name of the VM for `-ResourceName`, and the resource group of the VM for `-ResourceGroupName`.

```
New-AzConfigurationAssignment `
 -ResourceGroupName myResourceGroup `
 -Location eastus `
 -ResourceName myVM `
 -ResourceType VirtualMachines `
 -ProviderName Microsoft.Compute `
 -ConfigurationAssignmentName $config.Name `
 -MaintenanceConfigurationId $config.Id
```

### Dedicated host

To apply a configuration to a dedicated host, you also need to include `-ResourceType hosts`, `-ResourceParentName` with the name of the host group, and `-ResourceParentType hostGroups`.

```
New-AzConfigurationAssignment `
-ResourceGroupName myResourceGroup `
-Location eastus `
-ResourceName myHost `
-ResourceType hosts `
-ResourceParentName myHostGroup `
-ResourceParentType hostGroups `
-ProviderName Microsoft.Compute `
-ConfigurationAssignmentName $config.Name `
-MaintenanceConfigurationId $config.Id
```

## Check for pending updates

Use [Get-AzMaintenanceUpdate](#) to see if there are pending updates. Use `-subscription` to specify the Azure subscription of the VM if it is different from the one that you are logged into.

If there are no updates to show, this command will return nothing. Otherwise, it will return a `PSApplyUpdate` object:

```
{
 "maintenanceScope": "Host",
 "impactType": "Freeze",
 "status": "Pending",
 "impactDurationInSec": 9,
 "notBefore": "2020-02-21T16:47:44.8728029Z",
 "properties": {
 "resourceId": "/subscriptions/39c6cced-4d6c-4dd5-af86-57499cd3f846/resourcegroups/Ignite2019/providers/Microsoft.Compute/virtualMachines/MCDemo3"
 }
}
```

### Isolated VM

Check for pending updates for an isolated VM. In this example, the output is formatted as a table for readability.

```
Get-AzMaintenanceUpdate `
-ResourceGroupName myResourceGroup `
-ResourceName myVM `
-ResourceType VirtualMachines `
-ProviderName Microsoft.Compute | Format-Table
```

### Dedicated host

To check for pending updates for a dedicated host. In this example, the output is formatted as a table for readability. Replace the values for the resources with your own.

```
Get-AzMaintenanceUpdate `
-ResourceGroupName myResourceGroup `
-ResourceName myHost `
-ResourceType hosts `
-ResourceParentName myHostGroup `
-ResourceParentType hostGroups `
-ProviderName Microsoft.Compute | Format-Table
```

## Apply updates

Use [New-AzApplyUpdate](#) to apply pending updates.

### Isolated VM

Create a request to apply updates to an isolated VM.

```
New-AzApplyUpdate `
-ResourceGroupName myResourceGroup `
-ResourceName myVM `
-ResourceType VirtualMachines `
-ProviderName Microsoft.Compute
```

On success, this command will return a `PSApplyUpdate` object. You can use the Name attribute in the `Get-AzApplyUpdate` command to check the update status. See [Check update status](#).

## Dedicated host

Apply updates to a dedicated host.

```
New-AzApplyUpdate `
-ResourceGroupName myResourceGroup `
-ResourceName myHost `
-ResourceType hosts `
-ResourceParentName myHostGroup `
-ResourceParentType hostGroups `
-ProviderName Microsoft.Compute
```

## Check update status

Use `Get-AzApplyUpdate` to check on the status of an update. The commands shown below show the status of the latest update by using `default` for the `-ApplyUpdateName` parameter. You can substitute the name of the update (returned by the `New-AzApplyUpdate` command) to get the status of a specific update.

```
Status : Completed
ResourceId : /subscriptions/12ae7457-4a34-465c-94c1-
17c058c2bd25/resourcegroups/TestShants/providers/Microsoft.Comp
ute/virtualMachines/DXT-test-04-iso
LastUpdateTime : 1/1/2020 12:00:00 AM
Id : /subscriptions/12ae7457-4a34-465c-94c1-
17c058c2bd25/resourcegroups/TestShants/providers/Microsoft.Comp
ute/virtualMachines/DXT-test-04-iso/providers/Microsoft.Maintenance/applyUpdates/default
Name : default
Type : Microsoft.Maintenance/applyUpdates
```

`LastUpdateTime` will be the time when the update got complete, either initiated by you or by the platform in case self-maintenance window was not used. If there has never been an update applied through maintenance control it will show default value.

## Isolated VM

Check for updates to a specific virtual machine.

```
Get-AzApplyUpdate `
-ResourceGroupName myResourceGroup `
-ResourceName myVM `
-ResourceType VirtualMachines `
-ProviderName Microsoft.Compute `
-ApplyUpdateName default
```

## Dedicated host

Check for updates to a dedicated host.

```
Get-AzApplyUpdate `
-ResourceGroupName myResourceGroup `
-ResourceName myHost `
-ResourceType hosts `
-ResourceParentName myHostGroup `
-ResourceParentType hostGroups `
-ProviderName Microsoft.Compute `
-ApplyUpdateName myUpdateName
```

## Remove a maintenance configuration

Use [Remove-AzMaintenanceConfiguration](#) to delete a maintenance configuration.

```
Remove-AzMaintenanceConfiguration `
-ResourceGroupName myResourceGroup `
-Name $config.Name
```

## Next steps

To learn more, see [Maintenance and updates](#).

# Azure Metadata Service: Scheduled Events for Linux VMs

2/28/2020 • 6 minutes to read • [Edit Online](#)

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.

For information about Scheduled Events on Windows, see [Scheduled Events for Windows VMs](#).

## NOTE

Scheduled Events is generally available in all Azure Regions. See [Version and Region Availability](#) for latest release information.

## Why use Scheduled Events?

Many applications can benefit from time to prepare for VM maintenance. The time can be used to perform application-specific tasks that improve availability, reliability, and serviceability, including:

- Checkpoint and restore.
- Connection draining.
- Primary replica failover.
- Removal from a load balancer pool.
- Event logging.
- Graceful shutdown.

With Scheduled Events, your application can discover when maintenance will occur and trigger tasks to limit its impact.

Scheduled Events provides events in the following use cases:

- [Platform initiated maintenance](#) (for example, VM reboot, live migration or memory preserving updates for host)
- Degraded hardware
- User-initiated maintenance (for example, a user restarts or redeploys a VM)
- [Spot VM](#) and [Spot scale set](#) instance evictions.

## The Basics

Metadata Service exposes information about running VMs by using a REST endpoint that's accessible from within the VM. The information is available via a nonroutable IP so that it's not exposed outside the VM.

### Scope

Scheduled events are delivered to:

- Standalone Virtual Machines.
- All the VMs in a cloud service.

- All the VMs in an availability set.
- All the VMs in a scale set placement group.

As a result, check the `Resources` field in the event to identify which VMs are affected.

## Endpoint Discovery

For VNET enabled VMs, Metadata Service is available from a static nonroutable IP, `169.254.169.254`. The full endpoint for the latest version of Scheduled Events is:

```
http://169.254.169.254/metadata/scheduledevents?api-version=2019-01-01
```

If the VM is not created within a Virtual Network, the default cases for cloud services and classic VMs, additional logic is required to discover the IP address to use. To learn how to [discover the host endpoint](#), see this sample.

## Version and Region Availability

The Scheduled Events service is versioned. Versions are mandatory; the current version is `2019-01-01`.

| VERSION    | RELEASE TYPE         | REGIONS | RELEASE NOTES                                                                                                                                                                  |
|------------|----------------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2019-01-01 | General Availability | All     | <ul style="list-style-type: none"> <li>Added support for virtual machine scale sets EventType 'Terminate'</li> </ul>                                                           |
| 2017-11-01 | General Availability | All     | <ul style="list-style-type: none"> <li>Added support for Spot VM eviction EventType 'Preempt'</li> </ul>                                                                       |
| 2017-08-01 | General Availability | All     | <ul style="list-style-type: none"> <li>Removed prepended underscore from resource names for IaaS VMs</li> <li>Metadata header requirement enforced for all requests</li> </ul> |
| 2017-03-01 | Preview              | All     | <ul style="list-style-type: none"> <li>Initial release</li> </ul>                                                                                                              |

### NOTE

Previous preview releases of Scheduled Events supported `{latest}` as the api-version. This format is no longer supported and will be deprecated in the future.

## Enabling and Disabling Scheduled Events

Scheduled Events is enabled for your service the first time you make a request for events. You should expect a delayed response in your first call of up to two minutes.

Scheduled Events is disabled for your service if it does not make a request for 24 hours.

## User-initiated Maintenance

User-initiated VM maintenance via the Azure portal, API, CLI, or PowerShell results in a scheduled event. You then can test the maintenance preparation logic in your application, and your application can prepare for user-initiated maintenance.

If you restart a VM, an event with the type `Reboot` is scheduled. If you redeploy a VM, an event with the type `Redeploy` is scheduled.

# Use the API

## Headers

When you query Metadata Service, you must provide the header `Metadata:true` to ensure the request wasn't unintentionally redirected. The `Metadata:true` header is required for all scheduled events requests. Failure to include the header in the request results in a "Bad Request" response from Metadata Service.

## Query for events

You can query for scheduled events by making the following call:

### Bash

```
curl -H Metadata:true http://169.254.169.254/metadata/scheduledevents?api-version=2019-01-01
```

A response contains an array of scheduled events. An empty array means that currently no events are scheduled. In the case where there are scheduled events, the response contains an array of events.

```
{
 "DocumentIncarnation": {IncarnationID},
 "Events": [
 {
 "EventId": {eventID},
 "EventType": "Reboot" | "Redeploy" | "Freeze" | "Preempt" | "Terminate",
 "ResourceType": "VirtualMachine",
 "Resources": [{resourceName}],
 "EventStatus": "Scheduled" | "Started",
 "NotBefore": {timeInUTC},
 }
]
}
```

## Event Properties

| PROPERTY  | DESCRIPTION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EventId   | Globally unique identifier for this event.<br><br>Example: <ul style="list-style-type: none"><li>• 602d9444-d2cd-49c7-8624-8643e7171297</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| EventType | Impact this event causes.<br><br>Values: <ul style="list-style-type: none"><li>• <code>Freeze</code> : The Virtual Machine is scheduled to pause for a few seconds. CPU and network connectivity may be suspended, but there is no impact on memory or open files.</li><li>• <code>Reboot</code> : The Virtual Machine is scheduled for reboot (non-persistent memory is lost).</li><li>• <code>Redeploy</code> : The Virtual Machine is scheduled to move to another node (ephemeral disks are lost).</li><li>• <code>Preempt</code> : The Spot Virtual Machine is being deleted (ephemeral disks are lost).</li><li>• <code>Terminate</code> : The virtual machine is scheduled to be deleted.</li></ul> |

| PROPERTY     | DESCRIPTION                                                                                                                                                                                                                                                                                                                                                               |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ResourceType | Type of resource this event affects.<br><br>Values: <ul style="list-style-type: none"><li>VirtualMachine</li></ul>                                                                                                                                                                                                                                                        |
| Resources    | List of resources this event affects. The list is guaranteed to contain machines from at most one <a href="#">update domain</a> , but it might not contain all machines in the UD.<br><br>Example: <ul style="list-style-type: none"><li>["FrontEnd_IN_0", "BackEnd_IN_0"]</li></ul>                                                                                      |
| EventStatus  | Status of this event.<br><br>Values: <ul style="list-style-type: none"><li>Scheduled : This event is scheduled to start after the time specified in the <code>NotBefore</code> property.</li><li>Started : This event has started.</li></ul><br>No <code>Completed</code> or similar status is ever provided. The event is no longer returned when the event is finished. |
| NotBefore    | Time after which this event can start.<br><br>Example: <ul style="list-style-type: none"><li>Mon, 19 Sep 2016 18:29:47 GMT</li></ul>                                                                                                                                                                                                                                      |

## Event Scheduling

Each event is scheduled a minimum amount of time in the future based on the event type. This time is reflected in an event's `NotBefore` property.

| EVENT TYPE | MINIMUM NOTICE                     |
|------------|------------------------------------|
| Freeze     | 15 minutes                         |
| Reboot     | 15 minutes                         |
| Redeploy   | 10 minutes                         |
| Preempt    | 30 seconds                         |
| Terminate  | User Configurable: 5 to 15 minutes |

## Start an event

After you learn of an upcoming event and finish your logic for graceful shutdown, you can approve the outstanding event by making a `POST` call to Metadata Service with `EventId`. This call indicates to Azure that it can shorten the minimum notification time (when possible).

The following JSON sample is expected in the `POST` request body. The request should contain a list of `StartRequests`. Each `StartRequest` contains `EventId` for the event you want to expedite:

```
{
 "StartRequests" : [
 {
 "EventId": {EventId}
 }
]
}
```

#### Bash sample

```
curl -H Metadata:true -X POST -d '{"StartRequests": [{"EventId": "f020ba2e-3bc0-4c40-a10b-86575a9eabd5"}]}'
http://169.254.169.254/metadata/scheduledevents?api-version=2019-01-01
```

#### NOTE

Acknowledging an event allows the event to proceed for all `Resources` in the event, not just the VM that acknowledges the event. Therefore, you can choose to elect a leader to coordinate the acknowledgement, which might be as simple as the first machine in the `Resources` field.

## Python sample

The following sample queries Metadata Service for scheduled events and approves each outstanding event:

```

#!/usr/bin/python

import json
import socket
import urllib2

metadata_url = "http://169.254.169.254/metadata/scheduledevents?api-version=2019-01-01"
this_host = socket.gethostname()

def get_scheduled_events():
 req = urllib2.Request(metadata_url)
 req.add_header('Metadata', 'true')
 resp = urllib2.urlopen(req)
 data = json.loads(resp.read())
 return data

def handle_scheduled_events(data):
 for evt in data['Events']:
 eventid = evt['EventId']
 status = evt['EventStatus']
 resources = evt['Resources']
 eventtype = evt['EventType']
 resourcetype = evt['ResourceType']
 notbefore = evt['NotBefore'].replace(" ", "_")
 if this_host in resources:
 print("+ Scheduled Event. This host " + this_host +
 " is scheduled for " + eventtype + " not before " + notbefore)
 # Add logic for handling events here

def main():
 data = get_scheduled_events()
 handle_scheduled_events(data)

if __name__ == '__main__':
 main()

```

## Next steps

- Watch [Scheduled Events on Azure Friday](#) to see a demo.
- Review the Scheduled Events code samples in the [Azure Instance Metadata Scheduled Events GitHub repository](#).
- Read more about the APIs that are available in the [Instance Metadata Service](#).
- Learn about [planned maintenance for Linux virtual machines in Azure](#).

# What is Azure Monitor for VMs (preview)?

2/27/2020 • 2 minutes to read • [Edit Online](#)

Azure Monitor for VMs monitors your Azure virtual machines (VM) 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. The following key features deliver in-depth insight:

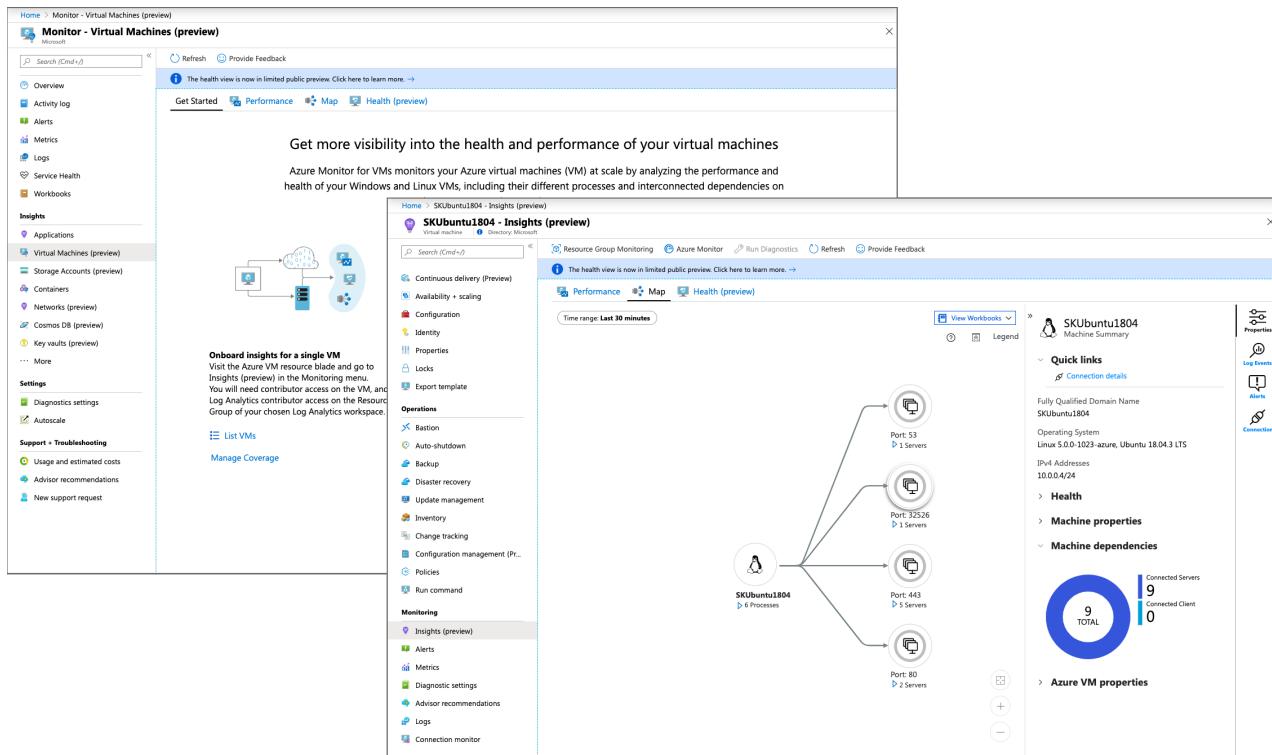
- **Pre-defined trending performance charts:** Display core performance metrics from the guest VM operating system.
- **Dependency map:** Displays the interconnected components with the VM from various resource groups and subscriptions.

## NOTE

We recently [announced changes](#) we are making to the Health feature based on the feedback we have received from our public preview customers. Given the number of changes we will be making, we are going to stop offering the Health feature for new customers. Existing customers can continue to use the health feature. For more details, please refer to our [General Availability FAQ](#).

Integration with Azure Monitor logs delivers powerful aggregation and filtering, and it can analyze data trends over time. Such comprehensive workload monitoring can't be achieved with Azure Monitor or Service Map alone.

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. For more information, see [access modes overview](#).



Azure Monitor for VMs can deliver predictable performance and availability of vital applications. It identifies

performance bottlenecks and network issues. Azure Monitor for VMs can also help you understand whether an issue is related to other dependencies.

## Data usage

When you deploy Azure Monitor for VMs, the data that's collected by your VMs is ingested and stored in Azure Monitor. Performance and dependency data collected are stored in a Log Analytics workspace. Based on the pricing that's published on the [Azure Monitor pricing page](#), Azure Monitor for VMs is billed for:

- The data that's ingested and stored.
- The alert rules that are created.
- The notifications that are sent.

The log size varies by the string lengths of performance counters, and it can increase with the number of logical disks and network adapters allocated to the VM. If you already have a workspace and are collecting these counters, no duplicate charges are applied. If you're already using Service Map, the only change you'll see is the additional connection data that's sent to Azure Monitor.

## Next steps

To understand the requirements and methods that help you monitor your virtual machines, review [Deploy Azure Monitor for VMs](#).

# Create, view, and manage metric alerts using Azure Monitor

2/27/2020 • 5 minutes to read • [Edit Online](#)

Metric alerts in Azure Monitor provide a way to get notified when one of your metrics crosses a threshold. Metric alerts work on a range of multi-dimensional platform metrics, custom metrics, Application Insights standard and custom metrics. In this article, we will describe how to create, view, and manage metric alert rules through Azure portal and Azure CLI. You can also create metric alert rules using Azure Resource Manager templates, which are described in [a separate article](#).

You can learn more about how metric alerts work from [metric alerts overview](#).

## Create with Azure portal

The following procedure describes how to create a metric alert rule in Azure portal:

1. In [Azure portal](#), click on **Monitor**. The Monitor blade consolidates all your monitoring settings and data in one view.
2. Click **Alerts** then click **+ New alert rule**.

### TIP

Most resource blades also have **Alerts** in their resource menu under **Monitoring**, you could create alerts from there as well.

3. Click **Select target**, in the context pane that loads, select a target resource that you want to alert on. Use **Subscription** and **Resource type** drop-downs to find the resource you want to monitor. You can also use the search bar to find your resource.
4. If the selected resource has metrics you can create alerts on, **Available signals** on the bottom right will include metrics. You can view the full list of resource types supported for metric alerts in this [article](#).
5. Once you have selected a target resource, click on **Add condition**.
6. You will see a list of signals supported for the resource, select the metric you want to create an alert on.
7. You will see a chart for the metric for the last six hours. Use the **Chart period** dropdown to select to see longer history for the metric.
8. If the metric has dimensions, you will see a dimensions table presented. Select one or more values per dimension.
  - The displayed dimension values are based on metric data from the last three days.
  - If the dimension value you're looking for isn't displayed, click "+" to add a custom value.
  - You can also **Select \*** for any of the dimensions. **Select \*** will dynamically scale the selection to all current and future values for a dimension.
9. The metric alert rule will evaluate the condition for all combinations of values selected. [Learn more about how alerting on multi-dimensional metrics works](#).
9. Select the **Threshold** type, **Operator**, and **Aggregation type**. This will determine the logic that the metric alert rule will evaluate.

- If you are using a **Static** threshold, continue to define a **Threshold value**. The metric chart can help determine what might be a reasonable threshold.
- If you are using a **Dynamic** threshold, continue to define the **Threshold sensitivity**. The metric chart will display the calculated thresholds based on recent data. [Learn more about Dynamic Thresholds condition type and sensitivity options](#).

10. Optionally, refine the condition by adjusting **Aggregation granularity** and **Frequency of evaluation**.
11. Click **Done**.
12. Optionally, add another criteria if you want to monitor a complex alert rule. Currently users can have alert rules with Dynamic Thresholds criteria as a single criterion.
13. Fill in **Alert details** like **Alert rule name**, **Description**, and **Severity**.
14. Add an action group to the alert either by selecting an existing action group or creating a new action group.
15. Click **Done** to save the metric alert rule.

**NOTE**

Metric alert rules created through portal are created in the same resource group as the target resource.

## View and manage with Azure portal

You can view and manage metric alert rules using the Manage Rules blade under Alerts. The procedure below shows you how to view your metric alert rules and edit one of them.

1. In Azure portal, navigate to **Monitor**
2. Click on **Alerts** and **Manage rules**
3. In the **Manage rules** blade, you can view all your alert rules across subscriptions. You can further filter the rules using **Resource group**, **Resource type**, and **Resource**. If you want to see only metric alerts, select **Signal type** as Metrics.

**TIP**

In the **Manage rules** blade, you can select multiple alert rules and enable/disable them. This might be useful when certain target resources need to be put under maintenance

4. Click on the name of the metric alert rule you want to edit
5. In the Edit Rule, click on the **Alert criteria** you want to edit. You can change the metric, threshold condition and other fields as required

**NOTE**

You can't edit the **Target resource** and **Alert Rule Name** after the metric alert is created.

6. Click **Done** to save your edits.

## With Azure CLI

The previous sections described how to create, view, and manage metric alert rules using Azure portal. This section will describe how to do the same using cross-platform [Azure CLI](#). Quickest way to start using Azure CLI is through

Azure Cloud Shell. For this article, we will use Cloud Shell.

1. Go to Azure portal, click on **Cloud Shell**.
2. At the prompt, you can use commands with `--help` option to learn more about the command and how to use it. For example, the following command shows you the list of commands available for creating, viewing, and managing metric alerts

```
az monitor metrics alert --help
```

3. You can create a simple metric alert rule that monitors if average Percentage CPU on a VM is greater than 90

```
az monitor metrics alert create -n {nameofthealert} -g {ResourceGroup} --scopes {VirtualMachineResourceID} --condition "avg Percentage CPU > 90" --description {descriptionofthealert}
```

4. You can view all the metric alerts in a resource group using the following command

```
az monitor metrics alert list -g {ResourceGroup}
```

5. You can see the details of a particular metric alert rule using the name or the resource ID of the rule.

```
az monitor metrics alert show -g {ResourceGroup} -n {AlertRuleName}
```

```
az monitor metrics alert show --ids {RuleResourceId}
```

6. You can disable a metric alert rule using the following command.

```
az monitor metrics alert update -g {ResourceGroup} -n {AlertRuleName} --enabled false
```

7. You can delete a metric alert rule using the following command.

```
az monitor metrics alert delete -g {ResourceGroup} -n {AlertRuleName}
```

## Next steps

- [Create metric alerts using Azure Resource Manager Templates](#).
- [Understand how metric alerts work](#).
- [Understand how metric alerts with Dynamic Thresholds condition work](#).
- [Understand the web hook schema for metric alerts](#)

# Create, view, and manage log alerts using Azure Monitor

2/27/2020 • 11 minutes to read • [Edit Online](#)

## Overview

This article shows you how to set up log alerts using the alerts interface inside Azure portal. Definition of an alert rule is in three parts:

- Target: Specific Azure resource, which is to be monitored
- Criteria: Specific condition or logic that when seen in Signal, should trigger action
- Action: Specific call sent to a receiver of a notification - email, SMS, webhook etc.

The term **Log Alerts** to describe alerts where signal is log query in a [Log Analytics workspace](#) or [Application Insights](#). Learn more about functionality, terminology, and types from [Log alerts - Overview](#).

### NOTE

Popular log data from [a Log Analytics workspace](#) is now also available on the metric platform in Azure Monitor. For details view, [Metric Alert for Logs](#)

## Managing log alerts from the Azure portal

Detailed next is step-by-step guide to using log alerts using the Azure portal interface.

### Create a log alert rule with the Azure portal

1. In the [portal](#), select **Monitor** and under the MONITOR section - choose **Alerts**.

The screenshot shows the 'Monitor - Alerts' page in the Azure portal. At the top left is the breadcrumb 'Home > Monitor - Alerts'. Below it is the title 'Monitor - Alerts' with the Microsoft logo. A search bar labeled 'Search (Ctrl+I)' is on the right. The navigation menu on the left includes: 'Overview' (with a circular icon), 'Activity log' (with a blue square icon), 'Alerts' (with a yellow exclamation mark icon, highlighted in blue), 'Metrics' (with a blue chart icon), 'Logs' (with a blue grid icon), 'Service Health' (with a blue heart icon), and 'Workbooks (preview)' (with a blue document icon).

2. Select the **New Alert Rule** button to create a new alert in Azure.



3. The Create Alert section is shown with the three parts consisting of: *Define alert condition*, *Define alert details*, and *Define action group*.

## Create rule

Rules management

|                                                                                                                 |                                                                                                                                     |                  |
|-----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|------------------|
|                                | <b>* RESOURCE</b><br>Select the target(s) that you wish to monitor<br><a href="#">Select</a>                                        | <b>HIERARCHY</b> |
|                                | <b>* CONDITION</b><br>No condition defined, click on 'Add condition' to select a signal and define its logic<br><a href="#">Add</a> |                  |
|                                | <b>ACTIONS</b><br>No configured actions<br><a href="#">Add</a>                                                                      |                  |
| <b>ALERT DETAILS</b>                                                                                            |                                                                                                                                     |                  |
| <b>* Alert rule name</b> <a href="#">?</a><br>Specify alert rule name. Sample: 'Percentage CPU greater than 70' |                                                                                                                                     |                  |
| Description<br>Specify alert description here...                                                                |                                                                                                                                     |                  |
| Enable rule upon creation<br><input checked="" type="radio"/> Yes <input type="radio"/> No                      |                                                                                                                                     |                  |

[Create alert rule](#)

4. Define the alert condition by using the **Select Resource** link and specifying the target by selecting a resource. Filter by choosing the *Subscription*, *Resource Type*, and required *Resource*.

#### NOTE

For creating a log alert - verify the **log** signal is available for the selected resource before you proceed.

## Select a resource



For metric and log based alert rules please select a specific target, for activity log alert rules you can select a subscription, a resource type or a resource group.

\* Filter by subscription i

Filter by resource type i

### RESOURCE

▼ **Fabrikam Enterprise**

▼ **FabrikamIT**



**logs**

Selection preview

Available signal(s) : Log, Metric, Activity Log

**Fabrikam Enterprise** >

**FabrikamIT** > **logs**

**Done**

5. **Log Alerts:** Ensure **Resource Type** is an analytics source like *Log Analytics* or *Application Insights* and signal type as **Log**, then once appropriate **resource** is chosen, click **Done**. Next use the **Add criteria** button to view list of signal options available for the resource and from the signal list **Custom log search** option for chosen log monitor service like *Log Analytics* or *Application Insights*.

## Configure signal logic

A signal can be of the form metric, a log search query or an activity log. Based on selected target(s), the list of supported signals is shown below. Select one to setup the alert condition.

### All signals (57)

| SIGNAL NAME                 |                      |                                                                                                    | MONITOR SERVICE | SIGNAL TYPE |
|-----------------------------|----------------------|----------------------------------------------------------------------------------------------------|-----------------|-------------|
| Custom log search           | Application Insights |  Log              |                 |             |
| PageView_Revenue            | Application Insights |  Log(Saved Query) |                 |             |
| All Administrative opera... | Administrative       |  Activity Log     |                 |             |
| Application Insights ana... | Administrative       |  Activity Log     |                 |             |
| Application Insights API... | Administrative       |  Activity Log     |                 |             |
| Application insights co...  | Administrative       |  Activity Log     |                 |             |
| Application insights co...  | Administrative       |  Activity Log     |                 |             |
| Application insights co...  | Administrative       |  Activity Log     |                 |             |
| Application Insights exp... | Administrative       |  Activity Log    |                 |             |
| Application Insights Co...  | Administrative       |  Activity Log   |                 |             |
| Subscription migration...   | Administrative       |  Activity Log   |                 |             |
| Migrate subscription to...  | Administrative       |  Activity Log   |                 |             |
| Rollback subscription to... | Administrative       |  Activity Log   |                 |             |
| All Security operations     | Security             |  Activity Log   |                 |             |
| Application Insights ana... | Security             |  Activity Log   |                 |             |
| Application Insights API... | Security             |  Activity Log   |                 |             |
| Application insights co...  | Security             |  Activity Log   |                 |             |
| Application insights co...  | Security             |  Activity Log   |                 |             |
| Application insights co...  | Security             |  Activity Log   |                 |             |
| Application Insights exp... | Security             |  Activity Log   |                 |             |

Done

#### NOTE

Alerts lists can import analytics query as signal type - **Log (Saved Query)**, as seen in above illustration. So users can perfect your query in Analytics and then save them for future use in alerts - more details on using saving query available at [using log query in Azure Monitor](#) or [shared query in application insights analytics](#).

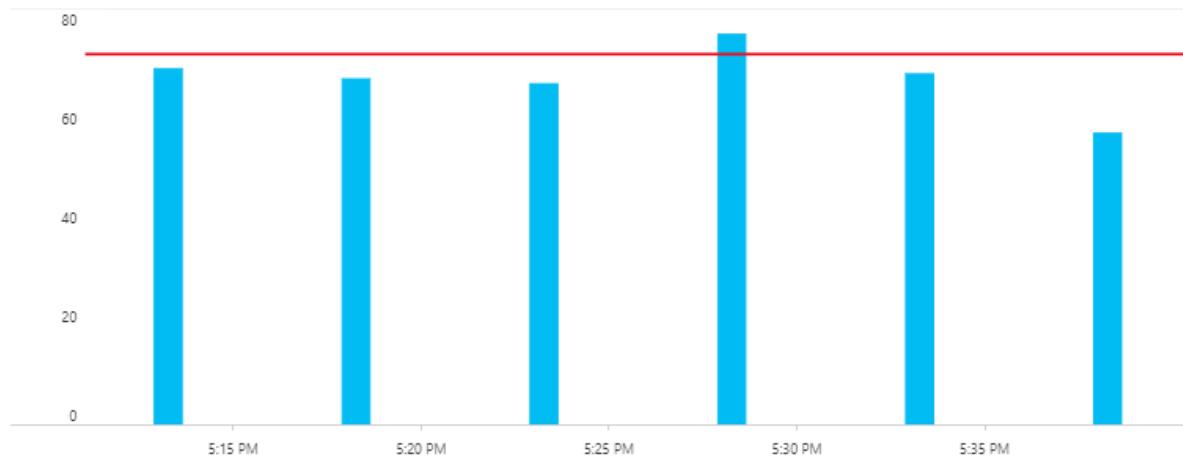
6. **Log Alerts:** Once selected, query for alerting can be stated in **Search Query** field; if the query syntax is incorrect the field displays error in RED. If the query syntax is correct - For reference historic data of the stated query is shown as a graph with option to tweak the time window from last six hours to last week.

## Configure signal logic

X

[-> Back to signal selection](#)

### Custom log search



\* Search query [?](#)

|                                            |                                     |
|--------------------------------------------|-------------------------------------|
| Event<br>  where EventLevelName == "Error" | <input checked="" type="checkbox"/> |
|--------------------------------------------|-------------------------------------|

[View result of query in Azure Monitor - Logs](#)

Query to be executed : Event | where EventLevelName == "Error" | count  
For time window : 7/19/2019, 5:28:16 PM - 7/19/2019, 5:38:16 PM

### Alert logic

|                                                 |                                            |                                                                               |
|-------------------------------------------------|--------------------------------------------|-------------------------------------------------------------------------------|
| Based on <a href="#">?</a><br>Number of results | Operator <a href="#">?</a><br>Greater than | * Threshold value <a href="#">?</a><br>75 <input checked="" type="checkbox"/> |
|-------------------------------------------------|--------------------------------------------|-------------------------------------------------------------------------------|

### Condition preview

Whenever the custom log search is greater than 75 count

### Evaluated based on

|                                               |                                               |
|-----------------------------------------------|-----------------------------------------------|
| * Period (in minutes) <a href="#">?</a><br>10 | Frequency (in minutes) <a href="#">?</a><br>5 |
|-----------------------------------------------|-----------------------------------------------|

[Done](#)

#### NOTE

Historical data visualization can only be shown if the query results have time details. If your query results in summarized data or specific column values - same is shown as a singular plot. For Metric Measurement type of Log Alerts using Application Insights or [switched to new API](#), you can specify which specific variable to group the data by using the **Aggregate on** option; as illustrated in below:

Configure signal logic

<- Back to signal selection

Custom log search

Pivoted on performanceBucket=<250... ▾

| Time    | Count |
|---------|-------|
| 4:50 PM | 70    |
| 4:55 PM | 80    |
| 5 PM    | 65    |
| 5:05 PM | 45    |
| 5:10 PM | 105   |

\* Search query ⓘ  
requests | summarize AggregatedValue=sum(itemCount) by bin(timestamp, 5min), performanceBucket

View result of query in Azure Monitor - Logs ⓘ

Query to be executed : requests | summarize AggregatedValue=sum(itemCount) by bin\_at(timestamp, 5min, now()), performanceBucket  
For time window : 7/19/2019, 4:43:06 PM - 7/19/2019, 5:13:06 PM

Alert logic

Based on ⓘ Metric measurement Aggregate value ⓘ Greater than \* Threshold value ⓘ 100

Trigger Alert Based On Consecutive breaches 1

Aggregate on ⓘ performanceBucket

Condition preview  
Whenever the custom log search is greater than 100 count

Evaluated based on

\* Period (in minutes) ⓘ 30 Frequency (in minutes) ⓘ 5

Done

7. **Log Alerts:** With the visualization in place, **Alert Logic** can be selected from shown options of Condition, Aggregation and finally Threshold. Finally specify in the logic, the time to assess for the specified condition, using **Period** option. Along with how often Alert should run by selecting **Frequency**. **Log Alerts** can be based on:

- **Number of Records:** An alert is created if the count of records returned by the query is either greater than or less than the value provided.
  - **Metric Measurement:** An alert is created if each *aggregate value* in the results exceeds the threshold value provided and it is *grouped by* chosen value. The number of breaches for an alert is the number of times the threshold is exceeded in the chosen time period. You can specify Total breaches for any combination of breaches across the results set or Consecutive breaches to require that the breaches must occur in consecutive samples.
8. As the second step, define a name for your alert in the **Alert rule name** field along with a **Description** detailing specifics for the alert and **Severity** value from the options provided. These details are reused in all alert emails, notifications, or push done by Azure Monitor. Additionally, user can choose to immediately activate the alert rule on creation by appropriately toggling **Enable rule upon creation** option.

For **Log Alerts** only, some additional functionality is available in Alert details:

- **SUPPRESS ALERTS:** When you turn on suppression for the alert rule, actions for the rule are disabled for a defined length of time after creating a new alert. The rule is still running and creates alert records provided the criteria is met. Allowing you time to correct the problem without running duplicate actions.

**ALERT DETAILS**

\* Alert rule name

Description

\* Severity

Enable rule upon creation

Suppress Alerts ?

**TIP**

Specify an suppress alert value greater than frequency of alert to ensure notifications are stopped without overlap

9. As the third and final step, specify if any **Action Group** needs to be triggered for the alert rule when alert condition is met. You can choose any existing Action Group with alert or create a new Action Group. According to selected Action Group, when alert is trigger Azure will: send email(s), send SMS(s), call Webhook(s), remediate using Azure Runbooks, push to your ITSM tool, etc. Learn more about [Action Groups](#).

**NOTE**

Refer to the [Azure subscription service limits](#) for limits on Runbook payloads triggered for log alerts via Azure action groups

For **Log Alerts** some additional functionality is available to override the default Actions:

- **Email Notification:** Overrides *e-mail subject* in the email, sent via Action Group; if one or more email actions exist in the said Action Group. You cannot modify the body of the mail and this field is **not** for email address.

- **Include custom Json payload:** Overrides the webhook JSON used by Action Groups; if one or more webhook actions exist in the said Action Group. User can specify format of JSON to be used for all webhooks configured in associated Action Group; for more information on webhook formats, see [webhook action for Log Alerts](#). View Webhook option is provided to check format using sample JSON data.

ACTIONS

No configured actions

Add

**Customize Actions**

Email subject ⓘ

Include custom Json payload for webhook ⓘ

10. If all fields are valid and with green tick the **create alert rule** button can be clicked and an alert is created in Azure Monitor - Alerts. All alerts can be viewed from the alerts Dashboard.

Home > ACMETelco-Portal - Logs (Analytics) > Create rule

Create rule

Rules management

**\* RESOURCE**

ACMETelco-Portal

**HIERARCHY**

Contoso Corp > ACMETelco

Select

**\* CONDITION**

Monthly cost in USD (Estimated) ⓘ

Whenever the Custom log search is Greater than 100 count

\$ 1.50

Total \$ 1.50

Add

**INFO** We currently support configuring only two metrics signals or one log search signal or one activity log signal per alert rule. An alert will be triggered when the conditions for all the above configured criteria are met

**ACTIONS**

View configured actions

Add

**Customize Actions**

Email subject ⓘ

Include custom Json payload for webhook ⓘ

**ALERT DETAILS**

\* Alert rule name ⓘ

Late Requests

Description

Checking if requests which are very late are exceeding threshold

\* Severity ⓘ

Sev 3

Enable rule upon creation

Yes  No

Suppress Alerts ⓘ

Create alert rule

Within a few minutes, the alert is active and triggers as previously described.

Users can also finalize their analytics query in [log analytics](#) and then push it to create an alert via 'Set Alert' button - then following instructions from Step 6 onwards in the above tutorial.

Run Time range: Set in query

Save Copy link Export New alert rule Pin

```
// List all computer heartbeats from the last hour
Heartbeat
| where TimeGenerated > ago(1h)
```

## View & manage log alerts in Azure portal

1. In the [portal](#), select **Monitor** and under the MONITOR section - choose **Alerts**.

2. The **Alerts Dashboard** is displayed - wherein all Azure Alerts (including log alerts) are displayed in a singular board; including every instance of when your log alert rule has fired. To learn more, see [Alert Management](#).

## NOTE

Log alert rules comprise of custom query-based logic provided by users and hence without a resolved state. Due to which every time the conditions specified in the log alert rule are met, it is fired.

3. Select the **Manage rules** button on the top bar, to navigate to the rule management section - where all alert rules created are listed; including alerts that have been disabled.



# Managing log alerts using Azure Resource Template

Log alerts in Azure Monitor are associated with resource type `Microsoft.Insights/scheduledQueryRules/`. For more information on this resource type, see [Azure Monitor - Scheduled Query Rules API reference](#). Log alerts for Application Insights or Log Analytics, can be created using [Scheduled Query Rules API](#).

## NOTE

Log alerts for Log Analytics can also be managed using legacy [Log Analytics Alert API](#) and legacy templates of [Log Analytics saved searches and alerts](#) as well. For more information on using the new ScheduledQueryRules API detailed here by default, see [Switch to new API for Log Analytics Alerts](#).

## Sample Log alert creation using Azure Resource Template

The following is the structure for [Scheduled Query Rules creation](#) based resource template using standard log search query of [number of results type log alert](#), with sample data set as variables.

```
{
 "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
 "contentVersion": "1.0.0.0",
 "parameters": {},
 "variables": {
 "alertLocation": "southcentralus",
 "alertName": "samplelogalert",
 "alertDescription": "Sample log search alert",
 "alertStatus": "true",
 "alertSource": {
 "Query": "requests",
 "SourceId": "/subscriptions/a123d7efg-123c-1234-5678-a12bc3defgh4/resourceGroups/myRG/providers/microsoft.insights/components/sampleAIapplication",
 "Type": "ResultCount"
 },
 "alertSchedule": {
 "Frequency": 15,
 "Time": 60
 },
 "alertActions": {
 "SeverityLevel": "4"
 },
 "alertTrigger": {
 "Operator": "GreaterThan",
 "Threshold": "1"
 },
 "actionGrp": {
 "ActionGroup": "/subscriptions/a123d7efg-123c-1234-5678-
```

```

a12bc3defgh4/resourceGroups/myRG/providers/microsoft.insights/actiongroups/sampleAG",
 "Subject": "Customized Email Header",
 "Webhook": "{ \"alertname\": \"#alertrulename\", \"IncludeSearchResults\":true }"
}
},
"resources": [
{
 "name": "[variables('alertName')]",
 "type": "Microsoft.Insights/scheduledQueryRules",
 "apiVersion": "2018-04-16",
 "location": "[variables('alertLocation')]",
 "properties": {
 "description": "[variables('alertDescription')]",
 "enabled": "[variables('alertStatus')]",
 "source": {
 "query": "[variables('alertSource').Query]",
 "dataSourceId": "[variables('alertSource').SourceId]",
 "queryType": "[variables('alertSource').Type]"
 },
 "schedule": {
 "frequencyInMinutes": "[variables('alertSchedule').Frequency]",
 "timeWindowInMinutes": "[variables('alertSchedule').Time]"
 },
 "action": {
 "odata.type": "Microsoft.WindowsAzure.Management.Monitoring.Alerts.Models.Microsoft.AppInsights.Nexus.DataContracts.Resources.ScheduledQueryRules.AlertingAction",
 "severity": "[variables('alertActions').SeverityLevel]",
 "aznsAction": {
 "actionGroup": "[array(variables('actionGrp').ActionGroup)]",
 "emailSubject": "[variables('actionGrp').Subject]",
 "customWebhookPayload": "[variables('actionGrp').Webhook]"
 },
 "trigger": {
 "thresholdOperator": "[variables('alertTrigger').Operator]",
 "threshold": "[variables('alertTrigger').Threshold]"
 }
 }
 }
}
]
}

```

The sample json above can be saved as (say) sampleScheduledQueryRule.json for the purpose of this walk through and can be deployed using [Azure Resource Manager in Azure portal](#).

### Log alert with cross-resource query using Azure Resource Template

The following is the structure for [Scheduled Query Rules creation](#) based resource template using [cross-resource log search query](#) of [metric measurement type log alert](#), with sample data set as variables.

```
{
 "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
 "contentVersion": "1.0.0.0",
 "parameters": {},
 "variables": {
 "alertLocation": "Region Name for your Application Insights App or Log Analytics Workspace",
 "alertName": "sample log alert",
 "alertDescr": "Sample log search alert",
 "alertStatus": "true",
 "alertSource": {
 "Query": "union workspace(\"servicews\").Update, app('serviceapp').requests | summarize AggregatedValue = count() by bin(TimeGenerated,1h), Classification",
 "Resource1": "/subscriptions/a123d7efg-123c-1234-5678-a12bc3defgh4/resourceGroups/contosoRG/providers/microsoft.OperationalInsights/workspaces/servicews",
 "Resource2": "/subscriptions/a123d7efg-123c-1234-5678-
```

```

a12bc3defgh4/resourceGroups/contosoRG/providers/microsoft.insights/components/serviceapp",
 "SourceId": "/subscriptions/a123d7efg-123c-1234-5678-
a12bc3defgh4/resourceGroups/contosoRG/providers/microsoft.OperationalInsights/workspaces/servicews",
 "Type":"ResultCount"
 },
 "alertSchedule":{
 "Frequency": 15,
 "Time": 60
 },
 "alertActions":{
 "SeverityLevel": "4",
 "SuppressTimeinMin": 20
 },
 "alertTrigger":{
 "Operator":"GreaterThan",
 "Threshold":"1"
 },
 "metricMeasurement": {
 "thresholdOperator": "Equal",
 "threshold": "1",
 "metricTriggerType": "Consecutive",
 "metricColumn": "Classification"
 },
 "actionGrp":{
 "ActionGroup": "/subscriptions/a123d7efg-123c-1234-5678-
a12bc3defgh4/resourceGroups/contosoRG/providers/microsoft.insights/actiongroups/sampleAG",
 "Subject": "Customized Email Header",
 "Webhook": "{ \"alertname\": \"#alertrulename\", \"IncludeSearchResults\":true }"
 }
 },
 "resources": [
 {
 "name": "[variables('alertName')]",
 "type": "Microsoft.Insights/scheduledQueryRules",
 "apiVersion": "2018-04-16",
 "location": "[variables('alertLocation')]",
 "properties": {
 "description": "[variables('alertDescr')]",
 "enabled": "[variables('alertStatus')]",
 "source": {
 "query": "[variables('alertSource').Query]",
 "authorizedResources": "[concat(array(variables('alertSource').Resource1),
array(variables('alertSource').Resource2))]",
 "dataSourceId": "[variables('alertSource').SourceId]",
 "queryType": "[variables('alertSource').Type]"
 },
 "schedule": {
 "frequencyInMinutes": "[variables('alertSchedule').Frequency]",
 "timeWindowInMinutes": "[variables('alertSchedule').Time]"
 },
 "action": {
 "odata.type": "Microsoft.WindowsAzure.Management.Monitoring.Alerts.Models.Microsoft.AppInsights.Nexus.DataContracts.Resources.ScheduledQueryRules.AlertingAction",
 "severity": "[variables('alertActions').SeverityLevel]",
 "throttlingInMin": "[variables('alertActions').SuppressTimeinMin]",
 "aznsAction": {
 "actionGroup": "[array(variables('actionGrp').ActionGroup)]",
 "emailSubject": "[variables('actionGrp').Subject]",
 "customWebhookPayload": "[variables('actionGrp').Webhook]"
 },
 "trigger": {
 "thresholdOperator": "[variables('alertTrigger').Operator]",
 "threshold": "[variables('alertTrigger').Threshold]",
 "metricTrigger": {
 "thresholdOperator": "[variables('metricMeasurement').thresholdOperator]",
 "threshold": "[variables('metricMeasurement').threshold]",
 "metricColumn": "[variables('metricMeasurement').metricColumn]",
 "metricTriggerType": "[variables('metricMeasurement').metricTriggerType]"
 }
 }
 }
 }
 }
]
}

```

```
 }
 }
}
}
```

#### IMPORTANT

When using cross-resource query in log alert, the usage of [authorizedResources](#) is mandatory and user must have access to the list of resources stated

The sample json above can be saved as (say) sampleScheduledQueryRule.json for the purpose of this walk through and can be deployed using [Azure Resource Manager in Azure portal](#).

## Managing log alerts using PowerShell

#### NOTE

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

Azure Monitor - [Scheduled Query Rules API](#) is a REST API and fully compatible with Azure Resource Manager REST API. And PowerShell cmdlets listed below are available to leverage the [Scheduled Query Rules API](#).

1. [New-AzScheduledQueryRule](#) : Powershell cmdlet to create a new log alert rule.
2. [Set-AzScheduledQueryRule](#) : Powershell cmdlet to update an existing log alert rule.
3. [New-AzScheduledQueryRuleSource](#) : Powershell cmdlet to create or update object specifying source parameters for a log alert. Used as input by [New-AzScheduledQueryRule](#) and [Set-AzScheduledQueryRule](#) cmdlet.
4. [New-AzScheduledQueryRuleSchedule](#): Powershell cmdlet to create or update object specifying schedule parameters for a log alert. Used as input by [New-AzScheduledQueryRule](#) and [Set-AzScheduledQueryRule](#) cmdlet.
5. [New-AzScheduledQueryRuleAlertingAction](#) : Powershell cmdlet to create or update object specifying action parameters for a log alert. Used as input by [New-AzScheduledQueryRule](#) and [Set-AzScheduledQueryRule](#) cmdlet.
6. [New-AzScheduledQueryRuleAznsActionGroup](#) : Powershell cmdlet to create or update object specifying action groups parameters for a log alert. Used as input by [New-AzScheduledQueryRuleAlertingAction](#) cmdlet.
7. [New-AzScheduledQueryRuleTriggerCondition](#) : Powershell cmdlet to create or update object specifying trigger condition parameters for log alert. Used as input by [New-AzScheduledQueryRuleAlertingAction](#) cmdlet.
8. [New-AzScheduledQueryRuleLogMetricTrigger](#) : Powershell cmdlet to create or update object specifying metric trigger condition parameters for [metric measurement type log alert](#). Used as input by [New-AzScheduledQueryRuleTriggerCondition](#) cmdlet.
9. [Get-AzScheduledQueryRule](#) : Powershell cmdlet to list existing log alert rules or a specific log alert rule
10. [Update-AzScheduledQueryRule](#) : Powershell cmdlet to enable or disable log alert rule
11. [Remove-AzScheduledQueryRule](#): Powershell cmdlet to delete an existing log alert rule

#### NOTE

ScheduledQueryRules PowerShell cmdlets can only manage rules created cmdlet itself or using Azure Monitor - [Scheduled Query Rules API](#). Log alert rules created using legacy [Log Analytics Alert API](#) and legacy templates of [Log Analytics saved searches and alerts](#) can be managed using ScheduledQueryRules PowerShell cmdlets only after user [switches API preference for Log Analytics Alerts](#).

Illustrated next are the steps for creation of a sample log alert rule using the scheduledQueryRules PowerShell cmdlets.

```
$source = New-AzScheduledQueryRuleSource -Query 'Heartbeat | summarize AggregatedValue = count() by bin(TimeGenerated, 5m), _ResourceId' -DataSourceId "/subscriptions/a123d7efg-123c-1234-5678-a12bc3defgh4/resourceGroups/contosoRG/providers/microsoft.OperationalInsights/workspaces/servicews"

$schedule = New-AzScheduledQueryRuleSchedule -FrequencyInMinutes 15 -TimeWindowInMinutes 30

$metricTrigger = New-AzScheduledQueryRuleLogMetricTrigger -ThresholdOperator "GreaterThan" -Threshold 2 - MetricTriggerType "Consecutive" -MetricColumn "_ResourceId"

$triggerCondition = New-AzScheduledQueryRuleTriggerCondition -ThresholdOperator "LessThan" -Threshold 5 - MetricTrigger $metricTrigger

$aznsActionGroup = New-AzScheduledQueryRuleAznsActionGroup -ActionGroup "/subscriptions/a123d7efg-123c-1234-5678-a12bc3defgh4/resourceGroups/contosoRG/providers/microsoft.insights/actiongroups/sampleAG" -EmailSubject "Custom email subject" -CustomWebhookPayload "{ `\"alert`:`#${alertrulename}`, `\"IncludeSearchResults`:true }"

$alertingAction = New-AzScheduledQueryRuleAlertingAction -AznsAction $aznsActionGroup -Severity "3" -Trigger $triggerCondition

New-AzScheduledQueryRule -ResourceGroupName "contosoRG" -Location "Region Name for your Application Insights App or Log Analytics Workspace" -Action $alertingAction -Enabled $true -Description "Alert description" - Schedule $schedule -Source $source -Name "Alert Name"
```

## Managing log alerts using CLI or API

Azure Monitor - [Scheduled Query Rules API](#) is a REST API and fully compatible with Azure Resource Manager REST API. Hence it can be used via Powershell using Resource Manager commands for Azure CLI.

#### NOTE

Log alerts for Log Analytics can also be managed using legacy [Log Analytics Alert API](#) and legacy templates of [Log Analytics saved searches and alerts](#) as well. For more information on using the new ScheduledQueryRules API detailed here by default, see [Switch to new API for Log Analytics Alerts](#).

Log alerts currently do not have dedicated CLI commands currently; but as illustrated below can be used via Azure Resource Manager CLI command for sample Resource Template shown earlier (sampleScheduledQueryRule.json) in the Resource Template section:

```
az group deployment create --resource-group contosoRG --template-file sampleScheduledQueryRule.json
```

On successful operation, 201 will be returned to state new alert rule creation or 200 will be returned if an existing alert rule was modified.

## Next steps

- Learn about [Log Alerts in Azure Alerts](#)

- Understand [Webhook actions for log alerts](#)
- Learn more about [Application Insights](#)
- Learn more about [log queries](#).

# Shared Image Galleries overview

11/13/2019 • 17 minutes to read • [Edit Online](#)

Shared Image Gallery is a service that helps you build structure and organization around your managed images. Shared Image Galleries provide:

- Managed global replication of images.
- Versioning and grouping of images for easier management.
- Highly available images with Zone Redundant Storage (ZRS) accounts in regions that support Availability Zones. ZRS offers better resilience against zonal failures.
- Sharing across subscriptions, and even between Active Directory (AD) tenants, using RBAC.
- Scaling your deployments with image replicas in each region.

Using a Shared Image Gallery you can share your images to different users, service principals, or AD groups within your organization. Shared images can be replicated to multiple regions, for quicker scaling of your deployments.

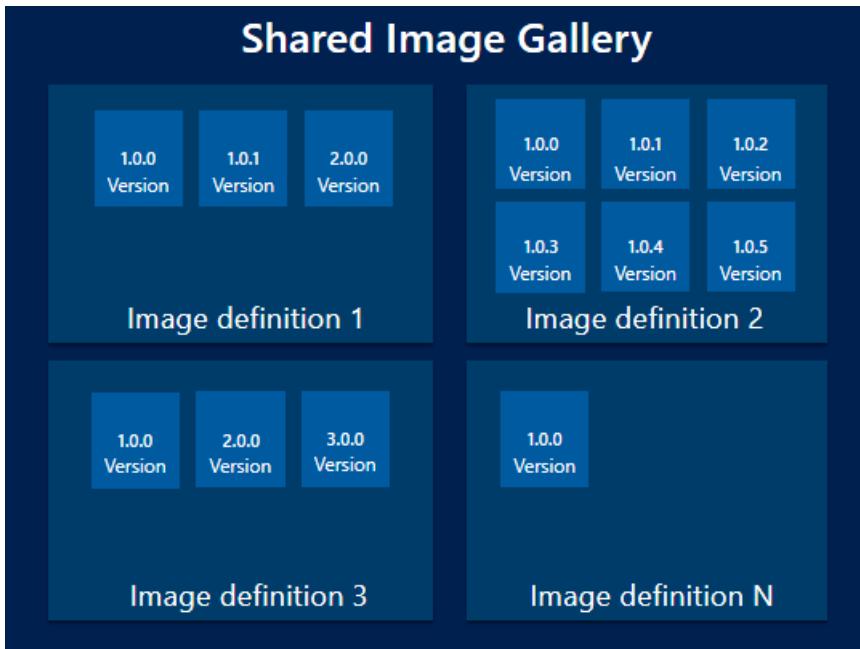
A managed image is a copy of either a full VM (including any attached data disks) or just the OS disk, depending on how you create the image. When you create a VM from the image, a copy of the VHDs in the image are used to create the disks for the new VM. The managed image remains in storage and can be used over and over again to create new VMs.

If you have a large number of managed images that you need to maintain and would like to make them available throughout your company, you can use a Shared Image Gallery as a repository that makes it easy to share your images.

The Shared Image Gallery feature has multiple resource types:

| RESOURCE                | DESCRIPTION                                                                                                                                                                                                                                                                                                                                  |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Managed image</b>    | A basic image that can be used alone or used to create an <b>image version</b> in an image gallery. Managed images are created from <b>generalized</b> VMs. A managed image is a special type of VHD that can be used to make multiple VMs and can now be used to create shared image versions.                                              |
| <b>Snapshot</b>         | A copy of a VHD that can be used to make an <b>image version</b> . Snapshots can be taken from a <b>specialized</b> VM (one that hasn't been generalized) then used alone or with snapshots of data disks, to create a specialized image version.                                                                                            |
| <b>Image gallery</b>    | Like the Azure Marketplace, an <b>image gallery</b> is a repository for managing and sharing images, but you control who has access.                                                                                                                                                                                                         |
| <b>Image definition</b> | Images are defined within a gallery and carry information about the image and requirements for using it within your organization. You can include information like whether the image is generalized or specialized, the operating system, minimum and maximum memory requirements, and release notes. It is a definition of a type of image. |

| RESOURCE             | DESCRIPTION                                                                                                                                                                                                                                                                                                                             |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Image version</b> | An <b>image version</b> 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 <b>image version</b> 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 information about using the image. An image definition is like a plan for all of the details around creating a specific image. You don't deploy a VM from an image definition, but from the image version created from the definition.

There are three parameters for each image definition that are used in combination - **Publisher**, **Offer** and **SKU**. These are used to find a specific image definition. You can have image versions that share one or two, but not all three values. For example, here are three image definitions and their values:

| IMAGE DEFINITION | PUBLISHER | OFFER   | SKU      |
|------------------|-----------|---------|----------|
| myImage1         | Contoso   | Finance | Backend  |
| myImage2         | Contoso   | Finance | Frontend |
| myImage3         | Testing   | Finance | Frontend |

All three of these have unique sets of values. The format is similar to how you can currently specify publisher, offer, and SKU for [Azure Marketplace images](#) in Azure PowerShell to get the latest version of a Marketplace image. Each image definition needs to have a unique set of these values.

The following are other parameters that can be set on your image definition so that you can more easily track your resources:

- Operating system state - You can set the OS state to [generalized or specialized](#).

- Operating system - can be either Windows or Linux.
- Description - use description to give more detailed information on why the image definition exists. For example, you might have an image definition for your front-end server that has the application pre-installed.
- Eula - can be used to point to an end-user license agreement specific to the image definition.
- Privacy Statement and Release notes - store release notes and privacy statements in Azure storage and provide a URI for accessing them as part of the image definition.
- End-of-life date - attach an end-of-life date to your image definition to be able to use automation to delete old image definitions.
- Tag - you can add tags when you create your image definition. For more information about tags, see [Using tags to organize your resources](#)
- Minimum and maximum vCPU and memory recommendations - if your image has vCPU and memory recommendations, you can attach that information to your image definition.
- Disallowed disk types - you can provide information about the storage needs for your VM. For example, if the image isn't suited for standard HDD disks, you add them to the disallow list.

## Generalized and specialized images

There are two operating system states supported by Shared Image 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 Windows, the Sysprep tool is used. For Linux, you can use `waagent -deprovision` or `-deprovision+user` parameters.

Specialized VMs have not been through a process to remove machine specific information and accounts. Also, VMs created from specialized images do not have an `osProfile` associated with them. This means that specialized images will have some limitations.

- Accounts that could be used to log into the VM can also be used on any VM created using the specialized image that is created from that VM.
- VMs will have the **Computer name** of the VM the image was taken from. You should change the computer name to avoid collisions.
- The `osProfile` is how some sensitive information is passed to the VM, using `secrets`. This may cause issues using KeyVault, WinRM and other functionality that uses `secrets` in the `osProfile`. In some cases, you can use managed service identities (MSI) to work around these limitations.

### IMPORTANT

Specialized images are currently in public preview. This preview version is provided without a service level agreement, and it's not recommended for production workloads. Certain features might not be supported or might have constrained capabilities. For more information, see [Supplemental Terms of Use for Microsoft Azure Previews](#).

**Known preview limitations** VMs can only be created from specialized images using the portal or API. There is no CLI or PowerShell support for the preview.

## Regional Support

Source regions are listed in the table below. All public regions can be target regions, but to replicate to Australia Central and Australia Central 2 you need to have your subscription whitelisted. To request whitelisting, go to: <https://azure.microsoft.com/global-infrastructure/australia/contact/>

| SOURCE REGIONS    |            |             |             |
|-------------------|------------|-------------|-------------|
| Australia Central | China East | South India | West Europe |

| Source Regions      |                |                  |                 |
|---------------------|----------------|------------------|-----------------|
| Australia Central 2 | China East 2   | Southeast Asia   | UK South        |
| Australia East      | China North    | Japan East       | UK West         |
| Australia Southeast | China North 2  | Japan West       | US DoD Central  |
| Brazil South        | East Asia      | Korea Central    | US DoD East     |
| Canada Central      | East US        | Korea South      | US Gov Arizona  |
| Canada East         | East US 2      | North Central US | US Gov Texas    |
| Central India       | East US 2 EUAP | North Europe     | US Gov Virginia |
| Central US          | France Central | South Central US | West India      |
| Central US EUAP     | France South   | West Central US  | West US         |
|                     |                |                  | West US 2       |

## Limits

There are limits, per subscription, for deploying resources using Shared Image Galleries:

- 100 shared image galleries, per subscription, per region
- 1,000 image definitions, per subscription, per region
- 10,000 image versions, per subscription, per region
- Any disk attached to the image must be less than or equal to 1TB in size

For more information, see [Check resource usage against limits](#) for examples on how to check your current usage.

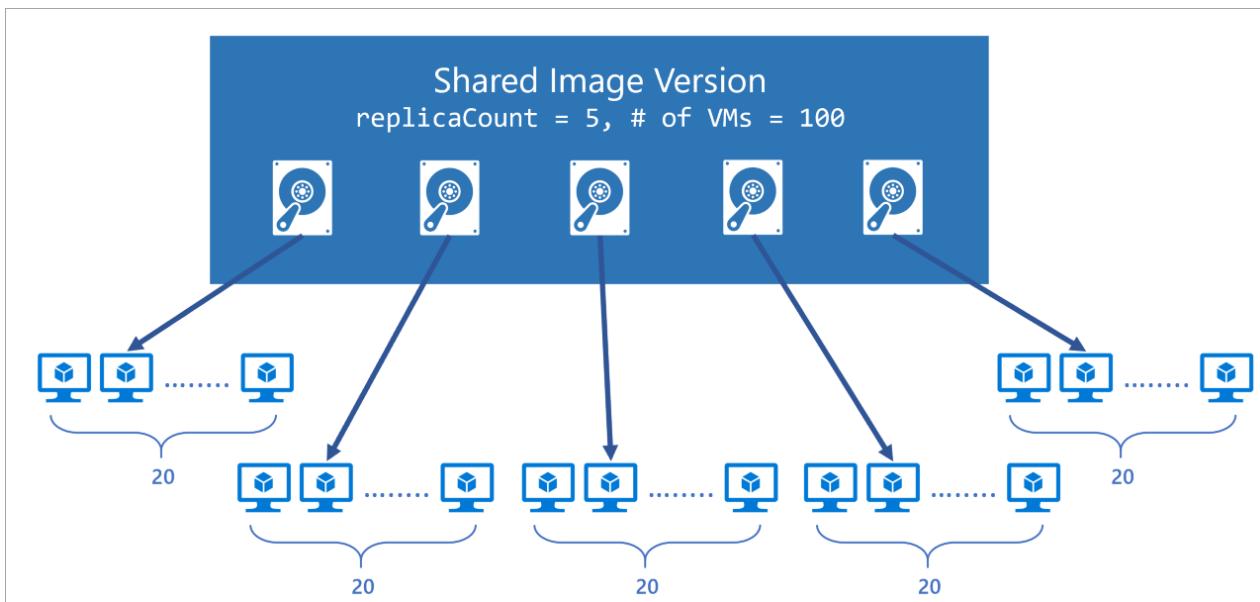
## Scaling

Shared Image Gallery allows you to specify the number of replicas you want Azure to keep of the images. 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.

With Shared Image Gallery, you can now deploy up to a 1,000 VM instances in a virtual machine scale set (up from 600 with managed images). Image replicas provide for better deployment performance, reliability and consistency. You can set a different replica count in each target region, based on the scale needs for the region. Since each replica is a deep copy of your image, this helps scale your deployments linearly with each extra replica. While we understand no two images or regions are the same, here's our general guideline on how to use replicas in a region:

- For non-Virtual Machine Scale Set (VMSS) Deployments - 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.
- For Virtual Machine Scale Set (VMSS) deployments - For every scale set deployment with up to 600 instances, we recommend you keep at least one replica. For example, if you are creating 5 scale sets concurrently, each with 600 VM instances using the same image in a single region, we suggest you keep at least 5 replicas of your image.

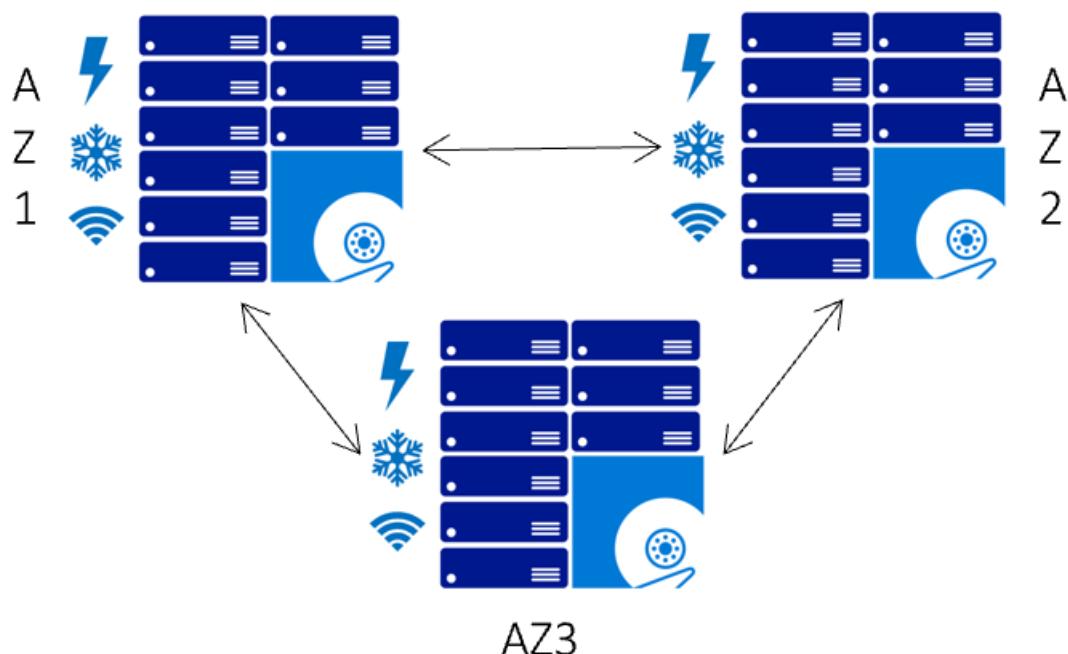
We always recommend you to overprovision the number of replicas due to factors like image size, content and OS type.



## Make your images highly available

Azure Zone Redundant Storage (ZRS) provides resilience against an Availability Zone failure in the region. With the general availability of Shared Image Gallery, you can choose to store your images in ZRS accounts in regions with Availability Zones.

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. Check the regional availability of ZRS [here](#).

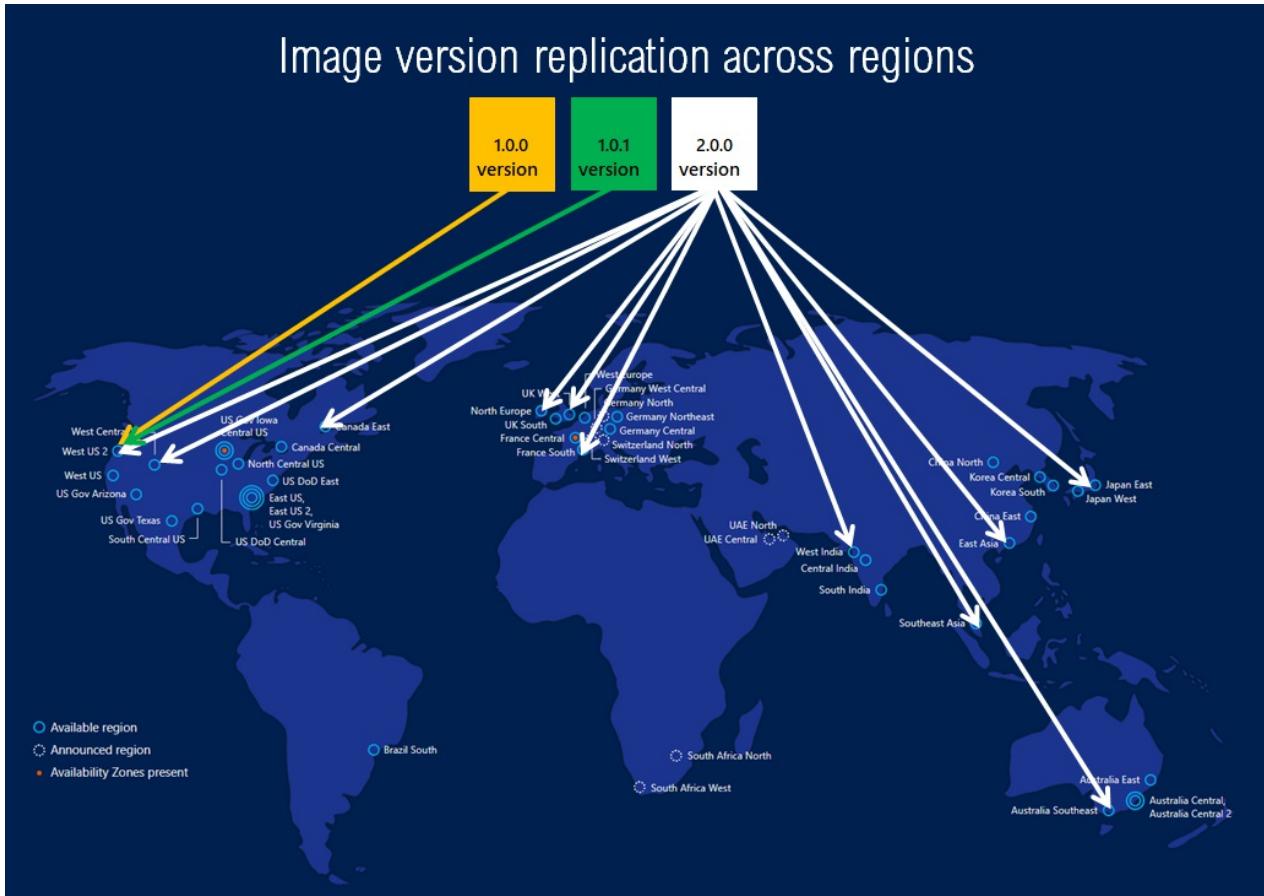


## Replication

Shared Image Gallery also allows you to replicate your images to other Azure regions automatically. Each Shared

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 multi-regions while all older versions are only available in 1 region. This can help save on storage costs for Shared Image versions.

The regions a Shared Image version is replicated to can be updated after creation time. The time it takes to replicate to different regions depends on the amount of data being copied and the number of regions the version is replicated to. This can take a few hours in some cases. While the replication is happening, you can view the status of replication per region. Once the image replication is complete in a region, you can then deploy a VM or scale-set using that image version in the region.



## Access

As the Shared Image Gallery, Image Definition, and Image version are all resources, they can be shared using the built-in native Azure RBAC controls. Using RBAC you can share these resources to other users, service principals, and groups. You can even share access to individuals outside of the tenant they were created within. Once a user has access to the Shared Image version, they can deploy a VM or a Virtual Machine Scale Set. Here is the sharing matrix that helps understand what the user gets access to:

| SHARED WITH USER     | SHARED IMAGE GALLERY | IMAGE DEFINITION | IMAGE VERSION |
|----------------------|----------------------|------------------|---------------|
| Shared Image Gallery | Yes                  | Yes              | Yes           |
| Image Definition     | No                   | Yes              | Yes           |

We recommend sharing at the Gallery level for the best experience. We do not recommend sharing individual image versions. For more information about RBAC, see [Manage access to Azure resources using RBAC](#).

Images can also be shared, at scale, even across tenants using a multi-tenant app registration. For more information about sharing images across tenants, see [Share gallery VM images across Azure tenants](#).

# Billing

There is no extra charge for using the Shared Image Gallery service. You will be charged for the following resources:

- Storage costs of storing the Shared Image versions. Cost depends on the number of replicas of the image version and the number of regions the version is replicated to. For example, if you have 2 images and both are replicated to 3 regions, then you will be charged for 6 managed disks based on their size. For more information, see [Managed Disks pricing](#).
- Network egress charges for replication of the first image version from the source region to the replicated regions. Subsequent replicas are handled within the region, so there are no additional charges.

## Updating resources

Once created, you can make some changes to the image gallery resources. These are limited to:

Shared image gallery:

- Description

Image definition:

- Recommended vCPUs
- Recommended memory
- Description
- End of life date

Image version:

- Regional replica count
- Target regions
- Exclude from latest
- End of life date

## SDK support

The following SDKs support creating Shared Image Galleries:

- [.NET](#)
- [Java](#)
- [Node.js](#)
- [Python](#)
- [Go](#)

## Templates

You can create Shared Image Gallery resource using templates. There are several Azure Quickstart Templates available:

- [Create a Shared Image Gallery](#)
- [Create an Image Definition in a Shared Image Gallery](#)
- [Create an Image Version in a Shared Image Gallery](#)
- [Create a VM from Image Version](#)

# Frequently asked questions

- [How can I list all the Shared Image Gallery resources across subscriptions?](#)
- [Can I move my existing image to the shared image gallery?](#)
- [Can I create an image version from a specialized disk?](#)
- [Can I move the Shared Image Gallery resource to a different subscription after it has been created?](#)
- [Can I replicate my image versions across clouds such as Azure China 21Vianet or Azure Germany or Azure Government Cloud?](#)
- [Can I replicate my image versions across subscriptions?](#)
- [Can I share image versions across Azure AD tenants?](#)
- [How long does it take to replicate image versions across the target regions?](#)
- [What is the difference between source region and target region?](#)
- [How do I specify the source region while creating the image version?](#)
- [How do I specify the number of image version replicas to be created in each region?](#)
- [Can I create the shared image gallery in a different location than the one for the image definition and image version?](#)
- [What are the charges for using the Shared Image Gallery?](#)
- [What API version should I use to create Shared Image Gallery and Image Definition and Image Version?](#)
- [What API version should I use to create Shared VM or Virtual Machine Scale Set out of the Image Version?](#)

## **How can I list all the Shared Image Gallery resources across subscriptions?**

To list all the Shared Image Gallery resources across subscriptions that you have access to on the Azure portal, follow the steps below:

1. Open the [Azure portal](#).
2. Go to **All Resources**.
3. Select all the subscriptions under which you'd like to list all the resources.
4. Look for resources of type **Private gallery**.

To see the image definitions and image versions, you should also select **Show hidden types**.

To list all the Shared Image Gallery resources across subscriptions that you have permissions to, use the following command in the Azure CLI:

```
az account list -otsv --query "[].id" | xargs -n 1 az sig list --subscription
```

## **Can I move my existing image to the shared image gallery?**

Yes. There are 3 scenarios based on the types of images you may have.

Scenario 1: If you have a managed image in the same subscription as your SIG, then you can create an image definition and image version from it.

Scenario 2: If you have an unmanaged image in the same subscription as your SIG, you can create a managed image from it, and then create an image definition and image version from it.

Scenario 3: If you have a VHD in your local file system, then you need to upload the VHD to a managed image, then you can create an image definition and image version from it.

- If the VHD is of a Windows VM, see [Upload a VHD](#).
- If the VHD is for a Linux VM, see [Upload a VHD](#)

## **Can I create an image version from a specialized disk?**

Yes, support for specialized disks as images is in preview. You can only create a VM from a specialized image using the portal ([Windows](#) or [Linux](#)) and API. There is no PowerShell support for the preview.

### **Can I move the Shared Image Gallery resource to a different subscription after it has been created?**

No, you cannot move the shared image gallery resource to a different subscription. However, you will be able to replicate the image versions in the gallery to other regions as required.

### **Can I replicate my image versions across clouds such as Azure China 21Vianet or Azure Germany or Azure Government Cloud?**

No, you cannot replicate image versions across clouds.

### **Can I replicate my image versions across subscriptions?**

No, you may replicate the image versions across regions in a subscription and use it in other subscriptions through RBAC.

### **Can I share image versions across Azure AD tenants?**

Yes, you can use RBAC to share to individuals across tenants. But, to share at scale, see "Share gallery images across Azure tenants" using [PowerShell](#) or [CLI](#).

### **How long does it take to replicate image versions across the target regions?**

The image version replication time is entirely dependent on the size of the image and the number of regions it is being replicated to. However, as a best practice, it is recommended that you keep the image small, and the source and target regions close for best results. You can check the status of the replication using the -ReplicationStatus flag.

### **What is the difference between source region and target region?**

Source region is the region in which your image version will be created, and target regions are the regions in which a copy of your image version will be stored. For each image version, you can only have one source region. Also, make sure that you pass the source region location as one of the target regions when you create an image version.

### **How do I specify the source region while creating the image version?**

While creating an image version, you can use the **--location** tag in CLI and the **-Location** tag in PowerShell to specify the source region. Please ensure the managed image that you are using as the base image to create the image version is in the same location as the location in which you intend to create the image version. Also, make sure that you pass the source region location as one of the target regions when you create an image version.

### **How do I specify the number of image version replicas to be created in each region?**

There are two ways you can specify the number of image version replicas to be created in each region:

1. The regional replica count which specifies the number of replicas you want to create per region.
2. The common replica count which is the default per region count in case regional replica count is not specified.

To specify the regional replica count, pass the location along with the number of replicas you want to create in that region: "South Central US=2".

If regional replica count is not specified with each location, then the default number of replicas will be the common replica count that you specified.

To specify the common replica count in CLI, use the **--replica-count** argument in the `az sig image-version create` command.

### **Can I create the shared image gallery in a different location than the one for the image definition and image version?**

Yes, it is possible. But, as a best practice, we encourage you to keep the resource group, shared image gallery, image definition, and image version in the same location.

## **What are the charges for using the Shared Image Gallery?**

There are no charges for using the Shared Image Gallery service, except the storage charges for storing the image versions and network egress charges for replicating the image versions from source region to target regions.

## **What API version should I use to create Shared Image Gallery and Image Definition and Image Version?**

To work with shared image galleries, image definitions, and image versions, we recommend you use API version 2018-06-01. Zone Redundant Storage (ZRS) requires version 2019-03-01 or later.

## **What API version should I use to create Shared VM or Virtual Machine Scale Set out of the Image Version?**

For VM and Virtual Machine Scale Set deployments using an image version, we recommend you use API version 2018-04-01 or higher.

## Next steps

Learn how to [deploy shared images](#).

# Create a shared image gallery with the Azure CLI

11/13/2019 • 7 minutes to read • [Edit Online](#)

A [Shared Image Gallery](#) simplifies custom image sharing across your organization. Custom images are like marketplace images, but you create them yourself. Custom images can be used to bootstrap configurations such as preloading applications, application configurations, and other OS configurations.

The Shared Image Gallery lets you share your custom VM images with others in your organization, within or across regions, within an AAD tenant. Choose which images you want to share, which regions you want to make them available in, and who you want to share them with. You can create multiple galleries so that you can logically group shared images.

The gallery is a top-level resource that provides full role-based access control (RBAC). Images can be versioned, and you can choose to replicate each image version to a different set of Azure regions. The gallery only works with Managed Images.

The Shared Image Gallery feature has multiple resource types. We will be using or building these in this article:

| RESOURCE                | DESCRIPTION                                                                                                                                                                                                                                                                                                                             |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Managed image</b>    | This is a basic image that can be used alone or used to create an <b>image version</b> in an image gallery. Managed images are created from generalized VMs. A managed image is a special type of VHD that can be used to make multiple VMs and can now be used to create shared image versions.                                        |
| <b>Image gallery</b>    | Like the Azure Marketplace, an <b>image gallery</b> is a repository for managing and sharing images, but you control who has access.                                                                                                                                                                                                    |
| <b>Image definition</b> | 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. It is a definition of a type of image.                                                             |
| <b>Image version</b>    | An <b>image version</b> 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 <b>image version</b> to create a VM, the image version is used to create new disks for the VM. Image versions can be used multiple times. |

## Before you begin

To complete the example in this article, you must have an existing managed image of a generalized VM. For more information, see [Tutorial: Create a custom image of an Azure VM with the Azure CLI](#). If the managed image contains a data disk, the data disk size cannot be more than 1 TB.

## Launch Azure Cloud Shell

The Azure Cloud Shell is a free interactive shell that you can use to run the steps in this article. It has common Azure tools preinstalled and configured to use with your account.

To open the Cloud Shell, just select **Try it** from the upper right corner of a code block. You can also launch Cloud Shell

in a separate browser tab by going to <https://shell.azure.com/bash>. Select **Copy** to copy the blocks of code, paste it into the Cloud Shell, and press enter to run it.

If you prefer to install and use the CLI locally, see [Install Azure CLI](#).

## Create an image gallery

An image gallery is the primary resource used for enabling image sharing. Allowed characters for Gallery name are uppercase or lowercase letters, digits, dots, and periods. The gallery name cannot contain dashes. Gallery names must be unique within your subscription.

Create an image gallery using [az sig create](#). The following example creates a gallery named *myGallery* in *myGalleryRG*.

```
az group create --name myGalleryRG --location WestCentralUS
az sig create --resource-group myGalleryRG --gallery-name myGallery
```

## Create an image definition

Image definitions create a logical grouping for images. They are used to manage information about the image versions that are created within them. Image definition names can be made up of uppercase or lowercase letters, digits, dots, dashes, and periods. For more information about the values you can specify for an image definition, see [Image definitions](#).

Create an initial image definition in the gallery using [az sig image-definition create](#).

```
az sig image-definition create \
--resource-group myGalleryRG \
--gallery-name myGallery \
--gallery-image-definition myImageDefinition \
--publisher myPublisher \
--offer myOffer \
--sku 16.04-LTS \
--os-type Linux
```

## Create an image version

Create versions of the image as needed using [az image gallery create-image-version](#). You will need to pass in the ID of the managed image to use as a baseline for creating the image version. You can use [az image list](#) to get information about images that are in a resource group.

Allowed characters for image version are numbers and periods. Numbers must be within the range of a 32-bit integer. Format: *MajorVersion.MinorVersion.Patch*.

In this example, the version of our image is *1.0.0* and we are going to create 2 replicas in the *West Central US* region, 1 replica in the *South Central US* region and 1 replica in the *East US 2* region using zone-redundant storage.

```
az sig image-version create \
--resource-group myGalleryRG \
--gallery-name myGallery \
--gallery-image-definition myImageDefinition \
--gallery-image-version 1.0.0 \
--target-regions "WestCentralUS" "SouthCentralUS=1" "EastUS2=1=Standard_ZRS" \
--replica-count 2 \
--managed-image "/subscriptions/<subscription
ID>/resourceGroups/myResourceGroup/providers/Microsoft.Compute/images/myImage"
```

#### NOTE

You need to wait for the image version to completely finish being built and replicated before you can use the same managed image to create another image version.

You can also store all of your image version replicas in [Zone Redundant Storage](#) by adding `--storage-account-type standard_zrs` when you create the image version.

## Share the gallery

We recommend that you share with other users at the gallery level. To get the object ID of your gallery, use [az sig show](#).

```
az sig show \
--resource-group myGalleryRG \
--gallery-name myGallery \
--query id
```

Use the object ID as a scope, along with an email address and [az role assignment create](#) to give a user access to the shared image gallery.

```
az role assignment create --role "Reader" --assignee <email address> --scope <gallery ID>
```

## Create a VM

Create a VM from the latest image version using [az vm create](#).

```
az vm create\
--resource-group myGalleryRG \
--name myVM \
--image "/subscriptions/subscription ID where the gallery is
located>/resourceGroups/myGalleryRG/providers/Microsoft.Compute/galleries/myGallery/images/myImageDefinition" \
--generate-ssh-keys
```

You can also use a specific version by using the image version ID for the `--image` parameter. For example, to use image version 1.0.0 type:

```
--image "/subscriptions/<subscription ID where the gallery is
located>/resourceGroups/myGalleryRG/providers/Microsoft.Compute/galleries/myGallery/images/myImageDefinition/versions/1.0.0"
```

## Using RBAC to share images

You can share images across subscriptions using Role-Based Access Control (RBAC). Any user that has read permissions to an image version, even across subscriptions, will be able to deploy a Virtual Machine using the image version.

For more information about how to share resources using RBAC, see [Manage access using RBAC and Azure CLI](#).

## List information

Get the location, status and other information about the available image galleries using [az sig list](#).

```
az sig list -o table
```

List the image definitions in a gallery, including information about OS type and status, using [az sig image-definition](#)

list.

```
az sig image-definition list --resource-group myGalleryRG --gallery-name myGallery -o table
```

List the shared image versions in a gallery, using [az sig image-version list](#).

```
az sig image-version list --resource-group myGalleryRG --gallery-name myGallery --gallery-image-definition myImageDefinition -o table
```

Get the ID of an image version using [az sig image-version show](#).

```
az sig image-version show \
--resource-group myGalleryRG \
--gallery-name myGallery \
--gallery-image-definition myImageDefinition \
--gallery-image-version 1.0.0 \
--query "id"
```

## Update resources

There are some limitations on what can be updated. The following items can be updated:

Shared image gallery:

- Description

Image definition:

- Recommended vCPUs
- Recommended memory
- Description
- End of life date

Image version:

- Regional replica count
- Target regions
- Exclusion from latest
- End of life date

If you plan on adding replica regions, do not delete the source managed image. The source managed image is needed for replicating the image version to additional regions.

Update the description of a gallery using ([az sig update](#).

```
az sig update \
--gallery-name myGallery \
--resource-group myGalleryRG \
--set description="My updated description."
```

Update the description of an image definition using [az sig image-definition update](#).

```
az sig image-definition update \
--gallery-name myGallery\
--resource-group myGalleryRG \
--gallery-image-definition myImageDefinition \
--set description="My updated description."
```

Update an image version to add a region to replicate to using [az sig image-version update](#). This change will take a while as the image gets replicated to the new region.

```
az sig image-version update \
--resource-group myGalleryRG \
--gallery-name myGallery \
--gallery-image-definition myImageDefinition \
--gallery-image-version 1.0.0 \
--add publishingProfile.targetRegions name=eastus
```

## Delete resources

You have to delete resources in reverse order, by deleting the image version first. After you delete all of the image versions, you can delete the image definition. After you delete all image definitions, you can delete the gallery.

Delete an image version using [az sig image-version delete](#).

```
az sig image-version delete \
--resource-group myGalleryRG \
--gallery-name myGallery \
--gallery-image-definition myImageDefinition \
--gallery-image-version 1.0.0
```

Delete an image definition using [az sig image-definition delete](#).

```
az sig image-definition delete \
--resource-group myGalleryRG \
--gallery-name myGallery \
--gallery-image-definition myImageDefinition
```

Delete an image gallery using [az sig delete](#).

```
az sig delete \
--resource-group myGalleryRG \
--gallery-name myGallery
```

## Next steps

[Azure Image Builder \(preview\)](#) can help automate image version creation, you can even use it to update and [create a new image version from an existing image version](#).

You can also create Shared Image Gallery resources using templates. There are several Azure Quickstart Templates available:

- [Create a Shared Image Gallery](#)
- [Create an Image Definition in a Shared Image Gallery](#)
- [Create an Image Version in a Shared Image Gallery](#)
- [Create a VM from Image Version](#)

For more information about Shared Image Galleries, see the [Overview](#). If you run into issues, see [Troubleshooting](#)

[shared image galleries.](#)

# Create an Azure Shared Image Gallery using the portal

12/9/2019 • 10 minutes to read • [Edit Online](#)

A [Shared Image Gallery](#) simplifies custom image sharing across your organization. Custom images are like marketplace images, but you create them yourself. Custom images can be used to bootstrap deployment tasks like preloading applications, application configurations, and other OS configurations.

The Shared Image Gallery lets you share your custom VM images with others in your organization, within or across regions, within an AAD tenant. Choose which images you want to share, which regions you want to make them available in, and who you want to share them with. You can create multiple galleries so that you can logically group shared images.

The gallery is a top-level resource that provides full role-based access control (RBAC). Images can be versioned, and you can choose to replicate each image version to a different set of Azure regions. The gallery only works with Managed Images.

The Shared Image Gallery feature has multiple resource types. We will be using or building these in this article:

| RESOURCE                | DESCRIPTION                                                                                                                                                                                                                                                                                                                                  |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Managed image</b>    | A basic image that can be used alone or used to create an <b>image version</b> in an image gallery. Managed images are created from <a href="#">generalized</a> VMs. A managed image is a special type of VHD that can be used to make multiple VMs and can now be used to create shared image versions.                                     |
| <b>Snapshot</b>         | A copy of a VHD that can be used to make an <b>image version</b> . Snapshots can be taken from a <a href="#">specialized</a> VM (one that hasn't been generalized) then used alone or with snapshots of data disks, to create a specialized image version.                                                                                   |
| <b>Image gallery</b>    | Like the Azure Marketplace, an <b>image gallery</b> is a repository for managing and sharing images, but you control who has access.                                                                                                                                                                                                         |
| <b>Image definition</b> | Images are defined within a gallery and carry information about the image and requirements for using it within your organization. You can include information like whether the image is generalized or specialized, the operating system, minimum and maximum memory requirements, and release notes. It is a definition of a type of image. |
| <b>Image version</b>    | An <b>image version</b> 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 <b>image version</b> to create a VM, the image version is used to create new disks for the VM. Image versions can be used multiple times.      |

## IMPORTANT

Specialized images are currently in public preview. This preview version is provided without a service level agreement, and it's not recommended for production workloads. Certain features might not be supported or might have constrained capabilities. For more information, see [Supplemental Terms of Use for Microsoft Azure Previews](#).

**Known preview limitations** VMs can only be created from specialized images using the portal or API. There is no CLI or PowerShell support for the preview.

## Before you begin

To complete the example in this article, you must have an existing managed image of a generalized VM, or a snapshot of a specialized VM. You can follow [Tutorial: Create a custom image of an Azure VM with Azure PowerShell](#) to create a managed image, or [Create a snapshot](#) for a specialized VM. For both managed images and snapshots, the data disk size cannot be more than 1 TB.

When working through this article, replace the resource group and VM names where needed.

## Sign in to Azure

Sign in to the Azure portal at <https://portal.azure.com>.

### NOTE

If you registered to use Shared Image Galleries during the preview, you might need to re-register the `Microsoft.Compute` provider. Open [Cloud Shell](#) and type: `az provider register -n Microsoft.Compute`

## Create an image gallery

An image gallery is the primary resource used for enabling image sharing. Allowed characters for Gallery name are uppercase or lowercase letters, digits, dots, and periods. The gallery name cannot contain dashes. Gallery names must be unique within your subscription.

The following example creates a gallery named *myGallery* in the *myGalleryRG* resource group.

1. Select **Create a resource** in the upper left-hand corner of the Azure portal.
2. Use the type **Shared image gallery** in the search box and select **Shared image gallery** in the results.
3. In the **Shared image gallery** page, click **Create**.
4. Select the correct subscription.
5. In **Resource group**, select **Create new** and type *myGalleryRG* for the name.
6. In **Name**, type *myGallery* for the name of the gallery.
7. Leave the default for **Region**.
8. You can type a short description of the gallery, like *My image gallery for testing*. and then click **Review + create**.
9. After validation passes, select **Create**.
10. When the deployment is finished, select **Go to resource**.

## Create an image definition

Image definitions create a logical grouping for images. They are used to manage information about the image versions that are created within them. Image definition names can be made up of uppercase or lowercase letters, digits, dots, dashes and periods. For more information about the values you can specify for an image definition,

see [Image definitions](#).

Create the gallery image definition inside of your gallery. In this example, the gallery image is named *myImageDefinition*.

1. On the page for your new image gallery, select **Add a new image definition** from the top of the page.
2. For **Image definition name**, type *myImageDefinition*.
3. For **Operating system**, select the correct option based on your source VM.
4. For **VM generation**, select the option based on your source VM. In most cases, this will be *Gen 1*. For more information, see [Support for generation 2 VMs](#).
5. For **Operating system state**, select the option based on your source VM. For more information, see [Generalized and specialized](#).
6. For **Publisher**, type *myPublisher*.
7. For **Offer**, type *myOffer*.
8. For **SKU**, type *mySKU*.
9. When finished, select **Review + create**.
10. After the image definition passes validation, select **Create**.
11. When the deployment is finished, select **Go to resource**.

## Create an image version

Create an image version from a managed image. In this example, the image version is *1.0.0* and it's replicated to both *West Central US* and *South Central US* datacenters. When choosing target regions for replication, remember that you also have to include the *source* region as a target for replication.

Allowed characters for image version are numbers and periods. Numbers must be within the range of a 32-bit integer. Format: *MajorVersion.MinorVersion.Patch*.

The steps for creating an image version are slightly different, depending on whether the source is a generalized image or a snapshot of a specialized VM.

### Option: Generalized

1. In the page for your image definition, select **Add version** from the top of the page.
2. In **Region**, select the region where your managed image is stored. Image versions need to be created in the same region as the managed image they are created from.
3. For **Name**, type *1.0.0*. The image version name should follow *major.minor.patch* format using integers.
4. In **Source image**, select your source managed image from the drop-down.
5. In **Exclude from latest**, leave the default value of *No*.
6. For **End of life date**, select a date from the calendar that is a couple of months in the future.
7. In **Replication**, leave the **Default replica count** as *1*. You need to replicate to the source region, so leave the first replica as the default and then pick a second replica region to be *East US*.
8. When you are done, select **Review + create**. Azure will validate the configuration.
9. When image version passes validation, select **Create**.
10. When the deployment is finished, select **Go to resource**.

It can take a while to replicate the image to all of the target regions.

### Option: Specialized

1. In the page for your image definition, select **Add version** from the top of the page.
2. In **Region**, select the region where your snapshot is stored. Image versions need to be created in the same region as the source they are created from.
3. For **Name**, type *1.0.0*. The image version name should follow *major.minor.patch* format using integers.

4. In **OS disk snapshot**, select the snapshot from your source VM from the drop-down. If your source VM had a data disk that you would like to include, select the correct **LUN** number from the drop-down, and then select the snapshot of the data disk for **Data disk snapshot**.
5. In **Exclude from latest**, leave the default value of *No*.
6. For **End of life date**, select a date from the calendar that is a couple of months in the future.
7. In **Replication**, leave the **Default replica count** as 1. You need to replicate to the source region, so leave the first replica as the default and then pick a second replica region to be *East US*.
8. When you are done, select **Review + create**. Azure will validate the configuration.
9. When image version passes validation, select **Create**.
10. When the deployment is finished, select **Go to resource**.

## Share the gallery

We recommend that you share access at the image gallery level. The following walks you through sharing the gallery that you just created.

1. Open the [Azure portal](#).
2. In the menu at the left, select **Resource groups**.
3. In the list of resource groups, select **myGalleryRG**. The blade for your resource group will open.
4. In the menu on the left of the **myGalleryRG** page, select **Access control (IAM)**.
5. Under **Add a role assignment**, select **Add**. The **Add a role assignment** pane will open.
6. Under **Role**, select **Reader**.
7. Under **assign access to**, leave the default of **Azure AD user, group, or service principal**.
8. Under **Select**, type in the email address of the person that you would like to invite.
9. If the user is outside of your organization, you will see the message **This user will be sent an email that enables them to collaborate with Microsoft**. Select the user with the email address and then click **Save**.

If the user is outside of your organization, they will get an email invitation to join the organization. The user needs to accept the invitation, then they will be able to see the gallery and all of the image definitions and versions in their list of resources.

## Create VMs

Now you can create one or more new VMs. This example creates a VM named *myVMfromImage*, in the *myResourceGroup* in the *East US* datacenter.

1. Go to your image definition. You can use the resource filter to show all image definitions available.
2. On the page for your image definition, select **Create VM** from the menu at the top of the page.
3. For **Resource group**, select **Create new** and type *myResourceGroup* for the name.
4. In **Virtual machine name**, type *myVM*.
5. For **Region**, select *East US*.
6. For **Availability options**, leave the default of *No infrastructure redundancy required*.
7. The value for **Image** is automatically filled with the **latest** image version if you started from the page for the image definition.
8. For **Size**, choose a VM size from the list of available sizes and then choose **Select**.
9. Under **Administrator account**, if the source VM was generalized, enter your **Username** and **SSH public key**. If the source VM was specialized, these options will be greyed out because the information from the source VM is used.
10. If you want to allow remote access to the VM, under **Public inbound ports**, choose **Allow selected ports** and then select **SSH (22)** from the drop-down. If you don't want to allow remote access to the VM, leave **None** selected for **Public inbound ports**.

11. When you are finished, select the **Review + create** button at the bottom of the page.
12. After the VM passes validation, select **Create** at the bottom of the page to start the deployment.

## Clean up resources

When no longer needed, you can delete the resource group, virtual machine, and all related resources. To do so, select the resource group for the virtual machine, select **Delete**, then confirm the name of the resource group to delete.

If you want to delete individual resources, you need to delete them in reverse order. For example, to delete an image definition, you need to delete all of the image versions created from that image.

## Next steps

You can also create Shared Image Gallery resource using templates. There are several Azure Quickstart Templates available:

- [Create a Shared Image Gallery](#)
- [Create an Image Definition in a Shared Image Gallery](#)
- [Create an Image Version in a Shared Image Gallery](#)
- [Create a VM from Image Version](#)

For more information about Shared Image Galleries, see the [Overview](#). If you run into issues, see [Troubleshooting shared image galleries](#).

# Share gallery VM images across Azure tenants

11/13/2019 • 3 minutes to read • [Edit Online](#)

Shared Image Galleries let you share images using RBAC. You can use RBAC to share images within your tenant, and even to individuals outside of your tenant. For more information about this simple sharing option, see the [Share the gallery](#).

But, if you want to share images outside of your Azure tenant, at scale, you should create an app registration to facilitate sharing. Using an app registration can enable more complex sharing scenarios, like:

- Managing shared images when one company acquires another, and the Azure infrastructure is spread across separate tenants.
- Azure Partners manage Azure infrastructure on behalf of their customers. Customization of images is done within the partners tenant, but the infrastructure deployments will happen in the customer's tenant.

## Create the app registration

Create an application registration that will be used by both tenants to share the image gallery resources.

1. Open the [App registrations \(preview\) in the Azure portal](#).
2. Select **New registration** from the menu at the top of the page.
3. In **Name**, type *myGalleryApp*.
4. In **Supported account types**, select **Accounts in any organizational directory and personal Microsoft accounts**.
5. In **Redirect URI**, type <https://www.microsoft.com> and then select **Register**. After the app registration has been created, the overview page will open.
6. On the overview page, copy the **Application (client) ID** and save for use later.
7. Select **Certificates & secrets**, and then select **New client secret**.
8. In **Description**, type *Shared image gallery cross-tenant app secret*.
9. In **Expires**, leave the default of **In 1 year** and then select **Add**.
10. Copy the value of the secret and save it to a safe place. You cannot retrieve it after you leave the page.

Give the app registration permission to use the shared image gallery.

1. In the Azure portal, select the Shared Image Gallery that you want to share with another tenant.
2. Select **Access control (IAM)**, and under **Add role assignment** select **Add**.
3. Under **Role**, select **Reader**.
4. Under **Assign access to:**, leave this as **Azure AD user, group, or service principal**.
5. Under **Select**, type *myGalleryApp* and select it when it shows up in the list. When you are done, select **Save**.

## Give Tenant 2 access

Give Tenant 2 access to the application by requesting a sign-in using a browser. Replace *<Tenant2 ID>* with the tenant ID for the tenant that you would like to share your image gallery with. Replace *<Application (client) ID>* with the application ID of the app registration you created. When done making the replacements, paste the URL into a browser and follow the sign-in prompts to sign into Tenant 2.

```
https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?client_id=<Application (client) ID>&response_type=code&redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
```

In the [Azure portal](#) sign in as Tenant 2 and give the app registration access to the resource group where you want to create the VM.

1. Select the resource group and then select **Access control (IAM)**. Under **Add role assignment** select **Add**.
2. Under **Role**, type **Contributor**.
3. Under **Assign access to:**, leave this as **Azure AD user, group, or service principal**.
4. Under **Select** type *myGalleryApp* then select it when it shows up in the list. When you are done, select **Save**.

#### NOTE

You need to wait for the image version to completely finish being built and replicated before you can use the same managed image to create another image version.

#### IMPORTANT

You cannot use the portal to deploy a VM from an image in another azure tenant. To create a VM from an image shared between tenants, you must use the Azure CLI or [Powershell](#).

## Create a VM using Azure CLI

Sign in the service principal for tenant 1 using the appId, the app key, and the ID of tenant 1. You can use

```
az account show --query "tenantId"
```

 to get the tenant IDs if needed.

```
az account clear
az login --service-principal -u '<app ID>' -p '<Secret>' --tenant '<tenant 1 ID>'
az account get-access-token
```

Sign in the service principal for tenant 2 using the appId, the app key, and the ID of tenant 2:

```
az login --service-principal -u '<app ID>' -p '<Secret>' --tenant '<tenant 2 ID>'
az account get-access-token
```

Create the VM. Replace the information in the example with your own.

```
az vm create \
 --resource-group myResourceGroup \
 --name myVM \
 --image "/subscriptions/<Tenant 1 subscription>/resourceGroups/<Resource group>/providers/Microsoft.Compute/galleries/<Gallery>/images/<Image definition>/versions/<version>" \
 --admin-username azureuser \
 --generate-ssh-keys
```

## Next steps

If you run into any issues, you can [troubleshoot shared image galleries](#).

# Troubleshooting shared image galleries

11/13/2019 • 3 minutes to read • [Edit Online](#)

If you run into issues while performing any operations on shared image galleries, image definitions, and image versions, run the failing command again in debug mode. Debug mode is activated by passing the **-debug** switch with CLI and the **-Debug** switch with PowerShell. Once you've located the error, follow this document to troubleshoot the errors.

## Unable to create a shared image gallery

Possible causes:

*The gallery name is invalid.*

Allowed characters for Gallery name are uppercase or lowercase letters, digits, dots, and periods. The gallery name cannot contain dashes. Change the gallery name and try again.

*The gallery name is not unique within your subscription.*

Pick another gallery name and try again.

## Unable to create an image definition

Possible causes:

*image definition name is invalid.*

Allowed characters for image definition are uppercase or lowercase letters, digits, dots, dashes, and periods. Change the image definition name and try again.

*The mandatory properties for creating an image definition are not populated.*

The properties such as name, publisher, offer, sku, and OS type are mandatory. Verify if all the properties are being passed.

Make sure that the **OSType**, either Linux or Windows, of the image definition is the same as the source managed image that you are using to create the image version.

## Unable to create an image version

Possible causes:

*Image version name is invalid.*

Allowed characters for image version are numbers and periods. Numbers must be within the range of a 32-bit integer. Format: *MajorVersion.MinorVersion.Patch*. Change the image version name and try again.

*Source managed image from which the image version is being created is not found.*

Check if the source image exists and is in the same region as the image version.

*The managed image isn't done being provisioned.*

Make sure the provisioning state of the source managed image is **Succeeded**.

*The target region list does not include the source region.*

The target region list must include the source region of the image version. Make sure you have included the source region in the list of target regions where you want Azure to replicate your image version to.

*Replication to all the target regions not completed.*

Use the **--expand ReplicationStatus** flag to check if the replication to all the specified target regions has been completed. If not, wait up to 6 hours for the job to complete. If it fails, run the command again to create and replicate the image version. If there are a lot of target regions the image version is being replicated to, consider doing the replication in phases.

## Unable to create a VM or a scale set

Possible causes:

*The user trying to create a VM or virtual machine scale set doesn't have the read access to the image version.*

Contact the subscription owner and ask them to give read access to the image version or the parent resources (like the shared image gallery or image definition) through [Role Based Access Control](#) (RBAC).

*The image version is not found.*

Verify that the region you are trying to create a VM or virtual machine scale in is included in the list of target regions of the image version. If the region is already in the list of target regions, then verify if the replication job has been completed. You can use the **-ReplicationStatus** flag to check if the replication to all the specified target regions has been completed.

*The VM or virtual machine scale set creation takes a long time.*

Verify that the **OSType** of the image version that you are trying to create the VM or virtual machine scale set from has the same **OSType** of the source managed image that you used to create the image version.

## Unable to share resources

The sharing of shared image gallery, image definition, and image version resources across subscriptions is enabled using [Role-Based Access Control](#) (RBAC).

## Replication is slow

Use the **--expand ReplicationStatus** flag to check if the replication to all the specified target regions has been completed. If not, wait for up to 6 hours for the job to complete. If it fails, trigger the command again to create and replicate the image version. If there are a lot of target regions the image version is being replicated to, consider doing the replication in phases.

## Azure limits and quotas

[Azure limits and quotas](#) apply to all shared image gallery, image definition, and image version resources. Make sure you are within the limits for your subscriptions.

## Next steps

Learn more about [shared image galleries](#).

# Preview: Azure Image Builder overview

7/9/2019 • 4 minutes to read • [Edit Online](#)

Standardized virtual machine (VM) images allow organizations to migrate to the cloud and ensure consistency in the deployments. Images typically include predefined security and configuration settings and necessary software. Setting up your own imaging pipeline requires time, infrastructure and setup, but with Azure VM Image Builder, just provide a simple configuration describing your image, submit it to the service, and the image is built, and distributed.

The Azure VM Image Builder (Azure Image Builder) lets you start with a Windows or Linux-based Azure Marketplace image, existing custom images or Red Hat Enterprise Linux (RHEL) ISO and begin to add your own customizations. Because the Image Builder is built on [HashiCorp Packer](#), you can also import your existing Packer shell provisioner scripts. You can also specify where you would like your images hosted, in the [Azure Shared Image Gallery](#), as a managed image or a VHD.

## IMPORTANT

Azure Image Builder is currently in public preview. This preview version is provided without a service level agreement, and it's not recommended for production workloads. Certain features might not be supported or might have constrained capabilities. For more information, see [Supplemental Terms of Use for Microsoft Azure Previews](#).

## Preview features

For the preview, these features are supported:

- Creation of golden baseline images, that includes your minimum security and corporate configurations, and allow departments to customize it further for their needs.
- Patching of existing images, Image Builder will allow you to continually patch existing custom images.
- Integration with the Azure Shared Image Gallery, allows you to distribute, version, and scale images globally, and gives you an image management system.
- Integration with existing image build pipelines, just call Image Builder from your pipeline, or use the simple Preview Image Builder Azure DevOps Task.
- Migrate an existing image customization pipeline to Azure. Use your existing scripts, commands, and processes to customize images.
- Use Red Hat Bring Your Own Subscription support. Create Red Hat Enterprise images for use with your eligible, unused Red Hat subscriptions.
- Creation of images in VHD format.

## Regions

The Azure Image Builder Service will be available for preview in these regions. Images can be distributed outside of these regions.

- East US
- East US 2
- West Central US
- West US
- West US 2

# OS support

AIB will support Azure Marketplace base OS images:

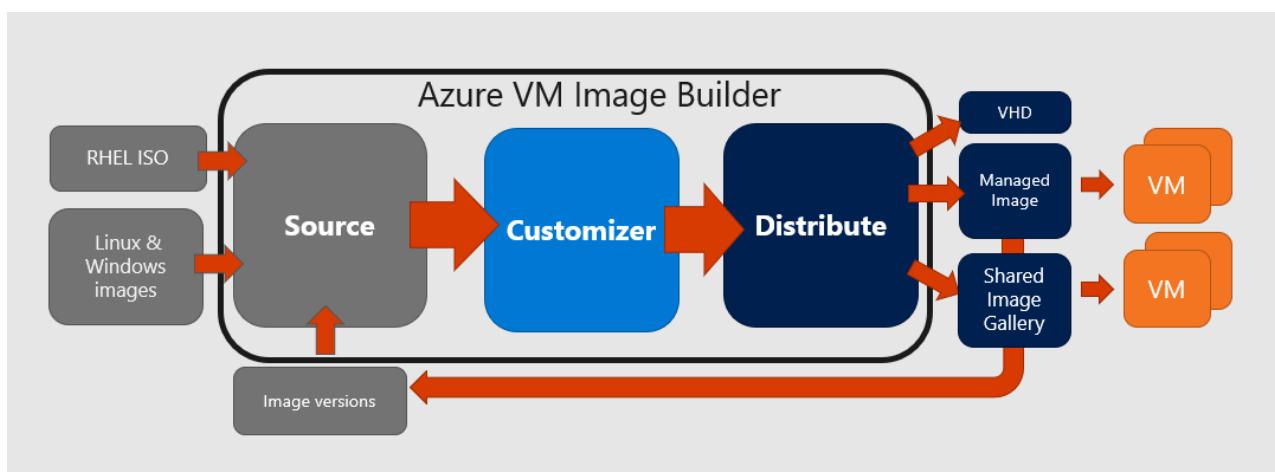
- Ubuntu 18.04
- Ubuntu 16.04
- RHEL 7.6, 7.7
- CentOS 7.6, 7.7
- SLES 12 SP4
- SLES 15, SLES 15 SP1
- Windows 10 RS5 Enterprise/Professional/Enterprise for Virtual Desktop (EVD)
- Windows 2016
- Windows 2019

AIB will support RHEL ISO's, as a source for:

- RHEL 7.3
- RHEL 7.4
- RHEL 7.5

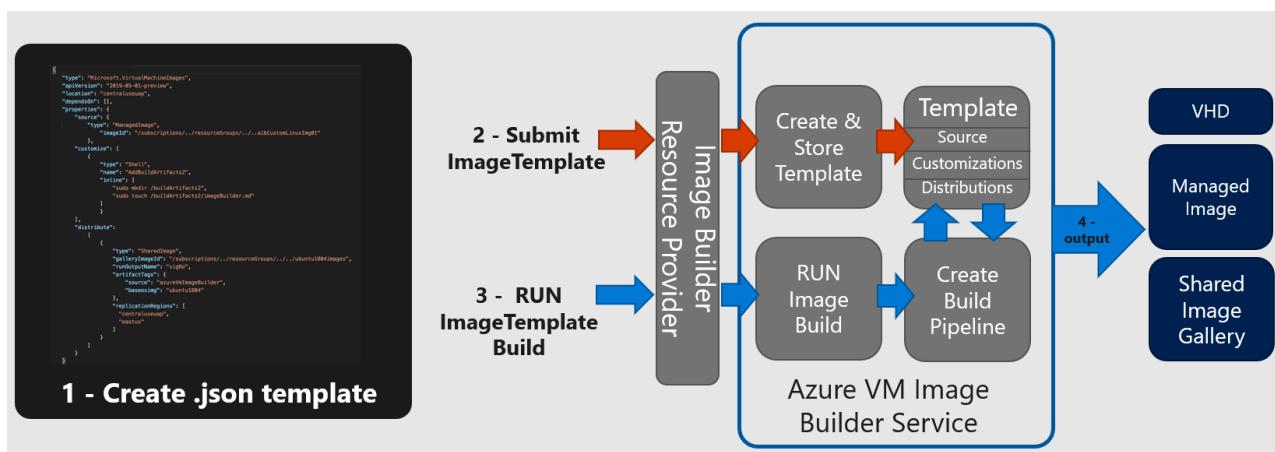
RHEL 7.6 ISOs are not supported, but are being tested.

## How it works



The Azure Image Builder is a fully managed Azure service that is accessible by an Azure resource provider. The Azure Image Builder process has three main parts: source, customize and distribute, these are represented in a template. The diagram below shows the components, with some of their properties.

### Image Builder process



1. Create the Image Template as a json file. This json file contains information about the image source, customizations, and distribution. There are multiple examples in the [Azure Image Builder GitHub repository](#).
2. Submit it to the service, this will create an Image Template artifact in the resource group you specify. In the background, Image Builder will download the source image or ISO, and scripts as needed. These are stored in a separate resource group that is automatically created in your subscription, in the format: IT\_<DestinationResourceGroup>\_<TemplateName>.
3. Once the Image Template is created, you can then build the image. In the background Image Builder uses the template and source files to create a VM (default size: Standard\_D1\_v2), network, public IP, NSG, and storage in the IT\_<DestinationResourceGroup>\_<TemplateName> resource group.
4. As part of the image creation, Image builder distributes the image it according to the template, then deletes the additional resources in the IT\_<DestinationResourceGroup>\_<TemplateName> resource group that was created for the process.

## Permissions

To allow Azure VM Image Builder to distribute images to either the managed images or to a Shared Image Gallery, you will need to provide 'Contributor' permissions for the service "Azure Virtual Machine Image Builder" (app ID: cf32a0cc-373c-47c9-9156-0db11f6a6dfc) on the resource groups.

If you are using an existing custom managed image or image version, then the Azure Image Builder will need a minimum of 'Reader' access to those resource groups.

You can assign access using the Azure CLI:

```
az role assignment create \
--assignee cf32a0cc-373c-47c9-9156-0db11f6a6dfc \
--role Contributor \
--scope /subscriptions/$subscriptionID/resourceGroups/<distributeResourceGroupName>
```

You can assign access using the PowerShell:

```
New-AzRoleAssignment -ObjectId ef511139-6170-438e-a6e1-763dc31bdf74 -Scope
/subscriptions/$subscriptionID/resourceGroups/<distributeResourceGroupName> -RoleDefinitionName Contributor
```

If the service account is not found, that may mean that the subscription where you are adding the role assignment has not yet registered for the resource provider.

## Costs

You will incur some compute, networking and storage costs when creating, building and storing images with Azure Image Builder. These costs are similar to the costs incurred in manually creating custom images. For the resources, you will be charged at your Azure rates.

During the image creation process, files are downloaded and stored in the `IT_<DestinationResourceGroup>_<TemplateName>` resource group, which will incur a small storage costs. If you do not want to keep these, delete the **Image Template** after the image build.

Image Builder creates a VM using a D1v2 VM size, and the storage, and networking needed for the VM. These resources will last for the duration of the build process, and will be deleted once Image Builder has finished creating the image.

Azure Image Builder will distribute the image to your chosen regions, which might incur network egress charges.

## Next steps

To try out the Azure Image Builder, see the articles for building [Linux](#) or [Windows](#) images.

# Preview: Create a Linux VM with Azure Image Builder

7/31/2019 • 5 minutes to read • [Edit Online](#)

This article shows you how you can create a customized Linux image using the Azure Image Builder and the Azure CLI. The example in this article uses three different [customizers](#) for customizing the image:

- Shell (ScriptUri) - downloads and runs a [shell script](#).
- Shell (inline) - runs specific commands. In this example, the inline commands include creating a directory and updating the OS.
- File - copies a [file from GitHub](#) into a directory on the VM.

You can also specify a `buildTimeoutInMinutes`. The default is 240 minutes, and you can increase a build time to allow for longer running builds.

We will be using a sample json template to configure the image. The json file we are using is here: [helloImageTemplateLinux.json](#).

## IMPORTANT

Azure Image Builder is currently in public preview. This preview version is provided without a service level agreement, and it's not recommended for production workloads. Certain features might not be supported or might have constrained capabilities. For more information, see [Supplemental Terms of Use for Microsoft Azure Previews](#).

## Register the features

To use Azure Image Builder during the preview, you need to register the new feature.

```
az feature register --namespace Microsoft.VirtualMachineImages --name VirtualMachineTemplatePreview
```

Check the status of the feature registration.

```
az feature show --namespace Microsoft.VirtualMachineImages --name VirtualMachineTemplatePreview | grep state
```

Check your registration.

```
az provider show -n Microsoft.VirtualMachineImages | grep registrationState
az provider show -n Microsoft.Storage | grep registrationState
```

If they do not say registered, run the following:

```
az provider register -n Microsoft.VirtualMachineImages
az provider register -n Microsoft.Storage
```

## Setup example variables

We will be using some pieces of information repeatedly, so we will create some variables to store that information.

```
Resource group name - we are using myImageBuilderRG in this example
imageResourceGroup=myImageBuilderRGLinux
Datacenter location - we are using West US 2 in this example
location=WestUS2
Name for the image - we are using myBuilderImage in this example
imageName=myBuilderImage
Run output name
runOutputName=aibLinux
```

Create a variable for your subscription ID. You can get this using `az account show | grep id`.

```
subscriptionID=<Your subscription ID>
```

## Create the resource group.

This is used to store the image configuration template artifact and the image.

```
az group create -n $imageResourceGroup -l $location
```

## Set permissions on the resource group

Give Image Builder 'contributor' permission to create the image in the resource group. Without the proper permissions, the image build will fail.

The `--assignee` value is the app registration ID for the Image Builder service.

```
az role assignment create \
 --assignee cf32a0cc-373c-47c9-9156-0db11f6a6dfc \
 --role Contributor \
 --scope /subscriptions/$subscriptionID/resourceGroups/$imageResourceGroup
```

## Download the template example

A parameterized sample image configuration template has been created for you to use. Download the sample json file and configure it with the variables you set earlier.

```
curl
https://raw.githubusercontent.com/danielsollondon/azvmimagebuilder/master/quickstarts/0_Creating_a_Custom_Linux_Managed_Image/helloImageTemplateLinux.json -o helloImageTemplateLinux.json

sed -i -e "s/<subscriptionID>/$subscriptionID/g" helloImageTemplateLinux.json
sed -i -e "s/<rgName>/$imageResourceGroup/g" helloImageTemplateLinux.json
sed -i -e "s/<region>/$location/g" helloImageTemplateLinux.json
sed -i -e "s/<imageName>/$imageName/g" helloImageTemplateLinux.json
sed -i -e "s/<runOutputName>/$runOutputName/g" helloImageTemplateLinux.json
```

You can modify this example .json as needed. For example, you can increase the value of `buildTimeoutInMinutes` to allow for longer running builds. You can edit the file in Cloud Shell using a text editor like `vi`.

```
vi helloImageTemplateLinux.json
```

#### NOTE

For source image, you must always [specify a version](#), you cannot use `latest`.

If you add or change the resource group where the image is being distributed, you need to make sure the [permissions are set for the resource group](#).

## Submit the image configuration

Submit the image configuration to the VM Image Builder service

```
az resource create \
--resource-group $imageResourceGroup \
--properties @helloImageTemplateLinux.json \
--is-full-object \
--resource-type Microsoft.VirtualMachineImages/imageTemplates \
-n helloImageTemplateLinux01
```

If it completes successfully, it will return a success message, and create an image builder configuration template artifact in the \$imageResourceGroup. You can see the resource group in the portal if you enable 'Show hidden types'.

Also, in the background, Image Builder creates a staging resource group in your subscription. Image Builder uses the staging resource group for the image build. The name of the resource group will be in this format:

`IT_<DestinationResourceGroup>_<TemplateName>`.

#### IMPORTANT

Do not delete the staging resource group directly. If you delete the image template artifact, it will automatically delete the staging resource group. For more information, see the [Clean up](#) section at the end of this article.

If the service reports a failure during the image configuration template submission, see the [troubleshooting](#) steps. You will also need to delete the template before you retry submitting the build. To delete the template:

```
az resource delete \
--resource-group $imageResourceGroup \
--resource-type Microsoft.VirtualMachineImages/imageTemplates \
-n helloImageTemplateLinux01
```

## Start the image build

Start the image build.

```
az resource invoke-action \
--resource-group $imageResourceGroup \
--resource-type Microsoft.VirtualMachineImages/imageTemplates \
-n helloImageTemplateLinux01 \
--action Run
```

Wait until the build is complete, for this example, it can take 10-15 minutes.

If you encounter any errors, please review these [troubleshooting](#) steps.

# Create the VM

Create the VM using the image you built.

```
az vm create \
 --resource-group $imageResourceGroup \
 --name myVM \
 --admin-username azureuser \
 --image $imageName \
 --location $location \
 --generate-ssh-keys
```

Get the IP address from the output of creating the VM and use it to SSH to the VM.

```
ssh azureuser@<pubIp>
```

You should see the image was customized with a Message of the Day as soon as your SSH connection is established!

```

** This VM was built from the: **
** !! AZURE VM IMAGE BUILDER Custom Image !! **
** You have just been Customized :-) **

```

Type `exit` when you are done to close the SSH connection.

## Check the source

In the Image Builder Template, in the 'Properties', you will see the source image, customization script it runs, and where it is distributed.

```
cat helloImageTemplateLinux.json
```

For more detailed information about this json file, see [Image builder template reference](#)

## Clean up

When you are done, you can delete the resources.

Delete the image builder template.

```
az resource delete \
 --resource-group $imageResourceGroup \
 --resource-type Microsoft.VirtualMachineImages/imageTemplates \
 -n helloImageTemplateLinux01
```

Delete the image resource group.

```
az group delete -n $imageResourceGroup
```

## Next steps

To learn more about the components of the json file used in this article, see [Image Builder template reference](#).

# Preview: Create an Azure Image Builder template

1/30/2020 • 15 minutes to read • [Edit Online](#)

Azure Image Builder uses a json file to pass information into the Image Builder service. In this article we will go over the sections of the json file, so you can build your own. To see examples of full json files, see the [Azure Image Builder GitHub](#).

This is the basic template format:

```
{
 "type": "Microsoft.VirtualMachineImages/imageTemplates",
 "apiVersion": "2019-05-01-preview",
 "location": "<region>",
 "tags": {
 "<name>": "<value>",
 "<name>": "<value>"
 },
 "identity": {},
 "dependsOn": [],
 "properties": {
 "buildTimeoutInMinutes": <minutes>,
 "vmProfile": {
 "
 "vmSize": "<vmSize>"
 "
 },
 "build": {},
 "customize": {},
 "distribute": {}
 }
}
```

## Type and API version

The `type` is the resource type, which must be `"Microsoft.VirtualMachineImages/imageTemplates"`. The `apiVersion` will change over time as the API changes, but should be `"2019-05-01-preview"` for preview.

```
"type": "Microsoft.VirtualMachineImages/imageTemplates",
"apiVersion": "2019-05-01-preview",
```

## Location

The location is the region where the custom image will be created. For the Image Builder preview, the following regions are supported:

- East US
- East US 2
- West Central US
- West US
- West US 2

```
"location": "<region>",
```

## vmProfile

By default Image Builder will use a "Standard\_D1\_v2" build VM, you can override this, for example, if you want to customize an Image for a GPU VM, you need a GPU VM size. This is optional.

```
{
 "vmSize": "Standard_D1_v2"
},
```

## osDiskSizeGB

By default, Image Builder will not change the size of the image, it will use the size from the source image. You can adjust the size of the OS Disk (Win and Linux), note, do not go too small than the minimum required space required for the OS. This is optional, and a value of 0 means leave the same size as the source image. This is optional.

```
{
 "osDiskSizeGB": 100
},
```

## Tags

These are key/value pairs you can specify for the image that's generated.

## Depends on (optional)

This optional section can be used to ensure that dependencies are completed before proceeding.

```
"dependsOn": [],
```

For more information, see [Define resource dependencies](#).

## Identity

By default, Image Builder supports using scripts, or copying files from multiple locations, such as GitHub and Azure storage. To use these, they must be publicly accessible.

You can also use an Azure User-Assigned Managed Identity, defined by you, to allow Image Builder access Azure Storage, as long as the identity has been granted a minimum of 'Storage Blob Data Reader' on the Azure storage account. This means you do not need to make the storage blobs externally accessible, or setup SAS Tokens.

```
"identity": {
 "type": "UserAssigned",
 "userAssignedIdentities": {
 "<imgBuilderId>": {}
 }
},
```

For a complete example, see [Use an Azure User-Assigned Managed Identity to access files in Azure Storage](#).

Image Builder support for a User-Assigned Identity:

- Supports a single identity only
- Does not support custom domain names

To learn more, see [What is managed identities for Azure resources?](#). For more information on deploying this feature, see [Configure managed identities for Azure resources on an Azure VM using Azure CLI](#).

## Properties: source

The `source` section contains information about the source image that will be used by Image Builder.

The API requires a 'SourceType' that defines the source for the image build, currently there are three types:

- ISO - use this when the source is a RHEL ISO.
- PlatformImage - indicated the source image is a Marketplace image.
- ManagedImage - use this when starting from a regular managed image.
- SharedImageVersion - this is used when you are using an image version in a Shared Image Gallery as the source.

### ISO source

Azure Image Builder only supports using published Red Hat Enterprise Linux 7.x Binary DVD ISOs, for preview. Image Builder supports:

- RHEL 7.3
- RHEL 7.4
- RHEL 7.5

```
"source": {
 "type": "ISO",
 "sourceURI": "<sourceURI from the download center>",
 "sha256Checksum": "<checksum associated with ISO>"
}
```

To get the `sourceURI` and `sha256Checksum` values, go to <https://access.redhat.com/downloads> then select the product **Red Hat Enterprise Linux**, and a supported version.

In the list of **Installers and Images for Red Hat Enterprise Linux Server**, you need to copy the link for Red Hat Enterprise Linux 7.x Binary DVD, and the checksum.

#### NOTE

The access tokens of the links are refreshed at frequent intervals, so every time you want to submit a template, you must check if the RH link address has changed.

### PlatformImage source

Azure Image Builder supports Windows Server and client, and Linux Azure Marketplace images, see [here](#) for the full list.

```
"source": {
 "type": "PlatformImage",
 "publisher": "Canonical",
 "offer": "UbuntuServer",
 "sku": "18.04-LTS",
 "version": "18.04.201903060"
},
```

The properties here are the same that are used to create VM's, using AZ CLI, run the below to get the properties:

```
az vm image list -l westus -f UbuntuServer -p Canonical --output table --all
```

#### NOTE

Version cannot be 'latest', you must use the command above to get a version number.

### ManagedImage source

Sets the source image as an existing managed image of a generalized VHD or VM. The source managed image must be of a supported OS, and be in the same region as your Azure Image Builder template.

```
"source": {
 "type": "ManagedImage",
 "imageId": "/subscriptions/<subscriptionId>/resourceGroups/{destinationResourceGroupName}/providers/Microsoft.Compute/images/<imageName>"
}
```

The `imageId` should be the ResourceId of the managed image. Use `az image list` to list available images.

### SharedImageVersion source

Sets the source image an existing image version in a Shared Image Gallery. The image version must be of a supported OS, and the image must be replicated to the same region as your Azure Image Builder template.

```
"source": {
 "type": "SharedImageVersion",
 "imageVersionID": "/subscriptions/<subscriptionId>/resourceGroups/<resourceGroup>/pro
viders/Microsoft.Compute/galleries/<sharedImageGalleryName>/images/<imageDefinitionName>/versions/<imageVersion>"
}
```

The `imageVersionId` should be the ResourceId of the image version. Use `az sig image-version list` to list image versions.

## Properties: buildTimeoutInMinutes

By default, the Image Builder will run for 240 minutes. After that, it will timeout and stop, whether or not the image build is complete. If the timeout is hit, you will see an error similar to this:

```
[ERROR] Failed while waiting for packerizer: Timeout waiting for microservice to
[ERROR] complete: 'context deadline exceeded'
```

If you do not specify a `buildTimeoutInMinutes` value, or set it to 0, it will use the default value. You can increase or decrease the value, up to the maximum of 960mins (16hrs). For Windows, we do not recommend setting this below 60 minutes. If you find you are hitting the timeout, review the [logs](#), to see if the customization step is waiting on something like user input.

If you find you need more time for customizations to complete, set this to what you think you need, with a little overhead. But, do not set it too high because you might have to wait for it to timeout before seeing an error.

## Properties: customize

Image Builder supports multiple 'customizers'. Customizers are functions that are used to customize your image, such as running scripts, or rebooting servers.

When using `customize`:

- You can use multiple customizers, but they must have a unique `name`.
- Customizers execute in the order specified in the template.
- If one customizer fails, then the whole customization component will fail and report back an error.
- It is strongly advised you test the script thoroughly before using it in a template. Debugging the script on your own VM will be easier.
- Do not put sensitive data in the scripts.
- The script locations need to be publicly accessible, unless you are using [MSI](#).

```
"customize": [
 {
 "type": "Shell",
 "name": "<name>",
 "scriptUri": "<path to script>",
 "sha256Checksum": "<sha256 checksum>"
 },
 {
 "type": "Shell",
 "name": "<name>",
 "inline": [
 "<command to run inline>"
]
 }
,
```

The `customize` section is an array. Azure Image Builder will run through the customizers in sequential order. Any failure in any customizer will fail the build process.

### Shell customizer

The shell customizer supports running shell scripts, these must be publicly accessible for the IB to access them.

```

"customize": [
 {
 "type": "Shell",
 "name": "<name>",
 "scriptUri": "<link to script>",
 "sha256Checksum": "<sha256 checksum>"
 },
],
 "customize": [
 {
 "type": "Shell",
 "name": "<name>",
 "inline": "<commands to run>"
 },
],

```

OS Support: Linux

Customize properties:

- **type** - Shell
- **name** - name for tracking the customization
- **scriptUri** - URI to the location of the file
- **inline** - array of shell commands, separated by commas.
- **sha256Checksum** - Value of sha256 checksum of the file, you generate this locally, and then Image Builder will checksum and validate.
  - To generate the sha256Checksum, using a terminal on Mac/Linux run: `sha256sum <fileName>`

For commands to run with super user privileges, they must be prefixed with `sudo`.

#### NOTE

When running the shell customizer with RHEL ISO source, you need to ensure your first customization shell handles registering with a Red Hat entitlement server before any customization occurs. Once customization is complete, the script should unregister with the entitlement server.

### Windows restart customizer

The Restart customizer allows you to restart a Windows VM and wait for it come back online, this allows you to install software that requires a reboot.

```

"customize": [
 {
 "type": "WindowsRestart",
 "restartCommand": "shutdown /r /f /t 0 /c",
 "restartCheckCommand": "echo Azure-Image-Builder-Rebooted-the-VM > c:\\buildArtifacts\\azureImageBuilderRestart.txt",
 "restartTimeout": "5m"
 }
],

```

OS Support: Windows

Customize properties:

- **Type:** WindowsRestart
- **restartCommand** - Command to execute the restart (optional). The default is `'shutdown /r /f /t 0 /c \"packer restart\"'`.
- **restartCheckCommand** – Command to check if restart succeeded (optional).
- **restartTimeout** - Restart timeout specified as a string of magnitude and unit. For example, `5m` (5 minutes) or `2h` (2 hours). The default is: '5m'

### Linux restart

There is no Linux Restart customizer, however, if you are installing drivers, or components that require a restart, you can install them and invoke a restart using the Shell customizer, there is a 20min SSH timeout to the build VM.

### PowerShell customizer

The shell customizer supports running PowerShell scripts and inline command, the scripts must be publicly accessible for the IB to access them.

```

"customize": [
 {
 "type": "PowerShell",
 "name": "<name>",
 "scriptUri": "<path to script>",
 "runElevated": "<true false>",
 "sha256Checksum": "<sha256 checksum>"
 },
 {
 "type": "PowerShell",
 "name": "<name>",
 "inline": "<PowerShell syntax to run>",
 "valid_exit_codes": "<exit code>",
 "runElevated": "<true or false>"
 }
],

```

OS support: Windows and Linux

Customize properties:

- **type** – PowerShell.
- **scriptUri** - URI to the location of the PowerShell script file.
- **inline** – Inline commands to be run, separated by commas.
- **valid\_exit\_codes** – Optional, valid codes that can be returned from the script/inline command, this will avoid reported failure of the script/inline command.
- **runElevated** – Optional, boolean, support for running commands and scripts with elevated permissions.
- **sha256Checksum** - Value of sha256 checksum of the file, you generate this locally, and then Image Builder will checksum and validate.
  - To generate the sha256Checksum, using a PowerShell on Windows [Get-Hash](#)

#### File customizer

The File customizer lets image builder download a file from a GitHub or Azure storage. If you have an image build pipeline that relies on build artifacts, you can then set the file customizer to download from the build share, and move the artifacts into the image.

```
"customize": [
 {
 "type": "File",
 "name": "<name>",
 "sourceUri": "<source location>",
 "destination": "<destination>",
 "sha256Checksum": "<sha256 checksum>"
 }
]
```

OS support: Linux and Windows

File customizer properties:

- **sourceUri** - an accessible storage endpoint, this can be GitHub or Azure storage. You can only download one file, not an entire directory. If you need to download a directory, use a compressed file, then uncompress it using the Shell or PowerShell customizers.
- **destination** – this is the full destination path and file name. Any referenced path and subdirectories must exist, use the Shell or PowerShell customizers to set these up beforehand. You can use the script customizers to create the path.

This is supported by Windows directories and Linux paths, but there are some differences:

- Linux OS's – the only path Image builder can write to is /tmp.
- Windows – No path restriction, but the path must exist.

If there is an error trying to download the file, or put it in a specified directory, the customize step will fail, and this will be in the customization.log.

#### NOTE

The file customizer is only suitable for small file downloads, < 20MB. For larger file downloads use a script or inline command, the use code to download files, such as, Linux `wget` or `curl`, Windows, `Invoke-WebRequest`.

Files in the File customizer can be downloaded from Azure Storage using [MSI](#).

#### Generalize

By default, Azure Image Builder will also run 'deprovision' code at the end of each image customization phase, to 'generalize' the image. Generalizing is a process where the image is set up so it can be reused to create multiple VMs. For Windows VMs, Azure Image Builder uses Sysprep. For Linux, Azure Image Builder runs 'waagent - deprovision'.

The commands Image Builder users to generalize may not be suitable for every situation, so Azure Image Builder will allow you to customize this command, if needed.

If you are migrating existing customization, and you are using different Sysprep/waagent commands, you can use the Image Builder generic commands, and if the VM creation fails, use your own Sysprep or waagent commands.

If Azure Image Builder creates a Windows custom image successfully, and you create a VM from it, then find that the VM creation fails or does not complete successfully, you will need to review the Windows Server Sysprep documentation or raise a support request with the Windows Server Sysprep Customer Services Support team, who can troubleshoot and advise on the correct Sysprep usage.

#### Default Sysprep command

```
echo '>>> Waiting for GA to start ...'
while ((Get-Service RdAgent).Status -ne 'Running') { Start-Sleep -s 5 }
while ((Get-Service WindowsAzureTelemetryService).Status -ne 'Running') { Start-Sleep -s 5 }
while ((Get-Service WindowsAzureGuestAgent).Status -ne 'Running') { Start-Sleep -s 5 }
echo '>>> Sysprepping VM ...'
if (Test-Path $Env:SystemRoot\windows\system32\Sysprep\unattend.xml){ rm $Env:SystemRoot\windows\system32\Sysprep\unattend.xml -Force }
$Env:SystemRoot\System32\Sysprep.exe /oobe /generalize /quiet /quit
while($true) { $imageState = Get-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup\State | Select ImageState; if($imageState.ImageState -ne 'IMAGE_STATE_GENERALIZE_RESEAL_TO_OOBE') { Write-Output $imageState.ImageState; Start-Sleep -s 5 } else { break } }
```

#### Default Linux deprovision command

```
/usr/sbin/waagent -force -deprovision+user && export HISTSIZE=0 && sync
```

#### Overriding the Commands

To override the commands, use the PowerShell or Shell script provisioners to create the command files with the exact file name, and put them in the correct directories:

- Windows: c:\DeprovisioningScript.ps1
- Linux: /tmp/DeprovisioningScript.sh

Image Builder will read these commands, these are written out to the AIB logs, 'customization.log'. See [troubleshooting](#) on how to collect logs.

## Properties: distribute

Azure Image Builder supports three distribution targets:

- **managedImage** - managed image.
- **sharedImage** - Shared Image Gallery.
- **VHD** - VHD in a storage account.

You can distribute an image to both of the target types in the same configuration, please see [examples](#).

Because you can have more than one target to distribute to, Image Builder maintains a state for every distribution target that can be accessed by querying the `[runOutputName]`. The `[runOutputName]` is an object you can query post distribution for information about that distribution. For example, you can query the location of the VHD, or regions where the image version was replicated to, or SIG Image version created. This is a property of every distribution target. The `[runOutputName]` must be unique to each distribution target. Here is an example, this is querying a Shared Image Gallery distribution:

```
subscriptionID=<subscriptionID>
imageResourceGroup=<resourceGroup of image template>
runOutputName=<runOutputName>

az resource show \
 --ids
"/subscriptions/$subscriptionID/resourcegroups/$imageResourceGroup/providers/Microsoft.VirtualMachineImages/imageTemplates/ImageTemplateLinuxRHEL77/runOutputs/$runOutputName" \
 --api-version=2019-05-01-preview
```

Output:

```
{
 "id": "/subscriptions/xxxxxx/resourcegroups/rheltest/providers/Microsoft.VirtualMachineImages/imageTemplates/ImageTemplateLinuxRHEL77/runOutputs/rhel77",
 "identity": null,
 "kind": null,
 "location": null,
 "managedBy": null,
 "name": "rhel77",
 "plan": null,
 "properties": {
 "artifactId": "/subscriptions/xxxxxx/resourceGroups/aibDevOpsImg/providers/Microsoft.Compute/galleries/devOpsSIG/images/rhel/versions/0.24105.52755",
 "provisioningState": "Succeeded"
 },
 "resourceGroup": "rheltest",
 "sku": null,
 "tags": null,
 "type": "Microsoft.VirtualMachineImages/imageTemplates/runOutputs"
}
```

### Distribute: managedImage

The image output will be a managed image resource.

```
"distribute": [
 {
 "type": "managedImage",
 "imageId": "<resource ID>",
 "location": "<region>",
 "runOutputName": "<name>",
 "artifactTags": {
 "<name>": "<value>",
 "<name>": "<value>"
 }
 }
]
```

Distribute properties:

- **type** - managedImage
- **imageId** - Resource ID of the destination image, expected format:  
`/subscriptions/<subscriptionId>/resourceGroups/<destinationResourceGroupName>/providers/Microsoft.Compute/images/<imageName>`
- **location** - location of the managed image.
- **runOutputName** - unique name for identifying the distribution.
- **artifactTags** - Optional user specified key value pair tags.

#### NOTE

The destination resource group must exist. If you want the image distributed to a different region, it will increase the deployment time .

### Distribute: sharedImage

The Azure Shared Image Gallery is a new Image Management service that allows managing of image region replication, versioning and sharing custom images. Azure Image Builder supports distributing with this service, so you can distribute images to regions supported by Shared Image Galleries.

A Shared Image Gallery is made up of:

- Gallery - Container for multiple shared images. A gallery is deployed in one region.
- Image definitions - a conceptual grouping for images.
- Image versions - this is an image type used for deploying a VM or scale set. Image versions can be replicated to other regions where VMs need to be deployed.

Before you can distribute to the Image Gallery, you must create a gallery and an image definition, see [Shared images](#).

```
{
 "type": "sharedImage",
 "galleryImageId": "<resource ID>",
 "runOutputName": "<name>",
 "artifactTags": {
 "<name>": "<value>",
 "<name>": "<value>"
 },
 "replicationRegions": [
 "<region where the gallery is deployed>",
 "<region>"
]
}
```

Distribute properties for shared image galleries:

- **type** - sharedImage
- **galleryImageId** – ID of the shared image gallery. The format is: /subscriptions/<subscriptionId>/resourceGroups/<resourceGroupName>/providers/Microsoft.Compute/galleries/<sharedImageGalleryName>/images/<imageGalleryName>
- **runOutputName** – unique name for identifying the distribution.
- **artifactTags** - Optional user specified key value pair tags.
- **replicationRegions** - Array of regions for replication. One of the regions must be the region where the Gallery is deployed.

#### NOTE

You can use Azure Image Builder in a different region to the gallery, but the Azure Image Builder service will need to transfer the image between the datacenters and this will take longer. Image Builder will automatically version the image, based on a monotonic integer, you cannot specify it currently.

#### Distribute: VHD

You can output to a VHD. You can then copy the VHD, and use it to publish to Azure MarketPlace, or use with Azure Stack.

```
{
 "type": "VHD",
 "runOutputName": "<VHD name>",
 "tags": {
 "<name>": "<value>",
 "<name>": "<value>"
 }
}
```

OS Support: Windows and Linux

Distribute VHD parameters:

- **type** - VHD.
- **runOutputName** – unique name for identifying the distribution.
- **tags** - Optional user specified key value pair tags.

Azure Image Builder does not allow the user to specify a storage account location, but you can query the status of the `runoutputs` to get the location.

```
az resource show \
--ids
"/subscriptions/$subscriptionId/resourcegroups/<imageResourceGroup>/providers/Microsoft.VirtualMachineImages/imageTemplates/<imageTemplateName>/runOutputs/<runOutputName>" | grep artifactUri
```

#### NOTE

Once the VHD has been created, copy it to a different location, as soon as possible. The VHD is stored in a storage account in the temporary resource group created when the image template is submitted to the Azure Image Builder service. If you delete the image template, then you will lose the VHD.

## Next steps

There are sample json files for different scenarios in the [Azure Image Builder GitHub](#).

# Preview: Create a Linux image and distribute it to a Shared Image Gallery

1/17/2020 • 4 minutes to read • [Edit Online](#)

This article shows you how you can use the Azure Image Builder, and the Azure CLI, to create an image version in a [Shared Image Gallery](#), then distribute the image globally. You can also do this using [Azure PowerShell](#).

We will be using a sample json template to configure the image. The json file we are using is here: [helloImageTemplateforSIG.json](#).

To distribute the image to a Shared Image Gallery, the template uses `sharedImage` as the value for the `distribute` section of the template.

## IMPORTANT

Azure Image Builder is currently in public preview. This preview version is provided without a service level agreement, and it's not recommended for production workloads. Certain features might not be supported or might have constrained capabilities. For more information, see [Supplemental Terms of Use for Microsoft Azure Previews](#).

## Register the features

To use Azure Image Builder during the preview, you need to register the new feature.

```
az feature register --namespace Microsoft.VirtualMachineImages --name VirtualMachineTemplatePreview
```

Check the status of the feature registration.

```
az feature show --namespace Microsoft.VirtualMachineImages --name VirtualMachineTemplatePreview | grep state
```

Check your registration.

```
az provider show -n Microsoft.VirtualMachineImages | grep registrationState
az provider show -n Microsoft.Storage | grep registrationState
```

If they do not say registered, run the following:

```
az provider register -n Microsoft.VirtualMachineImages
az provider register -n Microsoft.Storage
```

## Set variables and permissions

We will be using some pieces of information repeatedly, so we will create some variables to store that information.

For Preview, image builder will only support creating custom images in the same Resource Group as the source managed image. Update the resource group name in this example to be the same resource group as your source managed image.

```
Resource group name - we are using ibLinuxGalleryRG in this example
sigResourceGroup=ibLinuxGalleryRG
Datacenter location - we are using West US 2 in this example
location=westus2
Additional region to replicate the image to - we are using East US in this example
additionalRegion=eastus
name of the shared image gallery - in this example we are using myGallery
sigName=myIbGallery
name of the image definition to be created - in this example we are using myImageDef
imageDefName=myIbImageDef
image distribution metadata reference name
runOutputName=aibLinuxSIG
```

Create a variable for your subscription ID. You can get this using `az account show | grep id`.

```
subscriptionID=<Subscription ID>
```

Create the resource group.

```
az group create -n $sigResourceGroup -l $location
```

Give Azure Image Builder permission to create resources in that resource group. The `--assignee` value is the app registration ID for the Image Builder service.

```
az role assignment create \
--assignee cf32a0cc-373c-47c9-9156-0db11f6a6dfc \
--role Contributor \
--scope /subscriptions/$subscriptionID/resourceGroups/$sigResourceGroup
```

## Create an image definition and gallery

To use Image Builder with a shared image gallery, you need to have an existing image gallery and image definition. Image Builder will not create the image gallery and image definition for you.

If you don't already have a gallery and image definition to use, start by creating them. First, create an image gallery.

```
az sig create \
-g $sigResourceGroup \
--gallery-name $sigName
```

Then, create an image definition.

```
az sig image-definition create \
-g $sigResourceGroup \
--gallery-name $sigName \
--gallery-image-definition $imageDefName \
--publisher myIbPublisher \
--offer myOffer \
--sku 18.04-LTS \
--os-type Linux
```

## Download and configure the .json

Download the json template and configure it with your variables.

```
curl
https://raw.githubusercontent.com/danielsollondon/azvmimagebuilder/master/quickquickstarts/1_Creating_a_Custom_
Linux_Shared_Image_Gallery_Image/helloImageTemplateforSIG.json -o helloImageTemplateforSIG.json
sed -i -e "s/<subscriptionID>/$subscriptionID/g" helloImageTemplateforSIG.json
sed -i -e "s/<rgName>/$sigResourceGroup/g" helloImageTemplateforSIG.json
sed -i -e "s/<imageDefName>/$imageDefName/g" helloImageTemplateforSIG.json
sed -i -e "s/<sharedImageGalName>/$sigName/g" helloImageTemplateforSIG.json
sed -i -e "s/<region1>/$location/g" helloImageTemplateforSIG.json
sed -i -e "s/<region2>/$additionalRegion/g" helloImageTemplateforSIG.json
sed -i -e "s/<runOutputName>/$runOutputName/g" helloImageTemplateforSIG.json
```

## Create the image version

This next part will create the image version in the gallery.

Submit the image configuration to the Azure Image Builder service.

```
az resource create \
 --resource-group $sigResourceGroup \
 --properties @helloImageTemplateforSIG.json \
 --is-full-object \
 --resource-type Microsoft.VirtualMachineImages/imageTemplates \
 -n helloImageTemplateforSIG01
```

Start the image build.

```
az resource invoke-action \
 --resource-group $sigResourceGroup \
 --resource-type Microsoft.VirtualMachineImages/imageTemplates \
 -n helloImageTemplateforSIG01 \
 --action Run
```

Creating the image and replicating it to both regions can take a while. Wait until this part is finished before moving on to creating a VM.

## Create the VM

Create a VM from the image version that was created by Azure Image Builder.

```
az vm create \
 --resource-group $sigResourceGroup \
 --name myAibGalleryVM \
 --admin-username aibuser \
 --location $location \
 --image
 "/subscriptions/$subscriptionID/resourceGroups/$sigResourceGroup/providers/Microsoft.Compute/galleries/$sigName
 /images/$imageDefName/versions/latest" \
 --generate-ssh-keys
```

SSH into the VM.

```
ssh aibuser@<publicIpAddress>
```

You should see the image was customized with a *Message of the Day* as soon as your SSH connection is

established!

```

** This VM was built from the: **
** !! AZURE VM IMAGE BUILDER Custom Image !! **
** You have just been Customized :-) **

```

## Clean up resources

If you want to now try re-customizing the image version to create a new version of the same image, skip the next steps and go on to [Use Azure Image Builder to create another image version](#).

This will delete the image that was created, along with all of the other resource files. Make sure you are finished with this deployment before deleting the resources.

When deleting image gallery resources, you need delete all of the image versions before you can delete the image definition used to create them. To delete a gallery, you first need to have deleted all of the image definitions in the gallery.

Delete the image builder template.

```
az resource delete \
--resource-group $sigResourceGroup \
--resource-type Microsoft.VirtualMachineImages/imageTemplates \
-n helloImageTemplateforSIG01
```

Get the image version created by image builder, this always starts with `0.`, and then delete the image version

```
sigDefImgVersion=$(az sig image-version list \
-g $sigResourceGroup \
--gallery-name $sigName \
--gallery-image-definition $imageDefName \
--subscription $subscriptionID --query [].'name' -o json | grep 0. | tr -d '')\n\naz sig image-version delete \
-g $sigResourceGroup \
--gallery-image-version $sigDefImgVersion \
--gallery-name $sigName \
--gallery-image-definition $imageDefName \
--subscription $subscriptionID
```

Delete the image definition.

```
az sig image-definition delete \
-g $sigResourceGroup \
--gallery-name $sigName \
--gallery-image-definition $imageDefName \
--subscription $subscriptionID
```

Delete the gallery.

```
az sig delete -r $sigName -g $sigResourceGroup
```

Delete the resource group.

```
az group delete -n $sigResourceGroup -y
```

## Next steps

Learn more about [Azure Shared Image Galleries](#).

# Preview: Create a new VM image version from an existing image version using Azure Image Builder

12/9/2019 • 3 minutes to read • [Edit Online](#)

This article shows you how to take an existing image version in a [Shared Image Gallery](#), update it, and publish it as a new image version to the gallery.

We will be using a sample json template to configure the image. The json file we are using is here: [helloImageTemplateforSIGfromSIG.json](#).

## Register the features

To use Azure Image Builder during the preview, you need to register the new feature.

```
az feature register --namespace Microsoft.VirtualMachineImages --name VirtualMachineTemplatePreview
```

Check the status of the feature registration.

```
az feature show --namespace Microsoft.VirtualMachineImages --name VirtualMachineTemplatePreview | grep state
```

Check your registration.

```
az provider show -n Microsoft.VirtualMachineImages | grep registrationState
az provider show -n Microsoft.Storage | grep registrationState
```

If they do not say registered, run the following:

```
az provider register -n Microsoft.VirtualMachineImages
az provider register -n Microsoft.Storage
```

## Set variables and permissions

If you used [Create an image and distribute to a Shared Image Gallery](#) to create your Shared Image Gallery, you've already created some of the variables we need. If not, please setup some variables to be used for this example.

For Preview, image builder will only support creating custom images in the same Resource Group as the source managed image. Update the resource group name in this example to be the same resource group as your source managed image.

```
Resource group name
sigResourceGroup=ibLinuxGalleryRG
Gallery location
location=westus2
Additional region to replicate the image version to
additionalRegion=eastus
Name of the shared image gallery
sigName=myIbGallery
Name of the image definition to use
imageDefName=myIbImageDef
image distribution metadata reference name
runOutputName=aibSIGLinuxUpdate
```

Create a variable for your subscription ID. You can get this using `az account show | grep id`.

```
subscriptionID=<Subscription ID>
```

Get the image version that you want to update.

```
sigDefImgVersionId=$(az sig image-version list \
 -g $sigResourceGroup \
 --gallery-name $sigName \
 --gallery-image-definition $imageDefName \
 --subscription $subscriptionID --query [].'id' -o json | grep 0. | tr -d '"' | tr -d '[:space:]')
```

If you already have your own Shared Image Gallery, and did not follow the previous example, you will need to assign permissions for Image Builder to access the Resource Group, so it can access the gallery.

```
az role assignment create \
 --assignee cf32a0cc-373c-47c9-9156-0db11f6a6dfc \
 --role Contributor \
 --scope /subscriptions/$subscriptionID/resourceGroups/$sigResourceGroup
```

## Modify helloImage example

You can review the example we are about to use by opening the json file here: [helloImageTemplateforSIGfromSIG.json](#) along with the [Image Builder template reference](#).

Download the json example and configure it with your variables.

```
curl
https://raw.githubusercontent.com/danielsollondon/azvmimagebuilder/master/quickquickstarts/8_Creating_a_Custom_Linux_Shared_Image_Gallery_Image_from_SIG/helloImageTemplateforSIGfromSIG.json -o
helloImageTemplateforSIGfromSIG.json
sed -i -e "s/<subscriptionID>/$subscriptionID/g" helloImageTemplateforSIGfromSIG.json
sed -i -e "s/<rgName>/$sigResourceGroup/g" helloImageTemplateforSIGfromSIG.json
sed -i -e "s/<imageDefName>/$imageDefName/g" helloImageTemplateforSIGfromSIG.json
sed -i -e "s/<sharedImageGalName>/$sigName/g" helloImageTemplateforSIGfromSIG.json
sed -i -e "s/%<sigDefImgVersionId>%$sigDefImgVersionId%g" helloImageTemplateforSIGfromSIG.json
sed -i -e "s/<region1>/$location/g" helloImageTemplateforSIGfromSIG.json
sed -i -e "s/<region2>/$additionalRegion/g" helloImageTemplateforSIGfromSIG.json
sed -i -e "s/<runOutputName>/$runOutputName/g" helloImageTemplateforSIGfromSIG.json
```

## Create the image

Submit the image configuration to the VM Image Builder Service.

```
az resource create \
--resource-group $sigResourceGroup \
--properties @helloImageTemplateforSIGfromSIG.json \
--is-full-object \
--resource-type Microsoft.VirtualMachineImages/imageTemplates \
-n helloImageTemplateforSIGfromSIG01
```

Start the image build.

```
az resource invoke-action \
--resource-group $sigResourceGroup \
--resource-type Microsoft.VirtualMachineImages/imageTemplates \
-n helloImageTemplateforSIGfromSIG01 \
--action Run
```

Wait until the image has been built and replication before moving on to the next step.

## Create the VM

```
az vm create \
--resource-group $sigResourceGroup \
--name aibImgVm001 \
--admin-username azureuser \
--location $location \
--image
"/subscriptions/$subscriptionID/resourceGroups/$sigResourceGroup/providers/Microsoft.Compute/galleries/$imageName/images/$imageDefName/versions/latest" \
--generate-ssh-keys
```

Create an SSH connection to the VM using the public IP address of the VM.

```
ssh azureuser@<pubIp>
```

You should see the image was customized with a "Message of the Day" as soon as your SSH connection is established.

```

** This VM was built from the: **
** !! AZURE VM IMAGE BUILDER Custom Image !! **
** You have just been Customized :-) **

```

Type `exit` to close the SSH connection.

You can also list the image versions that are now available in your gallery.

```
az sig image-version list -g $sigResourceGroup -r $sigName -i $imageDefName -o table
```

## Next steps

To learn more about the components of the json file used in this article, see [Image builder template reference](#).

# Find Linux VM images in the Azure Marketplace with the Azure CLI

11/13/2019 • 9 minutes to read • [Edit Online](#)

This topic describes how to use the Azure CLI to find VM images in the Azure Marketplace. Use this information to specify a Marketplace image when you create a VM programmatically with the CLI, Resource Manager templates, or other tools.

Also browse available images and offers using the [Azure Marketplace](#) storefront, the [Azure portal](#), or [Azure PowerShell](#).

Make sure that you installed the latest [Azure CLI](#) and are logged in to an Azure account (`az login`).

## Terminology

A Marketplace image in Azure has the following attributes:

- **Publisher:** The organization that created the image. Examples: Canonical, MicrosoftWindowsServer
- **Offer:** The name of a group of related images created by a publisher. Examples: UbuntuServer, WindowsServer
- **SKU:** An instance of an offer, such as a major release of a distribution. Examples: 18.04-LTS, 2019-Datacenter
- **Version:** The version number of an image SKU.

To identify a Marketplace image when you deploy a VM programmatically, supply these values individually as parameters. Some tools accept an image *URN*, which combines these values, separated by the colon (:) character: *Publisher:Offer:SKU:Version*. In a URN, you can replace the version number with "latest", which selects the latest version of the image.

If the image publisher provides additional license and purchase terms, then you must accept those terms and enable programmatic deployment. You'll also need to supply *purchase plan* parameters when deploying a VM programmatically. See [Deploy an image with Marketplace terms](#).

## List popular images

Run the `az vm image list` command, without the `--all` option, to see a list of popular VM images in the Azure Marketplace. For example, run the following command to display a cached list of popular images in table format:

```
az vm image list --output table
```

The output includes the image URN (the value in the *Urn* column). When creating a VM with one of these popular Marketplace images, you can alternatively specify the *UrnAlias*, a shortened form such as *UbuntuLTS*.

| You are viewing an offline list of images, use --all to retrieve an up-to-date list |                      |           |                                         |
|-------------------------------------------------------------------------------------|----------------------|-----------|-----------------------------------------|
| Offer<br>UrnAlias                                                                   | Publisher<br>Version | Sku       | Urn                                     |
| CentOS                                                                              | OpenLogic<br>latest  | 7.5       | OpenLogic:CentOS:7.5:latest             |
| CoreOS                                                                              | CoreOS<br>latest     | Stable    | CoreOS:CoreOS:Stable:latest             |
| Debian                                                                              | credativ<br>latest   | 8         | credativ:Debian:8:latest                |
| UbuntuServer                                                                        | Canonical<br>latest  | 16.04-LTS | Canonical:UbuntuServer:16.04-LTS:latest |
| UbuntuLTS                                                                           | Canonical<br>latest  | 16.04-LTS | Canonical:UbuntuServer:16.04-LTS:latest |
| ...                                                                                 |                      |           |                                         |

## Find specific images

To find a specific VM image in the Marketplace, use the `az vm image list` command with the `--all` option. This version of the command takes some time to complete and can return lengthy output, so you usually filter the list by `--publisher` or another parameter.

For example, the following command displays all Debian offers (remember that without the `--all` switch, it only searches the local cache of common images):

```
az vm image list --offer Debian --all --output table
```

Partial output:

| Offer<br>Version        | Publisher | Sku | Urn                             |
|-------------------------|-----------|-----|---------------------------------|
| Debian<br>7.0.201602010 | credativ  | 7   | credativ:Debian:7:7.0.201602010 |
| Debian<br>7.0.201603020 | credativ  | 7   | credativ:Debian:7:7.0.201603020 |
| Debian<br>7.0.201604050 | credativ  | 7   | credativ:Debian:7:7.0.201604050 |
| Debian<br>7.0.201604200 | credativ  | 7   | credativ:Debian:7:7.0.201604200 |
| Debian<br>7.0.201606280 | credativ  | 7   | credativ:Debian:7:7.0.201606280 |
| Debian<br>7.0.201609120 | credativ  | 7   | credativ:Debian:7:7.0.201609120 |
| Debian<br>7.0.201611020 | credativ  | 7   | credativ:Debian:7:7.0.201611020 |
| Debian<br>7.0.201701180 | credativ  | 7   | credativ:Debian:7:7.0.201701180 |
| Debian<br>8.0.201602010 | credativ  | 8   | credativ:Debian:8:8.0.201602010 |
| Debian<br>8.0.201603020 | credativ  | 8   | credativ:Debian:8:8.0.201603020 |
| Debian<br>8.0.201604050 | credativ  | 8   | credativ:Debian:8:8.0.201604050 |
| Debian                  | credativ  | 8   | credativ:Debian:8:8.0.201604200 |

|               |          |   |                                 |
|---------------|----------|---|---------------------------------|
| 8.0.201604200 |          |   |                                 |
| Debian        | credativ | 8 | credativ:Debian:8:8.0.201606280 |
| 8.0.201606280 |          |   |                                 |
| Debian        | credativ | 8 | credativ:Debian:8:8.0.201609120 |
| 8.0.201609120 |          |   |                                 |
| Debian        | credativ | 8 | credativ:Debian:8:8.0.201611020 |
| 8.0.201611020 |          |   |                                 |
| Debian        | credativ | 8 | credativ:Debian:8:8.0.201701180 |
| 8.0.201701180 |          |   |                                 |
| Debian        | credativ | 8 | credativ:Debian:8:8.0.201703150 |
| 8.0.201703150 |          |   |                                 |
| Debian        | credativ | 8 | credativ:Debian:8:8.0.201704110 |
| 8.0.201704110 |          |   |                                 |
| Debian        | credativ | 8 | credativ:Debian:8:8.0.201704180 |
| 8.0.201704180 |          |   |                                 |
| Debian        | credativ | 8 | credativ:Debian:8:8.0.201706190 |
| 8.0.201706190 |          |   |                                 |
| Debian        | credativ | 8 | credativ:Debian:8:8.0.201706210 |
| 8.0.201706210 |          |   |                                 |
| Debian        | credativ | 8 | credativ:Debian:8:8.0.201708040 |
| 8.0.201708040 |          |   |                                 |
| Debian        | credativ | 8 | credativ:Debian:8:8.0.201710090 |
| 8.0.201710090 |          |   |                                 |
| Debian        | credativ | 8 | credativ:Debian:8:8.0.201712040 |
| 8.0.201712040 |          |   |                                 |
| Debian        | credativ | 8 | credativ:Debian:8:8.0.201801170 |
| 8.0.201801170 |          |   |                                 |
| Debian        | credativ | 8 | credativ:Debian:8:8.0.201803130 |
| 8.0.201803130 |          |   |                                 |
| Debian        | credativ | 8 | credativ:Debian:8:8.0.201803260 |
| 8.0.201803260 |          |   |                                 |
| Debian        | credativ | 8 | credativ:Debian:8:8.0.201804020 |
| 8.0.201804020 |          |   |                                 |
| Debian        | credativ | 8 | credativ:Debian:8:8.0.201804150 |
| 8.0.201804150 |          |   |                                 |
| Debian        | credativ | 8 | credativ:Debian:8:8.0.201805160 |
| 8.0.201805160 |          |   |                                 |
| Debian        | credativ | 8 | credativ:Debian:8:8.0.201807160 |
| 8.0.201807160 |          |   |                                 |
| Debian        | credativ | 8 | credativ:Debian:8:8.0.201901221 |
| 8.0.201901221 |          |   |                                 |
| ...           |          |   |                                 |

Apply similar filters with the `--location`, `--publisher`, and `--sku` options. You can perform partial matches on a filter, such as searching for `--offer Deb` to find all Debian images.

If you don't specify a particular location with the `--location` option, the values for the default location are returned. (Set a different default location by running `az configure --defaults location=<location>`.)

For example, the following command lists all Debian 8 SKUs in the West Europe location:

```
az vm image list --location westeurope --offer Deb --publisher credativ --sku 8 --all --output table
```

Partial output:

| Offer  | Publisher | Sku | Urn                             | Version       |
|--------|-----------|-----|---------------------------------|---------------|
| Debian | credativ  | 8   | credativ:Debian:8:8.0.201602010 | 8.0.201602010 |
| Debian | credativ  | 8   | credativ:Debian:8:8.0.201603020 | 8.0.201603020 |
| Debian | credativ  | 8   | credativ:Debian:8:8.0.201604050 | 8.0.201604050 |
| Debian | credativ  | 8   | credativ:Debian:8:8.0.201604200 | 8.0.201604200 |
| Debian | credativ  | 8   | credativ:Debian:8:8.0.201606280 | 8.0.201606280 |
| Debian | credativ  | 8   | credativ:Debian:8:8.0.201609120 | 8.0.201609120 |
| Debian | credativ  | 8   | credativ:Debian:8:8.0.201611020 | 8.0.201611020 |
| Debian | credativ  | 8   | credativ:Debian:8:8.0.201701180 | 8.0.201701180 |
| Debian | credativ  | 8   | credativ:Debian:8:8.0.201703150 | 8.0.201703150 |
| Debian | credativ  | 8   | credativ:Debian:8:8.0.201704110 | 8.0.201704110 |
| Debian | credativ  | 8   | credativ:Debian:8:8.0.201704180 | 8.0.201704180 |
| Debian | credativ  | 8   | credativ:Debian:8:8.0.201706190 | 8.0.201706190 |
| Debian | credativ  | 8   | credativ:Debian:8:8.0.201706210 | 8.0.201706210 |
| Debian | credativ  | 8   | credativ:Debian:8:8.0.201708040 | 8.0.201708040 |
| Debian | credativ  | 8   | credativ:Debian:8:8.0.201710090 | 8.0.201710090 |
| Debian | credativ  | 8   | credativ:Debian:8:8.0.201712040 | 8.0.201712040 |
| Debian | credativ  | 8   | credativ:Debian:8:8.0.201801170 | 8.0.201801170 |
| Debian | credativ  | 8   | credativ:Debian:8:8.0.201803130 | 8.0.201803130 |
| Debian | credativ  | 8   | credativ:Debian:8:8.0.201803260 | 8.0.201803260 |
| Debian | credativ  | 8   | credativ:Debian:8:8.0.201804020 | 8.0.201804020 |
| Debian | credativ  | 8   | credativ:Debian:8:8.0.201804150 | 8.0.201804150 |
| Debian | credativ  | 8   | credativ:Debian:8:8.0.201805160 | 8.0.201805160 |
| Debian | credativ  | 8   | credativ:Debian:8:8.0.201807160 | 8.0.201807160 |
| Debian | credativ  | 8   | credativ:Debian:8:8.0.201901221 | 8.0.201901221 |
| ...    |           |     |                                 |               |

## Navigate the images

Another way to find an image in a location is to run the [az vm image list-publishers](#), [az vm image list-offers](#), and [az vm image list-skus](#) commands in sequence. With these commands, you determine these values:

1. List the image publishers.
2. For a given publisher, list their offers.
3. For a given offer, list their SKUs.

Then, for a selected SKU, you can choose a version to deploy.

For example, the following command lists the image publishers in the West US location:

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

Partial output:

| Location | Name                                           |
|----------|------------------------------------------------|
| westus   | 128technology                                  |
| westus   | 1e                                             |
| westus   | 4psa                                           |
| westus   | 5nine-software-inc                             |
| westus   | 7isolutions                                    |
| westus   | a10networks                                    |
| westus   | abiquo                                         |
| westus   | acellion                                       |
| westus   | accessdata-group                               |
| westus   | accops                                         |
| westus   | Acronis                                        |
| westus   | Acronis.Backup                                 |
| westus   | actian-corp                                    |
| westus   | actian_matrix                                  |
| westus   | actifio                                        |
| westus   | activeeon                                      |
| westus   | advantech-webaccess                            |
| westus   | aerospike                                      |
| westus   | affinio                                        |
| westus   | aiscaler-cache-control-ddos-and-url-rewriting- |
| westus   | akamai-technologies                            |
| westus   | akumina                                        |
| ...      |                                                |

Use this information to find offers from a specific publisher. For example, for the *Canonical* publisher in the West US location, find offers by running `az vm image list-offers`. Pass the location and the publisher as in the following example:

```
az vm image list-offers --location westus --publisher Canonical --output table
```

Output:

| Location | Name                    |
|----------|-------------------------|
| westus   | Ubuntu15.04Snappy       |
| westus   | Ubuntu15.04SnappyDocker |
| westus   | UbunturollingSnappy     |
| westus   | UbuntuServer            |
| westus   | Ubuntu_Core             |

You see that in the West US region, Canonical publishes the *UbuntuServer* offer on Azure. But what SKUs? To get those values, run `az vm image list-skus` and set the location, publisher, and offer that you discovered:

```
az vm image list-skus --location westus --publisher Canonical --offer UbuntuServer --output table
```

Output:

| Location | Name              |
|----------|-------------------|
| westus   | 12.04.3-LTS       |
| westus   | 12.04.4-LTS       |
| westus   | 12.04.5-LTS       |
| westus   | 14.04.0-LTS       |
| westus   | 14.04.1-LTS       |
| westus   | 14.04.2-LTS       |
| westus   | 14.04.3-LTS       |
| westus   | 14.04.4-LTS       |
| westus   | 14.04.5-DAILY-LTS |
| westus   | 14.04.5-LTS       |
| westus   | 16.04-DAILY-LTS   |
| westus   | 16.04-LTS         |
| westus   | 16.04.0-LTS       |
| westus   | 18.04-DAILY-LTS   |
| westus   | 18.04-LTS         |
| westus   | 18.10             |
| westus   | 18.10-DAILY       |
| westus   | 19.04-DAILY       |

Finally, use the `az vm image list` command to find a specific version of the SKU you want, for example, `18.04-LTS`:

```
az vm image list --location westus --publisher Canonical --offer UbuntuServer --sku 18.04-LTS --all --output table
```

Partial output:

| Offer        | Publisher | Sku       | Urn                                              | Version         |
|--------------|-----------|-----------|--------------------------------------------------|-----------------|
| UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201804262 | 18.04.201804262 |
| UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201805170 | 18.04.201805170 |
| UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201805220 | 18.04.201805220 |
| UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201806130 | 18.04.201806130 |
| UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201806170 | 18.04.201806170 |
| UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201807240 | 18.04.201807240 |
| UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201808060 | 18.04.201808060 |
| UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201808080 | 18.04.201808080 |
| UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201808140 | 18.04.201808140 |
| UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201808310 | 18.04.201808310 |
| UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201809110 | 18.04.201809110 |
| UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201810030 | 18.04.201810030 |
| UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201810240 | 18.04.201810240 |
| UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201810290 | 18.04.201810290 |
| UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201811010 | 18.04.201811010 |
| UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201812031 | 18.04.201812031 |
| UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201812040 | 18.04.201812040 |
| UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201812060 | 18.04.201812060 |
| UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201901140 | 18.04.201901140 |
| UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201901220 | 18.04.201901220 |
| ...          |           |           |                                                  |                 |

Now you can choose precisely the image you want to use by taking note of the URN value. Pass this value with the `--image` parameter when you create a VM with the `az vm create` command. Remember that you can optionally replace the version number in the URN with "latest". This version is always the latest version of the image.

If you deploy a VM with a Resource Manager template, you set the image parameters individually in the `imageReference` properties. See the [template reference](#).

## Deploy an image with Marketplace terms

Some VM images in the Azure Marketplace have additional license and purchase terms that you must accept before you can deploy them programmatically.

To deploy a VM from such an image, you'll need to both accept the image's terms and enable programmatic deployment. You'll only need to do this once per subscription. Afterward, each time you deploy a VM programmatically from the image you'll also need to specify *purchase plan* parameters.

The following sections show how to:

- Find out whether a Marketplace image has additional license terms
- Accept the terms programmatically
- Provide purchase plan parameters when you deploy a VM programmatically

### View plan properties

To view an image's purchase plan information, run the `az vm image show` command. If the `plan` property in the output is not `null`, the image has terms you need to accept before programmatic deployment.

For example, the Canonical Ubuntu Server 18.04 LTS image doesn't have additional terms, because the `plan` information is `null`:

```
az vm image show --location westus --urn Canonical:UbuntuServer:18.04-LTS:latest
```

Output:

```
{
 "dataDiskImages": [],
 "id": "/Subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxx/Providers/Microsoft.Compute/Locations/westus/Publishers/Canonical/ArtifactTypes/VMImage/Offers/Ub
untuServer/Skus/18.04-LTS/Versions/18.04.201901220",
 "location": "westus",
 "name": "18.04.201901220",
 "osDiskImage": {
 "operatingSystem": "Linux"
 },
 "plan": null,
 "tags": null
}
```

Running a similar command for the RabbitMQ Certified by Bitnami image shows the following `plan` properties: `name`, `product`, and `publisher`. (Some images also have a `promotion code` property.) To deploy this image, see the following sections to accept the terms and enable programmatic deployment.

```
az vm image show --location westus --urn bitnami:rabbitmq:rabbitmq:latest
```

Output:

```
{
 "dataDiskImages": [],
 "id": "/Subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxx/Providers/Microsoft.Compute/Locations/westus/Publishers/bitnami/ArtifactTypes/VMImage/Offers/rabb
itmq/Skus/rabbitmq/Versions/3.7.1901151016",
 "location": "westus",
 "name": "3.7.1901151016",
 "osDiskImage": {
 "operatingSystem": "Linux"
 },
 "plan": {
 "name": "rabbitmq",
 "product": "rabbitmq",
 "publisher": "bitnami"
 },
 "tags": null
}
```

## Accept the terms

To view and accept the license terms, use the [az vm image accept-terms](#) command. When you accept the terms, you enable programmatic deployment in your subscription. You only need to accept terms once per subscription for the image. For example:

```
az vm image accept-terms --urn bitnami:rabbitmq:rabbitmq:latest
```

The output includes a `licenseTextLink` to the license terms, and indicates that the value of `accepted` is `true`:

```
{
 "accepted": true,
 "additionalProperties": {},
 "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxx/providers/Microsoft.MarketplaceOrdering/offertypes/bitnami/offers/rabbitmq/plans/rabbitmq",
 "licenseTextLink":
 "https://storelegalterms.blob.core.windows.net/legalterms/3E5ED_legalterms_BITNAMI%253a24RABBITMQ%253a24RABBIT
MQ%253a24IGRT7HHPIFOBV3IQYJHEN202FGUVXXZ3WUYIMEIVF3KCUNJ7GTVXNNM23I567GBMNDRFOY4WXJPN5PUYXNKB2QLAKCHP4IE5GO3B
2I.txt",
 "name": "rabbitmq",
 "plan": "rabbitmq",
 "privacyPolicyLink": "https://bitnami.com/privacy",
 "product": "rabbitmq",
 "publisher": "bitnami",
 "retrieveDatetime": "2019-01-25T20:37:49.937096Z",
 "signature":
 "XXXXXXLAZIK7ZL2YRV5JYQXONPV76NQJW3FKMDZYCRGXZYVDGX6BVY45J03BXVMNA2COBOEYG2N0760NORU7ITTRHGZDYNJXXXXXX",
 "type": "Microsoft.MarketplaceOrdering/offertypes"
}
```

## Deploy using purchase plan parameters

After accepting the terms for the image, you can deploy a VM in the subscription. To deploy the image by using the [az vm create](#) command, provide parameters for the purchase plan in addition to a URN for the image. For example, to deploy a VM with the RabbitMQ Certified by Bitnami image:

```
az group create --name myResourceGroupVM --location westus

az vm create --resource-group myResourceGroupVM --name myVM --image bitnami:rabbitmq:rabbitmq:latest --plan-
name rabbitmq --plan-product rabbitmq --plan-publisher bitnami
```

## Next steps

To create a virtual machine quickly by using the image information, see [Create and Manage Linux VMs with the Azure CLI](#).

# Information for Non-endorsed Distributions

1/16/2020 • 8 minutes to read • [Edit Online](#)

The Azure platform SLA applies to virtual machines running the Linux OS only when one of the [endorsed distributions](#) is used. For these endorsed distributions, pre-configured Linux images are provided in the Azure Marketplace.

- [Linux on Azure - Endorsed Distributions](#)
- [Support for Linux images in Microsoft Azure](#)

All distributions running on Azure have a number of prerequisites. This article can't be comprehensive, as every distribution is different. Even if you meet all the criteria below, you may need to significantly tweak your Linux system for it to run properly.

We recommend that you start with one of the [Linux on Azure Endorsed Distributions](#). The following articles show you how to prepare the various endorsed Linux distributions that are supported on Azure:

- [CentOS-based Distributions](#)
- [Debian Linux](#)
- [Oracle Linux](#)
- [Red Hat Enterprise Linux](#)
- [SLES & openSUSE](#)
- [Ubuntu](#)

This article focuses on general guidance for running your Linux distribution on Azure.

## General Linux Installation Notes

- The Hyper-V virtual hard disk (VHDX) format isn't supported in Azure, only *fixed VHD*. You can convert the disk to VHD format using Hyper-V Manager or the [Convert-VHD](#) cmdlet. If you're using VirtualBox, select **Fixed size** rather than the default (dynamically allocated) when creating the disk.
- Azure supports Gen1 (BIOS boot) & Gen2 (UEFI boot) Virtual machines.
- The maximum size allowed for the VHD is 1,023 GB.
- When installing the Linux system we recommend that you use standard partitions, rather than Logical Volume Manager (LVM) which is the default for many installations. Using standard partitions will avoid LVM name conflicts with cloned VMs, particularly if an OS disk is ever attached to another identical VM for troubleshooting. [LVM](#) or [RAID](#) may be used on data disks.
- Kernel support for mounting UDF file systems is necessary. At first boot on Azure the provisioning configuration is passed to the Linux VM by using UDF-formatted media that is attached to the guest. The Azure Linux agent must mount the UDF file system to read its configuration and provision the VM.
- Linux kernel versions earlier than 2.6.37 don't support NUMA on Hyper-V with larger VM sizes. This issue primarily impacts older distributions using the upstream Red Hat 2.6.32 kernel, and was fixed in Red Hat Enterprise Linux (RHEL) 6.6 (kernel-2.6.32-504). Systems running custom kernels older than 2.6.37, or RHEL-based kernels older than 2.6.32-504 must set the boot parameter `numa=off` on the kernel command line in grub.conf. For more information, see [Red Hat KB 436883](#).
- Don't configure a swap partition on the OS disk. The Linux agent can be configured to create a swap file on the temporary resource disk, as described in the following steps.
- All VHDs on Azure must have a virtual size aligned to 1 MB. When converting from a raw disk to VHD you must ensure that the raw disk size is a multiple of 1 MB before conversion, as described in the following steps.

## Installing kernel modules without Hyper-V

Azure runs on the Hyper-V hypervisor, so Linux requires certain kernel modules to run in Azure. If you have a VM that was created outside of Hyper-V, the Linux installers may not include the drivers for Hyper-V in the initial ramdisk (initrd or initramfs), unless the VM detects that it's running on a Hyper-V environment. When using a different virtualization system (such as VirtualBox, KVM, and so on) to prepare your Linux image, you may need to rebuild the initrd so that at least the hv\_vmbus and hv\_storvsc kernel modules are available on the initial ramdisk. This known issue is for systems based on the upstream Red Hat distribution, and possibly others.

The mechanism for rebuilding the initrd or initramfs image may vary depending on the distribution. Consult your distribution's documentation or support for the proper procedure. Here is one example for rebuilding the initrd by using the `mkinitrd` utility:

1. Back up the existing initrd image:

```
cd /boot
sudo cp initrd-`uname -r`.img initrd-`uname -r`.img.bak
```

2. Rebuild the initrd with the hv\_vmbus and hv\_storvsc kernel modules:

```
sudo mkinitrd --preload=hv_storvsc --preload=hv_vmbus -v -f initrd-`uname -r`.img `uname -r`
```

## Resizing VHDS

VHD images on Azure must have a virtual size aligned to 1 MB. Typically, VHDS created using Hyper-V are aligned correctly. If the VHD isn't aligned correctly, you may receive an error message similar to the following when you try to create an image from your VHD.

- The VHD `http://<mystorageaccount>.blob.core.windows.net/vhds/MyLinuxVM.vhd` has an unsupported virtual size of 21475270656 bytes. The size must be a whole number (in MBs).

In this case, resize the VM using either the Hyper-V Manager console or the [Resize-VHD](#) PowerShell cmdlet. If you aren't running in a Windows environment, we recommend using `qemu-img` to convert (if needed) and resize the VHD.

### NOTE

There is a [known bug in qemu-img](#) versions  $\geq 2.2.1$  that results in an improperly formatted VHD. The issue has been fixed in QEMU 2.6. We recommend using either `qemu-img` 2.2.0 or lower, or 2.6 or higher.

1. Resizing the VHD directly using tools such as `qemu-img` or `vbox-manage` may result in an unbootable VHD. We recommend first converting the VHD to a RAW disk image. If the VM image was created as a RAW disk image (the default for some hypervisors such as KVM), then you may skip this step.

```
qemu-img convert -f vpc -O raw MyLinuxVM.vhd MyLinuxVM.raw
```

2. Calculate the required size of the disk image so that the virtual size is aligned to 1 MB. The following bash shell script uses `qemu-img info` to determine the virtual size of the disk image, and then calculates the size to the next 1 MB.

```

rawdisk="MyLinuxVM.raw"
vhddisk="MyLinuxVM.vhd"

MB=$((1024*1024))
size=$(qemu-img info -f raw --output json "$rawdisk" | \
gawk 'match($0, /"virtual-size": ([0-9]+),/, val) {print val[1]}')

rounded_size=$(((($size+$MB-1)/$MB)*$MB))

echo "Rounded Size = $rounded_size"

```

3. Resize the raw disk using `$rounded_size` as set above.

```
qemu-img resize MyLinuxVM.raw $rounded_size
```

4. Now, convert the RAW disk back to a fixed-size VHD.

```
qemu-img convert -f raw -o subformat=fixed -O vpc MyLinuxVM.raw MyLinuxVM.vhd
```

Or, with qemu version 2.6+, include the `force_size` option.

```
qemu-img convert -f raw -o subformat=fixed,force_size -O vpc MyLinuxVM.raw MyLinuxVM.vhd
```

## Linux Kernel Requirements

The Linux Integration Services (LIS) drivers for Hyper-V and Azure are contributed directly to the upstream Linux kernel. Many distributions that include a recent Linux kernel version (such as 3.x) have these drivers available already, or otherwise provide backported versions of these drivers with their kernels. These drivers are constantly being updated in the upstream kernel with new fixes and features, so when possible we recommend running an [endorsed distribution](#) that includes these fixes and updates.

If you're running a variant of Red Hat Enterprise Linux versions 6.0 to 6.3, then you'll need to install the[latest LIS drivers for Hyper-V](#). Beginning with RHEL 6.4+ (and derivatives) the LIS drivers are already included with the kernel and so no additional installation packages are needed.

If a custom kernel is required, we recommend a recent kernel version (such as 3.8+). For distributions or vendors who maintain their own kernel, you'll need to regularly backport the LIS drivers from the upstream kernel to your custom kernel. Even if you're already running a relatively recent kernel version, we highly recommend keeping track of any upstream fixes in the LIS drivers and backport them as needed. The locations of the LIS driver source files are specified in the [MAINTAINERS](#) file in the Linux kernel source tree:

```

F: arch/x86/include/asm/mshyperv.h
F: arch/x86/include/uapi/asm/hyperv.h
F: arch/x86/kernel/cpu/mshyperv.c
F: drivers/hid/hid-hyperv.c
F: drivers/hv/
F: drivers/input/serio/hyperv-keyboard.c
F: drivers/net/hyperv/
F: drivers/scsi/storvsc_drv.c
F: drivers/video/fbdev/hyperv_fb.c
F: include/linux/hyperv.h
F: tools/hv/

```

The following patches must be included in the kernel. This list can't be complete for all distributions.

- [ata\\_piix](#): defer disks to the Hyper-V drivers by default
- [storvsc](#): Account for in-transit packets in the RESET path
- [storvsc](#): avoid usage of WRITE\_SAME
- [storvsc](#): Disable WRITE SAME for RAID and virtual host adapter drivers
- [storvsc](#): NULL pointer dereference fix
- [storvsc](#): ring buffer failures may result in I/O freeze
- [scsi\\_sysfs](#): protect against double execution of \_\_scsi\_remove\_device

## The Azure Linux Agent

The [Azure Linux Agent](#) `waagent` provisions a Linux virtual machine in Azure. You can get the latest version, file issues, or submit pull requests at the [Linux Agent GitHub repo](#).

- The Linux agent is released under the Apache 2.0 license. Many distributions already provide RPM or .deb packages for the agent, and these packages can easily be installed and updated.
- The Azure Linux Agent requires Python v2.6+.
- The agent also requires the `python-pyasn1` module. Most distributions provide this module as a separate package to be installed.
- In some cases, the Azure Linux Agent may not be compatible with NetworkManager. Many of the RPM/deb packages provided by distributions configure NetworkManager as a conflict to the `waagent` package. In these cases, it will uninstall NetworkManager when you install the Linux agent package.
- The Azure Linux Agent must be at or above the [minimum supported version](#).

## General Linux System Requirements

1. Modify the kernel boot line in GRUB or GRUB2 to include the following parameters, so that all console messages are sent to the first serial port. These messages can assist Azure support with debugging any issues.

```
console=ttyS0,115200n8 earlyprintk=ttyS0,115200 rootdelay=300
```

We also recommend *removing* the following parameters if they exist.

```
rhgb quiet crashkernel=auto
```

Graphical and quiet boot isn't useful in a cloud environment, where we want all logs sent to the serial port.

The `crashkernel` option may be left configured if needed, but note that this parameter reduces the amount of available memory in the VM by at least 128 MB, which may be problematic for smaller VM sizes.

2. Install the Azure Linux Agent.

The Azure Linux Agent is required for provisioning a Linux image on Azure. Many distributions provide the agent as an RPM or .deb package (the package is typically called `WALinuxAgent` or `walinuxagent`). The agent can also be installed manually by following the steps in the [Linux Agent Guide](#).

3. Ensure that the SSH server is installed, and configured to start at boot time. This configuration is usually the default.

4. Don't create swap space on the OS disk.

The Azure Linux Agent can automatically configure swap space using the local resource disk that is attached to the VM after provisioning on Azure. The local resource disk is a *temporary* disk, and might be emptied when the VM is deprovisioned. After installing the Azure Linux Agent (step 2 above), modify the

following parameters in /etc/waagent.conf as needed.

```
ResourceDisk.Format=y
ResourceDisk.Filesystem=ext4
ResourceDisk.MountPoint=/mnt/resource
ResourceDisk.EnableSwap=y
ResourceDisk.SwapSizeMB=2048 ## NOTE: Set this to your desired size.
```

- Run the following commands to deprovision the virtual machine.

```
sudo waagent -force -deprovision
export HISTSIZE=0
logout
```

**NOTE**

On Virtualbox you may see the following error after running `waagent -force -deprovision` that says `[Errno 5] Input/output error`. This error message is not critical and can be ignored.

- Shut down the virtual machine and upload the VHD to Azure.

# Prepare an Ubuntu virtual machine for Azure

1/20/2020 • 3 minutes to read • [Edit Online](#)

Ubuntu now publishes official Azure VHDs for download at <https://cloud-images.ubuntu.com/>. If you need to build your own specialized Ubuntu image for Azure, rather than use the manual procedure below it is recommended to start with these known working VHDs and customize as needed. The latest image releases can always be found at the following locations:

- Ubuntu 12.04/Precise: [ubuntu-12.04-server-cloudimg-amd64-disk1.vhd.zip](#)
- Ubuntu 14.04/Trusty: [ubuntu-14.04-server-cloudimg-amd64-disk1.vhd.zip](#)
- Ubuntu 16.04/Xenial: [ubuntu-16.04-server-cloudimg-amd64-disk1.vmdk](#)
- Ubuntu 18.04/Bionic: [bionic-server-cloudimg-amd64.vmdk](#)
- Ubuntu 18.10/Cosmic: [cosmic-server-cloudimg-amd64.vhd.zip](#)

## Prerequisites

This article assumes that you have already installed an Ubuntu Linux operating system to a virtual hard disk. Multiple tools exist to create .vhd files, for example a virtualization solution such as Hyper-V. For instructions, see [Install the Hyper-V Role and Configure a Virtual Machine](#).

### Ubuntu installation notes

- Please see also [General Linux Installation Notes](#) for more tips on preparing Linux for Azure.
- The VHDX format is not supported in Azure, only **fixed VHD**. You can convert the disk to VHD format using Hyper-V Manager or the convert-vhd cmdlet.
- When installing the Linux system it is recommended that you use standard partitions rather than LVM (often the default for many installations). This will avoid LVM name conflicts with cloned VMs, particularly if an OS disk ever needs to be attached to another VM for troubleshooting. [LVM](#) or [RAID](#) may be used on data disks if preferred.
- Do not configure a swap partition on the OS disk. The Linux agent can be configured to create a swap file on the temporary resource disk. More information about this can be found in the steps below.
- All VHDs on Azure must have a virtual size aligned to 1MB. When converting from a raw disk to VHD you must ensure that the raw disk size is a multiple of 1MB before conversion. See [Linux Installation Notes](#) for more information.

## Manual steps

### NOTE

Before attempting to create your own custom Ubuntu image for Azure, please consider using the pre-built and tested images from <https://cloud-images.ubuntu.com/> instead.

1. In the center pane of Hyper-V Manager, select the virtual machine.
2. Click **Connect** to open the window for the virtual machine.
3. Replace the current repositories in the image to use Ubuntu's Azure repository. The steps vary slightly depending on the Ubuntu version.

Before editing `/etc/apt/sources.list`, it is recommended to make a backup:

```
sudo cp /etc/apt/sources.list /etc/apt/sources.list.bak
```

Ubuntu 12.04:

```
sudo sed -i 's/[a-z][a-z].archive.ubuntu.com/azure.archive.ubuntu.com/g' /etc/apt/sources.list
sudo apt-get update
```

Ubuntu 14.04:

```
sudo sed -i 's/[a-z][a-z].archive.ubuntu.com/azure.archive.ubuntu.com/g' /etc/apt/sources.list
sudo apt-get update
```

Ubuntu 16.04:

```
sudo sed -i 's/[a-z][a-z].archive.ubuntu.com/azure.archive.ubuntu.com/g' /etc/apt/sources.list
sudo apt-get update
```

4. The Ubuntu Azure images are now following the *hardware enablement* (HWE) kernel. Update the operating system to the latest kernel by running the following commands:

Ubuntu 12.04:

```
sudo apt-get update
sudo apt-get install linux-image-generic-lts-trusty linux-cloud-tools-generic-lts-trusty
sudo apt-get install hv-kvp-daemon-init
(recommended) sudo apt-get dist-upgrade

sudo reboot
```

Ubuntu 14.04:

```
sudo apt-get update
sudo apt-get install linux-image-virtual-lts-vivid linux-lts-vivid-tools-common
sudo apt-get install hv-kvp-daemon-init
(recommended) sudo apt-get dist-upgrade

sudo reboot
```

Ubuntu 16.04:

```
sudo apt-get update
sudo apt-get install linux-generic-hwe-16.04 linux-cloud-tools-generic-hwe-16.04
(recommended) sudo apt-get dist-upgrade

sudo reboot
```

Ubuntu 18.04.04:

```
sudo apt-get update
sudo apt-get install --install-recommends linux-generic-hwe-18.04 xserver-xorg-hwe-18.04
sudo apt-get install --install-recommends linux-cloud-tools-generic-hwe-18.04
(recommended) sudo apt-get dist-upgrade

sudo reboot
```

## See also:

- <https://wiki.ubuntu.com/Kernel/LTSEnablementStack>
- <https://wiki.ubuntu.com/Kernel/RollingLTSEnablementStack>

5. Modify the kernel boot line for Grub to include additional kernel parameters for Azure. To do this open `/etc/default/grub` in a text editor, find the variable called `GRUB_CMDLINE_LINUX_DEFAULT` (or add it if needed) and edit it to include the following parameters:

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0,115200n8 earlyprintk=ttyS0,115200 rootdelay=300"
```

Save and close this file, and then run `sudo update-grub`. This will ensure all console messages are sent to the first serial port, which can assist Azure technical support with debugging issues.

6. Ensure that the SSH server is installed and configured to start at boot time. This is usually the default.
7. Install the Azure Linux Agent:

```
sudo apt-get update
sudo apt-get install walinuxagent
```

### NOTE

The `walinuxagent` package may remove the `NetworkManager` and `NetworkManager-gnome` packages, if they are installed.

8. Run the following commands to deprovision the virtual machine and prepare it for provisioning on Azure:

```
sudo waagent -force -deprovision
export HISTSIZE=0
logout
```

9. Click **Action -> Shut Down** in Hyper-V Manager. Your Linux VHD is now ready to be uploaded to Azure.

## References

[Ubuntu hardware enablement \(HWE\) kernel](#)

## Next steps

You're now ready to use your Ubuntu Linux virtual hard disk to create new virtual machines in Azure. If this is the first time that you're uploading the .vhd file to Azure, see [Create a Linux VM from a custom disk](#).

# Prepare a CentOS-based virtual machine for Azure

1/8/2020 • 9 minutes to read • [Edit Online](#)

Learn to create and upload an Azure virtual hard disk (VHD) that contains a CentOS-based Linux operating system.

- [Prepare a CentOS 6.x virtual machine for Azure](#)
- [Prepare a CentOS 7.0+ virtual machine for Azure](#)

## Prerequisites

This article assumes that you have already installed a CentOS (or similar derivative) Linux operating system to a virtual hard disk. Multiple tools exist to create .vhd files, for example a virtualization solution such as Hyper-V. For instructions, see [Install the Hyper-V Role and Configure a Virtual Machine](#).

### CentOS installation notes

- Please see also [General Linux Installation Notes](#) for more tips on preparing Linux for Azure.
- The VHDX format is not supported in Azure, only **fixed VHD**. You can convert the disk to VHD format using Hyper-V Manager or the convert-vhd cmdlet. If you are using VirtualBox this means selecting **Fixed size** as opposed to the default dynamically allocated when creating the disk.
- When installing the Linux system it is *recommended* that you use standard partitions rather than LVM (often the default for many installations). This will avoid LVM name conflicts with cloned VMs, particularly if an OS disk ever needs to be attached to another identical VM for troubleshooting. [LVM](#) or [RAID](#) may be used on data disks.
- Kernel support for mounting UDF file systems is required. At first boot on Azure the provisioning configuration is passed to the Linux VM via UDF-formatted media that is attached to the guest. The Azure Linux agent must be able to mount the UDF file system to read its configuration and provision the VM.
- Linux kernel versions below 2.6.37 do not support NUMA on Hyper-V with larger VM sizes. This issue primarily impacts older distributions using the upstream Red Hat 2.6.32 kernel, and was fixed in RHEL 6.6 (kernel-2.6.32-504). Systems running custom kernels older than 2.6.37, or RHEL-based kernels older than 2.6.32-504 must set the boot parameter `numa=off` on the kernel command-line in grub.conf. For more information see Red Hat [KB 436883](#).
- Do not configure a swap partition on the OS disk. The Linux agent can be configured to create a swap file on the temporary resource disk. More information about this can be found in the steps below.
- All VHDs on Azure must have a virtual size aligned to 1MB. When converting from a raw disk to VHD you must ensure that the raw disk size is a multiple of 1MB before conversion. See [Linux Installation Notes](#) for more information.

## CentOS 6.x

1. In Hyper-V Manager, select the virtual machine.
2. Click **Connect** to open a console window for the virtual machine.
3. In CentOS 6, NetworkManager can interfere with the Azure Linux agent. Uninstall this package by running the following command:

```
sudo rpm -e --nodeps NetworkManager
```

4. Create or edit the file `/etc/sysconfig/network` and add the following text:

```
NETWORKING=yes
HOSTNAME=localhost.localdomain
```

5. Create or edit the file `/etc/sysconfig/network-scripts/ifcfg-eth0` and add the following text:

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
TYPE=Ethernet
USERCTL=no
PEERDNS=yes
IPV6INIT=no
```

6. Modify udev rules to avoid generating static rules for the Ethernet interface(s). These rules can cause problems when cloning a virtual machine in Microsoft Azure or Hyper-V:

```
sudo ln -s /dev/null /etc/udev/rules.d/75-persistent-net-generator.rules
sudo rm -f /etc/udev/rules.d/70-persistent-net.rules
```

7. Ensure the network service will start at boot time by running the following command:

```
sudo chkconfig network on
```

8. If you would like to use the OpenLogic mirrors that are hosted within the Azure datacenters, then replace the `/etc/yum.repos.d/CentOS-Base.repo` file with the following repositories. This will also add the **[openlogic]** repository that includes additional packages such as the Azure Linux agent:

```

[openlogic]
name=CentOS-$releasever - openlogic packages for $basearch
baseurl=http://olcentgbl.trafficmanager.net/openlogic/$releasever/openlogic/$basearch/
enabled=1
gpgcheck=0

[base]
name=CentOS-$releasever - Base
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=os&infra=$infra
baseurl=http://olcentgbl.trafficmanager.net/centos/$releasever/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6

#released updates
[updates]
name=CentOS-$releasever - Updates
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=updates&infra=$infra
baseurl=http://olcentgbl.trafficmanager.net/centos/$releasever/updates/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6

#additional packages that may be useful
[extras]
name=CentOS-$releasever - Extras
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=extras&infra=$infra
baseurl=http://olcentgbl.trafficmanager.net/centos/$releasever/extras/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6

#additional packages that extend functionality of existing packages
[centosplus]
name=CentOS-$releasever - Plus
#mirrorlist=http://mirrorlist.centos.org/?
release=$releasever&arch=$basearch&repo=centosplus&infra=$infra
baseurl=http://olcentgbl.trafficmanager.net/centos/$releasever/centosplus/$basearch/
gpgcheck=1
enabled=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6

#contrib - packages by Centos Users
[contrib]
name=CentOS-$releasever - Contrib
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=contrib&infra=$infra
baseurl=http://olcentgbl.trafficmanager.net/centos/$releasever/contrib/$basearch/
gpgcheck=1
enabled=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6

```

#### NOTE

The rest of this guide will assume you are using at least the `[openlogic]` repo, which will be used to install the Azure Linux agent below.

- Add the following line to `/etc/yum.conf`:

```
http_caching=packages
```

- Run the following command to clear the current yum metadata and update the system with the latest packages:

```
yum clean all
```

Unless you are creating an image for an older version of CentOS, it is recommended to update all the packages to the latest:

```
sudo yum -y update
```

A reboot may be required after running this command.

11. (Optional) Install the drivers for the Linux Integration Services (LIS).

**IMPORTANT**

The step is **required** for CentOS 6.3 and earlier, and optional for later releases.

```
sudo rpm -e hypervkvpd ## (may return error if not installed, that's OK)
sudo yum install microsoft-hyper-v
```

Alternatively, you can follow the manual installation instructions on the [LIS download page](#) to install the RPM onto your VM.

12. Install the Azure Linux Agent and dependencies. Start and enable waagent service:

```
sudo yum install python-pyasn1 WALinuxAgent
sudo service waagent start
sudo chkconfig waagent on
```

The WALinuxAgent package will remove the NetworkManager and NetworkManager-gnome packages if they were not already removed as described in step 3.

13. Modify the kernel boot line in your grub configuration to include additional kernel parameters for Azure. To do this, open `/boot/grub/menu.lst` in a text editor and ensure that the default kernel includes the following parameters:

```
console=ttyS0 earlyprintk=ttyS0 rootdelay=300
```

This will also ensure all console messages are sent to the first serial port, which can assist Azure support with debugging issues.

In addition to the above, it is recommended to *remove* the following parameters:

```
rhgb quiet crashkernel=auto
```

Graphical and quiet boot are not useful in a cloud environment where we want all the logs to be sent to the serial port. The `crashkernel` option may be left configured if desired, but note that this parameter will reduce the amount of available memory in the VM by 128MB or more, which may be problematic on the smaller VM sizes.

### IMPORTANT

CentOS 6.5 and earlier must also set the kernel parameter `numa=off`. See Red Hat [KB 436883](#).

14. Ensure that the SSH server is installed and configured to start at boot time. This is usually the default.

15. Do not create swap space on the OS disk.

The Azure Linux Agent can automatically configure swap space using the local resource disk that is attached to the VM after provisioning on Azure. Note that the local resource disk is a *temporary* disk, and might be emptied when the VM is deprovisioned. After installing the Azure Linux Agent (see previous step), modify the following parameters in `/etc/waagent.conf` appropriately:

```
ResourceDisk.Format=y
ResourceDisk.Filesystem=ext4
ResourceDisk.MountPoint=/mnt/resource
ResourceDisk.EnableSwap=y
ResourceDisk.SwapSizeMB=2048 ## NOTE: set this to whatever you need it to be.
```

16. Run the following commands to deprovision the virtual machine and prepare it for provisioning on Azure:

```
sudo waagent -force -deprovision
export HISTSIZE=0
logout
```

17. Click **Action -> Shut Down** in Hyper-V Manager. Your Linux VHD is now ready to be uploaded to Azure.

## CentOS 7.0+

### Changes in CentOS 7 (and similar derivatives)

Preparing a CentOS 7 virtual machine for Azure is very similar to CentOS 6, however there are several important differences worth noting:

- The NetworkManager package no longer conflicts with the Azure Linux agent. This package is installed by default and we recommend that it is not removed.
- GRUB2 is now used as the default bootloader, so the procedure for editing kernel parameters has changed (see below).
- XFS is now the default file system. The ext4 file system can still be used if desired.

### Configuration Steps

1. In Hyper-V Manager, select the virtual machine.

2. Click **Connect** to open a console window for the virtual machine.

3. Create or edit the file `/etc/sysconfig/network` and add the following text:

```
NETWORKING=yes
HOSTNAME=localhost.localdomain
```

4. Create or edit the file `/etc/sysconfig/network-scripts/ifcfg-eth0` and add the following text:

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
TYPE=Ethernet
USERCTL=no
PEERDNS=yes
IPV6INIT=no
NM_CONTROLLED=no
```

5. Modify udev rules to avoid generating static rules for the Ethernet interface(s). These rules can cause problems when cloning a virtual machine in Microsoft Azure or Hyper-V:

```
sudo ln -s /dev/null /etc/udev/rules.d/75-persistent-net-generator.rules
```

6. If you would like to use the OpenLogic mirrors that are hosted within the Azure datacenters, then replace the `/etc/yum.repos.d/CentOS-Base.repo` file with the following repositories. This will also add the **[openlogic]** repository that includes packages for the Azure Linux agent:

```
[openlogic]
name=CentOS-$releasever - openlogic packages for $basearch
baseurl=http://olcentgbl.trafficmanager.net/openlogic/$releasever/openlogic/$basearch/
enabled=1
gpgcheck=0

[base]
name=CentOS-$releasever - Base
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=os&infra=$infra
baseurl=http://olcentgbl.trafficmanager.net/centos/$releasever/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

#released updates
[updates]
name=CentOS-$releasever - Updates
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=updates&infra=$infra
baseurl=http://olcentgbl.trafficmanager.net/centos/$releasever/updates/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

#additional packages that may be useful
[extras]
name=CentOS-$releasever - Extras
#mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=extras&infra=$infra
baseurl=http://olcentgbl.trafficmanager.net/centos/$releasever/extras/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

#additional packages that extend functionality of existing packages
[centosplus]
name=CentOS-$releasever - Plus
#mirrorlist=http://mirrorlist.centos.org/?
release=$releasever&arch=$basearch&repo=centosplus&infra=$infra
baseurl=http://olcentgbl.trafficmanager.net/centos/$releasever/centosplus/$basearch/
gpgcheck=1
enabled=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
```

#### NOTE

The rest of this guide will assume you are using at least the `[openlogic]` repo, which will be used to install the Azure Linux agent below.

7. Run the following command to clear the current yum metadata and install any updates:

```
sudo yum clean all
```

Unless you are creating an image for an older version of CentOS, it is recommended to update all the packages to the latest:

```
sudo yum -y update
```

A reboot maybe required after running this command.

8. Modify the kernel boot line in your grub configuration to include additional kernel parameters for Azure. To do this, open `/etc/default/grub` in a text editor and edit the `GRUB_CMDLINE_LINUX` parameter, for example:

```
GRUB_CMDLINE_LINUX="rootdelay=300 console=ttyS0 earlyprintk=ttyS0 net.ifnames=0"
```

This will also ensure all console messages are sent to the first serial port, which can assist Azure support with debugging issues. It also turns off the new CentOS 7 naming conventions for NICs. In addition to the above, it is recommended to *remove* the following parameters:

```
rhgb quiet crashkernel=auto
```

Graphical and quiet boot are not useful in a cloud environment where we want all the logs to be sent to the serial port. The `crashkernel` option may be left configured if desired, but note that this parameter will reduce the amount of available memory in the VM by 128MB or more, which may be problematic on the smaller VM sizes.

9. Once you are done editing `/etc/default/grub` per above, run the following command to rebuild the grub configuration:

```
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

10. If building the image from **VMware, VirtualBox or KVM**: Ensure the Hyper-V drivers are included in the initramfs:

Edit `/etc/dracut.conf`, add content:

```
add_drivers+=" hv_vmbus hv_netvsc hv_storvsc "
```

Rebuild the initramfs:

```
sudo dracut -f -v
```

11. Install the Azure Linux Agent and dependencies:

```
sudo yum install python-pyasn1 WALinuxAgent
sudo systemctl enable waagent
```

12. Do not create swap space on the OS disk.

The Azure Linux Agent can automatically configure swap space using the local resource disk that is attached to the VM after provisioning on Azure. Note that the local resource disk is a *temporary* disk, and might be emptied when the VM is deprovisioned. After installing the Azure Linux Agent (see previous step), modify the following parameters in `/etc/waagent.conf` appropriately:

```
ResourceDisk.Format=y
ResourceDisk.Filesystem=ext4
ResourceDisk.MountPoint=/mnt/resource
ResourceDisk.EnableSwap=y
ResourceDisk.SwapSizeMB=2048 ## NOTE: set this to whatever you need it to be.
```

13. Run the following commands to deprovision the virtual machine and prepare it for provisioning on Azure:

```
sudo waagent -force -deprovision
export HISTSIZE=0
logout
```

14. Click **Action -> Shut Down** in Hyper-V Manager. Your Linux VHD is now ready to be uploaded to Azure.

## Next steps

You're now ready to use your CentOS Linux virtual hard disk to create new virtual machines in Azure. If this is the first time that you're uploading the .vhd file to Azure, see [Create a Linux VM from a custom disk](#).

# Prepare a Red Hat-based virtual machine for Azure

1/16/2020 • 26 minutes to read • [Edit Online](#)

In this article, you will learn how to prepare a Red Hat Enterprise Linux (RHEL) virtual machine for use in Azure. The versions of RHEL that are covered in this article are 6.7+ and 7.1+. The hypervisors for preparation that are covered in this article are Hyper-V, kernel-based virtual machine (KVM), and VMware. For more information about eligibility requirements for participating in Red Hat's Cloud Access program, see [Red Hat's Cloud Access website](#) and [Running RHEL on Azure](#). For ways to automate building RHEL images see the [Azure Image Builder](#).

## Prepare a Red Hat-based virtual machine from Hyper-V Manager

### Prerequisites

This section assumes that you have already obtained an ISO file from the Red Hat website and installed the RHEL image to a virtual hard disk (VHD). For more details about how to use Hyper-V Manager to install an operating system image, see [Install the Hyper-V Role and Configure a Virtual Machine](#).

### RHEL installation notes

- Azure does not support the VHDX format. Azure supports only fixed VHD. You can use Hyper-V Manager to convert the disk to VHD format, or you can use the convert-vhd cmdlet. If you use VirtualBox, select **Fixed size** as opposed to the default dynamically allocated option when you create the disk.
- Azure supports Gen1 (BIOS boot) & Gen2 (UEFI boot) Virtual machines.
- The maximum size that's allowed for the VHD is 1,023 GB.
- Logical Volume Manager (LVM) is supported and may be used on the OS disk or data disks in Azure virtual machines. However, in general it is recommended to use standard partitions on the OS disk rather than LVM. This practice will avoid LVM name conflicts with cloned virtual machines, particularly if you ever need to attach an operating system disk to another identical virtual machine for troubleshooting. See also [LVM](#) and [RAID](#) documentation.
- Kernel support for mounting Universal Disk Format (UDF) file systems is required. At first boot on Azure, the UDF-formatted media that is attached to the guest passes the provisioning configuration to the Linux virtual machine. The Azure Linux Agent must be able to mount the UDF file system to read its configuration and provision the virtual machine.
- Do not configure a swap partition on the operating system disk. The Linux Agent can be configured to create a swap file on the temporary resource disk. More information about this can be found in the following steps.
- All VHDs on Azure must have a virtual size aligned to 1MB. When converting from a raw disk to VHD you must ensure that the raw disk size is a multiple of 1MB before conversion. More details can be found in the steps below. See also [Linux Installation Notes](#) for more information.

### Prepare a RHEL 6 virtual machine from Hyper-V Manager

1. In Hyper-V Manager, select the virtual machine.
2. Click **Connect** to open a console window for the virtual machine.
3. In RHEL 6, NetworkManager can interfere with the Azure Linux agent. Uninstall this package by running the following command:

```
sudo rpm -e --nodeps NetworkManager
```

4. Create or edit the `/etc/sysconfig/network` file, and add the following text:

```
NETWORKING=yes
HOSTNAME=localhost.localdomain
```

5. Create or edit the `/etc/sysconfig/network-scripts/ifcfg-eth0` file, and add the following text:

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
TYPE=Ethernet
USERCTL=no
PEERDNS=yes
IPV6INIT=no
```

6. Move (or remove) the udev rules to avoid generating static rules for the Ethernet interface. These rules cause problems when you clone a virtual machine in Microsoft Azure or Hyper-V:

```
sudo ln -s /dev/null /etc/udev/rules.d/75-persistent-net-generator.rules

sudo rm -f /etc/udev/rules.d/70-persistent-net.rules
```

7. Ensure that the network service will start at boot time by running the following command:

```
sudo chkconfig network on
```

8. Register your Red Hat subscription to enable the installation of packages from the RHEL repository by running the following command:

```
sudo subscription-manager register --auto-attach --username=XXX --password=XXX
```

9. The WALinuxAgent package, `WALinuxAgent-<version>`, has been pushed to the Red Hat extras repository. Enable the extras repository by running the following command:

```
subscription-manager repos --enable=rhel-6-server-extras-rpms
```

10. Modify the kernel boot line in your grub configuration to include additional kernel parameters for Azure. To do this modification, open `/boot/grub/menu.1st` in a text editor, and ensure that the default kernel includes the following parameters:

```
console=ttyS0 earlyprintk=ttyS0 rootdelay=300
```

This will also ensure that all console messages are sent to the first serial port, which can assist Azure support with debugging issues.

In addition, we recommended that you remove the following parameters:

```
rhgb quiet crashkernel=auto
```

Graphical and quiet boot are not useful in a cloud environment where we want all the logs to be sent to the serial port. You can leave the `crashkernel` option configured if desired. Note that this parameter reduces the amount of available memory in the virtual machine by 128 MB or more. This configuration might be problematic on smaller virtual machine sizes.

11. Ensure that the secure shell (SSH) server is installed and configured to start at boot time, which is usually the default. Modify `/etc/ssh/sshd_config` to include the following line:

```
ClientAliveInterval 180
```

12. Install the Azure Linux Agent by running the following command:

```
sudo yum install WALinuxAgent
sudo chkconfig waagent on
```

Installing the WALinuxAgent package removes the NetworkManager and NetworkManager-gnome packages if they were not already removed in step 3.

13. Do not create swap space on the operating system disk.

The Azure Linux Agent can automatically configure swap space by using the local resource disk that is attached to the virtual machine after the virtual machine is provisioned on Azure. Note that the local resource disk is a temporary disk and that it might be emptied if the virtual machine is deprovisioned. After you install the Azure Linux Agent in the previous step, modify the following parameters in `/etc/waagent.conf` appropriately:

```
ResourceDisk.Format=y
ResourceDisk.Filesystem=ext4
ResourceDisk.MountPoint=/mnt/resource
ResourceDisk.EnableSwap=y
ResourceDisk.SwapSizeMB=2048 ## NOTE: set this to whatever you need it to be.
```

14. Unregister the subscription (if necessary) by running the following command:

```
sudo subscription-manager unregister
```

15. Run the following commands to deprovision the virtual machine and prepare it for provisioning on Azure:

```
Note: if you are migrating a specific virtual machine and do not wish to create a generalized image,
skip the deprovision step
sudo waagent -force -deprovision

export HISTSIZE=0

logout
```

16. Click **Action > Shut Down** in Hyper-V Manager. Your Linux VHD is now ready to be uploaded to Azure.

#### Prepare a RHEL 7 virtual machine from Hyper-V Manager

1. In Hyper-V Manager, select the virtual machine.
2. Click **Connect** to open a console window for the virtual machine.
3. Create or edit the `/etc/sysconfig/network` file, and add the following text:

```
NETWORKING=yes
HOSTNAME=localhost.localdomain
```

4. Create or edit the `/etc/sysconfig/network-scripts/ifcfg-eth0` file, and add the following text:

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
TYPE=Ethernet
USERCTL=no
PEERDNS=yes
IPV6INIT=no
```

PERSISTENT\_DHCLIENT=yes NM\_CONTROLLED=yes

5. Ensure that the network service will start at boot time by running the following command:

```
sudo systemctl enable network
```

6. Register your Red Hat subscription to enable the installation of packages from the RHEL repository by running the following command:

```
sudo subscription-manager register --auto-attach --username=XXX --password=XXX
```

7. Modify the kernel boot line in your grub configuration to include additional kernel parameters for Azure. To do this modification, open `/etc/default/grub` in a text editor, and edit the `GRUB_CMDLINE_LINUX` parameter. For example:

```
GRUB_CMDLINE_LINUX="rootdelay=300 console=ttyS0 earlyprintk=ttyS0 net.ifnames=0"
```

This will also ensure that all console messages are sent to the first serial port, which can assist Azure support with debugging issues. This configuration also turns off the new RHEL 7 naming conventions for NICs. In addition, we recommend that you remove the following parameters:

```
rhgb quiet crashkernel=auto
```

Graphical and quiet boot are not useful in a cloud environment where we want all the logs to be sent to the serial port. You can leave the `crashkernel` option configured if desired. Note that this parameter reduces the amount of available memory in the virtual machine by 128 MB or more, which might be problematic on smaller virtual machine sizes.

8. After you are done editing `/etc/default/grub`, run the following command to rebuild the grub configuration:

```
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

9. Ensure that the SSH server is installed and configured to start at boot time, which is usually the default. Modify `/etc/ssh/sshd_config` to include the following line:

```
ClientAliveInterval 180
```

10. The WALinuxAgent package, `WALinuxAgent-<version>`, has been pushed to the Red Hat extras repository. Enable the extras repository by running the following command:

```
subscription-manager repos --enable=rhel-7-server-extras-rpms
```

11. Install the Azure Linux Agent by running the following command:

```
sudo yum install WALinuxAgent
sudo systemctl enable waagent.service
```

12. Do not create swap space on the operating system disk.

The Azure Linux Agent can automatically configure swap space by using the local resource disk that is attached to the virtual machine after the virtual machine is provisioned on Azure. Note that the local resource disk is a temporary disk, and it might be emptied if the virtual machine is deprovisioned. After you install the Azure Linux Agent in the previous step, modify the following parameters in `/etc/waagent.conf` appropriately:

```
ResourceDisk.Format=y
ResourceDisk.Filesystem=ext4
ResourceDisk.MountPoint=/mnt/resource
ResourceDisk.EnableSwap=y
ResourceDisk.SwapSizeMB=2048 ## NOTE: set this to whatever you need it to be.
```

13. If you want to unregister the subscription, run the following command:

```
sudo subscription-manager unregister
```

14. Run the following commands to deprovision the virtual machine and prepare it for provisioning on Azure:

```
Note: if you are migrating a specific virtual machine and do not wish to create a generalized image,
skip the deprovision step
sudo waagent -force -deprovision

export HISTSIZE=0

logout
```

15. Click **Action** > **Shut Down** in Hyper-V Manager. Your Linux VHD is now ready to be uploaded to Azure.

## Prepare a Red Hat-based virtual machine from KVM

### Prepare a RHEL 6 virtual machine from KVM

1. Download the KVM image of RHEL 6 from the Red Hat website.
2. Set a root password.

Generate an encrypted password, and copy the output of the command:

```
openssl passwd -1 changeme
```

Set a root password with guestfish:

```
guestfish --rw -a <image-name>
> <fs> run
> <fs> list-filesystems
> <fs> mount /dev/sda1 /
> <fs> vi /etc/shadow
> <fs> exit
```

Change the second field of the root user from "!!" to the encrypted password.

3. Create a virtual machine in KVM from the qcow2 image. Set the disk type to **qcow2**, and set the virtual network interface device model to **virtio**. Then, start the virtual machine, and sign in as root.
4. Create or edit the `/etc/sysconfig/network` file, and add the following text:

```
NETWORKING=yes
HOSTNAME=localhost.localdomain
```

5. Create or edit the `/etc/sysconfig/network-scripts/ifcfg-eth0` file, and add the following text:

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
TYPE=Ethernet
USERCTL=no
PEERDNS=yes
IPV6INIT=no
```

6. Move (or remove) the udev rules to avoid generating static rules for the Ethernet interface. These rules cause problems when you clone a virtual machine in Azure or Hyper-V:

```
sudo ln -s /dev/null /etc/udev/rules.d/75-persistent-net-generator.rules
sudo rm -f /etc/udev/rules.d/70-persistent-net.rules
```

7. Ensure that the network service will start at boot time by running the following command:

```
chkconfig network on
```

8. Register your Red Hat subscription to enable the installation of packages from the RHEL repository by running the following command:

```
subscription-manager register --auto-attach --username=XXX --password=XXX
```

9. Modify the kernel boot line in your grub configuration to include additional kernel parameters for Azure. To do this configuration, open `/boot/grub/menu.lst` in a text editor, and ensure that the default kernel includes the following parameters:

```
console=ttyS0 earlyprintk=ttyS0 rootdelay=300
```

This will also ensure that all console messages are sent to the first serial port, which can assist Azure support with debugging issues.

In addition, we recommend that you remove the following parameters:

```
rhgb quiet crashkernel=auto
```

Graphical and quiet boot are not useful in a cloud environment where we want all the logs to be sent to the serial port. You can leave the `crashkernel` option configured if desired. Note that this parameter reduces the amount of available memory in the virtual machine by 128 MB or more, which might be problematic on smaller virtual machine sizes.

10. Add Hyper-V modules to initramfs:

Edit `/etc/dracut.conf`, and add the following content:

```
add_drivers+=" hv_vmbus hv_netvsc hv_storvsc "
```

Rebuild initramfs:

```
dracut -f -v
```

11. Uninstall cloud-init:

```
yum remove cloud-init
```

12. Ensure that the SSH server is installed and configured to start at boot time:

```
chkconfig sshd on
```

Modify `/etc/ssh/sshd_config` to include the following lines:

```
PasswordAuthentication yes
ClientAliveInterval 180
```

13. The WALinuxAgent package, `WALinuxAgent-<version>`, has been pushed to the Red Hat extras repository.

Enable the extras repository by running the following command:

```
subscription-manager repos --enable=rhel-6-server-extras-rpms
```

14. Install the Azure Linux Agent by running the following command:

```
yum install WALinuxAgent

chkconfig waagent on
```

15. The Azure Linux Agent can automatically configure swap space by using the local resource disk that is attached to the virtual machine after the virtual machine is provisioned on Azure. Note that the local resource disk is a temporary disk, and it might be emptied if the virtual machine is deprovisioned. After you install the Azure Linux Agent in the previous step, modify the following parameters in `/etc/waagent.conf` appropriately:

```
ResourceDisk.Format=y
ResourceDisk.Filesystem=ext4
ResourceDisk.MountPoint=/mnt/resource
ResourceDisk.EnableSwap=y
ResourceDisk.SwapSizeMB=2048 ## NOTE: set this to whatever you need it to be.
```

16. Unregister the subscription (if necessary) by running the following command:

```
subscription-manager unregister
```

17. Run the following commands to deprovision the virtual machine and prepare it for provisioning on Azure:

```
Note: if you are migrating a specific virtual machine and do not wish to create a generalized image,
skip the deprovision step
waagent -force -deprovision

export HISTSIZE=0

logout
```

18. Shut down the virtual machine in KVM.

19. Convert the qcow2 image to the VHD format.

**NOTE**

There is a known bug in qemu-img versions >=2.2.1 that results in an improperly formatted VHD. The issue has been fixed in QEMU 2.6. It is recommended to use either qemu-img 2.2.0 or lower, or update to 2.6 or higher. Reference:  
<https://bugs.launchpad.net/qemu/+bug/1490611>.

First convert the image to raw format:

```
qemu-img convert -f qcow2 -O raw rhel-6.9.qcow2 rhel-6.9.raw
```

Make sure that the size of the raw image is aligned with 1 MB. Otherwise, round up the size to align with 1 MB:

```
MB=$((1024*1024))
size=$(qemu-img info -f raw --output json "rhel-6.9.raw" | \
gawk 'match($0, /"virtual-size": ([0-9]+),/, val) {print val[1]}'')
#
rounded_size=$(((size/$MB + 1)*$MB))
qemu-img resize rhel-6.9.raw $rounded_size
```

Convert the raw disk to a fixed-sized VHD:

```
qemu-img convert -f raw -o subformat=fixed -O vpc rhel-6.9.raw rhel-6.9.vhd
```

Or, with qemu version \*\*2.6+\*\* include the `force\_size` option:

```
qemu-img convert -f raw -o subformat=fixed,force_size -O vpc rhel-6.9.raw rhel-6.9.vhd
```

## Prepare a RHEL 7 virtual machine from KVM

1. Download the KVM image of RHEL 7 from the Red Hat website. This procedure uses RHEL 7 as the example.

## 2. Set a root password.

Generate an encrypted password, and copy the output of the command:

```
openssl passwd -1 changeme
```

Set a root password with guestfish:

```
guestfish --rw -a <image-name>
> <fs> run
> <fs> list-filesystems
> <fs> mount /dev/sda1 /
> <fs> vi /etc/shadow
> <fs> exit
```

Change the second field of root user from "!!" to the encrypted password.

3. Create a virtual machine in KVM from the qcow2 image. Set the disk type to **qcow2**, and set the virtual network interface device model to **virtio**. Then, start the virtual machine, and sign in as root.
4. Create or edit the `/etc/sysconfig/network` file, and add the following text:

```
NETWORKING=yes
HOSTNAME=localhost.localdomain
```

5. Create or edit the `/etc/sysconfig/network-scripts/ifcfg-eth0` file, and add the following text:

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
TYPE=Ethernet
USERCTL=no
PEERDNS=yes
IPV6INIT=no
```

PERSISTENT\_DHCLIENT=yes NM\_CONTROLLED=yes

6. Ensure that the network service will start at boot time by running the following command:

```
sudo systemctl enable network
```

7. Register your Red Hat subscription to enable installation of packages from the RHEL repository by running the following command:

```
subscription-manager register --auto-attach --username=XXX --password=XXX
```

8. Modify the kernel boot line in your grub configuration to include additional kernel parameters for Azure. To do this configuration, open `/etc/default/grub` in a text editor, and edit the `GRUB_CMDLINE_LINUX` parameter. For example:

```
GRUB_CMDLINE_LINUX="rootdelay=300 console=ttyS0 earlyprintk=ttyS0 net.ifnames=0"
```

This command also ensures that all console messages are sent to the first serial port, which can assist Azure support with debugging issues. The command also turns off the new RHEL 7 naming conventions for NICs.

In addition, we recommend that you remove the following parameters:

```
rhgb quiet crashkernel=auto
```

Graphical and quiet boot are not useful in a cloud environment where we want all the logs to be sent to the serial port. You can leave the `crashkernel` option configured if desired. Note that this parameter reduces the amount of available memory in the virtual machine by 128 MB or more, which might be problematic on smaller virtual machine sizes.

9. After you are done editing `/etc/default/grub`, run the following command to rebuild the grub configuration:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

10. Add Hyper-V modules into initramfs.

Edit `/etc/dracut.conf` and add content:

```
add_drivers+=" hv_vmbus hv_netvsc hv_storvsc "
```

Rebuild initramfs:

```
dracut -f -v
```

11. Uninstall cloud-init:

```
yum remove cloud-init
```

12. Ensure that the SSH server is installed and configured to start at boot time:

```
systemctl enable sshd
```

Modify `/etc/ssh/sshd_config` to include the following lines:

```
PasswordAuthentication yes
ClientAliveInterval 180
```

13. The WALinuxAgent package, `WALinuxAgent-<version>`, has been pushed to the Red Hat extras repository.

Enable the extras repository by running the following command:

```
subscription-manager repos --enable=rhel-7-server-extras-rpms
```

14. Install the Azure Linux Agent by running the following command:

```
yum install WALinuxAgent
```

Enable the waagent service:

```
systemctl enable waagent.service
```

15. Do not create swap space on the operating system disk.

The Azure Linux Agent can automatically configure swap space by using the local resource disk that is attached to the virtual machine after the virtual machine is provisioned on Azure. Note that the local resource disk is a temporary disk, and it might be emptied if the virtual machine is deprovisioned. After you install the Azure Linux Agent in the previous step, modify the following parameters in `/etc/waagent.conf` appropriately:

```
ResourceDisk.Format=y
ResourceDisk.Filesystem=ext4
ResourceDisk.MountPoint=/mnt/resource
ResourceDisk.EnableSwap=y
ResourceDisk.SwapSizeMB=2048 ## NOTE: set this to whatever you need it to be.
```

16. Unregister the subscription (if necessary) by running the following command:

```
subscription-manager unregister
```

17. Run the following commands to deprovision the virtual machine and prepare it for provisioning on Azure:

```
Note: if you are migrating a specific virtual machine and do not wish to create a generalized image,
skip the deprovision step
sudo waagent -force -deprovision

export HISTSIZE=0

logout
```

18. Shut down the virtual machine in KVM.

19. Convert the qcow2 image to the VHD format.

**NOTE**

There is a known bug in qemu-img versions >=2.2.1 that results in an improperly formatted VHD. The issue has been fixed in QEMU 2.6. It is recommended to use either qemu-img 2.2.0 or lower, or update to 2.6 or higher. Reference: <https://bugs.launchpad.net/qemu/+bug/1490611>.

```
First convert the image to raw format:
```

```
qemu-img convert -f qcow2 -O raw rhel-7.4.qcow2 rhel-7.4.raw
```

```
Make sure that the size of the raw image is aligned with 1 MB. Otherwise, round up the size to align with 1 MB:
```

```
MB=$((1024*1024))
size=$(qemu-img info -f raw --output json "rhel-7.4.raw" | \
gawk 'match($0, /"virtual-size": ([0-9]+),/, val) {print val[1]}'')
#
rounded_size=$(((size/$MB + 1)*$MB))
qemu-img resize rhel-7.4.raw $rounded_size
```

```
Convert the raw disk to a fixed-sized VHD:
```

```
qemu-img convert -f raw -o subformat=fixed -O vpc rhel-7.4.raw rhel-7.4.vhd
```

```
Or, with qemu version **2.6+** include the `force_size` option:
```

```
qemu-img convert -f raw -o subformat=fixed,force_size -O vpc rhel-7.4.raw rhel-7.4.vhd
```

## Prepare a Red Hat-based virtual machine from VMware

### Prerequisites

This section assumes that you have already installed a RHEL virtual machine in VMware. For details about how to install an operating system in VMware, see [VMware Guest Operating System Installation Guide](#).

- When you install the Linux operating system, we recommend that you use standard partitions rather than LVM, which is often the default for many installations. This will avoid LVM name conflicts with cloned virtual machine, particularly if an operating system disk ever needs to be attached to another virtual machine for troubleshooting. LVM or RAID can be used on data disks if preferred.
- Do not configure a swap partition on the operating system disk. You can configure the Linux agent to create a swap file on the temporary resource disk. You can find more information about this in the steps that follow.
- When you create the virtual hard disk, select **Store virtual disk as a single file**.

### Prepare a RHEL 6 virtual machine from VMware

- In RHEL 6, NetworkManager can interfere with the Azure Linux agent. Uninstall this package by running the following command:

```
sudo rpm -e --nodeps NetworkManager
```

- Create a file named **network** in the `/etc/sysconfig/` directory that contains the following text:

```
NETWORKING=yes
HOSTNAME=localhost.localdomain
```

- Create or edit the `/etc/sysconfig/network-scripts/ifcfg-eth0` file, and add the following text:

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
TYPE=Ethernet
USERCTL=no
PEERDNS=yes
IPV6INIT=no
```

4. Move (or remove) the udev rules to avoid generating static rules for the Ethernet interface. These rules cause problems when you clone a virtual machine in Azure or Hyper-V:

```
sudo ln -s /dev/null /etc/udev/rules.d/75-persistent-net-generator.rules
sudo rm -f /etc/udev/rules.d/70-persistent-net.rules
```

5. Ensure that the network service will start at boot time by running the following command:

```
sudo chkconfig network on
```

6. Register your Red Hat subscription to enable the installation of packages from the RHEL repository by running the following command:

```
sudo subscription-manager register --auto-attach --username=XXX --password=XXX
```

7. The WALinuxAgent package, `WALinuxAgent-<version>`, has been pushed to the Red Hat extras repository. Enable the extras repository by running the following command:

```
subscription-manager repos --enable=rhel-6-server-extras-rpms
```

8. Modify the kernel boot line in your grub configuration to include additional kernel parameters for Azure. To do this, open `/etc/default/grub` in a text editor, and edit the `GRUB_CMDLINE_LINUX` parameter. For example:

```
GRUB_CMDLINE_LINUX="rootdelay=300 console=ttyS0 earlyprintk=ttyS0"
```

This will also ensure that all console messages are sent to the first serial port, which can assist Azure support with debugging issues. In addition, we recommend that you remove the following parameters:

```
rhgb quiet crashkernel=auto
```

Graphical and quiet boot are not useful in a cloud environment where we want all the logs to be sent to the serial port. You can leave the `crashkernel` option configured if desired. Note that this parameter reduces the amount of available memory in the virtual machine by 128 MB or more, which might be problematic on smaller virtual machine sizes.

9. Add Hyper-V modules to initramfs:

Edit `/etc/dracut.conf`, and add the following content:

```
add_drivers+=" hv_vmbus hv_netvsc hv_storvsc "
```

Rebuild initramfs:

```
dracut -f -v
```

10. Ensure that the SSH server is installed and configured to start at boot time, which is usually the default. Modify `/etc/ssh/sshd_config` to include the following line:

`ClientAliveInterval 180`

11. Install the Azure Linux Agent by running the following command:

```
sudo yum install WALinuxAgent
sudo chkconfig waagent on
```

12. Do not create swap space on the operating system disk.

The Azure Linux Agent can automatically configure swap space by using the local resource disk that is attached to the virtual machine after the virtual machine is provisioned on Azure. Note that the local resource disk is a temporary disk, and it might be emptied if the virtual machine is deprovisioned. After you install the Azure Linux Agent in the previous step, modify the following parameters in `/etc/waagent.conf` appropriately:

```
ResourceDisk.Format=y
ResourceDisk.Filesystem=ext4
ResourceDisk.MountPoint=/mnt/resource
ResourceDisk.EnableSwap=y
ResourceDisk.SwapSizeMB=2048 ## NOTE: set this to whatever you need it to be.
```

13. Unregister the subscription (if necessary) by running the following command:

```
sudo subscription-manager unregister
```

14. Run the following commands to deprovision the virtual machine and prepare it for provisioning on Azure:

```
Note: if you are migrating a specific virtual machine and do not wish to create a generalized image,
skip the deprovision step
sudo waagent -force -deprovision

export HISTSIZE=0

logout
```

15. Shut down the virtual machine, and convert the VMDK file to a .vhdx file.

**NOTE**

There is a known bug in qemu-img versions >=2.2.1 that results in an improperly formatted VHD. The issue has been fixed in QEMU 2.6. It is recommended to use either qemu-img 2.2.0 or lower, or update to 2.6 or higher. Reference: <https://bugs.launchpad.net/qemu/+bug/1490611>.

```
First convert the image to raw format:
```

```
qemu-img convert -f vmdk -O raw rhel-6.9.vmdk rhel-6.9.raw
```

```
Make sure that the size of the raw image is aligned with 1 MB. Otherwise, round up the size to align with 1 MB:
```

```
MB=$((1024*1024))
size=$(qemu-img info -f raw --output json "rhel-6.9.raw" | \
gawk 'match($0, /"virtual-size": ([0-9]+),/, val) {print val[1]}')
#
rounded_size=$(((size/$MB + 1)*$MB))
qemu-img resize rhel-6.9.raw $rounded_size
```

```
Convert the raw disk to a fixed-sized VHD:
```

```
qemu-img convert -f raw -o subformat=fixed -O vpc rhel-6.9.raw rhel-6.9.vhd
```

```
Or, with qemu version **2.6+** include the `force_size` option:
```

```
qemu-img convert -f raw -o subformat=fixed,force_size -O vpc rhel-6.9.raw rhel-6.9.vhd
```

## Prepare a RHEL 7 virtual machine from VMware

1. Create or edit the `/etc/sysconfig/network` file, and add the following text:

```
NETWORKING=yes
HOSTNAME=localhost.localdomain
```

2. Create or edit the `/etc/sysconfig/network-scripts/ifcfg-eth0` file, and add the following text:

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
TYPE=Ethernet
USERCTL=no
PEERDNS=yes
IPV6INIT=no
```

```
PERSISTENT_DHCLIENT=yes NM_CONTROLLED=yes
```

3. Ensure that the network service will start at boot time by running the following command:

```
sudo systemctl enable network
```

4. Register your Red Hat subscription to enable the installation of packages from the RHEL repository by running the following command:

```
sudo subscription-manager register --auto-attach --username=XXX --password=XXX
```

5. Modify the kernel boot line in your grub configuration to include additional kernel parameters for Azure. To do this modification, open `/etc/default/grub` in a text editor, and edit the `GRUB_CMDLINE_LINUX` parameter. For example:

```
GRUB_CMDLINE_LINUX="rootdelay=300 console=ttyS0 earlyprintk=ttyS0 net.ifnames=0"
```

This configuration also ensures that all console messages are sent to the first serial port, which can assist

Azure support with debugging issues. It also turns off the new RHEL 7 naming conventions for NICs. In addition, we recommend that you remove the following parameters:

```
rhgb quiet crashkernel=auto
```

Graphical and quiet boot are not useful in a cloud environment where we want all the logs to be sent to the serial port. You can leave the `crashkernel` option configured if desired. Note that this parameter reduces the amount of available memory in the virtual machine by 128 MB or more, which might be problematic on smaller virtual machine sizes.

6. After you are done editing `/etc/default/grub`, run the following command to rebuild the grub configuration:

```
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. Add Hyper-V modules to initramfs.

Edit `/etc/dracut.conf`, add content:

```
add_drivers+=" hv_vmbus hv_netvsc hv_storvsc "
```

Rebuild initramfs:

```
dracut -f -v
```

8. Ensure that the SSH server is installed and configured to start at boot time. This setting is usually the default. Modify `/etc/ssh/sshd_config` to include the following line:

```
ClientAliveInterval 180
```

9. The WALinuxAgent package, `WALinuxAgent-<version>`, has been pushed to the Red Hat extras repository. Enable the extras repository by running the following command:

```
subscription-manager repos --enable=rhel-7-server-extras-rpms
```

10. Install the Azure Linux Agent by running the following command:

```
sudo yum install WALinuxAgent
sudo systemctl enable waagent.service
```

11. Do not create swap space on the operating system disk.

The Azure Linux Agent can automatically configure swap space by using the local resource disk that is attached to the virtual machine after the virtual machine is provisioned on Azure. Note that the local resource disk is a temporary disk, and it might be emptied if the virtual machine is deprovisioned. After you install the Azure Linux Agent in the previous step, modify the following parameters in `/etc/waagent.conf` appropriately:

```
ResourceDisk.Format=y
ResourceDisk.Filesystem=ext4
ResourceDisk.MountPoint=/mnt/resource
ResourceDisk.EnableSwap=y
ResourceDisk.SwapSizeMB=2048 ## NOTE: set this to whatever you need it to be.
```

12. If you want to unregister the subscription, run the following command:

```
sudo subscription-manager unregister
```

13. Run the following commands to deprovision the virtual machine and prepare it for provisioning on Azure:

```
Note: if you are migrating a specific virtual machine and do not wish to create a generalized image,
skip the deprovision step
sudo waagent -force -deprovision

export HISTSIZE=0

logout
```

14. Shut down the virtual machine, and convert the VMDK file to the VHD format.

#### NOTE

There is a known bug in qemu-img versions >=2.2.1 that results in an improperly formatted VHD. The issue has been fixed in QEMU 2.6. It is recommended to use either qemu-img 2.2.0 or lower, or update to 2.6 or higher. Reference: <https://bugs.launchpad.net/qemu/+bug/1490611>.

First convert the image to raw format:

```
qemu-img convert -f vmdk -O raw rhel-7.4.vmdk rhel-7.4.raw
```

Make sure that the size of the raw image is aligned with 1 MB. Otherwise, round up the size to align with 1 MB:

```
MB=$((1024*1024))
size=$(qemu-img info -f raw --output json "rhel-7.4.raw" | \
gawk 'match($0, /"virtual-size": ([0-9]+),/, val) {print val[1]}')

rounded_size=$(((size/$MB + 1)*$MB))
qemu-img resize rhel-7.4.raw $rounded_size
```

Convert the raw disk to a fixed-sized VHD:

```
qemu-img convert -f raw -o subformat=fixed -O vpc rhel-7.4.raw rhel-7.4.vhd
```

Or, with qemu version \*\*2.6+\*\* include the `force\_size` option:

```
qemu-img convert -f raw -o subformat=fixed,force_size -O vpc rhel-7.4.raw rhel-7.4.vhd
```

## Prepare a Red Hat-based virtual machine from an ISO by using a kickstart file automatically

### Prepare a RHEL 7 virtual machine from a kickstart file

1. Create a kickstart file that includes the following content, and save the file. For details about kickstart installation, see the [Kickstart Installation Guide](#).

```
Kickstart for provisioning a RHEL 7 Azure VM

System authorization information
auth --enablesshadow --passalgo=sha512

Use graphical install
text

Do not run the Setup Agent on first boot
firstboot --disable

Keyboard layouts
keyboard --vckeymap=us --xlayouts='us'

System language
lang en_US.UTF-8

Network information
network --bootproto=dhcp

Root password
rootpw --plaintext "to_be_disabled"

System services
services --enabled="sshd,waagent,NetworkManager"

System timezone
timezone Etc/UTC --isUtc --ntpservers
0.rhel.pool.ntp.org,1.rhel.pool.ntp.org,2.rhel.pool.ntp.org,3.rhel.pool.ntp.org

Partition clearing information
clearpart --all --initlabel

Clear the MBR
zerombr

Disk partitioning information
part /boot --fstype="xfs" --size=500
part / --fstype="xfs" --size=1 --grow --asprimary

System bootloader configuration
bootloader --location=mbr

Firewall configuration
firewall --disabled

Enable SELinux
selinux --enforcing

Don't configure X
skipx

Power down the machine after install
poweroff

%packages
@base
@console-internet
chrony
sudo
parted
-dracut-config-rescue

%end

%post --log=/var/log/anaconda/post-install.log

#!/bin/bash
```

```

Register Red Hat Subscription
subscription-manager register --username=XXX --password=XXX --auto-attach --force

Install latest repo update
yum update -y

Enable extras repo
subscription-manager repos --enable=rhel-7-server-extras-rpms

Install WALinuxAgent
yum install -y WALinuxAgent

Unregister Red Hat subscription
subscription-manager unregister

Enable waagent at boot-up
systemctl enable waagent

Disable the root account
usermod root -p '!!!'

Configure swap in WALinuxAgent
sed -i 's/^(\ResourceDisk\.EnableSwap\)=\[Nn]\$/\1=y/g' /etc/waagent.conf
sed -i 's/^(\ResourceDisk\.SwapSizeMB\)=\[0-9]*\$/\1=2048/g' /etc/waagent.conf

Set the cmdline
sed -i 's/^(\GRUB_CMDLINE_LINUX\)=.*"\$/\1="console=tty1 console=ttyS0 earlyprintk=ttyS0
rootdelay=300"/g' /etc/default/grub

Enable SSH keepalive
sed -i 's/^#\<\!(ClientAliveInterval\).*\$/\1 180/g' /etc/ssh/sshd_config

Build the grub cfg
grub2-mkconfig -o /boot/grub2/grub.cfg

Configure network
cat << EOF > /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
TYPE=Ethernet
USERCTL=no
PEERDNS=yes
IPV6INIT=no

```

PERSISTENT\_DHCLIENT=yes NM\_CONTROLLED=yes EOF

```

Deprovision and prepare for Azure if you are creating a generalized image
waagent -force -deprovision

%end

```

2. Place the kickstart file where the installation system can access it.
3. In Hyper-V Manager, create a new virtual machine. On the **Connect Virtual Hard Disk** page, select **Attach a virtual hard disk later**, and complete the New Virtual Machine Wizard.
4. Open the virtual machine settings:
  - a. Attach a new virtual hard disk to the virtual machine. Make sure to select **VHD Format** and **Fixed Size**.
  - b. Attach the installation ISO to the DVD drive.
  - c. Set the BIOS to boot from CD.

5. Start the virtual machine. When the installation guide appears, press **Tab** to configure the boot options.
6. Enter `inst.ks=<the location of the kickstart file>` at the end of the boot options, and press **Enter**.
7. Wait for the installation to finish. When it's finished, the virtual machine will be shut down automatically.  
Your Linux VHD is now ready to be uploaded to Azure.

## Known issues

### The Hyper-V driver could not be included in the initial RAM disk when using a non-Hyper-V hypervisor

In some cases, Linux installers might not include the drivers for Hyper-V in the initial RAM disk (initrd or initramfs) unless Linux detects that it is running in a Hyper-V environment.

When you're using a different virtualization system (that is, VirtualBox, Xen, etc.) to prepare your Linux image, you might need to rebuild initrd to ensure that at least the hv\_vmbus and hv\_storvsc kernel modules are available on the initial RAM disk. This is a known issue at least on systems that are based on the upstream Red Hat distribution.

To resolve this issue, add Hyper-V modules to initramfs and rebuild it:

Edit `/etc/dracut.conf`, and add the following content:

```
add_drivers+=" hv_vmbus hv_netvsc hv_storvsc "
```

Rebuild initramfs:

```
dracut -f -v
```

For more details, see the information about [rebuilding initramfs](#).

## Next steps

- You're now ready to use your Red Hat Enterprise Linux virtual hard disk to create new virtual machines in Azure. If this is the first time that you're uploading the .vhdx file to Azure, see [Create a Linux VM from a custom disk](#).
- For more details about the hypervisors that are certified to run Red Hat Enterprise Linux, see [the Red Hat website](#).
- To learn more about using production-ready RHEL BYOS images, go to the documentation page for [BYOS](#).

# Prepare a Debian VHD for Azure

1/8/2020 • 3 minutes to read • [Edit Online](#)

## Prerequisites

This section assumes that you have already installed a Debian Linux operating system from an .iso file downloaded from the [Debian website](#) to a virtual hard disk. Multiple tools exist to create .vhd files; Hyper-V is only one example. For instructions using Hyper-V, see [Install the Hyper-V Role and Configure a Virtual Machine](#).

## Installation notes

- See also [General Linux Installation Notes](#) for more tips on preparing Linux for Azure.
- The newer VHDX format is not supported in Azure. You can convert the disk to VHD format using Hyper-V Manager or the **convert-vhd** cmdlet.
- When installing the Linux system, it is recommended that you use standard partitions rather than LVM (often the default for many installations). This will avoid LVM name conflicts with cloned VMs, particularly if an OS disk ever needs to be attached to another VM for troubleshooting. [LVM](#) or [RAID](#) may be used on data disks if preferred.
- Do not configure a swap partition on the OS disk. The Azure Linux agent can be configured to create a swap file on the temporary resource disk. More information can be found in the steps below.
- All VHDs on Azure must have a virtual size aligned to 1MB. When converting from a raw disk to VHD, you must ensure that the raw disk size is a multiple of 1MB before conversion. For more information, see [Linux Installation Notes](#).

## Use Azure-Manage to create Debian VHDs

There are tools available for generating Debian VHDs for Azure, such as the `azure-manage` scripts from [Credativ](#). This is the recommended approach versus creating an image from scratch. For example, to create a Debian 8 VHD run the following commands to download the `azure-manage` utility (and dependencies) and run the `azure_build_image` script:

```
sudo apt-get update
sudo apt-get install git qemu-utils mbr kpartx debootstrap

sudo apt-get install python3-pip python3-dateutil python3-cryptography
sudo pip3 install azure-storage azure-servicemanagement-legacy azure-common pytest pyyaml
git clone https://github.com/credativ/azure-manage.git
cd azure-manage
sudo pip3 install .

sudo azure_build_image --option release=jessie --option image_size_gb=30 --option image_prefix=debian-jessie-azure section
```

## Manually prepare a Debian VHD

1. In Hyper-V Manager, select the virtual machine.
2. Click **Connect** to open a console window for the virtual machine.
3. If you installed the OS using an ISO, then comment out any line relating to "`deb cdrom`" in `/etc/apt/source.list`.

4. Edit the `/etc/default/grub` file and modify the **GRUB\_CMDLINE\_LINUX** parameter as follows to include additional kernel parameters for Azure.

```
GRUB_CMDLINE_LINUX="console=tty0 console=ttyS0,115200n8 earlyprintk=ttyS0,115200"
```

5. Rebuild the grub and run:

```
sudo update-grub
```

6. Add Debian's Azure repositories to `/etc/apt/sources.list` for either Debian 8 or 9:

#### Debian 8.x "Jessie"

```
deb http://debian-archive.trafficmanager.net/debian jessie main
deb-src http://debian-archive.trafficmanager.net/debian jessie main
deb http://debian-archive.trafficmanager.net/debian-security jessie/updates main
deb-src http://debian-archive.trafficmanager.net/debian-security jessie/updates
deb http://debian-archive.trafficmanager.net/debian jessie-updates main
deb-src http://debian-archive.trafficmanager.net/debian jessie-updates main
deb http://debian-archive.trafficmanager.net/debian jessie-backports main
deb-src http://debian-archive.trafficmanager.net/debian jessie-backports main
```

#### Debian 9.x "Stretch"

```
deb http://debian-archive.trafficmanager.net/debian stretch main
deb-src http://debian-archive.trafficmanager.net/debian stretch main
deb http://debian-archive.trafficmanager.net/debian-security stretch/updates main
deb-src http://debian-archive.trafficmanager.net/debian-security stretch/updates main
deb http://debian-archive.trafficmanager.net/debian stretch-updates main
deb-src http://debian-archive.trafficmanager.net/debian stretch-updates main
deb http://debian-archive.trafficmanager.net/debian stretch-backports main
deb-src http://debian-archive.trafficmanager.net/debian stretch-backports main
```

7. Install the Azure Linux Agent:

```
sudo apt-get update
sudo apt-get install waagent
```

8. For Debian 9+, it is recommended to use the new Debian Cloud kernel for use with VMs in Azure. To install this new kernel, first create a file called `/etc/apt/preferences.d/linux.pref` with the following contents:

```
Package: linux-* initramfs-tools
Pin: release n=stretch-backports
Pin-Priority: 500
```

Then run `"sudo apt-get install linux-image-cloud-amd64"` to install the new Debian Cloud kernel.

9. Deprovision the virtual machine and prepare it for provisioning on Azure and run:

```
sudo waagent -force -deprovision
export HISTSIZE=0
logout
```

10. Click **Action** -> Shut Down in Hyper-V Manager. Your Linux VHD is now ready to be uploaded to Azure.

## Next steps

You're now ready to use your Debian virtual hard disk to create new virtual machines in Azure. If this is the first time that you're uploading the .vhdx file to Azure, see [Create a Linux VM from a custom disk](#).

# Prepare a SLES or openSUSE virtual machine for Azure

1/8/2020 • 6 minutes to read • [Edit Online](#)

This article assumes that you have already installed a SUSE or openSUSE Linux operating system to a virtual hard disk. Multiple tools exist to create .vhdx files, for example a virtualization solution such as Hyper-V. For instructions, see [Install the Hyper-V Role and Configure a Virtual Machine](#).

## SLES / openSUSE installation notes

- Please see also [General Linux Installation Notes](#) for more tips on preparing Linux for Azure.
- The VHDX format is not supported in Azure, only **fixed VHD**. You can convert the disk to VHD format using Hyper-V Manager or the convert-vhd cmdlet.
- When installing the Linux system it is recommended that you use standard partitions rather than LVM (often the default for many installations). This will avoid LVM name conflicts with cloned VMs, particularly if an OS disk ever needs to be attached to another VM for troubleshooting. [LVM](#) or [RAID](#) may be used on data disks if preferred.
- Do not configure a swap partition on the OS disk. The Linux agent can be configured to create a swap file on the temporary resource disk. More information about this can be found in the steps below.
- All VHDs on Azure must have a virtual size aligned to 1MB. When converting from a raw disk to VHD you must ensure that the raw disk size is a multiple of 1MB before conversion. See [Linux Installation Notes](#) for more information.

## Use SUSE Studio

[SUSE Studio](#) can easily create and manage your SLES and openSUSE images for Azure and Hyper-V. This is the recommended approach for customizing your own SLES and openSUSE images.

As an alternative to building your own VHD, SUSE also publishes BYOS (Bring Your Own Subscription) images for SLES at [VMDepot](#).

## Prepare SUSE Linux Enterprise Server 11 SP4

1. In the center pane of Hyper-V Manager, select the virtual machine.
2. Click **Connect** to open the window for the virtual machine.
3. Register your SUSE Linux Enterprise system to allow it to download updates and install packages.
4. Update the system with the latest patches:

```
sudo zypper update
```

5. Install the Azure Linux Agent from the SLES repository:

```
sudo zypper install python-azure-agent
```

6. Check if waagent is set to "on" in chkconfig, and if not, enable it for autostart:

```
sudo chkconfig waagent on
```

7. Check if waagent service is running, and if not, start it:

```
sudo service waagent start
```

8. Modify the kernel boot line in your grub configuration to include additional kernel parameters for Azure. To do this open "/boot/grub/menu.lst" in a text editor and ensure that the default kernel includes the following parameters:

```
console=ttyS0 earlyprintk=ttyS0 rootdelay=300
```

This will ensure all console messages are sent to the first serial port, which can assist Azure support with debugging issues.

9. Confirm that /boot/grub/menu.lst and /etc/fstab both reference the disk using its UUID (by-uuid) instead of the disk ID (by-id).

Get disk UUID

```
ls /dev/disk/by-uuid/
```

If /dev/disk/by-id/ is used, update both /boot/grub/menu.lst and /etc/fstab with the proper by-uuid value

Before change

```
root=/dev/disk/by-id/SCSI-xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx-part1
```

After change

```
root=/dev/disk/by-uuid/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

10. Modify udev rules to avoid generating static rules for the Ethernet interface(s). These rules can cause problems when cloning a virtual machine in Microsoft Azure or Hyper-V:

```
sudo ln -s /dev/null /etc/udev/rules.d/75-persistent-net-generator.rules
sudo rm -f /etc/udev/rules.d/70-persistent-net.rules
```

11. It is recommended to edit the file "/etc/sysconfig/network/dhcp" and change the `DHCLIENT_SET_HOSTNAME` parameter to the following:

`DHCLIENT_SET_HOSTNAME="no"`

12. In "/etc/sudoers", comment out or remove the following lines if they exist:

```
Defaults targetpw # ask for the password of the target user i.e. root
ALL ALL=(ALL) ALL # WARNING! Only use this together with 'Defaults targetpw'!
```

13. Ensure that the SSH server is installed and configured to start at boot time. This is usually the default.

14. Do not create swap space on the OS disk.

The Azure Linux Agent can automatically configure swap space using the local resource disk that is attached to the VM after provisioning on Azure. Note that the local resource disk is a *temporary* disk, and might be emptied when the VM is deprovisioned. After installing the Azure Linux Agent (see previous step), modify the following parameters in /etc/waagent.conf appropriately:

```
ResourceDisk.Format=y ResourceDisk.Filesystem=ext4 ResourceDisk.MountPoint=/mnt/resource
ResourceDisk.EnableSwap=y ResourceDisk.SwapSizeMB=2048 ## NOTE: set this to whatever you need it to be.
```

- Run the following commands to deprovision the virtual machine and prepare it for provisioning on Azure:

```
sudo waagent -force -deprovision
export HISTSIZE=0
logout
```

- Click **Action -> Shut Down** in Hyper-V Manager. Your Linux VHD is now ready to be uploaded to Azure.

## Prepare openSUSE 13.1+

- In the center pane of Hyper-V Manager, select the virtual machine.
- Click **Connect** to open the window for the virtual machine.
- On the shell, run the command '`zypper lr`'. If this command returns output similar to the following, then the repositories are configured as expected--no adjustments are necessary (note that version numbers may vary):

| # | Alias                 | Name                  | Enabled | Refresh |
|---|-----------------------|-----------------------|---------|---------|
| 1 | Cloud:Tools_13.1      | Cloud:Tools_13.1      | Yes     | Yes     |
| 2 | openSUSE_13.1_OSS     | openSUSE_13.1_OSS     | Yes     | Yes     |
| 3 | openSUSE_13.1_Updates | openSUSE_13.1_Updates | Yes     | Yes     |

If the command returns "No repositories defined..." then use the following commands to add these repos:

```
sudo zypper ar -f http://download.opensuse.org/repositories/Cloud:Tools/openSUSE_13.1
Cloud:Tools_13.1
sudo zypper ar -f https://download.opensuse.org/distribution/13.1/repo/oss openSUSE_13.1_OSS
sudo zypper ar -f http://download.opensuse.org/update/13.1 openSUSE_13.1_Updates
```

You can then verify the repositories have been added by running the command '`zypper lr`' again. In case one of the relevant update repositories is not enabled, enable it with following command:

```
sudo zypper mr -e [NUMBER OF REPOSITORY]
```

- Update the kernel to the latest available version:

```
sudo zypper up kernel-default
```

Or to update the system with all the latest patches:

```
sudo zypper update
```

5. Install the Azure Linux Agent.

```
sudo zypper install WALinuxAgent
```

6. Modify the kernel boot line in your grub configuration to include additional kernel parameters for Azure. To do this, open "/boot/grub/menu.lst" in a text editor and ensure that the default kernel includes the following parameters:

```
console=ttyS0 earlyprintk=ttyS0 rootdelay=300
```

This will ensure all console messages are sent to the first serial port, which can assist Azure support with debugging issues. In addition, remove the following parameters from the kernel boot line if they exist:

```
libata.atapi_enabled=0 reserve=0x1f0,0x8
```

7. It is recommended to edit the file "/etc/sysconfig/network/dhcp" and change the `DHCLIENT_SET_HOSTNAME` parameter to the following:

```
DHCLIENT_SET_HOSTNAME="no"
```

8. **Important:** In "/etc/sudoers", comment out or remove the following lines if they exist:

```
Defaults targetpw # ask for the password of the target user i.e. root
ALL ALL=(ALL) ALL # WARNING! Only use this together with 'Defaults targetpw'!
```

9. Ensure that the SSH server is installed and configured to start at boot time. This is usually the default.

10. Do not create swap space on the OS disk.

The Azure Linux Agent can automatically configure swap space using the local resource disk that is attached to the VM after provisioning on Azure. Note that the local resource disk is a *temporary* disk, and might be emptied when the VM is deprovisioned. After installing the Azure Linux Agent (see previous step), modify the following parameters in /etc/waagent.conf appropriately:

```
ResourceDisk.Format=y ResourceDisk.Filesystem=ext4 ResourceDisk.MountPoint=/mnt/resource
ResourceDisk.EnableSwap=y ResourceDisk.SwapSizeMB=2048 ## NOTE: set this to whatever you need it
to be.
```

11. Run the following commands to deprovision the virtual machine and prepare it for provisioning on Azure:

```
sudo waagent -force -deprovision
export HISTSIZE=0
logout
```

12. Ensure the Azure Linux Agent runs at startup:

```
sudo systemctl enable waagent.service
```

13. Click **Action -> Shut Down** in Hyper-V Manager. Your Linux VHD is now ready to be uploaded to Azure.

## Next steps

You're now ready to use your SUSE Linux virtual hard disk to create new virtual machines in Azure. If this is the first time that you're uploading the .vhd file to Azure, see [Create a Linux VM from a custom disk](#).

# Prepare an Oracle Linux virtual machine for Azure

1/8/2020 • 7 minutes to read • [Edit Online](#)

This article assumes that you have already installed an Oracle Linux operating system to a virtual hard disk. Multiple tools exist to create .vhdx files, for example a virtualization solution such as Hyper-V. For instructions, see [Install the Hyper-V Role and Configure a Virtual Machine](#).

## Oracle Linux installation notes

- Please see also [General Linux Installation Notes](#) for more tips on preparing Linux for Azure.
- Hyper-V and Azure support Oracle Linux with either the Unbreakable Enterprise Kernel (UEK) or the Red Hat Compatible Kernel.
- Oracle's UEK2 is not supported on Hyper-V and Azure as it does not include the required drivers.
- The VHDX format is not supported in Azure, only **fixed VHD**. You can convert the disk to VHD format using Hyper-V Manager or the convert-vhd cmdlet.
- When installing the Linux system it is recommended that you use standard partitions rather than LVM (often the default for many installations). This will avoid LVM name conflicts with cloned VMs, particularly if an OS disk ever needs to be attached to another VM for troubleshooting. [LVM](#) or [RAID](#) may be used on data disks if preferred.
- Linux kernel versions earlier than 2.6.37 don't support NUMA on Hyper-V with larger VM sizes. This issue primarily impacts older distributions using the upstream Red Hat 2.6.32 kernel, and was fixed in Oracle Linux 6.6 and later
- Do not configure a swap partition on the OS disk. The Linux agent can be configured to create a swap file on the temporary resource disk. More information about this can be found in the steps below.
- All VHDs on Azure must have a virtual size aligned to 1MB. When converting from a raw disk to VHD you must ensure that the raw disk size is a multiple of 1MB before conversion. See [Linux Installation Notes](#) for more information.
- Make sure that the `Addons` repository is enabled. Edit the file `/etc/yum.repos.d/public-yum-ol6.repo` (Oracle Linux 6) or `/etc/yum.repos.d/public-yum-ol7.repo` (Oracle Linux 7), and change the line `enabled=0` to `enabled=1` under `[ol6_addons]` or `[ol7_addons]` in this file.

## Oracle Linux 6.4 and later

You must complete specific configuration steps in the operating system for the virtual machine to run in Azure.

1. In the center pane of Hyper-V Manager, select the virtual machine.
2. Click **Connect** to open the window for the virtual machine.
3. Uninstall NetworkManager by running the following command:

```
sudo rpm -e --nodeps NetworkManager
```

**Note:** If the package is not already installed, this command will fail with an error message. This is expected.

4. Create a file named **network** in the `/etc/sysconfig/` directory that contains the following text:

```
NETWORKING=yes
HOSTNAME=localhost.localdomain
```

5. Create a file named **ifcfg-eth0** in the `/etc/sysconfig/network-scripts/` directory that contains the following text:

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
TYPE=Ethernet
USERCTL=no
PEERDNS=yes
IPV6INIT=no
```

6. Modify udev rules to avoid generating static rules for the Ethernet interface(s). These rules can cause problems when cloning a virtual machine in Microsoft Azure or Hyper-V:

```
sudo ln -s /dev/null /etc/udev/rules.d/75-persistent-net-generator.rules
sudo rm -f /etc/udev/rules.d/70-persistent-net.rules
```

7. Ensure the network service will start at boot time by running the following command:

```
chkconfig network on
```

8. Install python-pyasn1 by running the following command:

```
sudo yum install python-pyasn1
```

9. Modify the kernel boot line in your grub configuration to include additional kernel parameters for Azure. To do this open `/boot/grub/menu.lst` in a text editor and ensure that the kernel includes the following parameters:

```
console=ttyS0 earlyprintk=ttyS0 rootdelay=300
```

This will ensure all console messages are sent to the first serial port, which can assist Azure support with debugging issues.

In addition to the above, it is recommended to *remove* the following parameters:

```
rhgb quiet crashkernel=auto
```

Graphical and quiet boot are not useful in a cloud environment where we want all the logs to be sent to the serial port.

The `crashkernel` option may be left configured if desired, but note that this parameter will reduce the amount of available memory in the VM by 128MB or more, which may be problematic on the smaller VM sizes.

10. Ensure that the SSH server is installed and configured to start at boot time. This is usually the default.
11. Install the Azure Linux Agent by running the following command. The latest version is 2.0.15.

```
sudo yum install WALinuxAgent
```

Note that installing the WALinuxAgent package will remove the NetworkManager and NetworkManager-gnome packages if they were not already removed as described in step 2.

## 12. Do not create swap space on the OS disk.

The Azure Linux Agent can automatically configure swap space using the local resource disk that is attached to the VM after provisioning on Azure. Note that the local resource disk is a *temporary* disk, and might be emptied when the VM is deprovisioned. After installing the Azure Linux Agent (see previous step), modify the following parameters in /etc/waagent.conf appropriately:

```
ResourceDisk.Format=y
ResourceDisk.Filesystem=ext4
ResourceDisk.MountPoint=/mnt/resource
ResourceDisk.EnableSwap=y
ResourceDisk.SwapSizeMB=2048 ## NOTE: set this to whatever you need it to be.
```

## 13. Run the following commands to deprovision the virtual machine and prepare it for provisioning on Azure:

```
sudo waagent -force -deprovision
export HISTSIZE=0
logout
```

## 14. Click **Action -> Shut Down** in Hyper-V Manager. Your Linux VHD is now ready to be uploaded to Azure.

# Oracle Linux 7.0 and later

## Changes in Oracle Linux 7

Preparing an Oracle Linux 7 virtual machine for Azure is very similar to Oracle Linux 6, however there are several important differences worth noting:

- Azure supports Oracle Linux with either the Unbreakable Enterprise Kernel (UEK) or the Red Hat Compatible Kernel. Oracle Linux with UEK is recommended.
- The NetworkManager package no longer conflicts with the Azure Linux agent. This package is installed by default and we recommend that it is not removed.
- GRUB2 is now used as the default bootloader, so the procedure for editing kernel parameters has changed (see below).
- XFS is now the default file system. The ext4 file system can still be used if desired.

## Configuration steps

1. In Hyper-V Manager, select the virtual machine.

2. Click **Connect** to open a console window for the virtual machine.

3. Create a file named **network** in the `/etc/sysconfig/` directory that contains the following text:

```
NETWORKING=yes
HOSTNAME=localhost.localdomain
```

4. Create a file named **ifcfg-eth0** in the `/etc/sysconfig/network-scripts/` directory that contains the following text:

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
TYPE=Ethernet
USERCTL=no
PEERDNS=yes
IPV6INIT=no
```

5. Modify udev rules to avoid generating static rules for the Ethernet interface(s). These rules can cause problems when cloning a virtual machine in Microsoft Azure or Hyper-V:

```
sudo ln -s /dev/null /etc/udev/rules.d/75-persistent-net-generator.rules
```

6. Ensure the network service will start at boot time by running the following command:

```
sudo chkconfig network on
```

7. Install the python-pyasn1 package by running the following command:

```
sudo yum install python-pyasn1
```

8. Run the following command to clear the current yum metadata and install any updates:

```
sudo yum clean all
sudo yum -y update
```

9. Modify the kernel boot line in your grub configuration to include additional kernel parameters for Azure. To do this open "/etc/default/grub" in a text editor and edit the `GRUB_CMDLINE_LINUX` parameter, for example:

```
GRUB_CMDLINE_LINUX="rootdelay=300 console=ttyS0 earlyprintk=ttyS0 net.ifnames=0"
```

This will also ensure all console messages are sent to the first serial port, which can assist Azure support with debugging issues. It also turns off the naming conventions for NICs in Oracle Linux 7 with the Unbreakable Enterprise Kernel. In addition to the above, it is recommended to *remove* the following parameters:

```
rhgb quiet crashkernel=auto
```

Graphical and quiet boot are not useful in a cloud environment where we want all the logs to be sent to the serial port.

The `crashkernel` option may be left configured if desired, but note that this parameter will reduce the amount of available memory in the VM by 128MB or more, which may be problematic on the smaller VM sizes.

10. Once you are done editing "/etc/default/grub" per above, run the following command to rebuild the grub configuration:

```
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

11. Ensure that the SSH server is installed and configured to start at boot time. This is usually the default.

12. Install the Azure Linux Agent by running the following command:

```
sudo yum install WALinuxAgent
sudo systemctl enable waagent
```

13. Do not create swap space on the OS disk.

The Azure Linux Agent can automatically configure swap space using the local resource disk that is attached to the VM after provisioning on Azure. Note that the local resource disk is a *temporary* disk, and might be emptied when the VM is deprovisioned. After installing the Azure Linux Agent (see the previous step), modify the following parameters in /etc/waagent.conf appropriately:

```
ResourceDisk.Format=y
ResourceDisk.Filesystem=ext4
ResourceDisk.MountPoint=/mnt/resource
ResourceDisk.EnableSwap=y
ResourceDisk.SwapSizeMB=2048 ## NOTE: set this to whatever you need it to be.
```

14. Run the following commands to deprovision the virtual machine and prepare it for provisioning on Azure:

```
sudo waagent -force -deprovision
export HISTSIZE=0
logout
```

15. Click **Action -> Shut Down** in Hyper-V Manager. Your Linux VHD is now ready to be uploaded to Azure.

## Next steps

You're now ready to use your Oracle Linux .vhd to create new virtual machines in Azure. If this is the first time that you're uploading the .vhd file to Azure, see [Create a Linux VM from a custom disk](#).

# Create and Upload an OpenBSD disk image to Azure

1/20/2020 • 3 minutes to read • [Edit Online](#)

This article shows you how to create and upload a virtual hard disk (VHD) that contains the OpenBSD operating system. After you upload it, you can use it as your own image to create a virtual machine (VM) in Azure through Azure CLI.

## Prerequisites

This article assumes that you have the following items:

- **An Azure subscription** - If you don't have an account, you can create one in just a couple of minutes. If you have an MSDN subscription, see [Monthly Azure credit for Visual Studio subscribers](#). Otherwise, learn how to [create a free trial account](#).
- **Azure CLI** - Make sure you have the latest [Azure CLI](#) installed and logged in to your Azure account with [az login](#).
- **OpenBSD operating system installed in a .vhd file** - A supported OpenBSD operating system ([6.6 version AMD64](#)) must be installed to a virtual hard disk. Multiple tools exist to create .vhd files. For example, you can use a virtualization solution such as Hyper-V to create the .vhd file and install the operating system. For instructions about how to install and use Hyper-V, see [Install Hyper-V and create a virtual machine](#).

## Prepare OpenBSD image for Azure

On the VM where you installed the OpenBSD operating system 6.1, which added Hyper-V support, complete the following procedures:

1. If DHCP is not enabled during installation, enable the service as follows:

```
echo dhcp > /etc/hostname.hvn0
```

2. Set up a serial console as follows:

```
echo "stty com0 115200" >> /etc/boot.conf
echo "set tty com0" >> /etc/boot.conf
```

3. Configure Package installation as follows:

```
echo "https://ftp.openbsd.org/pub/OpenBSD" > /etc/installurl
```

4. By default, the `root` user is disabled on virtual machines in Azure. Users can run commands with elevated privileges by using the `doas` command on OpenBSD VM. Doas is enabled by default. For more information, see [doas.conf](#).

5. Install and configure prerequisites for the Azure Agent as follows:

```
pkg_add py-setuptools openssl git
ln -sf /usr/local/bin/python2.7 /usr/local/bin/python
ln -sf /usr/local/bin/python2.7-2to3 /usr/local/bin/2to3
ln -sf /usr/local/bin/python2.7-config /usr/local/bin/python-config
ln -sf /usr/local/bin/pydoc2.7 /usr/local/bin/pydoc
```

6. The latest release of the Azure agent can always be found on [GitHub](https://github.com/Azure/WALinuxAgent). Install the agent as follows:

```
git clone https://github.com/Azure/WALinuxAgent
cd WALinuxAgent
python setup.py install
waagent -register-service
```

#### IMPORTANT

After you install Azure Agent, it's a good idea to verify that it's running as follows:

```
ps auxw | grep waagent
root 79309 0.0 1.5 9184 15356 p1 S 4:11PM 0:00.46 python /usr/local/sbin/waagent -
daemon (python2.7)
cat /var/log/waagent.log
```

7. Deprovision the system to clean it and make it suitable for reprovisioning. The following command also deletes the last provisioned user account and the associated data:

```
waagent -deprovision+user -force
```

Now you can shut down your VM.

## Prepare the VHD

The VHDX format is not supported in Azure, only **fixed VHD**. You can convert the disk to fixed VHD format using Hyper-V Manager or the Powershell [convert-vhd](#) cmdlet. An example is as following.

```
Convert-VHD OpenBSD61.vhdx OpenBSD61.vhd -VHDTType Fixed
```

## Create storage resources and upload

First, create a resource group with [az group create](#). The following example creates a resource group named *myResourceGroup* in the *eastus* location:

```
az group create --name myResourceGroup --location eastus
```

To upload your VHD, create a storage account with [az storage account create](#). Storage account names must be unique, so provide your own name. The following example creates a storage account named *mystorageaccount*:

```
az storage account create --resource-group myResourceGroup \
--name mystorageaccount \
--location eastus \
--sku Premium_LRS
```

To control access to the storage account, obtain the storage key with [az storage account keys list](#) as follows:

```
STORAGE_KEY=$(az storage account keys list \
--resource-group myResourceGroup \
--account-name mystorageaccount \
--query "[?keyName=='key1'] | [0].value" -o tsv)
```

To logically separate the VHDs you upload, create a container within the storage account with [az storage container create](#):

```
az storage container create \
--name vhds \
--account-name mystorageaccount \
--account-key ${STORAGE_KEY}
```

Finally, upload your VHD with [az storage blob upload](#) as follows:

```
az storage blob upload \
--container-name vhds \
--file ./OpenBSD61.vhd \
--name OpenBSD61.vhd \
--account-name mystorageaccount \
--account-key ${STORAGE_KEY}
```

## Create VM from your VHD

You can create a VM with a [sample script](#) or directly with [az vm create](#). To specify the OpenBSD VHD you uploaded, use the `--image` parameter as follows:

```
az vm create \
--resource-group myResourceGroup \
--name myOpenBSD61 \
--image "https://mystorageaccount.blob.core.windows.net/vhds/OpenBSD61.vhd" \
--os-type linux \
--admin-username azureuser \
--ssh-key-value ~/.ssh/id_rsa.pub
```

Obtain the IP address for your OpenBSD VM with [az vm list-ip-addresses](#) as follows:

```
az vm list-ip-addresses --resource-group myResourceGroup --name myOpenBSD61
```

Now you can SSH to your OpenBSD VM as normal:

```
ssh azureuser@<ip address>
```

## Next steps

If you want to know more about Hyper-V support on OpenBSD6.1, read [OpenBSD 6.1](#) and [hyperv.4](#).

If you want to create a VM from managed disk, read [az disk](#).

# Introduction to FreeBSD on Azure

11/13/2019 • 3 minutes to read • [Edit Online](#)

This article provides an overview of running a FreeBSD virtual machine in Azure.

## Overview

FreeBSD for Microsoft Azure is an advanced computer operating system used to power modern servers, desktops, and embedded platforms.

Microsoft Corporation is making images of FreeBSD available on Azure with the [Azure VM Guest Agent](#) pre-configured. Currently, the following FreeBSD versions are offered as images by Microsoft:

- [FreeBSD 10.4 on the Azure Marketplace](#)
- [FreeBSD 11.2 on the Azure Marketplace](#)
- [FreeBSD 12.0 on the Azure Marketplace](#)

The agent is responsible for communication between the FreeBSD VM and the Azure fabric for operations such as provisioning the VM on first use (user name, password or SSH key, host name, etc.) and enabling functionality for selective VM extensions.

As for future versions of FreeBSD, the strategy is to stay current and make the latest releases available shortly after they are published by the FreeBSD release engineering team.

### Create a FreeBSD VM through Azure CLI on FreeBSD

First you need to install [Azure CLI](#) though following command on a FreeBSD machine.

```
curl -L https://aka.ms/InstallAzureCli | bash
```

If bash is not installed on your FreeBSD machine, run following command before the installation.

```
sudo pkg install bash
```

If python is not installed on your FreeBSD machine, run following commands before the installation.

```
sudo pkg install python35
cd /usr/local/bin
sudo rm /usr/local/bin/python
sudo ln -s /usr/local/bin/python3.5 /usr/local/bin/python
```

During the installation, you are asked

Modify profile to update your \$PATH and enable shell/tab completion now? (Y/n) . If you answer `y` and enter `/etc/rc.conf` as a path to an rc file to update , you may meet the problem `ERROR: [Errno 13] Permission denied` . To resolve this problem, you should grant the write right to current user against the file `etc/rc.conf` .

Now you can sign in to Azure and create your FreeBSD VM. Below is an example to create a FreeBSD 11.0 VM. You can also add the parameter `--public-ip-address-dns-name` with a globally unique DNS name for a newly created Public IP.

```
az login
az group create --name myResourceGroup --location eastus
az vm create --name myFreeBSD11 \
 --resource-group myResourceGroup \
 --image MicrosoftOSTC:FreeBSD:11.0:latest \
 --admin-username azureuser \
 --generate-ssh-keys
```

Then you can sign in to your FreeBSD VM through the ip address that printed in the output of above deployment.

```
ssh azureuser@xx.xx.xx.xx -i /etc/ssh/ssh_host_rsa_key
```

## VM extensions for FreeBSD

Following are supported VM extensions in FreeBSD.

### VMAccess

The [VMAccess](#) extension can:

- Reset the password of the original sudo user.
- Create a new sudo user with the password specified.
- Set the public host key with the key given.
- Reset the public host key provided during VM provisioning if the host key is not provided.
- Open the SSH port (22) and restore the sshd\_config if reset\_ssh is set to true.
- Remove the existing user.
- Check disks.
- Repair an added disk.

### CustomScript

The [CustomScript](#) extension can:

- If provided, download the customized scripts from Azure Storage or external public storage (for example, GitHub).
- Run the entry point script.
- Support inline commands.
- Convert Windows-style newline in shell and Python scripts automatically.
- Remove BOM in shell and Python scripts automatically.
- Protect sensitive data in CommandToExecute.

#### NOTE

FreeBSD VM only supports CustomScript version 1.x by now.

## Authentication: user names, passwords, and SSH keys

When you're creating a FreeBSD virtual machine by using the Azure portal, you must provide a user name, password, or SSH public key. User names for deploying a FreeBSD virtual machine on Azure must not match names of system accounts (UID < 100) already present in the virtual machine ("root", for example). Currently, only the RSA SSH key is supported. A multiline SSH key must begin with `---- BEGIN SSH2 PUBLIC KEY ----` and end with `---- END SSH2 PUBLIC KEY ----`.

## Obtaining superuser privileges

The user account that is specified during virtual machine instance deployment on Azure is a privileged account. The package of sudo was installed in the published FreeBSD image. After you're logged in through this user account, you can run commands as root by using the command syntax.

```
$ sudo <COMMAND>
```

You can optionally obtain a root shell by using `sudo -s`.

## Known issues

The [Azure VM Guest Agent](#) version 2.2.2 has a [known issue](#) that causes the provision failure for FreeBSD VM on Azure. The fix was captured by [Azure VM Guest Agent](#) version 2.2.3 and later releases.

## Next steps

- Go to [Azure Marketplace](#) to create a FreeBSD VM.

# How to create an image of a virtual machine or VHD

11/13/2019 • 4 minutes to read • [Edit Online](#)

To create multiple copies of a virtual machine (VM) for use in Azure, capture an image of the VM or of the OS VHD. To create an image for deployment, you'll need to remove personal account information. In the following steps, you deprovision an existing VM, deallocate it and create an image. You can use this image to create VMs across any resource group within your subscription.

To create a copy of your existing Linux VM for backup or debugging, or to upload a specialized Linux VHD from an on-premises VM, see [Upload and create a Linux VM from custom disk image](#).

You can use the **Azure VM Image Builder (Public Preview)** service to build your custom image, no need to learn any tools, or setup build pipelines, simply providing an image configuration, and the Image Builder will create the Image. For more information, see [Getting Started with Azure VM Image Builder](#).

You'll need the following items before creating an image:

- An Azure VM created in the Resource Manager deployment model that uses managed disks. If you haven't yet created a Linux VM, you can use the [portal](#), the [Azure CLI](#), or [Resource Manager templates](#). Configure the VM as needed. For example, [add data disks](#), apply updates, and install applications.
- The latest [Azure CLI](#) installed and be logged in to an Azure account with [az login](#).

## Prefer a tutorial instead?

For a simplified version of this article, and for testing, evaluating, or learning about VMs in Azure, see [Create a custom image of an Azure VM by using the CLI](#). Otherwise, keep reading here to get the full picture.

## Step 1: Deprovision the VM

First you'll deprovision the VM by using the Azure VM agent to delete machine-specific files and data. Use the `waagent` command with the `-deprovision+user` parameter on your source Linux VM. For more information, see the [Azure Linux Agent user guide](#).

1. Connect to your Linux VM with an SSH client.
2. In the SSH window, enter the following command:

```
sudo waagent -deprovision+user
```

### NOTE

Only run this command on a VM that you'll capture as an image. This command does not guarantee that the image is cleared of all sensitive information or is suitable for redistribution. The `+user` parameter also removes the last provisioned user account. To keep user account credentials in the VM, use only `-deprovision`.

3. Enter **y** to continue. You can add the `-force` parameter to avoid this confirmation step.
4. After the command completes, enter **exit** to close the SSH client. The VM will still be running at this point.

## Step 2: Create VM image

Use the Azure CLI to mark the VM as generalized and capture the image. In the following examples, replace example parameter names with your own values. Example parameter names include *myResourceGroup*, *myVnet*, and *myVM*.

1. Deallocate the VM that you deprovisioned with [az vm deallocate](#). The following example deallocates the VM named *myVM* in the resource group named *myResourceGroup*.

```
az vm deallocate \
--resource-group myResourceGroup \
--name myVM
```

Wait for the VM to completely deallocate before moving on. This may take a few minutes to complete. The VM is shut down during deallocation.

2. Mark the VM as generalized with [az vm generalize](#). The following example marks the VM named *myVM* in the resource group named *myResourceGroup* as generalized.

```
az vm generalize \
--resource-group myResourceGroup \
--name myVM
```

A VM that has been generalized can no longer be restarted.

3. Create an image of the VM resource with [az image create](#). The following example creates an image named *myImage* in the resource group named *myResourceGroup* using the VM resource named *myVM*.

```
az image create \
--resource-group myResourceGroup \
--name myImage --source myVM
```

#### NOTE

The image is created in the same resource group as your source VM. You can create VMs in any resource group within your subscription from this image. From a management perspective, you may wish to create a specific resource group for your VM resources and images.

If you would like to store your image in zone-resilient storage, you need to create it in a region that supports [availability zones](#) and include the `--zone-resilient true` parameter.

This command returns JSON that describes the VM image. Save this output for later reference.

## Step 3: Create a VM from the captured image

Create a VM by using the image you created with [az vm create](#). The following example creates a VM named *myVMDeployed* from the image named *myImage*.

```
az vm create \
--resource-group myResourceGroup \
--name myVMDeployed \
--image myImage \
--admin-username azureuser \
--ssh-key-value ~/.ssh/id_rsa.pub
```

### Creating the VM in another resource group

You can create VMs from an image in any resource group within your subscription. To create a VM in a different resource group than the image, specify the full resource ID to your image. Use [az image list](#) to view a list of images. The output is similar to the following example.

```
"id": "/subscriptions/guid/resourceGroups/MYRESOURCEGROUP/providers/Microsoft.Compute/images/myImage",
"location": "westus",
"name": "myImage",
```

The following example uses [az vm create](#) to create a VM in a resource group other than the source image, by specifying the image resource ID.

```
az vm create \
--resource-group myOtherResourceGroup \
--name myOtherVMDeployed \
--image "/subscriptions/guid/resourceGroups/MYRESOURCEGROUP/providers/Microsoft.Compute/images/myImage" \
--admin-username azureuser \
--ssh-key-value ~/.ssh/id_rsa.pub
```

## Step 4: Verify the deployment

SSH into the virtual machine you created to verify the deployment and start using the new VM. To connect via SSH, find the IP address or FQDN of your VM with [az vm show](#).

```
az vm show \
--resource-group myResourceGroup \
--name myVMDeployed \
--show-details
```

## Next steps

You can create multiple VMs from your source VM image. To make changes to your image:

- Create a VM from your image.
- Make any updates or configuration changes.
- Follow the steps again to deprovision, deallocate, generalize, and create an image.
- Use this new image for future deployments. You may delete the original image.

For more information on managing your VMs with the CLI, see [Azure CLI](#).

# How to use Packer to create Linux virtual machine images in Azure

11/13/2019 • 6 minutes to read • [Edit Online](#)

Each virtual machine (VM) in Azure is created from an image that defines the Linux distribution and OS version. Images can include pre-installed applications and configurations. The Azure Marketplace provides many first and third-party images for most common distributions and application environments, or you can create your own custom images tailored to your needs. This article details how to use the open source tool [Packer](#) to define and build custom images in Azure.

## NOTE

Azure now has a service, Azure Image Builder (preview), for defining and creating your own custom images. Azure Image Builder is built on Packer, so you can even use your existing Packer shell provisioner scripts with it. To get started with Azure Image Builder, see [Create a Linux VM with Azure Image Builder](#).

## Create Azure resource group

During the build process, Packer creates temporary Azure resources as it builds the source VM. To capture that source VM for use as an image, you must define a resource group. The output from the Packer build process is stored in this resource group.

Create a resource group with [az group create](#). The following example creates a resource group named *myResourceGroup* in the *eastus* location:

```
az group create -n myResourceGroup -l eastus
```

## Create Azure credentials

Packer authenticates with Azure using a service principal. An Azure service principal is a security identity that you can use with apps, services, and automation tools like Packer. You control and define the permissions as to what operations the service principal can perform in Azure.

Create a service principal with [az ad sp create-for-rbac](#) and output the credentials that Packer needs:

```
az ad sp create-for-rbac --query "{ client_id: appId, client_secret: password, tenant_id: tenant }"
```

An example of the output from the preceding commands is as follows:

```
{
 "client_id": "f5b6a5cf-fbdf-4a9f-b3b8-3c2cd00225a4",
 "client_secret": "0e760437-bf34-4aad-9f8d-870be799c55d",
 "tenant_id": "72f988bf-86f1-41af-91ab-2d7cd011db47"
}
```

To authenticate to Azure, you also need to obtain your Azure subscription ID with [az account show](#):

```
az account show --query "{ subscription_id: id }"
```

You use the output from these two commands in the next step.

## Define Packer template

To build images, you create a template as a JSON file. In the template, you define builders and provisioners that carry out the actual build process. Packer has a [provisioner for Azure](#) that allows you to define Azure resources, such as the service principal credentials created in the preceding step.

Create a file named *ubuntu.json* and paste the following content. Enter your own values for the following:

| PARAMETER                                | WHERE TO OBTAIN                                                                   |
|------------------------------------------|-----------------------------------------------------------------------------------|
| <i>client_id</i>                         | First line of output from <code>az ad sp</code> create command - <i>appId</i>     |
| <i>client_secret</i>                     | Second line of output from <code>az ad sp</code> create command - <i>password</i> |
| <i>tenant_id</i>                         | Third line of output from <code>az ad sp</code> create command - <i>tenant</i>    |
| <i>subscription_id</i>                   | Output from <code>az account show</code> command                                  |
| <i>managed_image_resource_group_name</i> | Name of resource group you created in the first step                              |
| <i>managed_image_name</i>                | Name for the managed disk image that is created                                   |

```
{
 "builders": [
 {
 "type": "azure-arm",
 "client_id": "f5b6a5cf-fbdf-4a9f-b3b8-3c2cd00225a4",
 "client_secret": "0e760437-bf34-4aad-9f8d-870be799c55d",
 "tenant_id": "72f988bf-86f1-41af-91ab-2d7cd011db47",
 "subscription_id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx",
 "managed_image_resource_group_name": "myResourceGroup",
 "managed_image_name": "myPackerImage",
 "os_type": "Linux",
 "image_publisher": "Canonical",
 "image_offer": "UbuntuServer",
 "image_sku": "16.04-LTS",
 "azure_tags": {
 "dept": "Engineering",
 "task": "Image deployment"
 },
 "location": "East US",
 "vm_size": "Standard_DS2_v2"
 }
],
 "provisioners": [
 {
 "execute_command": "chmod +x {{ .Path }}; {{ .Vars }} sudo -E sh '{{ .Path }}'",

 "inline": [
 "apt-get update",
 "apt-get upgrade -y",
 "apt-get -y install nginx",

 "/usr/sbin/waagent -force -deprovision+user && export HISTSIZE=0 && sync"
],
 "inline_shebang": "/bin/sh -x",
 "type": "shell"
 }
]
}
```

This template builds an Ubuntu 16.04 LTS image, installs NGINX, then deprovisions the VM.

#### NOTE

If you expand on this template to provision user credentials, adjust the provisioner command that deprovisions the Azure agent to read `-deprovision` rather than `deprovision+user`. The `+user` flag removes all user accounts from the source VM.

## Build Packer image

If you don't already have Packer installed on your local machine, [follow the Packer installation instructions](#).

Build the image by specifying your Packer template file as follows:

```
./packer build ubuntu.json
```

An example of the output from the preceding commands is as follows:

```

azure-arm output will be in this color.

==> azure-arm: Running builder ...
 azure-arm: Creating Azure Resource Manager (ARM) client ...
==> azure-arm: Creating resource group ...
==> azure-arm: -> ResourceGroupName : 'packer-Resource-Group-swtxmqm7ly'
==> azure-arm: -> Location : 'East US'
==> azure-arm: -> Tags :
==> azure-arm: ->> dept : Engineering
==> azure-arm: ->> task : Image deployment
==> azure-arm: Validating deployment template ...
==> azure-arm: -> ResourceGroupName : 'packer-Resource-Group-swtxmqm7ly'
==> azure-arm: -> DeploymentName : 'pkrdpswtxmqm7ly'
==> azure-arm: Deploying deployment template ...
==> azure-arm: -> ResourceGroupName : 'packer-Resource-Group-swtxmqm7ly'
==> azure-arm: -> DeploymentName : 'pkrdpswtxmqm7ly'
==> azure-arm: Getting the VM's IP address ...
==> azure-arm: -> ResourceGroupName : 'packer-Resource-Group-swtxmqm7ly'
==> azure-arm: -> PublicIPAddressName : 'packerPublicIP'
==> azure-arm: -> NicName : 'packerNic'
==> azure-arm: -> Network Connection : 'PublicEndpoint'
==> azure-arm: -> IP Address : '40.76.218.147'
==> azure-arm: Waiting for SSH to become available...
==> azure-arm: Connected to SSH!
==> azure-arm: Provisioning with shell script: /var/folders/h1/ymh5bdx15wgdn5hvgj1wc0zh0000gn/T/packer-shell1868574263
 azure-arm: WARNING! The waagent service will be stopped.
 azure-arm: WARNING! Cached DHCP leases will be deleted.
 azure-arm: WARNING! root password will be disabled. You will not be able to login as root.
 azure-arm: WARNING! /etc/resolvconf/resolv.conf.d/tail and /etc/resolvconf/resolv.conf.d/original will be deleted.
 azure-arm: WARNING! packer account and entire home directory will be deleted.
==> azure-arm: Querying the machine's properties ...
==> azure-arm: -> ResourceGroupName : 'packer-Resource-Group-swtxmqm7ly'
==> azure-arm: -> ComputeName : 'pkrvmswtxmqm7ly'
==> azure-arm: -> Managed OS Disk : '/subscriptions/guid/resourceGroups/packer-Resource-Group-swtxmqm7ly/providers/Microsoft.Compute/disks/osdisk'
==> azure-arm: Powering off machine ...
==> azure-arm: -> ResourceGroupName : 'packer-Resource-Group-swtxmqm7ly'
==> azure-arm: -> ComputeName : 'pkrvmswtxmqm7ly'
==> azure-arm: Capturing image ...
==> azure-arm: -> Compute ResourceGroupName : 'packer-Resource-Group-swtxmqm7ly'
==> azure-arm: -> Compute Name : 'pkrvmswtxmqm7ly'
==> azure-arm: -> Compute Location : 'East US'
==> azure-arm: -> Image ResourceGroupName : 'myResourceGroup'
==> azure-arm: -> Image Name : 'myPackerImage'
==> azure-arm: -> Image Location : 'eastus'
==> azure-arm: Deleting resource group ...
==> azure-arm: -> ResourceGroupName : 'packer-Resource-Group-swtxmqm7ly'
==> azure-arm: Deleting the temporary OS disk ...
==> azure-arm: -> OS Disk : skipping, managed disk was used...
Build 'azure-arm' finished.

==> Builds finished. The artifacts of successful builds are:
--> azure-arm: Azure.ResourceManagement.VMImage:

ManagedImageResourceGroupName: myResourceGroup
ManagedImageName: myPackerImage
ManagedImageLocation: eastus

```

It takes a few minutes for Packer to build the VM, run the provisioners, and clean up the deployment.

## Create VM from Azure Image

You can now create a VM from your Image with [az vm create](#). Specify the Image you created with the `--image`

parameter. The following example creates a VM named *myVM* from *myPackerImage* and generates SSH keys if they do not already exist:

```
az vm create \
 --resource-group myResourceGroup \
 --name myVM \
 --image myPackerImage \
 --admin-username azureuser \
 --generate-ssh-keys
```

If you wish to create VMs in a different resource group or region than your Packer image, specify the image ID rather than image name. You can obtain the image ID with [az image show](#).

It takes a few minutes to create the VM. Once the VM has been created, take note of the `publicIpAddress` displayed by the Azure CLI. This address is used to access the NGINX site via a web browser.

To allow web traffic to reach your VM, open port 80 from the Internet with [az vm open-port](#):

```
az vm open-port \
 --resource-group myResourceGroup \
 --name myVM \
 --port 80
```

## Test VM and NGINX

Now you can open a web browser and enter `http://publicIpAddress` in the address bar. Provide your own public IP address from the VM create process. The default NGINX page is displayed as in the following example:



## Next steps

You can also use existing Packer provisioner scripts with [Azure Image Builder](#).

# Red Hat Enterprise Linux images in Azure

11/13/2019 • 7 minutes to read • [Edit Online](#)

This article describes available Red Hat Enterprise Linux (RHEL) images in the Azure Marketplace along with policies around their naming and retention.

Information on Red Hat support policies for all versions of RHEL can be found on the [Red Hat Enterprise Linux Life Cycle](#) page.

## IMPORTANT

RHEL images currently available in the Azure marketplace support either Bring-Your-Own-Subscription (BYOS) or Pay-As-You-Go (PAYG) licensing models. The [Azure Hybrid Use Benefit](#) and dynamic switching between BYOS and PAYG is not supported. Switching licensing mode requires redeploying the VM from the corresponding image.

## NOTE

For any issue related to RHEL images in the Azure marketplace gallery please file a support ticket with Microsoft.

## Images available in the UI

When you search for "Red Hat" in the Marketplace or when you create a resource in Azure portal UI, you'll see a subset of available RHEL images and related Red Hat products. You can always obtain the full set of available VM images using the Azure CLI/PowerShell/API.

To see the full set of available Red Hat images in Azure, run the following command

```
az vm image list --publisher RedHat --all
```

## Naming convention

VM images in Azure are organized by Publisher, Offer, SKU, and Version. The combination of Publisher:Offer:SKU:Version is the image URN and uniquely identifies the image to be used.

For example, `RedHat:RHEL:7-RAW:7.6.2018103108` refers to a RHEL 7.6 raw-partitioned image built on October 31, 2018.

A sample of how to create a RHEL 7.6 VM is shown below.

```
az vm create --name RhelVM --resource-group TestRG --image RedHat:RHEL:7-RAW:7.6.2018103108 --no-wait
```

## The "latest" moniker

Azure REST API allows use of moniker "latest" for version instead of the specific version. Using "latest" will provision the latest available image for the given Publisher, Offer, and SKU.

For example, `RedHat:RHEL:7-RAW:latest` refers to the latest RHEL 7 family raw-partitioned image available.

```
az vm create --name RhelVM --resource-group TestRG --image RedHat:RHEL:7-RAW:latest --no-wait
```

#### NOTE

In general, the comparison of versions to determine the latest follows the rules of the [CompareTo method](#).

### Current naming convention

All currently published RHEL images use the Pay-As-You-Go model and are connected to [Red Hat Update Infrastructure \(RHUI\) in Azure](#). A new naming convention has been adopted for RHEL 7 family images in which the disk partitioning scheme (raw, LVM) is specified in the SKU instead of the version. The RHEL image version will contain either 7-RAW or 7-LVM. The RHEL 6 family naming hasn't been changed at this time.

There will be 2 types of RHEL 7 image SKUs in this naming convention: SKUs that list the minor version, and SKUs that don't. If you want to use a 7-RAW or 7-LVM SKU, you can specify the RHEL minor version you want to deploy in the version. If you choose the "latest" version, you will be provisioned the latest minor release of RHEL.

#### NOTE

In the RHEL for SAP set of images, the RHEL version remains fixed. As such, their naming convention includes a particular version in the SKU.

#### NOTE

RHEL 6 set of images were not moved to the new naming convention.

### Extended Update Support (EUS)

As of April 2019, RHEL images are available that are attached to the Extended Update Support (EUS) repositories by default. More details on RHEL EUS are available in [Red Hat's documentation](#).

Instructions on how to switch your VM to EUS and more details about EUS support end-of-life dates are available [here](#).

#### NOTE

EUS is not supported on RHEL Extras. This means that if you are installing a package that is usually available from the RHEL Extras channel, you will not be able to do so while on EUS. The Red Hat Extras Product Life Cycle is detailed [here](#).

#### For customers that want to use EUS images:

Customers that want to use images that are attached to EUS repositories should use the RHEL image that contains a RHEL minor version number in the SKU. These images will be raw-partitioned (i.e. not LVM).

For example, you may see the following 2 RHEL 7.4 images available:

```
RedHat:RHEL:7-RAW:7.4.2018010506
RedHat:RHEL:7.4:7.4.2019041718
```

In this case, `RedHat:RHEL:7.4:7.4.2019041718` will be attached to EUS repositories by default, and `RedHat:RHEL:7-RAW:7.4.2018010506` will be attached to non-EUS repositories by default.

#### For customers that don't want to use EUS images:

If you don't want to use an image that is connected to EUS by default, deploy using an image that does not contain a minor version number in the SKU.

#### RHEL images with EUS

The following table will apply for RHEL images that contain a minor version in the SKU.

##### NOTE

At the time of writing, only RHEL 7.4 and later minor versions have EUS support. EUS is no longer supported for RHEL <= 7.3.

More details about RHEL EUS availability can be found [here](#).

| MINOR VERSION | EUS IMAGE EXAMPLE              | EUS STATUS                                                   |
|---------------|--------------------------------|--------------------------------------------------------------|
| RHEL 7.4      | RedHat:RHEL:7.4:7.4.2019041718 | Images published April 2019 and later will be EUS by default |
| RHEL 7.5      | RedHat:RHEL:7.5:7.5.2019060305 | Images published June 2019 and later will be EUS by default  |
| RHEL 7.6      | RedHat:RHEL:7.6:7.6.2019052206 | Images published May 2019 and later will be EUS by default   |
| RHEL 8.0      | N/A                            | No EUS available from Red Hat                                |

## List of RHEL images available

The following offers are SKUs are currently available for general use:

| OFFER | SKU      | PARTITIONING | PROVISIONING | NOTES                                                                      |
|-------|----------|--------------|--------------|----------------------------------------------------------------------------|
| RHEL  | 7-RAW    | RAW          | Linux Agent  | RHEL 7.x family of images.<br>Not attached to EUS repositories by default. |
|       | 7-LVM    | LVM          | Linux Agent  | RHEL 7.x family of images.<br>Not attached to EUS repositories by default. |
|       | 7-Raw-CI | Raw-CI       | Cloud-init   | RHEL 7.x family of images.<br>Not attached to EUS repositories by default. |
|       | 6.7      | RAW          | Linux Agent  |                                                                            |
|       | 6.8      | RAW          | Linux Agent  |                                                                            |
|       | 6.9      | RAW          | Linux Agent  |                                                                            |

| OFFER         | SKU  | PARTITIONING | PROVISIONING | NOTES                                                     |
|---------------|------|--------------|--------------|-----------------------------------------------------------|
|               | 6.10 | RAW          | Linux Agent  |                                                           |
|               | 7.2  | RAW          | Linux Agent  |                                                           |
|               | 7.3  | RAW          | Linux Agent  |                                                           |
|               | 7.4  | RAW          | Linux Agent  | Attached to EUS repositories by default as of April 2019. |
|               | 7.5  | RAW          | Linux Agent  | Attached to EUS repositories by default as of June 2019.  |
|               | 7.6  | RAW          | Linux Agent  | Attached to EUS repositories by default as of May 2019.   |
|               | 7.7  | LVM          | Linux Agent  | Attached to EUS repositories by default.                  |
| RHEL-SAP      | 7.4  | LVM          | Linux Agent  | RHEL 7.4 for SAP HANA and Business Apps                   |
|               | 7.5  | LVM          | Linux Agent  | RHEL 7.5 for SAP HANA and Business Apps                   |
| RHEL-SAP-HANA | 6.7  | RAW          | Linux Agent  | RHEL 6.7 for SAP HANA                                     |
|               | 7.2  | LVM          | Linux Agent  | RHEL 7.2 for SAP HANA                                     |
|               | 7.3  | LVM          | Linux Agent  | RHEL 7.3 for SAP HANA                                     |
| RHEL-SAP-APPS | 6.8  | RAW          | Linux Agent  | RHEL 6.8 for SAP Business Applications                    |
|               | 7.3  | LVM          | Linux Agent  | RHEL 7.3 for SAP Business Applications                    |
| RHEL-HA       | 7.4  | LVM          | Linux Agent  | RHEL 7.4 with HA Add-On                                   |
|               | 7.5  | LVM          | Linux Agent  | RHEL 7.5 with HA Add-On                                   |
|               | 7.6  | LVM          | Linux Agent  | RHEL 7.6 with HA Add-On                                   |

| OFFER       | SKU | PARTITIONING | PROVISIONING | NOTES                           |
|-------------|-----|--------------|--------------|---------------------------------|
| RHEL-SAP-HA | 7.4 | LVM          | Linux Agent  | RHEL 7.4 for SAP with HA Add-On |
|             | 7.5 | LVM          | Linux Agent  | RHEL 7.5 for SAP with HA Add-On |
|             | 7.6 | LVM          | Linux Agent  | RHEL 7.6 for SAP with HA Add-On |

### Old naming convention

The RHEL 7 family of images and the RHEL 6 family of images used specific versions in their SKUs up until the naming convention change explained above.

You will find numeric SKUs in the full image list. Microsoft and Red Hat will create new numeric SKUs when a new minor release comes out.

### Other available Offers and SKUs

The full list of available offers and SKUs may include additional images beyond what is listed in the above table, for example, `RedHat:rhel-ocp-marketplace:rhe174:7.4.1`. These offers may be used for providing support of specific marketplace solutions, or they could be published for previews and testing purposes. They may be changed or removed at any time without warning. Do not use them unless their presence has been publicly documented by either Microsoft or Red Hat.

## Publishing policy

Microsoft and Red Hat update images as new minor versions are released, as required to address specific CVEs, or for occasional configuration changes/updates. We strive to provide updated images as soon as possible - within three business days following a release or availability of a CVE fix.

We only update the current minor release in a given image family. With the release of a newer minor version, we stop updating the older minor version. For example, with the release of RHEL 7.6, RHEL 7.5 images are no longer going to be updated.

#### NOTE

Active Azure VMs provisioned from RHEL Pay-As-You-Go images are connected to the Azure RHUI and can receive updates and fixes as soon as they are released by Red Hat and replicated to the Azure RHUI (usually in less than 24 hours following the official release by Red Hat). These VMs do not require a new published image for getting the updates and customers have full control over when to initiate the update.

## Image retention policy

Our current policy is to keep all previously published images. We reserve the right to remove images that are known to cause problems of any kind. For example, images with incorrect configurations due to subsequent platform or component updates may be removed. Images that may be removed will follow the current Marketplace policy to provide notifications up to 30 days before image removal.

## Next steps

- Learn more about the Azure Red Hat Update Infrastructure [here](#).
- Information on Red Hat support policies for all versions of RHEL can be found on the [Red Hat Enterprise Linux](#)

[Life Cycle](#) page.

# Download a Linux VHD from Azure

11/13/2019 • 2 minutes to read • [Edit Online](#)

In this article, you learn how to download a Linux virtual hard disk (VHD) file from Azure using the Azure CLI and Azure portal.

If you haven't already done so, install [Azure CLI](#).

## Stop the VM

A VHD can't be downloaded from Azure if it's attached to a running VM. You need to stop the VM to download a VHD. If you want to use a VHD as an [image](#) to create other VMs with new disks, you need to deprovision and generalize the operating system contained in the file and stop the VM. To use the VHD as a disk for a new instance of an existing VM or data disk, you only need to stop and deallocate the VM.

To use the VHD as an image to create other VMs, complete these steps:

1. Use SSH, the account name, and the public IP address of the VM to connect to it and deprovision it. You can find the public IP address with [az network public-ip show](#). The `+user` parameter also removes the last provisioned user account. If you are baking account credentials in to the VM, leave out this `+user` parameter. The following example removes the last provisioned user account:

```
ssh azureuser@<publicIpAddress>
sudo waagent -deprovision+user -force
exit
```

2. Sign in to your Azure account with [az login](#).

3. Stop and deallocate the VM.

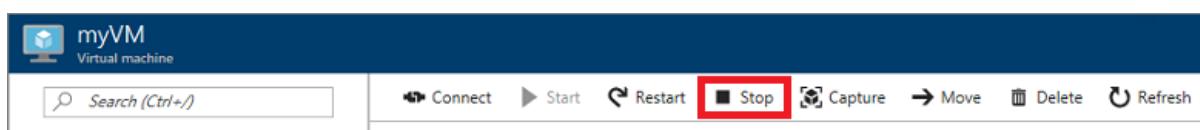
```
az vm deallocate --resource-group myResourceGroup --name myVM
```

4. Generalize the VM.

```
az vm generalize --resource-group myResourceGroup --name myVM
```

To use the VHD as a disk for a new instance of an existing VM or data disk, complete these steps:

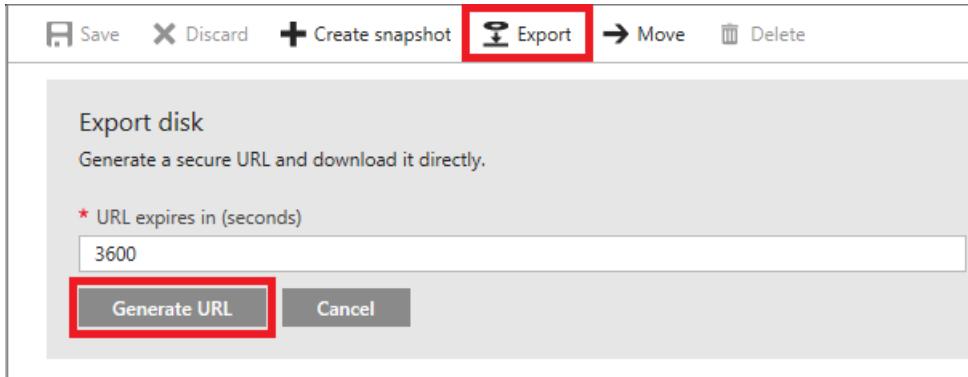
1. Sign in to the [Azure portal](#).
2. On the left menu, select **Virtual Machines**.
3. Select the VM from the list.
4. On the page for the VM, select **Stop**.



## Generate SAS URL

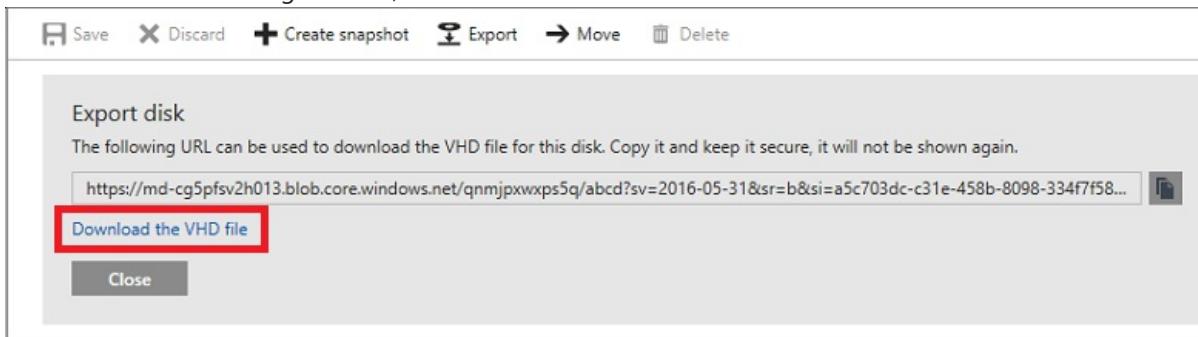
To download the VHD file, you need to generate a [shared access signature \(SAS\)](#) URL. When the URL is generated, an expiration time is assigned to the URL.

1. On the menu of the page for the VM, select **Disks**.
2. Select the operating system disk for the VM, and then select **Disk Export**.
3. Select **Generate URL**.



## Download VHD

1. Under the URL that was generated, select **Download the VHD file**. \*\*



2. You may need to select **Save** in the browser to start the download. The default name for the VHD file is *abcd*.



## Next steps

- Learn how to [upload and create a Linux VM from custom disk with the Azure CLI](#).
- [Manage Azure disks the Azure CLI](#).

2 minutes to read

# Manage the availability of Linux virtual machines

2/10/2020 • 9 minutes to read • [Edit Online](#)

Learn ways to set up and manage multiple virtual machines to ensure high availability for your Linux application in Azure. You can also [manage the availability of Windows virtual machines](#).

## Understand VM Reboots - maintenance vs. downtime

There are three scenarios that can lead to virtual machine in Azure being impacted: unplanned hardware maintenance, unexpected downtime, and planned maintenance.

- **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 will issue an unplanned hardware maintenance event to reduce the impact to the virtual machines hosted on that hardware. Azure uses [Live Migration](#) technology to migrate the 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. In cases where Live Migration cannot be used, the VM will experience Unexpected Downtime, as described below.
- **An Unexpected Downtime** is when the hardware or the physical infrastructure for the virtual machine fails unexpectedly. This 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. The attached OS and data disks are always preserved.

Virtual machines can also experience downtime in the unlikely event of an outage or disaster that affects an entire datacenter, or even an entire region. For these scenarios, Azure provides protection options including [availability zones](#) and [paired regions](#).

- **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 upon your Virtual Machines or Cloud Services (see [VM Preserving Maintenance](#)). While the Azure platform attempts to use VM Preserving Maintenance in all possible occasions, there are rare instances when these updates require a reboot of your virtual machine to apply the required updates to the underlying infrastructure. In this case, you can perform Azure Planned Maintenance with Maintenance-Redeploy operation by initiating the maintenance for their VMs in the suitable time window. For more information, see [Planned Maintenance for Virtual Machines](#).

To reduce the impact of downtime due to one or more of these events, we recommend the following high availability best practices for your virtual machines:

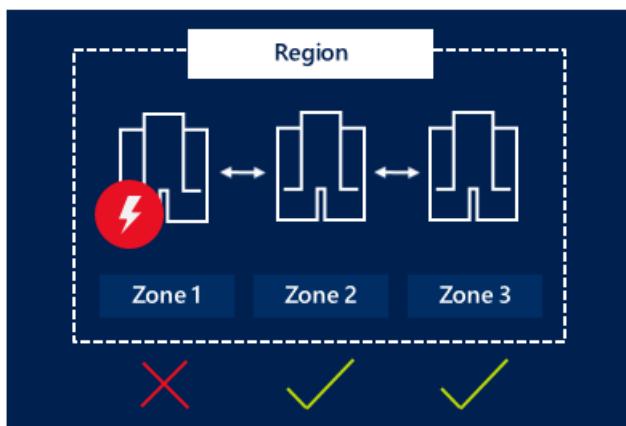
- [Configure multiple virtual machines in an availability set for redundancy](#)
- [Use managed disks for VMs in an availability set](#)
- [Use scheduled events to proactively response to VM impacting events](#)
- [Configure each application tier into separate availability sets](#)
- [Combine a Load Balancer with availability sets](#)
- [Use availability zones to protect from datacenter level failures](#)

## Use availability zones to protect from datacenter level failures

[Availability zones](#) expand the level of control you have to maintain the availability of the applications and data on your VMs. Availability Zones are unique physical locations within an Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking. To ensure resiliency, there are 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 from single-points-of-failure.

An Availability Zone in an Azure region is a combination of a **fault domain** and an **update domain**. For example, if you create three or more VMs across three zones in an Azure region, your VMs are effectively distributed across three fault domains and three update domains. The Azure platform recognizes this distribution across update domains to make sure that VMs in different zones are not updated at the same time.

With Availability Zones, Azure offers industry best 99.99% VM uptime SLA. By architecting your solutions to use replicated VMs in zones, you can protect your applications and data from the loss of a datacenter. If one zone is compromised, then replicated apps and data are instantly available in another zone.



Learn more about deploying a [Windows](#) or [Linux](#) VM in an Availability Zone.

## Configure multiple virtual machines in an availability set for redundancy

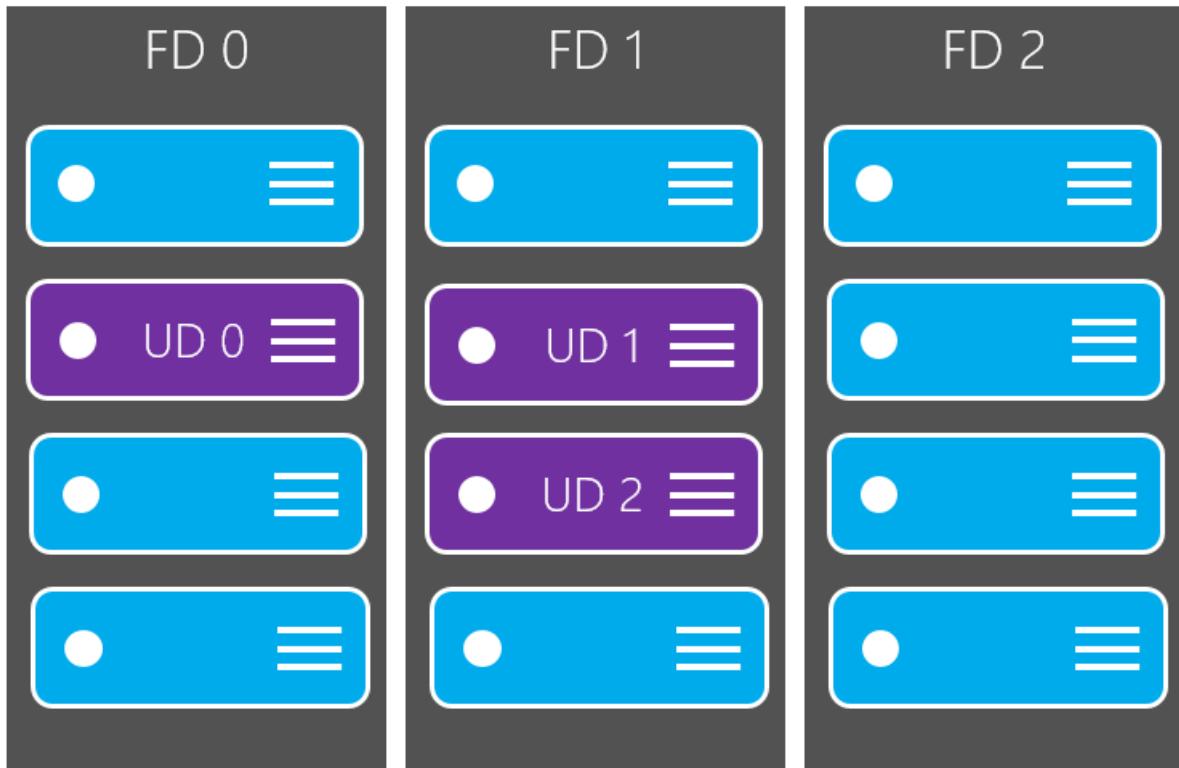
Availability sets are another datacenter configuration to provide VM redundancy and availability. This configuration within a datacenter ensures that during either a planned or unplanned maintenance event, at least one virtual machine is available and meets the 99.95% Azure SLA. For more information, see the [SLA for Virtual Machines](#).

### IMPORTANT

A single instance virtual machine in an availability set by itself should use Premium SSD or Ultra Disk for all operating system disks and data disks in order to qualify for the SLA for Virtual Machine connectivity of at least 99.9%.

Each virtual machine in your availability set is assigned an **update domain** and a **fault domain** by the underlying Azure platform. For a given availability set, five non-user-configurable update domains are assigned by default (Resource Manager deployments can then be increased to provide up to 20 update domains) to indicate groups of virtual machines and underlying physical hardware that can be rebooted at the same time. When more than five virtual machines are configured within a single availability set, the sixth virtual machine is placed into the same update domain as the first virtual machine, the seventh in the same update domain as the second virtual machine, and so on. The order of update domains being rebooted may not proceed sequentially during planned maintenance, but only one update domain is rebooted at a time. A rebooted update domain is given 30 minutes to recover before maintenance is initiated on a different update domain.

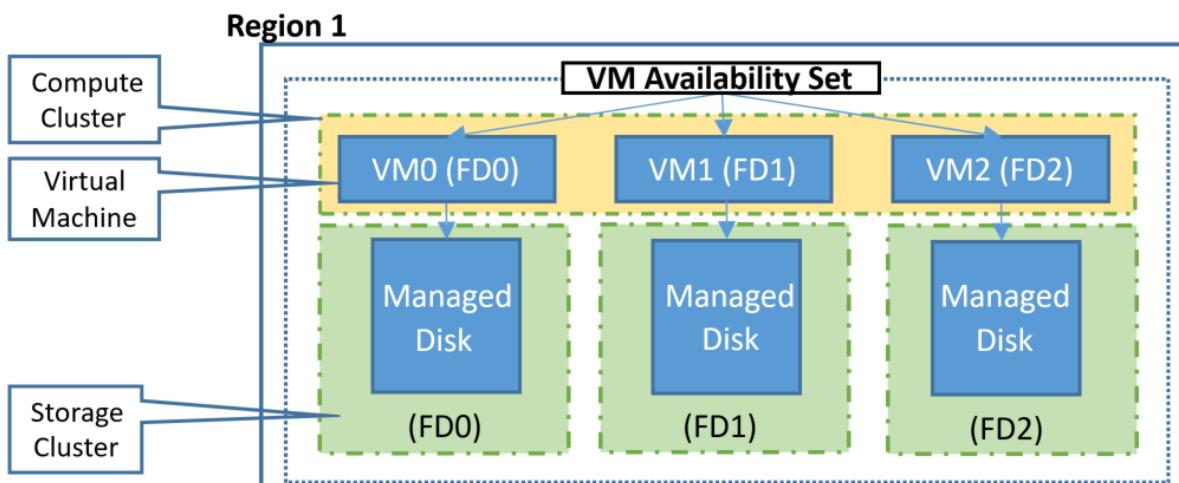
Fault domains define the group of virtual machines that share a common power source and network switch. By default, the virtual machines configured within your availability set are separated across up to three fault domains for Resource Manager deployments (two fault domains for Classic). While placing your virtual machines into an availability set does not protect your application from operating system or application-specific failures, it does limit the impact of potential physical hardware failures, network outages, or power interruptions.



## Use managed disks for VMs in an availability set

If you are currently using VMs with unmanaged disks, we highly recommend you [convert VMs in Availability Set to use Managed Disks](#).

Managed disks provide better reliability for Availability Sets by ensuring that the disks of VMs in an Availability Set are sufficiently isolated from each other to avoid single points of failure. It does this by automatically placing the disks in different storage fault domains (storage clusters) and aligning them with the VM fault domain. If a storage fault domain fails due to hardware or software failure, only the VM instance with disks on the storage fault domain fails.



## IMPORTANT

The number of fault domains for managed availability sets varies by region - either two or three per region. You can see the fault domain for each region by running the following scripts.

```
Get-AzComputeResourceSku | where{$_.ResourceType -eq 'availabilitySets' -and $_.Name -eq 'Aligned'}
```

```
az vm list-skus --resource-type availabilitySets --query '[?name==`Aligned`].
{Location:locationInfo[0].location, MaximumFaultDomainCount:capabilities[0].value}' -o Table
```

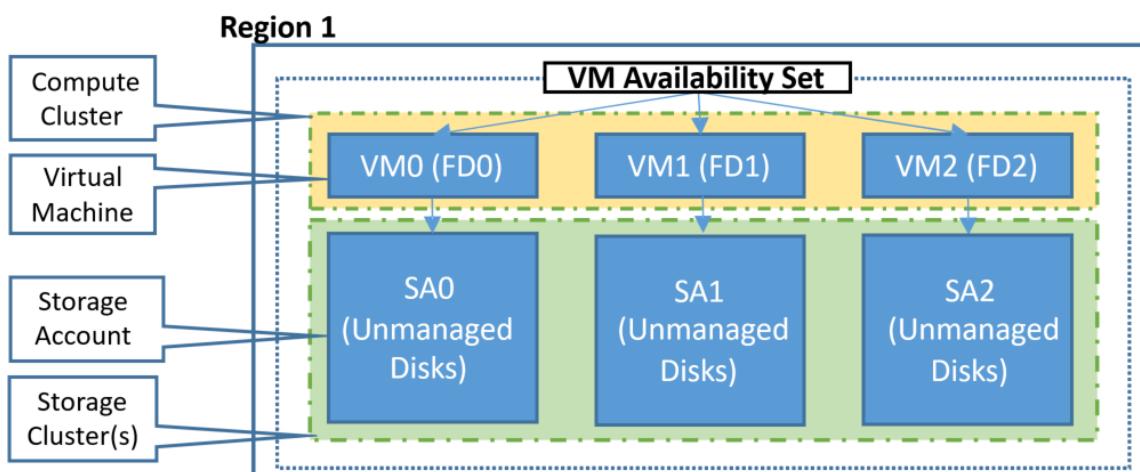
## NOTE

Under certain circumstances, 2 VMs in the same AvailabilitySet could shared the same FaultDomain. This can be confirmed by going into your availability set and checking the **Fault Domain** column. This can be cause from the following sequence while deploying the VMs:

- Deploy the 1st VM
- Stop/Deallocate the 1st VM
- Deploy the 2nd VM Under these circumstances, the OS Disk of the 2nd VM might be created on the same Fault Domain as the 1st VM, and so the 2nd VM will also land on the same FaultDomain. To avoid this issue, it's recommended to not stop/deallocate the VMs between deployments.

If you plan to use VMs with unmanaged disks, follow below best practices for Storage accounts where virtual hard disks (VHDs) of VMs are stored as [page blobs](#).

1. **Keep all disks (OS and data) associated with a VM in the same storage account**
2. **Review the limits on the number of unmanaged disks in an Azure Storage account** before adding more VHDs to a storage account
3. **Use a separate storage account for each VM in an Availability Set.** Do not share Storage accounts with multiple VMs in the same Availability Set. It is acceptable for VMs across different Availability Sets to share storage accounts if above best practices are followed



## Use scheduled events to proactively respond to VM impacting events

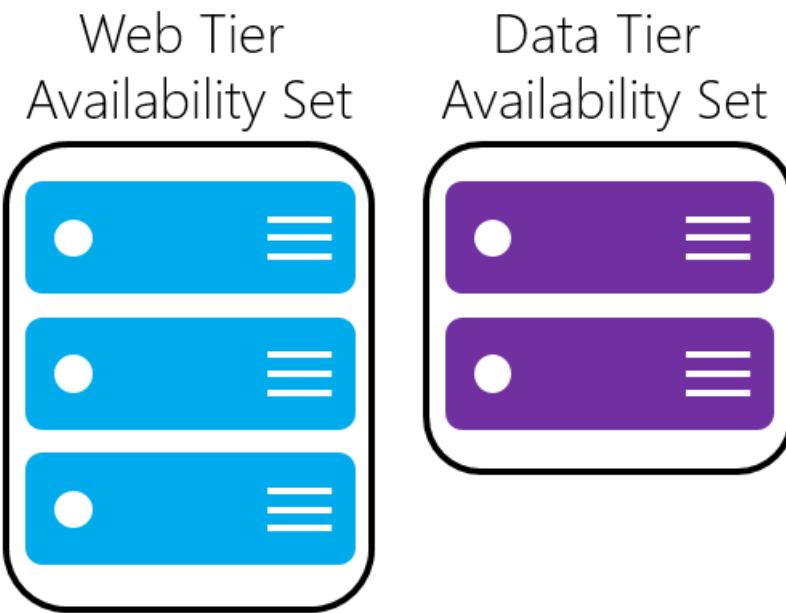
When you subscribe to [scheduled events](#), your VM is notified about upcoming maintenance events that can impact your VM. When scheduled events are enabled, your virtual machine is given a minimum amount of time before the maintenance activity is performed. For example, Host OS updates that might impact your VM are

queued up as events that specify the impact, as well as a time at which the maintenance will be performed if no action is taken. Schedule events are also queued up when Azure detects imminent hardware failure that might impact your VM, which allows you to decide when the healing should be performed. Customers can use the event to perform tasks prior to the maintenance, such as saving state, failing over to the secondary, and so on. After you complete your logic for gracefully handling the maintenance event, you can approve the outstanding scheduled event to allow the platform to proceed with maintenance.

## Configure each application tier into separate availability zones or availability sets

If your virtual machines are all nearly identical and serve the same purpose for your application, we recommend that you configure an availability zone or availability set for each tier of your application. If you place two different tiers in the same availability zone or set, all virtual machines in the same application tier can be rebooted at once. By configuring at least two virtual machines in an availability zone or set for each tier, you guarantee that at least one virtual machine in each tier is available.

For example, you could put all the virtual machines in the front end of your application running IIS, Apache, and Nginx in a single availability zone or set. Make sure that only front-end virtual machines are placed in the same availability zone or set. Similarly, make sure that only data-tier virtual machines are placed in their own availability zone or set, like your replicated SQL Server virtual machines, or your MySQL virtual machines.



## Combine a load balancer with availability zones or sets

Combine the [Azure Load Balancer](#) with an availability zone or set to get the most application resiliency. The Azure Load Balancer distributes traffic between multiple virtual machines. For our Standard tier virtual machines, the Azure Load Balancer is included. Not all virtual machine tiers include the Azure Load Balancer. For more information about load balancing your virtual machines, see [Load Balancing virtual machines](#).

If the load balancer is not configured to balance traffic across multiple virtual machines, then any planned maintenance event affects the only traffic-serving virtual machine, causing an outage to your application tier. Placing multiple virtual machines of the same tier under the same load balancer and availability set enables traffic to be continuously served by at least one instance.

For a tutorial on how to load balance across availability zones, see [Load balance VMs across all availability zones by using the Azure CLI](#).

## Next steps

To learn more about load balancing your virtual machines, see [Load Balancing virtual machines](#).

# Change the availability set for a VM

2/2/2020 • 2 minutes to read • [Edit Online](#)

The following steps describe how to change the availability set of a VM using Azure PowerShell. A VM can only be added to an availability set when it is created. To change the availability set, you need to delete and then recreate the virtual machine.

This article applies to both Linux and Windows VMs.

This article was last tested on 2/12/2019 using the [Azure Cloud Shell](#) and the [Az PowerShell module](#) version 1.2.0.

## Change the availability set

The following script provides an example of gathering the required information, deleting the original VM and then recreating it in a new availability set.

```
Set variables
$resourceGroup = "myResourceGroup"
$vmName = "myVM"
$newAvailSetName = "myAvailabilitySet"

Get the details of the VM to be moved to the Availability Set
$originalVM = Get-AzVM `-
 -ResourceGroupName $resourceGroup `-
 -Name $vmName

Create new availability set if it does not exist
$availSet = Get-AzAvailabilitySet `-
 -ResourceGroupName $resourceGroup `-
 -Name $newAvailSetName `-
 -ErrorAction Ignore
if (-Not $availSet) {
 $availSet = New-AzAvailabilitySet `-
 -Location $originalVM.Location `-
 -Name $newAvailSetName `-
 -ResourceGroupName $resourceGroup `-
 -PlatformFaultDomainCount 2 `-
 -PlatformUpdateDomainCount 2 `-
 -Sku Aligned
}

Remove the original VM
Remove-AzVM -ResourceGroupName $resourceGroup -Name $vmName

Create the basic configuration for the replacement VM.
$newVM = New-AzVMConfig `-
 -VMName $originalVM.Name `-
 -VMSize $originalVM.HardwareProfile.VmSize `-
 -AvailabilitySetId $availSet.Id

For a Linux VM, change the last parameter from -Windows to -Linux
Set-AzVMOSDisk `-
 -VM $newVM -CreateOption Attach `-
 -ManagedDiskId $originalVM.StorageProfile.OsDisk.ManagedDisk.Id `-
 -Name $originalVM.StorageProfile.OsDisk.Name `-
 -Windows

Add Data Disks
foreach ($disk in $originalVM.StorageProfile.DataDisks) {
 Add-AzVMDataDisk -VM $newVM `-
```

```

 -Name $disk.Name `
 -ManagedDiskId $disk.ManagedDisk.Id `
 -Caching $disk.Caching `
 -Lun $disk.Lun `
 -DiskSizeInGB $disk.DiskSizeGB `
 -CreateOption Attach
}

Add NIC(s) and keep the same NIC as primary
foreach ($nic in $originalVM.NetworkProfile.NetworkInterfaces) {
if ($nic.Primary -eq "True")
{
 Add-AzVMNetworkInterface `
 -VM $newVM `
 -Id $nic.Id -Primary
}
else
{
 Add-AzVMNetworkInterface `
 -VM $newVM `
 -Id $nic.Id
}
}

Recreate the VM
New-AzVM `
 -ResourceGroupName $resourceGroup `
 -Location $originalVM.Location `
 -VM $newVM `
 -DisableBginfoExtension

```

## Next steps

Add additional storage to your VM by adding an additional [data disk](#).

# Deploy VMs to proximity placement groups using Azure CLI

10/30/2019 • 2 minutes to read • [Edit Online](#)

To get VMs as close as possible, achieving the lowest possible latency, you should deploy them within a [proximity placement group](#).

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.

## Create the proximity placement group

Create a proximity placement group using [az ppg create](#).

```
az group create --name myPPGGroup --location westus
az ppg create \
-n myPPG \
-g myPPGGroup \
-l westus \
-t standard
```

## List proximity placement groups

You can list all of your proximity placement groups using [az ppg list](#).

```
az ppg list -o table
```

## Create a VM

Create a VM within the proximity placement group using [new az vm](#).

```
az vm create \
-n myVM \
-g myPPGGroup \
--image UbuntuLTS \
--ppg myPPG \
--generate-ssh-keys \
--size Standard_D1_v2 \
-l westus
```

You can see the VM in the proximity placement group using [az ppg show](#).

```
az ppg show --name myppg --resource-group myppggroup --query "virtualMachines"
```

## Availability Sets

You can also create an availability set in your proximity placement group. Use the same [--ppg](#) parameter with [az](#)

`vm availability-set create` to create an availability set and all of the VMs in the availability set will also be created in the same proximity placement group.

## Scale sets

You can also create a scale set in your proximity placement group. Use the same `--ppg` parameter with `az vmss create` to create a scale set and all of the instances will be created in the same proximity placement group.

## Next steps

Learn more about the [Azure CLI](#) commands for proximity placement groups.

# Create a proximity placement group using the portal

10/30/2019 • 2 minutes to read • [Edit Online](#)

To get VMs as close as possible, achieving the lowest possible latency, you should deploy them within a [proximity placement group](#).

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.

## Create the proximity placement group

1. Type **proximity placement group** in the search.
2. Under **Services** in the search results, select **Proximity placement groups**.
3. In the **Proximity placement groups** page, select **Add**.
4. In the **Basics** tab, under **Project details**, make sure the correct subscription is selected.
5. In **Resource group** either select **Create new** to create a new group or select an existing resource group from the drop-down.
6. In **Region** select the location where you want the proximity placement group to be created.
7. In **Proximity placement group name** type a name and then select **Review + create**.
8. After validation passes, select **Create** to create the proximity placement group.

Home > New > Proximity Placement Group > Create Proximity Placement Group

## Create Proximity Placement Group

Basics Tags Review + create

Fill out the required fields and then review the information on the Review + create tab. Once you're satisfied, click Create to deploy.

**Project details**

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

Subscription \* ⓘ Pay-As-You-Go

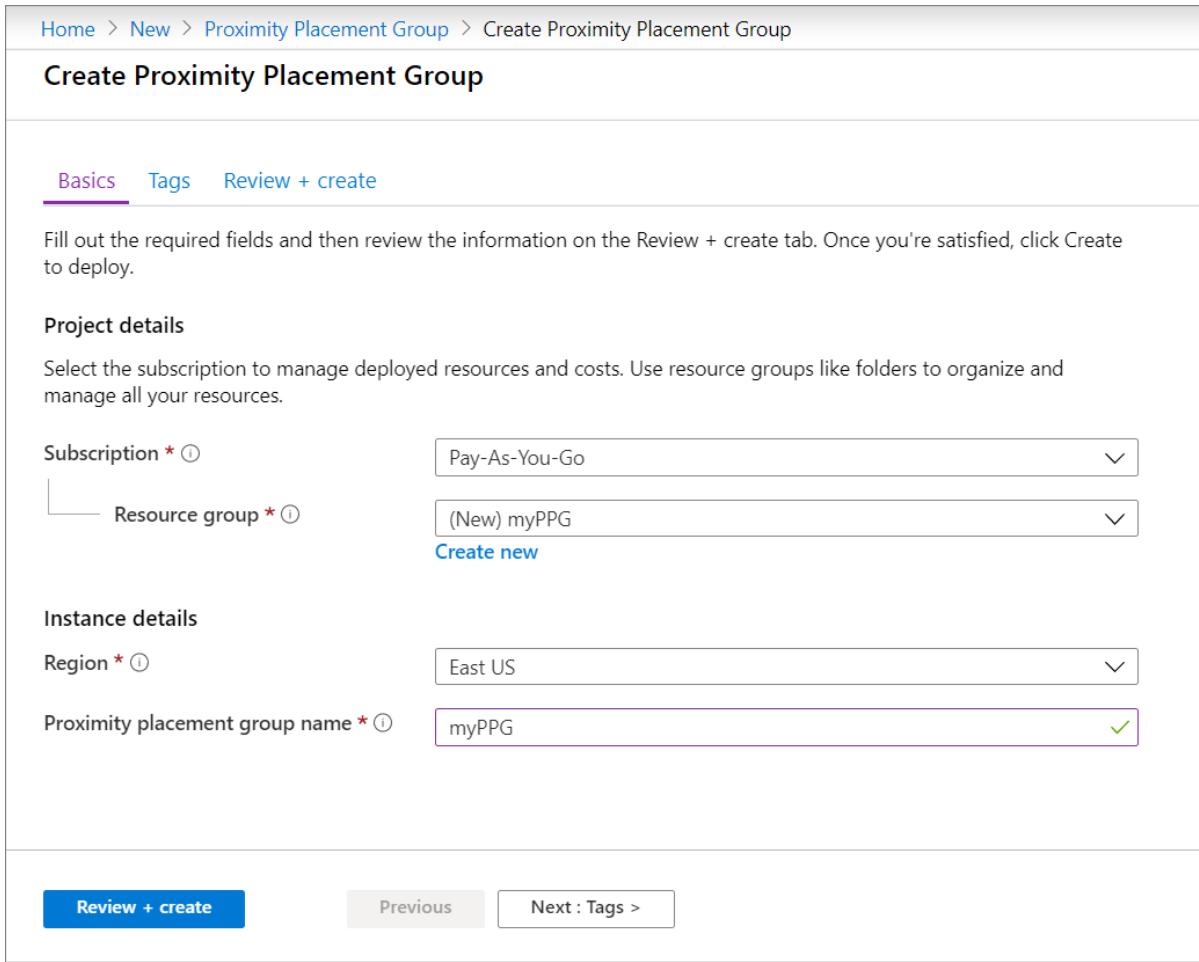
Resource group \* ⓘ (New) myPPG Create new

**Instance details**

Region \* ⓘ East US

Proximity placement group name \* ⓘ myPPG ✓

**Review + create** Previous Next : Tags >



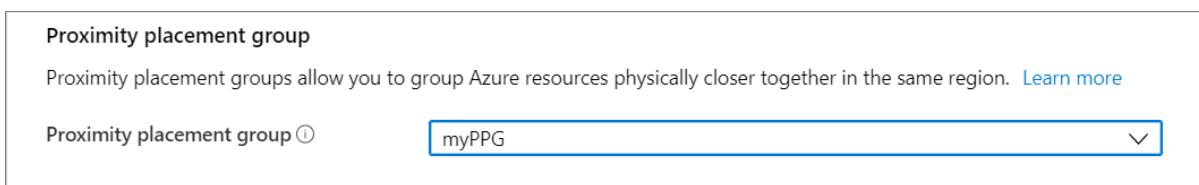
## Create a VM

1. While creating a VM in the portal, go to the **Advanced** tab.
2. In the **Proximity placement group** selection, select the correct placement group.

Proximity placement group

Proximity placement groups allow you to group Azure resources physically closer together in the same region. [Learn more](#)

Proximity placement group ⓘ myPPG



3. When you are done making all of the other required selections, select **Review + create**.
4. After it passes validation, select **Create** to deploy the VM in the placement group.

## Next steps

You can also use the [Azure PowerShell](#) to create proximity placement groups.

# Create a Linux virtual machine in an availability zone with the Azure CLI

11/13/2019 • 4 minutes to read • [Edit Online](#)

This article steps through using the Azure CLI to create a Linux VM in an Azure availability zone. An [availability zone](#) is a physically separate zone in an Azure region. Use availability zones to protect your apps and data from an unlikely failure or loss of an entire datacenter.

To use an availability zone, create your virtual machine in a [supported Azure region](#).

Make sure that you have installed the latest [Azure CLI](#) and logged in to an Azure account with [az login](#).

## Check VM SKU availability

The availability of VM sizes, or SKUs, may vary by region and zone. To help you plan for the use of Availability Zones, you can list the available VM SKUs by Azure region and zone. This ability makes sure that you choose an appropriate VM size, and obtain the desired resiliency across zones. For more information on the different VM types and sizes, see [VM Sizes overview](#).

You can view the available VM SKUs with the `az vm list-skus` command. The following example lists available VM SKUs in the `eastus2` region:

```
az vm list-skus --location eastus2 --output table
```

The output is similar to the following condensed example, which shows the Availability Zones in which each VM size is available:

| ResourceType    | Locations | Name            | [...] | Tier     | Size   | Zones |
|-----------------|-----------|-----------------|-------|----------|--------|-------|
| virtualMachines | eastus2   | Standard_DS1_v2 |       | Standard | DS1_v2 | 1,2,3 |
| virtualMachines | eastus2   | Standard_DS2_v2 |       | Standard | DS2_v2 | 1,2,3 |
| [...]           |           |                 |       |          |        |       |
| virtualMachines | eastus2   | Standard_F1s    |       | Standard | F1s    | 1,2,3 |
| virtualMachines | eastus2   | Standard_F2s    |       | Standard | F2s    | 1,2,3 |
| [...]           |           |                 |       |          |        |       |
| virtualMachines | eastus2   | Standard_D2s_v3 |       | Standard | D2_v3  | 1,2,3 |
| virtualMachines | eastus2   | Standard_D4s_v3 |       | Standard | D4_v3  | 1,2,3 |
| [...]           |           |                 |       |          |        |       |
| virtualMachines | eastus2   | Standard_E2_v3  |       | Standard | E2_v3  | 1,2,3 |
| virtualMachines | eastus2   | Standard_E4_v3  |       | Standard | E4_v3  | 1,2,3 |

## Create resource group

Create a resource group with the `az group create` command.

An Azure resource group is a logical container into which Azure resources are deployed and managed. A resource group must be created before a virtual machine. In this example, a resource group named `myResourceGroupVM` is created in the `eastus2` region. East US 2 is one of the Azure regions that supports availability zones.

```
az group create --name myResourceGroupVM --location eastus2
```

The resource group is specified when creating or modifying a VM, which can be seen throughout this article.

## Create virtual machine

Create a virtual machine with the [az vm create](#) command.

When creating a virtual machine, several options are available such as operating system image, disk sizing, and administrative credentials. In this example, a virtual machine is created with a name of *myVM* running Ubuntu Server. The VM is created in availability zone 1. By default, the VM is created in the *Standard\_DS1\_v2* size.

```
az vm create --resource-group myResourceGroupVM --name myVM --location eastus2 --image UbuntuLTS --generate-ssh-keys --zone 1
```

It may take a few minutes to create the VM. Once the VM has been created, the Azure CLI outputs information about the VM. Take note of the `zones` value, which indicates the availability zone in which the VM is running.

```
{
 "fqdns": "",
 "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxx/resourceGroups/myResourceGroupVM/providers/Microsoft.Compute/virtualMachines/myVM",
 "location": "eastus2",
 "macAddress": "00-0D-3A-23-9A-49",
 "powerState": "VM running",
 "privateIpAddress": "10.0.0.4",
 "publicIpAddress": "52.174.34.95",
 "resourceGroup": "myResourceGroupVM",
 "zones": "1"
}
```

## Confirm zone for managed disk and IP address

When the VM is deployed in an availability zone, a managed disk for the VM is created in the same availability zone. By default, a public IP address is also created in that zone. The following examples get information about these resources.

To verify that the VM's managed disk is in the availability zone, use the [az vm show](#) command to return the disk ID. In this example, the disk ID is stored in a variable that is used in a later step.

```
osdiskname=$(az vm show -g myResourceGroupVM -n myVM --query "storageProfile.osDisk.name" -o tsv)
```

Now you can get information about the managed disk:

```
az disk show --resource-group myResourceGroupVM --name $osdiskname
```

The output shows that the managed disk is in the same availability zone as the VM:

```
{
 "creationData": {
 "createOption": "FromImage",
 "imageReference": {
 "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxx/Providers/Microsoft.Compute/Locations/westeurope/Publishers/Canonical/ArtifactTypes/VMImage/Offer
s/UbuntuServer/Skus/16.04-LTS/Versions/latest",
 "lun": null
 },
 "sourceResourceId": null,
 "sourceUri": null,
 "storageAccountId": null
 },
 "diskSizeGb": 30,
 "encryptionSettings": null,
 "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxx/resourceGroups/myResourceGroupVM/providers/Microsoft.Compute/disks/osdisk_761c570dab",
 "location": "eastus2",
 "managedBy": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxx/resourceGroups/myResourceGroupVM/providers/Microsoft.Compute/virtualMachines/myVM",
 "name": "myVM_osdisk_761c570dab",
 "osType": "Linux",
 "provisioningState": "Succeeded",
 "resourceGroup": "myResourceGroupVM",
 "sku": {
 "name": "Premium_LRS",
 "tier": "Premium"
 },
 "tags": {},
 "timeCreated": "2018-03-05T22:16:06.892752+00:00",
 "type": "Microsoft.Compute/disks",
 "zones": [
 "1"
]
}
```

Use the [az vm list-ip-addresses](#) command to return the name of public IP address resource in *myVM*. In this example, the name is stored in a variable that is used in a later step.

```
ipaddressname=$(az vm list-ip-addresses -g myResourceGroupVM -n myVM --query "
[].virtualMachine.network.publicIpAddresses[].name" -o tsv)
```

Now you can get information about the IP address:

```
az network public-ip show --resource-group myResourceGroupVM --name $ipaddressname
```

The output shows that the IP address is in the same availability zone as the VM:

```
{
 "dnsSettings": null,
 "etag": "W/\"b7ad25eb-3191-4c8f-9cec-c5e4a3a37d35\"",
 "id": "/subscriptions/xxxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/myResourceGroupVM/providers/Microsoft.Network/publicIPAddresses/myVMPublicIP",
 "idleTimeoutInMinutes": 4,
 "ipAddress": "52.174.34.95",
 "ipConfiguration": {
 "etag": null,
 "id": "/subscriptions/xxxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/myResourceGroupVM/providers/Microsoft.Network/networkInterfaces/myVMVMNic/ipConfig
urations/ipconfigmyVM",
 "name": null,
 "privateIpAddress": null,
 "privateIpAllocationMethod": null,
 "provisioningState": null,
 "publicIpAddress": null,
 "resourceGroup": "myResourceGroupVM",
 "subnet": null
 },
 "location": "eastUS2",
 "name": "myVMPublicIP",
 "provisioningState": "Succeeded",
 "publicIpAddressVersion": "IPv4",
 "publicIpAllocationMethod": "Dynamic",
 "resourceGroup": "myResourceGroupVM",
 "resourceGuid": "8c70a073-09be-4504-0000-000000000000",
 "tags": {},
 "type": "Microsoft.Network/publicIPAddresses",
 "zones": [
 "1"
]
}
```

## Next steps

In this article, you learned how to create a VM in an availability zone. Learn more about [availability](#) for Azure VMs.

2 minutes to read

2 minutes to read

2 minutes to read

# Install and configure Terraform to provision Azure resources

2/19/2020 • 4 minutes to read • [Edit Online](#)

Terraform provides an easy way to define, preview, and deploy cloud infrastructure by using a [simple templating language](#). This article describes the necessary steps to use Terraform to provision resources in Azure.

To learn more about how to use Terraform with Azure, visit the [Terraform Hub](#).

## NOTE

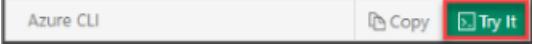
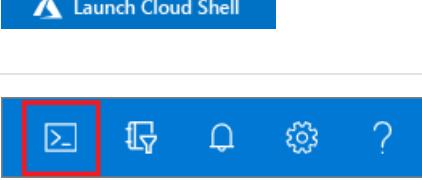
For Terraform specific support, please reach out to Terraform directly using one of their community channels:

- The [Terraform section](#) of the community portal contains questions, use cases, and useful patterns.
- For provider-related questions please visit the [Terraform Providers](#) section of the community portal.

## Use Azure Cloud Shell

Azure hosts Azure Cloud Shell, an interactive shell environment that you can use through your browser. You can use either Bash or PowerShell with Cloud Shell to work with Azure services. You can use the Cloud Shell preinstalled commands to run the code in this article without having to install anything on your local environment.

To start Azure Cloud Shell:

| OPTION                                                                                                                                                    | EXAMPLE/LINK                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Select <b>Try It</b> in the upper-right corner of a code block.<br>Selecting <b>Try It</b> doesn't automatically copy the code to Cloud Shell.            |  |
| Go to <a href="https://shell.azure.com">https://shell.azure.com</a> , or select the <b>Launch Cloud Shell</b> button to open Cloud Shell in your browser. |  |
| Select the <b>Cloud Shell</b> button on the menu bar at the upper right in the <a href="#">Azure portal</a> .                                             |                                                                                      |

To run the code in this article in Azure Cloud Shell:

1. Start Cloud Shell.
2. Select the **Copy** button on a code block to copy the code.
3. Paste the code into the Cloud Shell session by selecting **Ctrl+Shift+V** on Windows and Linux or by selecting **Cmd+Shift+V** on macOS.
4. Select **Enter** to run the code.

Terraform is installed by default in the [Cloud Shell](#). If you choose to install Terraform locally, complete the next step, otherwise continue to [Set up Terraform access to Azure](#).

## Install Terraform

To install Terraform, [download](#) the appropriate package for your operating system into a separate install directory. The download contains a single executable file, for which you should also define a global path. For instructions on how to set the path on Linux and Mac, go to [this webpage](#). For instructions on how to set the path on Windows, go to [this webpage](#).

Verify your path configuration with the `terraform` command. A list of available Terraform options is shown, as in the following example output:

```
azureuser@Azure:~$ terraform
Usage: terraform [--version] [--help] <command> [args]
```

## Set up Terraform access to Azure

To enable Terraform to provision resources into Azure, create an [Azure AD service principal](#). The service principal grants your Terraform scripts to provision resources in your Azure subscription.

If you have multiple Azure subscriptions, first query your account with [az account list](#) to get a list of subscription ID and tenant ID values:

```
az account list --query "[].{name:name, subscriptionId:id, tenantId:tenantId}"
```

To use a selected subscription, set the subscription for this session with [az account set](#). Set the `SUBSCRIPTION_ID` environment variable to hold the value of the returned `id` field from the subscription you want to use:

```
az account set --subscription="${SUBSCRIPTION_ID}"
```

Now you can create a service principal for use with Terraform. Use [az ad sp create-for-rbac](#), and set the *scope* to your subscription as follows:

```
az ad sp create-for-rbac --role="Contributor" --scopes="/subscriptions/${SUBSCRIPTION_ID}"
```

Your `appId`, `password`, `sp_name`, and `tenant` are returned. Make a note of the `appId` and `password`.

## Configure Terraform environment variables

To configure Terraform to use your Azure AD service principal, set the following environment variables, which are then used by the [Azure Terraform modules](#). You can also set the environment if working with an Azure cloud other than Azure public.

- `ARM_SUBSCRIPTION_ID`
- `ARM_CLIENT_ID`
- `ARM_CLIENT_SECRET`
- `ARM_TENANT_ID`
- `ARM_ENVIRONMENT`

You can use the following sample shell script to set those variables:

```
#!/bin/sh
echo "Setting environment variables for Terraform"
export ARM_SUBSCRIPTION_ID=your_subscription_id
export ARM_CLIENT_ID=your_appId
export ARM_CLIENT_SECRET=your_password
export ARM_TENANT_ID=your_tenant_id

Not needed for public, required for usgovernment, german, china
export ARM_ENVIRONMENT=public
```

## Run a sample script

Create a file `test.tf` in an empty directory and paste in the following script.

```
provider "azurerm" {
}
resource "azurerm_resource_group" "rg" {
 name = "testResourceGroup"
 location = "westus"
}
```

Save the file and then initialize the Terraform deployment. This step downloads the Azure modules required to create an Azure resource group.

```
terraform init
```

The output is similar to the following example:

```
* provider_azurerm: version = "~> 0.3"
Terraform has been successfully initialized!
```

You can preview the actions to be completed by the Terraform script with `terraform plan`. When ready to create the resource group, apply your Terraform plan as follows:

```
terraform apply
```

The output is similar to the following example:

```
An execution plan has been generated and is shown below.
Resource actions are indicated with the following symbols:
+ create
```

```
Terraform will perform the following actions:
```

```
+ azurerm_resource_group.rg
 id: <computed>
 location: "westus"
 name: "testResourceGroup"
 tags.%: <computed>

azurerm_resource_group.rg: Creating...
 location: "" => "westus"
 name: "" => "testResourceGroup"
 tags.%: "" => "<computed>"
azurerm_resource_group.rg: Creation complete after 1s
```

## Next steps

In this article, you installed Terraform or used the Cloud Shell to configure Azure credentials and start creating resources in your Azure subscription. To create a more complete Terraform deployment in Azure, see the following article:

[Create an Azure VM with Terraform](#)

# Create a complete Linux virtual machine infrastructure in Azure with Terraform

2/19/2020 • 7 minutes to read • [Edit Online](#)

Terraform allows you to define and create complete infrastructure deployments in Azure. You build Terraform templates in a human-readable format that create and configure Azure resources in a consistent, reproducible manner. This article shows you how to create a complete Linux environment and supporting resources with Terraform. You can also learn how to [Install and configure Terraform](#).

## NOTE

For Terraform specific support, please reach out to Terraform directly using one of their community channels:

- The [Terraform section](#) of the community portal contains questions, use cases, and useful patterns.
- For provider-related questions please visit the [Terraform Providers](#) section of the community portal.

## Create Azure connection and resource group

Let's go through each section of a Terraform template. You can also see the full version of the [Terraform template](#) that you can copy and paste.

The `provider` section tells Terraform to use an Azure provider. To get values for `subscription_id`, `client_id`, `client_secret`, and `tenant_id`, see [Install and configure Terraform](#).

## TIP

If you create environment variables for the values or are using the [Azure Cloud Shell Bash experience](#), you don't need to include the variable declarations in this section.

```
provider "azurerm" {
 subscription_id = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
 client_id = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
 client_secret = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
 tenant_id = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
}
```

The following section creates a resource group named `myResourceGroup` in the `eastus` location:

```
resource "azurerm_resource_group" "myterraformgroup" {
 name = "myResourceGroup"
 location = "eastus"

 tags = {
 environment = "Terraform Demo"
 }
}
```

In additional sections, you reference the resource group with  
`azurerm_resource_group.myterraformgroup.name`.

## Create virtual network

The following section creates a virtual network named *myVnet* in the *10.0.0.0/16* address space:

```
resource "azurerm_virtual_network" "myterraformnetwork" {
 name = "myVnet"
 address_space = ["10.0.0.0/16"]
 location = "eastus"
 resource_group_name = azurerm_resource_group.myterraformgroup.name

 tags = {
 environment = "Terraform Demo"
 }
}
```

The following section creates a subnet named *mySubnet* in the *myVnet* virtual network:

```
resource "azurerm_subnet" "myterraformsubnet" {
 name = "mySubnet"
 resource_group_name = azurerm_resource_group.myterraformgroup.name
 virtual_network_name = azurerm_virtual_network.myterraformnetwork.name
 address_prefix = "10.0.2.0/24"
}
```

## Create public IP address

To access resources across the Internet, create and assign a public IP address to your VM. The following section creates a public IP address named *myPublicIP*:

```
resource "azurerm_public_ip" "myterraformpublicip" {
 name = "myPublicIP"
 location = "eastus"
 resource_group_name = azurerm_resource_group.myterraformgroup.name
 allocation_method = "Dynamic"

 tags = {
 environment = "Terraform Demo"
 }
}
```

## Create Network Security Group

Network Security Groups control the flow of network traffic in and out of your VM. The following section creates a network security group named *myNetworkSecurityGroup* and defines a rule to allow SSH traffic on TCP port 22:

```

resource "azurerm_network_security_group" "myterraformnsg" {
 name = "myNetworkSecurityGroup"
 location = "eastus"
 resource_group_name = azurerm_resource_group.myterraformgroup.name

 security_rule {
 name = "SSH"
 priority = 1001
 direction = "Inbound"
 access = "Allow"
 protocol = "Tcp"
 source_port_range = "*"
 destination_port_range = "22"
 source_address_prefix = "*"
 destination_address_prefix = "*"
 }

 tags = {
 environment = "Terraform Demo"
 }
}

```

## Create virtual network interface card

A virtual network interface card (NIC) connects your VM to a given virtual network, public IP address, and network security group. The following section in a Terraform template creates a virtual NIC named *myNIC* connected to the virtual networking resources you have created:

```

resource "azurerm_network_interface" "myterraformnic" {
 name = "myNIC"
 location = "eastus"
 resource_group_name = azurerm_resource_group.myterraformgroup.name
 network_security_group_id = azurerm_network_security_group.myterraformnsg.id

 ip_configuration {
 name = "myNicConfiguration"
 subnet_id = "${azurerm_subnet.myterraformsubnet.id}"
 private_ip_address_allocation = "Dynamic"
 public_ip_address_id = "${azurerm_public_ip.myterraformpublicip.id}"
 }

 tags = {
 environment = "Terraform Demo"
 }
}

```

## Create storage account for diagnostics

To store boot diagnostics for a VM, you need a storage account. These boot diagnostics can help you troubleshoot problems and monitor the status of your VM. The storage account you create is only to store the boot diagnostics data. As each storage account must have a unique name, the following section generates some random text:

```

resource "random_id" "randomId" {
 keepers = [
 # Generate a new ID only when a new resource group is defined
 azurerm_resource_group.myterraformgroup.name
]

 byte_length = 8
}

```

Now you can create a storage account. The following section creates a storage account, with the name based on the random text generated in the preceding step:

```

resource "azurerm_storage_account" "mystorageaccount" {
 name = diag${random_id.randomId.hex}"
 resource_group_name = azurerm_resource_group.myterraformgroup.name
 location = "eastus"
 account_replication_type = "LRS"
 account_tier = "Standard"

 tags = {
 environment = "Terraform Demo"
 }
}

```

## Create virtual machine

The final step is to create a VM and use all the resources created. The following section creates a VM named *myVM* and attaches the virtual NIC named *myNIC*. The latest *Ubuntu 16.04-LTS* image is used, and a user named *azureuser* is created with password authentication disabled.

SSH key data is provided in the *ssh\_keys* section. Provide a valid public SSH key in the *key\_data* field.

```

resource "azurerm_virtual_machine" "myterraformvm" {
 name = "myVM"
 location = "eastus"
 resource_group_name = azurerm_resource_group.myterraformgroup.name
 network_interface_ids = [azurerm_network_interface.myterraformnic.id]
 vm_size = "Standard_DS1_v2"

 storage_os_disk {
 name = "myOsDisk"
 caching = "ReadWrite"
 create_option = "FromImage"
 managed_disk_type = "Premium_LRS"
 }

 storage_image_reference {
 publisher = "Canonical"
 offer = "UbuntuServer"
 sku = "16.04.0-LTS"
 version = "latest"
 }

 os_profile {
 computer_name = "myvm"
 admin_username = "azureuser"
 }

 os_profile_linux_config {
 disable_password_authentication = true
 ssh_keys {
 path = "/home/azureuser/.ssh/authorized_keys"
 key_data = "ssh-rsa AAAAB3Nz{snip}hwhqT9h"
 }
 }

 boot_diagnostics {
 enabled = "true"
 storage_uri = azurerm_storage_account.mystorageaccount.primary_blob_endpoint
 }

 tags = {
 environment = "Terraform Demo"
 }
}

```

## Complete Terraform script

To bring all these sections together and see Terraform in action, create a file called *terraform\_azure.tf* and paste the following content:

```

Configure the Microsoft Azure Provider
provider "azurerm" {
 subscription_id = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
 client_id = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
 client_secret = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
 tenant_id = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
}

Create a resource group if it doesn't exist
resource "azurerm_resource_group" "myterraformgroup" {
 name = "myResourceGroup"
 location = "eastus"

 tags = {
 environment = "Terraform Demo"
 }
}

```

```

}

Create virtual network
resource "azurerm_virtual_network" "myterraformnetwork" {
 name = "myVnet"
 address_space = ["10.0.0.0/16"]
 location = "eastus"
 resource_group_name = azurerm_resource_group.myterraformgroup.name

 tags = {
 environment = "Terraform Demo"
 }
}

Create subnet
resource "azurerm_subnet" "myterraformsubnet" {
 name = "mySubnet"
 resource_group_name = azurerm_resource_group.myterraformgroup.name
 virtual_network_name = azurerm_virtual_network.myterraformnetwork.name
 address_prefix = "10.0.1.0/24"
}

Create public IPs
resource "azurerm_public_ip" "myterraformpublicip" {
 name = "myPublicIP"
 location = "eastus"
 resource_group_name = azurerm_resource_group.myterraformgroup.name
 allocation_method = "Dynamic"

 tags = {
 environment = "Terraform Demo"
 }
}

Create Network Security Group and rule
resource "azurerm_network_security_group" "myterraformnsg" {
 name = "myNetworkSecurityGroup"
 location = "eastus"
 resource_group_name = azurerm_resource_group.myterraformgroup.name

 security_rule {
 name = "SSH"
 priority = 1001
 direction = "Inbound"
 access = "Allow"
 protocol = "Tcp"
 source_port_range = "*"
 destination_port_range = "22"
 source_address_prefix = "*"
 destination_address_prefix = "*"
 }

 tags = {
 environment = "Terraform Demo"
 }
}

Create network interface
resource "azurerm_network_interface" "myterraformnic" {
 name = "myNIC"
 location = "eastus"
 resource_group_name = azurerm_resource_group.myterraformgroup.name
 network_security_group_id = azurerm_network_security_group.myterraformnsg.id

 ip_configuration {
 name = "myNicConfiguration"
 subnet_id = azurerm_subnet.myterraformsubnet.id
 private_ip_address_allocation = "Dynamic"
 public_ip_address_id = azurerm_public_ip.myterraformpublicip.id
 }
}

```

```

 public_ip_address_id = azurerm_public_ip.myterraformpublicip.id
 }

 tags = {
 environment = "Terraform Demo"
 }
}

Generate random text for a unique storage account name
resource "random_id" "randomId" {
 keepers = [
 # Generate a new ID only when a new resource group is defined
 resource_group = azurerm_resource_group.myterraformgroup.name
]

 byte_length = 8
}

Create storage account for boot diagnostics
resource "azurerm_storage_account" "mystorageaccount" {
 name = "diag${random_id.randomId.hex}"
 resource_group_name = azurerm_resource_group.myterraformgroup.name
 location = "eastus"
 account_tier = "Standard"
 account_replication_type = "LRS"

 tags = {
 environment = "Terraform Demo"
 }
}

Create virtual machine
resource "azurerm_virtual_machine" "myterraformvm" {
 name = "myVM"
 location = "eastus"
 resource_group_name = azurerm_resource_group.myterraformgroup.name
 network_interface_ids = [azurerm_network_interface.myterraformnic.id]
 vm_size = "Standard_DS1_v2"

 storage_os_disk {
 name = "myOsDisk"
 caching = "ReadWrite"
 create_option = "FromImage"
 managed_disk_type = "Premium_LRS"
 }

 storage_image_reference {
 publisher = "Canonical"
 offer = "UbuntuServer"
 sku = "16.04.0-LTS"
 version = "latest"
 }

 os_profile {
 computer_name = "myvm"
 admin_username = "azureuser"
 }

 os_profile_linux_config {
 disable_password_authentication = true
 ssh_keys {
 path = "/home/azureuser/.ssh/authorized_keys"
 key_data = "ssh-rsa AAAAB3Nz{snip}hwhqT9h"
 }
 }

 boot_diagnostics {
 enabled = "true"
 storage_uri = azurerm_storage_account.mystorageaccount.primary_blob_endpoint
 }
}

```

```
}

tags = {
 environment = "Terraform Demo"
}
}
```

## Build and deploy the infrastructure

With your Terraform template created, the first step is to initialize Terraform. This step ensures that Terraform has all the prerequisites to build your template in Azure.

```
terraform init
```

The next step is to have Terraform review and validate the template. This step compares the requested resources to the state information saved by Terraform and then outputs the planned execution. Resources are *not* created in Azure.

```
terraform plan
```

After you execute the previous command, you should see something like the following screen:

```
Refreshing Terraform state in-memory prior to plan...
The refreshed state will be used to calculate this plan, but will not be
persisted to local or remote state storage.
```

```
...
```

```
Note: You didn't specify an "-out" parameter to save this plan, so when
"apply" is called, Terraform can't guarantee this is what will execute.
```

```
+ azurerm_resource_group.myterraform
 <snip>
+ azurerm_virtual_network.myterraformnetwork
 <snip>
+ azurerm_network_interface.myterraformnic
 <snip>
+ azurerm_network_security_group.myterraformnsg
 <snip>
+ azurerm_public_ip.myterraformpublicip
 <snip>
+ azurerm_subnet.myterraformsubnet
 <snip>
+ azurerm_virtual_machine.myterraformvm
 <snip>
```

```
Plan: 7 to add, 0 to change, 0 to destroy.
```

If everything looks correct and you are ready to build the infrastructure in Azure, apply the template in Terraform:

```
terraform apply
```

Once Terraform completes, your VM infrastructure is ready. Obtain the public IP address of your VM with [az vm show](#):

```
az vm show --resource-group myResourceGroup --name myVM -d --query [publicIps] --o tsv
```

You can then SSH to your VM:

```
ssh azureuser@<publicIps>
```

## Next steps

You have created basic infrastructure in Azure by using Terraform. For more complex scenarios, including examples that use load balancers and virtual machine scale sets, see numerous [Terraform examples for Azure](#). For an up-to-date list of supported Azure providers, see the [Terraform documentation](#).

# cloud-init support for virtual machines in Azure

2/2/2020 • 7 minutes to read • [Edit Online](#)

This article explains the support that exists for [cloud-init](#) to configure a virtual machine (VM) or virtual machine scale sets at provisioning time in Azure. These cloud-init configurations are run on first boot once the resources have been provisioned by Azure.

VM Provisioning is the process where the Azure will pass down your VM Create parameter values, such as hostname, username, password etc., and make them available to the VM as it boots up. A 'provisioning agent' will consume those values, configure the VM, and report back when completed.

Azure supports two provisioning agents [cloud-init](#), and the [Azure Linux Agent \(WALA\)](#).

## cloud-init overview

[cloud-init](#) is a widely used approach to customize a Linux VM as it boots for the first time. You can use cloud-init to install packages and write files, or to configure users and security. Because cloud-init is called during the initial boot process, there are no additional steps or required agents to apply your configuration. For more information on how to properly format your `#cloud-config` files or other inputs, see the [cloud-init documentation site](#).

`#cloud-config` files are text files encoded in base64.

cloud-init also works across distributions. For example, you don't use **apt-get install** or **yum install** to install a package. Instead you can define a list of packages to install. cloud-init automatically uses the native package management tool for the distro you select.

We are actively working with our endorsed Linux distro partners in order to have cloud-init enabled images available in the Azure marketplace. These images will make your cloud-init deployments and configurations work seamlessly with VMs and virtual machine scale sets. Initially we collaborate with the endorsed Linux distro partners and upstream to ensure cloud-init functions with the OS on Azure, then the packages are updated and made publically available in the distro package repositories.

There are two stages to making cloud-init available to the endorsed Linux distro OS's on Azure, package support, and then image support:

- 'cloud-init package support on Azure' documents which cloud-init packages onwards are supported or in preview, so you can use these packages with the OS in a custom image.
- 'image cloud-init ready' documents if the image is already configured to use cloud-init.

### Canonical

| PUBLISHER / VERSION | OFFER        | SKU         | VERSION | IMAGE CLOUD-INIT READY | CLOUD-INIT PACKAGE SUPPORT ON AZURE |
|---------------------|--------------|-------------|---------|------------------------|-------------------------------------|
| Canonical 18.04     | UbuntuServer | 18.04-LTS   | latest  | yes                    | yes                                 |
| Canonical 16.04     | UbuntuServer | 16.04-LTS   | latest  | yes                    | yes                                 |
| Canonical 14.04     | UbuntuServer | 14.04.5-LTS | latest  | yes                    | yes                                 |

### RHEL

| PUBLISHER / VERSION | OFFER     | SKU        | VERSION        | IMAGE CLOUD-INIT READY                                                                                                                   | CLOUD-INIT PACKAGE SUPPORT ON AZURE                |
|---------------------|-----------|------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|
| RedHat 7.6          | RHEL      | 7-RAW-CI   | 7.6.2019072418 | yes                                                                                                                                      | yes - support from package version: 18.2-1.el7_6.2 |
| RedHat 7.7          | RHEL      | 7-RAW-CI   | 7.7.2019081601 | yes (note this is a preview image, and once all RHEL 7.7 images support cloud-init, this will be removed mid 2020, notice will be given) | yes - support from package version: 18.5-3.el7     |
| RedHat 7.7          | RHEL      | 7-RAW      | n/a            | no - image updates to start Feb 2020                                                                                                     | yes - support from package version: 18.5-3.el7     |
| RedHat 7.7          | RHEL      | 7-LVM      | n/a            | no - image updates to start Feb 2020                                                                                                     | yes - support from package version: 18.5-3.el7     |
| RedHat 7.7          | RHEL      | 7.7        | n/a            | no - image updates to start Feb 2020                                                                                                     | yes - support from package version: 18.5-3.el7     |
| RedHat 7.7          | rhel-byos | rhel-lvm77 | n/a            | no - image updates to start Feb 2020                                                                                                     | yes - support from package version: 18.5-3.el7     |

## CentOS

| PUBLISHER / VERSION | OFFER  | SKU  | VERSION      | IMAGE CLOUD-INIT READY                                                                                                                     | CLOUD-INIT PACKAGE SUPPORT ON AZURE                   |
|---------------------|--------|------|--------------|--------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| OpenLogic 7.7       | CentOS | 7-CI | 7.7.20190920 | yes (note this is a preview image, and once all CentOS 7.7 images support cloud-init, this will be removed mid 2020, notice will be given) | yes - support from package version: 18.5-3.el7 centos |

- CentOS 7.7 images that will be cloud-init enabled be updated here in Feb 2020

## Oracle

| PUBLISHER / VERSION | OFFER        | SKU   | VERSION | IMAGE CLOUD-INIT READY                                                                                                                                     | CLOUD-INIT PACKAGE SUPPORT ON AZURE        |
|---------------------|--------------|-------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|
| Oracle 7.7          | Oracle-Linux | 77-ci | 7.7.01  | preview image<br>(note this is a preview image, and it once all Oracle 7.7 images support cloud-init, this will be removed mid 2020, notice will be given) | no, in preview, package is: 18.5-3.0.1.el7 |

## Debian & SuSE SLES

We are currently working to preview support, expect updates in February and March 2020.

Currently Azure Stack will support the provisioning of cloud-init enabled images.

## What is the difference between cloud-init and the Linux Agent (WALA)?

WALA is an Azure platform-specific agent used to provision and configure VMs, and handle [Azure extensions](#).

We are enhancing the task of configuring VMs to use cloud-init instead of the Linux Agent in order to allow existing cloud-init customers to use their current cloud-init scripts, or new customers to take advantage of the rich cloud-init configuration functionality. If you have existing investments in cloud-init scripts for configuring Linux systems, there are **no additional settings required** to enable cloud-init process them.

cloud-init cannot process Azure extensions, so WALA is still required in the image to process extensions, but will need to have its provisioning code disabled, for endorsed Linux distros images that are being converted to provision by cloud-init, they will have WALA installed, and setup correctly.

When creating a VM, if you do not include the Azure CLI `--custom-data` switch at provisioning time, cloud-init or WALA takes the minimal VM provisioning parameters required to provision the VM and complete the deployment with the defaults. If you reference the cloud-init configuration with the `--custom-data` switch, whatever is contained in your custom data will be available to cloud-init when the VM boots.

cloud-init configurations applied to VMs do not have time constraints and will not cause a deployment to fail by timing out. This is not true for WALA, if you change the WALA defaults to process custom-data, it cannot exceed the total VM provisioning time allowance of 40mins, if so, the VM Create will fail.

## Deploying a cloud-init enabled Virtual Machine

Deploying a cloud-init enabled virtual machine is as simple as referencing a cloud-init enabled distribution during deployment. Linux distribution maintainers have to choose to enable and integrate cloud-init into their base Azure published images. Once you have confirmed the image you want to deploy is cloud-init enabled, you can use the Azure CLI to deploy the image.

The first step in deploying this image is to create a resource group with the `az group create` command. An Azure resource group is a logical container into which Azure resources are deployed and managed.

The following example creates a resource group named `myResourceGroup` in the `eastus` location.

```
az group create --name myResourceGroup --location eastus
```

The next step is to create a file in your current shell, named *cloud-init.txt* and paste the following configuration. For this example, create the file in the Cloud Shell not on your local machine. You can use any editor you wish. Enter `sensible-editor cloud-init.txt` to create the file and see a list of available editors. Choose #1 to use the **nano** editor. Make sure that the whole cloud-init file is copied correctly, especially the first line:

```
#cloud-config
package_upgrade: true
packages:
- httpd
```

Press `ctrl-X` to exit the file, type `y` to save the file and press `enter` to confirm the file name on exit.

The final step is to create a VM with the `az vm create` command.

The following example creates a VM named *centos74* and creates SSH keys if they do not already exist in a default key location. To use a specific set of keys, use the `--ssh-key-value` option. Use the `--custom-data` parameter to pass in your cloud-init config file. Provide the full path to the *cloud-init.txt* config if you saved the file outside of your present working directory. The following example creates a VM named *centos74*:

```
az vm create \
--resource-group myResourceGroup \
--name centos74 \
--image OpenLogic:CentOS-CI:7-CI:latest \
--custom-data cloud-init.txt \
--generate-ssh-keys
```

When the VM has been created, the Azure CLI shows information specific to your deployment. Take note of the `publicIpAddress`. This address is used to access the VM. It takes some time for the VM to be created, the packages to install, and the app to start. There are background tasks that continue to run after the Azure CLI returns you to the prompt. You can SSH into the VM and use the steps outlined in the Troubleshooting section to view the cloud-init logs.

## Troubleshooting cloud-init

Once the VM has been provisioned, cloud-init will run through all the modules and script defined in `--custom-data` in order to configure the VM. If you need to troubleshoot any errors or omissions from the configuration, you need to search for the module name (`disk_setup` or `runcmd` for example) in the cloud-init log - located in **/var/log/cloud-init.log**.

### NOTE

Not every module failure results in a fatal cloud-init overall configuration failure. For example, using the `runcmd` module, if the script fails, cloud-init will still report provisioning succeeded because the runcmd module executed.

For more details of cloud-init logging, refer to the [cloud-init documentation](#)

## Next steps

For cloud-init examples of configuration changes, see the following documents:

- [Add an additional Linux user to a VM](#)

- Run a package manager to update existing packages on first boot
- Change VM local hostname
- Install an application package, update configuration files and inject keys

# Use cloud-init to set hostname for a Linux VM in Azure

11/13/2019 • 2 minutes to read • [Edit Online](#)

This article shows you how to use [cloud-init](#) to configure a specific hostname on a virtual machine (VM) or virtual machine scale sets (VMSS) at provisioning time in Azure. These cloud-init scripts run on first boot once the resources have been provisioned by Azure. For more information about how cloud-init works natively in Azure and the supported Linux distros, see [cloud-init overview](#)

## Set the hostname with cloud-init

By default, the hostname is the same as the VM name when you create a new virtual machine in Azure. To run a cloud-init script to change this default hostname when you create a VM in Azure with [az vm create](#), specify the cloud-init file with the `--custom-data` switch.

To see upgrade process in action, create a file in your current shell named `cloud_init_hostname.txt` and paste the following configuration. For this example, create the file in the Cloud Shell not on your local machine. You can use any editor you wish. Enter `sensible-editor cloud_init_hostname.txt` to create the file and see a list of available editors. Choose #1 to use the **nano** editor. Make sure that the whole cloud-init file is copied correctly, especially the first line.

```
#cloud-config
hostname: myhostname
```

Before deploying this image, you need to create a resource group with the [az group create](#) command. An Azure resource group is a logical container into which Azure resources are deployed and managed. The following example creates a resource group named `myResourceGroup` in the `eastus` location.

```
az group create --name myResourceGroup --location eastus
```

Now, create a VM with [az vm create](#) and specify the cloud-init file with `--custom-data cloud_init_hostname.txt` as follows:

```
az vm create \
--resource-group myResourceGroup \
--name centos74 \
--image OpenLogic:CentOS:7-CI:latest \
--custom-data cloud_init_hostname.txt \
--generate-ssh-keys
```

Once created, the Azure CLI shows information about the VM. Use the `publicIpAddress` to SSH to your VM. Enter your own address as follows:

```
ssh <publicIpAddress>
```

To see the VM name, use the `hostname` command as follows:

```
hostname
```

The VM should report the hostname as that value set in the cloud-init file, as shown in the following example output:

```
myhostname
```

## Next steps

For additional cloud-init examples of configuration changes, see the following:

- [Add an additional Linux user to a VM](#)
- [Run a package manager to update existing packages on first boot](#)
- [Change VM local hostname](#)
- [Install an application package, update configuration files and inject keys](#)

# Use cloud-init to update and install packages in a Linux VM in Azure

12/9/2019 • 2 minutes to read • [Edit Online](#)

This article shows you how to use [cloud-init](#) to update packages on a Linux virtual machine (VM) or virtual machine scale sets at provisioning time in Azure. These cloud-init scripts run on first boot once the resources have been provisioned by Azure. For more information about how cloud-init works natively in Azure and the supported Linux distros, see [cloud-init overview](#)

## Update a VM with cloud-init

For security purposes, you may want to configure a VM to apply the latest updates on first boot. As cloud-init works across different Linux distros, there is no need to specify `apt` or `yum` for the package manager. Instead, you define `package_upgrade` and let the cloud-init process determine the appropriate mechanism for the distro in use. This workflow allows you to use the same cloud-init scripts across distros.

To see upgrade process in action, create a file in your current shell named `cloud_init_upgrade.txt` and paste the following configuration. For this example, create the file in the Cloud Shell not on your local machine. You can use any editor you wish. Enter `sensible-editor cloud_init_upgrade.txt` to create the file and see a list of available editors. Choose #1 to use the **nano** editor. Make sure that the whole cloud-init file is copied correctly, especially the first line.

```
#cloud-config
package_upgrade: true
packages:
- httpd
```

Before deploying this image, you need to create a resource group with the [az group create](#) command. An Azure resource group is a logical container into which Azure resources are deployed and managed. The following example creates a resource group named `myResourceGroup` in the `eastus` location.

```
az group create --name myResourceGroup --location eastus
```

Now, create a VM with [az vm create](#) and specify the cloud-init file with `--custom-data cloud_init_upgrade.txt` as follows:

```
az vm create \
--resource-group myResourceGroup \
--name centos74 \
--image OpenLogic:CentOS:7-CI:latest \
--custom-data cloud_init_upgrade.txt \
--generate-ssh-keys
```

SSH to the public IP address of your VM shown in the output from the preceding command. Enter your own **publicIpAddress** as follows:

```
ssh <publicIpAddress>
```

Run the package management tool and check for updates.

```
sudo yum update
```

As cloud-init checked for and installed updates on boot, there should be no additional updates to apply. You see the update process, number of altered packages as well as the installation of `httpd` by running `yum history` and review the output similar to the one below.

```
Loaded plugins: fastestmirror, langpacks
ID | Command line | Date and time | Action(s) | Altered
-----+-----+-----+-----+-----+
 3 | -t -y install httpd | 2018-04-20 22:42 | Install | 5
 2 | -t -y upgrade | 2018-04-20 22:38 | I, U | 65
 1 | | 2017-12-12 20:32 | Install | 522
```

## Next steps

For additional cloud-init examples of configuration changes, see the following:

- [Add an additional Linux user to a VM](#)
- [Run a package manager to update existing packages on first boot](#)
- [Change VM local hostname](#)
- [Install an application package, update configuration files and inject keys](#)

# Use cloud-init to add a user to a Linux VM in Azure

11/13/2019 • 2 minutes to read • [Edit Online](#)

This article shows you how to use [cloud-init](#) to add a user on a virtual machine (VM) or virtual machine scale sets (VMSS) at provisioning time in Azure. This cloud-init script runs on first boot once the resources have been provisioned by Azure. For more information about how cloud-init works natively in Azure and the supported Linux distros, see [cloud-init overview](#).

## Add a user to a VM with cloud-init

One of the first tasks on any new Linux VM is to add an additional user for yourself to avoid the use of `root`. SSH keys are best practice for security and usability. Keys are added to the `~/.ssh/authorized_keys` file with this cloud-init script.

To add a user to a Linux VM, create a file in your current shell named `cloud_init_add_user.txt` and paste the following configuration. For this example, create the file in the Cloud Shell not on your local machine. You can use any editor you wish. Enter `sensible-editor cloud_init_add_user.txt` to create the file and see a list of available editors. Choose #1 to use the **nano** editor. Make sure that the whole cloud-init file is copied correctly, especially the first line. You need to provide your own public key (such as the contents of `~/.ssh/id_rsa.pub`) for the value of `ssh-authorized-keys:` - it has been shortened here to simplify the example.

```
#cloud-config
users:
 - default
 - name: myadminuser
 groups: sudo
 shell: /bin/bash
 sudo: ['ALL=(ALL) NOPASSWD:ALL']
 ssh-authorized-keys:
 - ssh-rsa AAAAB3
```

### NOTE

The `#cloud-config` file includes the `- default` parameter included. This will append the user, to the existing admin user created during provisioning. If you create a user without the `- default` parameter - the auto generated admin user created by the Azure platform would be overwritten.

Before deploying this image, you need to create a resource group with the [az group create](#) command. An Azure resource group is a logical container into which Azure resources are deployed and managed. The following example creates a resource group named `myResourceGroup` in the `eastus` location.

```
az group create --name myResourceGroup --location eastus
```

Now, create a VM with [az vm create](#) and specify the cloud-init file with `--custom-data cloud_init_add_user.txt` as follows:

```
az vm create \
--resource-group myResourceGroup \
--name centos74 \
--image OpenLogic:CentOS:7-CI:latest \
--custom-data cloud_init_add_user.txt \
--generate-ssh-keys
```

SSH to the public IP address of your VM shown in the output from the preceding command. Enter your own **publicIpAddress** as follows:

```
ssh <publicIpAddress>
```

To confirm your user was added to the VM and the specified groups, view the contents of the */etc/group* file as follows:

```
cat /etc/group
```

The following example output shows the user from the *cloud\_init\_add\_user.txt* file has been added to the VM and the appropriate group:

```
root:x:0:
<snip />
sudo:x:27:myadminuser
<snip />
myadminuser:x:1000:
```

## Next steps

For additional cloud-init examples of configuration changes, see the following:

- [Add an additional Linux user to a VM](#)
- [Run a package manager to update existing packages on first boot](#)
- [Change VM local hostname](#)
- [Install an application package, update configuration files and inject keys](#)

# Use cloud-init to configure a swap partition on a Linux VM

11/13/2019 • 2 minutes to read • [Edit Online](#)

This article shows you how to use [cloud-init](#) to configure the swap partition on various Linux distributions. The swap partition was traditionally configured by the Linux Agent (WALA) based on which distributions required one. This document will outline the process for building the swap partition on demand during provisioning time using cloud-init. For more information about how cloud-init works natively in Azure and the supported Linux distros, see [cloud-init overview](#)

## Create swap partition for Ubuntu based images

By default on Azure, Ubuntu gallery images do not create swap partitions. To enable swap partition configuration during VM provisioning time using cloud-init - please see the [AzureSwapPartitions document](#) on the Ubuntu wiki.

## Create swap partition for Red Hat and CentOS based images

Create a file in your current shell named *cloud\_init\_swappart.txt* and paste the following configuration. For this example, create the file in the Cloud Shell not on your local machine. You can use any editor you wish. Enter `sensible-editor cloud_init_swappart.txt` to create the file and see a list of available editors. Choose #1 to use the **nano** editor. Make sure that the whole cloud-init file is copied correctly, especially the first line.

```
#cloud-config
disk_setup:
 ephemeral0:
 table_type: gpt
 layout: [66, [33,82]]
 overwrite: true
fs_setup:
 - device: ephemeral0.1
 filesystem: ext4
 - device: ephemeral0.2
 filesystem: swap
mounts:
 - ["ephemeral0.1", "/mnt"]
 - ["ephemeral0.2", "none", "swap", "sw", "0", "0"]
```

Before deploying this image, you need to create a resource group with the [az group create](#) command. An Azure resource group is a logical container into which Azure resources are deployed and managed. The following example creates a resource group named *myResourceGroup* in the *eastus* location.

```
az group create --name myResourceGroup --location eastus
```

Now, create a VM with [az vm create](#) and specify the cloud-init file with `--custom-data cloud_init_swappart.txt` as follows:

```
az vm create \
--resource-group myResourceGroup \
--name centos74 \
--image OpenLogic:CentOS:7-CI:latest \
--custom-data cloud_init_swappart.txt \
--generate-ssh-keys
```

## Verify swap partition was created

SSH to the public IP address of your VM shown in the output from the preceding command. Enter your own **publicIpAddress** as follows:

```
ssh <publicIpAddress>
```

Once you have SSH'ed into the vm, check if the swap partition was created

```
swapon -s
```

The output from this command should look like this:

| Filename  | Type      | Size    | Used | Priority |
|-----------|-----------|---------|------|----------|
| /dev/sdb2 | partition | 2494440 | 0    | -1       |

### NOTE

If you have an existing Azure image that has a swap partition configured and you want to change the swap partition configuration for new images, you should remove the existing swap partition. Please see 'Customize Images to provision by cloud-init' document for more details.

## Next steps

For additional cloud-init examples of configuration changes, see the following:

- [Add an additional Linux user to a VM](#)
- [Run a package manager to update existing packages on first boot](#)
- [Change VM local hostname](#)
- [Install an application package, update configuration files and inject keys](#)

# Use cloud-init to run a bash script in a Linux VM in Azure

11/13/2019 • 2 minutes to read • [Edit Online](#)

This article shows you how to use [cloud-init](#) to run an existing bash script on a Linux virtual machine (VM) or virtual machine scale sets (VMSS) at provisioning time in Azure. These cloud-init scripts run on first boot once the resources have been provisioned by Azure. For more information about how cloud-init works natively in Azure and the supported Linux distros, see [cloud-init overview](#)

## Run a bash script with cloud-init

With cloud-init you do not need to convert your existing scripts into a cloud-config, cloud-init accepts multiple input types, one of which is a bash script.

If you have been using the Linux Custom Script Azure Extension to run your scripts, you can migrate them to use cloud-init. However, Azure Extensions have integrated reporting to alert to script failures, a cloud-init image deployment will NOT fail if the script fails.

To see this functionality in action, create a simple bash script for testing. Like the cloud-init `#cloud-config` file, this script must be local to where you will be running the Azure CLI commands to provision your virtual machine. For this example, create the file in the Cloud Shell not on your local machine. You can use any editor you wish. Enter `sensible-editor simple_bash.sh` to create the file and see a list of available editors. Choose #1 to use the **nano** editor. Make sure that the whole cloud-init file is copied correctly, especially the first line.

```
#!/bin/sh
echo "this has been written via cloud-init" + $(date) >> /tmp/myScript.txt
```

Before deploying this image, you need to create a resource group with the [az group create](#) command. An Azure resource group is a logical container into which Azure resources are deployed and managed. The following example creates a resource group named *myResourceGroup* in the *eastus* location.

```
az group create --name myResourceGroup --location eastus
```

Now, create a VM with [az vm create](#) and specify the bash script file with `--custom-data simple_bash.sh` as follows:

```
az vm create \
--resource-group myResourceGroup \
--name centos74 \
--image OpenLogic:CentOS:7-CI:latest \
--custom-data simple_bash.sh \
--generate-ssh-keys
```

## Verify bash script has run

SSH to the public IP address of your VM shown in the output from the preceding command. Enter your own **publicIpAddress** as follows:

```
ssh <publicIpAddress>
```

Change to the **/tmp** directory and verify that myScript.txt file exists and has the appropriate text inside of it. If it does not, you can check the **/var/log/cloud-init.log** for more details. Search for the following entry:

```
Running config-scripts-user using lock Running command ['/var/lib/cloud/instance/scripts/part-001']
```

## Next steps

For additional cloud-init examples of configuration changes, see the following:

- [Add an additional Linux user to a VM](#)
- [Run a package manager to update existing packages on first boot](#)
- [Change VM local hostname](#)
- [Install an application package, update configuration files and inject keys](#)

# Prepare an existing Linux Azure VM image for use with cloud-init

11/13/2019 • 3 minutes to read • [Edit Online](#)

This article shows you how to take an existing Azure virtual machine and prepare it to be redeployed and ready to use cloud-init. The resulting image can be used to deploy a new virtual machine or virtual machine scale sets - either of which could then be further customized by cloud-init at deployment time. These cloud-init scripts run on first boot once the resources have been provisioned by Azure. For more information about how cloud-init works natively in Azure and the supported Linux distros, see [cloud-init overview](#)

## Prerequisites

This document assumes you already have a running Azure virtual machine running a supported version of the Linux operating system. You have already configured the machine to suit your needs, installed all the required modules, processed all the required updates and have tested it to ensure it meets your requirements.

## Preparing RHEL 7.6 / CentOS 7.6

You need to SSH into your Linux VM and run the following commands in order to install cloud-init.

```
sudo yum makecache fast
sudo yum install -y gdisk cloud-utils-growpart
sudo yum install -y cloud-init
```

Update the `cloud_init_modules` section in `/etc/cloud/cloud.cfg` to include the following modules:

```
- disk_setup
- mounts
```

Here is a sample of what a general-purpose `cloud_init_modules` section looks like.

```
cloud_init_modules:
- migrator
- bootcmd
- write-files
- growpart
- resizefs
- disk_setup
- mounts
- set_hostname
- update_hostname
- update_etc_hosts
- rsyslog
- users-groups
- ssh
```

A number of tasks relating to provisioning and handling ephemeral disks need to be updated in `/etc/waagent.conf`. Run the following commands to update the appropriate settings.

```
sed -i 's/Provisioning.Enabled=y/Provisioning.Enabled=n/g' /etc/waagent.conf
sed -i 's/Provisioning.UseCloudInit=n/Provisioning.UseCloudInit=y/g' /etc/waagent.conf
sed -i 's/ResourceDisk.Format=y/ResourceDisk.Format=n/g' /etc/waagent.conf
sed -i 's/ResourceDisk.EnableSwap=y/ResourceDisk.EnableSwap=n/g' /etc/waagent.conf
cloud-init clean
```

Allow only Azure as a datasource for the Azure Linux Agent by creating a new file

/etc/cloud/cloud.cfg.d/91-azure\_datasource.cfg using an editor of your choice with the following line:

```
Azure Data Source config
datasource_list: [Azure]
```

If your existing Azure image has a swap file configured and you want to change the swap file configuration for new images using cloud-init, you need to remove the existing swap file.

For Red Hat based images - follow the instructions in the following Red Hat document explaining how to [remove the swap file](#).

For CentOS images with swapfile enabled, you can run the following command to turn off the swapfile:

```
sudo swapoff /mnt/resource/swapfile
```

Ensure the swapfile reference is removed from `/etc/fstab` - it should look something like the following output:

```
/etc/fstab
Accessible filesystems, by reference, are maintained under '/dev/disk'
See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=99cf66df-2fef-4aad-b226-382883643a1c / xfs defaults 0 0
UUID=7c473048-a4e7-4908-bad3-a9be22e9d37d /boot xfs defaults 0 0
```

To save space and remove the swap file you can run the following command:

```
rm /mnt/resource/swapfile
```

## Extra step for cloud-init prepared image

### NOTE

If your image was previously a **cloud-init** prepared and configured image, you need to do the following steps.

The following three commands are only used if the VM you are customizing to be a new specialized source image was previously provisioned by cloud-init. You do NOT need to run these if your image was configured using the Azure Linux Agent.

```
sudo cloud-init clean --logs
sudo waagent -deprovision+user -force
```

## Finalizing Linux Agent setting

All Azure platform images have the Azure Linux Agent installed, regardless if it was configured by cloud-init or not.

Run the following command to finish deprovisioning the user from the Linux machine.

```
sudo waagent -deprovision+user -force
```

For more information about the Azure Linux Agent deprovision commands, see the [Azure Linux Agent](#) for more details.

Exit the SSH session, then from your bash shell, run the following AzureCLI commands to deallocate, generalize and create a new Azure VM image. Replace `myResourceGroup` and `sourceVmName` with the appropriate information reflecting your sourceVM.

```
az vm deallocate --resource-group myResourceGroup --name sourceVmName
az vm generalize --resource-group myResourceGroup --name sourceVmName
az image create --resource-group myResourceGroup --name myCloudInitImage --source sourceVmName
```

## Next steps

For additional cloud-init examples of configuration changes, see the following:

- [Add an additional Linux user to a VM](#)
- [Run a package manager to update existing packages on first boot](#)
- [Change VM local hostname](#)
- [Install an application package, update configuration files and inject keys](#)

# Azure and Jenkins

2/26/2020 • 2 minutes to read • [Edit Online](#)

Jenkins is a popular open-source automation server used to set up continuous integration and delivery (CI/CD) for your software projects. You can host your Jenkins deployment in Azure or extend your existing Jenkins configuration using Azure resources. Jenkins plugins are also available to simplify CI/CD of your applications to Azure.

This article is an introduction to using Azure with Jenkins, detailing the core Azure features available to Jenkins users. For more information about getting started with your own Jenkins server in Azure, see [Create a Jenkins server on Azure](#).

## Host your Jenkins servers in Azure

Host Jenkins in Azure to centralize your build automation and scale your deployment as the needs of your software projects grow. You can deploy Jenkins in Azure using:

- [The Jenkins solution template](#) in Azure Marketplace.
- [Azure virtual machines](#). See our [tutorial](#) to create a Jenkins instance on a VM.
- On a Kubernetes cluster running in [Azure Container Service](#), see our [how-to](#).

Monitor and manage your Azure Jenkins deployment using [Azure Monitor logs](#) and the [Azure CLI](#).

## Scale your build automation on demand

Add build agents to your existing Jenkins deployment to scale your Jenkins build capacity as the number of builds and complexity of your jobs and pipelines increase. You can run these build agents on Azure virtual machines by using the [Azure VM Agents plug-in](#). See our [tutorial](#) for more details.

Once configured with an [Azure service principal](#), Jenkins jobs and pipelines can use this credential to:

- Securely store and archive build artifacts in [Azure Storage](#) using the [Azure Storage plug-in](#). Review the [Jenkins storage how-to](#) to learn more.
- Manage and configure Azure resources with the [Azure CLI](#).

## Deploy your code into Azure services

Use Jenkins plugins to deploy your applications to Azure as part of your Jenkins CI/CD pipelines. Deploying into [Azure App Service](#) and [Azure Container Service](#) lets you stage, test, and release updates to your applications without managing the underlying infrastructure.

Plug-ins are available to deploy to the following services and environments:

- [Azure App Service on Linux](#). See the [tutorial](#) to get started.
- [Azure App Service](#). See the [how-to](#) to get started.

# Create a Jenkins server on an Azure Linux VM from the Azure portal

11/18/2019 • 5 minutes to read • [Edit Online](#)

This quickstart shows how to install [Jenkins](#) on an Ubuntu Linux VM with the tools and plug-ins configured to work with Azure. When you're finished, you have a Jenkins server running in Azure building a sample Java app from [GitHub](#).

## Prerequisites

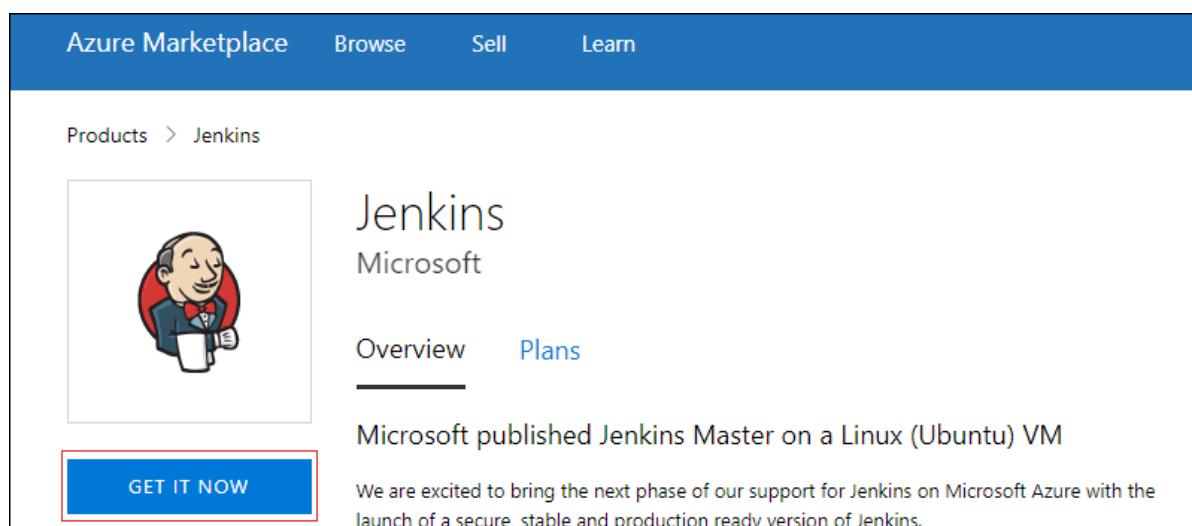
- An Azure subscription
- Access to SSH on your computer's command line (such as the Bash shell or [PuTTY](#))

If you don't have an [Azure subscription](#), create a [free account](#) before you begin.

## Create the Jenkins VM from the solution template

Jenkins supports a model where the Jenkins server delegates work to one or more agents to allow a single Jenkins installation to host a large number of projects or to provide different environments needed for builds or tests. The steps in this section guide you through installing and configuring a Jenkins server on Azure.

1. In your browser, open the [Azure Marketplace image for Jenkins](#).
2. Select **GET IT NOW**.



3. After reviewing the pricing details and terms information, select **Continue**.

## Create this app in Azure



Jenkins  
By Microsoft

### Software plan

Jenkins

Pricing: This solution template deploys software components and Azure infrastructure components. The price is the cost of those components.

Details: Microsoft published Jenkins Master on a Linux (Ubuntu) VM

I agree to the provider's [terms of use](#) and [privacy policy](#) and understand that the rights to use this product do not come from Microsoft, unless Microsoft is the provider. Use of Azure Marketplace is governed by separate [terms](#).

**Continue**

4. Select **Create** to configure the Jenkins server in the Azure portal.

 Jenkins  
Microsoft

We are excited to bring the next phase of our support for Jenkins on Microsoft Azure with the launch of a secure, stable and production ready version of Jenkins.

**Note:** For instructions on connecting to this Jenkins instance once deployed, please browse to the URL or public IP of this instance. The URL is the Domain name label you enter in Settings and the suffix shown below this field.

This solution template will install the latest stable Jenkins version on a Linux (Ubuntu 14.04 LTS) VM along with tools and plugins configured to work with Azure. This includes –

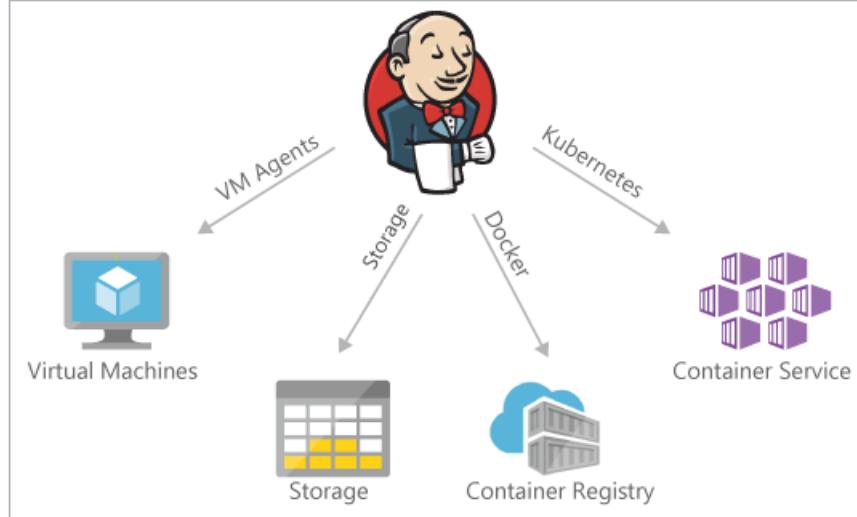
- git for source control
- Azure Credentials plugin for connecting securely
- Azure VM Agents plugin for elastic build, test and continuous integration
- Azure Storage plugin for storing artifacts
- Azure CLI to deploy apps using scripts

For a detailed walkthrough of the steps this solution automates for you, please visit our [blog post](#).

This solution template is designed to configure a Jenkins instance following best practices with minimal Azure knowledge. With a handful of user inputs and a simple single-click deployment through the Azure portal, you can provision a fully configured Jenkins instance in minutes, which can use Azure services anywhere across the globe.

[!\[\]\(6a9d7419638dc80c9d67e2be564b3c10\_img.jpg\)](#) [!\[\]\(b79e62a43c51fa077cd738b84f5daad9\_img.jpg\)](#) [!\[\]\(c97ae01cc0926ae5a960d42f1fb476b1\_img.jpg\)](#) [!\[\]\(54a7ba86d4ca9ad6e72598883a967b39\_img.jpg\)](#) [!\[\]\(b32445a53800560512f6397a22b5625d\_img.jpg\)](#) [!\[\]\(603545e9aa6d733673b2f49f7c1acf5d\_img.jpg\)](#)

---



**PUBLISHED**

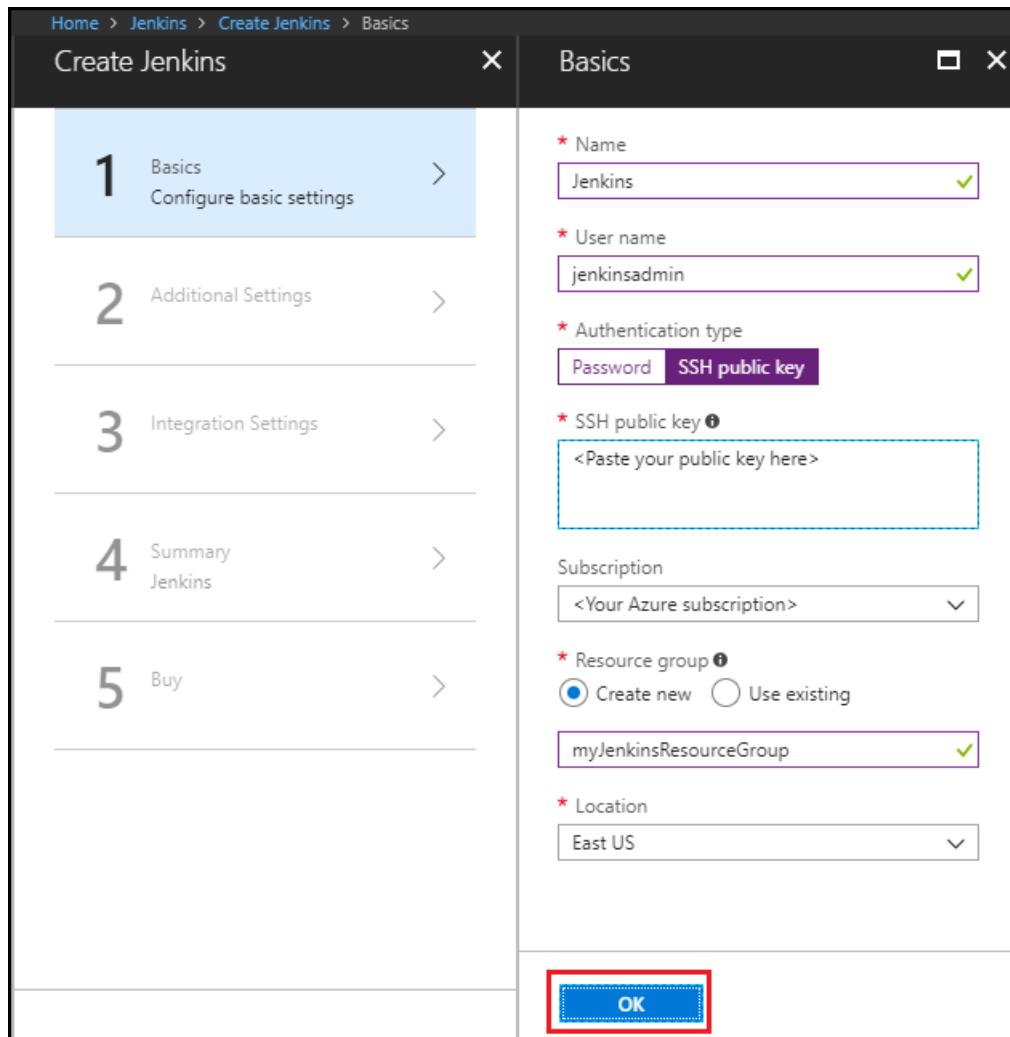
Select a deployment model [?](#)

5. In the **Basics** tab, specify the following values:

- **Name** - Enter `Jenkins`.
- **User name** - Enter the user name to use when signing in to the virtual machine on which Jenkins is running. The user name must meet [specific requirements](#).
- **Authentication type** - Select **SSH public key**.
- **SSH public key** - Copy and paste an RSA public key in single-line format (starting with `ssh-rsa`) or multi-line PEM format. You can generate SSH keys using ssh-keygen on Linux and macOS, or PuTTYGen on Windows. For more information about SSH keys and Azure, see the article, [How to](#)

Use SSH keys with Windows on Azure.

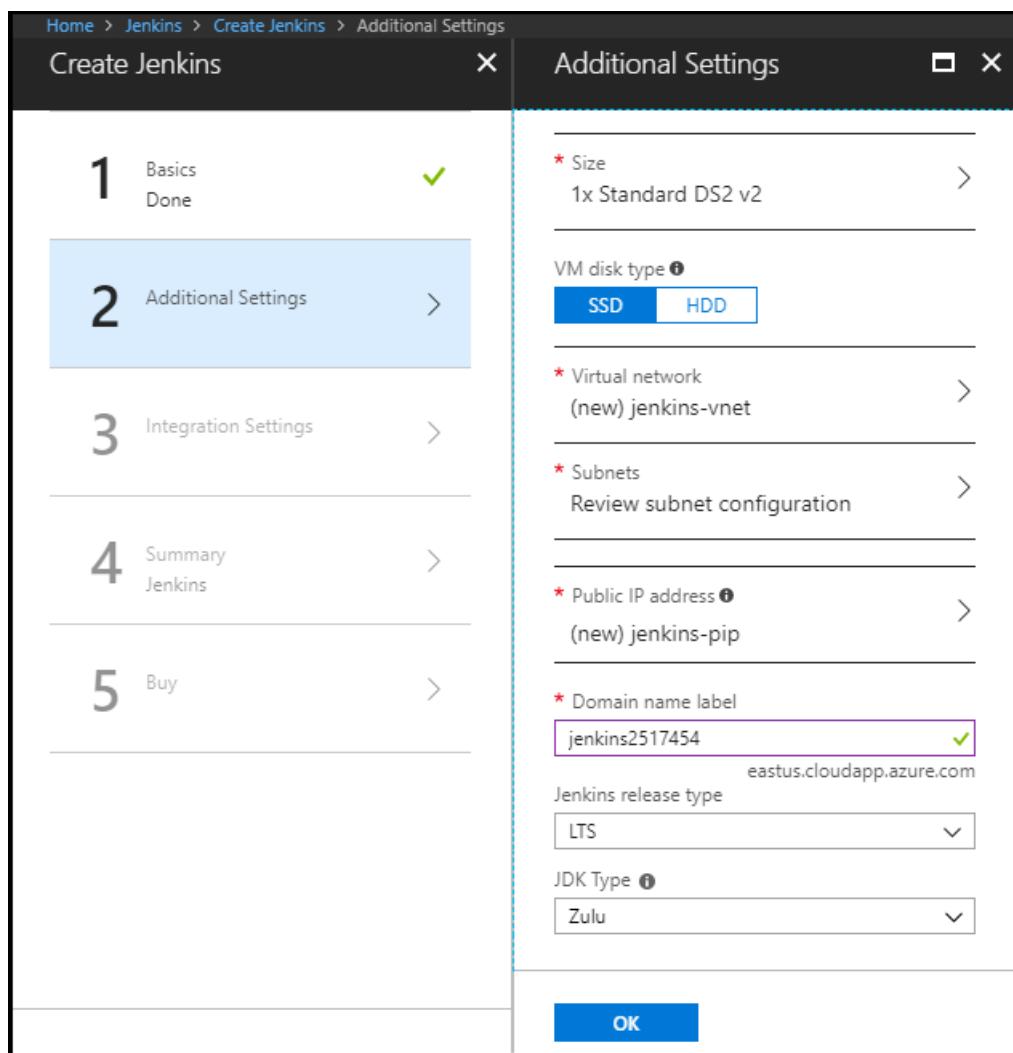
- **Subscription** - Select the Azure subscription into which you want to install Jenkins.
- **Resource group** - Select **Create new**, and enter a name for the resource group that serves as a logical container for the collection of resources that make up your Jenkins installation.
- **Location** - Select **East US**.



6. Select **OK** to proceed to the **Additional Settings** tab.
7. In the **Additional Settings** tab, specify the following values:
  - **Size** - Select the appropriate sizing option for your Jenkins virtual machine.
  - **VM disk type** - Specify either HDD (hard-disk drive) or SSD (solid-state drive) to indicate which storage disk type is allowed for the Jenkins virtual machine.
  - **Virtual network** - (Optional) Select **Virtual network** to modify the default settings.
  - **Subnets** - Select **Subnets**, verify the information, and select **OK**.
  - **Public IP address** - The IP address name defaults to the Jenkins name you specified in the previous page with a suffix of -IP. You can select the option to change that default.
  - **Domain name label** - Specify the value for the fully qualified URL to the Jenkins virtual machine.
  - **Jenkins release type** - Select the desired release type from the options: **LTS**, **Weekly build**, or **Azure Verified**. The **LTS** and **Weekly build** options are explained in the article, [Jenkins LTS Release Line](#). The **Azure Verified** option refers to a [Jenkins LTS version](#) that has been verified to run on

Azure.

- **JDK Type** - JDK to be installed. Default is Zulu tested, certified builds of OpenJDK.



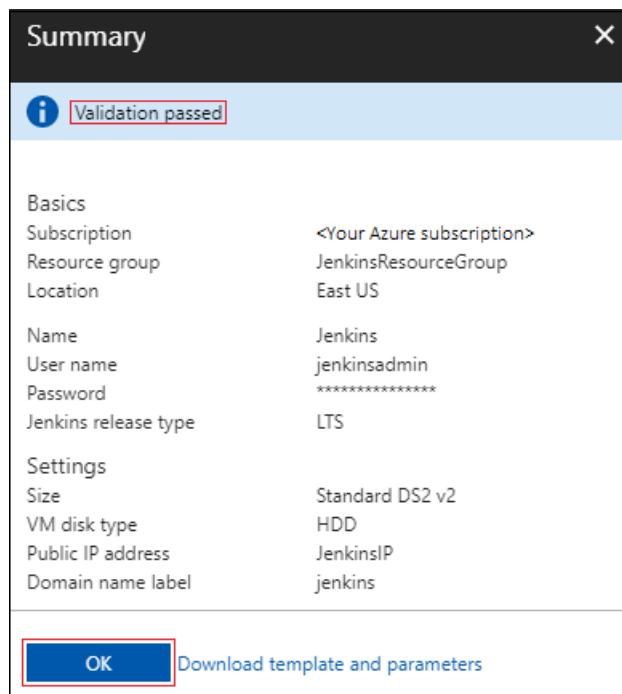
8. Select **OK** to proceed to the **Integration Settings** tab.

9. In the **Integration Settings** tab, specify the following values:

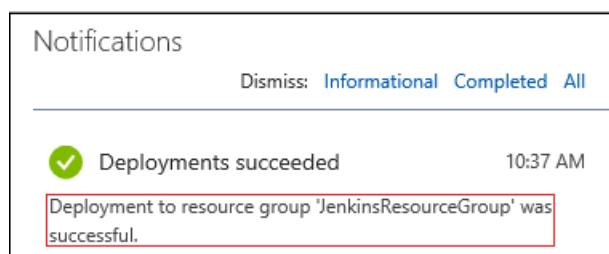
- **Service Principal** - The service principal is added into Jenkins as a credential for authentication with Azure. **Auto** means that the principal will be created by MSI (Managed Service Identity). **Manual** means that the principal should be created by you.
  - **Application ID** and **Secret** - If you select the **Manual** option for the **Service Principal** option, you'll need to specify the **Application ID** and **Secret** for your service principal. When [creating a service principal](#), note that the default role is **Contributor**, which is sufficient for working with Azure resources.
- **Enable Cloud Agents** - Specify the default cloud template for agents where **ACI** refers to Azure Container Instance, and **VM** refers to virtual machines. You can also specify **No** if you don't wish to enable a cloud agent.

10. Select **OK** to proceed to the **Summary** tab.

11. When the **Summary** tab displays, the information entered is validated. Once you see the **Validation passed** message (at the top of the tab), select **OK**.



12. When the **Create** tab displays, select **Create** to create the Jenkins virtual machine. When your server is ready, a notification displays in the Azure portal.



## Connect to Jenkins

Navigate to your virtual machine (for example, <http://jenkins2517454.eastus.cloudapp.azure.com/>) in your web browser. The Jenkins console is inaccessible through unsecured HTTP so instructions are provided on the page to access the Jenkins console securely from your computer using an SSH tunnel.

The screenshot shows the Jenkins On Azure landing page. At the top, there's a Jenkins logo and the word 'Jenkins'. Below that, a large banner with the text 'Jenkins On Azure'. The main content area contains the following text:

This Jenkins instance does not support https, so logging in through a public IP address has been disabled (it would expose your password and other information to eavesdropping). To securely login, you need to connect to the Jenkins instance using SSH port forwarding.

`ssh -L 127.0.0.1:8080:localhost:8080 username@jenkins2517454.eastus.cloudapp.azure.com`

If you don't want to publicly expose this Jenkins instance, you need to remove the nginx reverse-proxy.

`sudo apt-get purge nginx nginx-common`

Set up the tunnel using the `ssh` command on the page from the command line, replacing `username` with the name of the virtual machine admin user chosen earlier when setting up the virtual machine from the solution

template.

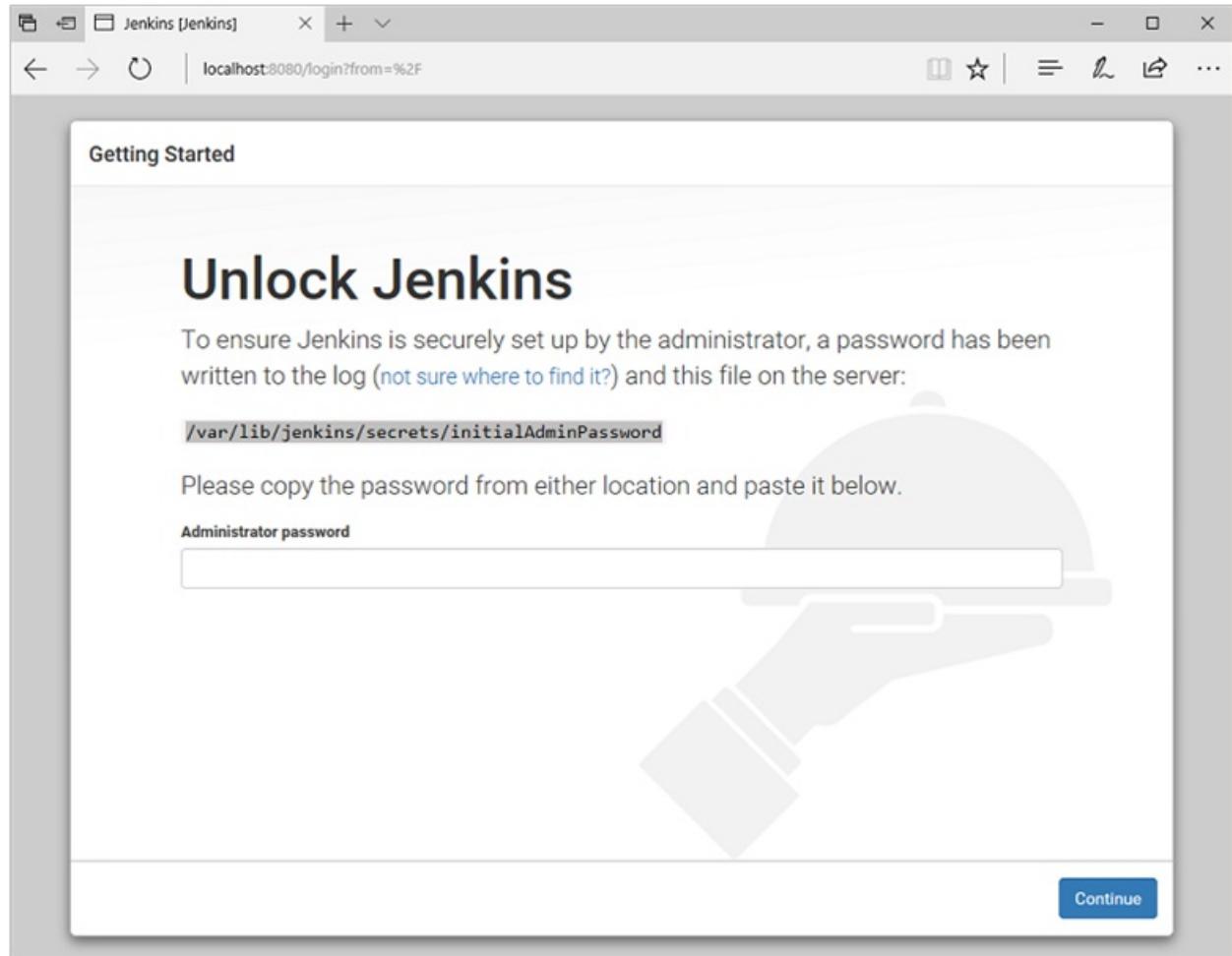
```
ssh -L 127.0.0.1:8080:localhost:8080 jenkinsadmin@jenkins2517454.eastus.cloudapp.azure.com
```

After you have started the tunnel, navigate to <http://localhost:8080/> on your local machine.

Get the initial password by running the following command in the command line while connected through SSH to the Jenkins VM.

```
sudo cat /var/lib/jenkins/secrets/initialAdminPassword
```

Unlock the Jenkins dashboard for the first time using this initial password.



Select **Install suggested plugins** on the next page and then create a Jenkins admin user used to access the Jenkins dashboard.

The screenshot shows the Jenkins dashboard at [localhost:8080](http://localhost:8080). The main header includes the Jenkins logo, a search bar, and links for Devops and log out. On the left, a sidebar lists options like New Item, People, Build History, Manage Jenkins, My Views, and Credentials. The central area features a large "Welcome to Jenkins!" message with a "create new jobs" link, and sections for Build Queue (empty) and Build Executor Status (1 Idle, 2 Idle). At the bottom, it shows the page was generated on Jun 19, 2017, at 6:02:58 PM UTC, with links to REST API and Jenkins version 2.46.3.

The Jenkins server is now ready to build code.

## Create your first job

Select **Create new jobs** from the Jenkins console, then name it **mySampleApp** and select **Freestyle project**, then select **OK**.

The screenshot shows the "Enter an item name" dialog. The item name "mySampleApp" is entered, and the "Freestyle project" option is selected, highlighted with a red box. Below it, there is descriptive text about Freestyle projects and Pipeline. The Pipeline section is partially visible.

Select the **Source Code Management** tab, enable **Git**, and enter the following URL in **Repository URL** field:

```
https://github.com/spring-guides/gs-spring-boot.git
```

## Source Code Management

The screenshot shows the Jenkins configuration interface for Source Code Management. The 'Git' option is selected. In the 'Repositories' section, there is one repository defined with the 'Repository URL' set to `https://github.com/spring-guides/gs-spring-boot.git`. A red box highlights this URL field.

Select the **Build** tab, then select **Add build step, Invoke Gradle script**. Select **Use Gradle Wrapper**, then enter `complete` in **Wrapper location** and `build` for **Tasks**.

The screenshot shows the Jenkins build step configuration for 'Invoke Gradle script'. The 'Use Gradle Wrapper' option is selected. The 'Wrapper location' field contains `complete` and the 'Tasks' field contains `build`. A red box highlights the 'Use Gradle Wrapper' radio button.

Select **Advanced** and then enter `complete` in the **Root Build script** field. Select **Save**.

The screenshot shows the Jenkins advanced configuration for the root build script. The 'Root Build script' field contains `complete`, which is highlighted with a red box.

## Build the code

Select **Build Now** to compile the code and package the sample app. When your build completes, select the **Workspace** link for the project.

The screenshot shows the Jenkins workspace for the project 'mySampleApp'. It features a 'Workspace' link next to a folder icon, both of which are highlighted with a red box. Below this, there is a 'Recent Changes' link. The 'Permalinks' section lists four recent builds.

| Link                        | Date       |
|-----------------------------|------------|
| Last build (#19)            | 13 sec ago |
| Last stable build (#19)     | 13 sec ago |
| Last successful build (#19) | 13 sec ago |
| Last completed build (#19)  | 13 sec ago |

Navigate to `complete/build/libs` and ensure the `gs-spring-boot-0.1.0.jar` is there to verify that your build was successful. Your Jenkins server is now ready to build your own projects in Azure.

# Troubleshooting the Jenkins solution template

If you encounter any bugs with the Jenkins solution template, file an issue in the [Jenkins GitHub repo](#).

## Next Steps

[Add Azure VMs as Jenkins agents](#)

# Scale your Jenkins deployments to meet demand with Azure VM agents

11/18/2019 • 4 minutes to read • [Edit Online](#)

This tutorial shows how to use the Jenkins [Azure VM Agents plugin](#) to add on-demand capacity with Linux virtual machines running in Azure.

In this tutorial, you will:

- Install the Azure VM Agents plugin
- Configure the plugin to create resources in your Azure subscription
- Set the compute resources available to each agent
- Set the operating system and tools installed on each agent
- Create a new Jenkins freestyle job
- Run the job on an Azure VM agent

## Prerequisites

- An Azure subscription
- A Jenkins master server. If you don't have one, view the [quickstart](#) to set up one in Azure.

If you don't have an [Azure subscription](#), create a [free account](#) before you begin.

## Install Azure VM Agents plugin

### TIP

If you deployed Jenkins on Azure using the [solution template](#), the Azure VM Agent plugin is already installed.

1. From the Jenkins dashboard, select **Manage Jenkins**, then select **Manage Plugins**.
2. Select the **Available** tab, then search for **Azure VM Agents**. Select the checkbox next to the entry for the plugin and select **Install without restart** from the bottom of the dashboard.

## Configure the Azure VM Agents plugin

1. From the Jenkins dashboard, select **Manage Jenkins**, then **Configure System**.
2. Scroll to the bottom of the page and find the **Cloud** section with the **Add new cloud** dropdown and choose **Microsoft Azure VM Agents**.
3. Select an existing service principal from **Add** drop-down in the **Azure Credentials** section. If none is listed, perform the following steps to [create a service principal](#) for your Azure account and add it to your Jenkins configuration:
  - a. Select **Add** next to **Azure Credentials** and choose **Jenkins**.
  - b. In the **Add Credentials** dialog, select **Microsoft Azure Service Principal** from the **Kind** drop-down.
  - c. Create an Active Directory Service principal from the Azure CLI or [Cloud Shell](#).

```
az ad sp create-for-rbac --name jenkins_sp --password secure_password
```

```
{
 "appId": "BBBBBBBB-BBBB-BBBB-BBBB-BBBBBBBBBB",
 "displayName": "jenkins_sp",
 "name": "http://jenkins_sp",
 "password": "secure_password",
 "tenant": "CCCCCCCC-CCCC-CCCC-CCCCCCCC"
}
```

d. Enter the credentials from the service principal into the **Add credentials** dialog. If you don't know your Azure subscription ID, you can query it from the CLI:

```
az account list
```

```
{
 "cloudName": "AzureCloud",
 "id": "AAAAAAA-AAAA-AAAA-AAAA-AAAAAAA",
 "isDefault": true,
 "name": "Visual Studio Enterprise",
 "state": "Enabled",
 "tenantId": "CCCCCCCC-CCCC-CCCC-CCCCCCCC",
 "user": {
 "name": "raisa@fabrikam.com",
 "type": "user"
 }
}
```

The completed service principal should use the `id` field for **Subscription ID**, the `appId` value for **Client ID**, `password` for **Client Secret**, and `tenant` for **Tenant ID**. Select **Add** to add the service principal and then configure the plugin to use the newly created credential.

The screenshot shows the 'Add Credentials' dialog with the following fields filled in:

- Domain:** Global credentials (unrestricted)
- Kind:** Microsoft Azure Service Principal
- Scope:** Global (Jenkins, nodes, items, all child items, etc)
- Subscription ID:** AAAAAAAA-AAAA-AAAA-AAAA-AAAAAAA
- Client ID:** BBBBCCCC-BBBB-BBBB-BBBB-BBBBBBBB
- Client Secret:** (redacted)
- Or, Certificate:** --- Select a Certificate --- (dropdown menu) | Add (button)
- Tenant ID:** CCCCCCCC-CCCC-CCCC-CCCC-CCCCCC
- Azure Environment:** Azure

- In the **Resource Group Name** section, leave **Create new** selected and enter `myJenkinsAgentGroup`.
- Select **Verify configuration** to connect to Azure to test the profile settings.

6. Select **Apply** to update the plugin configuration.

## Configure agent resources

Configure a template for use to define an Azure VM agent. This template defines the compute resources each agent has when created.

1. Select **Add** next to **Add Azure Virtual Machine Template**.
2. Enter `defaulttemplate` for the **Name**
3. Enter `ubuntu` for the **Label**
4. Select the desired [Azure region](#) from the combo box.
5. Select a [VM size](#) from the drop-down under **Virtual Machine Size**. A general-purpose `Standard_DS1_v2` size is fine for this tutorial.
6. Leave the **Retention time** at `60`. This setting defines the number of minutes Jenkins can wait before it deallocated idle agents. Specify 0 if you do not want idle agents to be removed automatically.

| General Configuration                              |                                                                                  |
|----------------------------------------------------|----------------------------------------------------------------------------------|
| Name                                               | <input type="text" value="defaulttemplate"/> <a href="#">?</a>                   |
| Description                                        | <input type="text"/> <a href="#">?</a>                                           |
| Labels                                             | <input type="text" value="ubuntu"/> <a href="#">?</a>                            |
| Region                                             | <input type="text" value="East US"/> <a href="#">?</a>                           |
| Virtual Machine Size                               | <input type="text" value="Standard_DS1_v2"/> <a href="#">?</a>                   |
| Storage Account Name                               | <input type="text" value="jnhwip6riim7wcpt1n9pfa"/> <a href="#">?</a>            |
| Retention Time (in minutes)                        | <input type="text" value="60"/> <a href="#">?</a>                                |
| Shutdown Only (Do Not Delete) After Retention Time | <input type="checkbox"/>                                                         |
| Usage                                              | <input type="text" value="Use this node as much as possible"/> <a href="#">?</a> |

## Configure agent operating system and tools

In the **Image Configuration** section of the plugin configuration, select **Ubuntu 16.04 LTS**. Check the boxes next to **Install Git (Latest)**, **Install Maven (V3.5.0)**, and **Install Docker** to install these tools on newly created agents.

| Image Configuration                                 |                                                                 |
|-----------------------------------------------------|-----------------------------------------------------------------|
| <input checked="" type="radio"/> Use Built-In Image | <input type="text" value="Ubuntu 16.04 LTS"/> <a href="#">?</a> |
| Pre-installed Tools                                 |                                                                 |
| Install Git (Latest)                                | <input checked="" type="checkbox"/>                             |
| Install Maven (V3.5.0)                              | <input checked="" type="checkbox"/>                             |
| Install Docker (Only for Linux)                     | <input checked="" type="checkbox"/>                             |

Select **Add** next to **Admin Credentials**, then select **Jenkins**. Enter a username and password used to sign in to the agents, making sure they satisfy the [username and password policy](#) for administrative accounts on Azure VMs.

Select **Verify Template** to verify the configuration and then select **Save** to save your changes and return to the Jenkins dashboard.

## Create a job in Jenkins

1. Within the Jenkins dashboard, click **New Item**.
2. Enter `demoproject1` for the name and select **Freestyle project**, then select **OK**.
3. In the **General** tab, choose **Restrict where project can be run** and type `ubuntu` in **Label Expression**. You see a message confirming that the label is served by the cloud configuration created in the previous step.

The screenshot shows the Jenkins 'General' configuration page for a new project. The 'Project name' is set to 'demoproject1'. Under 'Restrict where this project can be run', the 'Label Expression' is set to 'ubuntu'. A note below the expression states 'Label ubuntu is serviced by no nodes and 1 cloud'. There are several other optional checkboxes listed, such as 'Enable project-based security', 'Discard old builds', and 'GitHub project', none of which are checked.

4. In the **Source Code Management** tab, select **Git** and add the following URL into the **Repository URL** field:  
`https://github.com/spring-projects/spring-petclinic.git`
5. In the **Build** tab, select **Add build step**, then **Invoke top-level Maven targets**. Enter `package` in the **Goals** field.
6. Select **Save** to save the job definition.

## Build the new job on an Azure VM agent

1. Go back to the Jenkins dashboard.
2. Select the job you created in the previous step, then click **Build now**. A new build is queued, but does not start until an agent VM is created in your Azure subscription.
3. Once the build is complete, go to **Console output**. You see that the build was performed remotely on an Azure agent.



## Console Output

Started by user Devops

Building remotely on [defaulttemplate45db20](#) (ubuntu) in workspace /home/devops/workspace/demoproject1

Finished: SUCCESS

## Troubleshooting the Jenkins plugin

If you encounter any bugs with the Jenkins plugins, file an issue in the [Jenkins JIRA](#) for the specific component.

## Next steps

[CI/CD to Azure App Service](#)

# Using Azure Storage with a Jenkins continuous integration solution

2/26/2020 • 9 minutes to read • [Edit Online](#)

This article illustrates how to use Blob storage as a repository of build artifacts created by a Jenkins continuous integration (CI) solution, or as a source of downloadable files to be used in a build process. One of the scenarios where you would find this solution useful is when you're coding in an agile development environment (using Java or other languages), builds are running based on continuous integration, and you need a repository for your build artifacts, so that you could, for example, share them with other organization members, your customers, or maintain an archive. Another scenario is when your build job itself requires other files, for example, dependencies to download as part of the build input.

In this tutorial, you will be using the Azure Storage Plugin for Jenkins CI made available by Microsoft.

## Jenkins overview

Jenkins enables continuous integration of a software project by allowing developers to easily integrate their code changes and have builds produced automatically and frequently, thereby increasing the productivity of the developers. Builds are versioned, and build artifacts can be uploaded to various repositories. This article shows how to use Azure blob storage as the repository of the build artifacts. It will also show how to download dependencies from Azure blob storage.

More information about Jenkins can be found at [Meet Jenkins](#).

## Benefits of using the Blob service

Benefits of using the Blob service to host your agile development build artifacts include:

- High availability of your build artifacts and/or downloadable dependencies.
- Performance when your Jenkins CI solution uploads your build artifacts.
- Performance when your customers and partners download your build artifacts.
- Control over user access policies, with a choice between anonymous access, expiration-based shared access signature access, private access, etc.

## Prerequisites

- A Jenkins continuous integration solution.

If you currently don't have a Jenkins CI solution, you can run a Jenkins CI solution using the following technique:

1. On a Java-enabled machine, download jenkins.war from <https://jenkins-ci.org>.
2. At a command prompt that is opened to the folder that contains jenkins.war, run:

```
java -jar jenkins.war
```

3. In your browser, open <http://localhost:8080/> to open the Jenkins dashboard, which you will use to install and configure the Azure Storage plugin.

While a typical Jenkins CI solution would be set up to run as a service, running the Jenkins war at the command line will be sufficient for this tutorial.

- An Azure account. You can sign up for an Azure account at <https://www.azure.com>.
- An Azure storage account. If you don't already have a storage account, you can create one using the steps at [Create a Storage Account](#).
- Familiarity with the Jenkins CI solution is recommended but not required, as the following content will use a basic example to show you the steps needed when using the Blob service as a repository for Jenkins CI build artifacts.

## How to use the Blob service with Jenkins CI

To use the Blob service with Jenkins, you'll need to install the Azure Storage plugin, configure the plugin to use your storage account, and then create a post-build action that uploads your build artifacts to your storage account. These steps are described in the following sections.

## How to install the Azure Storage plugin

1. Within the Jenkins dashboard, select **Manage Jenkins**.
2. In the **Manage Jenkins** page, select **Manage Plugins**.
3. Select the **Available** tab.
4. In the **Artifact Uploaders** section, check **Microsoft Azure Storage plugin**.
5. Select either **Install without restart** or **Download now and install after restart**.
6. Restart Jenkins.

## How to configure the Azure Storage plugin to use your storage account

1. Within the Jenkins dashboard, select **Manage Jenkins**.
2. In the **Manage Jenkins** page, select **Configure System**.
3. In the **Microsoft Azure Storage Account Configuration** section:
  - a. Enter your storage account name, which you can obtain from the [Azure portal](#).
  - b. Enter your storage account key, also obtainable from the [Azure portal](#).
  - c. Use the default value for **Blob Service Endpoint URL** if you are using the global Azure cloud. If you are using a different Azure cloud, use the endpoint as specified in the [Azure portal](#) for your storage account.
  - d. Select **Validate storage credentials** to validate your storage account.
  - e. [Optional] If you have additional storage accounts that you want made available to your Jenkins CI, select **Add more Storage Accounts**.
  - f. Select **Save** to save your settings.

## How to create a post-build action that uploads your build artifacts to your storage account

For instructional purposes, you first need to create a job that will create several files, and then add in the post-build action to upload the files to your storage account.

1. Within the Jenkins dashboard, select **New Item**.
2. Name the job **MyJob**, select **Build a free-style software project**, and then select **OK**.
3. In the **Build** section of the job configuration, select **Add build step** and select **Execute Windows batch command**.

4. In **Command**, use the following commands:

```
md text
cd text
echo Hello Azure Storage from Jenkins > hello.txt
date /t > date.txt
time /t >> date.txt
```

5. In the **Post-build Actions** section of the job configuration, select **Add post-build action** and select **Upload artifacts to Azure Blob storage**.
6. For **Storage account name**, select the storage account to use.
7. For **Container name**, specify the container name. (The container will be created if it does not already exist when the build artifacts are uploaded.) You can use environment variables, so for this example enter  `${JOB_NAME}` as the container name.

#### Tip

Below the **Command** section where you entered a script for **Execute Windows batch command** is a link to the environment variables recognized by Jenkins. Select that link to learn the environment variable names and descriptions. Environment variables that contain special characters, such as the **BUILD\_URL** environment variable, are not allowed as a container name or common virtual path.

8. Select **Make new container public by default** for this example. (If you want to use a private container, you'll need to create a shared access signature to allow access, which is beyond the scope of this article. You can learn more about shared access signatures at [Using Shared Access Signatures \(SAS\)](#).)
9. [Optional] Select **Clean container before uploading** if you want the container to be cleared of contents before build artifacts are uploaded (leave it unchecked if you do not want to clean the contents of the container).
10. For **List of Artifacts to upload**, enter `text/*.txt`.
11. For **Common virtual path for uploaded artifacts**, for purposes of this tutorial, enter  `${BUILD\_ID}/${BUILD\_NUMBER}` .
12. Select **Save** to save your settings.
13. In the Jenkins dashboard, select **Build Now** to run **MyJob**. Examine the console output for status. Status messages for Azure storage will be included in the console output when the post-build action starts to upload build artifacts.
14. Upon successful completion of the job, you can examine the build artifacts by opening the public blob.
  - Sign in to the [Azure portal](#).
  - Select **Storage**.
  - Select the storage account name that you used for Jenkins.
  - Select **Containers**.
  - Select the container named **myjob**, which is the lowercase version of the job name that you assigned when you created the Jenkins job. Container names and blob names are lowercase (and case-sensitive) in Azure storage. Within the list of blobs for the container named **myjob**, you should see **hello.txt** and **date.txt**. Copy the URL for either of these items and open it in your browser. You will see the text file that was uploaded as a build artifact.

Only one post-build action that uploads artifacts to Azure blob storage can be created per job. The single post-build action to upload artifacts to Azure blob storage can specify different files (including wildcards) and paths to files within **List of Artifacts to upload** using a semi-colon as a separator. For example, if your Jenkins build

produces JAR files and TXT files in your workspace's **build** folder, and you want to upload both to Azure blob storage, use the following value for the **List of Artifacts to upload** option: `build/*.jar;build/*.txt`. You can also use double-colon syntax to specify a path to use within the blob name. For example, if you want the JARs to get uploaded using **binaries** in the blob path and the TXT files to get uploaded using **notices** in the blob path, use the following value for the **List of Artifacts to upload** option: `build/*.jar::binaries;build/*.txt::notices`.

## How to create a build step that downloads from Azure blob storage

The following steps illustrate to configure a build step to download items from Azure blob storage, which is useful if you want to include items in your build. An example of using this pattern is JARs that you might want to persist in Azure blob storage.

1. In the **Build** section of the job configuration, select **Add build step** and select **Download from Azure Blob storage**.
2. For **Storage account name**, select the storage account to use.
3. For **Container name**, specify the name of the container that has the blobs you want to download. You can use environment variables.
4. For **Blob name**, specify the blob name. You can use environment variables. Also, you can use an asterisk, as a wildcard after you specify the initial letter(s) of the blob name. For example, `project\*` would specify all blobs whose names start with `project`.
5. [Optional] For **Download path**, specify the path on the Jenkins machine where you want to download files from Azure blob storage. Environment variables can also be used. (If you do not provide a value for **Download path**, the files from Azure blob storage will be downloaded to the job's workspace.)

If you have additional items you want to download from Azure blob storage, you can create additional build steps.

After you run a build, you can check the build history console output, or look at your download location, to see whether the blobs you expected were successfully downloaded.

## Components used by the Blob service

This section provides an overview of the Blob service components.

- **Storage Account:** All access to Azure Storage is done through a storage account. A storage account is the highest level of the namespace for accessing blobs. An account can contain an unlimited number of containers, as long as their total size is under 100 TB.
- **Container:** A container provides a grouping of a set of blobs. All blobs must be in a container. An account can contain an unlimited number of containers. A container can store an unlimited number of blobs.
- **Blob:** A file of any type and size. There are two types of blobs that can be stored in Azure Storage: block and page blobs. Most files are block blobs. A single block blob can be up to 200 GB in size. This tutorial uses block blobs. Page blobs, another blob type, can be up to 1 TB in size, and are more efficient when ranges of bytes in a file are modified frequently. For more information about blobs, see [Understanding Block Blobs, Append Blobs, and Page Blobs](#).
- **URL format:** Blobs are addressable using the following URL format:

```
http://storageaccount.blob.core.windows.net/container_name/blob_name
```

(The format above applies to the global Azure cloud. If you are using a different Azure cloud, use the endpoint within the [Azure portal](#) to determine your URL endpoint.)

In the format above, `storageaccount` represents the name of your storage account, `container_name` represents the name of your container, and `blob_name` represents the name of your blob, respectively. Within the container name, you can have multiple paths, separated by a forward slash, `/`. The example

container name used for this tutorial was **MyJob**, and  **\${BUILD\_ID}/ \${BUILD\_NUMBER}** was used for the common virtual path, resulting in the blob having a URL of the following form:

```
http://example.blob.core.windows.net/myjob/2014-04-14_23-57-00/1/hello.txt
```

## Troubleshooting the Jenkins plugin

If you encounter any bugs with the Jenkins plugins, file an issue in the [Jenkins JIRA](#) for the specific component.

## Next steps

[Jenkins on Azure](#)

2 minutes to read

# How to use Docker Machine to create hosts in Azure

11/13/2019 • 3 minutes to read • [Edit Online](#)

This article details how to use [Docker Machine](#) to create hosts in Azure. The `docker-machine` command creates a Linux virtual machine (VM) in Azure then installs Docker. You can then manage your Docker hosts in Azure using the same local tools and workflows. To use docker-machine in Windows 10, you must use Linux bash.

## Create VMs with Docker Machine

First, obtain your Azure subscription ID with `az account show` as follows:

```
sub=$(az account show --query "id" -o tsv)
```

You create Docker host VMs in Azure with `docker-machine create` by specifying `azure` as the driver. For more information, see the [Docker Azure Driver documentation](#)

The following example creates a VM named `myVM`, based on "Standard D2 v2" plan, creates a user account named `azureuser`, and opens port `80` on the host VM. Follow any prompts to log in to your Azure account and grant Docker Machine permissions to create and manage resources.

```
docker-machine create -d azure \
--azure-subscription-id $sub \
--azure-ssh-user azureuser \
--azure-open-port 80 \
--azure-size "Standard_DS2_v2" \
myvm
```

The output looks similar to the following example:

```
Creating CA: /Users/user/.docker/machine/certs/ca.pem
Creating client certificate: /Users/user/.docker/machine/certs/cert.pem
Running pre-create checks...
(myvm) Completed machine pre-create checks.
Creating machine...
(myvm) Querying existing resource group. name="docker-machine"
(myvm) Creating resource group. name="docker-machine" location="westus"
(myvm) Configuring availability set. name="docker-machine"
(myvm) Configuring network security group. name="myvm-firewall" location="westus"
(myvm) Querying if virtual network already exists. rg="docker-machine" location="westus" name="docker-machine-vnet"
(myvm) Creating virtual network. name="docker-machine-vnet" rg="docker-machine" location="westus"
(myvm) Configuring subnet. name="docker-machine" vnet="docker-machine-vnet" cidr="192.168.0.0/16"
(myvm) Creating public IP address. name="myvm-ip" static=false
(myvm) Creating network interface. name="myvm-nic"
(myvm) Creating storage account. sku=Standard_LRS name="vhdski0hvfazyd8mn991cg50" location="westus"
(myvm) Creating virtual machine. location="westus" size="Standard_A2" username="azureuser"
osImage="canonical:UbuntuServer:16.04.0-LTS:latest" name="myvm"
Waiting for machine to be running, this may take a few minutes...
Detecting operating system of created instance...
Waiting for SSH to be available...
Detecting the provisioner...
Provisioning with ubuntu(systemd)...
Installing Docker...
Copying certs to the local machine directory...
Copying certs to the remote machine...
Setting Docker configuration on the remote daemon...
Checking connection to Docker...
Docker is up and running!
To see how to connect your Docker Client to the Docker Engine running on this virtual machine, run: docker-machine env myvm
```

## Configure your Docker shell

To connect to your Docker host in Azure, define the appropriate connection settings. As noted at the end of the output, view the connection information for your Docker host as follows:

```
docker-machine env myvm
```

The output is similar to the following example:

```
export DOCKER_TLS_VERIFY="1"
export DOCKER_HOST="tcp://40.68.254.142:2376"
export DOCKER_CERT_PATH="/Users/user/.docker/machine/machines/machine"
export DOCKER_MACHINE_NAME="machine"
Run this command to configure your shell:
eval $(docker-machine env myvm)
```

To define the connection settings, you can either run the suggested configuration command (`eval $(docker-machine env myvm)`), or you can set the environment variables manually.

## Run a container

To see a container in action, let's run a basic NGINX webserver. Create a container with `docker run` and expose port 80 for web traffic as follows:

```
docker run -d -p 80:80 --restart=always nginx
```

The output is similar to the following example:

```
Unable to find image 'nginx:latest' locally
latest: Pulling from library/nginx
ff3d52d8f55f: Pull complete
226f4ec56ba3: Pull complete
53d7dd52b97d: Pull complete
Digest: sha256:41ad9967ea448d7c2b203c699b429abe1ed5af331cd92533900c6d77490e0268
Status: Downloaded newer image for nginx:latest
675e6056cb81167fe38ab98bf397164b01b998346d24e567f9eb7a7e94fba14a
```

View running containers with `docker ps`. The following example output shows the NGINX container running with port 80 exposed:

| CONTAINER ID       | IMAGE | COMMAND                 | CREATED       | STATUS       | PORTS                       |
|--------------------|-------|-------------------------|---------------|--------------|-----------------------------|
| NAMES              |       |                         |               |              |                             |
| d5b78f27b335       | nginx | "nginx -g 'daemon off'" | 5 minutes ago | Up 5 minutes | 0.0.0.0:80->80/tcp, 443/tcp |
| festive_mirzakhani |       |                         |               |              |                             |

## Test the container

Obtain the public IP address of Docker host as follows:

```
docker-machine ip myvm
```

To see the container in action, open a web browser and enter the public IP address noted in the output of the preceding command:



## Next steps

For examples on using Docker Compose, see [Get started with Docker and Compose in Azure](#).

# Get started with Docker and Compose to define and run a multi-container application in Azure

11/13/2019 • 3 minutes to read • [Edit Online](#)

With [Compose](#), you use a simple text file to define an application consisting of multiple Docker containers. You then spin up your application in a single command that does everything to deploy your defined environment. As an example, this article shows you how to quickly set up a WordPress blog with a backend MariaDB SQL database on an Ubuntu VM. You can also use Compose to set up more complex applications.

This article was last tested on 2/14/2019 using the [Azure Cloud Shell](#) and the [Azure CLI](#) version 2.0.58.

## Create Docker host with Azure CLI

Install the latest [Azure CLI](#) and log in to an Azure account using [az login](#).

First, create a resource group for your Docker environment with [az group create](#). The following example creates a resource group named *myResourceGroup* in the *eastus* location:

```
az group create --name myDockerGroup --location eastus
```

Create a file named *cloud-init.txt* and paste the following configuration. Enter `sensible-editor cloud-init.txt` to create the file and see a list of available editors.

```
#include https://get.docker.com
```

Now create a VM with [az vm create](#). Use the `--custom-data` parameter to pass in your cloud-init config file. Provide the full path to the *cloud-init.txt* config if you saved the file outside of your present working directory. The following example creates a VM named *myDockerVM* and opens port 80 to web traffic.

```
az vm create \
 --resource-group myDockerGroup \
 --name myDockerVM \
 --image UbuntuLTS \
 --admin-username azureuser \
 --generate-ssh-keys \
 --custom-data cloud-init.txt
az vm open-port --port 80 \
 --resource-group myDockerGroup \
 --name myDockerVM
```

It takes a few minutes for the VM to be created, the packages to install, and the app to start. There are background tasks that continue to run after the Azure CLI returns you to the prompt. When the VM has been created, take note of the `publicIpAddress` displayed by the Azure CLI.

## Install Compose

SSH to your new Docker host VM. Provide your own IP address.

```
ssh azureuser@10.10.111.11
```

Install Compose on the VM.

```
sudo apt install docker-compose
```

## Create a docker-compose.yml configuration file

Create a `docker-compose.yml` configuration file to define the Docker containers to run on the VM. The file specifies the image to run on each container, necessary environment variables and dependencies, ports, and the links between containers. For details on yml file syntax, see [Compose file reference](#).

Create a `docker-compose.yml` file. Use your favorite text editor to add some data to the file. The following example creates the file with a prompt for `sensible-editor` to pick an editor that you wish to use.

```
sensible-editor docker-compose.yml
```

Paste the following example into your Docker Compose file. This configuration uses images from the [DockerHub Registry](#) to install WordPress (the open source blogging and content management system) and a linked backend MariaDB SQL database. Enter your own `MYSQL_ROOT_PASSWORD`.

```
wordpress:
 image: wordpress
 links:
 - db:mysql
 ports:
 - 80:80

db:
 image: mariadb
 environment:
 MYSQL_ROOT_PASSWORD: <your password>
```

## Start the containers with Compose

In the same directory as your `docker-compose.yml` file, run the following command (depending on your environment, you might need to run `docker-compose` using `sudo`):

```
sudo docker-compose up -d
```

This command starts the Docker containers specified in `docker-compose.yml`. It takes a minute or two for this step to complete. You'll see output similar to the following:

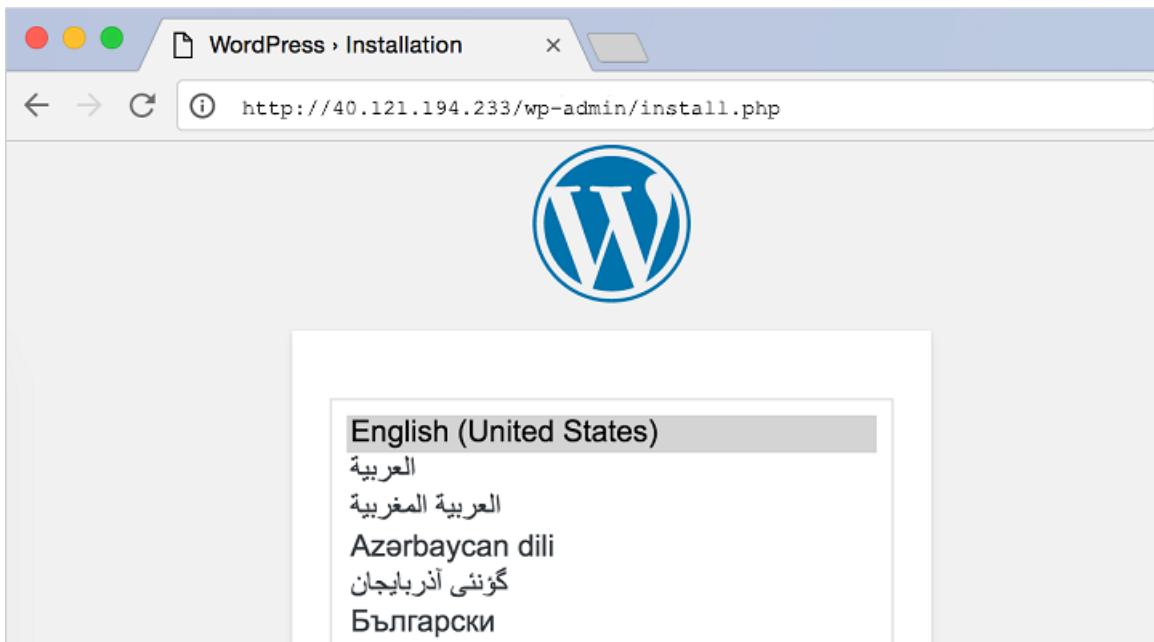
```
Creating wordpress_db_1...
Creating wordpress_wordpress_1...
...
```

To verify that the containers are up, type `sudo docker-compose ps`. You should see something like:

| Name                  | Command                        | State | Ports              |
|-----------------------|--------------------------------|-------|--------------------|
| azureuser_db_1        | docker-entrypoint.sh mysqld    | Up    | 3306/tcp           |
| azureuser_wordpress_1 | docker-entrypoint.sh apach ... | Up    | 0.0.0.0:80->80/tcp |

You can now connect to WordPress directly on the VM on port 80. Open a web browser and enter the IP address

name of your VM. You should now see the WordPress start screen, where you can complete the installation and get started with the application.



## Next steps

- Check out the [Compose command-line reference](#) and [user guide](#) for more examples of building and deploying multi-container apps.
- Use an Azure Resource Manager template, either your own or one contributed from the [community](#), to deploy an Azure VM with Docker and an application set up with Compose. For example, the [Deploy a WordPress blog with Docker](#) template uses Docker and Compose to quickly deploy WordPress with a MySQL backend on an Ubuntu VM.
- Try integrating Docker Compose with a Docker Swarm cluster. See [Using Compose with Swarm](#) for scenarios.

# Cloud Foundry on Azure

11/13/2019 • 2 minutes to read • [Edit Online](#)

Cloud Foundry is an open-source platform-as-a-service (PaaS) for building, deploying, and operating 12-factor applications developed in various languages and frameworks. This document describes the options you have for running Cloud Foundry on Azure and how you can get started.

## Cloud Foundry offerings

There are two forms of Cloud Foundry available to run on Azure: open-source Cloud Foundry (OSS CF) and Pivotal Cloud Foundry (PCF). OSS CF is an entirely [open-source](#) version of Cloud Foundry managed by the Cloud Foundry Foundation. Pivotal Cloud Foundry is an enterprise distribution of Cloud Foundry from Pivotal Software Inc. We look at some of the differences between the two offerings.

### Open-source Cloud Foundry

You can deploy OSS Cloud Foundry on Azure by first deploying a BOSH director and then deploying Cloud Foundry, using the [instructions provided on GitHub](#). To learn more about using OSS CF, see the [documentation](#) provided by the Cloud Foundry Foundation.

Microsoft provides best-effort support for OSS CF through the following community channels:

- #bosh-azure-cpi channel on [Cloud Foundry Slack](#)
- [cf-bosh mailing list](#)
- GitHub issues for the [CPI](#) and [service broker](#)

#### NOTE

The level of support for your Azure resources, such as the virtual machines where you run Cloud Foundry, is based on your Azure support agreement. Best-effort community support only applies to the Cloud Foundry-specific components.

### Pivotal Cloud Foundry

Pivotal Cloud Foundry includes the same core platform as the OSS distribution, along with a set of proprietary management tools and enterprise support. To run PCF on Azure, you must acquire a license from Pivotal. The PCF offer from the Azure marketplace includes a 90-day trial license.

The tools include [Pivotal Operations Manager](#), a web application that simplifies deployment and management of a Cloud Foundry foundation, and [Pivotal Apps Manager](#), a web application for managing users and applications.

In addition to the support channels listed for OSS CF above, a PCF license entitles you to contact Pivotal for support. Microsoft and Pivotal have also enabled support workflows that allow you to contact either party for assistance and have your inquiry routed appropriately depending on where the issue lies.

## Azure Service Broker

Cloud Foundry encourages the "[twelve-factor app](#)" methodology, which promotes a clean separation of stateless application processes and stateful backing services. [Service brokers](#) offer a consistent way to provision and bind backing services to applications. The [Azure service broker](#) provides some of the key Azure services through this channel, including Azure storage and Azure SQL.

If you are using Pivotal Cloud Foundry, the service broker is also [available as a tile](#) from the Pivotal Network.

## Related resources

### Azure DevOps Services plugin

Cloud Foundry is well suited to agile software development, including the use of continuous integration (CI) and continuous delivery (CD). If you use Azure DevOps Services to manage your projects and would like to set up a CI/CD pipeline targeting Cloud Foundry, you can use the [Azure DevOps Services Cloud Foundry build extension](#). The plugin makes it simple to configure and automate deployments to Cloud Foundry, whether running in Azure or another environment.

## Next steps

- [Deploy Pivotal Cloud Foundry from the Azure Marketplace](#)
- [Deploy an app to Cloud Foundry in Azure](#)

# Deploy your first app to Cloud Foundry on Microsoft Azure

11/13/2019 • 4 minutes to read • [Edit Online](#)

Cloud Foundry is a popular open-source application platform available on Microsoft Azure. In this article, we show how to deploy and manage an application on Cloud Foundry in an Azure environment.

## Create a Cloud Foundry environment

There are several options for creating a Cloud Foundry environment on Azure:

- Use the [Pivotal Cloud Foundry offer](#) in the Azure Marketplace to create a standard environment that includes PCF Ops Manager and the Azure Service Broker. You can find [complete instructions](#) for deploying the marketplace offer in the Pivotal documentation.
- Create a customized environment by [deploying Pivotal Cloud Foundry manually](#).
- [Deploy the open-source Cloud Foundry packages directly](#) by setting up a [BOSH](#) director, a VM that coordinates the deployment of the Cloud Foundry environment.

### IMPORTANT

If you are deploying PCF from the Azure Marketplace, make a note of the SYSTEMDOMAINURL and the admin credentials required to access the Pivotal Apps Manager, both of which are described in the marketplace deployment guide. They are needed to complete this tutorial. For marketplace deployments, the SYSTEMDOMAINURL is in the form <https://system.ip-address.cfpcfazure.com>.

## Connect to the Cloud Controller

The Cloud Controller is the primary entry point to a Cloud Foundry environment for deploying and managing applications. The core Cloud Controller API (CCAPI) is a REST API, but it is accessible through various tools. In this case, we interact with it through the [Cloud Foundry CLI](#). You can install the CLI on Linux, MacOS, or Windows, but if you'd prefer not to install it at all, it is available pre-installed in the [Azure Cloud Shell](#).

To log in, prepend `api` to the SYSTEMDOMAINURL that you obtained from the marketplace deployment. Since the default deployment uses a self-signed certificate, you should also include the `--skip-ssl-validation` switch.

```
cf login -a https://api.SYSTEMDOMAINURL --skip-ssl-validation
```

You are prompted to log in to the Cloud Controller. Use the admin account credentials that you acquired from the marketplace deployment steps.

Cloud Foundry provides *orgs* and *spaces* as namespaces to isolate the teams and environments within a shared deployment. The PCF marketplace deployment includes the default *system* org and a set of spaces created to contain the base components, like the autoscaling service and the Azure service broker. For now, choose the *system* space.

## Create an org and space

If you type `cf apps`, you see a set of system applications that have been deployed in the system space within the

system org.

You should keep the *system* org reserved for system applications, so create an org and space to house our sample application.

```
cf create-org myorg
cf create-space dev -o myorg
```

Use the target command to switch to the new org and space:

```
cf target -o testorg -s dev
```

Now, when you deploy an application, it is automatically created in the new org and space. To confirm that there are currently no apps in the new org/space, type `cf apps` again.

#### NOTE

For more information about orgs and spaces and how they can be used for role-based access control (RBAC), see the [Cloud Foundry documentation](#).

## Deploy an application

Let's use a sample Cloud Foundry application called Hello Spring Cloud, which is written in Java and based on the [Spring Framework](#) and [Spring Boot](#).

### Clone the Hello Spring Cloud repository

The Hello Spring Cloud sample application is available on GitHub. Clone it to your environment and change into the new directory:

```
git clone https://github.com/cloudfoundry-samples/hello-spring-cloud
cd hello-spring-cloud
```

### Build the application

Build the app using [Apache Maven](#).

```
mvn clean package
```

### Deploy the application with cf push

You can deploy most applications to Cloud Foundry using the `push` command:

```
cf push
```

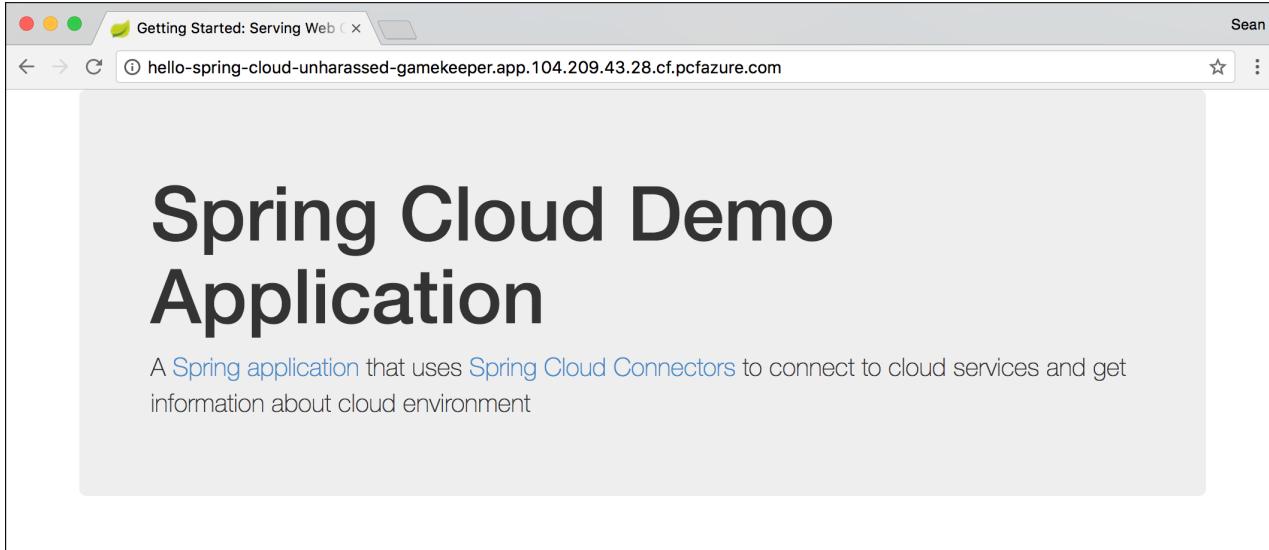
When you *push* an application, Cloud Foundry detects the type of application (in this case, a Java app) and identifies its dependencies (in this case, the Spring framework). It then packages everything required to run your code into a standalone container image, known as a *droplet*. Finally, Cloud Foundry schedules the application on one of the available machines in your environment and creates a URL where you can reach it, which is available in the output of the command.

```
Showing health and status for app hello-spring-cloud in org myorg / space dev as admin...
OK

requested state: started
instances: 1/1
usage: 1G x 1 instances
urls: hello-spring-cloud-unharassed-gamekeeper.app.104.209.43.28.cf.pcfazure.com
last uploaded: Tue Jun 6 06:36:43 UTC 2017
stack: cflinuxfs2
buildpack: container-certificate-trust-store=2.0.0_RELEASE java-buildpack=v3.13-offline-https://github.com/cloudfoundry/java-buildpack.git#03b493f java-main open-jdk-like-jre=1.8.0_121 open-jdk-like-memory-calculator=2.0.2_RELEASE spring-auto-reconfiguration=1.10...

 state since cpu memory disk details
#0 running 2017-06-06 06:37:19 AM 0.0% 147M of 1G 157.8M of 1G
sean@Azure:~/hello-spring-cloud$
```

To see the hello-spring-cloud application, open the provided URL in your browser:



#### NOTE

To learn more about what happens during `cf push`, see [How Applications Are Staged](#) in the Cloud Foundry documentation.

## View application logs

You can use the Cloud Foundry CLI to view logs for an application by its name:

```
cf logs hello-spring-cloud
```

By default, the logs command uses *tail*, which shows new logs as they are written. To see new logs appear, refresh the hello-spring-cloud app in the browser.

To view logs that have already been written, add the `recent` switch:

```
cf logs --recent hello-spring-cloud
```

## Scale the application

By default, `cf push` only creates a single instance of your application. To ensure high availability and enable scale out for higher throughput, you generally want to run more than one instance of your applications. You can easily scale out already deployed applications using the `scale` command:

```
cf scale -i 2 hello-spring-cloud
```

Running the `cf app` command on the application shows that Cloud Foundry is creating another instance of the application. Once the application has started, Cloud Foundry automatically starts load balancing traffic to it.

## Next steps

- [Read the Cloud Foundry documentation](#)
- [Set up the Azure DevOps Services plugin for Cloud Foundry](#)
- [Configure the Microsoft Log Analytics Nozzle for Cloud Foundry](#)

# OpenShift in Azure

11/13/2019 • 2 minutes to read • [Edit Online](#)

OpenShift is an open and extensible container application platform that brings Docker and Kubernetes to the enterprise.

OpenShift includes Kubernetes for container orchestration and management. It adds developer-centric and operations-centric tools that enable:

- Rapid application development.
- Easy deployment and scaling.
- Long-term lifecycle maintenance for teams and applications.

There are multiple versions of OpenShift available. Of these versions, only two are available today for customers to deploy in Azure: OpenShift Container Platform and OKD (formerly OpenShift Origin).

## Azure Red Hat OpenShift

Microsoft Azure Red Hat OpenShift is a fully managed offering of OpenShift running in Azure. This service is jointly managed and supported by Microsoft and Red Hat. For more details, see the [Azure Red Hat OpenShift Service](#) documentation.

## OpenShift Container Platform

Container Platform is an enterprise-ready [commercial version](#) from and supported by Red Hat. With this version, customers purchase the necessary entitlements for OpenShift Container Platform and are responsible for installation and management of the entire infrastructure.

Because customers "own" the entire platform, they can install it in their on-premises datacenter, or in a public cloud (such as Azure).

## OKD

OKD is an [open-source](#) upstream project of OpenShift that's community supported. OKD can be installed on CentOS or Red Hat Enterprise Linux (RHEL).

## Next steps

- [Configure common prerequisites for OpenShift in Azure](#)
- [Deploy OpenShift Container Platform in Azure](#)
- [Deploy OpenShift Container Platform Self-Managed Marketplace Offer](#)
- [Deploy OpenShift in Azure Stack](#)
- [Post-deployment tasks](#)
- [Troubleshoot OpenShift deployment](#)

# Deploy OpenShift Container Platform 4.x in Azure

11/13/2019 • 2 minutes to read • [Edit Online](#)

Deployment of OpenShift Container Platform (OCP) 4.2 is now supported in Azure via the Installer-Provisioned Infrastructure (IPI) model. The landing page for trying OpenShift 4 is [try.openshift.com](https://try.openshift.com). To install OCP 4.2 in Azure, visit the [Red Hat OpenShift Cluster Manager](#) page. Red Hat credentials are required to access this site.

## Notes

- An Azure Active Directory (AAD) Service Principal (SP) is required to install and run OCP 4.x in Azure
  - The SP must be granted the API permission of **Application.ReadWrite.OwnedBy** for Azure Active Directory Graph
  - An AAD Tenant Administrator must grant Admin Consent for this API permission to take effect
  - The SP must be granted **Contributor** and **User Access Administrator** roles to the subscription
- The installation model for OCP 4.x is different than 3.x and there are no Azure Resource Manager templates available for deploying OCP 4.x in Azure
- If issues are encountered during the installation process, contact the appropriate company (Microsoft or Red Hat)

| ISSUE DESCRIPTION                                                                      | CONTACT POINT |
|----------------------------------------------------------------------------------------|---------------|
| Azure specific issues (AAD, SP, Azure Subscription, etc.)                              | Microsoft     |
| OpenShift-specific issues (Installation failures / errors, Red Hat subscription, etc.) | Red Hat       |

## Next steps

- [Getting started with OpenShift Container Platform](#)

# Common prerequisites for deploying OpenShift Container Platform 3.11 in Azure

11/13/2019 • 5 minutes to read • [Edit Online](#)

This article describes common prerequisites for deploying OpenShift Container Platform or OKD in Azure.

The installation of OpenShift uses Ansible playbooks. Ansible uses Secure Shell (SSH) to connect to all cluster hosts to complete installation steps.

When ansible makes the SSH connection to the remote hosts, it can't enter a password. For this reason, the private key can't have a password (passphrase) associated with it or deployment fails.

Because the virtual machines (VMs) deploy via Azure Resource Manager templates, the same public key is used for access to all VMs. The corresponding private key must be on the VM that executes all the playbooks as well. To perform this action securely, an Azure key vault is used to pass the private key into the VM.

If there's a need for persistent storage for containers, then persistent volumes are required. OpenShift supports Azure virtual hard disks (VHDs) for persistent volumes, but Azure must first be configured as the cloud provider.

In this model, OpenShift:

- Creates a VHD object in an Azure storage account or a managed disk.
- Mounts the VHD to a VM and formats the volume.
- Mounts the volume to the pod.

For this configuration to work, OpenShift needs permissions to perform these tasks in Azure. A service principal is used for this purpose. The service principal is a security account in Azure Active Directory that is granted permissions to resources.

The service principal needs to have access to the storage accounts and VMs that make up the cluster. If all OpenShift cluster resources deploy to a single resource group, the service principal can be granted permissions to that resource group.

This guide describes how to create the artifacts associated with the prerequisites.

- Create a key vault to manage SSH keys for the OpenShift cluster.
- Create a service principal for use by the Azure Cloud Provider.

If you don't have an Azure subscription, create a [free account](#) before you begin.

## Sign in to Azure

Sign in to your Azure subscription with the [az login](#) command and follow the on-screen directions, or click **Try it** to use Cloud Shell.

```
az login
```

## Create a resource group

Create a resource group with the [az group create](#) command. An Azure resource group is a logical container into which Azure resources are deployed and managed. You should use a dedicated resource group to host the key

vault. This group is separate from the resource group into which the OpenShift cluster resources deploy.

The following example creates a resource group named *keyvaultrg* in the *eastus* location:

```
az group create --name keyvaultrg --location eastus
```

## Create a key vault

Create a key vault to store the SSH keys for the cluster with the [az keyvault create](#) command. The key vault name must be globally unique and must be enabled for template deployment or the deployment will fail with "KeyVaultParameterReferenceSecretRetrieveFailed" error.

The following example creates a key vault named *keyvault* in the *keyvaultrg* resource group:

```
az keyvault create --resource-group keyvaultrg --name keyvault \
 --enabled-for-template-deployment true \
 --location eastus
```

## Create an SSH key

An SSH key is needed to secure access to the OpenShift cluster. Create an SSH key pair by using the [ssh-keygen](#) command (on Linux or macOS):

```
ssh-keygen -f ~/.ssh/openshift_rsa -t rsa -N ''
```

### NOTE

Your SSH key pair can't have a password / passphrase.

For more information on SSH keys on Windows, see [How to create SSH keys on Windows](#). Be sure to export the private key in OpenSSH format.

## Store the SSH private key in Azure Key Vault

The OpenShift deployment uses the SSH key you created to secure access to the OpenShift master. To enable the deployment to securely retrieve the SSH key, store the key in Key Vault by using the following command:

```
az keyvault secret set --vault-name keyvault --name keysecret --file ~/.ssh/openshift_rsa
```

## Create a service principal

OpenShift communicates with Azure by using a username and password or a service principal. An Azure service principal is a security identity that you can use with apps, services, and automation tools like OpenShift. You control and define the permissions as to which operations the service principal can perform in Azure. It's best to scope the permissions of the service principal to specific resource groups rather than the entire subscription.

Create a service principal with [az ad sp create-for-rbac](#) and output the credentials that OpenShift needs.

The following example creates a service principal and assigns it contributor permissions to a resource group named *openshiftrg*.

First, create the resource group named *openshiftrg*:

```
az group create -l eastus -n openshiftrg
```

Create service principal:

```
az group show --name openshiftrg --query id
```

Save the output of the command and use in place of \$scope in next command

```
az ad sp create-for-rbac --name openshiftsp \
--role Contributor --scopes $scope \
```

Take note of the appId property and password returned from the command:

```
{
 "appId": "11111111-abcd-1234-efgh-111111111111",
 "displayName": "openshiftsp",
 "name": "http://openshiftsp",
 "password": {Strong Password},
 "tenant": "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX"
}
```

#### WARNING

Be sure to write down the secure password as it will not be possible to retrieve this password again.

For more information on service principals, see [Create an Azure service principal with Azure CLI](#).

## Prerequisites applicable only to Resource Manager template

Secrets will need to be created for the SSH private key (**sshPrivateKey**), Azure AD client secret (**aadClientSecret**), OpenShift admin password (**openshiftPassword**), and Red Hat Subscription Manager password or activation key (**rhsmPasswordOrActivationKey**). Additionally, if custom SSL certificates are used, then six additional secrets will need to be created - **routingcafile**, **routingcertfile**, **routingkeyfile**, **mastercafile**, **mastercertfile**, and **masterkeyfile**. These parameters will be explained in more detail.

The template references specific secret names so you **must** use the bolded names listed above (case sensitive).

### Custom Certificates

By default, the template will deploy an OpenShift cluster using self-signed certificates for the OpenShift web console and the routing domain. If you want to use custom SSL certificates, set 'routingCertType' to 'custom' and 'masterCertType' to 'custom'. You'll need the CA, Cert, and Key files in .pem format for the certificates. It is possible to use custom certificates for one but not the other.

You'll need to store these files in Key Vault secrets. Use the same Key Vault as the one used for the private key. Rather than require 6 additional inputs for the secret names, the template is hard-coded to use specific secret names for each of the SSL certificate files. Store the certificate data using the information from the following table.

| SECRET NAME    | CERTIFICATE FILE |
|----------------|------------------|
| mastercafile   | master CA file   |
| mastercertfile | master CERT file |

| SECRET NAME     | CERTIFICATE FILE  |
|-----------------|-------------------|
| masterkeyfile   | master Key file   |
| routingcafile   | routing CA file   |
| routingcertfile | routing CERT file |
| routingkeyfile  | routing Key file  |

Create the secrets using the Azure CLI. Below is an example.

```
az keyvault secret set --vault-name KeyVaultName -n mastercafile --file ~/certificates/masterca.pem
```

## Next steps

This article covered the following topics:

- Create a key vault to manage SSH keys for the OpenShift cluster.
- Create a service principal for use by the Azure Cloud Solution Provider.

Next, deploy an OpenShift cluster:

- [Deploy OpenShift Container Platform](#)
- [Deploy OpenShift Container Platform Self-Managed Marketplace Offer](#)

# Deploy OpenShift Container Platform 3.11 in Azure

12/31/2019 • 11 minutes to read • [Edit Online](#)

You can use one of several methods to deploy OpenShift Container Platform 3.11 in Azure:

- You can manually deploy the necessary Azure infrastructure components and then follow the [OpenShift Container Platform documentation](#).
- You can also use an existing [Resource Manager template](#) that simplifies the deployment of the OpenShift Container Platform cluster.
- Another option is to use the [Azure Marketplace offer](#).

For all options, a Red Hat subscription is required. During the deployment, the Red Hat Enterprise Linux instance is registered to the Red Hat subscription and attached to the Pool ID that contains the entitlements for OpenShift Container Platform. Make sure you have a valid Red Hat Subscription Manager (RHSM) username, password, and Pool ID. You can use an Activation Key, Org ID, and Pool ID. You can verify this information by signing in to <https://access.redhat.com>.

## Deploy using the OpenShift Container Platform Resource Manager 3.11 template

### Private Clusters

Deploying private OpenShift clusters requires more than just not having a public IP associated to the master load balancer (web console) or to the infra load balancer (router). A private cluster generally uses a custom DNS server (not the default Azure DNS), a custom domain name (such as contoso.com), and pre-defined virtual network(s). For private clusters, you need to configure your virtual network with all the appropriate subnets and DNS server settings in advance. Then use **existingMasterSubnetReference**, **existingInfraSubnetReference**, **existingCnsSubnetReference**, and **existingNodeSubnetReference** to specify the existing subnet for use by the cluster.

If private master is selected (**masterClusterType**=private), a static private IP needs to be specified for **masterPrivateClusterIp**. This IP will be assigned to the front end of the master load balancer. The IP must be within the CIDR for the master subnet and not in use. **masterClusterDnsType** must be set to "custom" and the master DNS name must be provided for **masterClusterDns**. The DNS name must map to the static Private IP and will be used to access the console on the master nodes.

If private router is selected (**routerClusterType**=private), a static private IP needs to be specified for **routerPrivateClusterIp**. This IP will be assigned to the front end of the infra load balancer. The IP must be within the CIDR for the infra subnet and not in use. **routingSubDomainType** must be set to "custom" and the wildcard DNS name for routing must be provided for **routingSubDomain**.

If private masters and private router are selected, the custom domain name must also be entered for **domainName**

After successful deployment, the Bastion Node is the only node with a public IP that you can ssh into. Even if the master nodes are configured for public access, they aren't exposed for ssh access.

To deploy using the Resource Manager template, you use a parameters file to supply the input parameters. To further customize the deployment, fork the GitHub repo and change the appropriate items.

Some common customization options include, but aren't limited to:

- Bastion VM size (variable in azuredeploy.json)

- Naming conventions (variables in azuredeploy.json)
- OpenShift cluster specifics, modified via hosts file (deployOpenShift.sh)

## Configure the parameters file

The [OpenShift Container Platform template](#) has multiple branches available for different versions of OpenShift Container Platform. Based on your needs, you can deploy directly from the repo or you can fork the repo and make custom changes to the templates or scripts before deploying.

Use the `appId` value from the service principal you created earlier for the `aadClientId` parameter.

The following example shows a parameters file named `azuredeploy.parameters.json` with all the required inputs.

```
{
 "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
 "contentVersion": "1.0.0.0",
 "parameters": {
 "_artifactsLocation": {
 "value": "https://raw.githubusercontent.com/Microsoft/openshift-container-platform/master"
 },
 "location": {
 "value": "eastus"
 },
 "masterVmSize": {
 "value": "Standard_E2s_v3"
 },
 "infraVmSize": {
 "value": "Standard_D4s_v3"
 },
 "nodeVmSize": {
 "value": "Standard_D4s_v3"
 },
 "cnsVmSize": {
 "value": "Standard_E4s_v3"
 },
 "osImageType": {
 "value": "defaultgallery"
 },
 "marketplaceOsImage": {
 "value": {
 "publisher": "RedHat",
 "offer": "RHEL",
 "sku": "7-RAW",
 "version": "latest"
 }
 },
 "storageKind": {
 "value": "changeme"
 },
 "openshiftClusterPrefix": {
 "value": "changeme"
 },
 "minorVersion": {
 "value": "69"
 },
 "masterInstanceCount": {
 "value": 3
 },
 "infraInstanceCount": {
 "value": 3
 },
 "nodeInstanceCount": {
 "value": 3
 },
 "cnsInstanceCount": {
 "value": 3
 }
 }
}
```

```
"osDiskSize": {
 "value": 64
},
"dataDiskSize": {
 "value": 64
},
"cnsGlusterDiskSize": {
 "value": 128
},
"adminUsername": {
 "value": "changeme"
},
"enableMetrics": {
 "value": "false"
},
"enableLogging": {
 "value": "false"
},
"enableCNS": {
 "value": "false"
},
"rhsmUsernameOrOrgId": {
 "value": "changeme"
},
"rhsmPoolId": {
 "value": "changeme"
},
"rhsmBrokerPoolId": {
 "value": "changeme"
},
"sshPublicKey": {
 "value": "GEN-SSH-PUB-KEY"
},
"keyVaultSubscriptionId": {
 "value": "255a325e-8276-4ada-af8f-33af5658eb34"
},
"keyVaultResourceGroup": {
 "value": "changeme"
},
"keyVaultName": {
 "value": "changeme"
},
"enableAzure": {
 "value": "true"
},
"adClientId": {
 "value": "changeme"
},
"domainName": {
 "value": "contoso.com"
},
"masterClusterDnsType": {
 "value": "default"
},
"masterClusterDns": {
 "value": "console.contoso.com"
},
"routingSubDomainType": {
 "value": "nipio"
},
"routingSubDomain": {
 "value": "apps.contoso.com"
},
"virtualNetworkNewOrExisting": {
 "value": "new"
},
"virtualNetworkName": {
 "value": "changeme"
}.
```

```

 },
 "addressPrefixes": {
 "value": "10.0.0.0/14"
 },
 "masterSubnetName": {
 "value": "changeme"
 },
 "masterSubnetPrefix": {
 "value": "10.1.0.0/16"
 },
 "infraSubnetName": {
 "value": "changeme"
 },
 "infraSubnetPrefix": {
 "value": "10.2.0.0/16"
 },
 "nodeSubnetName": {
 "value": "changeme"
 },
 "nodeSubnetPrefix": {
 "value": "10.3.0.0/16"
 },
 "existingMasterSubnetReference": {
 "value": "/subscriptions/abc686f6-963b-4e64-bff4-
99dc369ab1cd/resourceGroups/vnetresourcegroup/providers/Microsoft.Network/virtualNetworks/openshiftvnet/subnet
s/mastersubnet"
 },
 "existingInfraSubnetReference": {
 "value": "/subscriptions/abc686f6-963b-4e64-bff4-
99dc369ab1cd/resourceGroups/vnetresourcegroup/providers/Microsoft.Network/virtualNetworks/openshiftvnet/subnet
s/infrasubnet"
 },
 "existingCnsSubnetReference": {
 "value": "/subscriptions/abc686f6-963b-4e64-bff4-
99dc369ab1cd/resourceGroups/vnetresourcegroup/providers/Microsoft.Network/virtualNetworks/openshiftvnet/subnet
s/cnssubnet"
 },
 "existingNodeSubnetReference": {
 "value": "/subscriptions/abc686f6-963b-4e64-bff4-
99dc369ab1cd/resourceGroups/vnetresourcegroup/providers/Microsoft.Network/virtualNetworks/openshiftvnet/subnet
s/nodesubnet"
 },
 "masterClusterType": {
 "value": "public"
 },
 "masterPrivateClusterIp": {
 "value": "10.1.0.200"
 },
 "routerClusterType": {
 "value": "public"
 },
 "routerPrivateClusterIp": {
 "value": "10.2.0.200"
 },
 "routingCertType": {
 "value": "selfsigned"
 },
 "masterCertType": {
 "value": "selfsigned"
 }
}
}

```

Replace the parameters with your specific information.

Different releases may have different parameters so verify the necessary parameters for the branch you use.

### **azuredeploy.Parameters.json file explained**

| PROPERTY                            | DESCRIPTION                                                                                                                                                                         | VALID OPTIONS                 | DEFAULT VALUE                                                                                                                                                                 |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>_artifactsLocation</code>     | URL for artifacts (json, scripts, etc.)                                                                                                                                             |                               | <a href="https://raw.githubusercontent.com/Microsoft/openshift-container-platform/master">https://raw.githubusercontent.com/Microsoft/openshift-container-platform/master</a> |
| <code>location</code>               | Azure region to deploy resources to                                                                                                                                                 |                               |                                                                                                                                                                               |
| <code>masterVmSize</code>           | Size of the Master VM. Select from one of the allowed VM sizes listed in the azuredeploy.json file                                                                                  |                               | Standard_E2s_v3                                                                                                                                                               |
| <code>infraVmSize</code>            | Size of the Infra VM. Select from one of the allowed VM sizes listed in the azuredeploy.json file                                                                                   |                               | Standard_D4s_v3                                                                                                                                                               |
| <code>nodeVmSize</code>             | Size of the App Node VM. Select from one of the allowed VM sizes listed in the azuredeploy.json file                                                                                |                               | Standard_D4s_v3                                                                                                                                                               |
| <code>cnsVmSize</code>              | Size of the Container Native Storage (CNS) Node VM. Select from one of the allowed VM sizes listed in the azuredeploy.json file                                                     |                               | Standard_E4s_v3                                                                                                                                                               |
| <code>osImageType</code>            | The RHEL image to use.<br>defaultgallery: On-Demand;<br>marketplace: third-party image                                                                                              | defaultgallery<br>marketplace | defaultgallery                                                                                                                                                                |
| <code>marketplaceOsImage</code>     | If <code>osImageType</code> is marketplace, then enter the appropriate values for 'publisher', 'offer', 'sku', 'version' of the marketplace offer. This parameter is an object type |                               |                                                                                                                                                                               |
| <code>storageKind</code>            | The type of storage to be used                                                                                                                                                      | managed<br>unmanaged          | managed                                                                                                                                                                       |
| <code>openshiftClusterPrefix</code> | Cluster Prefix used to configure hostnames for all nodes. Between 1 and 20 characters                                                                                               |                               | mycluster                                                                                                                                                                     |
| <code>minoVersion</code>            | The minor version of OpenShift Container Platform 3.11 to deploy                                                                                                                    |                               | 69                                                                                                                                                                            |
| <code>masterInstanceCount</code>    | Number of Masters nodes to deploy                                                                                                                                                   | 1, 3, 5                       | 3                                                                                                                                                                             |

| PROPERTY                         | DESCRIPTION                                                                                          | VALID OPTIONS                                                                                                 | DEFAULT VALUE |
|----------------------------------|------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|---------------|
| <code>infraInstanceCount</code>  | Number of infra nodes to deploy                                                                      | 1, 2, 3                                                                                                       | 3             |
| <code>nodeInstanceCount</code>   | Number of Nodes to deploy                                                                            | 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30 | 2             |
| <code>cnsInstanceCount</code>    | Number of CNS nodes to deploy                                                                        | 3, 4                                                                                                          | 3             |
| <code>osDiskSize</code>          | Size of OS disk for the VM (in GB)                                                                   | 64, 128, 256, 512, 1024, 2048                                                                                 | 64            |
| <code>dataDiskSize</code>        | Size of data disk to attach to nodes for Docker volume (in GB)                                       | 32, 64, 128, 256, 512, 1024, 2048                                                                             | 64            |
| <code>cnsGlusterDiskSize</code>  | Size of data disk to attach to CNS nodes for use by glusterfs (in GB)                                | 32, 64, 128, 256, 512, 1024, 2048                                                                             | 128           |
| <code>adminUsername</code>       | Admin username for both OS (VM) login and initial OpenShift user                                     |                                                                                                               | ocpadmin      |
| <code>enableMetrics</code>       | Enable Metrics. Metrics require more resources so select proper size for Infra VM                    | true<br>false                                                                                                 | false         |
| <code>enableLogging</code>       | Enable Logging. elasticsearch pod requires 8 GB RAM so select proper size for Infra VM               | true<br>false                                                                                                 | false         |
| <code>enableCNS</code>           | Enable Container Native Storage                                                                      | true<br>false                                                                                                 | false         |
| <code>rhsmUsernameOrOrgId</code> | Red Hat Subscription Manager Username or Organization ID                                             |                                                                                                               |               |
| <code>rhsmPoolId</code>          | The Red Hat Subscription Manager Pool ID that contains your OpenShift entitlements for compute nodes |                                                                                                               |               |

| PROPERTY                            | DESCRIPTION                                                                                                                                                                              | VALID OPTIONS     | DEFAULT VALUE       |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|---------------------|
| <code>rhsmBrokerPoolId</code>       | The Red Hat Subscription Manager Pool ID that contains your OpenShift entitlements for masters and infra nodes. If you don't have different pool IDs, enter same pool ID as 'rhsmPoolId' |                   |                     |
| <code>sshPublicKey</code>           | Copy your SSH Public Key here                                                                                                                                                            |                   |                     |
| <code>keyVaultSubscriptionId</code> | The Subscription ID of the subscription that contains the Key Vault                                                                                                                      |                   |                     |
| <code>keyVaultResourceGroup</code>  | The name of the Resource Group that contains the Key Vault                                                                                                                               |                   |                     |
| <code>keyVaultName</code>           | The name of the Key Vault you created                                                                                                                                                    |                   |                     |
| <code>enableAzure</code>            | Enable Azure Cloud Provider                                                                                                                                                              | true<br>false     | true                |
| <code>aadClientId</code>            | Azure Active Directory Client ID also known as Application ID for Service Principal                                                                                                      |                   |                     |
| <code>domainName</code>             | Name of the custom domain name to use (if applicable). Set to "none" if not deploying fully private cluster                                                                              |                   | none                |
| <code>masterClusterDnsType</code>   | Domain type for OpenShift web console. 'default' will use DNS label of master infra public IP. 'custom' allows you to define your own name                                               | default<br>custom | default             |
| <code>masterClusterDns</code>       | The custom DNS name to use to access the OpenShift web console if you selected 'custom' for <code>masterClusterDnsType</code>                                                            |                   | console.contoso.com |
| <code>routingSubDomainType</code>   | If set to 'nipio', <code>routingSubDomain</code> will use nip.io. Use 'custom' if you have your own domain that you want to use for routing                                              | nipio<br>custom   | nipio               |

| PROPERTY                                     | DESCRIPTION                                                                                                               | VALID OPTIONS   | DEFAULT VALUE        |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|-----------------|----------------------|
| <code>routingSubDomain</code>                | The wildcard DNS name you want to use for routing if you selected 'custom' for <code>routingSubDomainType</code>          |                 | apps.contoso.com     |
| <code>virtualNetworkNewOrExisting</code>     | Select whether to use an existing Virtual Network or create a new Virtual Network                                         | existing<br>new | new                  |
| <code>virtualNetworkResourceGroupName</code> | Name of the Resource Group for the new Virtual Network if you selected 'new' for <code>virtualNetworkNewOrExisting</code> |                 | resourceGroup().name |
| <code>virtualNetworkName</code>              | The name of the new Virtual Network to create if you selected 'new' for <code>virtualNetworkNewOrExisting</code>          |                 | openshiftvnet        |
| <code>addressPrefixes</code>                 | Address prefix of the new virtual network                                                                                 |                 | 10.0.0.0/14          |
| <code>masterSubnetName</code>                | The name of the master subnet                                                                                             |                 | mastersubnet         |
| <code>masterSubnetPrefix</code>              | CIDR used for the master subnet - needs to be a subset of the addressPrefix                                               |                 | 10.1.0.0/16          |
| <code>infraSubnetName</code>                 | The name of the infra subnet                                                                                              |                 | infrasubnet          |
| <code>infraSubnetPrefix</code>               | CIDR used for the infra subnet - needs to be a subset of the addressPrefix                                                |                 | 10.2.0.0/16          |
| <code>nodeSubnetName</code>                  | The name of the node subnet                                                                                               |                 | nodesubnet           |
| <code>nodeSubnetPrefix</code>                | CIDR used for the node subnet - needs to be a subset of the addressPrefix                                                 |                 | 10.3.0.0/16          |
| <code>existingMasterSubnetReference</code>   | Full reference to existing subnet for master nodes. Not needed if creating new vNet / Subnet                              |                 |                      |
| <code>existingInfraSubnetReference</code>    | Full reference to existing subnet for infra nodes. Not needed if creating new vNet / Subnet                               |                 |                      |

| PROPERTY                                 | DESCRIPTION                                                                                                                                                                                                                                                                                                                    | VALID OPTIONS     | DEFAULT VALUE |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|---------------|
| <code>existingCnsSubnetReference</code>  | Full reference to existing subnet for CNS nodes. Not needed if creating new vNet / Subnet                                                                                                                                                                                                                                      |                   |               |
| <code>existingNodeSubnetReference</code> | Full reference to existing subnet for compute nodes. Not needed if creating new vNet / Subnet                                                                                                                                                                                                                                  |                   |               |
| <code>masterClusterType</code>           | Specify whether the cluster uses private or public master nodes. If private is chosen, the master nodes won't be exposed to the Internet via a public IP. Instead, it will use the private IP specified in the <code>masterPrivateClusterIp</code>                                                                             | public<br>private | public        |
| <code>masterPrivateClusterIp</code>      | If private master nodes are selected, then a private IP address must be specified for use by the internal load balancer for master nodes. This static IP must be within the CIDR block for the master subnet and not already in use. If public master nodes are selected, this value won't be used but must still be specified |                   | 10.1.0.200    |
| <code>routerClusterType</code>           | Specify whether the cluster uses private or public infra nodes. If private is chosen, the infra nodes won't be exposed to the Internet via a public IP. Instead, it will use the private IP specified in the <code>routerPrivateClusterIp</code>                                                                               | public<br>private | public        |
| <code>routerPrivateClusterIp</code>      | If private infra nodes are selected, then a private IP address must be specified for use by the internal load balancer for infra nodes. This static IP must be within the CIDR block for the master subnet and not already in use. If public infra nodes are selected, this value won't be used but must still be specified    |                   | 10.2.0.200    |

| PROPERTY                     | DESCRIPTION                                                                                                                                     | VALID OPTIONS        | DEFAULT VALUE |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|---------------|
| <code>routingCertType</code> | Use custom certificate for routing domain or the default self-signed certificate<br>- follow instructions in <b>Custom Certificates</b> section | selfsigned<br>custom | selfsigned    |
| <code>masterCertType</code>  | Use custom certificate for master domain or the default self-signed certificate<br>- follow instructions in <b>Custom Certificates</b> section  | selfsigned<br>custom | selfsigned    |

## Deploy using Azure CLI

### NOTE

The following command requires Azure CLI 2.0.8 or later. You can verify the CLI version with the `az --version` command. To update the CLI version, see [Install Azure CLI](#).

The following example deploys the OpenShift cluster and all related resources into a resource group named `openshiftrg`, with a deployment name of `myOpenShiftCluster`. The template is referenced directly from the GitHub repo, and a local parameters file named `azuredeploy.parameters.json` file is used.

```
az group deployment create -g openshiftrg --name myOpenShiftCluster \
 --template-uri https://raw.githubusercontent.com/Microsoft/openshift-container-
platform/master/azuredeploy.json \
 --parameters @./azuredeploy.parameters.json
```

The deployment takes at least 60 minutes to complete, based on the total number of nodes deployed and options configured. The Bastion DNS FQDN and URL of the OpenShift console prints to the terminal when the deployment finishes.

```
{
 "Bastion DNS FQDN": "bastiondns4hawllzaavu6g.eastus.cloudapp.azure.com",
 "OpenShift Console URL": "http://openshiftlb.eastus.cloudapp.azure.com/console"
}
```

If you don't want to tie up the command line waiting for the deployment to complete, add `--no-wait` as one of the options for the group deployment. The output from the deployment can be retrieved from the Azure portal in the deployment section for the resource group.

## Connect to the OpenShift cluster

When the deployment finishes, retrieve the connection from the output section of the deployment. Connect to the OpenShift console with your browser by using the **OpenShift Console URL**. You can also SSH to the Bastion host. Following is an example where the admin username is `clusteradmin` and the bastion public IP DNS FQDN is `bastiondns4hawllzaavu6g.eastus.cloudapp.azure.com`:

```
$ ssh clusteradmin@bastiondns4hawllzaavu6g.eastus.cloudapp.azure.com
```

## Clean up resources

Use the [az group delete](#) command to remove the resource group, OpenShift cluster, and all related resources when they're no longer needed.

```
az group delete --name openshiftrg
```

## Next steps

- [Post-deployment tasks](#)
- [Troubleshoot OpenShift deployment in Azure](#)
- [Getting started with OpenShift Container Platform](#)

# Configure prerequisites

12/31/2019 • 7 minutes to read • [Edit Online](#)

Before using the Marketplace offer to deploy a self-managed OpenShift Container Platform 3.11 cluster in Azure, a few prerequisites must be configured. Read the [OpenShift prerequisites](#) article for instructions to create an ssh key (without a passphrase), Azure key vault, key vault secret, and a service principal.

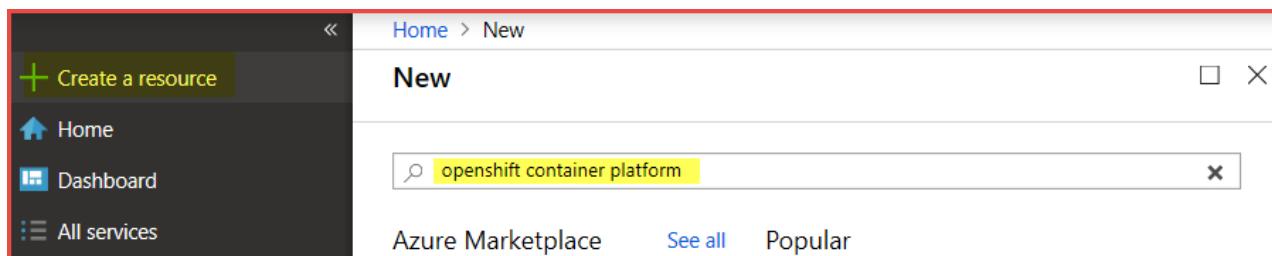
## Deploy using the Marketplace offer

The simplest way to deploy a self-managed OpenShift Container Platform 3.11 cluster into Azure is to use the [Azure Marketplace offer](#).

This option is the simplest, but it also has limited customization capabilities. The Marketplace offer deploys OpenShift Container Platform 3.11.82 and includes the following configuration options:

- **Master Nodes:** Three (3) Master Nodes with configurable instance type.
- **Infra Nodes:** Three (3) Infra Nodes with configurable instance type.
- **Nodes:** The number of Nodes (between 1 and 9) and the instance type are configurable.
- **Disk Type:** Managed Disks are used.
- **Networking:** Support for new or existing Network and custom CIDR range.
- **CNS:** CNS can be enabled.
- **Metrics:** Hawkular Metrics can be enabled.
- **Logging:** EFK Logging can be enabled.
- **Azure Cloud Provider:** Enabled by default, can be disabled.

In the upper left of the Azure portal, click **Create a resource**, enter 'openshift container platform' into the search box and hit Enter.



The Results page will open with **Red Hat OpenShift Container Platform 3.11 Self-Managed** in the list.

| Results                                                                                                                               |           |          |
|---------------------------------------------------------------------------------------------------------------------------------------|-----------|----------|
| NAME                                                                                                                                  | PUBLISHER | CATEGORY |
|  Red Hat OpenShift Container Platform Self-Managed | Red Hat   | Compute  |

Click the offer to view details of the offer. To deploy this offer, click **Create**. The UI to enter necessary parameters will appear. The first screen is the **Basics** blade.

## Red Hat OpenShift Container Platform Self-Managed



### Red Hat OpenShift Container Platform Self-Managed

Red Hat

Create

Save for later

#### This is the Self-Managed offer

Read [Deployment Guide](#) for Azure Marketplace before deploying.

Red Hat OpenShift Container Platform helps organizations develop, deploy, and manage container-based applications seamlessly across physical, virtual, and public cloud infrastructures. OpenShift Container Platform brings application development and IT operations teams together in order to modernize applications, accelerate development processes, and deliver new services faster.

#### OpenShift Highlights:

- Simple to use with powerful tools for developers
- For traditional, stateful, and cloud-native applications
- Built on proven open source technologies including Red Hat Enterprise Linux, Kubernetes, and Docker
- Enterprise-grade security, compliance, and container management
- Expanded applications support with new and updated runtimes

This offering includes one bastion host, three master nodes, three infrastructure nodes, and a customizable number and size of application nodes.

- The number of application nodes is configurable between one and nine hosts with six options for the size of the virtual machines.
- The bastion host serves as a jump host for access to the OpenShift cluster nodes and system management.

#### Useful Links

[OpenShift Container Platform Documentation](#)

[OpenShift Container Platform Overview](#)

[OpenShift Container Platform Reference Architecture for Azure](#)

[Red Hat Cloud Access Program](#)

[Red Hat Solutions On Azure](#)

[Deploy OpenShift on Azure](#)

The screenshot shows the 'OPENSHIFT CONTAINER PLATFORM' interface. At the top, there's a navigation bar with 'Web Tier 1 > Add to Project'. Below it is a search bar labeled 'Filter by keyword' and a 'Browse' button. The main area is divided into two sections: 'Instant Apps' and 'xPaaS'. Under 'Instant Apps', there are four items: 'jenkins-ephemeral' (RED HAT JBoss), 'jenkins-persistent' (RED HAT JBoss), 'ruby-helloworld-sample' (RED HAT JBoss Ruby), and 'java-s2i-karaf2-camel-amq' (See all). Under 'xPaaS', there are four items: 'ts-java-openshift:1.0' (RED HAT JBoss Java), 'ts-karaf-openshift:1.0' (RED HAT JBoss Karaf), 'boss-decisionserver63-openshift:1.2' (RED HAT JBoss DecisionServer), and 'boss-decisionserver63-openshift:1.3' (RED HAT JBoss DecisionServer).

## Basics

To get help on any of the input parameters, hover over the **i** next to the parameter name.

Enter values for the input parameters and click **OK**.

| INPUT PARAMETER               | PARAMETER DESCRIPTION                                                                        |
|-------------------------------|----------------------------------------------------------------------------------------------|
| VM Admin User Name            | The administrator user to be created on all VM instances                                     |
| SSH Public Key for Admin User | SSH public key used to log into VM - must not have a passphrase                              |
| Subscription                  | Azure subscription to deploy cluster into                                                    |
| Resource Group                | Create a new resource group or select an existing empty resource group for cluster resources |
| Location                      | Azure region to deploy cluster into                                                          |

Create Red Hat OpenShift Co... X
Basics X

**1** Basics >  
Configure basic settings

**2** Infrastructure Settings >  
Configure Infrastructure Settings

**3** OpenShift Container Plat... >  
Configure OpenShift Container Pl...

**4** Additional Settings >  
Additional Settings

**5** Summary >  
Red Hat OpenShift Container Plat...

**6** Buy >

\* VM Admin User Name i

\* SSH Public Key for VM Admin User i

Subscription

\* Resource group i  
 v  
[Create new](#)

\* Location  
 v

## Infrastructure Settings

Enter values for the input parameters and click **OK**.

| INPUT PARAMETER             | PARAMETER DESCRIPTION                                                                                                               |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| OCP Cluster Name Prefix     | Cluster Prefix used to configure hostnames for all nodes.<br>Between 1 and 20 characters                                            |
| Master Node Size            | Accept the default VM size or click <b>Change size</b> to select a different VM size. Select appropriate VM size for your work load |
| Infrastructure Node Size    | Accept the default VM size or click <b>Change size</b> to select a different VM size. Select appropriate VM size for your work load |
| Number of Application Nodes | Accept the default VM size or click <b>Change size</b> to select a different VM size. Select appropriate VM size for your work load |
| Application Node Size       | Accept the default VM size or click <b>Change size</b> to select a different VM size. Select appropriate VM size for your work load |
| Bastion Host Size           | Accept the default VM size or click <b>Change size</b> to select a different VM size. Select appropriate VM size for your work load |

| INPUT PARAMETER                                           | PARAMETER DESCRIPTION                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| New or Existing Virtual Network                           | Create a new vNet (Default) or use an existing vNet                                                                                                                                                                                                                   |
| Choose Default CIDR Settings or customize IP Range (CIDR) | Accept default CIDR ranges or Select <b>Custom IP Range</b> and enter custom CIDR information. Default Settings will create vNet with CIDR of 10.0.0.0/14, master subnet with 10.1.0.0/16, infra subnet with 10.2.0.0/16, and compute and cns subnet with 10.3.0.0/16 |
| Key Vault Resource Group Name                             | The name of the Resource Group that contains the Key Vault                                                                                                                                                                                                            |
| Key Vault Name                                            | The name of the Key Vault that contains the secret with the ssh private key. Only alphanumeric characters and dashes are allowed, and be between 3 and 24 characters                                                                                                  |
| Secret Name                                               | The name of the secret that contains the ssh private key. Only alphanumeric characters and dashes are allowed                                                                                                                                                         |

**Create Red Hat OpenShift Container Platform**

**Infrastructure Settings**

1 Basics Done ✓

2 Infrastructure Settings > Configure Infrastructure Settings

3 OpenShift Container Platform... > Configure OpenShift Container Pl...

4 Additional Settings > Additional Settings

5 Summary > Red Hat OpenShift Container Plat...

6 Buy >

\* OCP Cluster Name Prefix ⓘ ocpcluster

\* Master Node Size ⓘ 3x Standard D4s v3  
4 vcpus, 16 GB memory [Change size](#)

\* Infrastructure Node Size ⓘ 3x Standard E2s v3  
2 vcpus, 16 GB memory [Change size](#)

Number of Application Nodes ⓘ 3 ✓

\* Application Node Size ⓘ 3x Standard D2s v3  
2 vcpus, 8 GB memory [Change size](#)

\* Bastion Host Size ⓘ 1x Standard DS2 v2  
2 vcpus, 7 GB memory [Change size](#)

New or Existing Virtual Network ⓘ  
 Default (New)  Existing

Choosing the default or to customize the Virtual Network ⓘ  
 Default Settings  Custom IP Range

\* Key Vault Resource Group Name ⓘ keyvaultrg ✓

\* Key Vault Name ⓘ keyvault ✓

\* Secret Name ⓘ sshprivatekey

## Change size

To select a different VM size, click **Change size**. The VM selection window will open. Select the VM size you want and click **Select**.

Showing 4 VM sizes. | Subscription: [REDACTED] | Region: East US | Current size: Standard\_D4s\_v3

| VM SIZE | OFFERING | FAMILY           | VCPUS | RAM (GB) | DATA DISKS | MAX IOPS | TEMPORARY STORA... | PREMIUM DISK SUP... | COST/MONTH (ESTI...) |
|---------|----------|------------------|-------|----------|------------|----------|--------------------|---------------------|----------------------|
| D2s_v3  | Standard | General purpose  | 2     | 8        | 4          | 3200     | 16 GB              | Yes                 | [REDACTED]           |
| D4s_v3  | Standard | General purpose  | 4     | 16       | 8          | 6400     | 32 GB              | Yes                 | [REDACTED]           |
| E2s_v3  | Standard | Memory optimized | 2     | 16       | 4          | 3200     | 32 GB              | Yes                 | [REDACTED]           |
| E4s_v3  | Standard | Memory optimized | 4     | 32       | 8          | 6400     | 64 GB              | Yes                 | [REDACTED]           |

## Existing Virtual Network

| INPUT PARAMETER                                 | PARAMETER DESCRIPTION                                                                                            |
|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Existing Virtual Network Name                   | Name of the existing vNet                                                                                        |
| Subnet name for master nodes                    | Name of existing subnet for master nodes. Needs to contain at least 16 IP addresses and follow RFC 1918          |
| Subnet name for infra nodes                     | Name of existing subnet for infra nodes. Needs to contain at least 32 IP addresses and follow RFC 1918           |
| Subnet name for compute and cns nodes           | Name of existing subnet for compute and cns nodes. Needs to contain at least 32 IP addresses and follow RFC 1918 |
| Resource Group for the existing Virtual Network | Name of resource group that contains the existing vNet                                                           |

New or Existing Virtual Network ⓘ

Default (New)  Existing

\* Existing Virtual Network Name  
ocpvnet ✓

\* Subnet name for master nodes ⓘ  
mastersubnet ✓

\* Subnet name for infra nodes ⓘ  
infrasubnet ✓

\* Subnet name for compute and cns nodes ⓘ  
nodesubnet ✓

\* Resource Group for the existing Virtual Network ⓘ  
vnetresourcegroup ✓

## Custom IP Range

| INPUT PARAMETER                                                  | PARAMETER DESCRIPTION                     |
|------------------------------------------------------------------|-------------------------------------------|
| Address Range for the Virtual Network                            | Custom CIDR for the vNet                  |
| Address Range for the subnet containing the master nodes         | Custom CIDR for master subnet             |
| Address Range for the subnet containing the infrastructure nodes | Custom CIDR for infrastructure subnet     |
| Address Range for subnet containing the compute and cns nodes    | Custom CIDR for the compute and cns nodes |

Choosing the default or to customize the Virtual Network [?](#)

[Default Settings](#) [Custom IP Range](#)

\* Address Range for the VirtualNetwork (default is 10.0.0.0/14) [?](#)  
10.0.0.0/16 ✓

\* Address Range for the subnet containing the master, infra, and cns nodes (default is 10.1.0.0/16) [?](#)  
10.0.10.0/24 ✓

\* Address Range for the subnet containing all the infrastructure nodes (default is 10.2.0.0/16) [?](#)  
10.0.20.0/24 ✓

\* Address Range for the subnet containing all the cns and compute nodes (default is 10.3.0.0/16) [?](#)  
10.0.30.0/24 ✓

## OpenShift Container Platform 3.11

Enter values for the Input Parameters and click **OK**

| INPUT PARAMETER                                                          | PARAMETER DESCRIPTION                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OpenShift Admin User Password                                            | Password for the initial OpenShift user. This user will also be the cluster admin                                                                                                                                                                                                 |
| Confirm OpenShift Admin User Password                                    | Retype the OpenShift Admin User Password                                                                                                                                                                                                                                          |
| Red Hat Subscription Manager User Name                                   | User Name to access your Red Hat Subscription or Organization ID. This credential is used to register the RHEL instance to your subscription and will not be stored by Microsoft or Red Hat                                                                                       |
| Red Hat Subscription Manager User Password                               | Password to access your Red Hat Subscription or Activation Key. This credential is used to register the RHEL instance to your subscription and will not be stored by Microsoft or Red Hat                                                                                         |
| Red Hat Subscription Manager OpenShift Pool ID                           | Pool ID that contains OpenShift Container Platform entitlement. Ensure you have enough entitlements of OpenShift Container Platform for the installation of the cluster                                                                                                           |
| Red Hat Subscription Manager OpenShift Pool ID for Broker / Master Nodes | Pool ID that contains OpenShift Container Platform entitlements for Broker / Master Nodes. Ensure you have enough entitlements of OpenShift Container Platform for the installation of the cluster. If not using broker / master pool ID, enter the pool ID for Application Nodes |
| Configure Azure Cloud Provider                                           | Configure OpenShift to use Azure Cloud Provider. Necessary if using Azure disk attach for persistent volumes. Default is Yes                                                                                                                                                      |

| INPUT PARAMETER                             | PARAMETER DESCRIPTION                                                                                                     |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Azure AD Service Principal Client ID GUID   | Azure AD Service Principal Client ID GUID - also known as AppID. Only needed if Configure Azure Cloud Provider set to Yes |
| Azure AD Service Principal Client ID Secret | Azure AD Service Principal Client ID Secret. Only needed if Configure Azure Cloud Provider set to Yes                     |

**Create Red Hat OpenShift Container Platform**

1 Basics ✓

2 Infrastructure Settings ✓

3 OpenShift Container Platform > Configure OpenShift Container Platform

4 Additional Settings > Additional Settings

5 Summary > Red Hat OpenShift Container Platform

6 Buy >

**OpenShift Container Platform**

\* OpenShift Admin User Password ✓  
••••••••

\* Confirm OpenShift Admin User Password ✓  
••••••••

\* Red Hat Subscription Manager User Name  
? rsmusername ✓

\* Red Hat Subscription Manager User Password ✓  
••••••••

\* Red Hat Subscription Manager OpenShift Pool ID ✓  
8abcd12345e6f7890123abdbe01a000a

\* Red Hat Subscription Manager OpenShift Pool ID for Broker / Master Nodes ✓  
8abcd12345e6f7890123abdbe01a000b

Configure Azure Cloud Provider ? Yes No

\* Azure AD Service Principal Client ID GUID ? abcd1234-5678-9ef0-89cb-d6da4f6cde12 ✓

\* Azure AD Service Principal Client ID Secret ? •••••••••••••• ✓

## Additional Settings

The Additional Settings blade allows the configuration of CNS for glusterfs storage, Logging, Metrics, and Router Sub domain. The default won't install any of these options and will use nip.io as the router sub domain for testing purposes. Enabling CNS will install three additional compute nodes with three additional attached disks that will host glusterfs pods.

Enter values for the Input Parameters and click **OK**

| INPUT PARAMETER | PARAMETER DESCRIPTION |
|-----------------|-----------------------|
|-----------------|-----------------------|

| INPUT PARAMETER                          | PARAMETER DESCRIPTION                                                                                              |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Configure Container Native Storage (CNS) | Installs CNS in the OpenShift cluster and enable it as storage.<br>Will be default if Azure Provider is disabled   |
| Configure Cluster Logging                | Installs EFK logging functionality into the cluster. Size infra nodes appropriately to host EFK pods               |
| Configure Metrics for the Cluster        | Installs Hawkular metrics into the OpenShift cluster. Size infra nodes appropriately to host Hawkular metrics pods |
| Default Router Sub domain                | Select nipio for testing or custom to enter your own sub domain for production                                     |

**Create Red Hat OpenShift Co... X**

**Additional Settings X**

1 Basics Done ✓

2 Infrastructure Settings Done ✓

3 OpenShift Container Platfor... Done ✓

4 Additional Settings > Additional Settings

5 Summary > Red Hat OpenShift Container Plat...

6 Buy >

Configure Container Native Storage (CNS) ⓘ

Configure Cluster Logging ⓘ

Configure Metrics for the Cluster ⓘ

Default Router Subdomain ⓘ  
 ▾

#### Additional Settings - Extra Parameters

| INPUT PARAMETER             | PARAMETER DESCRIPTION                                                                                                                                         |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (CNS) Node Size             | Accept the default node size or select <b>Change size</b> to select a new VM size                                                                             |
| Enter your custom subdomain | The custom routing domain to be used for exposing applications via the router on the OpenShift cluster. Be sure to create the appropriate wildcard DNS entry] |

Create Red Hat OpenShift Co... X Additional Settings □ X

|                                                    |                                                                                                                                                |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 Basics<br>Done                                   | Configure Container Native Storage (CNS) <small>i</small><br><input type="button" value="Yes"/> <input type="button" value="No"/>              |
| 2 Infrastructure Settings<br>Done                  | * CNS Node Size <small>i</small><br><b>3x Standard E4s v3</b><br>4 vcpus, 32 GB memory<br><a href="#">Change size</a>                          |
| 3 OpenShift Container Plat...<br>Done              | Configure Cluster Logging <small>i</small><br><input type="button" value="Yes"/> <input type="button" value="No"/>                             |
| 4 Additional Settings ><br>Additional Settings     | Configure Metrics for the Cluster <small>i</small><br><input type="button" value="Yes"/> <input type="button" value="No"/>                     |
| 5 Summary ><br>Red Hat OpenShift Container Plat... | Default Router Subdomain <small>i</small><br><input style="width: 200px;" type="text" value="custom"/> <input type="button" value="▼"/>        |
| 6 Buy >                                            | * Enter your custom subdomain <small>i</small><br><input style="width: 200px;" type="text" value="apps.contoso.com"/> <input type="checkbox"/> |

## Summary

Validation occurs at this stage to check core quota is sufficient to deploy the total number of VMs selected for the cluster. Review all the parameters that were entered. If the inputs are acceptable, click **OK** to continue.

Create Red Hat OpenShift Co... X
Summary X

- 1** Basics ✓  
Done
- 2** Infrastructure Settings ✓  
Done
- 3** OpenShift Container Plat... ✓  
Done
- 4** Additional Settings ✓  
Done
- 5** Summary >  
Red Hat OpenShift Container Plat...
- 6** Buy >

**Validation passed**

|                                       |                                      |
|---------------------------------------|--------------------------------------|
| Basics                                |                                      |
| Subscription                          | openshift-resourcegroup              |
| Resource group                        | East US                              |
| Location                              |                                      |
| VM Admin User Name                    | clusteradmin                         |
| SSH Public Key for VM Admi...         |                                      |
|                                       |                                      |
| Infrastructure Settings               |                                      |
| OCP Cluster Name Prefix               | ocpcluster                           |
| Master Node Size                      | Standard D4s v3                      |
| Infrastructure Node Size              | Standard D4s v3                      |
| Number of Application Nodes           | 3                                    |
| Application Node Size                 | Standard D4s v3                      |
| Bastion Host Size                     | Standard DS2 v2                      |
| New or Existing Virtual Netw...       | Default (New)                        |
| Choosing the default or to cus...     | Default Settings                     |
| Key Vault Resource Group N...         |                                      |
| Key Vault Name                        | sshprivatekey                        |
| Secret Name                           |                                      |
|                                       |                                      |
| OpenShift Container Platform Settings |                                      |
| OpenShift Admin User Passw...         | *****                                |
| Red Hat Subscription Manag...         | rhmusername                          |
| Red Hat Subscription Manag...         | *****                                |
| Red Hat Subscription Manag...         | 8abcd12345e6f7890123abdbe01a000a     |
| Red Hat Subscription Manag...         | 8abcd12345e6f7890123abdbe01a000b     |
| Configure Azure Cloud Provi...        | Yes                                  |
| Azure AD Service Principal Cl...      | abcd1234-5678-9ef0-89cb-d6da4f6cde12 |
| Azure AD Service Principal Cl...      | *****                                |
|                                       |                                      |
| Additional Settings                   |                                      |
| Configure Container Native S...       | Yes                                  |
| CNS Node Size                         | Standard E4s v3                      |
| Configure Cluster Logging             | No                                   |
| Configure Metrics for the Clu...      | No                                   |
| Default Router Subdomain              | nipio                                |

## Buy

Confirm contact information on the Buy page and click **Purchase** to accept the terms of use and start deployment of the OpenShift Container Platform cluster.

**Create Red Hat OpenShift Co... X**

| Create   |                                     |   |
|----------|-------------------------------------|---|
| <b>1</b> | Basics                              | ✓ |
|          | Done                                |   |
| <b>2</b> | Infrastructure Settings             | ✓ |
|          | Done                                |   |
| <b>3</b> | OpenShift Container Platfor...      | ✓ |
|          | Done                                |   |
| <b>4</b> | Additional Settings                 | ✓ |
|          | Done                                |   |
| <b>5</b> | Summary                             | ✓ |
|          | Red Hat OpenShift Container Plat... |   |
| <b>6</b> | Buy                                 | > |

Red Hat OpenShift Container Platform Self-Managed by Red Hat  
[Terms of use](#) | [privacy policy](#)

Deploying this template will result in various actions being performed, which may include the deployment of one or more Azure resources or Marketplace offerings and/or transmission of the information you provided as part of the deployment process to one or more parties, as specified in the template. You are responsible for reviewing the text of the template to determine which actions will be performed and which resources or offerings will be deployed, and for locating and reviewing the pricing and legal terms associated with those resources or offerings.

Current retail prices for Azure resources are set forth [here](#) and may not reflect discounts applicable to your Azure subscription.

Prices for Marketplace offerings are set forth [here](#), and the legal terms associated with any Marketplace offering may be found in the Azure portal; both are subject to change at any time prior to deployment.

Neither subscription credits nor monetary commitment funds may be used to purchase non-Microsoft offerings. These purchases are billed separately. If any Microsoft products are included in a Marketplace offering (e.g., Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.

**Template deployment is intended for advanced users only.** If you are uncertain which actions will be performed by this template, which resources or offerings will be deployed, or what prices or legal terms pertain to those resources or offerings, do not deploy this template.

**Terms of use**

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) provided above as well as the legal terms and privacy statement(s) associated with each Marketplace offering that will be deployed using this template, if any; (b) authorize Microsoft to charge or bill my current payment method for the fees associated with my use of the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); (c) agree that Microsoft may share my contact information and transaction details with any third-party sellers of the offering(s); and (d) give Microsoft permission to share my contact information so that the provider of the template can contact me regarding this product and related products. Microsoft assumes no responsibility for any actions performed by third-party templates and does not provide rights for third-party products or services. See the [Azure Marketplace Terms](#) for additional terms.

**By clicking Create, you give Microsoft permission to use or share your account information so that the provider or Microsoft can contact you regarding this product and related products.**

Name:

\* Preferred e-mail address:

\* Preferred phone number:

**Create**

## Connect to the OpenShift cluster

When the deployment finishes, retrieve the connection from the output section of the deployment. Connect to the OpenShift console with your browser by using the **OpenShift Console URL**. You can also SSH to the Bastion host. Following is an example where the admin username is clusteradmin and the bastion public IP DNS FQDN is bastiondns4hawllzaavu6g.eastus.cloudapp.azure.com:

```
$ ssh clusteradmin@bastiondns4hawllzaavu6g.eastus.cloudapp.azure.com
```

## Clean up resources

Use the [az group delete](#) command to remove the resource group, OpenShift cluster, and all related resources when they're no longer needed.

```
az group delete --name openshifttrg
```

## Next steps

- [Post-deployment tasks](#)
- [Troubleshoot OpenShift deployment in Azure](#)
- [Getting started with OpenShift Container Platform](#)
-

# Deploy OpenShift Container Platform or OKD in Azure Stack

11/13/2019 • 2 minutes to read • [Edit Online](#)

OpenShift can be deployed in Azure Stack. There are some key differences between Azure and Azure Stack so deployment will differ slightly and capabilities will also differ slightly.

Currently, the Azure Cloud Provider doesn't work in Azure Stack. For this reason, you won't be able to use disk attach for persistent storage in Azure Stack. Instead, you can configure other storage options such as NFS, iSCSI, GlusterFS, etc. As an alternative, you can enable CNS and use GlusterFS for persistent storage. If CNS is enabled, three additional nodes will be deployed with additional storage for GlusterFS usage.

You can use one of several methods to deploy OpenShift Container Platform or OKD in Azure Stack:

- You can manually deploy the necessary Azure infrastructure components and then follow the [OpenShift Container Platform documentation](#) or [OKD documentation](#).
- You can also use an existing [Resource Manager template](#) that simplifies the deployment of the OpenShift Container Platform cluster.
- You can also use an existing [Resource Manager template](#) that simplifies the deployment of the OKD cluster.

If using the Resource Manager template, select the proper branch (azurestack-release-3.x). The templates for Azure won't work as the API versions are different between Azure and Azure Stack. The RHEL image reference is currently hard-coded as a variable in the azuredeploy.json file and will need to be changed to match your image.

```
"imageReference": {
 "publisher": "Redhat",
 "offer": "RHEL-OCP",
 "sku": "7-4",
 "version": "latest"
}
```

For all options, a Red Hat subscription is required. During the deployment, the Red Hat Enterprise Linux instance is registered to the Red Hat subscription and attached to the Pool ID that contains the entitlements for OpenShift Container Platform. Make sure you have a valid Red Hat Subscription Manager (RHSM) username, password, and Pool ID. Alternatively, you can use an Activation Key, Org ID, and Pool ID. You can verify this information by signing in to <https://access.redhat.com>.

## Azure Stack prerequisites

A RHEL image (OpenShift Container Platform) or CentOS image (OKD) needs to be added to your Azure Stack environment to deploy an OpenShift cluster. Contact your Azure Stack administrator to add these images. Instructions can be found here:

- <https://docs.microsoft.com/azure/azure-stack/azure-stack-add-vm-image>
- <https://docs.microsoft.com/azure/azure-stack/azure-stack-marketplace-azure-items>
- <https://docs.microsoft.com/azure/azure-stack/azure-stack-redhat-create-upload-vhd>

## Deploy by using the OpenShift Container Platform or OKD Resource Manager template

To deploy by using the Resource Manager template, you use a parameters file to supply the input parameters. To further customize the deployment, fork the GitHub repo and change the appropriate items.

Some common customization options include, but aren't limited to:

- Bastion VM size (variable in azuredeploy.json)
- Naming conventions (variables in azuredeploy.json)
- OpenShift cluster specifics, modified via hosts file (deployOpenShift.sh)
- RHEL image reference (variable in azuredeploy.json)

For the steps to deploy using the Azure CLI, follow the appropriate section in the [OpenShift Container Platform](#) section or the [OKD](#) section.

## Next steps

- [Post-deployment tasks](#)
- [Troubleshoot OpenShift deployment in Azure](#)

# Post-deployment tasks

11/13/2019 • 3 minutes to read • [Edit Online](#)

After you deploy an OpenShift cluster, you can configure additional items. This article covers:

- How to configure single sign-on by using Azure Active Directory (Azure AD)
- How to configure Azure Monitor logs to monitor OpenShift
- How to configure metrics and logging
- How to install Open Service Broker for Azure (OSBA)

## Configure single sign-on by using Azure Active Directory

To use Azure Active Directory for authentication, first you need to create an Azure AD app registration. This process involves two steps: creating the app registration, and configuring permissions.

### Create an app registration

These steps use the Azure CLI to create the app registration, and the GUI (portal) to set the permissions. To create the app registration, you need the following five pieces of information:

- Display name: App registration name (for example, OCPAzureAD)
- Home page: OpenShift console URL (for example, <https://masterdns343khhde.westus.cloudapp.azure.com/console>)
- Identifier URI: OpenShift console URL (for example, <https://masterdns343khhde.westus.cloudapp.azure.com/console>)
- Reply URL: Master public URL and the app registration name (for example, <https://masterdns343khhde.westus.cloudapp.azure.com/oauth2callback/OCPAzureAD>)
- Password: Secure password (use a strong password)

The following example creates an app registration by using the preceding information:

```
az ad app create --display-name OCPAzureAD --homepage
https://masterdns343khhde.westus.cloudapp.azure.com/console --reply-urls
https://masterdns343khhde.westus.cloudapp.azure.com/oauth2callback/hwocpadint --identifier-uris
https://masterdns343khhde.westus.cloudapp.azure.com/console --password {Strong Password}
```

If the command is successful, you get a JSON output similar to:

```
{
 "appId": "12345678-ca3c-427b-9a04-ab12345cd678",
 "appPermissions": null,
 "availableToOtherTenants": false,
 "displayName": "OCPAzureAD",
 "homepage": "https://masterdns343khhde.westus.cloudapp.azure.com/console",
 "identifierUris": [
 "https://masterdns343khhde.westus.cloudapp.azure.com/console"
],
 "objectId": "62cd74c9-42bb-4b9f-b2b5-b6ee88991c80",
 "objectType": "Application",
 "replyUrls": [
 "https://masterdns343khhde.westus.cloudapp.azure.com/oauth2callback/OCPAzureAD"
]
}
```

Take note of the appId property returned from the command for a later step.

In the Azure portal:

1. Select **Azure Active Directory > App Registration**.
2. Search for your app registration (for example, OCPAzureAD).
3. In the results, click the app registration.
4. Under **Settings**, select **Required permissions**.
5. Under **Required Permissions**, select **Add**.

The screenshot shows the Azure portal interface for managing app registrations. On the left, the 'OCPAzureAD' app registration is selected. In the center, the 'Required permissions' section is displayed under the 'API ACCESS' tab. The 'Required permissions' link is highlighted with a red box. On the right, a modal window titled 'Add API access' is open, showing two steps: '1 Select an API' and '2 Select permissions'. Step 1 is also highlighted with a red box.

6. Click Step 1: Select API, and then click **Windows Azure Active Directory (Microsoft.Azure.ActiveDirectory)**. Click **Select** at the bottom.

The screenshot shows the 'Select an API' modal window. It contains a search bar with the placeholder text 'Search for other applications with Service Principal name'. Below the search bar, a list of applications is displayed, with 'Windows Azure Active Directory (Microsoft.Azure.ActiveDirectory)' highlighted by a yellow box. Other items in the list include 'Office 365 Exchange Online (Microsoft.Exchange)' and others which are partially visible.

7. On Step 2: Select Permissions, select **Sign in and read user profile** under **Delegated Permissions**, and then click **Select**.

## Enable Access

| APPLICATION PERMISSIONS                    | REQUIRES ADMIN |
|--------------------------------------------|----------------|
| Read directory data                        | ✓ Yes          |
| Read and write domains                     | ✓ Yes          |
| Read and write directory data              | ✓ Yes          |
| Read and write devices                     | ✓ Yes          |
| Read all hidden memberships                | ✓ Yes          |
| Manage apps that this app creates or owns  | ✓ Yes          |
| Read and write all applications            | ✓ Yes          |
| Read and write domains                     | ✓ Yes          |
| DELEGATED PERMISSIONS                      | REQUIRES ADMIN |
| Access the directory as the signed-in user | ✗ No           |
| Read directory data                        | ✓ Yes          |
| Read and write directory data              | ✓ Yes          |
| Read and write all groups                  | ✓ Yes          |
| Read all groups                            | ✓ Yes          |
| Read all users' full profiles              | ✓ Yes          |
| Read all users' basic profiles             | ✗ No           |
| Sign in and read user profile              | ✗ No           |
| Read hidden memberships                    | ✓ Yes          |

8. Select **Done**.

### Configure OpenShift for Azure AD authentication

To configure OpenShift to use Azure AD as an authentication provider, the /etc/origin/master/master-config.yaml file must be edited on all master nodes.

Find the tenant ID by using the following CLI command:

```
az account show
```

In the yaml file, find the following lines:

```
oauthConfig:
 assetPublicURL: https://masterdns343khhde.westus.cloudapp.azure.com/console/
 grantConfig:
 method: auto
 identityProviders:
 - challenge: true
 login: true
 mappingMethod: claim
 name: htpasswd_auth
 provider:
 apiVersion: v1
 file: /etc/origin/master/htpasswd
 kind: HTPasswdPasswordIdentityProvider
```

Insert the following lines immediately after the preceding lines:

```
- name: <App Registration Name>
 challenge: false
 login: true
 mappingMethod: claim
 provider:
 apiVersion: v1
 kind: OpenIDIdentityProvider
 clientID: <appId>
 clientSecret: <Strong Password>
 claims:
 id:
 - sub
 preferredUsername:
 - unique_name
 name:
 - name
 email:
 - email
 urls:
 authorize: https://login.microsoftonline.com/<tenant Id>/oauth2/authorize
 token: https://login.microsoftonline.com/<tenant Id>/oauth2/token
```

Make sure the text aligns correctly under identityProviders. Find the tenant ID by using the following CLI command: `az account show`

Restart the OpenShift master services on all master nodes:

```
sudo /usr/local/bin/master-restart api
sudo /usr/local/bin/master-restart controllers
```

In the OpenShift console, you now see two options for authentication: htpasswd\_auth and [App Registration].

## Monitor OpenShift with Azure Monitor logs

There are three ways to add the Log Analytics agent to OpenShift.

- Install the Log Analytics agent for Linux directly on each OpenShift node
- Enable Azure Monitor VM Extension on each OpenShift node
- Install the Log Analytics agent as an OpenShift daemon-set

Read the full [instructions](#) for more details.

## Configure metrics and logging

Based on the branch, the Azure Resource Manager templates for OpenShift Container Platform and OKD may provide input parameters for enabling metrics and logging as part of the installation.

The OpenShift Container Platform Marketplace offer also provides an option to enable metrics and logging during cluster installation.

If metrics / logging wasn't enabled during the installation of the cluster, they can easily be enabled after the fact.

### Azure Cloud Provider in use

SSH to the bastion node or first master node (based on template and branch in use) using the credentials provided during deployment. Issue the following command:

```
ansible-playbook /usr/share/ansible/openshift-ansible/playbooks/openshift-metrics/config.yml \
-e openshift_metrics_install_metrics=True \
-e openshift_metrics_cassandra_storage_type=dynamic

ansible-playbook /usr/share/ansible/openshift-ansible/playbooks/openshift-logging/config.yml \
-e openshift_logging_install_logging=True \
-e openshift_logging_es_pvc_dynamic=true
```

### Azure Cloud Provider not in use

```
ansible-playbook /usr/share/ansible/openshift-ansible/playbooks/openshift-metrics/config.yml \
-e openshift_metrics_install_metrics=True

ansible-playbook /usr/share/ansible/openshift-ansible/playbooks/openshift-logging/config.yml \
-e openshift_logging_install_logging=True
```

## Install Open Service Broker for Azure (OSBA)

Open Service Broker for Azure, or OSBA, lets you provision Azure Cloud Services directly from OpenShift. OSBA is an Open Service Broker API implementation for Azure. The Open Service Broker API is a spec that defines a common language for cloud providers that cloud native applications can use to manage cloud services without lock-in.

To install OSBA on OpenShift, follow the instructions located here: <https://github.com/Azure/open-service-broker-azure#openshift-project-template>.

#### NOTE

Only complete the steps in the OpenShift Project Template section and not the entire Installing section.

## Next steps

- [Getting started with OpenShift Container Platform](#)

# Troubleshoot OpenShift Container Platform 3.11 deployment in Azure

11/13/2019 • 4 minutes to read • [Edit Online](#)

If the OpenShift cluster doesn't deploy successfully, the Azure portal will provide error output. The output may be difficult to read which makes it difficult to identify the problem. Quickly scan this output for exit code 3, 4 or 5. The following provides information on these three exit codes:

- Exit code 3: Your Red Hat Subscription User Name / Password or Organization ID / Activation Key is incorrect
- Exit code 4: Your Red Hat Pool ID is incorrect or there are no entitlements available
- Exit code 5: Unable to provision Docker Thin Pool Volume

For all other exit codes, connect to the host(s) via ssh to view the log files.

## **OpenShift Container Platform 3.11**

SSH to the ansible playbook host. For the template or the Marketplace offer, use the bastion host. From the bastion, you can SSH to all other nodes in the cluster (master, infra, CNS, compute). You'll need to be root to view the log files. Root is disabled for SSH access by default so don't use root to SSH to other nodes.

## **OKD**

SSH to the ansible playbook host. For the OKD template (version 3.9 and earlier), use the master-0 host. For the OKD template (version 3.10 and later), use the bastion host. From the ansible playbook host, you can SSH to all other nodes in the cluster (master, infra, CNS, compute). You'll need to be root (sudo su -) to view the log files. Root is disabled for SSH access by default so don't use root to SSH to other nodes.

## Log files

The log files (stderr and stdout) for the host preparation scripts are located in

`/var/lib/waagent/custom-script/download/0` on all hosts. If an error occurred during the preparation of the host, view these log files to determine the error.

If the preparation scripts ran successfully, then the log files in the `/var/lib/waagent/custom-script/download/1` directory of the ansible playbook host will need to be examined. If the error occurred during the actual installation of OpenShift, the stdout file will display the error. Use this information to contact Support for further assistance.

Example output

```

TASK [openshift_storage_glusterfs : Load heketi topology] ****
fatal: [mycluster-master-0]: FAILED! => {"changed": true, "cmd": ["oc", "--config=/tmp/openshift-glusterfs-ansible-IbhnUM/admin.kubeconfig", "rsh", "--namespace=glusterfs", "deploy-heketi-storage-1-d9x15", "heketi-cli", "-s", "http://localhost:8080", "--user", "admin", "--secret", "VuojURT0/96E42Vv8+XHfsFpSS8R20rH10iMs30qARQ=", "topology", "load", "--json=/tmp/openshift-glusterfs-ansible-IbhnUM/topology.json", "2>&1"], "delta": "0:00:21.477831", "end": "2018-05-20 02:49:11.912899", "failed": true, "failed_when_result": true, "rc": 0, "start": "2018-05-20 02:48:50.435068", "stderr": "", "stderr_lines": [], "stdout": "Creating cluster ... ID: 794b285745b1c5d7089e1c5729ec7cd2\n\tAllowing file volumes on cluster.\n\tAllowing block volumes on cluster.\n\tCreating node mycluster-cns-0 ... ID: 45f1a3bfc20a4196e59ebb567e0e02b4\n\tAdding device /dev/sdd ... OK\n\tAdding device /dev/sde ...\nOK\n\tAdding device /dev/sdf ... OK\n\tCreating node mycluster-cns-1 ... ID: 596f80d7bbd78a1ea548930f23135131\n\tAdding device /dev/sdc ... Unable to add device: Unable to execute command on glusterfs-storage-4zc42: Device /dev/sdc excluded by a filter.\n\tAdding device /dev/sde ... OK\n\tAdding device /dev/sdd ... OK\n\tCreating node mycluster-cns-2 ... ID: 42c0170aa2799559747622acceba2e3f\n\tAdding device /dev/sde ... OK\n\tAdding device /dev/sdf ...\nOK\n\tAdding device /dev/sdd ... OK", "stdout_lines": ["Creating cluster ... ID: 794b285745b1c5d7089e1c5729ec7cd2", "\tAllowing file volumes on cluster.", "\tAllowing block volumes on cluster.", "\tCreating node mycluster-cns-0 ... ID: 45f1a3bfc20a4196e59ebb567e0e02b4", "\tAdding device /dev/sdd ... OK", "\tAdding device /dev/sde ... OK", "\tAdding device /dev/sdf ... OK", "\tCreating node mycluster-cns-1 ... ID: 596f80d7bbd78a1ea548930f23135131", "\tAdding device /dev/sdc ... Unable to add device: Unable to execute command on glusterfs-storage-4zc42: Device /dev/sdc excluded by a filter.", "\tAdding device /dev/sde ... OK", "\tAdding device /dev/sdd ... OK", "\tCreating node mycluster-cns-2 ... ID: 42c0170aa2799559747622acceba2e3f", "\tAdding device /dev/sde ... OK", "\tAdding device /dev/sdf ... OK", "\tAdding device /dev/sdd ... OK"]}

PLAY RECAP ****
mycluster-cns-0 : ok=146 changed=57 unreachable=0 failed=0
mycluster-cns-1 : ok=146 changed=57 unreachable=0 failed=0
mycluster-cns-2 : ok=146 changed=57 unreachable=0 failed=0
mycluster-infra-0 : ok=143 changed=55 unreachable=0 failed=0
mycluster-infra-1 : ok=143 changed=55 unreachable=0 failed=0
mycluster-infra-2 : ok=143 changed=55 unreachable=0 failed=0
mycluster-master-0 : ok=502 changed=198 unreachable=0 failed=1
mycluster-master-1 : ok=348 changed=140 unreachable=0 failed=0
mycluster-master-2 : ok=348 changed=140 unreachable=0 failed=0
mycluster-node-0 : ok=143 changed=55 unreachable=0 failed=0
mycluster-node-1 : ok=143 changed=55 unreachable=0 failed=0
localhost : ok=13 changed=0 unreachable=0 failed=0

INSTALLER STATUS ****
Initialization : Complete (0:00:39)
Health Check : Complete (0:00:24)
etcd Install : Complete (0:01:24)
Master Install : Complete (0:14:59)
Master Additional Install : Complete (0:01:10)
Node Install : Complete (0:10:58)
GlusterFS Install : In Progress (0:03:33)
This phase can be restarted by running: playbooks/openshift-glusterfs/config.yml

Failure summary:

1. Hosts: mycluster-master-0
Play: Configure GlusterFS
Task: Load heketi topology
Message: Failed without returning a message.

```

The most common errors during installation are:

1. Private key has passphrase
2. Key vault secret with private key wasn't created correctly
3. Service principal credentials were entered incorrectly
4. Service principal doesn't have contributor access to the resource group

### Private Key has a passphrase

You'll see an error that permission was denied for ssh. ssh to the ansible playbook host to check for a passphrase on the private key.

### **Key vault secret with private key wasn't created correctly**

The private key is copied into the ansible playbook host - `~/.ssh/id_rsa`. Confirm this file is correct. Test by opening an SSH session to one of the cluster nodes from the ansible playbook host.

### **Service principal credentials were entered incorrectly**

When providing the input to the template or Marketplace offer, the incorrect information was provided. Make sure you use the correct appId (clientId) and password (clientSecret) for the service principal. Verify by issuing the following azure cli command.

```
az login --service-principal -u <client id> -p <client secret> -t <tenant id>
```

### **Service principal doesn't have contributor access to the resource group**

If the Azure cloud provider is enabled, then the service principal used must have contributor access to the resource group. Verify by issuing the following azure cli command.

```
az group update -g <openshift resource group> --set tags.sptest=test
```

## **Additional tools**

For some errors, you can also use the following commands to get more information:

1. `systemctl status <service>`
2. `journalctl -xe`

# Use Azure to host and run SAP workload scenarios

2/27/2020 • 12 minutes to read • [Edit Online](#)

When you use Microsoft Azure, you can reliably run your mission-critical SAP workloads and scenarios on a scalable, compliant, and enterprise-proven platform. You get the scalability, flexibility, and cost savings of Azure. With the expanded partnership between Microsoft and SAP, you can run SAP applications across development and test and production scenarios in Azure and be fully supported. From SAP NetWeaver to SAP S/4HANA, SAP BI on Linux to Windows, and SAP HANA to SQL, we've got you covered.

Besides hosting SAP NetWeaver scenarios with the different DBMS on Azure, you can host other SAP workload scenarios, like SAP BI on Azure.

The uniqueness of Azure for SAP HANA is an offer that sets Azure apart. To enable hosting more memory and CPU resource-demanding SAP scenarios that involve SAP HANA, Azure offers the use of customer-dedicated bare-metal hardware. Use this solution to run SAP HANA deployments that require up to 24 TB (120-TB scale-out) of memory for S/4HANA or other SAP HANA workload.

Hosting SAP workload scenarios in Azure also can create requirements of identity integration and single sign-on. This situation can occur when you use Azure Active Directory (Azure AD) to connect different SAP components and SAP software-as-a-service (SaaS) or platform-as-a-service (PaaS) offers. A list of such integration and single sign-on scenarios with Azure AD and SAP entities is described and documented in the section "AAD SAP identity integration and single sign-on."

## Changes to the SAP workload section

Changes to documents in the SAP on Azure workload section are listed at the end of this article. The entries in the change log are kept for around 180 days.

## You want to know

If you have specific questions, we are going to point you to specific documents or flows in this section of the start page. You want to know:

- What Azure VMs and HANA Large Instance units are supported for which SAP software releases and which operating system versions. Read the document [What SAP software is supported for Azure deployment](#) for answers and the process to find the information
- What SAP deployment scenarios are supported with Azure VMs and HANA Large Instances. Information about the supported scenarios can be found in the documents:
  - [SAP workload on Azure virtual machine supported scenarios](#)
  - [Supported scenarios for HANA Large Instance](#)

## SAP HANA on Azure (Large Instances)

A series of documents leads you through SAP HANA on Azure (Large Instances), or for short, HANA Large Instances. For information on HANA Large Instances start with the document [Overview and architecture of SAP HANA on Azure \(Large Instances\)](#) and go through the related documentation in the HANA Large Instance section

## SAP HANA on Azure virtual machines

This section of the documentation covers different aspects of SAP HANA. As a prerequisite, you should be familiar with the principal services of Azure that provide elementary services of Azure IaaS. So, you need knowledge of

Azure compute, storage, and networking. Many of these subjects are handled in the SAP NetWeaver-related [Azure planning guide](#).

For information on HANA on Azure, see the following articles and their subarticles:

- [Quickstart: Manual installation of single-instance SAP HANA on Azure VMs](#)
- [Deploy SAP S/4HANA or BW/4HANA on Azure](#)
- [SAP HANA infrastructure configurations and operations on Azure](#)
- [SAP HANA high availability for Azure virtual machines](#)
- [SAP HANA availability within one Azure region](#)
- [SAP HANA availability across Azure regions](#)
- [High availability of SAP HANA on Azure virtual machines](#)
- [Backup guide for SAP HANA on Azure virtual machines](#)
- [SAP HANA Azure Backup on file level](#)
- [SAP HANA backup based on storage snapshots](#)

## SAP NetWeaver deployed on Azure virtual machines

This section lists planning and deployment documentation for SAP NetWeaver and Business One on Azure. The documentation focuses on the basics and the use of non-HANA databases with an SAP workload on Azure. The documents and articles for high availability are also the foundation for HANA high availability in Azure, such as:

- [SAP Business One on Azure virtual machines](#)
- [Deploy SAP IDES EHP7 SP3 for SAP ERP 6.0 on Azure](#)
- [Run SAP NetWeaver on Microsoft Azure SUSE Linux VMs](#)
- [Azure Virtual Machines planning and implementation for SAP NetWeaver](#)
- [Azure Virtual Machines deployment for SAP NetWeaver](#)
- [Protect a multitier SAP NetWeaver application deployment by using Site Recovery](#)
- [SAP LaMa connector for Azure](#)

For information on non-HANA databases under an SAP workload on Azure, see:

- [Considerations for Azure Virtual Machines DBMS deployment for SAP workload](#)
- [SQL Server Azure Virtual Machines DBMS deployment for SAP NetWeaver](#)
- [Oracle Azure Virtual Machines DBMS deployment for SAP workload](#)
- [IBM DB2 Azure Virtual Machines DBMS deployment for SAP workload](#)
- [SAP ASE Azure Virtual Machines DBMS deployment for SAP workload](#)
- [SAP MaxDB, Live Cache, and Content Server deployment on Azure VMs](#)

For information on SAP HANA databases on Azure, see the section "SAP HANA on Azure virtual machines."

For information on high availability of an SAP workload on Azure, see:

- [Azure Virtual Machines high availability for SAP NetWeaver](#)

This document points to various other architecture and scenario documents. In later scenario documents, links to detailed technical documents that explain the deployment and configuration of the different high-availability methods are provided. The different documents that show how to establish and configure high availability for an SAP NetWeaver workload cover Linux and Windows operating systems.

For information on integration between Azure Active Directory (Azure AD) and SAP services and single sign-on, see:

- [Tutorial: Azure Active Directory integration with SAP Cloud for Customer](#)

- [Tutorial: Azure Active Directory integration with SAP Cloud Platform Identity Authentication](#)
- [Tutorial: Azure Active Directory integration with SAP Cloud Platform](#)
- [Tutorial: Azure Active Directory integration with SAP NetWeaver](#)
- [Tutorial: Azure Active Directory integration with SAP Business ByDesign](#)
- [Tutorial: Azure Active Directory integration with SAP HANA](#)
- [Your S/4HANA environment: Fiori Launchpad SAML single sign-on with Azure AD](#)

For information on integration of Azure services into SAP components, see:

- [Use SAP HANA in Power BI Desktop](#)
- [DirectQuery and SAP HANA](#)
- [Use the SAP BW Connector in Power BI Desktop](#)
- [Azure Data Factory offers SAP HANA and Business Warehouse data integration](#)

## Change Log

- 02/26/2020: Change in [SAP HANA Azure virtual machine storage configurations](#) to clarify file system choice for HANA on Azure
- 02/25/2020: Change in [High availability architecture and scenarios for SAP](#) to include the link to the HA for SAP NetWeaver on Azure VMs on RHEL multi-SID guide
- 02/26/2020: Change in [High availability for SAP NW on Azure VMs on SLES for SAP applications](#), [High availability for SAP NW on Azure VMs on SLES with ANF for SAP applications](#), [Azure VMs high availability for SAP NetWeaver on RHEL](#) and [Azure VMs high availability for SAP NetWeaver on RHEL with Azure NetApp Files](#) to remove the statement that multi-SID ASCS/ERS cluster is not supported
- 02/26/2020: Release of [High availability for SAP NetWeaver on Azure VMs on RHEL multi-SID guide](#) to add a link to the SUSE multi-SID cluster guide
- 02/25/2020: Change in [High availability architecture and scenarios for SAP](#) to add links to newer HA articles
- 02/25/2020: Change in [High availability of IBM Db2 LUW on Azure VMs on SUSE Linux Enterprise Server with Pacemaker](#) to point to document that describes access to public endpoint with Standard Azure Load balancer
- 02/21/2020: Complete revision of the article [SAP ASE Azure Virtual Machines DBMS deployment for SAP workload](#)
- 02/21/2020: Change in [SAP HANA Azure virtual machine storage configuration](#) to represent new recommendation in stripe size for /hana/data and adding setting of I/O scheduler
- 02/21/2020: Changes in HANA Large Instance documents to represent newly certified SKUs of S224 and S224m
- 02/21/2020: Change in [Azure VMs high availability for SAP NetWeaver on RHEL](#) and [Azure VMs high availability for SAP NetWeaver on RHEL with Azure NetApp Files](#) to adjust the cluster constraints for enqueue server replication 2 architecture (ENSA2)
- 02/20/2020: Change in [High availability for SAP NetWeaver on Azure VMs on SLES multi-SID guide](#) to add a link to the SUSE multi-SID cluster guide
- 02/13/2020: Changes to [Azure Virtual Machines planning and implementation for SAP NetWeaver](#) to implement links to new documents
- 02/13/2020: Added new document [SAP workload on Azure virtual machine supported scenario](#)
- 02/13/2020: Added new document [What SAP software is supported for Azure deployment](#)
- 02/13/2020: Change in [High availability of IBM Db2 LUW on Azure VMs on Red Hat Enterprise Linux Server](#) to point to document that describes access to public endpoint with Standard Azure Load balancer
- 02/13/2020: Add the new VM types to [SAP certifications and configurations running on Microsoft Azure](#)
- 02/13/2020: Add new SAP support notes [SAP workloads on Azure: planning and deployment checklist](#)
- 02/13/2020: Change in [Azure VMs high availability for SAP NetWeaver on RHEL](#) and [Azure VMs high availability for SAP NetWeaver on RHEL with Azure NetApp Files](#)

availability for SAP NetWeaver on RHEL with Azure NetApp Files to align the cluster resources timeouts to the Red Hat timeout recommendations

- 02/11/2020: Release of [SAP HANA on Azure Large Instance migration to Azure Virtual Machines](#)
- 02/07/2020: Change in [Public endpoint connectivity for VMs using Azure Standard ILB in SAP HA scenarios](#) to update sample NSG screenshot
- 02/03/2020: Change in [High availability for SAP NW on Azure VMs on SLES for SAP applications](#) and [High availability for SAP NW on Azure VMs on SLES with ANF for SAP applications](#) to remove the warning about using dash in the host names of cluster nodes on SLES
- 01/28/2020: Change in [High availability of SAP HANA on Azure VMs on RHEL](#) to align the SAP HANA cluster resources timeouts to the Red Hat timeout recommendations
- 01/17/2020: Change in [Azure proximity placement groups for optimal network latency with SAP applications](#) to change the section of moving existing VMs into a proximity placement group
- 01/17/2020: Change in [SAP workload configurations with Azure Availability Zones](#) to point to procedure that automates measurements of latency between Availability Zones
- 01/16/2020: Change in [How to install and configure SAP HANA \(Large Instances\) on Azure](#) to adapt OS releases to HANA IaaS hardware directory
- 01/16/2020: Changes in [High availability for SAP NetWeaver on Azure VMs on SLES multi-SID guide](#) to add instructions for SAP systems, using enqueue server 2 architecture (ENSA2)
- 01/10/2020: Changes in [SAP HANA scale-out with standby node on Azure VMs with Azure NetApp Files on SLES](#) and in [SAP HANA scale-out with standby node on Azure VMs with Azure NetApp Files on RHEL](#) to add instructions on how to make `nfs4_disable_idmapping` changes permanent.
- 01/10/2020: Changes in [High availability for SAP NetWeaver on Azure VMs on SLES with Azure NetApp Files for SAP applications](#) and in [Azure Virtual Machines high availability for SAP NetWeaver on RHEL with Azure NetApp Files for SAP applications](#) to add instructions how to mount Azure NetApp Files NFSv4 volumes.
- 12/23/2019: Release of [High availability for SAP NetWeaver on Azure VMs on SLES multi-SID guide](#)
- 12/18/2019: Release of [SAP HANA scale-out with standby node on Azure VMs with Azure NetApp Files on RHEL](#)
- 11/21/2019: Changes in [SAP HANA scale-out with standby node on Azure VMs with Azure NetApp Files on SUSE Linux Enterprise Server](#) to simplify the configuration for NFS ID mapping and change the recommended primary network interface to simplify routing.
- 11/15/2019: Minor changes in [High availability for SAP NetWeaver on SUSE Linux Enterprise Server with Azure NetApp Files for SAP applications](#) and [High availability for SAP NetWeaver on Red Hat Enterprise Linux with Azure NetApp Files for SAP applications](#) to clarify capacity pool size restrictions and remove statement that only NFSv3 version is supported.
- 11/12/2019: Release of [High availability for SAP NetWeaver on Windows with Azure NetApp Files \(SMB\)](#)
- 11/08/2019: Changes in [High availability of SAP HANA on Azure VMs on SUSE Linux Enterprise Server](#), [Set up SAP HANA System Replication on Azure virtual machines \(VMs\)](#), [Azure Virtual Machines high availability for SAP NetWeaver on SUSE Linux Enterprise Server for SAP applications](#), [Azure Virtual Machines high availability for SAP NetWeaver on SUSE Linux Enterprise Server with Azure NetApp Files](#), [Azure Virtual Machines high availability for SAP NetWeaver on Red Hat Enterprise Linux](#), [Azure Virtual Machines high availability for SAP NetWeaver on Red Hat Enterprise Linux with Azure NetApp Files](#), [High availability for NFS on Azure VMs on SUSE Linux Enterprise Server](#), [GlusterFS on Azure VMs on Red Hat Enterprise Linux for SAP NetWeaver](#) to recommend Azure standard load balancer
- 11/08/2019: Changes in [SAP workload planning and deployment checklist](#) to clarify encryption recommendation
- 11/04/2019: Changes in [Setting up Pacemaker on SUSE Linux Enterprise Server in Azure](#) to create the cluster directly with unicast configuration
- 10/29/2019: Release of [Public endpoint connectivity for Virtual Machines using Azure Standard Load Balancer in SAP high-availability scenarios](#)

- 10/25/2019: Changes in [SAP HANA Azure virtual machine storage configurations](#) and [SAP HANA scale-out with standby node on Azure VMs with Azure NetApp Files on SUSE Linux Enterprise Server](#) to clarify NFS protocol for /hana/shared volume
- 10/22/2019: Change in [High availability for SAP NetWeaver on Azure VMs on SUSE Linux Enterprise Server for SAP applications](#), [High availability for SAP NetWeaver on Azure VMs on SUSE Linux Enterprise Server with Azure NetApp Files for SAP applications](#), [High availability for NFS on Azure VMs on SUSE Linux Enterprise Server](#), [Setting up Pacemaker on SUSE Linux Enterprise Server in Azure](#), [High availability of IBM Db2 LUW on Azure VMs on SUSE Linux Enterprise Server with Pacemaker](#), and [High availability of SAP HANA on Azure VMs on SUSE Linux Enterprise Server](#) for Azure Load-Balancer Detection Hardening
- Changes ANF section and header section in [SAP HANA Azure virtual machine storage configurations](#)
- 10/21/2019: Release of [SAP HANA scale-out with standby node on Azure VMs with Azure NetApp Files on SLES](#)
- 10/16/2019: Fix broken links in [Backup and restore](#)
- 10/16/2019: Change the minimum recommended OS from SLES 12 SP3 to SLES 12 SP4 in [High availability of IBM Db2 LUW on Azure VMs on SUSE Linux Enterprise Server with Pacemaker](#)
- 10/11/2019: Changes to Ultra disk storage configurations and introduction of ANF in [SAP HANA Azure virtual machine storage configurations](#)
- 10/01/2019: Change in [graphics of Azure proximity placement groups for optimal network latency with SAP applications](#) to get more clarity
- 10/01/2019: Change in [SAP HANA infrastructure configurations and operations on Azure](#) to correct statements around highly available NFS share for /hana/shared.
- 09/28/2019: Change in [Setting up Pacemaker on Red Hat Enterprise Linux in Azure](#) to clarify SBD as a fencing mechanism is not supported on RHEL clusters
- 09/17/2019: Change in NetWeaver Planning and Deployment Guide to unify terms around VM Extension for SAP
- 08/22/2019: Changes in [Setting up Pacemaker on SUSE Linux Enterprise Server in Azure](#) to update the URLs for custom role creation
- 08/16/2019: Changes in [Setting up Pacemaker on Red Hat Enterprise Linux in Azure](#) to remind customers to update the actions in the custom role, if updating to the new version of the Azure fence agent
- 08/15/2019: Changes in [SAP HANA Azure virtual machine storage configurations](#) to reflect General Availability of Ultra disk (formerly Ultra SSD)
- 08/01/2019: Changes to [Setting up Pacemaker on SUSE Linux Enterprise Server in Azure](#) to integrate changes specifically for SLES 15

# Create an Oracle Database in an Azure VM

1/8/2020 • 6 minutes to read • [Edit Online](#)

This guide details using the Azure CLI to deploy an Azure virtual machine from the [Oracle marketplace gallery image](#) in order to create an Oracle 12c database. Once the server is deployed, you will connect via SSH in order to configure the Oracle database.

If you don't have an Azure subscription, create a [free account](#) before you begin.

If you choose to install and use the CLI locally, this quickstart requires that you are running the Azure CLI version 2.0.4 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

## Create a resource group

Create a resource group with the `az group create` command. An Azure resource group is a logical container into which Azure resources are deployed and managed.

The following example creates a resource group named *myResourceGroup* in the *eastus* location.

```
az group create --name myResourceGroup --location eastus
```

## Create virtual machine

To create a virtual machine (VM), use the `az vm create` command.

The following example creates a VM named `myVM`. It also creates SSH keys, if they do not already exist in a default key location. To use a specific set of keys, use the `--ssh-key-value` option.

```
az vm create \
 --resource-group myResourceGroup \
 --name myVM \
 --image Oracle:Oracle-Database-Ee:12.1.0.2:latest \
 --size Standard_DS2_v2 \
 --admin-username azureuser \
 --generate-ssh-keys
```

After you create the VM, Azure CLI displays information similar to the following example. Note the value for `publicIpAddress`. You use this address to access the VM.

```
{
 "fqdns": "",
 "id": "/subscriptions/{snip}/resourceGroups/myResourceGroup/providers/Microsoft.Compute/virtualMachines/myVM",
 "location": "westus",
 "macAddress": "00-0D-3A-36-2F-56",
 "powerState": "VM running",
 "privateIpAddress": "10.0.0.4",
 "publicIpAddress": "13.64.104.241",
 "resourceGroup": "myResourceGroup"
}
```

## Connect to the VM

To create an SSH session with the VM, use the following command. Replace the IP address with the `publicIpAddress` value for your VM.

```
ssh azureuser@<publicIpAddress>
```

## Create the database

The Oracle software is already installed on the Marketplace image. Create a sample database as follows.

1. Switch to the *oracle* superuser, then initialize the listener for logging:

```
$ sudo su - oracle
$ lsnrctl start
```

The output is similar to the following:

```
Copyright (c) 1991, 2014, Oracle. All rights reserved.

Starting /u01/app/oracle/product/12.1.0/dbhome_1/bin/tnslsnr: please wait...

TNSLSNR for Linux: Version 12.1.0.2.0 - Production
Log messages written to /u01/app/oracle/diag/tnslsnr/myVM/listener/alert/log.xml
Listening on: (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)
(HOST=myVM.twltkue3xvsujaz1bvlrhfuiwf.dx.internal.cloudapp.net)(PORT=1521)))

Connecting to (ADDRESS=(PROTOCOL=tcp)(HOST=)(PORT=1521))
STATUS of the LISTENER

Alias LISTENER
Version TNSLSNR for Linux: Version 12.1.0.2.0 - Production
Start Date 23-MAR-2017 15:32:08
Uptime 0 days 0 hr. 0 min. 0 sec
Trace Level off
Security ON: Local OS Authentication
SNMP OFF
Listener Log File /u01/app/oracle/diag/tnslsnr/myVM/listener/alert/log.xml
Listening Endpoints Summary...
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=myVM.twltkue3xvsujaz1bvlrhfuiwf.dx.internal.cloudapp.net)
(PORT=1521)))
The listener supports no services
The command completed successfully
```

2. Create the database:

```
dbca -silent \
 -createDatabase \
 -templateName General_Purpose.dbc \
 -gdbname cdb1 \
 -sid cdb1 \
 -responseFile NO_VALUE \
 -characterSet AL32UTF8 \
 -sysPassword OraPasswd1 \
 -systemPassword OraPasswd1 \
 -createAsContainerDatabase true \
 -numberOfPDBs 1 \
 -pdbName pdb1 \
 -pdbAdminPassword OraPasswd1 \
 -databaseType MULTIPURPOSE \
 -automaticMemoryManagement false \
 -storageType FS \
 -ignorePreReqs
```

It takes a few minutes to create the database.

### 3. Set Oracle variables

Before you connect, you need to set two environment variables: *ORACLE\_HOME* and *ORACLE\_SID*.

```
ORACLE_HOME=/u01/app/oracle/product/12.1.0/dbhome_1; export ORACLE_HOME
ORACLE_SID=cdb1; export ORACLE_SID
```

You also can add *ORACLE\_HOME* and *ORACLE\_SID* variables to the .bashrc file. This would save the environment variables for future sign-ins. Confirm the following statements have been added to the `~/.bashrc` file using editor of your choice.

```
Add ORACLE_HOME.
export ORACLE_HOME=/u01/app/oracle/product/12.1.0/dbhome_1
Add ORACLE_SID.
export ORACLE_SID=cdb1
```

## Oracle EM Express connectivity

For a GUI management tool that you can use to explore the database, set up Oracle EM Express. To connect to Oracle EM Express, you must first set up the port in Oracle.

### 1. Connect to your database using sqlplus:

```
sqlplus / as sysdba
```

### 2. Once connected, set the port 5502 for EM Express

```
exec DBMS_XDB_CONFIG.SETHTTPSPORT(5502);
```

### 3. Open the container PDB1 if not already opened, but first check the status:

```
select con_id, name, open_mode from v$pdbs;
```

The output is similar to the following:

| CON_ID | NAME      | OPEN_MODE |
|--------|-----------|-----------|
| 2      | PDB\$SEED | READ ONLY |
| 3      | PDB1      | MOUNT     |

4. If the OPEN\_MODE for `PDB1` is not READ WRITE, then run the followings commands to open PDB1:

```
alter session set container=pdb1;
alter database open;
```

You need to type `quit` to end the sqlplus session and type `exit` to logout of the oracle user.

## Automate database startup and shutdown

The Oracle database by default doesn't automatically start when you restart the VM. To set up the Oracle database to start automatically, first sign in as root. Then, create and update some system files.

1. Sign on as root

```
sudo su -
```

2. Using your favorite editor, edit the file `/etc/oratab` and change the default `N` to `Y`:

```
cdb1:/u01/app/oracle/product/12.1.0/dbhome_1:Y
```

3. Create a file named `/etc/init.d/dbora` and paste the following contents:

```
#!/bin/sh
chkconfig: 345 99 10
Description: Oracle auto start-stop script.
#
Set ORA_HOME to be equivalent to $ORACLE_HOME.
ORA_HOME=/u01/app/oracle/product/12.1.0/dbhome_1
ORA_OWNER=oracle

case "$1" in
'start')
 # Start the Oracle databases:
 # The following command assumes that the Oracle sign-in
 # will not prompt the user for any values.
 # Remove "&" if you don't want startup as a background process.
 su - $ORA_OWNER -c "$ORA_HOME/bin/dbstart $ORA_HOME" &
 touch /var/lock/subsys/dbora
 ;;

'stop')
 # Stop the Oracle databases:
 # The following command assumes that the Oracle sign-in
 # will not prompt the user for any values.
 su - $ORA_OWNER -c "$ORA_HOME/bin/dbshut $ORA_HOME" &
 rm -f /var/lock/subsys/dbora
 ;;
esac
```

4. Change permissions on files with `chmod` as follows:

```
chgrp dba /etc/init.d/dbora
chmod 750 /etc/init.d/dbora
```

5. Create symbolic links for startup and shutdown as follows:

```
ln -s /etc/init.d/dbora /etc/rc.d/rc0.d/K01dbora
ln -s /etc/init.d/dbora /etc/rc.d/rc3.d/S99dbora
ln -s /etc/init.d/dbora /etc/rc.d/rc5.d/S99dbora
```

6. To test your changes, restart the VM:

```
reboot
```

## Open ports for connectivity

The final task is to configure some external endpoints. To set up the Azure Network Security Group that protects the VM, first exit your SSH session in the VM (should have been kicked out of SSH when rebooting in previous step).

1. To open the endpoint that you use to access the Oracle database remotely, create a Network Security Group rule with [az network nsg rule create](#) as follows:

```
az network nsg rule create \
 --resource-group myResourceGroup\
 --nsg-name myVmNSG \
 --name allow-oracle \
 --protocol tcp \
 --priority 1001 \
 --destination-port-range 1521
```

2. To open the endpoint that you use to access Oracle EM Express remotely, create a Network Security Group rule with [az network nsg rule create](#) as follows:

```
az network nsg rule create \
 --resource-group myResourceGroup \
 --nsg-name myVmNSG \
 --name allow-oracle-EM \
 --protocol tcp \
 --priority 1002 \
 --destination-port-range 5502
```

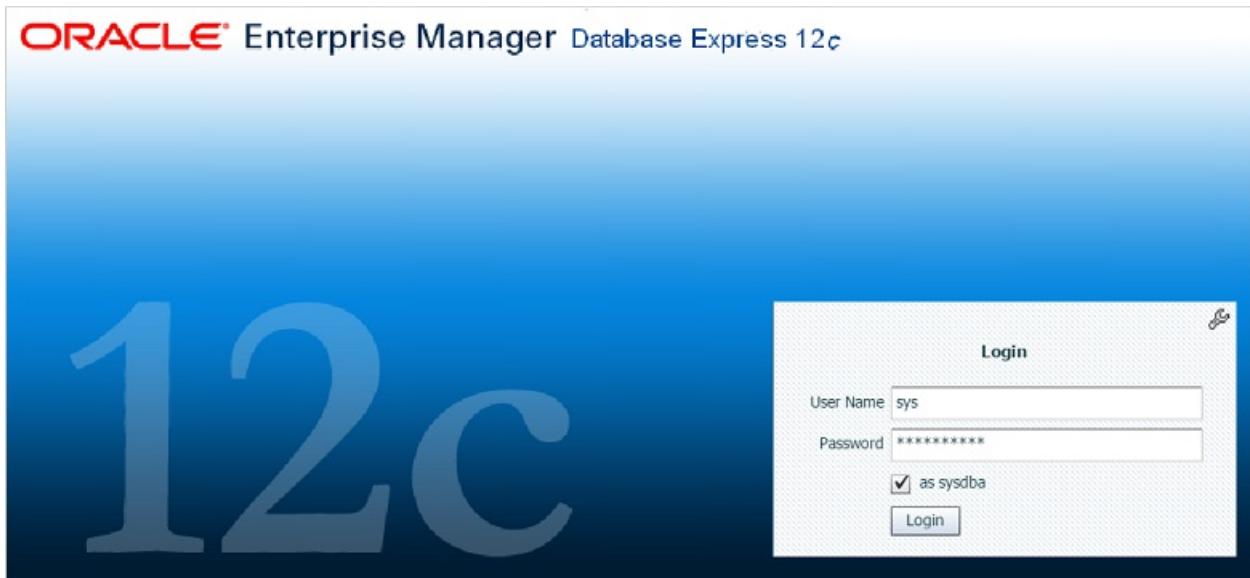
3. If needed, obtain the public IP address of your VM again with [az network public-ip show](#) as follows:

```
az network public-ip show \
 --resource-group myResourceGroup \
 --name myVMPublicIP \
 --query [ipAddress] \
 --output tsv
```

4. Connect EM Express from your browser. Make sure your browser is compatible with EM Express (Flash install is required):

```
https://<VM ip address or hostname>:5502/em
```

You can log in by using the **SYS** account, and check the **as sysdba** checkbox. Use the password **OraPasswd1** that you set during installation.



## Clean up resources

Once you have finished exploring your first Oracle database on Azure and the VM is no longer needed, you can use the [az group delete](#) command to remove the resource group, VM, and all related resources.

```
az group delete --name myResourceGroup
```

## Next steps

Learn about other Oracle solutions on Azure.

Try the [Installing and Configuring Oracle Automated Storage Management](#) tutorial.

# Install the Elastic Stack on an Azure VM

2/4/2019 • 5 minutes to read • [Edit Online](#)

This article walks you through how to deploy [Elasticsearch](#), [Logstash](#), and [Kibana](#), on an Ubuntu VM in Azure. To see the Elastic Stack in action, you can optionally connect to Kibana and work with some sample logging data.

In this tutorial you learn how to:

- Create an Ubuntu VM in an Azure resource group
- Install Elasticsearch, Logstash, and Kibana on the VM
- Send sample data to Elasticsearch with Logstash
- Open ports and work with data in the Kibana console

This deployment is suitable for basic development with the Elastic Stack. For more on the Elastic Stack, including recommendations for a production environment, see the [Elastic documentation](#) and the [Azure Architecture Center](#).

## Use Azure Cloud Shell

Azure hosts Azure Cloud Shell, an interactive shell environment that you can use through your browser. You can use either Bash or PowerShell with Cloud Shell to work with Azure services. You can use the Cloud Shell preinstalled commands to run the code in this article without having to install anything on your local environment.

To start Azure Cloud Shell:

| OPTION                                                                                                                                                    | EXAMPLE/LINK                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Select <b>Try It</b> in the upper-right corner of a code block.<br>Selecting <b>Try It</b> doesn't automatically copy the code to Cloud Shell.            |  |
| Go to <a href="https://shell.azure.com">https://shell.azure.com</a> , or select the <b>Launch Cloud Shell</b> button to open Cloud Shell in your browser. |  |
| Select the <b>Cloud Shell</b> button on the menu bar at the upper right in the <a href="#">Azure portal</a> .                                             |  |

To run the code in this article in Azure Cloud Shell:

1. Start Cloud Shell.
2. Select the **Copy** button on a code block to copy the code.
3. Paste the code into the Cloud Shell session by selecting **Ctrl+Shift+V** on Windows and Linux or by selecting **Cmd+Shift+V** on macOS.
4. Select **Enter** to run the code.

If you choose to install and use the CLI locally, this tutorial requires that you are running the Azure CLI version 2.0.4 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

## Create a resource group

Create a resource group with the `az group create` command. An Azure resource group is a logical container into

which Azure resources are deployed and managed.

The following example creates a resource group named *myResourceGroup* in the *eastus* location.

```
az group create --name myResourceGroup --location eastus
```

## Create a virtual machine

Create a VM with the [az vm create](#) command.

The following example creates a VM named *myVM* and creates SSH keys if they do not already exist in a default key location. To use a specific set of keys, use the `--ssh-key-value` option.

```
az vm create \
 --resource-group myResourceGroup \
 --name myVM \
 --image UbuntuLTS \
 --admin-username azureuser \
 --generate-ssh-keys
```

When the VM has been created, the Azure CLI shows information similar to the following example. Take note of the `publicIpAddress`. This address is used to access the VM.

```
{
 "fqdns": "",
 "id": "/subscriptions/<subscription
ID>/resourceGroups/myResourceGroup/providers/Microsoft.Compute/virtualMachines/myVM",
 "location": "eastus",
 "macAddress": "00-0D-3A-23-9A-49",
 "powerState": "VM running",
 "privateIpAddress": "10.0.0.4",
 "publicIpAddress": "40.68.254.142",
 "resourceGroup": "myResourceGroup"
}
```

## SSH into your VM

If you don't already know the public IP address of your VM, run the [az network public-ip list](#) command:

```
az network public-ip list --resource-group myResourceGroup --query [].ipAddress
```

Use the following command to create an SSH session with the virtual machine. Substitute the correct public IP address of your virtual machine. In this example, the IP address is *40.68.254.142*.

```
ssh azureuser@40.68.254.142
```

## Install the Elastic Stack

Import the Elasticsearch signing key and update your APT sources list to include the Elastic package repository:

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
echo "deb https://artifacts.elastic.co/packages/5.x/apt stable main" | sudo tee -a
/etc/apt/sources.list.d/elastic-5.x.list
```

Install the Java Virtual on the VM and configure the JAVA\_HOME variable-this is necessary for the Elastic Stack components to run.

```
sudo apt update && sudo apt install openjdk-8-jre-headless
export JAVA_HOME=/usr/lib/jvm/java-8-openjdk-amd64
```

Run the following commands to update Ubuntu package sources and install Elasticsearch, Kibana, and Logstash.

```
sudo apt update && sudo apt install elasticsearch kibana logstash
```

#### NOTE

Detailed installation instructions, including directory layouts and initial configuration, are maintained in [Elastic's documentation](#)

## Start Elasticsearch

Start Elasticsearch on your VM with the following command:

```
sudo systemctl start elasticsearch.service
```

This command produces no output, so verify that Elasticsearch is running on the VM with this `curl` command:

```
sudo curl -XGET 'localhost:9200/'
```

If Elasticsearch is running, you see output like the following:

```
{
 "name" : "w6Z4NwR",
 "cluster_name" : "elasticsearch",
 "cluster_uuid" : "SDzCajBoSK2EkXmHvJVaDQ",
 "version" : {
 "number" : "5.6.3",
 "build_hash" : "1a2f265",
 "build_date" : "2017-10-06T20:33:39.012Z",
 "build_snapshot" : false,
 "lucene_version" : "6.6.1"
 },
 "tagline" : "You Know, for Search"
}
```

## Start Logstash and add data to Elasticsearch

Start Logstash with the following command:

```
sudo systemctl start logstash.service
```

Test Logstash in interactive mode to make sure it's working correctly:

```
sudo /usr/share/logstash/bin/logstash -e 'input { stdin { } } output { stdout { } }'
```

This is a basic logstash [pipeline](#) that echoes standard input to standard output.

```
The stdin plugin is now waiting for input:
hello azure
2017-10-11T20:01:08.904Z myVM hello azure
```

Set up Logstash to forward the kernel messages from this VM to Elasticsearch. Create a new file in an empty directory called `vm-syslog-logstash.conf` and paste in the following Logstash configuration:

```
input {
 stdin {
 type => "stdin-type"
 }

 file {
 type => "syslog"
 path => ["/var/log/*.log", "/var/log/*/*.log", "/var/log/messages", "/var/log/syslog"]
 start_position => "beginning"
 }
}

output {

 stdout {
 codec => rubydebug
 }
 elasticsearch {
 hosts => "localhost:9200"
 }
}
```

Test this configuration and send the syslog data to Elasticsearch:

```
sudo /usr/share/logstash/bin/logstash -f vm-syslog-logstash.conf
```

You see the syslog entries in your terminal echoed as they are sent to Elasticsearch. Use `CTRL+C` to exit out of Logstash once you've sent some data.

## Start Kibana and visualize the data in Elasticsearch

Edit `/etc/kibana/kibana.yml` and change the IP address Kibana listens on so you can access it from your web browser.

```
server.host:"0.0.0.0"
```

Start Kibana with the following command:

```
sudo systemctl start kibana.service
```

Open port 5601 from the Azure CLI to allow remote access to the Kibana console:

```
az vm open-port --port 5601 --resource-group myResourceGroup --name myVM
```

Open up the Kibana console and select **Create** to generate a default index based on the syslog data you sent to Elasticsearch earlier.

Management / Kibana

Index Patterns Saved Objects Advanced Settings

Configure an index pattern

In order to use Kibana you must configure at least one index pattern. Index patterns are used to identify the Elasticsearch index to run search and analytics against. They are also used to configure fields.

**Index pattern** [advanced options](#)

logstash-\*

Patterns allow you to define dynamic index names using \* as a wildcard. Example: logstash-\*

**Time Filter field name** [refresh fields](#)

@timestamp

Expand index pattern when searching [DEPRECATED]

With this option selected, searches against any time-based index pattern that contains a wildcard will automatically be expanded to query only the indices that contain data within the currently selected time range.

Searching against the index pattern logstash-\* will actually query Elasticsearch for the specific matching indices (e.g. logstash-2015.12.21) that fall within the current time range.

With recent changes to Elasticsearch, this option should no longer be necessary and will likely be removed in future versions of Kibana.

Use event times to create index names [DEPRECATED]

**Create**

Select **Discover** on the Kibana console to search, browse, and filter through the syslog events.

Kibana

12 hits

Search... (e.g. status:200 AND extension:PHP)

Uses lucene query syntax

Actions ▾

**logstash-\***

Selected Fields

⌚ @timestamp  
t @version  
t message  
t type

Available Fields

t \_id  
t \_index  
# \_score  
t \_type  
t host  
t path

| Time                            | @timestamp                      | @version | message                                                                                                                                                                                | type   |
|---------------------------------|---------------------------------|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| October 13th 2017, 14:05:25.686 | October 13th 2017, 14:05:25.686 | 1        | [2017-10-13T21:05:24,910] [WARN] syslog [o.e.d.i.m.TypeParsers ] field [include_in_all] is deprecated, as [__all] is deprecated, and will be disallowed in 6.0, use [copy_to] instead. | syslog |
| October 13th 2017, 14:05:25.687 | October 13th 2017, 14:05:25.687 | 1        | [2017-10-13T21:05:24,907] [WARN] syslog [o.e.d.i.m.TypeParsers ] field [include_in_all] is deprecated, as [__all] is deprecated, and will be disallowed in 6.0, use [copy_to] instead. | syslog |
| October 13th 2017, 14:05:25.686 | October 13th 2017, 14:05:25.686 | 1        | [2017-10-13T21:05:24,889] [WARN] syslog [o.e.d.i.m.TypeParsers ] field [include_in_all] is                                                                                             | syslog |

## Next steps

In this tutorial, you deployed the Elastic Stack into a development VM in Azure. You learned how to:

- Create an Ubuntu VM in an Azure resource group
- Install Elasticsearch, Logstash, and Kibana on the VM
- Send sample data to Elasticsearch from Logstash
- Open ports and work with data in the Kibana console

# How to use FreeBSD's Packet Filter to create a secure firewall in Azure

11/13/2019 • 2 minutes to read • [Edit Online](#)

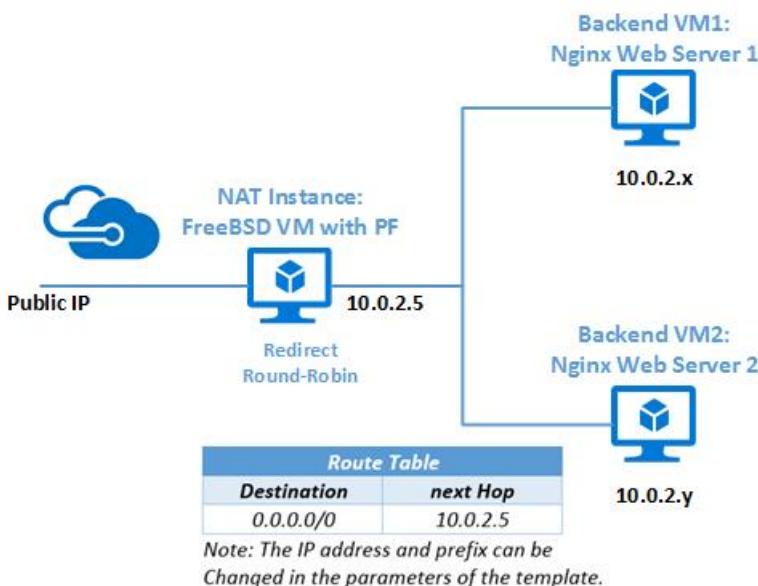
This article introduces how to deploy a NAT firewall using FreeBSD's Packer Filter through Azure Resource Manager template for common web server scenario.

## What is PF?

PF (Packet Filter, also written pf) is a BSD licensed stateful packet filter, a central piece of software for firewalling. PF has since evolved quickly and now has several advantages over other available firewalls. Network Address Translation (NAT) is in PF since day one, then packet scheduler and active queue management have been integrated into PF, by integrating the ALTQ and making it configurable through PF's configuration. Features such as pfsync and CARP for failover and redundancy, authpf for session authentication, and ftp-proxy to ease firewalling the difficult FTP protocol, have also extended PF. In short, PF is a powerful and feature-rich firewall.

## Get started

If you are interested in setting up a secure firewall in the cloud for your web servers, then let's get started. You can also apply the scripts used in this Azure Resource Manager template to set up your networking topology. The Azure Resource Manager template set up a FreeBSD virtual machine that performs NAT /redirection using PF and two FreeBSD virtual machines with the Nginx web server installed and configured. In addition to performing NAT for the two web servers egress traffic, the NAT/ redirection virtual machine intercepts HTTP requests and redirect them to the two web servers in round-robin fashion. The VNet uses the private non-routable IP address space 10.0.0.2/24 and you can modify the parameters of the template. The Azure Resource Manager template also defines a route table for the whole VNet, which is a collection of individual routes used to override Azure default routes based on the destination IP address.



## Deploy through Azure CLI

You need the latest [Azure CLI](#) installed and logged in to an Azure account using [az login](#). Create a resource group with [az group create](#). The following example creates a resource group name `myResourceGroup` in the `West US` location.

```
az group create --name myResourceGroup --location westus
```

Next, deploy the template [pf-freebsd-setup](#) with `az group deployment create`. Download `azuredeploy.parameters.json` under the same path and define your own resource values, such as `adminPassword`, `networkPrefix`, and `domainNamePrefix`.

```
az group deployment create --resource-group myResourceGroup --name myDeploymentName \
--template-uri https://raw.githubusercontent.com/Azure/azure-quickstart-templates/master/pf-freebsd-
setup/azuredeploy.json \
--parameters '@azuredeploy.parameters.json' --verbose
```

After about five minutes, you will get the information of `"provisioningState": "Succeeded"`. Then you can ssh to the frontend VM (NAT) or access Nginx web server in a browser using the public IP address or FQDN of the frontend VM (NAT). The following example lists FQDN and public IP address that assigned to the frontend VM (NAT) in the `myResourceGroup` resource group.

```
az network public-ip list --resource-group myResourceGroup
```

## Next steps

Do you want to set up your own NAT in Azure? Open Source, free but powerful? Then PF is a good choice. By using the template [pf-freebsd-setup](#), you only need five minutes to set up a NAT firewall with round-robin load balancing using FreeBSD's PF in Azure for common web server scenario.

If you want to learn the offering of FreeBSD in Azure, refer to [introduction to FreeBSD on Azure](#).

If you want to know more about PF, refer to [FreeBSD handbook](#) or [PF-User's Guide](#).

# Install MySQL on a virtual machine running OpenSUSE Linux in Azure

11/13/2019 • 2 minutes to read • [Edit Online](#)

MySQL is a popular, open-source SQL database. This tutorial shows you how to create a virtual machine running OpenSUSE Linux, then install MySQL.

If you choose to install and use the CLI locally, you need Azure CLI version 2.0 or later. To find the version, run `az --version`. If you need to install or upgrade, see [Install Azure CLI](#).

## Create a virtual machine running OpenSUSE Linux

First, create a resource group. In this example, the resource group is named *mySQLSUSEResourceGroup* and it is created in the *East US* region.

```
az group create --name mySQLSUSEResourceGroup --location eastus
```

Create the VM. In this example, the VM is named *myVM* and the VM size is *Standard\_D2s\_v3*, but you should choose the [VM size](#) you think is most appropriate for your workload.

```
az vm create --resource-group mySQLSUSEResourceGroup \
 --name myVM \
 --image openSUSE-Leap \
 --size Standard_D2s_v3 \
 --generate-ssh-keys
```

You also need to add a rule to the network security group to allow traffic over port 3306 for MySQL.

```
az vm open-port --port 3306 --resource-group mySQLSUSEResourceGroup --name myVM
```

## Connect to the VM

You'll use SSH to connect to the VM. In this example, the public IP address of the VM is *10.111.112.113*. You can see the IP address in the output when you created the VM.

```
ssh 10.111.112.113
```

## Update the VM

After you're connected to the VM, install system updates and patches.

```
sudo zypper update
```

Follow the prompts to update your VM.

## Install MySQL

Install the MySQL in the VM over SSH. Reply to prompts as appropriate.

```
sudo zypper install mysql
```

Set MySQL to start when the system boots.

```
sudo systemctl enable mysql
```

Verify that MySQL is enabled.

```
systemctl is-enabled mysql
```

This should return: enabled.

Restart the server.

```
sudo reboot
```

## MySQL password

After installation, the MySQL root password is empty by default. Run the **mysql\_secure\_installation** script to secure MySQL. The script prompts you to change the MySQL root password, remove anonymous user accounts, disable remote root sign in, remove test databases, and reload the privileges table.

Once the server reboots, ssh to the VM again.

```
ssh 10.111.112.113
```

```
mysql_secure_installation
```

## Sign in to MySQL

You can now sign in and enter the MySQL prompt.

```
mysql -u root -p
```

This switches you to the MySQL prompt where you can issue SQL statements to interact with the database.

Now, create a new MySQL user.

```
CREATE USER 'mysqluser'@'localhost' IDENTIFIED BY 'password';
```

The semi-colon (;) at the end of the line is crucial for ending the command.

## Create a database

Create a database and grant the `mysqluser` user permissions.

```
CREATE DATABASE testdatabase;
GRANT ALL ON testdatabase.* TO 'mysqluser'@'localhost' IDENTIFIED BY 'password';
```

Database user names and passwords are only used by scripts connecting to the database. Database user account names do not necessarily represent actual user accounts on the system.

Enable sign in from another computer. In this example, the IP address of the computer to allow sign in from is 10.112.113.114.

```
GRANT ALL ON testdatabase.* TO 'mysqluser'@'10.112.113.114' IDENTIFIED BY 'password';
```

To exit the MySQL database administration utility, type:

```
quit
```

## Next steps

For details about MySQL, see the [MySQL Documentation](#).

# How to install and configure MongoDB on a Linux VM

12/23/2019 • 5 minutes to read • [Edit Online](#)

MongoDB is a popular open-source, high-performance NoSQL database. This article shows you how to install and configure MongoDB on a Linux VM with the Azure CLI. Examples are shown that detail how to:

- [Manually install and configure a basic MongoDB instance](#)
- [Create a basic MongoDB instance using a Resource Manager template](#)
- [Create a complex MongoDB sharded cluster with replica sets using a Resource Manager template](#)

## Manually install and configure MongoDB on a VM

MongoDB [provide installation instructions](#) for Linux distros including Red Hat / CentOS, SUSE, Ubuntu, and Debian. The following example creates a *CentOS* VM. To create this environment, you need the latest [Azure CLI](#) installed and logged in to an Azure account using [az login](#).

Create a resource group with [az group create](#). The following example creates a resource group named *myResourceGroup* in the *eastus* location:

```
az group create --name myResourceGroup --location eastus
```

Create a VM with [az vm create](#). The following example creates a VM named *myVM* with a user named *azureuser* using SSH public key authentication

```
az vm create \
 --resource-group myResourceGroup \
 --name myVM \
 --image CentOS \
 --admin-username azureuser \
 --generate-ssh-keys
```

SSH to the VM using your own username and the `publicIpAddress` listed in the output from the previous step:

```
ssh azureuser@<publicIpAddress>
```

To add the installation sources for MongoDB, create a **yum** repository file as follows:

```
sudo touch /etc/yum.repos.d/mongodb-org-3.6.repo
```

Open the MongoDB repo file for editing, such as with `vi` or `nano`. Add the following lines:

```
[mongodb-org-3.6]
name=MongoDB Repository
baseurl=https://repo.mongodb.org/yum/redhat/$releasever/mongodb-org/3.6/x86_64/
gpgcheck=1
enabled=1
gpgkey=https://www.mongodb.org/static/pgp/server-3.6.asc
```

Install MongoDB using **yum** as follows:

```
sudo yum install -y mongodb-org
```

By default, SELinux is enforced on CentOS images that prevents you from accessing MongoDB. Install policy management tools and configure SELinux to allow MongoDB to operate on its default TCP port 27017 as follows:

```
sudo yum install -y policycoreutils-python
sudo semanage port -a -t mongod_port_t -p tcp 27017
```

Start the MongoDB service as follows:

```
sudo service mongod start
```

Verify the MongoDB installation by connecting using the local `mongo` client:

```
mongo
```

Now test the MongoDB instance by adding some data and then searching:

```
> db
test
> db.foo.insert({ a : 1 })
> db.foo.find()
{ "_id" : ObjectId("57ec477cd639891710b90727"), "a" : 1 }
> exit
```

If desired, configure MongoDB to start automatically during a system reboot:

```
sudo chkconfig mongod on
```

## Create basic MongoDB instance on CentOS using a template

You can create a basic MongoDB instance on a single CentOS VM using the following Azure quickstart template from GitHub. This template uses the Custom Script extension for Linux to add a **yum** repository to your newly created CentOS VM and then install MongoDB.

- Basic MongoDB instance on CentOS - <https://raw.githubusercontent.com/Azure/azure-quickstart-templates/master/mongodb-on-centos/azuredploy.json>

To create this environment, you need the latest [Azure CLI](#) installed and logged in to an Azure account using `az login`. First, create a resource group with `az group create`. The following example creates a resource group named `myResourceGroup` in the `eastus` location:

```
az group create --name myResourceGroup --location eastus
```

Next, deploy the MongoDB template with `az group deployment create`. When prompted, enter your own unique values for `newStorageAccountName`, `dnsNameForPublicIP`, and admin username and password:

```
az group deployment create --resource-group myResourceGroup \
--template-uri https://raw.githubusercontent.com/Azure/azure-quickstart-templates/master/mongodb-on-
centos/azuredeploy.json
```

Log on to the VM using the public DNS address of your VM. You can view the public DNS address with [az vm show](#):

```
az vm show -g myResourceGroup -n myLinuxVM -d --query [fqdns] -o tsv
```

SSH to your VM using your own username and public DNS address:

```
ssh azureuser@mypublicdns.eastus.cloudapp.azure.com
```

Verify the MongoDB installation by connecting using the local `mongo` client as follows:

```
mongo
```

Now test the instance by adding some data and searching as follows:

```
> db
test
> db.foo.insert({ a : 1 })
> db.foo.find()
{ "_id" : ObjectId("57ec477cd639891710b90727"), "a" : 1 }
> exit
```

## Create a complex MongoDB Sharded Cluster on CentOS using a template

You can create a complex MongoDB sharded cluster using the following Azure quickstart template from GitHub. This template follows the [MongoDB sharded cluster best practices](#) to provide redundancy and high availability. The template creates two shards, with three nodes in each replica set. One config server replica set with three nodes is also created, plus two **mongos** router servers to provide consistency to applications from across the shards.

- [MongoDB Sharding Cluster on CentOS](#) - <https://raw.githubusercontent.com/Azure/azure-quickstart-templates/master/mongodb-sharding-centos/azuredeploy.json>

### WARNING

Deploying this complex MongoDB sharded cluster requires more than 20 cores, which is typically the default core count per region for a subscription. Open an Azure support request to increase your core count.

To create this environment, you need the latest [Azure CLI](#) installed and logged in to an Azure account using [az login](#). First, create a resource group with [az group create](#). The following example creates a resource group named *myResourceGroup* in the *eastus* location:

```
az group create --name myResourceGroup --location eastus
```

Next, deploy the MongoDB template with [az group deployment create](#). Define your own resource names and sizes where needed such as for *mongoAdminUsername*, *sizeOfDataDiskInGB*, and *configNodeVmSize*:

```
az group deployment create --resource-group myResourceGroup \
--parameters '{
 "adminUsername": {"value": "azureuser"},

 "adminPassword": {"value": "P@ssw0rd!"},

 "mongoAdminUsername": {"value": "mongoadmin"},

 "mongoAdminPassword": {"value": "P@ssw0rd!"},

 "dnsNamePrefix": {"value": "mypublicdns"},

 "environment": {"value": "AzureCloud"},

 "numDataDisks": {"value": "4"},

 "sizeOfDataDiskInGB": {"value": 20},

 "centOsVersion": {"value": "7.0"},

 "routerNodeVmSize": {"value": "Standard_DS3_v2"},

 "configNodeVmSize": {"value": "Standard_DS3_v2"},

 "replicaNodeVmSize": {"value": "Standard_DS3_v2"},

 "zabbixServerIPAddress": {"value": "Null"} }' \
--template-uri https://raw.githubusercontent.com/Azure/azure-quickstart-templates/master/mongodb-sharding-
centos/azuredeploy.json \
--name myMongoDBCluster \
--no-wait
```

This deployment can take over an hour to deploy and configure all the VM instances. The `--no-wait` flag is used at the end of the preceding command to return control to the command prompt once the template deployment has been accepted by the Azure platform. You can then view the deployment status with [az group deployment show](#). The following example views the status for the `myMongoDBCluster` deployment in the `myResourceGroup` resource group:

```
az group deployment show \
--resource-group myResourceGroup \
--name myMongoDBCluster \
--query [properties.provisioningState] \
--output tsv
```

## Next steps

In these examples, you connect to the MongoDB instance locally from the VM. If you want to connect to the MongoDB instance from another VM or network, ensure the appropriate [Network Security Group rules are created](#).

These examples deploy the core MongoDB environment for development purposes. Apply the required security configuration options for your environment. For more information, see the [MongoDB security docs](#).

For more information about creating using templates, see the [Azure Resource Manager overview](#).

The Azure Resource Manager templates use the Custom Script Extension to download and execute scripts on your VMs. For more information, see [Using the Azure Custom Script Extension with Linux Virtual Machines](#).

# Install and configure PostgreSQL on Azure

1/8/2020 • 5 minutes to read • [Edit Online](#)

PostgreSQL is an advanced open-source database similar to Oracle and DB2. It includes enterprise-ready features such as full ACID compliance, reliable transactional processing, and multi-version concurrency control. It also supports standards such as ANSI SQL and SQL/MED (including foreign data wrappers for Oracle, MySQL, MongoDB, and many others). It is highly extensible with support for over 12 procedural languages, GIN and GiST indexes, spatial data support, and multiple NoSQL-like features for JSON or key-value-based applications.

In this article, you will learn how to install and configure PostgreSQL on an Azure virtual machine running Linux.

## Install PostgreSQL

### NOTE

You must already have an Azure virtual machine running Linux in order to complete this tutorial. To create and set up a Linux VM before proceeding, see the [Azure Linux VM tutorial](#).

In this case, use port 1999 as the PostgreSQL port.

Connect to the Linux VM you created via PuTTY. If this is the first time you're using an Azure Linux VM, see [How to Use SSH with Linux on Azure](#) to learn how to use PuTTY to connect to a Linux VM.

1. Run the following command to switch to the root (admin):

```
sudo su -
```

2. Some distributions have dependencies that you must install before installing PostgreSQL. Check for your distro in this list and run the appropriate command:

- Red Hat base Linux:

```
yum install readline-devel gcc make zlib-devel openssl openssl-devel libxml2-devel pam-devel
pam libxslt-devel tcl-devel python-devel -y
```

- Debian base Linux:

```
apt-get install readline-devel gcc make zlib-devel openssl openssl-devel libxml2-devel pam-devel
pam libxslt-devel tcl-devel python-devel -y
```

- SUSE Linux:

```
zypper install readline-devel gcc make zlib-devel openssl openssl-devel libxml2-devel pam-devel
pam libxslt-devel tcl-devel python-devel -y
```

3. Download PostgreSQL into the root directory, and then unzip the package:

```
wget https://ftp.postgresql.org/pub/source/v9.3.5/postgresql-9.3.5.tar.bz2 -P /root/
tar jxvf postgresql-9.3.5.tar.bz2
```

The above is an example. You can find the more detailed download address in the [Index of /pub/source/](#).

4. To start the build, run these commands:

```
cd postgresql-9.3.5
./configure --prefix=/opt/postgresql-9.3.5
```

5. If you want to build everything that can be built, including the documentation (HTML and man pages) and additional modules (`contrib`), run the following command instead:

```
gmake install-world
```

You should receive the following confirmation message:

```
PostgreSQL, contrib, and documentation successfully made. Ready to install.
```

## Configure PostgreSQL

1. (Optional) Create a symbolic link to shorten the PostgreSQL reference to not include the version number:

```
ln -s /opt/postgresql-9.3.5 /opt/pgsql
```

2. Create a directory for the database:

```
mkdir -p /opt/pgsql_data
```

3. Create a non-root user and modify that user's profile. Then, switch to this new user (called `postgres` in our example):

```
useradd postgres
chown -R postgres:postgres /opt/pgsql_data
su - postgres
```

### NOTE

For security reasons, PostgreSQL uses a non-root user to initialize, start, or shut down the database.

4. Edit the `bash_profile` file by entering the commands below. These lines will be added to the end of the `bash_profile` file:

```
cat >> ~/.bash_profile <<EOF
export PGPORT=1999
export PGDATA=/opt/pgsql_data
export LANG=en_US.utf8
export PGHOME=/opt/pgsql
export PATH=\$PATH:\$PGHOME/bin
export MANPATH=\$MANPATH:\$PGHOME/share/man
export DATA=`date +"%Y%m%d%H%M"`
export PGUSER=postgres
alias rm='rm -i'
alias ll='ls -lh'
EOF
```

5. Execute the *bash\_profile* file:

```
$ source .bash_profile
```

6. Validate your installation by using the following command:

```
$ which psql
```

If your installation is successful, you will see the following response:

```
/opt/pgsql/bin/psql
```

7. You can also check the PostgreSQL version:

```
$ psql -V
```

8. Initialize the database:

```
$ initdb -D \$PGDATA -E UTF8 --locale=C -U postgres -W
```

You should receive the following output:

```
WARNING: enabling "trust" authentication for local connections
You can change this by editing pg_hba.conf or using the option -A
--auth-local and --auth-host, the next time you run initdb.
```

```
Success. You can now start the database server using:
```

```
postgres -D /opt/pgsql_data
or
pg_ctl -D /opt/pgsql_data -l logfile start
```

## Set up PostgreSQL

Run the following commands:

```
cd /root/postgresql-9.3.5/contrib/start-scripts
cp linux /etc/init.d/postgresql
```

Modify two variables in the /etc/init.d/postgresql file. The prefix is set to the installation path of PostgreSQL: **/opt/pgsql**. PGDATA is set to the data storage path of PostgreSQL: **/opt/pgsql\_data**.

```
sed -i '32s#usr/local#opt#' /etc/init.d/postgresql
sed -i '35s#usr/local/pgsql/data#opt/pgsql_data#' /etc/init.d/postgresql
```

```
root@test:~
27 # contrib/start-scripts/linux
28
29 ## EDIT FROM HERE
30
31 # Installation prefix
32 prefix=/opt/pgsql
33
34 # Data directory
35 PGDATA="/opt/pgsql_data"
36
```

Change the file to make it executable:

```
chmod +x /etc/init.d/postgresql
```

Start PostgreSQL:

```
/etc/init.d/postgresql start
```

Check if the endpoint of PostgreSQL is on:

```
netstat -tunlp|grep 1999
```

You should see the following output:

```
[root@test start-scripts]# netstat -tunlp|grep 1999
tcp 0 0 127.0.0.1:1999 0.0.0.0:* LISTEN
tcp 0 0 ::1:1999 ::* LISTEN
```

## Connect to the Postgres database

Switch to the postgres user once again:

```
su - postgres
```

Create a Postgres database:

```
$ createdb events
```

Connect to the events database that you just created:

```
$ psql -d events
```

## Create and delete a Postgres table

Now that you have connected to the database, you can create tables in it.

For example, create a new example Postgres table by using the following command:

```
CREATE TABLE potluck (name VARCHAR(20), food VARCHAR(30), confirmed CHAR(1), signup_date DATE);
```

You have now set up a four-column table with the following column names and restrictions:

1. The "name" column has been limited by the VARCHAR command to be under 20 characters long.
2. The "food" column indicates the food item that each person will bring. VARCHAR limits this text to be under 30 characters.
3. The "confirmed" column records whether the person has RSVP'd to the potluck. The acceptable values are "Y" and "N".
4. The "date" column shows when they signed up for the event. Postgres requires that dates be written as yyyy-mm-dd.

You should see the following if your table has been successfully created:

```
[postgres@test ~] $ psql -d events
psql (9.3.5)
Type "help" for help.

events=# CREATE TABLE potluck (name VARCHAR(20),
events(# food VARCHAR(30),
events(# confirmed CHAR(1),
events(# signup_date DATE);
CREATE TABLE
```

You can also check the table structure by using the following command:

```
events=# \dt
 List of relations
 Schema | Name | Type | Owner
-----+-----+-----+
 public | potluck | table | postgres
(1 row)
```

## Add data to a table

First, insert information into a row:

```
INSERT INTO potluck (name, food, confirmed, signup_date) VALUES('John', 'Casserole', 'Y', '2012-04-11');
```

You should see this output:

```
events=# INSERT INTO potluck (name, food, confirmed, signup_date) VALUES('John', 'Casserole', 'Y', '2012-04-11')
INSERT 0 1
```

You can add a couple more people to the table as well. Here are some options, or you can create your own:

```
INSERT INTO potluck (name, food, confirmed, signup_date) VALUES('Sandy', 'Key Lime Tarts', 'N', '2012-04-14');

INSERT INTO potluck (name, food, confirmed, signup_date) VALUES ('Tom', 'BBQ','Y', '2012-04-18');

INSERT INTO potluck (name, food, confirmed, signup_date) VALUES('Tina', 'Salad', 'Y', '2012-04-18');
```

## Show tables

Use the following command to show a table:

```
select * from potluck;
```

The output is:

```
events=# select * from potluck;
 name | food | confirmed | signup_date
-----+-----+-----+-----+
 John | Casserole | Y | 2012-04-11
 Sandy | Key Lime Tarts | N | 2012-04-14
 Tom | BBQ | Y | 2012-04-18
 Tina | Salad | Y | 2012-04-18
(4 rows)
```

## Delete data in a table

Use the following command to delete data in a table:

```
delete from potluck where name='John';
```

This deletes all the information in the "John" row. The output is:

```
events=# DELETE FROM potluck WHERE name = 'John' ;
DELETE 1
```

## Update data in a table

Use the following command to update data in a table. For this one, Sandy has confirmed that they are attending, so we will change the RSVP from "N" to "Y":

```
UPDATE potluck set confirmed = 'Y' WHERE name = 'Sandy';
```

## Get more information about PostgreSQL

Now that you have completed the installation of PostgreSQL in an Azure Linux VM, you can enjoy using it in Azure. To learn more about PostgreSQL, visit the [PostgreSQL website](#).

# IBM DB2 pureScale on Azure

12/27/2019 • 6 minutes to read • [Edit Online](#)

The IBM DB2 pureScale environment provides a database cluster for Azure with high availability and scalability on Linux operating systems. This article shows an architecture for running DB2 pureScale on Azure.

## Overview

Enterprises have long used traditional relational database management system (RDBMS) platforms to cater to their online transaction processing (OLTP) needs. These days, many are migrating their mainframe-based database environments to Azure as a way to expand capacity, reduce costs, and maintain a steady operational cost structure. Migration is often the first step in modernizing a legacy platform.

Recently, an enterprise customer rehosted its IBM DB2 environment running on z/OS to IBM DB2 pureScale on Azure. The Db2 pureScale database cluster solution provides high availability and scalability on Linux operating systems. The customer ran Db2 successfully as a standalone, scale-up instance on a single virtual machine (VM) in a large scale-up system on Azure prior to installing Db2 pureScale.

Though not identical to the original environment, IBM DB2 pureScale on Linux delivers similar high-availability and scalability features as IBM DB2 for z/OS running in a Parallel Sysplex configuration on the mainframe. In this scenario, the cluster is connected via iSCSI to a shared storage cluster. We used the GlusterFS file system, a free, scalable, open source distributed file system specifically optimized for cloud storage. However, IBM no longer supports this solution. To maintain your support from IBM, you need to use a supported iSCSI-compatible file system. Microsoft offers Storage Spaces Direct (S2D) as an option.

This article describes the architecture used for this Azure migration. The customer used Red Hat Linux 7.4 to test the configuration. This version is available from the Azure Marketplace. Before you choose a Linux distribution, make sure to verify the currently supported versions. For details, see the documentation for [IBM DB2 pureScale](#) and [GlusterFS](#).

This article is a starting point for your DB2 implementation plan. Your business requirements will differ, but the same basic pattern applies. You can also use this architectural pattern for online analytical processing (OLAP) applications on Azure.

This article doesn't cover differences and possible migration tasks for moving an IBM DB2 for z/OS database to IBM DB2 pureScale running on Linux. And it doesn't provide sizing estimations and workload analyses for moving from DB2 z/OS to DB2 pureScale.

To help you decide on the best DB2 pureScale architecture for your environment, we recommend that you fully estimate sizing and make a hypothesis. On the source system, make sure to consider DB2 z/OS Parallel Sysplex with data-sharing architecture, Coupling Facility configuration, and distributed data facility (DDF) usage statistics.

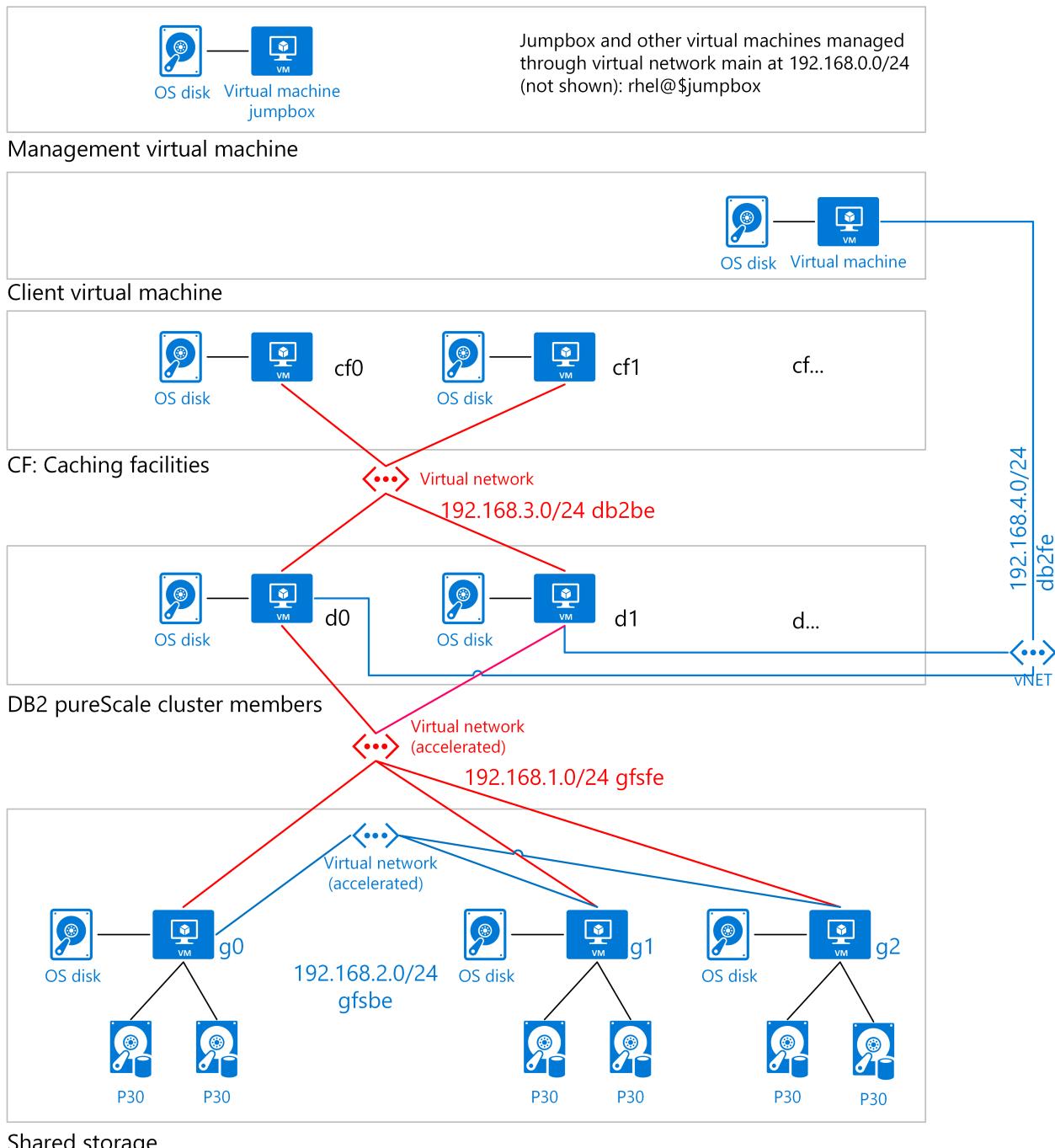
### NOTE

This article describes one approach to DB2 migration, but there are others. For example, DB2 pureScale can also run in virtualized on-premises environments. IBM supports DB2 on Microsoft Hyper-V in various configurations. For more information, see [DB2 pureScale virtualization architecture](#) in the IBM Knowledge Center.

## Architecture

To support high availability and scalability on Azure, you can use a scale-out, shared data architecture for DB2

pureScale. The customer migration used the following example architecture.



The diagram shows the logical layers needed for a DB2 pureScale cluster. These include virtual machines for a client, for management, for caching, for the database engine, and for shared storage.

In addition to the database engine nodes, the diagram includes two nodes used for cluster caching facilities (CFs). A minimum of two nodes are used for the database engine itself. A DB2 server that belongs to a pureScale cluster is called a member.

The cluster is connected via iSCSI to a three-node shared storage cluster to provide scale-out storage and high availability. DB2 pureScale is installed on Azure virtual machines running Linux.

This approach is a template that you can modify for the size and scale of your organization. It's based on the following:

- Two or more database members are combined with at least two CF nodes. The nodes manage a global buffer pool (GBP) for shared memory and global lock manager (GLM) services to control shared access and lock contention from active members. One CF node acts as the primary and the other as the secondary, failover CF node. To avoid a single point of failure in the environment, a DB2 pureScale cluster requires at least three database members.

least four nodes.

- High-performance shared storage (shown in P30 size in the diagram). Each node uses this storage.
- High-performance networking for the data members and shared storage.

## Compute considerations

This architecture runs the application, storage, and data tiers on Azure virtual machines. The [deployment setup scripts](#) create the following:

- A DB2 pureScale cluster. The type of compute resources you need on Azure depends on your setup. In general, you can use two approaches:
  - Use a multi-node, high-performance computing (HPC)-style network where small to medium-sized instances access shared storage. For this HPC type of configuration, Azure memory-optimized E-series or storage-optimized L-series [virtual machines](#) provide the needed compute power.
  - Use fewer large virtual machine instances for the data engines. For large instances, the largest memory-optimized M-series virtual machines are ideal for heavy in-memory workloads. You might need a dedicated instance, depending on the size of the logical partition (LPAR) that's used to run DB2.
- The DB2 CF uses memory-optimized virtual machines, such as E-series or L-series.
- A shared storage cluster that uses Standard\_DS4\_v2 virtual machines running Linux.
- The management jumpbox is a Standard\_DS2\_v2 virtual machine running Linux. An alternative is Azure Bastion, a service that provides a secure RDP/SSH experience for all the VMs in your virtual network.
- The client is a Standard\_DS3\_v2 virtual machine running Windows (used for testing).
- *Optional.* A witness server. This is needed only with certain earlier versions of Db2 pureScale. This example uses a Standard\_DS3\_v2 virtual machine running Linux (used for DB2 pureScale).

### NOTE

A DB2 pureScale cluster requires at least two DB2 instances. It also requires a cache instance and a lock manager instance.

## Storage considerations

Like Oracle RAC, DB2 pureScale is a high-performance block I/O, scale-out database. We recommend using the largest [Azure premium SSD](#) option that suits your needs. Smaller storage options might be suitable for development and test environments, while production environments often need more storage capacity. The example architecture uses [P30](#) because of its ratio of IOPS to size and price. Regardless of size, use Premium Storage for best performance.

DB2 pureScale uses a shared-everything architecture, where all data is accessible from all cluster nodes. Premium storage must be shared across multiple instances, whether on demand or on dedicated instances.

A large DB2 pureScale cluster can require 200 terabytes (TB) or more of premium shared storage, with IOPS of 100,000. DB2 pureScale supports an iSCSI block interface that you can use on Azure. The iSCSI interface requires a shared storage cluster that you can implement with S2D or another tool. This type of solution creates a virtual storage area network (vSAN) device in Azure. DB2 pureScale uses the vSAN to install the clustered file system that's used to share data among virtual machines.

## Networking considerations

IBM recommends InfiniBand networking for all members in a DB2 pureScale cluster. DB2 pureScale also uses remote direct memory access (RDMA), where available, for the CFs.

During setup, you create an Azure [resource group](#) to contain all the virtual machines. In general, you group resources based on their lifetime and who will manage them. The virtual machines in this architecture require [accelerated networking](#). It's an Azure feature that provides consistent, ultra-low network latency via single-root I/O virtualization (SR-IOV) to a virtual machine.

Every Azure virtual machine is deployed into a virtual network that has subnets: main, Gluster FS front end (gfsfe), Gluster FS back end (bfsbe), DB2 pureScale (db2be), and DB2 pureScale front end (db2fe). The installation script also creates the primary [NICs](#) on the virtual machines in the main subnet.

Use [network security groups](#) to restrict network traffic within the virtual network and to isolate the subnets.

On Azure, DB2 pureScale needs to use TCP/IP as the network connection for storage.

## Next steps

- [Deploy this architecture on Azure](#)

# Deploy IBM DB2 pureScale on Azure

1/20/2020 • 5 minutes to read • [Edit Online](#)

This article describes how to deploy an [example architecture](#) that an enterprise customer recently used to migrate from its IBM DB2 environment running on z/OS to IBM DB2 pureScale on Azure.

To follow the steps used for the migration, see the installation scripts in the [DB2onAzure](#) repository on GitHub. These scripts are based on the architecture for a typical, medium-sized online transaction processing (OLTP) workload.

## Get started

To deploy this architecture, download and run the deploy.sh script found in the [DB2onAzure](#) repository on GitHub.

The repository also has scripts for setting up a Grafana dashboard. You can use the dashboard to query Prometheus, the open-source monitoring and alerting system included with DB2.

### NOTE

The deploy.sh script on the client creates private SSH keys and passes them to the deployment template over HTTPS. For greater security, we recommend using [Azure Key Vault](#) to store secrets, keys, and passwords.

## How the deployment script works

The deploy.sh script creates and configures the Azure resources for this architecture. The script prompts you for the Azure subscription and virtual machines used in the target environment, and then performs the following operations:

- Sets up the resource group, virtual network, and subnets on Azure for the installation.
- Sets up the network security groups and SSH for the environment.
- Sets up multiple NICs on both the shared storage and the DB2 pureScale virtual machines.
- Creates the shared storage virtual machines. If you use Storage Spaces Direct or another storage solution, see [Storage Spaces Direct overview](#).
- Creates the jumpbox virtual machine.
- Creates the DB2 pureScale virtual machines.
- Creates the witness virtual machine that DB2 pureScale pings. Skip this part of the deployment if your version of Db2 pureScale does not require a witness.
- Creates a Windows virtual machine to use for testing but doesn't install anything on it.

Next, the deployment scripts set up an iSCSI virtual storage area network (vSAN) for shared storage on Azure. In this example, iSCSI connects to the shared storage cluster. In the original customer solution, GlusterFS was used. However, IBM no longer supports this approach. To maintain your support from IBM, you need to use a supported iSCSI-compatible file system. Microsoft offers Storage Spaces Direct (S2D) as an option.

This solution also gives you the option to install the iSCSI targets as a single Windows node. iSCSI provides a shared block storage interface over TCP/IP that allows the DB2 pureScale setup procedure to use a device interface to connect to shared storage.

The deployment scripts run these general steps:

1. Set up a shared storage cluster on Azure. This step involves at least two Linux nodes.
2. Set up an iSCSI Direct interface on target Linux servers for the shared storage cluster.
3. Set up the iSCSI initiator on the Linux virtual machines. The initiator will access the shared storage cluster by using an iSCSI target. For setup details, see [How To Configure An iSCSI Target And Initiator In Linux](#) in the RootUsers documentation.
4. Install the shared storage layer for the iSCSI interface.

After the scripts create the iSCSI device, the final step is to install DB2 pureScale. As part of the DB2 pureScale setup, [IBM Spectrum Scale](#) (formerly known as GPFS) is compiled and installed on the GlusterFS cluster. This clustered file system enables DB2 pureScale to share data among the virtual machines that run the DB2 pureScale engine. For more information, see the [IBM Spectrum Scale](#) documentation on the IBM website.

## DB2 pureScale response file

The GitHub repository includes DB2server.rsp, a response (.rsp) file that enables you to generate an automated script for the DB2 pureScale installation. The following table lists the DB2 pureScale options that the response file uses for setup. You can customize the response file as needed for your environment.

**NOTE**

A sample response file, DB2server.rsp, is included in the [DB2onAzure](#) repository on GitHub. If you use this file, you must edit it before it can work in your environment.

| SCREEN NAME         | FIELD                                 | VALUE                                                    |
|---------------------|---------------------------------------|----------------------------------------------------------|
| Welcome             |                                       | New Install                                              |
| Choose a Product    |                                       | DB2 Version 11.1.3.3. Server Editions with DB2 pureScale |
| Configuration       | Directory                             | /data1/opt/ibm/db2/V11.1                                 |
|                     | Select the installation type          | Typical                                                  |
|                     | I agree to the IBM terms              | Checked                                                  |
| Instance Owner      | Existing User For Instance, User name | DB2sdin1                                                 |
| Fenced User         | Existing User, User name              | DB2sdfe1                                                 |
| Cluster File System | Shared disk partition device path     | /dev/dm-2                                                |
|                     | Mount point                           | /DB2sd_1804a                                             |
|                     | Shared disk for data                  | /dev/dm-1                                                |
|                     | Mount point (Data)                    | /DB2fs/datafs1                                           |
|                     | Shared disk for log                   | /dev/dm-0                                                |

| SCREEN NAME               | FIELD                                        | VALUE                                                                                                 |
|---------------------------|----------------------------------------------|-------------------------------------------------------------------------------------------------------|
|                           | Mount point (Log)                            | /DB2fs/logfs1                                                                                         |
|                           | DB2 Cluster Services Tiebreaker. Device path | /dev/dm-3                                                                                             |
| Host List                 | d1 [eth1], d2 [eth1], cf1 [eth1], cf2 [eth1] |                                                                                                       |
|                           | Preferred primary CF                         | cf1                                                                                                   |
|                           | Preferred secondary CF                       | cf2                                                                                                   |
| Response File and Summary | first option                                 | Install DB2 Server Edition with the IBM DB2 pureScale feature and save my settings in a response file |
|                           | Response file name                           | /root/DB2server.rsp                                                                                   |

### Notes about this deployment

- The values for /dev-dm0, /dev-dm1, /dev-dm2, and /dev-dm3 can change after a restart on the virtual machine where the setup takes place (d0 in the automated script). To find the right values, you can issue the following command before completing the response file on the server where the setup will run:

```
[root@d0 rhel]# ls -als /dev/mapper
total 0
0 drwxr-xr-x 2 root root 140 May 30 11:07 .
0 drwxr-xr-x 19 root root 4060 May 30 11:31 ..
0 crw----- 1 root root 10, 236 May 30 11:04 control
0 lrwxrwxrwx 1 root root 7 May 30 11:07 db2data1 -> ../dm-1
0 lrwxrwxrwx 1 root root 7 May 30 11:07 db2log1 -> ../dm-0
0 lrwxrwxrwx 1 root root 7 May 30 11:26 db2shared -> ../dm-2
0 lrwxrwxrwx 1 root root 7 May 30 11:08 db2tieb -> ../dm-3
```

- The setup scripts use aliases for the iSCSI disks so that the actual names can be found easily.
- When the setup script is run on d0, the **/dev/dm-\*** values might be different on d1, cf0, and cf1. The difference in values doesn't affect the DB2 pureScale setup.

## Troubleshooting and known issues

The GitHub repo includes a knowledge base that the authors maintain. It lists potential problems you might have and resolutions you can try. For example, known problems can happen when:

- You're trying to reach the gateway IP address.
- You're compiling General Public License (GPL).
- The security handshake between hosts fails.
- The DB2 installer detects an existing file system.
- You're manually installing IBM Spectrum Scale.
- You're installing DB2 pureScale when IBM Spectrum Scale is already created.
- You're removing DB2 pureScale and IBM Spectrum Scale.

For more information about these and other known problems, see the kb.md file in the [DB2onAzure](#) repo.

## Next steps

- [Creating required users for a DB2 pureScale Feature installation](#)
- [DB2icrt - Create instance command](#)
- [DB2 pureScale Clusters Data Solution](#)
- [IBM Data Studio](#)
- [Azure Virtual Data Center Lift and Shift Guide](#)

# Add a disk to a Linux VM

11/13/2019 • 8 minutes to read • [Edit Online](#)

This article shows you how to attach a persistent disk to your VM so that you can preserve your data - even if your VM is reprovisioned due to maintenance or resizing.

## Attach a new disk to a VM

If you want to add a new, empty data disk on your VM, use the `az vm disk attach` command with the `--new` parameter. If your VM is in an Availability Zone, the disk is automatically created in the same zone as the VM. For more information, see [Overview of Availability Zones](#). The following example creates a disk named `myDataDisk` that is 50 Gb in size:

```
az vm disk attach \
-g myResourceGroup \
--vm-name myVM \
--name myDataDisk \
--new \
--size-gb 50
```

## Attach an existing disk

To attach an existing disk, find the disk ID and pass the ID to the `az vm disk attach` command. The following example queries for a disk named `myDataDisk` in `myResourceGroup`, then attaches it to the VM named `myVM`:

```
diskId=$(az disk show -g myResourceGroup -n myDataDisk --query 'id' -o tsv)

az vm disk attach -g myResourceGroup --vm-name myVM --name $diskId
```

## Connect to the Linux VM to mount the new disk

To partition, format, and mount your new disk so your Linux VM can use it, SSH into your VM. For more information, see [How to use SSH with Linux on Azure](#). The following example connects to a VM with the public DNS entry of `mypublicdns.westus.cloudapp.azure.com` with the username `azureuser`:

```
ssh azureuser@mypublicdns.westus.cloudapp.azure.com
```

Once connected to your VM, you're ready to attach a disk. First, find the disk using `dmesg` (the method you use to discover your new disk may vary). The following example uses `dmesg` to filter on `SCSI` disks:

```
dmesg | grep SCSI
```

The output is similar to the following example:

```
[0.294784] SCSI subsystem initialized
[0.573458] Block layer SCSI generic (bsg) driver version 0.4 loaded (major 252)
[7.110271] sd 2:0:0:0: [sda] Attached SCSI disk
[8.079653] sd 3:0:1:0: [sdb] Attached SCSI disk
[1828.162306] sd 5:0:0:0: [sdc] Attached SCSI disk
```

#### NOTE

It is recommended that you use the latest versions of fdisk or parted that are available for your distro.

Here, *sdc* is the disk that we want. Partition the disk with `parted`, if the disk size is 2 tebibytes (TiB) or larger then you must use GPT partitioning, if it is under 2TiB, then you can use either MBR or GPT partitioning. If you're using MBR partitioning, you can use `fdisk`. Make it a primary disk on partition 1, and accept the other defaults. The following example starts the `fdisk` process on `/dev/sdc`:

```
sudo fdisk /dev/sdc
```

Use the `n` command to add a new partition. In this example, we also choose `p` for a primary partition and accept the rest of the default values. The output will be similar to the following example:

```
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF disklabel
Building a new DOS disklabel with disk identifier 0x2a59b123.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.

Warning: invalid flag 0x0000 of partition table 4 will be corrected by w(rite)

Command (m for help): n
Partition type:
 p primary (0 primary, 0 extended, 4 free)
 e extended
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-10485759, default 2048):
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-10485759, default 10485759):
Using default value 10485759
```

Print the partition table by typing `p` and then use `w` to write the table to disk and exit. The output should look similar to the following example:

```
Command (m for help): p

Disk /dev/sdc: 5368 MB, 5368709120 bytes
255 heads, 63 sectors/track, 652 cylinders, total 10485760 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x2a59b123

 Device Boot Start End Blocks Id System
/dev/sdc1 2048 10485759 5241856 83 Linux

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
```

Use the below command to update the kernel:

```
partprobe
```

Now, write a file system to the partition with the `mkfs` command. Specify your filesystem type and the device name. The following example creates an `ext4` filesystem on the `/dev/sdc1` partition that was created in the preceding steps:

```
sudo mkfs -t ext4 /dev/sdc1
```

The output is similar to the following example:

```
mke2fs 1.42.9 (4-Feb-2014)
Discarding device blocks: done
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
327680 inodes, 1310464 blocks
65523 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=1342177280
40 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
 32768, 98304, 163840, 229376, 294912, 819200, 884736
Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

Now, create a directory to mount the file system using `mkdir`. The following example creates a directory at `/datadrive`:

```
sudo mkdir /datadrive
```

Use `mount` to then mount the filesystem. The following example mounts the `/dev/sdc1` partition to the `/datadrive` mount point:

```
sudo mount /dev/sdc1 /datadrive
```

To ensure that the drive is remounted automatically after a reboot, it must be added to the `/etc/fstab` file. It is also highly recommended that the UUID (Universally Unique Identifier) is used in `/etc/fstab` to refer to the drive rather than just the device name (such as, `/dev/sdc1`). If the OS detects a disk error during boot, using the UUID avoids the incorrect disk being mounted to a given location. Remaining data disks would then be assigned those same device IDs. To find the UUID of the new drive, use the `blkid` utility:

```
sudo blkid
```

The output looks similar to the following example:

```
/dev/sda1: UUID="11111111-1b1b-1c1c-1d1d-1e1e1e1e1e" TYPE="ext4"
/dev/sdb1: UUID="22222222-2b2b-2c2c-2d2d-2e2e2e2e2e" TYPE="ext4"
/dev/sdc1: UUID="33333333-3b3b-3c3c-3d3d-3e3e3e3e3e" TYPE="ext4"
```

#### NOTE

Improperly editing the `/etc/fstab` file could result in an unbootable system. If unsure, refer to the distribution's documentation for information on how to properly edit this file. It is also recommended that a backup of the `/etc/fstab` file is created before editing.

Next, open the `/etc/fstab` file in a text editor as follows:

```
sudo vi /etc/fstab
```

In this example, use the UUID value for the `/dev/sdc1` device that was created in the previous steps, and the mountpoint of `/datadrive`. Add the following line to the end of the `/etc/fstab` file:

```
UUID=33333333-3b3b-3c3c-3d3d-3e3e3e3e3e /datadrive ext4 defaults,nofail 1 2
```

#### NOTE

Later removing a data disk without editing fstab could cause the VM to fail to boot. Most distributions provide either the `nofail` and/or `nobootwait` fstab options. These options allow a system to boot even if the disk fails to mount at boot time. Consult your distribution's documentation for more information on these parameters.

The `nofail` option ensures that the VM starts even if the filesystem is corrupt or the disk does not exist at boot time. Without this option, you may encounter behavior as described in [Cannot SSH to Linux VM due to FSTAB errors](#)

The Azure VM Serial Console can be used for console access to your VM if modifying fstab has resulted in a boot failure. More details are available in the [Serial Console documentation](#).

## TRIM/UNMAP support for Linux in Azure

Some Linux kernels support TRIM/UNMAP operations to discard unused blocks on the disk. This feature is primarily useful in standard storage to inform Azure that deleted pages are no longer valid and can be discarded, and can save money if you create large files and then delete them.

There are two ways to enable TRIM support in your Linux VM. As usual, consult your distribution for the recommended approach:

- Use the `discard` mount option in `/etc/fstab`, for example:

```
UUID=33333333-3b3b-3c3c-3d3d-3e3e3e3e3e /datadrive ext4 defaults,discard 1 2
```

- In some cases, the `discard` option may have performance implications. Alternatively, you can run the `fstrim` command manually from the command line, or add it to your crontab to run regularly:

### Ubuntu

```
sudo apt-get install util-linux
sudo fstrim /datadrive
```

### RHEL/CentOS

```
sudo yum install util-linux
sudo fstrim /datadrive
```

## Troubleshooting

When adding data disks to a Linux VM, you may encounter errors if a disk does not exist at LUN 0. If you are adding a disk manually using the `az vm disk attach -new` command and you specify a LUN (`--lun`) rather than allowing the Azure platform to determine the appropriate LUN, take care that a disk already exists / will exist at LUN 0.

Consider the following example showing a snippet of the output from `lsscsi`:

```
[5:0:0:0] disk Msft Virtual Disk 1.0 /dev/sdc
[5:0:0:1] disk Msft Virtual Disk 1.0 /dev/sdd
```

The two data disks exist at LUN 0 and LUN 1 (the first column in the `lsscsi` output details `[host:channel:target:lun]`). Both disks should be accessible from within the VM. If you had manually specified the first disk to be added at LUN 1 and the second disk at LUN 2, you may not see the disks correctly from within your VM.

#### NOTE

The Azure `host` value is 5 in these examples, but this may vary depending on the type of storage you select.

This disk behavior is not an Azure problem, but the way in which the Linux kernel follows the SCSI specifications. When the Linux kernel scans the SCSI bus for attached devices, a device must be found at LUN 0 in order for the system to continue scanning for additional devices. As such:

- Review the output of `lsscsi` after adding a data disk to verify that you have a disk at LUN 0.
- If your disk does not show up correctly within your VM, verify a disk exists at LUN 0.

## Next steps

- To ensure your Linux VM is configured correctly, review the [Optimize your Linux machine performance](#) recommendations.
- Expand your storage capacity by adding additional disks and [configure RAID](#) for additional performance.

# Use the portal to attach a data disk to a Linux VM

12/4/2019 • 8 minutes to read • [Edit Online](#)

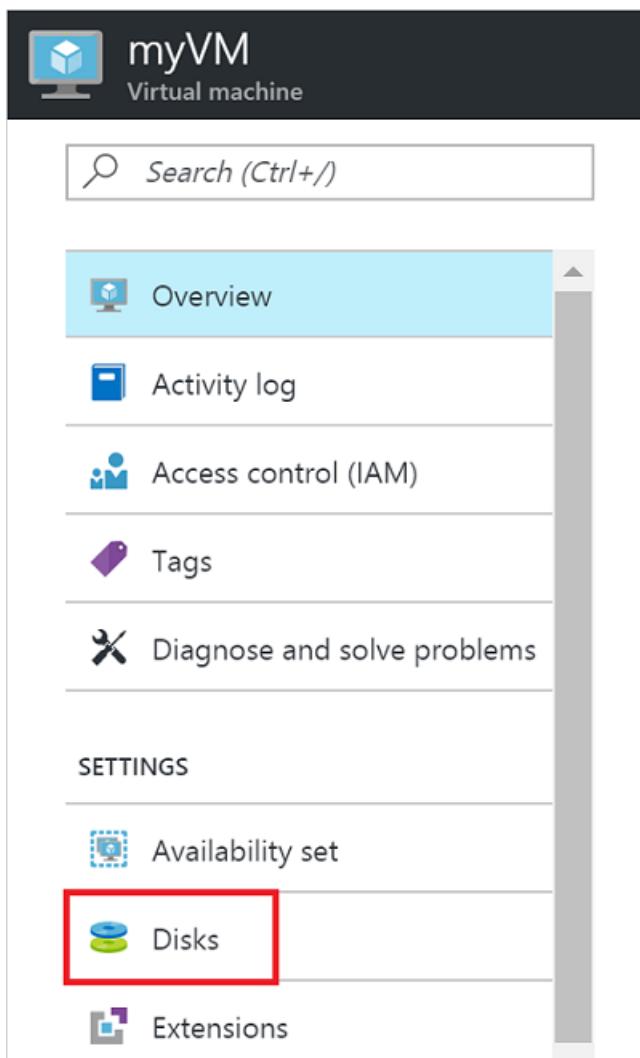
This article shows you how to attach both new and existing disks to a Linux virtual machine through the Azure portal. You can also [attach a data disk to a Windows VM in the Azure portal](#).

Before you attach disks to your VM, review these tips:

- The size of the virtual machine controls how many data disks you can attach. For details, see [Sizes for virtual machines](#).
- Disks attached to virtual machines are actually .vhdx files stored in Azure. For details, see our [Introduction to managed disks](#).
- After attaching the disk, you need to [connect to the Linux VM to mount the new disk](#).

## Find the virtual machine

1. Go to the [Azure portal](#) to find the VM. Search for and select **Virtual machines**.
2. Choose the VM from the list.
3. In the **Virtual machines** page sidebar, under **Settings**, choose **Disks**.



## Attach a new disk

1. On the **Disks** pane, click **+ Add data disk**.
2. Click the drop-down menu for **Name** and select **Create disk**:

The screenshot shows the 'Disks' pane in the Azure portal. At the top, there are 'Save' and 'Discard' buttons. Below that, the 'OS disk' section is shown, listing 'myVM' with a size of 'Premium\_LRS'. The 'Data disks' section follows, with a table header: LUN, NAME, SIZE, ACCOUNT TYPE. A LUN 0 row is present, and below it is a dropdown menu. This dropdown menu is highlighted with a red box and contains two options: 'Create disk' and 'All disks', with 'Create disk' being the selected item.

3. Enter a name for your managed disk. Review the default settings, update as necessary, and then click **Create**.

The screenshot shows the 'Create managed disk' dialog box. It includes fields for Name (set to 'myDataDisk'), Resource group (set to 'myResourceGroup'), Account type (set to 'Premium\_LRS'), Source type (set to 'None (empty disk)'), and Size (set to '1023'). Below these, estimated performance values are listed: IOPS limit (5000) and Throughput limit (MB/s) (200). At the bottom, a 'Create' button is highlighted with a red box.

4. Click **Save** to create the managed disk and update the VM configuration:

The screenshot shows the 'Disk' configuration page for a virtual machine. It includes sections for 'OS disk' and 'Data disks'. The 'OS disk' section lists 'myVM' with a size of 1023 GiB, account type 'Premium\_LRS', and caching set to 'Read/write'. The 'Data disks' section shows 'myDataDisk' (LUN 0) with a size of 1023 GiB, account type 'Premium\_LRS', and caching set to 'None'. A 'Save' button is highlighted with a red box at the top left.

- After Azure creates the disk and attaches it to the virtual machine, the new disk is listed in the virtual machine's disk settings under **Data Disks**. As managed disks are a top-level resource, the disk appears at the root of the resource group:

The screenshot shows the 'myResourceGroup' resource group details page. The 'Disks' section lists managed disks: 'myAvailabilitySet' (Availability set, West US), 'myDataDisk' (Disk, West US), and 'myNetworkSecurityGroup' (Network security group, West US). The 'myDataDisk' row is highlighted with a red box.

## Attach an existing disk

- On the **Disk** pane, click **+ Add data disk**.
- Click the drop-down menu for **Name** to view a list of existing managed disks accessible to your Azure subscription. Select the managed disk to attach:

Save Discard

**OS disk**

| NAME | SIZE | ACCOUNT TYPE |
|------|------|--------------|
| myVM |      | Premium_LRS  |

**Data disks**

| LUN | NAME       | SIZE     | ACCOUNT TYPE |
|-----|------------|----------|--------------|
| 0   | myDataDisk | 1023 GiB | Premium_LRS  |
| 1   |            |          |              |

Create disk

**Disks in resource group 'myResourceGroup'**

myExistingDisk  
size: 1023 GiB, account type: Premium\_LRS

**All disks**

myExistingDisk  
size: 1023 GiB, account type: Premium\_LRS, resource group: MYRESOURCEGROUP

- Click **Save** to attach the existing managed disk and update the VM configuration:

Save Discard

**OS disk**

| NAME | SIZE | ACCOUNT TYPE | ENCRYPTION | CACHING    |
|------|------|--------------|------------|------------|
| myVM |      | Premium_LRS  |            | Read/write |

**Data disks**

| LUN | NAME           | SIZE     | ACCOUNT TYPE | ENCRYPTION | CACHING |
|-----|----------------|----------|--------------|------------|---------|
| 0   | myDataDisk     | 1023 GiB | Premium_LRS  |            | None    |
| 1   | myExistingDisk | 1023 GiB | Premium_LRS  |            | None    |

+ Add data disk

- After Azure attaches the disk to the virtual machine, it's listed in the virtual machine's disk settings under **Data Disks**.

## Connect to the Linux VM to mount the new disk

To partition, format, and mount your new disk so your Linux VM can use it, SSH into your VM. For more information, see [How to use SSH with Linux on Azure](#). The following example connects to a VM with the public DNS entry of *mypublicdns.westus.cloudapp.azure.com* with the username *azureuser*:

```
ssh azureuser@mypublicdns.westus.cloudapp.azure.com
```

Once connected to your VM, you're ready to attach a disk. First, find the disk using `dmesg` (the method you use to discover your new disk may vary). The following example uses `dmesg` to filter on *SCSI* disks:

```
dmesg | grep SCSI
```

The output is similar to the following example:

```
[0.294784] SCSI subsystem initialized
[0.573458] Block layer SCSI generic (bsg) driver version 0.4 loaded (major 252)
[7.110271] sd 2:0:0:0: [sda] Attached SCSI disk
[8.079653] sd 3:0:1:0: [sdb] Attached SCSI disk
[1828.162306] sd 5:0:0:0: [sdc] Attached SCSI disk
```

Here, `sdc` is the disk that we want.

### Partition a new disk

If you are using an existing disk that contains data, skip to mounting the disk. If you are attaching a new disk, you need to partition the disk.

#### NOTE

It is recommended that you use the latest versions of `fdisk` or `parted` that are available for your distro.

Partition the disk with `fdisk`. If the disk size is 2 tebibytes (TiB) or larger then you must use GPT partitioning, you can use `parted` to perform GPT partitioning. If disk size is under 2TiB, then you can use either MBR or GPT partitioning. Make it a primary disk on partition 1, and accept the other defaults. The following example starts the `fdisk` process on `/dev/sdc`:

```
sudo fdisk /dev/sdc
```

Use the `n` command to add a new partition. In this example, we also choose `p` for a primary partition and accept the rest of the default values. The output will be similar to the following example:

```
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF disklabel
Building a new DOS disklabel with disk identifier 0x2a59b123.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.

Warning: invalid flag 0x0000 of partition table 4 will be corrected by w(rite)

Command (m for help): n
Partition type:
 p primary (0 primary, 0 extended, 4 free)
 e extended
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-10485759, default 2048):
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-10485759, default 10485759):
Using default value 10485759
```

Print the partition table by typing `p` and then use `w` to write the table to disk and exit. The output should look similar to the following example:

```

Command (m for help): p

Disk /dev/sdc: 5368 MB, 5368709120 bytes
255 heads, 63 sectors/track, 652 cylinders, total 10485760 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x2a59b123

 Device Boot Start End Blocks Id System
 /dev/sdc1 2048 10485759 5241856 83 Linux

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.

```

Now, write a file system to the partition with the `mkfs` command. Specify your filesystem type and the device name. The following example creates an `ext4` filesystem on the `/dev/sdc1` partition that was created in the preceding steps:

```
sudo mkfs -t ext4 /dev/sdc1
```

The output is similar to the following example:

```

mke2fs 1.42.9 (4-Feb-2014)
Discarding device blocks: done
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
327680 inodes, 1310464 blocks
65523 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=1342177280
40 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
 32768, 98304, 163840, 229376, 294912, 819200, 884736
Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done

```

#### **Alternate method using parted**

The `fdisk` utility needs interactive input and hence is not ideal for use within automation scripts. However, the `parted` utility can be scripted and hence lends itself better in automation scenarios. The `parted` utility can be used to partition and to format a data disk. For the walkthrough below, we use a new data disk `/dev/sdc` and format it using the [XFS](#) filesystem.

```

sudo parted /dev/sdc --script mklabel gpt mkpart xfspart xfs 0% 100%
partprobe /dev/sdc1

```

As seen above, we use the `partprobe` utility to make sure the kernel is immediately aware of the new partition and filesystem. Failure to use `partprobe` can cause the `blkid` or `lsblk` commands to not return the UUID for the new filesystem immediately.

## Mount the disk

Create a directory to mount the file system using `mkdir`. The following example creates a directory at `/datadrive`:

```
sudo mkdir /datadrive
```

Use `mount` to then mount the filesystem. The following example mounts the `/dev/sdc1` partition to the `/datadrive` mount point:

```
sudo mount /dev/sdc1 /datadrive
```

To ensure that the drive is remounted automatically after a reboot, it must be added to the `/etc/fstab` file. It is also highly recommended that the UUID (Universally Unique Identifier) is used in `/etc/fstab` to refer to the drive rather than just the device name (such as, `/dev/sdc1`). If the OS detects a disk error during boot, using the UUID avoids the incorrect disk being mounted to a given location. Remaining data disks would then be assigned those same device IDs. To find the UUID of the new drive, use the `blkid` utility:

```
sudo -i blkid
```

The output looks similar to the following example:

```
/dev/sda1: UUID="11111111-1b1b-1c1c-1d1d-1e1e1e1e1e" TYPE="ext4"
/dev/sdb1: UUID="22222222-2b2b-2c2c-2d2d-2e2e2e2e2e" TYPE="ext4"
/dev/sdc1: UUID="33333333-3b3b-3c3c-3d3d-3e3e3e3e3e" TYPE="ext4"
```

### NOTE

Improperly editing the `/etc/fstab` file could result in an unbootable system. If unsure, refer to the distribution's documentation for information on how to properly edit this file. It is also recommended that a backup of the `/etc/fstab` file is created before editing.

Next, open the `/etc/fstab` file in a text editor as follows:

```
sudo vi /etc/fstab
```

In this example, use the UUID value for the `/dev/sdc1` device that was created in the previous steps, and the mountpoint of `/datadrive`. Add the following line to the end of the `/etc/fstab` file:

```
UUID=33333333-3b3b-3c3c-3d3d-3e3e3e3e3e /datadrive ext4 defaults,nofail 1 2
```

When done, save the `/etc/fstab` file and reboot the system.

### NOTE

Later removing a data disk without editing fstab could cause the VM to fail to boot. Most distributions provide either the `nofail` and/or `nobootwait` fstab options. These options allow a system to boot even if the disk fails to mount at boot time. Consult your distribution's documentation for more information on these parameters.

The `nofail` option ensures that the VM starts even if the filesystem is corrupt or the disk does not exist at boot time. Without this option, you may encounter behavior as described in [Cannot SSH to Linux VM due to FSTAB errors](#)

## TRIM/UNMAP support for Linux in Azure

Some Linux kernels support TRIM/UNMAP operations to discard unused blocks on the disk. This feature is primarily useful in standard storage to inform Azure that deleted pages are no longer valid and can be discarded, and can save money if you create large files and then delete them.

There are two ways to enable TRIM support in your Linux VM. As usual, consult your distribution for the recommended approach:

- Use the `discard` mount option in `/etc/fstab`, for example:

```
UUID=33333333-3b3b-3c3c-3d3d-3e3e3e3e3e /datadrive ext4 defaults,discard 1 2
```

- In some cases, the `discard` option may have performance implications. Alternatively, you can run the `fstrim` command manually from the command line, or add it to your crontab to run regularly:

### Ubuntu

```
sudo apt-get install util-linux
sudo fstrim /datadrive
```

### RHEL/CentOS

```
sudo yum install util-linux
sudo fstrim /datadrive
```

## Next steps

You can also [attach a data disk](#) using the Azure CLI.

# How to detach a data disk from a Linux virtual machine

11/13/2019 • 2 minutes to read • [Edit Online](#)

When you no longer need a data disk that's attached to a virtual machine, you can easily detach it. This removes the disk from the virtual machine, but doesn't remove it from storage. In this article, we are working with an Ubuntu LTS 16.04 distribution. If you are using a different distribution, the instructions for unmounting the disk might be different.

## WARNING

If you detach a disk it is not automatically deleted. If you have subscribed to Premium storage, you will continue to incur storage charges for the disk. For more information, see [Pricing and Billing when using Premium Storage](#).

If you want to use the existing data on the disk again, you can reattach it to the same virtual machine, or another one.

## Connect to the VM to unmount the disk

Before you can detach the disk using either CLI or the portal, you need to unmount the disk and removed references to it from your fstab file.

Connect to the VM. In this example, the public IP address of the VM is `10.0.1.4` with the username `azureuser`:

```
ssh azureuser@10.0.1.4
```

First, find the data disk that you want to detach. The following example uses `dmesg` to filter on SCSI disks:

```
dmesg | grep SCSI
```

The output is similar to the following example:

```
[0.294784] SCSI subsystem initialized
[0.573458] Block layer SCSI generic (bsg) driver version 0.4 loaded (major 252)
[7.110271] sd 2:0:0:0: [sda] Attached SCSI disk
[8.079653] sd 3:0:1:0: [sdb] Attached SCSI disk
[1828.162306] sd 5:0:0:0: [sdc] Attached SCSI disk
```

Here, `sdc` is the disk that we want to detach. You also should grab the UUID of the disk.

```
sudo -i blkid
```

The output looks similar to the following example:

```
/dev/sda1: UUID="11111111-1b1b-1c1c-1d1d-1e1e1e1e1e" TYPE="ext4"
/dev/sdb1: UUID="22222222-2b2b-2c2c-2d2d-2e2e2e2e2e" TYPE="ext4"
/dev/sdc1: UUID="33333333-3b3b-3c3c-3d3d-3e3e3e3e3e" TYPE="ext4"
```

Edit the `/etc/fstab` file to remove references to the disk.

#### NOTE

Improperly editing the `/etc/fstab` file could result in an unbootable system. If unsure, refer to the distribution's documentation for information on how to properly edit this file. It is also recommended that a backup of the `/etc/fstab` file is created before editing.

Open the `/etc/fstab` file in a text editor as follows:

```
sudo vi /etc/fstab
```

In this example, the following line needs to be deleted from the `/etc/fstab` file:

```
UUID=33333333-3b3b-3c3c-3d3d-3e3e3e3e3e /datadrive ext4 defaults,nofail 1 2
```

Use `umount` to unmount the disk. The following example unmounts the `/dev/sdc1` partition from the `/datadrive` mount point:

```
sudo umount /dev/sdc1 /datadrive
```

## Detach a data disk using Azure CLI

This example detaches the `myDataDisk` disk from VM named `myVM` in `myResourceGroup`.

```
az vm disk detach \
 -g myResourceGroup \
 --vm-name myVm \
 -n myDataDisk
```

The disk stays in storage but is no longer attached to a virtual machine.

## Detach a data disk using the portal

1. In the left menu, select **Virtual Machines**.
2. Select the virtual machine that has the data disk you want to detach and click **Stop** to deallocate the VM.
3. In the virtual machine pane, select **Disks**.
4. At the top of the **Disk** pane, select **Edit**.
5. In the **Disk** pane, to the far right of the data disk that you would like to detach, click the  detach button.
6. After the disk has been removed, click **Save** on the top of the pane.
7. In the virtual machine pane, click **Overview** and then click the **Start** button at the top of the pane to restart the VM.

The disk stays in storage but is no longer attached to a virtual machine.

## Next steps

If you want to reuse the data disk, you can just [attach it to another VM](#).

# Using Managed Disks in Azure Resource Manager Templates

12/10/2019 • 5 minutes to read • [Edit Online](#)

This document walks through the differences between managed and unmanaged disks when using Azure Resource Manager templates to provision virtual machines. The examples help you to update existing templates that are using unmanaged Disks to managed disks. For reference, we are using the [101-vm-simple-windows](#) template as a guide. You can see the template using both [managed Disks](#) and a prior version using [unmanaged disks](#) if you'd like to directly compare them.

## Unmanaged Disks template formatting

To begin, let's take a look at how unmanaged disks are deployed. When creating unmanaged disks, you need a storage account to hold the VHD files. You can create a new storage account or use one that already exists. This article shows you how to create a new storage account. Create a storage account resource in the resources block as shown below.

```
{
 "type": "Microsoft.Storage/storageAccounts",
 "apiVersion": "2018-07-01",
 "name": "[variables('storageAccountName')]",
 "location": "[resourceGroup().location]",
 "sku": {
 "name": "Standard_LRS"
 },
 "kind": "Storage",
 "properties": {}
}
```

Within the virtual machine object, add a dependency on the storage account to ensure that it's created before the virtual machine. Within the `storageProfile` section, specify the full URI of the VHD location, which references the storage account and is needed for the OS disk and any data disks.

```
{
 "type": "Microsoft.Compute/virtualMachines",
 "apiVersion": "2018-10-01",
 "name": "[variables('vmName')]",
 "location": "[resourceGroup().location]",
 "dependsOn": [
 "[resourceId('Microsoft.Storage/storageAccounts/', variables('storageAccountName'))]",
 "[resourceId('Microsoft.Network/networkInterfaces/', variables('nicName'))]"
],
 "properties": {
 "hardwareProfile": {...},
 "osProfile": {...},
 "storageProfile": {
 "imageReference": {
 "publisher": "MicrosoftWindowsServer",
 "offer": "WindowsServer",
 "sku": "[parameters('windowsOSVersion')]",
 "version": "latest"
 },
 "osDisk": {
 "name": "osdisk",
 "vhd": {
 "uri": "[concat(reference(resourceId('Microsoft.Storage/storageAccounts/',
variables('storageAccountName'))).primaryEndpoints.blob, 'vhds/osdisk.vhd')]"
 },
 "caching": "ReadWrite",
 "createOption": "FromImage"
 },
 "dataDisks": [
 {
 "name": "datadisk1",
 "diskSizeGB": 1023,
 "lun": 0,
 "vhd": {
 "uri": "[concat(reference(resourceId('Microsoft.Storage/storageAccounts/',
variables('storageAccountName'))).primaryEndpoints.blob, 'vhds/datadisk1.vhd')]"
 },
 "createOption": "Empty"
 }
]
 },
 "networkProfile": {...},
 "diagnosticsProfile": {...}
 }
}
```

## Managed disks template formatting

With Azure Managed Disks, the disk becomes a top-level resource and no longer requires a storage account to be created by the user. Managed disks were first exposed in the [2016-04-30-preview](#) API version, they are available in all subsequent API versions and are now the default disk type. The following sections walk through the default settings and detail how to further customize your disks.

### NOTE

It is recommended to use an API version later than [2016-04-30-preview](#) as there were breaking changes between [2016-04-30-preview](#) and [2017-03-30](#).

### Default managed disk settings

To create a VM with managed disks, you no longer need to create the storage account resource. Referencing the template example below, there are some differences from the previous unmanged disk examples to note:

- The `apiVersion` is a version that supports managed disks.
- `osDisk` and `dataDisks` no longer refer to a specific URI for the VHD.
- When deploying without specifying additional properties, the disk will use a storage type based on the size of the VM. For example, if you are using a VM size that supports premium storage (sizes with "s" in their name such as Standard\_D2s\_v3) then premium disks will be configured by default. You can change this by using the `sku` setting of the disk to specify a storage type.
- If no name for the disk is specified, it takes the format of `<VMName>_OsDisk_1_<randomstring>` for the OS disk and `<VMName>_disk<#>_<randomstring>` for each data disk.
  - If a VM is being created from a custom image then the default settings for storage account type and disk name are retrieved from the disk properties defined in the custom image resource. These can be overridden by specifying values for these in the template.
- By default, Azure disk encryption is disabled.
- By default, disk caching is Read/Write for the OS disk and None for data disks.
- In the example below there is still a storage account dependency, though this is only for storage of diagnostics and is not needed for disk storage.

```
{
 "type": "Microsoft.Compute/virtualMachines",
 "apiVersion": "2018-10-01",
 "name": "[variables('vmName')]",
 "location": "[resourceGroup().location]",
 "dependsOn": [
 "[resourceId('Microsoft.Storage/storageAccounts/', variables('storageAccountName'))]",
 "[resourceId('Microsoft.Network/networkInterfaces/', variables('nicName'))]"
],
 "properties": {
 "hardwareProfile": {...},
 "osProfile": {...},
 "storageProfile": {
 "imageReference": {
 "publisher": "MicrosoftWindowsServer",
 "offer": "WindowsServer",
 "sku": "[parameters('windowsOSVersion')]",
 "version": "latest"
 },
 "osDisk": {
 "createOption": "FromImage"
 },
 "dataDisks": [
 {
 "diskSizeGB": 1023,
 "lun": 0,
 "createOption": "Empty"
 }
]
 },
 "networkProfile": {...},
 "diagnosticsProfile": {...}
 }
}
```

## Using a top-level managed disk resource

As an alternative to specifying the disk configuration in the virtual machine object, you can create a top-level disk resource and attach it as part of the virtual machine creation. For example, you can create a disk resource as follows to use as a data disk.

```
{
 "type": "Microsoft.Compute/disks",
 "apiVersion": "2018-06-01",
 "name": "[concat(variables('vmName'),'-datadisk1')]",
 "location": "[resourceGroup().location]",
 "sku": {
 "name": "Standard_LRS"
 },
 "properties": {
 "creationData": {
 "createOption": "Empty"
 },
 "diskSizeGB": 1023
 }
}
```

Within the VM object, reference the disk object to be attached. Specifying the resource ID of the managed disk created in the `managedDisk` property allows the attachment of the disk as the VM is created. The `apiVersion` for the VM resource is set to `2017-03-30`. A dependency on the disk resource is added to ensure it's successfully created before VM creation.

```
{
 "type": "Microsoft.Compute/virtualMachines",
 "apiVersion": "2018-10-01",
 "name": "[variables('vmName')]",
 "location": "[resourceGroup().location]",
 "dependsOn": [
 "[resourceId('Microsoft.Storage/storageAccounts/', variables('storageAccountName'))]",
 "[resourceId('Microsoft.Network/networkInterfaces/', variables('nicName'))]",
 "[resourceId('Microsoft.Compute/disks/', concat(variables('vmName'),'-datadisk1'))]"
],
 "properties": {
 "hardwareProfile": {...},
 "osProfile": {...},
 "storageProfile": {
 "imageReference": {
 "publisher": "MicrosoftWindowsServer",
 "offer": "WindowsServer",
 "sku": "[parameters('windowsOSVersion')]",
 "version": "latest"
 },
 "osDisk": {
 "createOption": "FromImage"
 },
 "dataDisks": [
 {
 "lun": 0,
 "name": "[concat(variables('vmName'),'-datadisk1')]",
 "createOption": "attach",
 "managedDisk": {
 "id": "[resourceId('Microsoft.Compute/disks/', concat(variables('vmName'),'-datadisk1'))]"
 }
 }
]
 },
 "networkProfile": {...},
 "diagnosticsProfile": {...}
 }
}
```

## Create managed availability sets with VMs using managed disks

To create managed availability sets with VMs using managed disks, add the `sku` object to the availability set

resource and set the `name` property to `Aligned`. This property ensures that the disks for each VM are sufficiently isolated from each other to avoid single points of failure. Also note that the `apiVersion` for the availability set resource is set to `2018-10-01`.

```
{
 "type": "Microsoft.Compute/availabilitySets",
 "apiVersion": "2018-10-01",
 "location": "[resourceGroup().location]",
 "name": "[variables('avSetName')]",
 "properties": {
 "PlatformUpdateDomainCount": 3,
 "PlatformFaultDomainCount": 2
 },
 "sku": {
 "name": "Aligned"
 }
}
```

## Standard SSD disks

Below are the parameters needed in the Resource Manager template to create Standard SSD Disks:

- `apiVersion` for Microsoft.Compute must be set as `2018-04-01` (or later)
- Specify `managedDisk.storageAccountType` as `StandardSSD_LRS`

The following example shows the `properties.storageProfile.osDisk` section for a VM that uses Standard SSD Disks:

```
"osDisk": {
 "osType": "Windows",
 "name": "myOsDisk",
 "caching": "ReadWrite",
 "createOption": "FromImage",
 "managedDisk": {
 "storageAccountType": "StandardSSD_LRS"
 }
}
```

For a complete template example of how to create a Standard SSD disk with a template, see [Create a VM from a Windows Image with Standard SSD Data Disks](#).

## Additional scenarios and customizations

To find full information on the REST API specifications, please review the [create a managed disk REST API documentation](#). You will find additional scenarios, as well as default and acceptable values that can be submitted to the API through template deployments.

## Next steps

- For full templates that use managed disks visit the following Azure Quickstart Repo links.
  - [Windows VM with managed disk](#)
  - [Linux VM with managed disk](#)
- Visit the [Azure Managed Disks Overview](#) document to learn more about managed disks.
- Review the template reference documentation for virtual machine resources by visiting the [Microsoft.Compute/virtualMachines template reference](#) document.
- Review the template reference documentation for disk resources by visiting the [Microsoft.Compute/disks template reference](#) document.
- For information on how to use managed disks in Azure virtual machine scale sets, visit the [Use data disks with scale sets](#) document.



# Enable shared disk

2/19/2020 • 3 minutes to read • [Edit Online](#)

This article covers how to enable the shared disks (preview) feature for Azure managed disks. Azure shared disks (preview) is a new feature for Azure managed disks that enables you to attach a managed disk to multiple virtual machines (VMs) simultaneously. Attaching a managed disk to multiple VMs allows you to either deploy new or migrate existing clustered applications to Azure.

If you are looking for conceptual information on managed disks that have shared disks enabled, refer to [Azure shared disks](#).

## Limitations

While in preview, managed disks that have shared disks enabled are subject to the following limitations:

- Currently only available with premium SSDs.
- Currently only supported in the West Central US region.
- All virtual machines sharing a disk must be deployed in the same [proximity placement groups](#).
- Can only be enabled on data disks, not OS disks.
- Only basic disks can be used with some versions of Windows Server Failover Cluster, for details see [Failover clustering hardware requirements and storage options](#).
- ReadOnly host caching is not available for premium SSDs with `maxShares>1`.
- Availability sets and virtual machine scale sets can only be used with `FaultDomainCount` set to 1.
- Azure Backup and Azure Site Recovery support is not yet available.

If you're interested in trying shared disks then [sign up for our preview](#).

## Disk sizes

For now, only premium SSDs can enable shared disks. The disk sizes that support this feature are P15 and greater. Different disk sizes may have a different `maxShares` limit, which you cannot exceed when setting the `maxShares` value.

For each disk, you can define a `maxShares` value that represents the maximum number of nodes that can simultaneously share the disk. For example, if you plan to set up a 2-node failover cluster, you would set `maxShares=2`. The maximum value is an upper bound. Nodes can join or leave the cluster (mount or unmount the disk) as long as the number of nodes is lower than the specified `maxShares` value.

### NOTE

The `maxShares` value can only be set or edited when the disk is detached from all nodes.

The following table illustrates the allowed maximum values for `maxShares` by disk size:

| DISK SIZES    | MAXSHARES LIMIT |
|---------------|-----------------|
| P15, P20      | 2               |
| P30, P40, P50 | 5               |

| DISK SIZES    | MAXSHARES LIMIT |
|---------------|-----------------|
| P60, P70, P80 | 10              |

The IOPS and bandwidth limits for a disk are not affected by the `maxShares` value. For example, the max IOPS of a P15 disk are 1100 whether `maxShares = 1` or `maxShares > 1`.

## Deploy an Azure shared disk

To deploy a managed disk with the shared disk feature enabled, use the new property `maxShares` and define a value `>1`. This makes the disk shareable across multiple VMs.

### IMPORTANT

The value of `maxShares` can only be set or changed when a disk is unmounted from all VMs. See the [Disk sizes](#) for the allowed values for `maxShares`.

Before using the following template, replace `[parameters('dataDiskName')]`, `[resourceGroup().location]`, `[parameters('dataDiskSizeGB')]`, and `[parameters('maxShares')]` with your own values.

```
{
 "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
 "contentVersion": "1.0.0.0",
 "parameters": {
 "dataDiskName": {
 "type": "string",
 "defaultValue": "mySharedDisk"
 },
 "dataDiskSizeGB": {
 "type": "int",
 "defaultValue": 1024
 },
 "maxShares": {
 "type": "int",
 "defaultValue": 2
 }
 },
 "resources": [
 {
 "type": "Microsoft.Compute/disks",
 "name": "[parameters('dataDiskName')]",
 "location": "[resourceGroup().location]",
 "apiVersion": "2019-07-01",
 "sku": {
 "name": "Premium_LRS"
 },
 "properties": {
 "creationData": {
 "createOption": "Empty"
 },
 "diskSizeGB": "[parameters('dataDiskSizeGB')]",
 "maxShares": "[parameters('maxShares')]"
 }
 }
]
}
```

## Using Azure shared disks with your VMs

Once you've deployed a shared disk with `maxShares>1`, you can mount the disk to one or more of your VMs.

## IMPORTANT

All VMs sharing a disk must be deployed in the same [proximity placement group](#).

```
$resourceGroup = "myResourceGroup"
.setLocation = "WestCentralUS"
$ppgName = "myPPG"
$ppg = New-AzProximityPlacementGroup `
 -Location $location `
 -Name $ppgName `
 -ResourceGroupName $resourceGroup `
 -ProximityPlacementGroupType Standard

$vm = New-AzVm -ResourceGroupName $resourceGroup -Name "myVM" -Location $location -VirtualNetworkName "myVnet"
-SubnetName "mySubnet" -SecurityGroupName "myNetworkSecurityGroup" -PublicIpAddressName "myPublicIpAddress" -
ProximityPlacementGroup $ppg.Id

$dataDisk = Get-AzDisk -ResourceGroupName $resourceGroup -DiskName "mySharedDisk"

$vm = Add-AzVMDataDisk -VM $vm -Name "mySharedDisk" -CreateOption Attach -ManagedDiskId $dataDisk.Id -Lun 0

update-AzVm -VM $vm -ResourceGroupName $resourceGroup
```

## Supported SCSI PR commands

Once you've mounted the shared disk to your VMs in your cluster, you can establish quorum and read/write to the disk using SCSI PR. The following PR commands are available when using Azure shared disks:

To interact with the disk, start with the persistent-reservation-action list:

```
PR_REGISTER_KEY
PR_REGISTER_AND_IGNORE
PR_GET_CONFIGURATION
PR_RESERVE
PR_PREEMPT_RESERVATION
PR_CLEAR_RESERVATION
PR_RELEASE_RESERVATION
```

When using PR\_RESERVE, PR\_PREEMPT\_RESERVATION, or PR\_RELEASE\_RESERVATION, provide one of the following persistent-reservation-type:

```
PR_NONE
PR_WRITE_EXCLUSIVE
PR_EXCLUSIVE_ACCESS
PR_WRITE_EXCLUSIVE_REGISTRANTS_ONLY
PR_EXCLUSIVE_ACCESS_REGISTRANTS_ONLY
PR_WRITE_EXCLUSIVE_ALL_REGISTRANTS
PR_EXCLUSIVE_ACCESS_ALL_REGISTRANTS
```

You also need to provide a persistent-reservation-key when using PR\_RESERVE, PR\_REGISTER\_AND\_IGNORE, PR\_REGISTER\_KEY, PR\_PREEMPT\_RESERVATION, PR\_CLEAR\_RESERVATION, or PR\_RELEASE-RESERVATION.

## Next steps

If you're interested in trying shared disks, [sign up for our preview](#).

# Upload a vhd to Azure using Azure CLI

11/24/2019 • 5 minutes to read • [Edit Online](#)

This article explains how to upload a vhd from your local machine to an Azure managed disk. Previously, you had to follow a more involved process that included staging your data in a storage account, and managing that storage account. Now, you no longer need to manage a storage account, or stage data in it to upload a vhd. Instead, you create an empty managed disk, and upload a vhd directly to it. This simplifies uploading on-premises VMs to Azure and enables you to upload a vhd up to 32 TiB directly into a large managed disk.

If you are providing a backup solution for IaaS VMs in Azure, we recommend you use direct upload to restore customer backups to managed disks. If you are uploading a VHD from a machine external to Azure, speeds will depend on your local bandwidth. If you are using an Azure VM, then your bandwidth will be the same as standard HDDs.

Currently, direct upload is supported for standard HDD, standard SSD, and premium SSD managed disks. It is not yet supported for ultra SSDs.

## Prerequisites

- Download the latest [version of AzCopy v10](#).
- [Install the Azure CLI](#).
- A vhd file, stored locally
- If you intend to upload a vhd from on-premises: A vhd that [has been prepared for Azure](#), stored locally.
- Or, a managed disk in Azure, if you intend to perform a copy action.

## Create an empty managed disk

To upload your vhd to Azure, you'll need to create an empty managed disk that is configured for this upload process. Before you create one, there's some additional information you should know about these disks.

This kind of managed disk has two unique states:

- ReadToUpload, which means the disk is ready to receive an upload but, no [secure access signature](#) (SAS) has been generated.
- ActiveUpload, which means that the disk is ready to receive an upload and the SAS has been generated.

While in either of these states, the managed disk will be billed at [standard HDD pricing](#), regardless of the actual type of disk. For example, a P10 will be billed as an S10. This will be true until `revoke-access` is called on the managed disk, which is required in order to attach the disk to a VM.

Before you can create an empty standard HDD for uploading, you'll need to have the file size of the vhd you want to upload, in bytes. To get that, you can use either `wc -c <yourFileName>.vhf` or `ls -al <yourFileName>.vhf`. This value is used when specifying the **--upload-size-bytes** parameter.

Create an empty standard HDD for uploading by specifying both the **--for-upload** parameter and the **--upload-size-bytes** parameter in a [disk create cmdlet](#):

```
az disk create -n mydiskname -g resourcegroupname -l westus2 --for-upload --upload-size-bytes 34359738880 --sku standard_lrs
```

If you would like to upload either a premium SSD or a standard SSD, replace **standard\_lrs** with either

**premium\_LRS** or **standardssd\_lrs**. Ultra SSD is not yet supported.

You have now created an empty managed disk that is configured for the upload process. To upload a vhd to the disk, you'll need a writeable SAS, so that you can reference it as the destination for your upload.

To generate a writable SAS of your empty managed disk, use the following command:

```
az disk grant-access -n mydiskname -g resourcegroupname --access-level Write --duration-in-seconds 86400
```

Sample returned value:

```
{
 "accessSas": "https://md-impexp-t0rdsfgsdfg4.blob.core.windows.net/w2c3mj0ksfg1/abcd?sv=2017-04-
17&sr=b&si=600a9281-d39e-4cc3-91d2-923c4a696537&sig=xXaT6mFgf139ycT87CADyFxb%2BnPXBElYirYRlbnJZbs%3D"
}
```

## Upload vhd

Now that you have a SAS for your empty managed disk, you can use it to set your managed disk as the destination for your upload command.

Use AzCopy v10 to upload your local VHD file to a managed disk by specifying the SAS URI you generated.

This upload has the same throughput as the equivalent [standard HDD](#). For example, if you have a size that equates to S4, you will have a throughput of up to 60 MiB/s. But, if you have a size that equates to S70, you will have a throughput of up to 500 MiB/s.

```
AzCopy.exe copy "c:\somewhere\mydisk.vhd""sas-URI" --blob-type PageBlob
```

If your SAS expires during upload, and you haven't called `revoke-access` yet, you can get a new SAS to continue the upload using `grant-access`, again.

After the upload is complete, and you no longer need to write any more data to the disk, revoke the SAS. Revoking the SAS will change the state of the managed disk and allow you to attach the disk to a VM.

```
az disk revoke-access -n mydiskname -g resourcegroupname
```

## Copy a managed disk

Direct upload also simplifies the process of copying a managed disk. You can either copy within the same region or cross-region (to another region).

The follow script will do this for you, the process is similar to the steps described earlier, with some differences since you're working with an existing disk.

### IMPORTANT

You need to add an offset of 512 when you're providing the disk size in bytes of a managed disk from Azure. This is because Azure omits the footer when returning the disk size. The copy will fail if you do not do this. The following script already does this for you.

Replace the `<sourceResourceGroupHere>`, `<sourceDiskNameHere>`, `<targetDiskNameHere>`, `<targetResourceGroupHere>`, and `<yourTargetLocationHere>` (an example of a location value would be uswest2) with your values, then run the

following script in order to copy a managed disk.

```
sourceDiskName = <sourceDiskNameHere>
sourceRG = <sourceResourceGroupHere>
targetDiskName = <targetDiskNameHere>
targetRG = <targetResourceGroupHere>
targetLocale = <yourTargetLocationHere>

sourceDiskSizeBytes= $(az disk show -g $sourceRG -n $sourceDiskName --query '[uniqueId]' -o tsv)

az disk create -g $targetRG -n $targetDiskName -l $targetLocale --for-upload --upload-size-bytes
$((sourceDiskSizeBytes+512)) --sku standard_lrs

targetSASURI = $(az disk grant-access -n $targetDiskName -g $targetRG --access-level Write --duration-in-
seconds 86400 -o tsv)

sourceSASURI=$(az disk grant-access -n $sourceDiskName -g $sourceRG --duration-in-seconds 86400 --query
[accessSas] -o tsv)

.\azcopy copy $sourceSASURI $targetSASURI --blob-type PageBlob

az disk revoke-access -n $sourceDiskName -g $sourceRG

az disk revoke-access -n $targetDiskName -g $targetRG
```

## Next steps

Now that you've successfully uploaded a vhd to a managed disk, you can attach the disk as a [data disk to an existing VM](#) or [attach the disk to a VM as an OS disk](#), to create a new VM.

# Expand virtual hard disks on a Linux VM with the Azure CLI

11/13/2019 • 3 minutes to read • [Edit Online](#)

This article describes how to expand managed disks for a Linux virtual machine (VM) with the Azure CLI. You can [add data disks](#) to provide for additional storage space, and you can also expand an existing data disk. The default virtual hard disk size for the operating system (OS) is typically 30 GB on a Linux VM in Azure.

## WARNING

Always make sure that your filesystem is in a healthy state, your disk partition table type will support the new size, and ensure your data is backed up before you perform disk resize operations. For more information, see [Back up Linux VMs in Azure](#).

## Expand an Azure Managed Disk

Make sure that you have the latest [Azure CLI](#) installed and are signed in to an Azure account by using [az login](#).

This article requires an existing VM in Azure with at least one data disk attached and prepared. If you do not already have a VM that you can use, see [Create and prepare a VM with data disks](#).

In the following samples, replace example parameter names such as *myResourceGroup* and *myVM* with your own values.

- Operations on virtual hard disks can't be performed with the VM running. Deallocate your VM with [az vm deallocate](#). The following example deallocates the VM named *myVM* in the resource group named *myResourceGroup*:

```
az vm deallocate --resource-group myResourceGroup --name myVM
```

## NOTE

The VM must be deallocated to expand the virtual hard disk. Stopping the VM with `az vm stop` does not release the compute resources. To release compute resources, use `az vm deallocate`.

- View a list of managed disks in a resource group with [az disk list](#). The following example displays a list of managed disks in the resource group named *myResourceGroup*:

```
az disk list \
 --resource-group myResourceGroup \
 --query '[*].{Name:name,Gb:diskSizeGb,Tier:accountType}' \
 --output table
```

Expand the required disk with [az disk update](#). The following example expands the managed disk named *myDataDisk* to 200 GB:

```
az disk update \
--resource-group myResourceGroup \
--name myDataDisk \
--size-gb 200
```

#### NOTE

When you expand a managed disk, the updated size is rounded up to the nearest managed disk size. For a table of the available managed disk sizes and tiers, see [Azure Managed Disks Overview - Pricing and Billing](#).

3. Start your VM with `az vm start`. The following example starts the VM named *myVM* in the resource group named *myResourceGroup*:

```
az vm start --resource-group myResourceGroup --name myVM
```

## Expand a disk partition and filesystem

To use an expanded disk, expand the underlying partition and filesystem.

1. SSH to your VM with the appropriate credentials. You can see the public IP address of your VM with `az vm show`:

```
az vm show --resource-group myResourceGroup --name myVM -d --query [publicIps] --o tsv
```

2. Expand the underlying partition and filesystem.

- a. If the disk is already mounted, unmount it:

```
sudo umount /dev/sdc1
```

- b. Use `parted` to view disk information and resize the partition:

```
sudo parted /dev/sdc
```

View information about the existing partition layout with `print`. The output is similar to the following example, which shows the underlying disk is 215 GB:

```
GNU Parted 3.2
Using /dev/sdc1
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted) print
Model: Unknown Msft Virtual Disk (scsi)
Disk /dev/sdc1: 215GB
Sector size (logical/physical): 512B/4096B
Partition Table: loop
Disk Flags:

Number Start End Size File system Flags
 0.00B 107GB 107GB ext4
```

- c. Expand the partition with `resizepart`. Enter the partition number, *1*, and a size for the new partition:

```
(parted) resizepart
Partition number? 1
End? [107GB]? 215GB
```

d. To exit, enter `quit`.

3. With the partition resized, verify the partition consistency with `e2fsck`:

```
sudo e2fsck -f /dev/sdc1
```

4. Resize the filesystem with `resize2fs`:

```
sudo resize2fs /dev/sdc1
```

5. Mount the partition to the desired location, such as `/datadrive`:

```
sudo mount /dev/sdc1 /datadrive
```

6. To verify the data disk has been resized, use `df -h`. The following example output shows the data drive `/dev/sdc1` is now 200 GB:

| Filesystem | Size | Used | Avail | Use% | Mounted on |
|------------|------|------|-------|------|------------|
| /dev/sdc1  | 197G | 60M  | 187G  | 1%   | /datadrive |

## Next steps

- If you need additional storage, you can also [add data disks to a Linux VM](#).
- For more information about disk encryption, see [Azure Disk Encryption for Linux VMs](#).

# Use Azure Storage Explorer to manage Azure managed disks

11/12/2019 • 2 minutes to read • [Edit Online](#)

Storage Explorer 1.10.0 enables users to upload, download, and copy managed disks, as well as create snapshots. Because of these additional capabilities, you can use Storage Explorer to migrate data from on-premises to Azure, and migrate data across Azure regions.

## Prerequisites

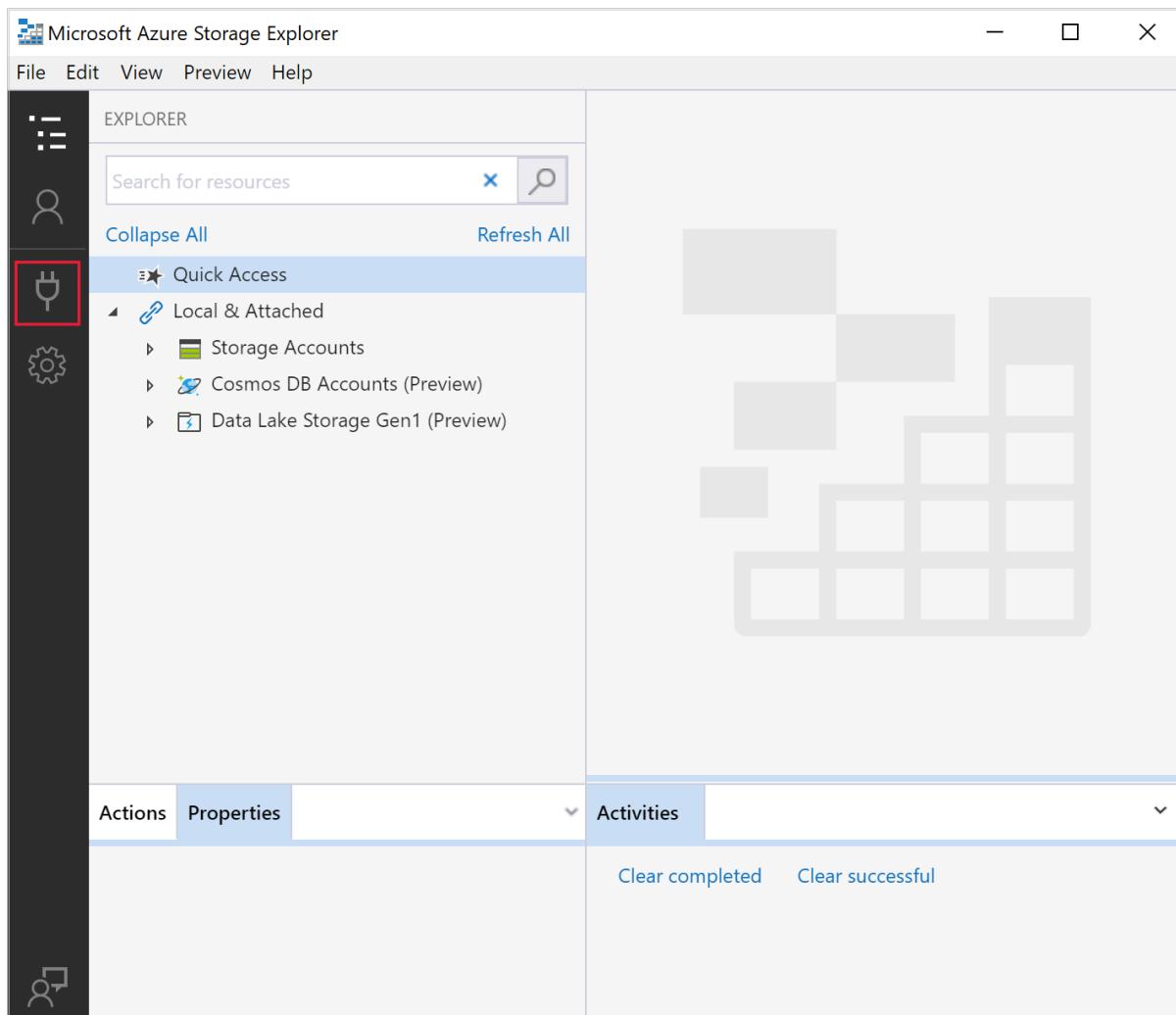
To complete this article, you'll need the following:

- An Azure subscription
- One or more Azure managed disks
- The latest version of [Azure Storage Explorer](#)

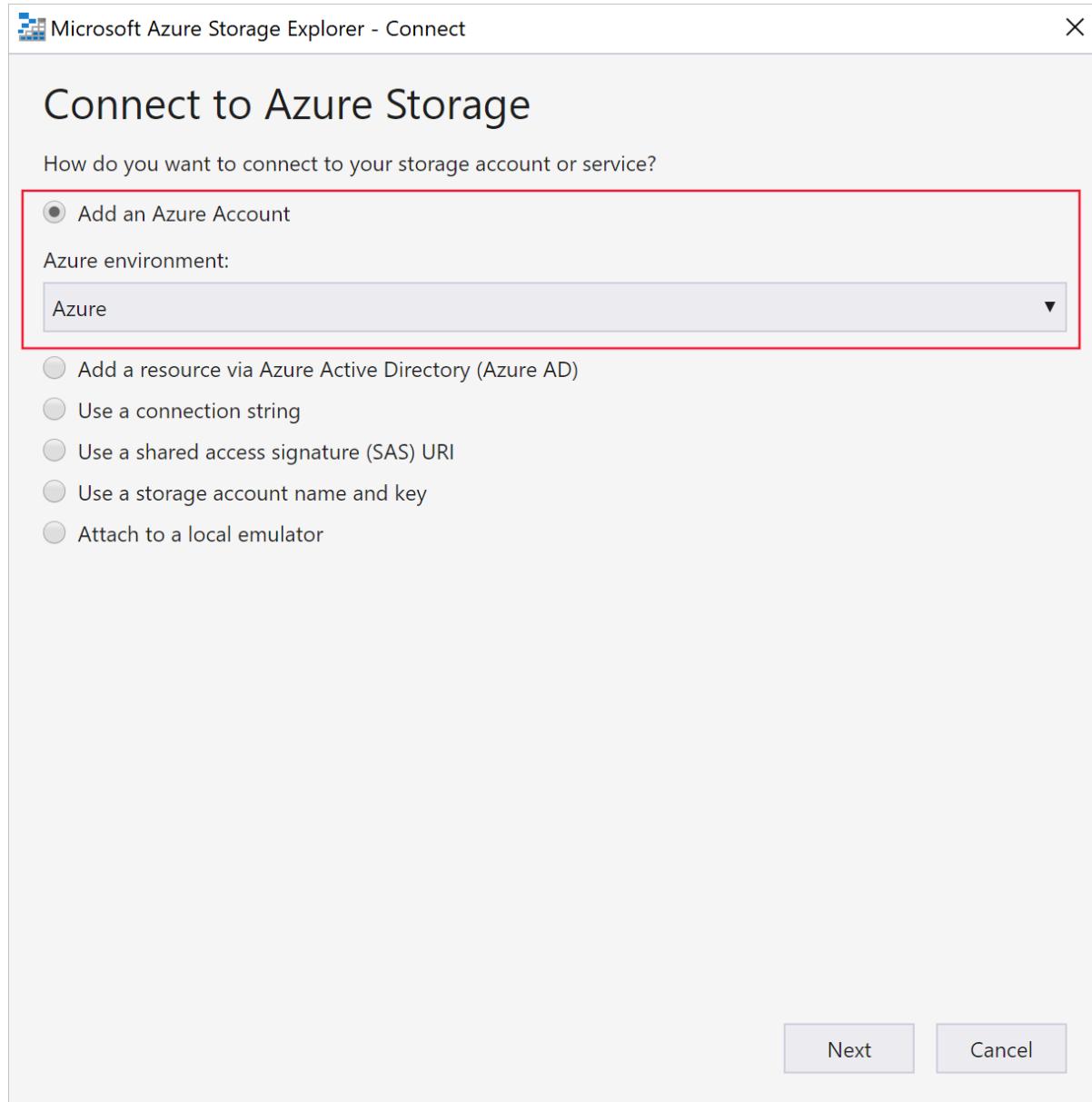
## Connect to an Azure subscription

If your Storage Explorer isn't connected to Azure, you will not be able to use it to manage resources. This section goes over connecting it to your Azure account so that you can manage resources using Storage Explorer.

1. Launch Azure Storage Explorer and click the **plug-in** icon on the left.



2. Select **Add an Azure Account**, and then click **Next**.



3. In the **Azure Sign in** dialog box, enter your Azure credentials.



# Sign in

Email, phone, or Skype

No account? [Create one!](#)

Can't access your account?

[Sign-in options](#)

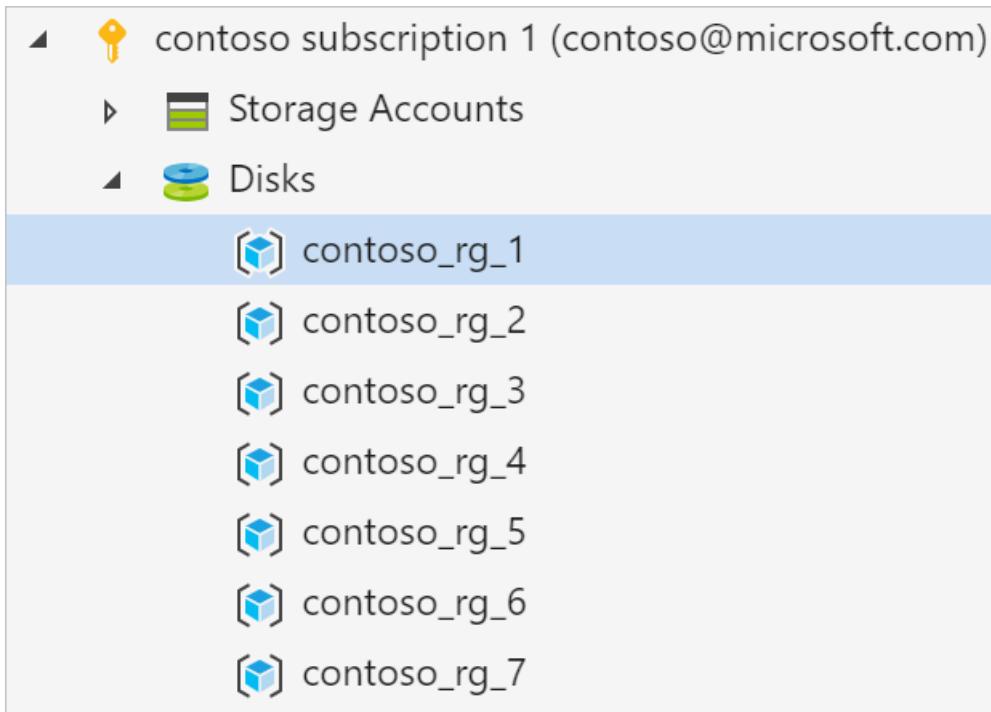
Next

4. Select your subscription from the list and then click **Apply**.

The screenshot shows the Microsoft Azure Storage Explorer interface. On the left, there's a dark sidebar with icons for accounts, preview, and help. The main area has a title bar "Microsoft Azure Storage Explorer" and a menu bar with File, Edit, View, Preview, and Help. A central panel titled "ACCOUNT MANAGEMENT" displays a list of subscriptions. It shows "Microsoft contoso@microsoft.com" at the top with a "Remove" button. Below it, there's a section for "Show resources from these subscriptions:" with a checkbox for "All subscriptions". Underneath, two specific subscriptions are listed: "contoso subscription 1" with the ID "00000000-0000-0000-000000000000" and "contoso subscription 2" with the ID "11111111-1111-1111-1111-111111111111". At the bottom of this panel, there's an "Add an account..." link. At the very bottom of the window, there are "Apply" and "Cancel" buttons.

## Upload a managed disk from an on-prem VHD

1. On the left pane, expand **Disks** and select the resource group that you want to upload your disk to.



2. Select **Upload**.

| Disk Name      | SKU | Size | Disk State | Owner VM | Location |
|----------------|-----|------|------------|----------|----------|
| No disks found |     |      |            |          |          |

3. In **Upload VHD** specify your source VHD, the name of the disk, the OS type, the region you want to upload the disk to, as well as the account type. In some regions Availability zones are supported, for those regions you can select a zone of your choice.
4. Select **Create** to begin uploading your disk.

 Microsoft Azure Storage Explorer - Upload VHD X

## Upload VHD

Select a VHD from which to create a disk and then specify the remaining parameters.

Source VHD:

 ...

Disk name:

OS type:

 ▼

Region:

 ▼

Availability zone:

 ▼

Account type:

 ▼

Create Cancel

5. The status of the upload will now display in **Activities**.

Activities

Clear completed Clear successful

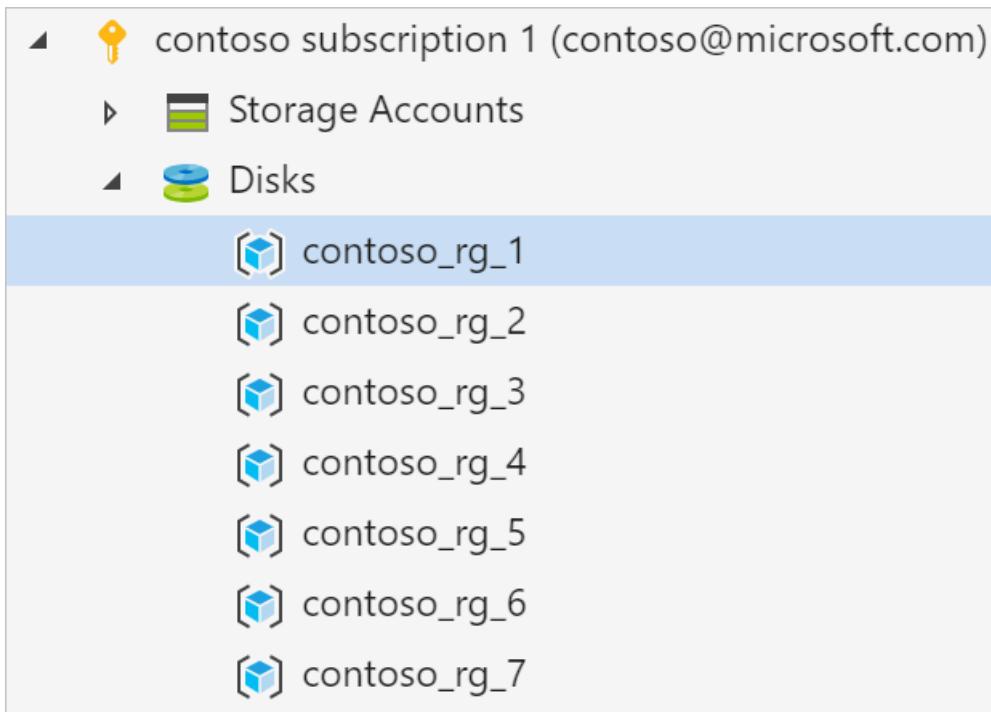
 Uploading 'C:\Users\Administrator\Downloads\mydisk\_onprem.vhd' to disk 'mydisk\_azure' in resource group 'contoso\_rg\_1'

6. If the upload has finished and you don't see the disk in the right pane, select **Refresh**.

## Download a managed disk

The following steps explain how to download a managed disk to an on-prem VHD. A disk's state must be **Unattached** in order to be downloaded, you cannot download an **Attached** disk.

1. On the left pane, if it isn't already expanded, expand **Disks** and select the resource group that you want to download your disk from.



2. On the right pane, select the disk you want to download.
3. Select **Download** and then choose where you would like to save the disk.

The screenshot shows the Azure portal's 'Disks' blade for the 'contoso\_rg\_1' resource group. The top navigation bar includes 'Upload', 'Download' (which is highlighted with a red box), 'Copy', 'Paste', 'Delete', 'Create Snapshot', and 'Refresh' buttons. Below the toolbar is a table with columns: Disk Name, SKU, Size, Disk State, Owner VM, and Location. A single row is selected, showing 'mydisk\_azure' as the disk name, 'Premium' as the SKU, '32 GB' as the size, 'Unattached' as the state, 'centralus' as the location, and no owner VM listed. At the bottom of the table, it says 'Showing 1 to 1 of 1 discovered disks'.

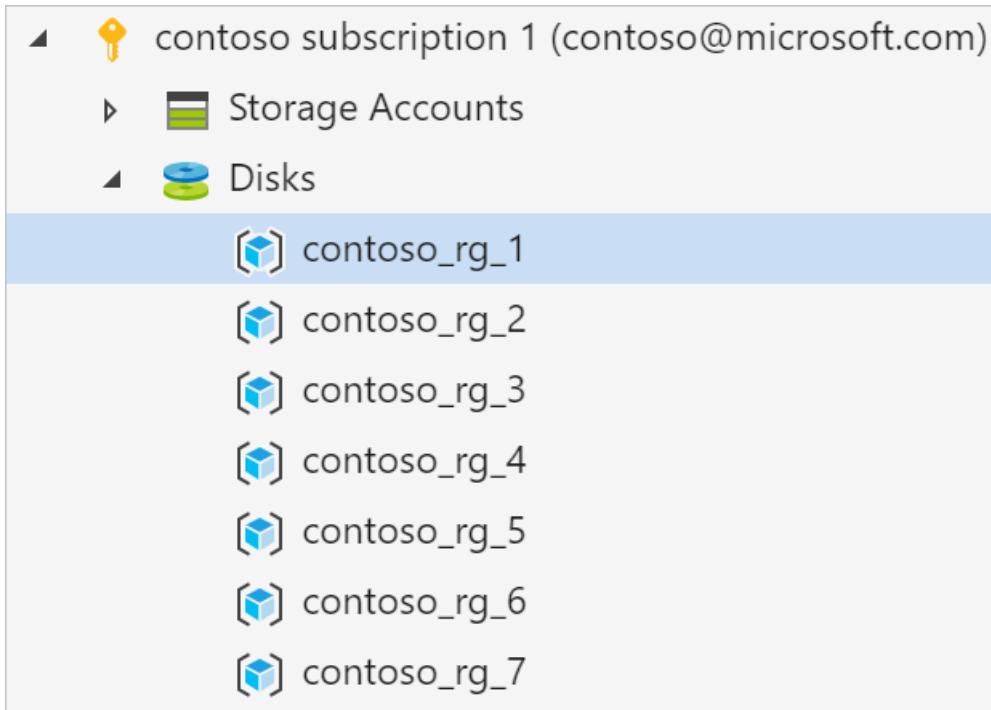
4. Select **Save** and your disk will begin downloading. The status of the download will display in **Activities**.

The screenshot shows the 'Activities' blade. It has tabs for 'Activities' (selected) and 'Jobs'. Below the tabs are 'Clear completed' and 'Clear successful' buttons. A single activity is listed: 'Downloading disk 'mydisk\_azure' in resource group 'contoso\_rg\_1' to 'C:\Users\Administrator\Downloads\mydisk\_download\_from\_azure.vhd''. The status of the activity is shown as a blue circular icon followed by the task name.

## Copy a managed disk

With Storage Explorer, you can copy a managed disk within or across regions. To copy a disk:

1. From the **Disks** dropdown on the left, select the resource group that contains the disk you want to copy.

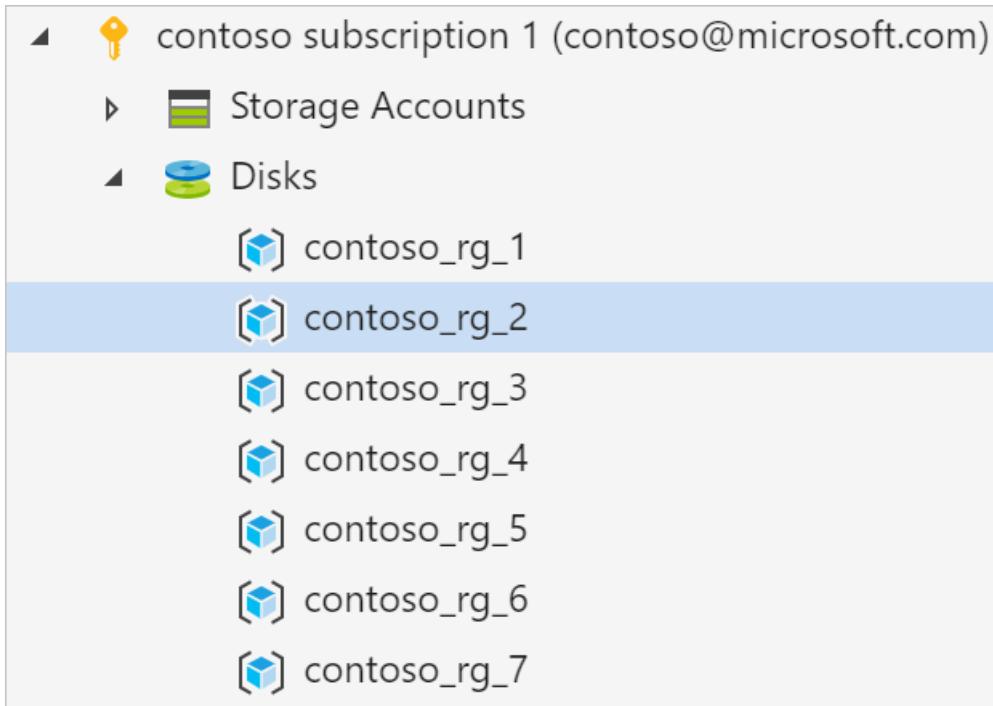


2. On the right pane, select the disk you'd like to copy and select **Copy**.

| Disk Name    | SKU     | Size  | Disk State | Owner VM | Location  |
|--------------|---------|-------|------------|----------|-----------|
| mydisk_azure | Premium | 32 GB | Unattached |          | centralus |

Showing 1 to 1 of 1 discovered disks

3. On the left pane, select the resource group you'd like to paste the disk in.



4. Select **Paste** on the right pane.

A screenshot of the 'Disks' blade for the resource group 'contoso\_rg\_2'. The title bar shows 'contoso\_rg\_2'. The toolbar includes buttons for Upload, Download, Copy, Paste (which is highlighted with a red box), Delete, Create Snapshot, and Refresh. Below the toolbar is a table header with columns: Disk Name, SKU, Size, Disk State, Owner VM, and Location. A message 'No disks found' is displayed below the table. At the bottom, it says 'Showing 0 to 0 of 0 entries'.

5. In the **Paste Disk** dialog, fill in the values. You can also specify an Availability zone in supported regions.



## Paste Disk

Choose the name for the disk and and then specify the remaining parameters.

Disk name:

Region:



Availability zone:



Account type:



6. Select **Paste** and your disk will begin copying, the status is displayed in **Activities**.

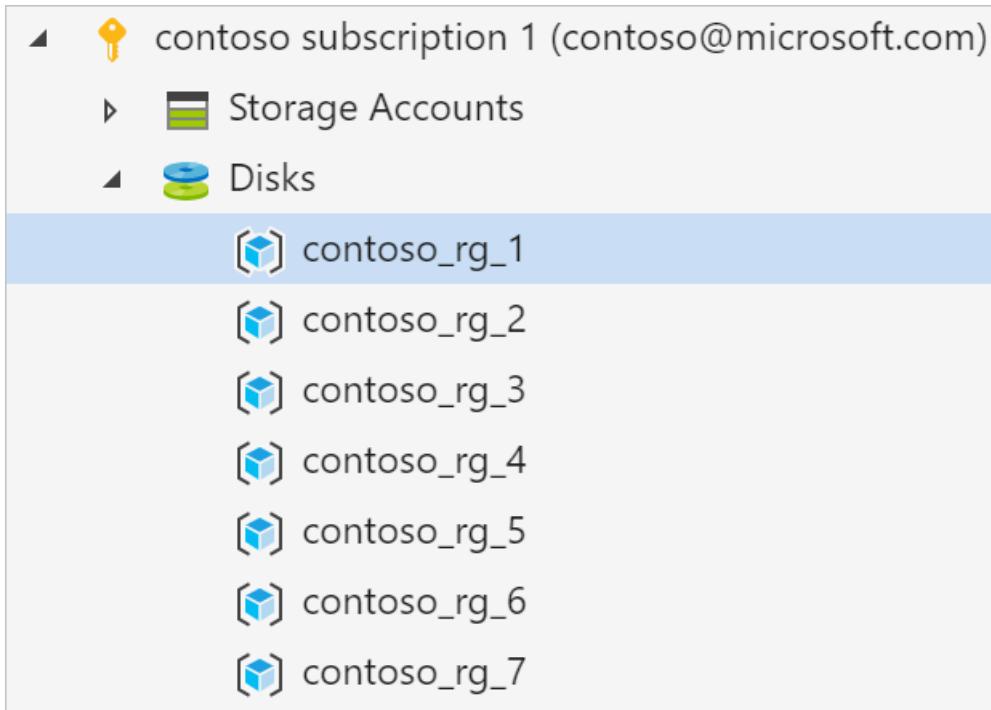
Activities

Clear completed   Clear successful

🕒 Copying disk 'mydisk\_azure' in resource group 'contoso\_rg\_1' to disk 'mydisk\_azure\_paste' in resource group 'contoso\_rg\_2'

## Create a snapshot

1. From the **Disks** dropdown on the left, select the resource group that contains the disk you want to snapshot.



2. On the right, select the disk you'd like to snapshot and select **Create Snapshot**.

The screenshot shows the 'Disks' blade for the 'contoso\_rg\_1' resource group. At the top, there is a toolbar with 'Upload', 'Download', 'Copy', 'Paste', 'Delete', 'Create Snapshot' (which is highlighted with a red box), and 'Refresh'. Below the toolbar is a table with the following data:

| Disk Name    | SKU     | Size  | Disk State | Owner VM | Location  |
|--------------|---------|-------|------------|----------|-----------|
| mydisk_azure | Premium | 32 GB | Unattached |          | centralus |

At the bottom of the blade, it says 'Showing 1 to 1 of 1 discovered disks'.

3. In **Create Snapshot**, specify the name of the snapshot as well as the resource group you want to create it in. Then select **Create**.

 Microsoft Azure Storage Explorer - Create Snapshot X

## Create Snapshot

Specify the name of the snapshot and what resource group to create it in.

Snapshot name:

Resource group:

Create Cancel

4. Once the snapshot has been created, you can select **Open in Portal** in **Activities** to view the snapshot in the Azure portal.

Activities

[Clear completed](#) [Clear successful](#)

✓ Successfully created snapshot 'mydisk\_azure\_snapshot\_20190901' from disk 'mydisk\_azure' in resource group 'contoso\_rg\_1' Open in Portal

## Next steps

Learn how to [Create a VM from a VHD by using the Azure portal](#).

Learn how to [Attach a managed data disk to a Windows VM by using the Azure portal](#).

# Create a snapshot

11/13/2019 • 2 minutes to read • [Edit Online](#)

Take a snapshot of an OS or data disk for backup or to troubleshoot VM issues. A snapshot is a full, read-only copy of a VHD.

## Use Azure CLI

The following example requires that you use [Cloud Shell](#) or have the Azure CLI installed.

The following steps show how to take a snapshot using the **az snapshot create** command with the **--source-disk** parameter. The following example assumes that there is a VM called *myVM* in the *myResourceGroup* resource group.

Get the disk ID using [az vm show](#).

```
osDiskId=$(az vm show \
 -g myResourceGroup \
 -n myVM \
 --query "storageProfile.osDisk.managedDisk.id" \
 -o tsv)
```

Take a snapshot named *osDisk-backup* using [az snapshot create](#).

```
az snapshot create \
 -g myResourceGroup \
 --source "$osDiskId" \
 --name osDisk-backup
```

### NOTE

If you would like to store your snapshot in zone-resilient storage, you need to create it in a region that supports [availability zones](#) and include the **--sku Standard\_ZRS** parameter.

You can see a list of the snapshots using [az snapshot list](#).

```
az snapshot list \
 -g myResourceGroup \
 -o table
```

## Use Azure portal

1. Sign in to the [Azure portal](#).
2. Starting in the upper-left, click **Create a resource** and search for **snapshot**. Select **Snapshot** from the search results.
3. In the **Snapshot** blade, click **Create**.
4. Enter a **Name** for the snapshot.
5. Select an existing resource group or type the name for a new one.
6. For **Source disk**, select the managed disk to snapshot.

7. Select the **Account type** to use to store the snapshot. Use **Standard HDD** unless you need it stored on a high performing SSD.
8. Click **Create**.

## Next steps

Create a virtual machine from a snapshot by creating a managed disk from the snapshot and then attaching the new managed disk as the OS disk. For more information, see the [Create a VM from a snapshot](#) script.

# Reduce costs with Azure Disks Reservation

1/30/2020 • 6 minutes to read • [Edit Online](#)

Save on your Azure Disk Storage usage with reserved capacity. Azure Disk Storage reservations combined with Azure Reserved Virtual Machine Instances let you lower your total virtual machine (VM) costs. The reservation discount is applied automatically to the matching disks in the selected reservation scope. Because of this automatic application, you don't need to assign a reservation to a managed disk to get the discounts.

Discounts are applied hourly depending on the disk usage. Unused reserved capacity doesn't carry over. Azure Disk Storage reservation discounts don't apply to unmanaged disks, ultra disks, or page blob consumption.

## Determine your storage needs

Before you purchase a reservation, determine your storage needs. Currently, Azure Disk Storage reservations are available only for select Azure premium SSD SKUs. The SKU of a premium SSD determines the disk's size and performance.

When determining your storage needs, don't think of disks based on just capacity. For example, you can't have a reservation for a P40 disk and use that to pay for two smaller P30 disks. When purchasing a reservation, you're only purchasing a reservation for the total number of disks per SKU.

A disk reservation is made per disk SKU. As a result, the reservation consumption is based on the unit of the disk SKUs instead of the provided size.

For example, assume you reserve one P40 disk that has 2 TiB of provisioned storage capacity. Also assume you allocate only two P30 disks. The P40 reservation in that case doesn't account for P30 consumption, and you pay the pay-as-you-go rate on the P30 disks.

| PRE<br>MIU<br>M<br>SSD<br>SIZE<br>S | P1*        | P2*        | P3*        | P4         | P6         | P10         | P15         | P20         | P30         | P40         | P50         | P60         | P70         | P80         |
|-------------------------------------|------------|------------|------------|------------|------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| Disk size in GiB                    | 4          | 8          | 16         | 32         | 64         | 128         | 256         | 512         | 1,024       | 2,048       | 4,096       | 8,192       | 16,384      | 32,767      |
| IOP S per disk                      | 120        | 120        | 120        | 120        | 240        | 500         | 1,100       | 2,300       | 5,000       | 7,500       | 7,500       | 16,000      | 18,000      | 20,000      |
| Throughput per disk                 | 25 MiB/sec | 25 MiB/sec | 25 MiB/sec | 25 MiB/sec | 50 MiB/sec | 100 MiB/sec | 125 MiB/sec | 150 MiB/sec | 200 MiB/sec | 250 MiB/sec | 250 MiB/sec | 500 MiB/sec | 750 MiB/sec | 900 MiB/sec |

| PRE<br>MIU<br>M<br>SSD<br>SIZE<br>S | P1*          | P2*          | P3*          | P4           | P6           | P10          | P15          | P20          | P30                 | P40                 | P50                 | P60                 | P70                 | P80                 |
|-------------------------------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|
| Max burst IOP S per disk **         | 3,500        | 3,500        | 3,500        | 3,500        | 3,500        | 3,500        | 3,500        | 3,500        |                     |                     |                     |                     |                     |                     |
| Max burst throughput per disk **    | 170 MiB /sec |                     |                     |                     |                     |                     |                     |
| Max burst duration**                | 30 min       |                     |                     |                     |                     |                     |                     |
| Eligible for reservation            | No           | Yes, up to one year |

\*Denotes a disk size that is currently in preview, for regional availability information see [New disk sizes: Managed and unmanaged](#).

\*\*Denotes a feature that is currently in preview, see [Disk bursting](#) for more information.

## Purchase considerations

We recommend the following practices when considering disk reservation purchase:

- Analyze your usage information to help determine which reservations you should purchase. Make sure you track the usage in disk SKUs instead of provisioned or used disk capacity.
- Examine your disk reservation along with your VM reservation. We highly recommend making reservations for both VM usage and disk usage for maximum savings. You can start with determining the right VM reservation and then evaluate the disk reservation. Generally, you'll have a standard configuration for each of your workloads. For example, a SQL Server server might have two P40 data disks and one P30 operating system disk.

This kind of pattern can help you determine the reserved amount you might purchase. This approach can simplify the evaluation process and ensure that you have an aligned plan for both your VM and disks. The plan contains considerations like subscriptions or regions.

# Purchase restrictions

Reservation discounts are currently unavailable for the following:

- Unmanaged disks or page blobs.
- Standard SSDs or standard hard-disk drives (HDDs).
- Premium SSD SKUs smaller than P30: P1, P2, P3, P4, P6, P10, P15, and P20 SSD SKUs.
- Disks in Azure Government, Azure Germany, or Azure China regions.

In rare circumstances, Azure limits the purchase of new reservations to a subset of disk SKUs because of low capacity in a region.

## Buy a disk reservation

You can purchase Azure Disk Storage reservations through the [Azure portal](#). You can pay for the reservation either up front or with monthly payments. For more information about purchasing with monthly payments, see [Purchase reservations with monthly payments](#).

Follow these steps to purchase reserved capacity:

1. Go to the [Purchase reservations](#) pane in the Azure portal.
2. Select **Azure Managed Disks** to purchase a reservation.

The screenshot shows the 'Purchase reservations' page in the Azure portal. It lists ten services with their respective icons and descriptions. The 'Azure Managed Disks' section is highlighted with a red box. Each service has a 'Buy' button below it.

| Service                                                    | Description                                                                                                                             | Buy Button |
|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>Virtual machine</b><br>By Microsoft Corp.               | Save on virtual machine costs by buying reserved instances for 1 or 3 years                                                             | Buy        |
| <b>SQL Database</b><br>By Microsoft Corp.                  | Save on SQL Database compute costs by buying reserved vCores for 1 or 3 years                                                           | Buy        |
| <b>Azure SQL Data Warehouse</b><br>By Microsoft Corp.      | Save up to 65% on SQL Data Warehouse costs by buying reserved capacity for 1 or 3 years                                                 | Buy        |
| <b>Azure Cosmos DB</b><br>By Microsoft Corp.               | Save up to 65% on Cosmos DB by buying reserved throughput capacity for 1 or 3 years                                                     | Buy        |
| <b>Azure Blob Storage</b><br>By Microsoft Corp.            | Save on Azure Storage costs for Block Blobs and Azure Data Lake Storage by buying Azure Blob Storage Reserved Capacity for 1 or 3 years | Buy        |
| <b>Azure Database for MySQL</b><br>By Microsoft Corp.      | Save on Azure Database for MySQL compute costs by buying reserved vCores for 1 year                                                     | Buy        |
| <b>Azure Database for MariaDB</b><br>By Microsoft Corp.    | Save on Azure Database for MariaDB compute costs by buying reserved vCores for 1 year                                                   | Buy        |
| <b>Azure Database for PostgreSQL</b><br>By Microsoft Corp. | Save on Azure Database for PostgreSQL single server compute costs by buying reserved vCores for 1 year                                  | Buy        |
| <b>Azure Managed Disks</b><br>By Microsoft Corp.           | Save on Premium SSD Managed Disks by buying reserved disks for 1 year                                                                   | Buy        |
| <b>Azure Databricks</b><br>By Microsoft Corp.              | Save on your Azure Databricks costs by pre-purchasing DBUs for 1 or 3 years                                                             | Buy        |

3. Specify the required values described in the following table:

| ELEMENT | DESCRIPTION |
|---------|-------------|
|         |             |

| ELEMENT                  | DESCRIPTION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Scope</b>             | <p>How many subscriptions can use the billing benefit associated with the reservation. This value also specifies how the reservation is applied to specific subscriptions.</p> <p>If you select <b>Shared</b>, the reservation discount is applied to Azure Storage capacity in every subscription within your billing context. The billing context is based on how you signed up for Azure. For enterprise customers, the shared scope is the enrollment and includes all subscriptions within the enrollment. For pay-as-you-go customers, the shared scope includes all individual subscriptions with pay-as-you-go rates created by the account administrator.</p> <p>If you select <b>Single subscription</b>, the reservation discount is applied to Azure Storage capacity in the selected subscription.</p> <p>If you select <b>Single resource group</b>, the reservation discount is applied to Azure Storage capacity in the selected subscription and in that subscription's selected resource group.</p> <p>You can change the reservation scope after you purchase the reservation.</p> |
| <b>Subscription</b>      | <p>The subscription you use to pay for the Azure Storage reservation. The payment method on the selected subscription is used in charging the costs. The subscription must be one of the following types:</p> <ul style="list-style-type: none"> <li>Enterprise Agreement (offer numbers MS-AZR-0017P and MS-AZR-0148P). For an Enterprise subscription, the charges are deducted from the enrollment's monetary commitment balance or charged as overage.</li> <li>Individual subscription with pay-as-you-go rates (offer numbers MS-AZR-0003P and MS-AZR-0023P). For an individual subscription with pay-as-you-go rates, the charges are billed to the credit card or invoice payment method on the subscription.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Disks</b>             | The SKU you want to create.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Region</b>            | The region where the reservation is in effect.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Billing frequency</b> | How often the account is billed for the reservation. Options include <b>Monthly</b> and <b>Upfront</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

Select the product you want to purchase X

Save on your Premium SSD Managed Disks usage by purchasing reserved capacity. Discounts are applied hourly on the disk usage, any unused reserved capacity does not carry over. Reservation discount does not apply to Premium SSD Unmanaged Disks or Page Blob consumption. [Learn More](#)

Scope \* Shared Subscription \* Sub for RI Testing

Region : **West Europe** Disk : **Select a value** Billing frequency : **Select a value** Reset filters

| ↑↓ | Name                      | ↑↓ | Disk | ↑↓ | Region      | ↑↓ | Term     | ↑↓ | Billing frequency | ↑↓ |
|----|---------------------------|----|------|----|-------------|----|----------|----|-------------------|----|
|    | Premium SSD Managed Disks |    | P30  |    | West Europe |    | One Year |    | Upfront           |    |
|    | Premium SSD Managed Disks |    | P30  |    | West Europe |    | One Year |    | Monthly           |    |
|    | Premium SSD Managed Disks |    | P40  |    | West Europe |    | One Year |    | Upfront           |    |
|    | Premium SSD Managed Disks |    | P40  |    | West Europe |    | One Year |    | Monthly           |    |
|    | Premium SSD Managed Disks |    | P50  |    | West Europe |    | One Year |    | Upfront           |    |
|    | Premium SSD Managed Disks |    | P50  |    | West Europe |    | One Year |    | Monthly           |    |
|    | Premium SSD Managed Disks |    | P60  |    | West Europe |    | One Year |    | Upfront           |    |
|    | Premium SSD Managed Disks |    | P60  |    | West Europe |    | One Year |    | Monthly           |    |
|    | Premium SSD Managed Disks |    | P70  |    | West Europe |    | One Year |    | Upfront           |    |
|    | Premium SSD Managed Disks |    | P70  |    | West Europe |    | One Year |    | Monthly           |    |
|    | Premium SSD Managed Disks |    | P80  |    | West Europe |    | One Year |    | Upfront           |    |
|    | Premium SSD Managed Disks |    | P80  |    | West Europe |    | One Year |    | Monthly           |    |

Select Cancel

4. After you specify the values for your reservation, the Azure portal displays the cost. The portal also shows the discount percentage over pay-as-you-go billing. Select **Next** to continue to the **Purchase reservations** pane.
5. On the **Purchase reservations** pane, you can name your reservation and select the total quantity of reservations you want to make. The number of reservations maps to the number of disks. For example, if you want to reserve a hundred disks, enter the **Quantity** value **100**.
6. Review the total cost of the reservation.

Home > Reservations > Purchase reservations

**Purchase reservations**

Products Review + buy

 Azure Managed Disks Download Cart

| ↑↓ | Reservation name         | ↑↓ | Product                                                  | ↑↓ | Scalability | Unit price↑↓ | Quantity↑↓                                                                               | Subtotal (% Discount)↑↓ | Billing frequency↑↓ |                                                                                       |
|----|--------------------------|----|----------------------------------------------------------|----|-------------|--------------|------------------------------------------------------------------------------------------|-------------------------|---------------------|---------------------------------------------------------------------------------------|
|    | Disk_RI_01-14-2020_10-31 |    | Premium SSD Managed Disks   P30   West Europe   One Year |    | Shared      | <price>      | <input style="border: 1px solid red; width: 40px; height: 20px;" type="text" value="1"/> | <subtotal>              | Upfront             |  |

Next: Review + buy Total reservation cost <total-cost>

After you purchase a reservation, it's automatically applied to any existing Disk Storage resources that match the reservation terms. If you haven't created any Disk Storage resources yet, the reservation applies whenever you create a resource that matches the reservation terms. In either case, the reservation term begins immediately after a successful purchase.

## Cancel, exchange, or refund reservations

You can cancel, exchange, or refund reservations within certain limitations. For more information, see [Self-service exchanges and refunds for Azure Reservations](#).

## Expiration of a reservation

When a reservation expires, any Azure Disk Storage capacity that you use under that reservation is billed at the pay-as-you-go rate. Reservations don't renew automatically.

You'll receive an email notification 30 days before the expiration of the reservation and again on the expiration date. To continue taking advantage of the cost savings that a reservation provides, renew it no later than the expiration date.

## Need help? Contact us

If you have questions or need help, [create a support request](#).

## Next steps

- [What are Azure Reservations?](#)
- [Understand how your reservation discount is applied to Azure Disk Storage](#)

# Creating an incremental snapshot (preview) for managed disks

11/13/2019 • 5 minutes to read • [Edit Online](#)

Incremental snapshots (preview) are point in time backups for managed disks that, when taken, consist only of all the changes since the last snapshot. When you attempt to download or otherwise use an incremental snapshot, the full VHD is used. This new capability for managed disk snapshots can potentially allow them to be more cost effective, since you are no longer required to store the entire disk with each individual snapshot, unless you choose to. Just like regular snapshots, incremental snapshots can be used to create a full managed disk or, to make a regular snapshot.

There are a few differences between an incremental snapshot and a regular snapshot. Incremental snapshots will always use standard HDDs storage, irrespective of the storage type of the disk, whereas regular snapshots can use premium SSDs. If you are using regular snapshots on Premium Storage to scale up VM deployments, we recommend you use custom images on standard storage in the [Shared Image Gallery](#). It will help you to achieve a more massive scale with lower cost. Additionally, incremental snapshots potentially offer better reliability with [zone-redundant storage](#) (ZRS). If ZRS is available in the selected region, an incremental snapshot will use ZRS automatically. If ZRS is not available in the region, then the snapshot will default to [locally-redundant storage](#) (LRS). You can override this behavior and select one manually but, we do not recommend that.

Incremental snapshots also offer a differential capability, which is uniquely available to managed disks. They enable you to get the changes between two incremental snapshots of the same managed disks, down to the block level. You can use this capability to reduce your data footprint when copying snapshots across regions.

## Supported regions

Only the following regions are currently supported:

- Available as a GA offering in the West Central US, Canada East, Canada Central regions.
- Available as a public preview in the East US, East US 2, Central US, North Europe, South East Asia regions.

## Restrictions

- Incremental snapshots currently cannot be created after you've changed the size of a disk (during preview only).
- Incremental snapshots currently cannot be moved between subscriptions.
- You can currently only generate SAS URIs of up to five snapshots of a particular snapshot family at any given time.
- You cannot create an incremental snapshot for a particular disk outside of that disk's subscription.
- Up to seven incremental snapshots per disk can be created every five minutes.
- A total of 200 incremental snapshots can be created for a single disk.

## PowerShell

You can use Azure PowerShell to create an incremental snapshot. You will need the latest version of Azure PowerShell, the following command will either install it or update your existing installation to latest:

```
Install-Module -Name Az -AllowClobber -Scope CurrentUser
```

Once that is installed, login to your PowerShell session with `az login`.

To create an incremental snapshot with Azure PowerShell, set the configuration with [New-AzSnapshotConfig](#) with the `-Incremental` parameter and then pass that as a variable to [New-AzSnapshot](#) through the `-Snapshot` parameter.

Replace `<yourDiskNameHere>`, `<yourResourceGroupNameHere>`, and `<yourDesiredSnapshotNameHere>` with your values, then you can use the following script to create an incremental snapshot:

```
Get the disk that you need to backup by creating an incremental snapshot
$yourDisk = Get-AzDisk -DiskName <yourDiskNameHere> -ResourceGroupName <yourResourceGroupNameHere>

Create an incremental snapshot by setting the SourceUri property with the value of the Id property of the disk
$snapshotConfig=New-AzSnapshotConfig -SourceUri $yourDisk.Id -Location $yourDisk.Location -CreateOption Copy -Incremental
New-AzSnapshot -ResourceGroupName <yourResourceGroupNameHere> -SnapshotName <yourDesiredSnapshotNameHere> -Snapshot $snapshotConfig
```

You can identify incremental snapshots from the same disk with the `SourceResourceId` and the `SourceUniqueId` properties of snapshots. `SourceResourceId` is the Azure Resource Manager resource ID of the parent disk.

`SourceUniqueId` is the value inherited from the `UniqueId` property of the disk. If you were to delete a disk and then create a new disk with the same name, the value of the `UniqueId` property changes.

You can use `SourceResourceId` and `SourceUniqueId` to create a list of all snapshots associated with a particular disk. Replace `<yourResourceGroupNameHere>` with your value and then you can use the following example to list your existing incremental snapshots:

```
$snapshots = Get-AzSnapshot -ResourceGroupName <yourResourceGroupNameHere>

$incrementalSnapshots = New-Object System.Collections.ArrayList
foreach ($snapshot in $snapshots)
{
 if($snapshot.Incremental -and $snapshot.CreationData.SourceResourceId -eq $yourDisk.Id -and $snapshot.CreationData.SourceUniqueId -eq $yourDisk.UniqueId){
 $incrementalSnapshots.Add($snapshot)
 }
}

$incrementalSnapshots
```

## CLI

You can create an incremental snapshot with the Azure CLI, you will need the latest version of Azure CLI.

On Windows, the following command will either install or update your existing installation to the latest version:

```
Invoke-WebRequest -Uri https://aka.ms/installazurecliwindows -OutFile .\AzureCLI.msi; Start-Process msieexec.exe -Wait -ArgumentList '/I AzureCLI.msi /quiet'
```

On Linux, the CLI installation will vary depending on operating system version. See [Install the Azure CLI](#) for your particular Linux version.

To create an incremental snapshot, use `az snapshot create` with the `--incremental` parameter.

The following example creates an incremental snapshot, replace `<yourDesiredSnapshotNameHere>`, `<yourResourceGroupNameHere>`, `<exampleDiskName>`, and `<exampleLocation>` with your own values, then run the

example:

```
sourceResourceId=$(az disk show -g <yourResourceGroupNameHere> -n <exampleDiskName> --query '[id]' -o tsv)

az snapshot create -g <yourResourceGroupNameHere> \
-n <yourDesiredSnapshotNameHere> \
-l <exampleLocation> \
--source "$sourceResourceId" \
--incremental
```

You can identify incremental snapshots from the same disk with the `SourceResourceId` and the `SourceUniqueId` properties of snapshots. `SourceResourceId` is the Azure Resource Manager resource ID of the parent disk.

`SourceUniqueId` is the value inherited from the `UniqueId` property of the disk. If you were to delete a disk and then create a new disk with the same name, the value of the `UniqueId` property changes.

You can use `SourceResourceId` and `SourceUniqueId` to create a list of all snapshots associated with a particular disk. The following example will list all incremental snapshots associated with a particular disk but, it requires some setup.

This example uses jq for querying the data. To run the example, you must [install jq](#).

Replace `<yourResourceGroupNameHere>` and `<exampleDiskName>` with your values, then you can use the following example to list your existing incremental snapshots, as long as you've also installed jq:

```
sourceUniqueId=$(az disk show -g <yourResourceGroupNameHere> -n <exampleDiskName> --query '[uniqueId]' -o tsv)

sourceResourceId=$(az disk show -g <yourResourceGroupNameHere> -n <exampleDiskName> --query '[id]' -o tsv)

az snapshot list -g <yourResourceGroupNameHere> -o json \
| jq -cr --arg SUID "$sourceUniqueId" --arg SRID "$sourceResourceId" '.[] | select(.incremental==true and
.creationData.sourceUniqueId==$SUID and .creationData.sourceResourceId==$SRID)'
```

## Resource Manager template

You can also use Azure Resource Manager templates to create an incremental snapshot. You'll need to make sure the `apiVersion` is set to **2019-03-01** and that the `incremental` property is also set to true. The following snippet is an example of how to create an incremental snapshot with Resource Manager templates:

```
{
 "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
 "contentVersion": "1.0.0.0",
 "parameters": {
 "diskName": {
 "type": "string",
 "defaultValue": "contosodisk1"
 },
 "diskResourceId": {
 "defaultValue": "<your_managed_disk_resource_ID>",
 "type": "String"
 }
 },
 "resources": [
 {
 "type": "Microsoft.Compute/snapshots",
 "name": "[concat(parameters('diskName'), '_snapshot1')]",
 "location": "[resourceGroup().location]",
 "apiVersion": "2019-03-01",
 "properties": {
 "creationData": {
 "createOption": "Copy",
 "sourceResourceId": "[parameters('diskResourceId')]"
 },
 "incremental": true
 }
 }
]
}
```

## Next steps

If you'd like to see sample code demonstrating the differential capability of incremental snapshots, using .NET, see [Copy Azure Managed Disks backups to another region with differential capability of incremental snapshots](#).

# Back up Azure unmanaged VM disks with incremental snapshots

1/26/2020 • 7 minutes to read • [Edit Online](#)

## Overview

Azure Storage provides the capability to take snapshots of blobs. Snapshots capture the blob state at that point in time. In this article, we describe a scenario in which you can maintain backups of virtual machine disks using snapshots. You can use this methodology when you choose not to use Azure Backup and Recovery Service, and wish to create a custom backup strategy for your virtual machine disks.

Azure virtual machine disks are stored as page blobs in Azure Storage. Since we are describing a backup strategy for virtual machine disks in this article, we refer to snapshots in the context of page blobs. To learn more about snapshots, refer to [Creating a Snapshot of a Blob](#).

## What is a snapshot?

A blob snapshot is a read-only version of a blob that is captured at a point in time. Once a snapshot has been created, it can be read, copied, or deleted, but not modified. Snapshots provide a way to back up a blob as it appears at a moment in time. Until REST version 2015-04-05, you had the ability to copy full snapshots. With the REST version 2015-07-08 and above, you can also copy incremental snapshots.

## Full snapshot copy

Snapshots can be copied to another storage account as a blob to keep backups of the base blob. You can also copy a snapshot over its base blob, which is like restoring the blob to an earlier version. When a snapshot is copied from one storage account to another, it occupies the same space as the base page blob. Therefore, copying whole snapshots from one storage account to another is slow and consumes much space in the target storage account.

### NOTE

If you copy the base blob to another destination, the snapshots of the blob are not copied along with it. Similarly, if you overwrite a base blob with a copy, snapshots associated with the base blob are not affected and stay intact under the base blob name.

### Back up disks using snapshots

As a backup strategy for your virtual machine disks, you can take periodic snapshots of the disk or page blob, and copy them to another storage account using tools like [Copy Blob](#) operation or [AzCopy](#). You can copy a snapshot to a destination page blob with a different name. The resulting destination page blob is a writeable page blob and not a snapshot. Later in this article, we describe steps to take backups of virtual machine disks using snapshots.

### Restore disks using snapshots

When it is time to restore your disk to a stable version that was previously captured in one of the backup snapshots, you can copy a snapshot over the base page blob. After the snapshot is promoted to the base page blob, the snapshot remains, but its source is overwritten with a copy that can be both read and written. Later in this article we describe steps to restore a previous version of your disk from its snapshot.

### Implementing full snapshot copy

You can implement a full snapshot copy by doing the following,

- First, take a snapshot of the base blob using the [Snapshot Blob](#) operation.
- Then, copy the snapshot to a target storage account using [Copy Blob](#).
- Repeat this process to maintain backup copies of your base blob.

## Incremental snapshot copy

The new feature in the [GetPageRanges](#) API provides a much better way to back up the snapshots of your page blobs or disks. The API returns the list of changes between the base blob and the snapshots, which reduces the amount of storage space used on the backup account. The API supports page blobs on Premium Storage as well as Standard Storage. Using this API, you can build faster and more efficient backup solutions for Azure VMs. This API will be available with the REST version 2015-07-08 and higher.

Incremental Snapshot Copy allows you to copy from one storage account to another the difference between,

- Base blob and its Snapshot OR
- Any two snapshots of the base blob

Provided the following conditions are met,

- The blob was created on Jan-1-2016 or later.
- The blob was not overwritten with [PutPage](#) or [Copy Blob](#) between two snapshots.

**Note:** This feature is available for Premium and Standard Azure Page Blobs.

When you have a custom backup strategy using snapshots, copying the snapshots from one storage account to another can be slow and can consume much storage space. Instead of copying the entire snapshot to a backup storage account, you can write the difference between consecutive snapshots to a backup page blob. This way, the time to copy and the space to store backups is substantially reduced.

### Implementing Incremental Snapshot Copy

You can implement incremental snapshot copy by doing the following,

- Take a snapshot of the base blob using [Snapshot Blob](#).
- Copy the snapshot to the target backup storage account in same or any other Azure region using [Copy Blob](#).  
This is the backup page blob. Take a snapshot of the backup page blob and store it in the backup account.
- Take another snapshot of the base blob using [Snapshot Blob](#).
- Get the difference between the first and second snapshots of the base blob using [GetPageRanges](#). Use the new parameter **prevsnapshot**, to specify the DateTime value of the snapshot you want to get the difference with.  
When this parameter is present, the REST response includes only the pages that were changed between target snapshot and previous snapshot including clear pages.
- Use [PutPage](#) to apply these changes to the backup page blob.
- Finally, take a snapshot of the backup page blob and store it in the backup storage account.

In the next section, we will describe in more detail how you can maintain backups of disks using Incremental Snapshot Copy

## Scenario

In this section, we describe a scenario that involves a custom backup strategy for virtual machine disks using snapshots.

Consider a DS-series Azure VM with a premium storage P30 disk attached. The P30 disk called *mypremiumdisk* is stored in a premium storage account called *mypremiumaccount*. A standard storage account called *mybackupstdaccount* is used for storing the backup of *mypremiumdisk*. We would like to keep a snapshot of *mypremiumdisk* every 12 hours.

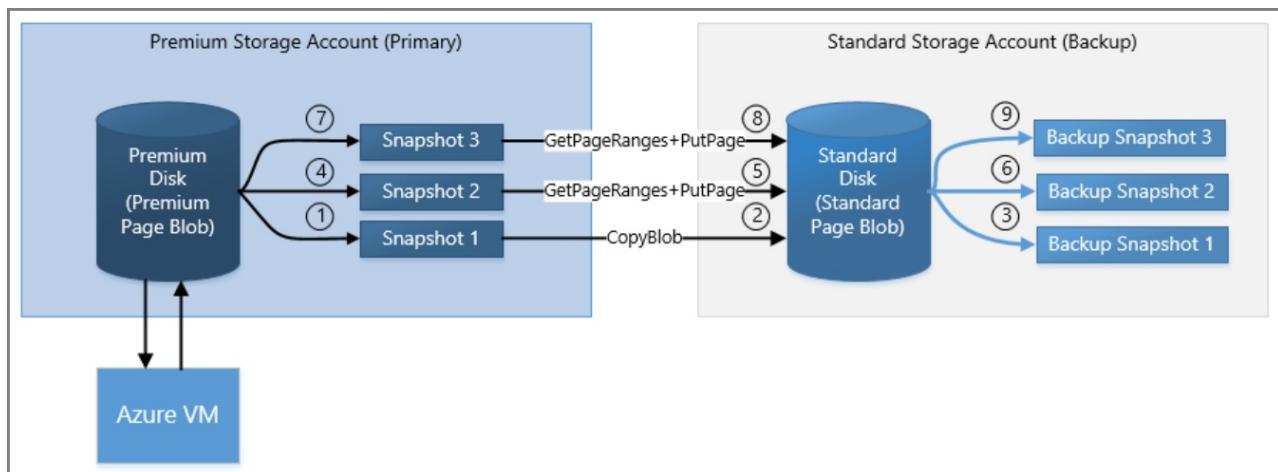
To learn about creating a storage account, see [Create a storage account](#).

To learn about backing up Azure VMs, refer to [Plan Azure VM backups](#).

## Steps to maintain backups of a disk using incremental snapshots

The following steps describe how to take snapshots of *mypremiumdisk* and maintain the backups in *mybackupsdaccount*. The backup is a standard page blob called *mybackupsdpageblob*. The backup page blob always reflects the same state as the last snapshot of *mypremiumdisk*.

1. Create the backup page blob for your premium storage disk, by taking a snapshot of *mypremiumdisk* called *mypremiumdisk\_ss1*.
2. Copy this snapshot to *mybackupsdaccount* as a page blob called *mybackupsdpageblob*.
3. Take a snapshot of *mybackupsdpageblob* called *mybackupsdpageblob\_ss1*, using [Snapshot Blob](#) and store it in *mybackupsdaccount*.
4. During the backup window, create another snapshot of *mypremiumdisk*, say *mypremiumdisk\_ss2*, and store it in *mypremiumaccount*.
5. Get the incremental changes between the two snapshots, *mypremiumdisk\_ss2* and *mypremiumdisk\_ss1*, using [GetPageRanges](#) on *mypremiumdisk\_ss2* with the **prevsnapshot** parameter set to the timestamp of *mypremiumdisk\_ss1*. Write these incremental changes to the backup page blob *mybackupsdpageblob* in *mybackupsdaccount*. If there are deleted ranges in the incremental changes, they must be cleared from the backup page blob. Use [PutPage](#) to write incremental changes to the backup page blob.
6. Take a snapshot of the backup page blob *mybackupsdpageblob*, called *mybackupsdpageblob\_ss2*. Delete the previous snapshot *mypremiumdisk\_ss1* from premium storage account.
7. Repeat steps 4–6 every backup window. In this way, you can maintain backups of *mypremiumdisk* in a standard storage account.



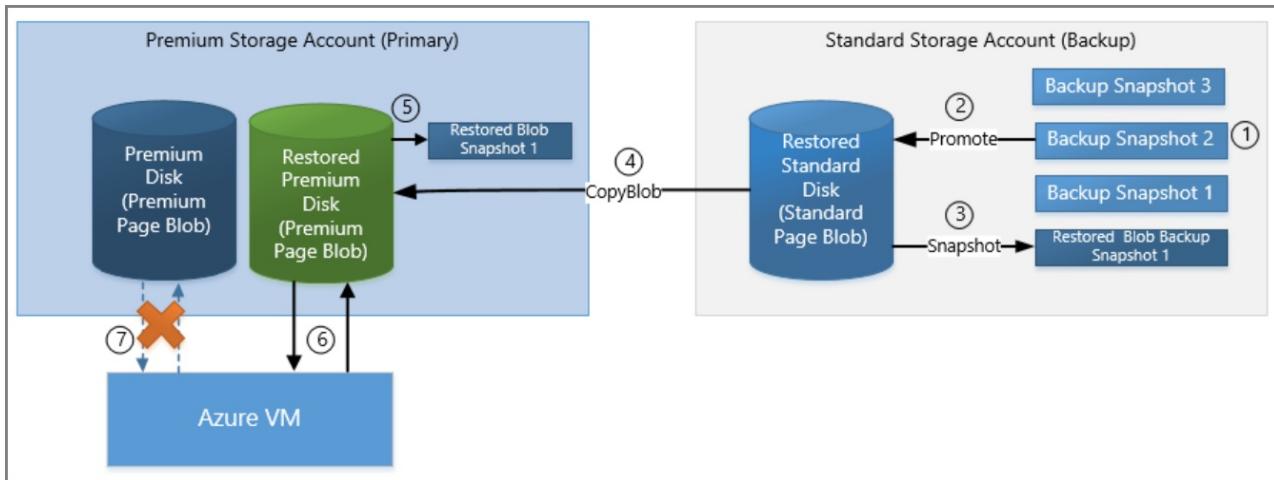
## Steps to restore a disk from snapshots

The following steps, describe how to restore the premium disk, *mypremiumdisk* to an earlier snapshot from the backup storage account *mybackupsdaccount*.

1. Identify the point in time that you wish to restore the premium disk to. Let's say that it is snapshot *mybackupsdpageblob\_ss2*, which is stored in the backup storage account *mybackupsdaccount*.
2. In *mybackupsdaccount*, promote the snapshot *mybackupsdpageblob\_ss2* as the new backup base page blob *mybackupsdpageblobrestored*.
3. Take a snapshot of this restored backup page blob, called *mybackupsdpageblobrestored\_ss1*.
4. Copy the restored page blob *mybackupsdpageblobrestored* from *mybackupsdaccount* to *mypremiumaccount* as the new premium disk *mypremiumdiskrestored*.
5. Take a snapshot of *mypremiumdiskrestored*, called *mypremiumdiskrestored\_ss1* for making future incremental

backups.

6. Point the DS series VM to the restored disk *mypremiumdiskrestored* and detach the old *mypremiumdisk* from the VM.
7. Begin the Backup process described in previous section for the restored disk *mypremiumdiskrestored*, using the *mybackupstdpageblobrestored* as the backup page blob.



## Next Steps

Use the following links to learn more about creating snapshots of a blob and planning your VM backup infrastructure.

- [Creating a Snapshot of a Blob](#)
- [Plan your VM Backup Infrastructure](#)

# Migrate to Premium Storage by using Azure Site Recovery

11/13/2019 • 11 minutes to read • [Edit Online](#)

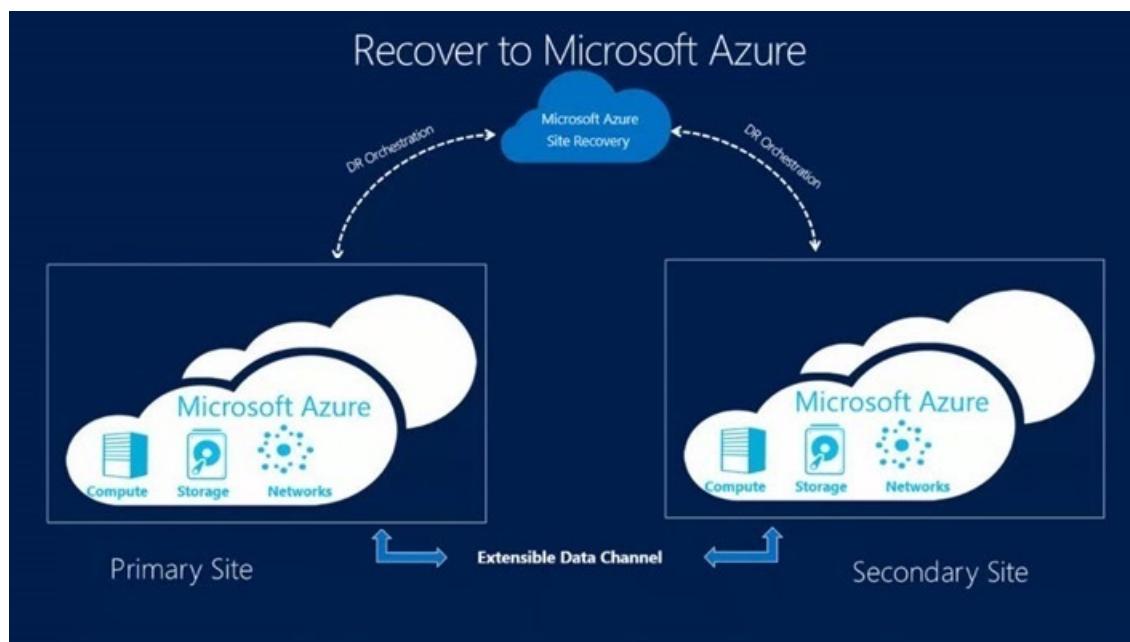
Azure premium SSDs delivers high-performance, low-latency disk support for virtual machines (VMs) that are running I/O-intensive workloads. This guide helps you migrate your VM disks from a standard storage account to a premium storage account by using [Azure Site Recovery](#).

Site Recovery is an Azure service that contributes to your strategy for business continuity and disaster recovery by orchestrating the replication of on-premises physical servers and VMs to the cloud (Azure) or to a secondary datacenter. When outages occur in your primary location, you fail over to the secondary location to keep applications and workloads available. You fail back to your primary location when it returns to normal operation.

Site Recovery provides test failovers to support disaster recovery drills without affecting production environments. You can run failovers with minimal data loss (depending on replication frequency) for unexpected disasters. In the scenario of migrating to Premium Storage, you can use the [failover in Site Recovery](#) to migrate target disks to a premium storage account.

We recommend migrating to Premium Storage by using Site Recovery because this option provides minimal downtime. This option also avoids the manual execution of copying disks and creating new VMs. Site Recovery will systematically copy your disks and create new VMs during failover.

Site Recovery supports a number of types of failover with minimal or no downtime. To plan your downtime and estimate data loss, see the [types of failover in Site Recovery](#). If you [prepare to connect to Azure VMs after failover](#), you should be able to connect to the Azure VM by using RDP after failover.



## Azure Site Recovery components

These Site Recovery components are relevant to this migration scenario:

- **Configuration server** is an Azure VM that coordinates communication and manages data replication and recovery processes. On this VM, you run a single setup file to install the configuration server and an additional component, called a process server, as a replication gateway. Read about [configuration server](#)

[prerequisites](#). You set up the configuration server only once, and you can use it for all migrations to the same region.

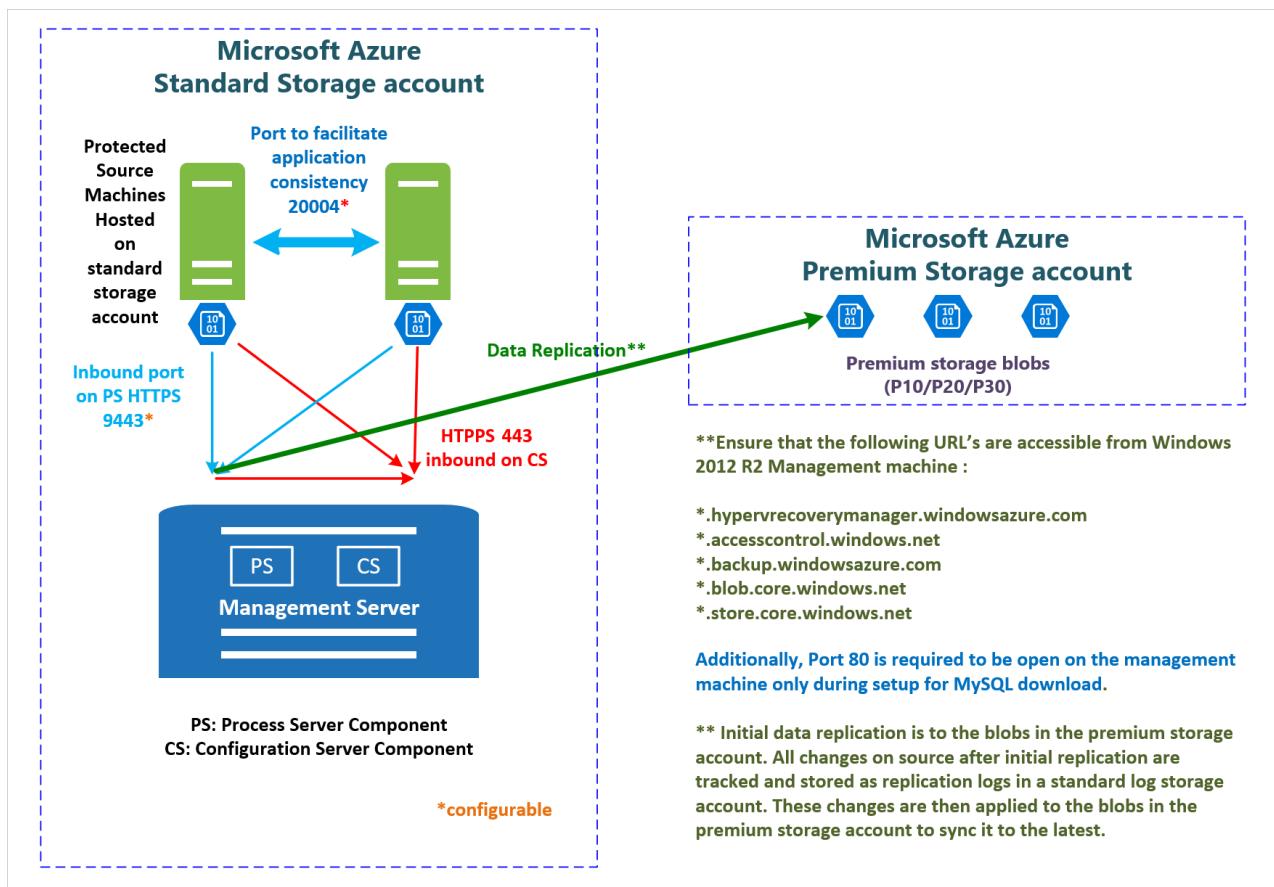
- **Process server** is a replication gateway that:

1. Receives replication data from source VMs.
2. Optimizes the data with caching, compression, and encryption.
3. Sends the data to a storage account.

It also handles push installation of the mobility service to source VMs and performs automatic discovery of source VMs. The default process server is installed on the configuration server. You can deploy additional standalone process servers to scale your deployment. Read about [best practices for process server deployment](#) and [deploying additional process servers](#). You set up the process server only once, and you can use it for all migrations to the same region.

- **Mobility service** is a component that is deployed on every standard VM that you want to replicate. It captures data writes on the standard VM and forwards them to the process server. Read about [replicated machine prerequisites](#).

This graphic shows how these components interact:



#### NOTE

Site Recovery does not support the migration of Storage Spaces disks.

For additional components for other scenarios, see [Scenario architecture](#).

## Azure essentials

These are the Azure requirements for this migration scenario:

- An Azure subscription.

- An Azure premium storage account to store replicated data.
- An Azure virtual network to which VMs will connect when they're created at failover. The Azure virtual network must be in the same region as the one in which Site Recovery runs.
- An Azure standard storage account to store replication logs. This can be the same storage account for the VM disks that are being migrated.

## Prerequisites

- Understand the relevant migration scenario components in the preceding section.
- Plan your downtime by learning about [failover in Site Recovery](#).

## Setup and migration steps

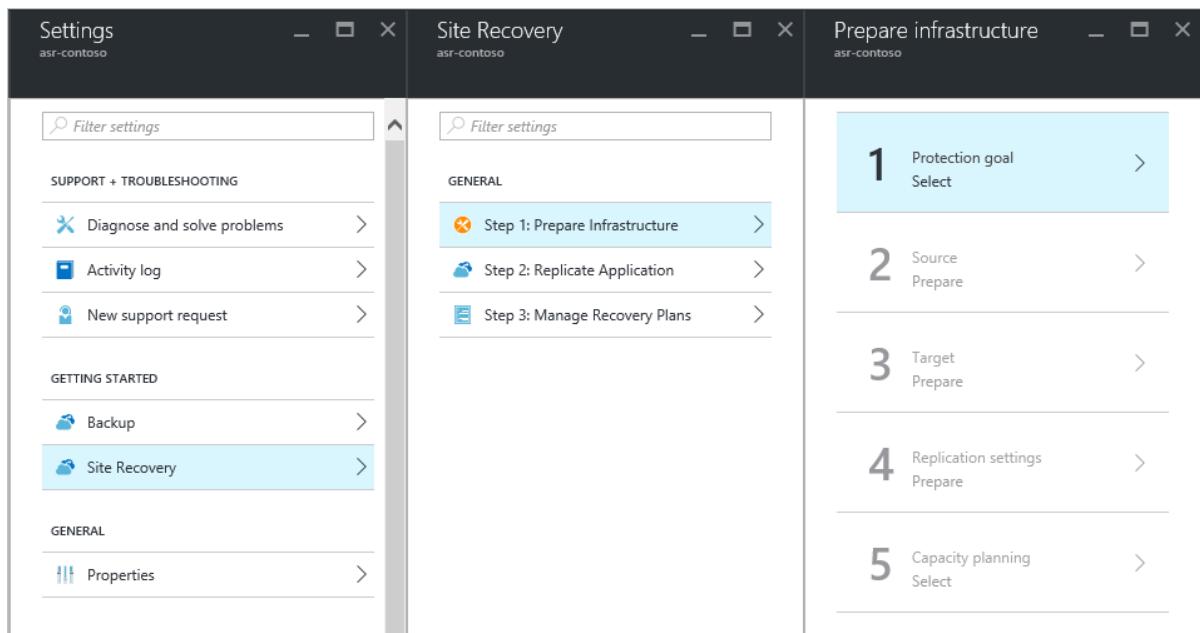
You can use Site Recovery to migrate Azure IaaS VMs between regions or within same region. The following instructions are tailored for this migration scenario from the article [Replicate VMware VMs or physical servers to Azure](#). Please follow the links for detailed steps in addition to the instructions in this article.

### Step 1: Create a Recovery Services vault

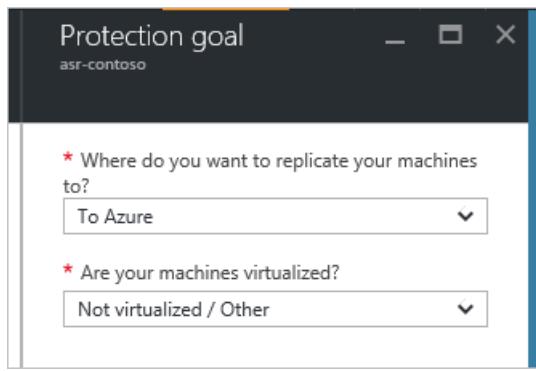
1. Open the [Azure portal](#).
2. Select **Create a resource > Management > Backup and Site Recovery (OMS)**. Alternatively, you can select **Browse > Recovery Services Vault > Add**.
3. Specify a region that VMs will be replicated to. For the purpose of migration in the same region, select the region where your source VMs and source storage accounts are.

### Step 2: Choose your protection goals

1. On the VM where you want to install the configuration server, open the [Azure portal](#).
2. Go to **Recovery Services vaults > Settings > Site Recovery > Step 1: Prepare Infrastructure > Protection goal**.



3. Under **Protection goal**, in the first drop-down list, select **To Azure**. In the second drop-down list, select **Not virtualized / Other**, and then select **OK**.

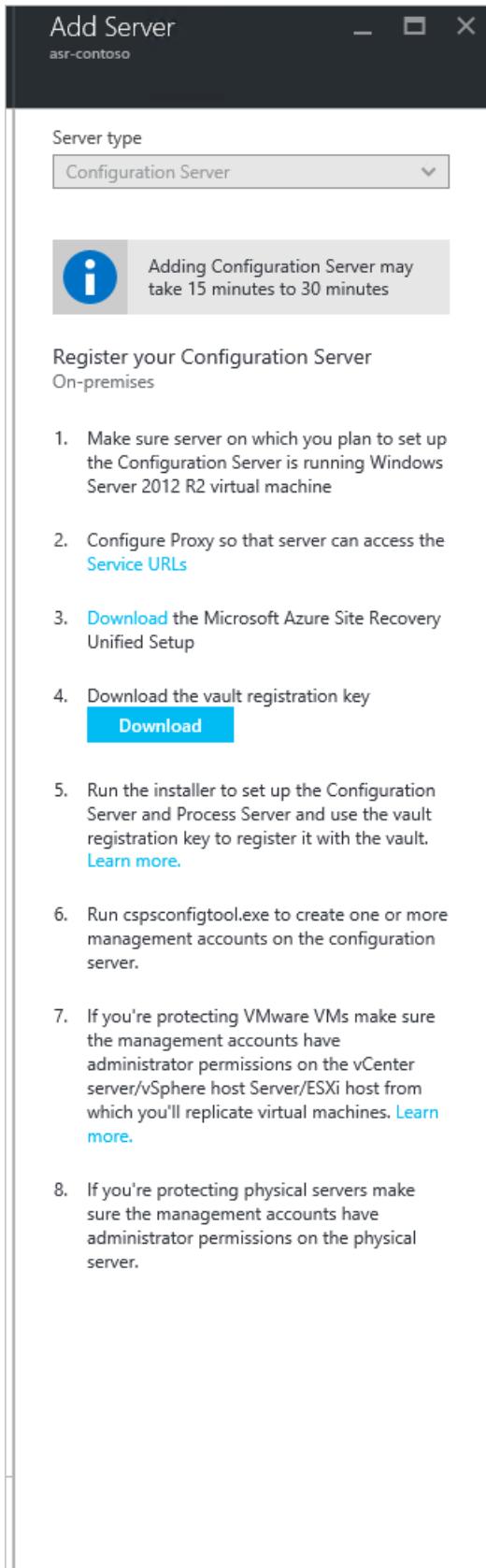


### Step 3: Set up the source environment (configuration server)

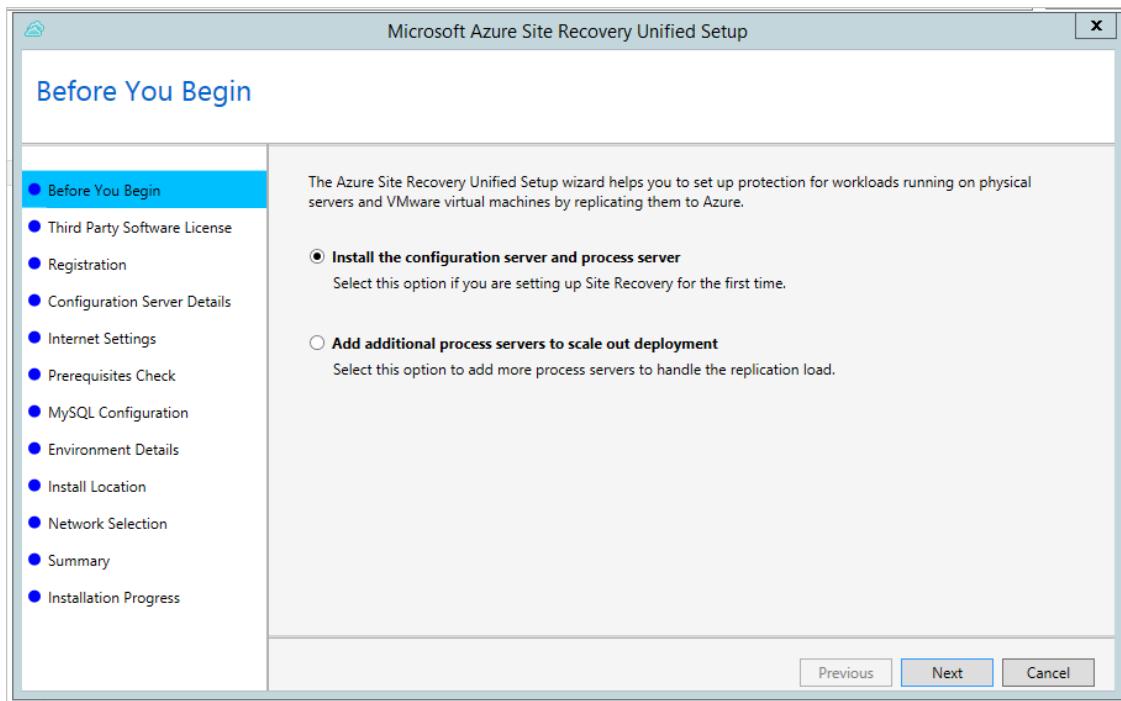
1. Download **Azure Site Recovery Unified Setup** and the vault registration key by going to the **Prepare infrastructure > Prepare source > Add Server** panes.

You will need the vault registration key to run the unified setup. The key is valid for five days after you generate it.

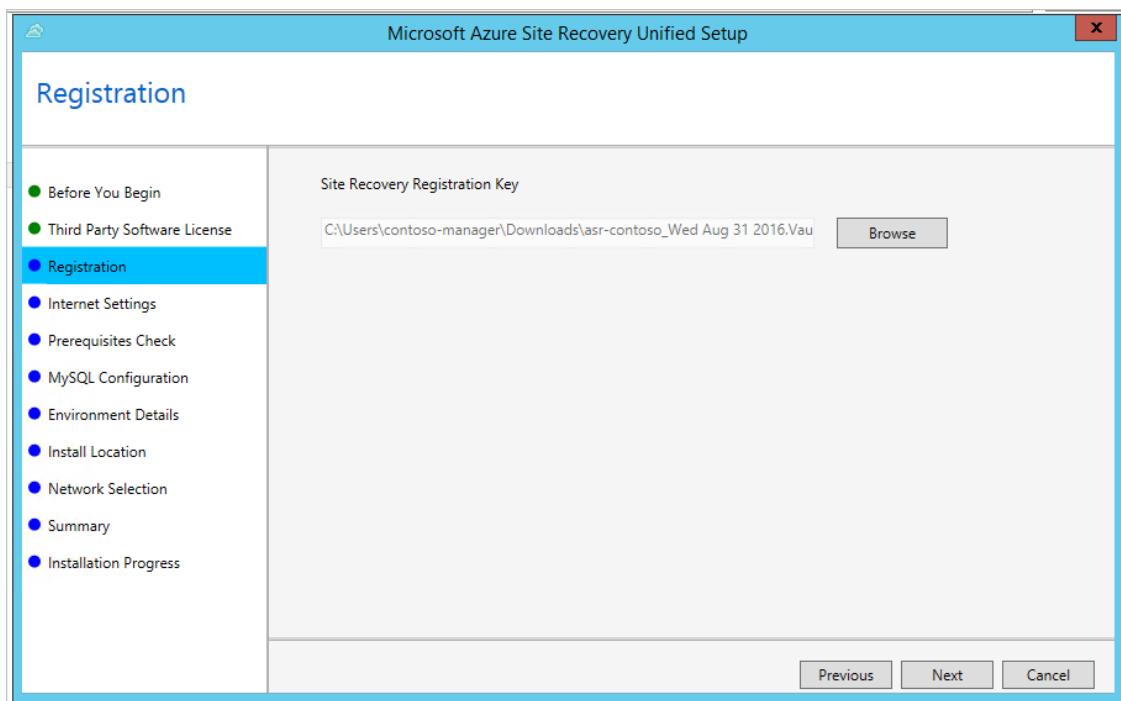
2. In the **Add Server** pane, add a configuration server.



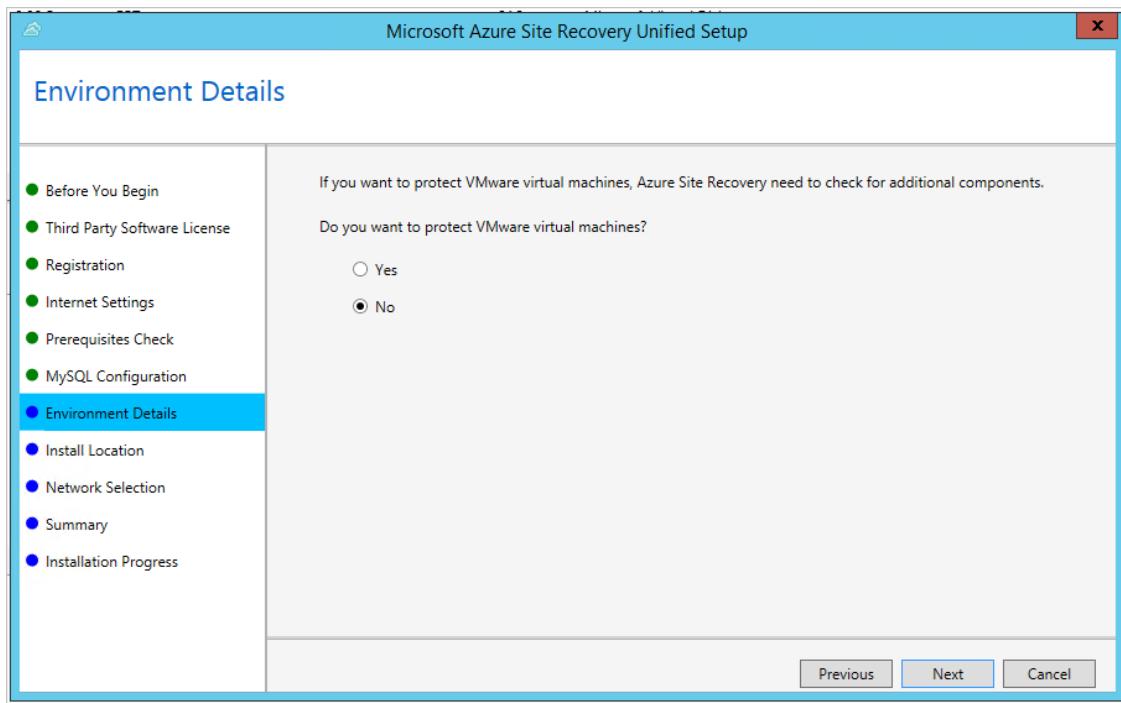
3. On the VM that you're using as the configuration server, run Unified Setup to install the configuration server and the process server. You can [walk through the screenshots](#) to complete the installation. You can refer to the following screenshots for steps specified for this migration scenario.
    - a. In **Before You Begin**, select **Install the configuration server and process server**.



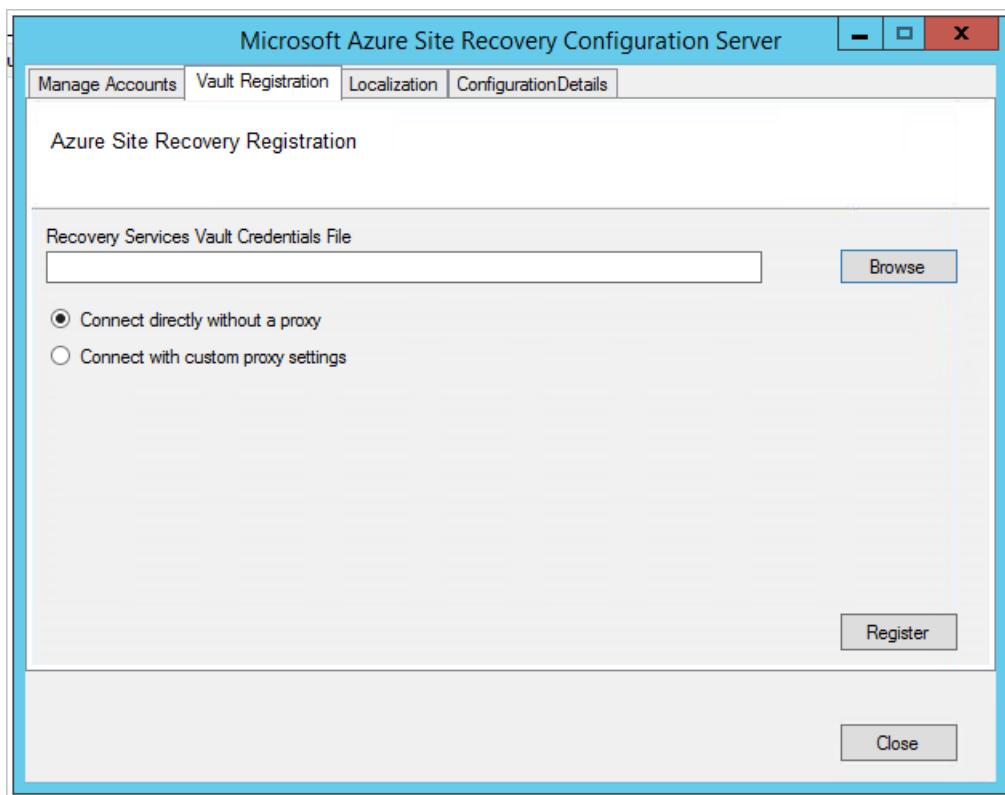
- b. In **Registration**, browse and select the registration key that you downloaded from the vault.



- c. In **Environment Details**, select whether you're going to replicate VMware VMs. For this migration scenario, choose **No**.



4. After the installation is complete, do the following in the **Microsoft Azure Site Recovery Configuration Server** window:
  - a. Use the **Manage Accounts** tab to create the account that Site Recovery can use for automatic discovery. (In the scenario about protecting physical machines, setting up the account isn't relevant, but you need at least one account to enable one of the following steps. In this case, you can name the account and password as any.)
  - b. Use the **Vault Registration** tab to upload the vault credential file.



#### Step 4: Set up the target environment

Select **Prepare infrastructure > Target**, and specify the deployment model that you want to use for VMs after failover. You can choose **Classic** or **Resource Manager**, depending on your scenario.

The screenshot shows two windows side-by-side. The left window is titled 'Prepare infrastructure' and lists five steps: 1. Protection goal (VMware VMs/physical servers t...), 2. Source (CONTOSO-CONFIG), 3. Target (Prepare, highlighted in blue), 4. Replication settings (Prepare), and 5. Capacity planning (Select). The right window is titled 'Target' and shows the configuration for step 3. It includes sections for 'Step 1 : Select Azure subscription' (Subscription: Visual Studio Enterprise, Deployment model: Classic selected), 'Step 2 : Ensure that at least one compatible Azure storage account exist' (Storage account(s): Found 5 compatible Azure storage accounts out of 6 available in the subscription), and 'Step 3 : Ensure that at least one compatible Azure virtual network exist' (Network(s): Found 2 compatible Azure virtual networks out of 2 available in the subscription).

Site Recovery checks that you have one or more compatible Azure storage accounts and networks.

#### NOTE

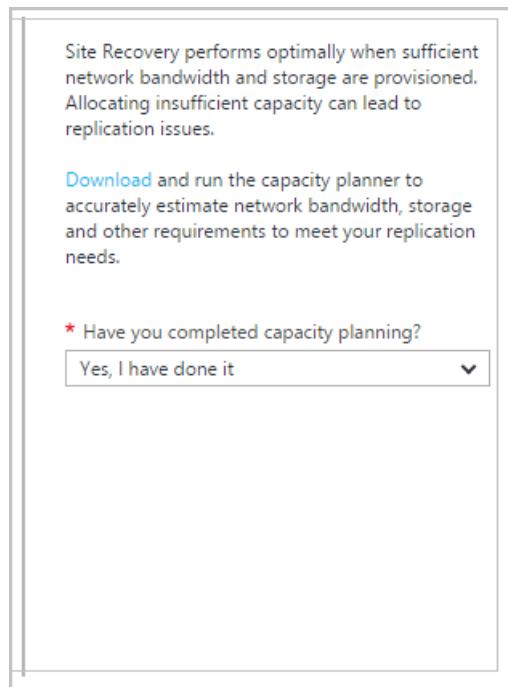
If you're using a premium storage account for replicated data, you need to set up an additional standard storage account to store replication logs.

#### Step 5: Set up replication settings

To verify that your configuration server is successfully associated with the replication policy that you create, follow [Set up replication settings](#).

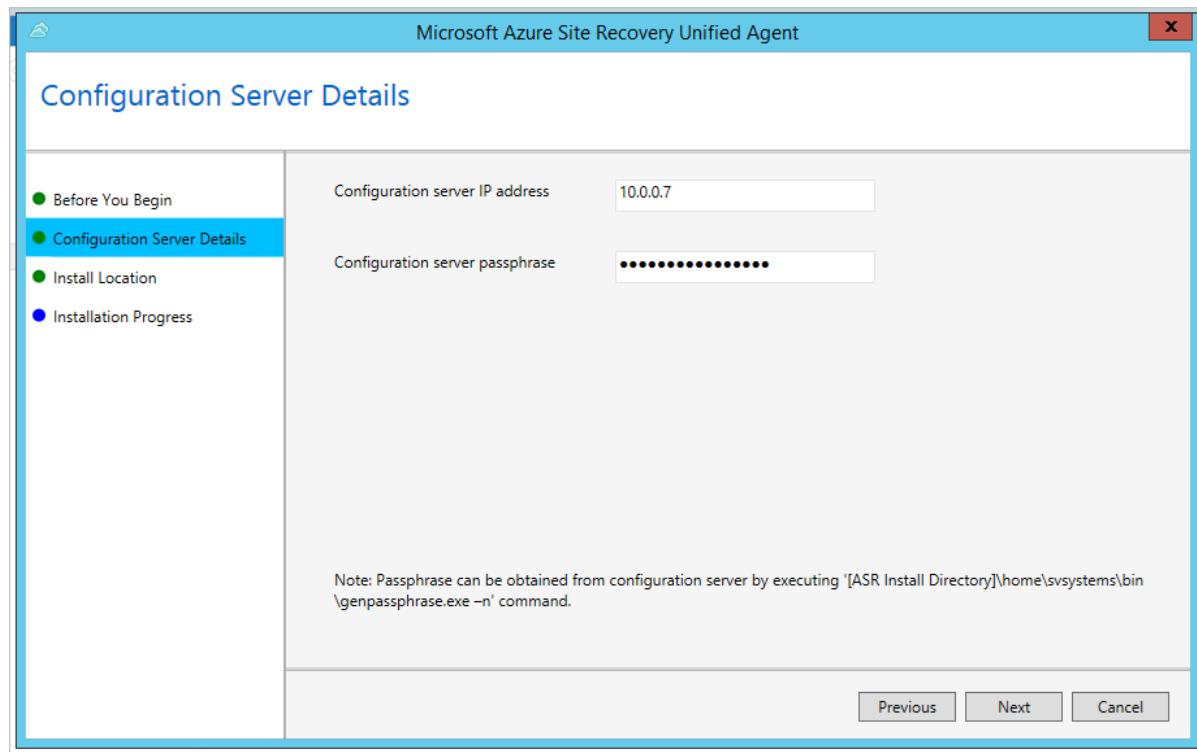
#### Step 6: Plan capacity

1. Use the [capacity planner](#) to accurately estimate network bandwidth, storage, and other requirements to meet your replication needs.
2. When you're done, select **Yes, I have done it** in **Have you completed capacity planning?**



## Step 7: Install the mobility service and enable replication

1. You can choose to [push installation](#) to your source VMs or to [manually install the mobility service](#) on your source VMs. You can find the requirement of pushing installation and the path of the manual installer in the provided link. If you're doing a manual installation, you might need to use an internal IP address to find the configuration server.



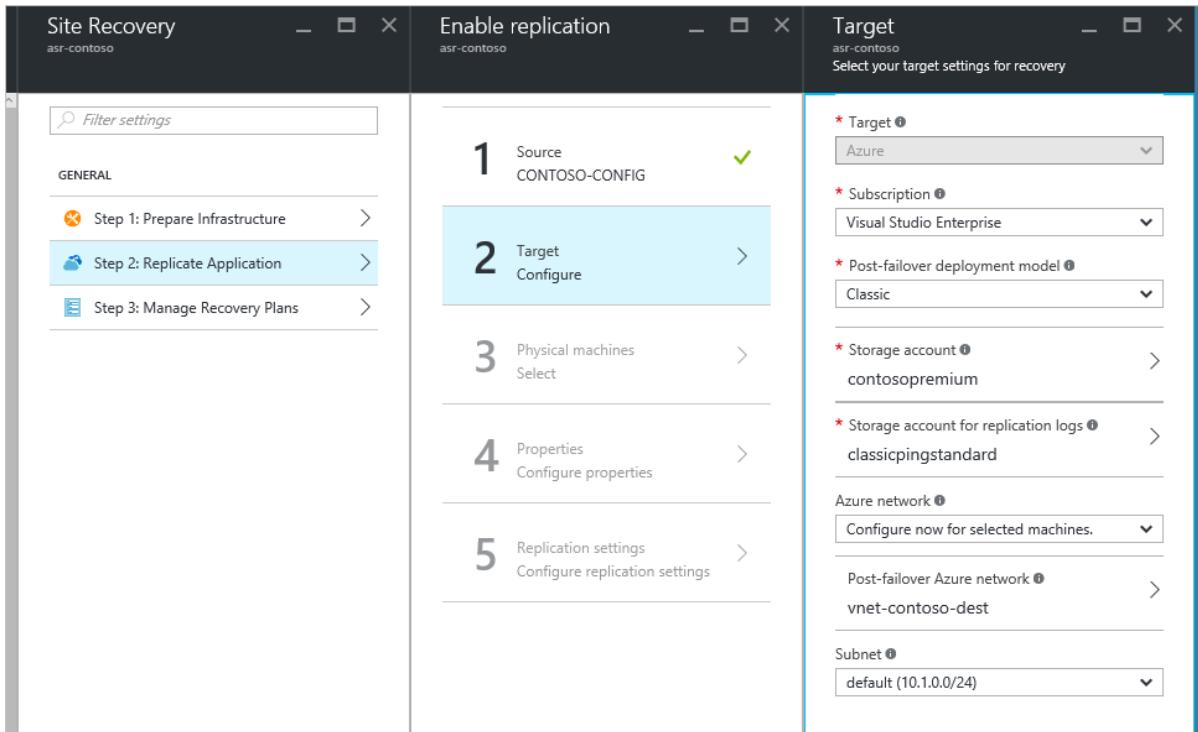
The failed-over VM will have two temporary disks: one from the primary VM and the other created during the provisioning of the VM in the recovery region. To exclude the temporary disk before replication, install the mobility service before you enable replication. To learn more about how to exclude the temporary disk, see [Exclude disks from replication](#).

2. Enable replication as follows:
  - a. Select **Replicate Application > Source**. After you've enabled replication for the first time, select **+Replicate** in the vault to enable replication for additional machines.

- b. In step 1, set up **Source** as your process server.
- c. In step 2, specify the post-failover deployment model, a premium storage account to migrate to, a standard storage account to save logs, and a virtual network to fail to.
- d. In step 3, add protected VMs by IP address. (You might need an internal IP address to find them.)
- e. In step 4, configure the properties by selecting the accounts that you set up previously on the process server.
- f. In step 5, choose the replication policy that you created previously in "Step 5: Set up replication settings."
- g. Select **OK**.

#### **NOTE**

When an Azure VM is deallocated and started again, there is no guarantee that it will get the same IP address. If the IP address of the configuration server/process server or the protected Azure VMs changes, the replication in this scenario might not work correctly.



When you design your Azure Storage environment, we recommend that you use separate storage accounts for each VM in an availability set. We recommend that you follow the best practice in the storage layer to [use multiple storage accounts for each availability set](#). Distributing VM disks to multiple storage accounts helps to improve storage availability and distributes the I/O across the Azure storage infrastructure.

If your VMs are in an availability set, instead of replicating disks of all VMs into one storage account, we highly recommend migrating multiple VMs multiple times. That way, the VMs in the same availability set do not share a single storage account. Use the **Enable Replication** pane to set up a destination storage account for each VM, one at a time.

You can choose a post-failover deployment model according to your need. If you choose Azure Resource Manager as your post-failover deployment model, you can fail over a VM (Resource Manager) to a VM (Resource Manager), or you can fail over a VM (classic) to a VM (Resource Manager).

#### **Step 8: Run a test failover**

To check whether your replication is complete, select your Site Recovery instance and then select **Settings > Replicated Items**. You will see the status and percentage of your replication process.

After initial replication is complete, run a test failover to validate your replication strategy. For detailed steps of a

test failover, see [Run a test failover in Site Recovery](#).

#### NOTE

Before you run any failover, make sure that your VMs and replication strategy meet the requirements. For more information about running a test failover, see [Test failover to Azure in Site Recovery](#).

You can see the status of your test failover in **Settings > Jobs > YOUR\_FAILOVER\_PLAN\_NAME**. In the pane, you can see a breakdown of the steps and success/failure results. If the test failover fails at any step, select the step to check the error message.

#### Step 9: Run a failover

After the test failover is completed, run a failover to migrate your disks to Premium Storage and replicate the VM instances. Follow the detailed steps in [Run a failover](#).

Be sure to select **Shut down VMs and synchronize the latest data**. This option specifies that Site Recovery should try to shut down the protected VMs and synchronize the data so that the latest version of the data will be failed over. If you don't select this option or the attempt doesn't succeed, the failover will be from the latest available recovery point for the VM.

Site Recovery will create a VM instance whose type is the same as or similar to a Premium Storage-capable VM. You can check the performance and price of various VM instances by going to [Windows Virtual Machines Pricing](#) or [Linux Virtual Machines Pricing](#).

### Post-migration steps

1. **Configure replicated VMs to the availability set if applicable.** Site Recovery does not support migrating VMs along with the availability set. Depending on the deployment of your replicated VM, do one of the following:
  - For a VM created through the classic deployment model: Add the VM to the availability set in the Azure portal. For detailed steps, go to [Add an existing virtual machine to an availability set](#).
  - For a VM created through the Resource Manager deployment model: Save your configuration of the VM and then delete and re-create the VMs in the availability set. To do so, use the script at [Set Azure Resource Manager VM Availability Set](#). Before you run this script, check its limitations and plan your downtime.
2. **Delete old VMs and disks.** Make sure that the Premium disks are consistent with source disks and that the new VMs perform the same function as the source VMs. Delete the VM and delete the disks from your source storage accounts in the Azure portal. If there's a problem in which the disk is not deleted even though you deleted the VM, see [Troubleshoot storage resource deletion errors](#).
3. **Clean the Azure Site Recovery infrastructure.** If Site Recovery is no longer needed, you can clean its infrastructure. Delete replicated items, the configuration server, and the recovery policy, and then delete the Azure Site Recovery vault.

### Troubleshooting

- [Monitor and troubleshoot protection for virtual machines and physical servers](#)
- [Microsoft Azure Site Recovery forum](#)

### Next steps

For specific scenarios for migrating virtual machines, see the following resources:

- [Migrate Azure Virtual Machines between Storage Accounts](#)
- [Upload a Linux virtual hard disk](#)
- [Migrating Virtual Machines from Amazon AWS to Microsoft Azure](#)

Also, see the following resources to learn more about Azure Storage and Azure Virtual Machines:

- [Azure Storage](#)
- [Azure Virtual Machines](#)
- [Select a disk type for IaaS VMs](#)

# Convert a Linux virtual machine from unmanaged disks to managed disks

12/10/2019 • 4 minutes to read • [Edit Online](#)

If you have existing Linux virtual machines (VMs) that use unmanaged disks, you can convert the VMs to use [Azure Managed Disks](#). This process converts both the OS disk and any attached data disks.

This article shows you how to convert VMs by using the Azure CLI. If you need to install or upgrade it, see [Install Azure CLI](#).

## Before you begin

- Review [the FAQ about migration to Managed Disks](#).
- The conversion requires a restart of the VM, so schedule the migration of your VMs during a pre-existing maintenance window.
- The conversion is not reversible.
- Be aware that any users with the [Virtual Machine Contributor](#) role will not be able to change the VM size (as they could pre-conversion). This is because VMs with managed disks require the user to have the Microsoft.Compute/disks/write permission on the OS disks.
- Be sure to test the conversion. Migrate a test virtual machine before you perform the migration in production.
- During the conversion, you deallocate the VM. The VM receives a new IP address when it is started after the conversion. If needed, you can [assign a static IP address](#) to the VM.
- Review the minimum version of the Azure VM agent required to support the conversion process. For information on how to check and update your agent version, see [Minimum version support for VM agents in Azure](#)
- The original VHDs and the storage account used by the VM before conversion are not deleted. They continue to incur charges. To avoid being billed for these artifacts, delete the original VHD blobs after you verify that the conversion is complete. If you need to find these unattached disks in order to delete them, see our article [Find and delete unattached Azure managed and unmanaged disks](#).

## Convert single-instance VMs

This section covers how to convert single-instance Azure VMs from unmanaged disks to managed disks. (If your VMs are in an availability set, see the next section.) You can use this process to convert the VMs from premium (SSD) unmanaged disks to premium managed disks, or from standard (HDD) unmanaged disks to standard managed disks.

1. Deallocate the VM by using `az vm deallocate`. The following example deallocates the VM named `myVM` in the resource group named `myResourceGroup` :

```
az vm deallocate --resource-group myResourceGroup --name myVM
```

2. Convert the VM to managed disks by using `az vm convert`. The following process converts the VM named

`myVM`, including the OS disk and any data disks:

```
az vm convert --resource-group myResourceGroup --name myVM
```

3. Start the VM after the conversion to managed disks by using `az vm start`. The following example starts the VM named `myVM` in the resource group named `myResourceGroup`.

```
az vm start --resource-group myResourceGroup --name myVM
```

## Convert VMs in an availability set

If the VMs that you want to convert to managed disks are in an availability set, you first need to convert the availability set to a managed availability set.

All VMs in the availability set must be deallocated before you convert the availability set. Plan to convert all VMs to managed disks after the availability set itself has been converted to a managed availability set. Then, start all the VMs and continue operating as normal.

1. List all VMs in an availability set by using `az vm availability-set list`. The following example lists all VMs in the availability set named `myAvailabilitySet` in the resource group named `myResourceGroup`:

```
az vm availability-set show \
 --resource-group myResourceGroup \
 --name myAvailabilitySet \
 --query [virtualMachines[*].id] \
 --output table
```

2. Deallocate all the VMs by using `az vm deallocate`. The following example deallocates the VM named `myVM` in the resource group named `myResourceGroup`:

```
az vm deallocate --resource-group myResourceGroup --name myVM
```

3. Convert the availability set by using `az vm availability-set convert`. The following example converts the availability set named `myAvailabilitySet` in the resource group named `myResourceGroup`:

```
az vm availability-set convert \
 --resource-group myResourceGroup \
 --name myAvailabilitySet
```

4. Convert all the VMs to managed disks by using `az vm convert`. The following process converts the VM named `myVM`, including the OS disk and any data disks:

```
az vm convert --resource-group myResourceGroup --name myVM
```

5. Start all the VMs after the conversion to managed disks by using `az vm start`. The following example starts the VM named `myVM` in the resource group named `myResourceGroup`:

```
az vm start --resource-group myResourceGroup --name myVM
```

## Convert using the Azure portal

You can also convert unmanaged disks to managed disks using the Azure portal.

1. Sign in to the [Azure portal](#).
2. Select the VM from the list of VMs in the portal.
3. In the blade for the VM, select **Disks** from the menu.
4. At the top of the **Disks** blade, select **Migrate to managed disks**.
5. If your VM is in an availability set, there will be a warning on the **Migrate to managed disks** blade that you need to convert the availability set first. The warning should have a link you can click to convert the availability set. Once the availability set is converted or if your VM is not in an availability set, click **Migrate** to start the process of migrating your disks to managed disks.

The VM will be stopped and restarted after migration is complete.

## Next steps

For more information about storage options, see [Azure Managed Disks overview](#).

# Convert Azure managed disks storage from Standard to Premium or Premium to Standard

12/10/2019 • 4 minutes to read • [Edit Online](#)

There are four disk types of Azure managed disks: Azure ultra SSDs (preview), premium SSD, standard SSD, and standard HDD. You can switch between the three GA disk types (premium SSD, standard SSD, and standard HDD) based on your performance needs. You are not yet able to switch from or to an ultra SSD, you must deploy a new one.

This functionality is not supported for unmanaged disks. But you can easily [convert an unmanaged disk to a managed disk](#) to be able to switch between disk types.

This article shows how to convert managed disks from Standard to Premium or Premium to Standard by using the Azure CLI. To install or upgrade the tool, see [Install Azure CLI](#).

## Before you begin

- Disk conversion requires a restart of the virtual machine (VM), so schedule the migration of your disk storage during a pre-existing maintenance window.
- For unmanaged disks, first [convert to managed disks](#) so you can switch between storage options.

## Switch all managed disks of a VM between Premium and Standard

This example shows how to convert all of a VM's disks from Standard to Premium storage or from Premium to Standard storage. To use Premium managed disks, your VM must use a [VM size](#) that supports Premium storage. This example also switches to a size that supports Premium storage.

```

#resource group that contains the virtual machine
rgName='yourResourceGroup'

#Name of the virtual machine
vmName='yourVM'

#Premium capable size
#Required only if converting from Standard to Premium
size='Standard_DS2_v2'

#Choose between Standard_LRS and Premium_LRS based on your scenario
sku='Premium_LRS'

#Deallocate the VM before changing the size of the VM
az vm deallocate --name $vmName --resource-group $rgName

#Change the VM size to a size that supports Premium storage
#Skip this step if converting storage from Premium to Standard
az vm resize --resource-group $rgName --name $vmName --size $size

#Update the SKU of all the data disks
az vm show -n $vmName -g $rgName --query storageProfile.dataDisks[*].managedDisk -o tsv \
| awk -v sku=$sku '{system("az disk update --sku \"sku\" --ids \"$1\"")}'

#Update the SKU of the OS disk
az vm show -n $vmName -g $rgName --query storageProfile.osDisk.managedDisk -o tsv \
| awk -v sku=$sku '{system("az disk update --sku \"sku\" --ids \"$1\"")}'

az vm start --name $vmName --resource-group $rgName

```

## Switch individual managed disks between Standard and Premium

For your dev/test workload, you might want to have a mix of Standard and Premium disks to reduce your costs. You can choose to upgrade only those disks that need better performance. This example shows how to convert a single VM disk from Standard to Premium storage or from Premium to Standard storage. To use Premium managed disks, your VM must use a [VM size](#) that supports Premium storage. This example also switches to a size that supports Premium storage.

```

#resource group that contains the managed disk
rgName='yourResourceGroup'

#Name of your managed disk
diskName='yourManagedDiskName'

#Premium capable size
#Required only if converting from Standard to Premium
size='Standard_DS2_v2'

#Choose between Standard_LRS and Premium_LRS based on your scenario
sku='Premium_LRS'

#Get the parent VM Id
vmId=$(az disk show --name $diskName --resource-group $rgName --query managedBy --output tsv)

#Deallocate the VM before changing the size of the VM
az vm deallocate --ids $vmId

#Change the VM size to a size that supports Premium storage
#Skip this step if converting storage from Premium to Standard
az vm resize --ids $vmId --size $size

Update the SKU
az disk update --sku $sku --name $diskName --resource-group $rgName

az vm start --ids $vmId

```

## Switch managed disks between Standard HDD and Standard SSD

This example shows how to convert a single VM disk from Standard HDD to Standard SSD or from Standard SSD to Standard HDD.

```

#resource group that contains the managed disk
rgName='yourResourceGroup'

#Name of your managed disk
diskName='yourManagedDiskName'

#Choose between Standard_LRS and StandardSSD_LRS based on your scenario
sku='StandardSSD_LRS'

#Get the parent VM ID
vmId=$(az disk show --name $diskName --resource-group $rgName --query managedBy --output tsv)

#Deallocate the VM before changing the disk type
az vm deallocate --ids $vmId

Update the SKU
az disk update --sku $sku --name $diskName --resource-group $rgName

az vm start --ids $vmId

```

## Switch managed disks between Standard and Premium in Azure portal

Follow these steps:

1. Sign in to the [Azure portal](#).
2. Select the VM from the list of **Virtual machines**.

3. If the VM isn't stopped, select **Stop** at the top of the VM **Overview** pane, and wait for the VM to stop.
4. In the pane for the VM, select **Disks** from the menu.
5. Select the disk that you want to convert.
6. Select **Configuration** from the menu.
7. Change the **Account type** from **Standard HDD** to **Premium SSD** or from **Premium SSD** to **Standard HDD**.
8. Select **Save**, and close the disk pane.

The update of the disk type is instantaneous. You can restart your VM after the conversion.

## Next steps

Make a read-only copy of a VM by using [snapshots](#).

# Move files to and from a Linux VM using SCP

11/13/2019 • 2 minutes to read • [Edit Online](#)

This article shows how to move files from your workstation up to an Azure Linux VM, or from an Azure Linux VM down to your workstation, using Secure Copy (SCP). Moving files between your workstation and a Linux VM, quickly and securely, is critical for managing your Azure infrastructure.

For this article, you need a Linux VM deployed in Azure using [SSH public and private key files](#). You also need an SCP client for your local computer. It is built on top of SSH and included in the default Bash shell of most Linux and Mac computers and some Windows shells.

## Quick commands

Copy a file up to the Linux VM

```
scp file azureuser@azurehost:directory/targetfile
```

Copy a file down from the Linux VM

```
scp azureuser@azurehost:directory/file targetfile
```

## Detailed walkthrough

As examples, we move an Azure configuration file up to a Linux VM and pull down a log file directory, both using SCP and SSH keys.

## SSH key pair authentication

SCP uses SSH for the transport layer. SSH handles the authentication on the destination host, and it moves the file in an encrypted tunnel provided by default with SSH. For SSH authentication, usernames and passwords can be used. However, SSH public and private key authentication are recommended as a security best practice. Once SSH has authenticated the connection, SCP then begins copying the file. Using a properly configured `~/.ssh/config` and SSH public and private keys, the SCP connection can be established by just using a server name (or IP address). If you only have one SSH key, SCP looks for it in the `~/.ssh/` directory, and uses it by default to log in to the VM.

For more information on configuring your `~/.ssh/config` and SSH public and private keys, see [Create SSH keys](#).

## SCP a file to a Linux VM

For the first example, we copy an Azure configuration file up to a Linux VM that is used to deploy automation. Because this file contains Azure API credentials, which include secrets, security is important. The encrypted tunnel provided by SSH protects the contents of the file.

The following command copies the local `.azure/config` file to an Azure VM with FQDN `myservereastus.cloudapp.azure.com`. The admin user name on the Azure VM is `azureuser`. The file is targeted to the `/home/azureuser/` directory. Substitute your own values in this command.

```
scp ~/.azure/config azureuser@myserver.eastus.cloudapp.com:/home/azureuser/config
```

## SCP a directory from a Linux VM

For this example, we copy a directory of log files from the Linux VM down to your workstation. A log file may or may not contain sensitive or secret data. However, using SCP ensures the contents of the log files are encrypted. Using SCP to transfer the files is the easiest way to get the log directory and files down to your workstation while also being secure.

The following command copies files in the `/home/azureuser/logs/` directory on the Azure VM to the local `/tmp` directory:

```
scp -r azureuser@myserver.eastus.cloudapp.com:/home/azureuser/logs/. /tmp/
```

The `-r` cli flag instructs SCP to recursively copy the files and directories from the point of the directory listed in the command. Also notice that the command-line syntax is similar to a `cp` copy command.

## Next steps

- [Manage users, SSH, and check or repair disks on Azure Linux VMs using the VMAccess Extension](#)

# Enable Write Accelerator

11/13/2019 • 8 minutes to read • [Edit Online](#)

Write Accelerator is a disk capability for M-Series Virtual Machines (VMs) on Premium Storage with Azure Managed Disks exclusively. As the name states, the purpose of the functionality is to improve the I/O latency of writes against Azure Premium Storage. Write Accelerator is ideally suited where log file updates are required to persist to disk in a highly performant manner for modern databases.

Write Accelerator is generally available for M-series VMs in the Public Cloud.

## Planning for using Write Accelerator

Write Accelerator should be used for the volumes that contain the transaction log or redo logs of a DBMS. It is not recommended to use Write Accelerator for the data volumes of a DBMS as the feature has been optimized to be used against log disks.

Write Accelerator only works in conjunction with [Azure managed disks](#).

### IMPORTANT

Enabling Write Accelerator for the operating system disk of the VM will reboot the VM.

To enable Write Accelerator to an existing Azure disk that is NOT part of a volume build out of multiple disks with Windows disk or volume managers, Windows Storage Spaces, Windows Scale-out file server (SOFS), Linux LVM, or MDADM, the workload accessing the Azure disk needs to be shut down. Database applications using the Azure disk MUST be shut down.

If you want to enable or disable Write Accelerator for an existing volume that is built out of multiple Azure Premium Storage disks and striped using Windows disk or volume managers, Windows Storage Spaces, Windows Scale-out file server (SOFS), Linux LVM or MDADM, all disks building the volume must be enabled or disabled for Write Accelerator in separate steps.

**Before enabling or disabling Write Accelerator in such a configuration, shut down the Azure VM.**

Enabling Write Accelerator for OS disks should not be necessary for SAP-related VM configurations.

### Restrictions when using Write Accelerator

When using Write Accelerator for an Azure disk/VHD, these restrictions apply:

- The Premium disk caching must be set to 'None' or 'Read Only'. All other caching modes are not supported.
- Snapshot are not currently supported for Write Accelerator-enabled disks. During backup, the Azure Backup service automatically excludes Write Accelerator-enabled disks attached to the VM.
- Only smaller I/O sizes (<=512 KiB) are taking the accelerated path. In workload situations where data is getting bulk loaded or where the transaction log buffers of the different DBMS are filled to a larger degree before getting persisted to the storage, chances are that the I/O written to disk is not taking the accelerated path.

There are limits of Azure Premium Storage VHDs per VM that can be supported by Write Accelerator. The current limits are:

| VM SKU              | NUMBER OF WRITE ACCELERATOR DISKS | WRITE ACCELERATOR DISK IOPS PER VM |
|---------------------|-----------------------------------|------------------------------------|
| M416ms_v2, M416s_v2 | 16                                | 20000                              |
| M208ms_v2, M208s_v2 | 8                                 | 10000                              |

| VM SKU                    | NUMBER OF WRITE ACCELERATOR DISKS | WRITE ACCELERATOR DISK IOPS PER VM |
|---------------------------|-----------------------------------|------------------------------------|
| M128ms, M128s             | 16                                | 20000                              |
| M64ms, M64ls, M64s        | 8                                 | 10000                              |
| M32ms, M32ls, M32ts, M32s | 4                                 | 5000                               |
| M16ms, M16s               | 2                                 | 2500                               |
| M8ms, M8s                 | 1                                 | 1250                               |

The IOPS limits are per VM and *not* per disk. All Write Accelerator disks share the same IOPS limit per VM.

## Enabling Write Accelerator on a specific disk

The next few sections will describe how Write Accelerator can be enabled on Azure Premium Storage VHDs.

### Prerequisites

The following prerequisites apply to the usage of Write Accelerator at this point in time:

- The disks you want to apply Azure Write Accelerator against need to be [Azure managed disks](#) on Premium Storage.
- You must be using an M-series VM

## Enabling Azure Write Accelerator using Azure PowerShell

The Azure Power Shell module from version 5.5.0 include the changes to the relevant cmdlets to enable or disable Write Accelerator for specific Azure Premium Storage disks. In order to enable or deploy disks supported by Write Accelerator, the following Power Shell commands got changed, and extended to accept a parameter for Write Accelerator.

A new switch parameter, **-WriteAccelerator** has been added to the following cmdlets:

- [Set-AzVMOsDisk](#)
- [Add-AzVMDataDisk](#)
- [Set-AzVMDataDisk](#)
- [Add-AzVmssDataDisk](#)

Not giving the parameter sets the property to false and will deploy disks that have no support by Write Accelerator.

A new switch parameter, **-OsDiskWriteAccelerator** was added to the following cmdlets:

- [Set-AzVmssStorageProfile](#)

Not specifying the parameter sets the property to false by default, returning disks that don't leverage Write Accelerator.

A new optional Boolean (non-nullable) parameter, **-OsDiskWriteAccelerator** was added to the following cmdlets:

- [Update-AzVM](#)
- [Update-AzVmss](#)

Specify either \$true or \$false to control support of Azure Write Accelerator with the disks.

Examples of commands could look like:

```

New-AzVMConfig | Set-AzVMOsDisk | Add-AzVMDataDisk -Name "datadisk1" | Add-AzVMDataDisk -Name "logdisk1" -WriteAccelerator | New-AzVM

Get-AzVM | Update-AzVM -OsDiskWriteAccelerator $true

New-AzVmssConfig | Set-AzVmssStorageProfile -OsDiskWriteAccelerator | Add-AzVmssDataDisk -Name "datadisk1" -WriteAccelerator:$false | Add-AzVmssDataDisk -Name "logdisk1" -WriteAccelerator | New-AzVmss

Get-AzVmss | Update-AzVmss -OsDiskWriteAccelerator:$false

```

Two main scenarios can be scripted as shown in the following sections.

### **Adding a new disk supported by Write Accelerator using PowerShell**

You can use this script to add a new disk to your VM. The disk created with this script uses Write Accelerator.

Replace `myVM`, `myWAVMs`, `log001`, size of the disk, and LunID of the disk with values appropriate for your specific deployment.

```

Specify your VM Name
$vmName="myVM"
#Specify your Resource Group
$rgName = "myWAVMs"
#data disk name
$datadiskname = "log001"
#LUN Id
$lunid=8
#size
$size=1023
#Pulls the VM info for later
$vm=Get-AzVM -ResourceGroupName $rgname -Name $vmname
#add a new VM data disk
Add-AzVMDataDisk -CreateOption empty -DiskSizeInGB $size -Name $vmname-$datadiskname -VM $vm -Caching None -WriteAccelerator:$true -lun $lunid
#Updates the VM with the disk config - does not require a reboot
Update-AzVM -ResourceGroupName $rgname -VM $vm

```

### **Enabling Write Accelerator on an existing Azure disk using PowerShell**

You can use this script to enable Write Accelerator on an existing disk. Replace `myVM`, `myWAVMs`, and `test-log001` with values appropriate for your specific deployment. The script adds Write Accelerator to an existing disk where the value for `$newstatus` is set to '\$true'. Using the value '\$false' will disable Write Accelerator on a given disk.

```

#Specify your VM Name
$vmName="myVM"
#Specify your Resource Group
$rgName = "myWAVMs"
#data disk name
$datadiskname = "test-log001"
#new Write Accelerator status ($true for enabled, $false for disabled)
$newstatus = $true
#Pulls the VM info for later
$vm=Get-AzVM -ResourceGroupName $rgname -Name $vmname
#add a new VM data disk
Set-AzVMDataDisk -VM $vm -Name $datadiskname -Caching None -WriteAccelerator:$newstatus
#Updates the VM with the disk config - does not require a reboot
Update-AzVM -ResourceGroupName $rgname -VM $vm

```

## NOTE

Executing the script above will detach the disk specified, enable Write Accelerator against the disk, and then attach the disk again

## Enabling Write Accelerator using the Azure portal

You can enable Write Accelerator via the portal where you specify your disk caching settings:

| NAME                                             | SIZE    | STORAGE ACCOUNT TYPE | ENCRYPTION  | HOST CACHING |
|--------------------------------------------------|---------|----------------------|-------------|--------------|
| myWAVM_OsDisk_1_f8678795084e451c8bfdb83786e03e7c | 127 GiB | Premium_LRS          | Not enabled | Read/write   |

| LUN | NAME    | SIZE     | STORAGE ACCOUNT TYPE | ENCRYPTION  | HOST CACHING                  |
|-----|---------|----------|----------------------|-------------|-------------------------------|
| 0   | WADisk1 | 1023 GiB | Premium_LRS          | Not enabled | Read-only + Write Accelerator |
| 1   | WADisk2 | 1023 GiB | Premium_LRS          | Not enabled | None + Write Accelerator      |

## Enabling Write Accelerator using the Azure CLI

You can use the [Azure CLI](#) to enable Write Accelerator.

To enable Write Accelerator on an existing disk, use [az vm update](#), you may use the following examples if you replace the diskName, VMName, and ResourceGroup with your own values:

```
az vm update -g group1 -n vm1 -write-accelerator 1=true
```

To attach a disk with Write Accelerator enabled use [az vm disk attach](#), you may use the following example if you substitute in your own values: `az vm disk attach -g group1 -vm-name vm1 -disk d1 --enable-write-accelerator`

To disable Write Accelerator, use [az vm update](#), setting the properties to false:

```
az vm update -g group1 -n vm1 -write-accelerator 0=false 1=false
```

## Enabling Write Accelerator using Rest APIs

To deploy through Azure Rest API, you need to install the Azure armclient.

### Install armclient

To run armclient, you need to install it through Chocolatey. You can install it through cmd.exe or powershell. Use elevated rights for these commands ("Run as Administrator").

Using cmd.exe, run the following command:

```
@"%SystemRoot%\System32\WindowsPowerShell\v1.0\powershell.exe" -NoProfile -InputFormat None -ExecutionPolicy Bypass -Command "iex ((New-Object System.Net.WebClient).DownloadString('https://chocolatey.org/install.ps1'))"
& SET "PATH=%PATH%;%ALLUSERSPROFILE%\chocolatey\bin"
```

Using Power Shell, run the following command:

```
Set-ExecutionPolicy Bypass -Scope Process -Force; iex ((New-Object System.Net.WebClient).DownloadString('https://chocolatey.org/install.ps1'))
```

Now you can install the armclient by using the following command in either cmd.exe or PowerShell

```
choco install armclient
```

## Getting your current VM configuration

To change the attributes of your disk configuration, you first need to get the current configuration in a JSON file.

You can get the current configuration by executing the following command:

```
armclient GET /subscriptions/<<subscription-ID>>/resourceGroups/<<ResourceGroup>>/providers/Microsoft.Compute/virtualMachines/<<virtualmachinename>>?api-version=2017-12-01 <<filename.json>>
```

Replace the terms within '<< >>' with your data, including the file name the JSON file should have.

The output could look like:

```
{
 "properties": {
 "vmId": "2444c93e-f8bb-4a20-af2d-1658d9dbbbc",
 "hardwareProfile": {
 "vmSize": "Standard_M64s"
 },
 "storageProfile": {
 "imageReference": {
 "publisher": "SUSE",
 "offer": "SLES-SAP",
 "sku": "12-SP3",
 "version": "latest"
 },
 "osDisk": {
 "osType": "Linux",
 "name": "mylittlesap_OsDisk_1_754a1b8bb390468e9b4c429b81cc5f5a",
 "createOption": "FromImage",
 "caching": "ReadWrite",
 "managedDisk": {
 "storageAccountType": "Premium_LRS",
 "id": "/subscriptions/XXXXXXXXXXXXXXXXXXXXXXXXXXXX/resourceGroups/mylittlesap/providers/Microsoft.Compute/disks/mylittlesap_OsDisk_1_754a1b8bb390468e9b4c429b81cc5f5a"
 },
 "diskSizeGB": 30
 },
 "dataDisks": [
 {
 "lun": 0,
 "name": "data1",
 "createOption": "Attach",
 "caching": "None",
 "managedDisk": {
 "storageAccountType": "Premium_LRS",
 "id": "/subscriptions/XXXXXXXXXXXXXXXXXXXXXXXXXXXX/resourceGroups/mylittlesap/providers/Microsoft.Compute/disks/data1"
 },
 "diskSizeGB": 1023
 },
 {
 "lun": 1,
 "name": "log1",
 "createOption": "Attach",
 "caching": "None",
 "managedDisk": {
 "storageAccountType": "Premium_LRS",
 "id": "/subscriptions/XXXXXXXXXXXXXXXXXXXXXXXXXXXX/resourceGroups/mylittlesap/providers/Microsoft.Compute/disks/data2"
 }
 }
]
 }
 }
}
```

```

 },
 "diskSizeGB": 1023
 }
]
},
"osProfile": {
 "computerName": "mylittlesapVM",
 "adminUsername": "pl",
 "linuxConfiguration": {
 "disablePasswordAuthentication": false
 },
 "secrets": []
},
"networkProfile": {
 "networkInterfaces": [
 {
 "id": "/subscriptions/XXXXXXXXXXXXXXXXXXXX/resourceGroups/mylittlesap/providers/Microsoft.Network/networkInterfaces/mylittlesap518"
 }
]
},
"diagnosticsProfile": {
 "bootDiagnostics": {
 "enabled": true,
 "storageUri": "https://mylittlesapdiag895.blob.core.windows.net/"
 }
},
"provisioningState": "Succeeded"
},
"type": "Microsoft.Compute/virtualMachines",
"location": "westeurope",
"id": "/subscriptions/XXXXXXXXXXXXXXXXXXXX/resourceGroups/mylittlesap/providers/Microsoft.Compute/virtualMachines/mylittlesapVM",
"name": "mylittlesapVM"

```

Next, update the JSON file and to enable Write Accelerator on the disk called 'log1'. This can be accomplished by adding this attribute into the JSON file after the cache entry of the disk.

```

{
 "lun": 1,
 "name": "log1",
 "createOption": "Attach",
 "caching": "None",
 "writeAcceleratorEnabled": true,
 "managedDisk": {
 "storageAccountType": "Premium_LRS",
 "id": "/subscriptions/XXXXXXXXXXXXXXXXXXXX/resourceGroups/mylittlesap/providers/Microsoft.Compute/disks/data2"
 },
 "diskSizeGB": 1023
}

```

Then update the existing deployment with this command:

```
armclient PUT /subscriptions/<<subscription-ID</>>/resourceGroups/<<ResourceGroup>>/providers/Microsoft.Compute/virtualMachines/<<virtualmachinename>>?api-version=2017-12-01 @<<filename.json>>
```

The output should look like the one below. You can see that Write Accelerator enabled for one disk.

```
{
 "properties": {
 "osProfile": {
 "computerName": "mylittlesapVM",
 "adminUsername": "pl",
 "linuxConfiguration": {
 "disablePasswordAuthentication": false
 },
 "secrets": []
 },
 "networkProfile": {
 "networkInterfaces": [
 {
 "id": "/subscriptions/XXXXXXXXXXXXXXXXXXXX/resourceGroups/mylittlesap/providers/Microsoft.Network/networkInterfaces/mylittlesap518"
 }
]
 },
 "diagnosticsProfile": {
 "bootDiagnostics": {
 "enabled": true,
 "storageUri": "https://mylittlesapdiag895.blob.core.windows.net/"
 }
 },
 "provisioningState": "Succeeded"
 },
 "type": "Microsoft.Compute/virtualMachines",
 "location": "westeurope",
 "id": "/subscriptions/XXXXXXXXXXXXXXXXXXXX/resourceGroups/mylittlesap/providers/Microsoft.Compute/virtualMachines/mylittlesapVM",
 "name": "mylittlesapVM"
}
```

```
 "vmSize": "Standard_M64s"
 },
 "storageProfile": {
 "imageReference": {
 "publisher": "SUSE",
 "offer": "SLES-SAP",
 "sku": "12-SP3",
 "version": "latest"
 },
 "osDisk": {
 "osType": "Linux",
 "name": "mylittlesap_OsDisk_1_754a1b8bb390468e9b4c429b81cc5f5a",
 "createOption": "FromImage",
 "caching": "ReadWrite",
 "managedDisk": {
 "storageAccountType": "Premium_LRS",
 "id": "/subscriptions/XXXXXXXXXXXXXXXXXXXXXX/resourceGroups/mylittlesap/providers/Microsoft.Compute/disks/mylittlesap_OsDisk_1_754a1b8bb390468e9b4c429b81cc5f5a"
 },
 "diskSizeGB": 30
 },
 "dataDisks": [
 {
 "lun": 0,
 "name": "data1",
 "createOption": "Attach",
 "caching": "None",
 "managedDisk": {
 "storageAccountType": "Premium_LRS",
 "id": "/subscriptions/XXXXXXXXXXXXXXXXXXXXXX/resourceGroups/mylittlesap/providers/Microsoft.Compute/disks/data1"
 },
 "diskSizeGB": 1023
 },
 {
 "lun": 1,
 "name": "log1",
 "createOption": "Attach",
 "caching": "None",
 "writeAcceleratorEnabled": true,
 "managedDisk": {
 "storageAccountType": "Premium_LRS",
 "id": "/subscriptions/XXXXXXXXXXXXXXXXXXXXXX/resourceGroups/mylittlesap/providers/Microsoft.Compute/disks/data2"
 },
 "diskSizeGB": 1023
 }
]
 },
 "osProfile": {
 "computerName": "mylittlesapVM",
 "adminUsername": "pl",
 "linuxConfiguration": {
 "disablePasswordAuthentication": false
 },
 "secrets": []
 },
 "networkProfile": {
 "networkInterfaces": [
 {
 "id": "/subscriptions/XXXXXXXXXXXXXXXXXXXXXX/resourceGroups/mylittlesap/providers/Microsoft.Network/networkInterfaces/mylittlesap518"
 }
]
 }
}
```

```
],
 },
 "diagnosticsProfile": {
 "bootDiagnostics": {
 "enabled": true,
 "storageUri": "https://mylittlesapdiag895.blob.core.windows.net/"
 }
 },
 "provisioningState": "Succeeded"
},
"type": "Microsoft.Compute/virtualMachines",
"location": "westeurope",
"id":
"/subscriptions/XXXXXXXXXXXXXXXXXXXXXX/resourceGroups/mylittlesap/providers/Microsoft.Compute/vir
tualMachines/mylittlesapVM",
"name": "mylittlesapVM"
```

Once you've made this change, the drive should be supported by Write Accelerator.

# Using Azure ultra disks

11/15/2019 • 8 minutes to read • [Edit Online](#)

Azure ultra disks offer high throughput, high IOPS, and consistent low latency disk storage for Azure IaaS virtual machines (VMs). This new offering provides top of the line performance at the same availability levels as our existing disks offerings. One major benefit of ultra disks is the ability to dynamically change the performance of the SSD along with your workloads without the need to restart your VMs. Ultra disks are suited for data-intensive workloads such as SAP HANA, top tier databases, and transaction-heavy workloads.

## GA scope and limitations

For now, ultra disks have additional limitations, they are as follows:

- Are supported in the following regions, with a varying number of availability zones per region:
  - East US 2
  - East US
  - West US 2
  - SouthEast Asia
  - North Europe
  - West Europe
  - UK South
- Can only be used with availability zones (availability sets and single VM deployments outside of zones will not have the ability to attach an ultra disk)
- Are only supported on the following VM series:
  - [ESv3](#)
  - [DSv3](#)
  - FSv2
  - [M](#)
  - [Mv2](#)
- Not every VM size is available in every supported region with ultra disks
- Are only available as data disks and only support 4k physical sector size. Due to the 4K native sector size of Ultra Disk, there are some applications that won't be compatible with ultra disks. One example would be Oracle Database, which requires release 12.2 or later in order to support ultra disks.
- Can only be created as empty disks
- Do not yet support disk snapshots, VM images, availability sets, and Azure disk encryption
- Do not yet support integration with Azure Backup or Azure Site Recovery
- The current maximum limit for IOPS on GA VMs is 80,000.
- If you would like to participate in a limited preview of a VM that can accomplish 160,000 IOPS with ultra disks, please email [UltraDiskFeedback@microsoft.com](mailto:UltraDiskFeedback@microsoft.com)

## Determine VM size and region availability

To leverage ultra disks, you need to determine which availability zone you are in. Not every region supports every VM size with ultra disks. To determine if your region, zone, and VM size support ultra disks, run either of the following commands, make sure to replace the **region**, **vmSize**, and **subscription** values first:

CLI:

```

$subscription = "<yourSubID>"
example value is southeastasia
$region = "<yourLocation>"
example value is Standard_E64s_v3
$vmSize = "<yourVMSize>

az vm list-skus --resource-type virtualMachines --location $region --query "[?
name=='$vmSize'].locationInfo[0].zoneDetails[0].Name" --subscription $subscription

```

PowerShell:

```

$region = "southeastasia"
$vmSize = "Standard_E64s_v3"
(Get-AzComputeResourceSku | where {$_.Locations.Contains($region) -and ($_.Name -eq $vmSize) -and
$_.LocationInfo[0].ZoneDetails.Count -gt 0})[0].LocationInfo[0].ZoneDetails

```

The response will be similar to the form below, where X is the zone to use for deploying in your chosen region. X could be either 1, 2, or 3.

Preserve the **Zones** value, it represents your availability zone and you will need it in order to deploy an Ultra disk.

| RESOURCETYPE | NAME         | LOCATION | ZONES | RESTRICTION | CAPABILITY | VALUE |
|--------------|--------------|----------|-------|-------------|------------|-------|
| disks        | UltraSSD_LRS | eastus2  | X     |             |            |       |

#### NOTE

If there was no response from the command, then the selected VM size is not supported with ultra disks in the selected region.

Now that you know which zone to deploy to, follow the deployment steps in this article to either deploy a VM with an ultra disk attached or attach an ultra disk to an existing VM.

## Deploy an ultra disk using Azure Resource Manager

First, determine the VM size to deploy. For a list of supported VM sizes, see [GA scope and limitations](#) section.

If you would like to create a VM with multiple ultra disks, refer to the sample [Create a VM with multiple ultra disks](#).

If you intend to use your own template, make sure that **apiVersion** for `Microsoft.Compute/virtualMachines` and `Microsoft.Compute/Disks` is set as `2018-06-01` (or later).

Set the disk sku to **UltraSSD\_LRS**, then set the disk capacity, IOPS, availability zone, and throughput in MBps to create an ultra disk.

Once the VM is provisioned, you can partition and format the data disks and configure them for your workloads.

## Deploy an ultra disk using the Azure portal

This section covers deploying a virtual machine equipped with an ultra disk as a data disk. It assumes you have familiarity with deploying a virtual machine, if you do not, see our [Quickstart: Create a Windows virtual machine in the Azure portal](#).

- Sign in to the [Azure portal](#) and navigate to deploy a virtual machine (VM).
- Make sure to choose a [supported VM size and region](#).
- Select **Availability zone** in **Availability options**.

- Fill in the remaining entries with selections of your choice.
- Select **Disks**.

The screenshot shows the 'Create a virtual machine' blade in the Microsoft Azure portal. The 'Disks' tab is selected. In the 'Instance details' section, several fields are highlighted with a red box: 'Virtual machine name' (myVMName), 'Region' (US West US 2), 'Availability options' (Availability zone), 'Availability zone' (1), 'Image' (Ubuntu Server 18.04 LTS), and 'Size' (Standard D2s v3). The 'Enable Ultra Disk compatibility' checkbox is also highlighted with a red box.

- On the Disks blade, select **Yes** for **Enable Ultra Disk compatibility**.
- Select **Create and attach a new disk** to attach an ultra disk now.

## Create a virtual machine

**Basics** **Disks** **Networking** **Management** **Advanced** **Tags** **Review + create**

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

**Disk options**

**OS disk type \*** Premium SSD

**Enable Ultra Disk compatibility**  Yes  No

**Data disks**

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

| LUN | Name | Size (GiB) | Disk type | Host caching |
|-----|------|------------|-----------|--------------|
|     |      |            |           |              |

[Create and attach a new disk](#) [Attach an existing disk](#)

- On the **Create a new disk** blade, enter a name, then select **Change size**.
- Change the **Account type** to **Ultra Disk**.
- Change the values of **Custom disk size (GiB)**, **Disk IOPS**, and **Disk throughput** to ones of your choice.
- Select **OK** in both blades.
- Continue with the VM deployment, it will be the same as you would deploy any other VM.

## Attach an ultra disk using the Azure portal

Alternatively, if your existing VM is in a region/availability zone that is capable of using ultra disks, you can make use of ultra disks without having to create a new VM. By enabling ultra disks on your existing VM, then attaching them as data disks.

- Navigate to your VM and select **Disks**.
- Select **Edit**.

- Select **Yes** for **Enable Ultra Disk compatibility**.

- Select **Save**.
- Select **Add data disk** then in the dropdown for **Name** select **Create disk**.

- Fill in a name for your new disk, then select **Change size**.
- Change the **Account type** to **Ultra Disk**.
- Change the values of **Custom disk size (GiB)**, **Disk IOPS**, and **Disk throughput** to ones of your choice.

- Select **OK** then select **Create**.

Create managed disk

Create a new disk to store applications and data on your VM. Disk pricing varies based on storage type, and number of transactions.

Disk name \*

Resource group \*  [Create new](#)

Location

Availability zone

Source type

Size \*   
Ultra Disk, 2048 IOPS, 8 MB/s [Change size](#)

Account type

| Max size  | Disk tier | Max IOPS | Max throughput |
|-----------|-----------|----------|----------------|
| 65536 GiB | U         | 160000   | 2000           |

Create a custom size  
Enter the size of the disk you would like to create. You will be charged the same rate for your provisioned disk, regardless of how much of the disk space is being used For example, a 200 GiB disk is provisioned on a 256 GiB disk, so you would be billed for the 256 GiB provisioned.

Custom disk size (GiB) \*

Disk IOPS \*

Disk throughput (MB/s) \*

- After you are returned to your disk's blade, select **Save**.

[Save](#) [Discard](#) [Refresh](#) [Encryption](#) [Swap OS Disk](#)

Managed disks created since June 10, 2017 are encrypted at rest with Storage Service Encryption (SSE). You may also want to enable Azure Disk Encryption. [Edit](#)

Disk settings

Enable Ultra Disk compatibility  Yes  No

OS disk

| Name                                                      | Size   | Storage account type | Encryption  | Host caching |
|-----------------------------------------------------------|--------|----------------------|-------------|--------------|
| newfinalbuttonittest_OsDisk_1_b2fd08ca503c41acb6a040ac... | 30 GiB | Premium SSD          | Not enabled | Read/write   |

Data disks

| LUN | Name      | Size     | Storage account type | Encryption  | Host caching |
|-----|-----------|----------|----------------------|-------------|--------------|
| 0   | new-ultra | 1024 GiB | Ultra Disk           | Not enabled | None         |
| 1   | ultra-new | 1024 GiB | Ultra Disk           | Not enabled | None         |

[+ Add data disk](#)

### Adjust the performance of an ultra disk using the Azure portal

Ultra disks offer a unique capability that allows you to adjust their performance. You can make these adjustments from the Azure portal, on the disks themselves.

- Navigate to your VM and select **Disks**.
- Select the ultra disk you'd like to modify the performance of.

Search (Ctrl+ /) << Edit Refresh Encryption

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

**Settings**

Networking  
Disks **(highlighted)**  
Size  
Security  
Extensions  
Continuous delivery (Preview)  
Availability + scaling

Managed disks created since June 10, 2023

The virtual machine must be stopped/

Disk settings

Enable Ultra Disk compatibility i  
 Yes  No

OS disk

Name: ultravm\_OsDisk\_1\_12f247eec85d4ee1a7

Data disks

| LUN | Name                                  |
|-----|---------------------------------------|
| 0   | <b>new-ultra</b> <b>(highlighted)</b> |
| 1   | ultra-new                             |

- Select **Configuration** and then make your modifications.
- Select **Save**.

Search (Ctrl+ /) << Save Discard

Overview  
Activity log  
Access control (IAM)  
Tags

**Settings**

Configuration **(highlighted)**  
Disk Export  
Properties  
Locks  
Export template

Account type i  
Ultra Disk

Changing account type for Ultra Disks is not currently supported.

|                          |      |
|--------------------------|------|
| Size (GiB) *             | 1050 |
| Disk IOPS *              | 2548 |
| Disk throughput (MB/s) * | 10   |

Deploy an ultra disk using CLI

First, determine the VM size to deploy. See the [GA scope and limitations](#) section for a list of supported VM sizes.

You must create a VM that is capable of using ultra disks, in order to attach an ultra disk.

Replace or set the **\$vmname**, **\$rgname**, **\$diskname**, **\$location**, **\$password**, **\$user** variables with your own values. Set **\$zone** to the value of your availability zone that you got from the [start of this article](#). Then run the following CLI command to create an ultra enabled VM:

```
az vm create --subscription $subscription -n $vmname -g $rgname --image Win2016Datacenter --ultra-ssd-enabled true --zone $zone --authentication-type password --admin-password $password --admin-username $user --size Standard_D4s_v3 --location $location
```

## Create an ultra disk using CLI

Now that you have a VM that is capable of attaching ultra disks, you can create and attach an ultra disk to it.

```
$location="eastus2"
$subscription="xxx"
$rgname="ultraRG"
$diskname="ssd1"
$vmname="ultravm1"
$zone=123

#create an ultra disk
az disk create `
--subscription $subscription `
-n $diskname `
-g $rgname `
--size-gb 4 `
--location $location `
--zone $zone `
--sku UltraSSD_LRS `
--disk-iops-read-write 1000 `
--disk-mbps-read-write 50
```

## Attach an ultra disk to a VM using CLI

Alternatively, if your existing VM is in a region/availability zone that is capable of using ultra disks, you can make use of ultra disks without having to create a new VM.

```
$rgName = "<yourResourceGroupName>"
$vmName = "<yourVMName>"
$diskName = "<yourDiskName>"
$subscriptionId = "<yourSubscriptionID>"

az vm disk attach -g $rgName --vm-name $vmName --disk $diskName --subscription $subscriptionId
```

## Adjust the performance of an ultra disk using CLI

Ultra disks offer a unique capability that allows you to adjust their performance, the following command depicts how to use this feature:

```
az disk update `
--subscription $subscription `
--resource-group $rgname `
--name $diskName `
--set diskIopsReadWrite=80000 `
--set diskMbpsReadWrite=800
```

# Deploy an ultra disk using PowerShell

First, determine the VM size to deploy. See the [GA scope and limitations](#) section for a list of supported VM sizes.

To use ultra disks, you must create a VM that is capable of using ultra disks. Replace or set the **\$resourcegroup** and **\$vmName** variables with your own values. Set **\$zone** to the value of your availability zone that you got from the [start of this article](#). Then run the following **New-AzVm** command to create an ultra enabled VM:

```
New-AzVm `
 -ResourceGroupName $resourcegroup `
 -Name $vmName `
 -Location "eastus2" `
 -Image "Win2016Datacenter" `
 -EnableUltraSSD `
 -size "Standard_D4s_v3" `
 -zone $zone
```

## Create an ultra disk using PowerShell

Now that you have a VM that is capable of using ultra disks, you can create and attach an ultra disk to it:

```
$diskconfig = New-AzDiskConfig `
 -Location 'EastUS2' `
 -DiskSizeGB 8 `
 -DiskIOPSReadWrite 1000 `
 -DiskMBpsReadWrite 100 `
 -AccountType UltraSSD_LRS `
 -CreateOption Empty `
 -zone $zone;

New-AzDisk `
 -ResourceGroupName $resourceGroup `
 -DiskName 'Disk02' `
 -Disk $diskconfig;
```

## Attach an ultra disk to a VM using PowerShell

Alternatively, if your existing VM is in a region/availability zone that is capable of using ultra disks, you can make use of ultra disks without having to create a new VM.

```
add disk to VM
$subscription = "<yourSubscriptionID>"
$resourceGroup = "<yourResourceGroup>"
$vmName = "<yourVMName>"
$diskName = "<yourDiskName>"
$lun = 1
Login-AzureRMAccount -SubscriptionId $subscription
$vm = Get-AzVM -ResourceGroupName $resourceGroup -Name $vmName
$disk = Get-AzDisk -ResourceGroupName $resourceGroup -Name $diskName
$vm = Add-AzVMDataDisk -VM $vm -Name $diskName -CreateOption Attach -ManagedDiskId $disk.Id -Lun $lun
Update-AzVM -VM $vm -ResourceGroupName $resourceGroup
```

## Adjust the performance of an ultra disk using PowerShell

Ultra disks have a unique capability that allows you to adjust their performance, the following command is an example that adjusts the performance without having to detach the disk:

```
$diskupdateconfig = New-AzDiskUpdateConfig -DiskMBpsReadWrite 2000
Update-AzDisk -ResourceGroupName $resourceGroup -DiskName $diskName -DiskUpdate $diskupdateconfig
```

## Next steps

If you would like to try the new disk type [request access with this survey](#).

# Benchmarking a disk

1/7/2020 • 8 minutes to read • [Edit Online](#)

Benchmarking is the process of simulating different workloads on your application and measuring the application performance for each workload. Using the steps described in the [designing for high performance article](#). By running benchmarking tools on the VMs hosting the application, you can determine the performance levels that your application can achieve with Premium Storage. In this article, we provide you examples of benchmarking a Standard DS14 VM provisioned with Azure Premium Storage disks.

We have used common benchmarking tools lometer and FIO, for Windows and Linux respectively. These tools spawn multiple threads simulating a production like workload, and measure the system performance. Using the tools you can also configure parameters like block size and queue depth, which you normally cannot change for an application. This gives you more flexibility to drive the maximum performance on a high scale VM provisioned with premium disks for different types of application workloads. To learn more about each benchmarking tool visit [lometer](#) and [FIO](#).

To follow the examples below, create a Standard DS14 VM and attach 11 Premium Storage disks to the VM. Of the 11 disks, configure 10 disks with host caching as "None" and stripe them into a volume called NoCacheWrites. Configure host caching as "ReadOnly" on the remaining disk and create a volume called CacheReads with this disk. Using this setup, you are able to see the maximum Read and Write performance from a Standard DS14 VM. For detailed steps about creating a DS14 VM with premium disks, go to [Designing for high performance](#).

## *Warming up the Cache*

The disk with ReadOnly host caching are able to give higher IOPS than the disk limit. To get this maximum read performance from the host cache, first you must warm up the cache of this disk. This ensures that the Read IOs that the benchmarking tool will drive on CacheReads volume, actually hits the cache, and not the disk directly. The cache hits result in additional IOPS from the single cache enabled disk.

### **IMPORTANT**

You must warm up the cache before running benchmarking, every time VM is rebooted.

## Tools

### **lometer**

[Download the lometer tool](#) on the VM.

#### **Test file**

lometer uses a test file that is stored on the volume on which you run the benchmarking test. It drives Reads and Writes on this test file to measure the disk IOPS and Throughput. lometer creates this test file if you have not provided one. Create a 200 GB test file called iobw.tst on the CacheReads and NoCacheWrites volumes.

#### **Access specifications**

The specifications, request IO size, % read/write, % random/sequential are configured using the "Access Specifications" tab in lometer. Create an access specification for each of the scenarios described below. Create the access specifications and "Save" with an appropriate name like – RandomWrites\_8K, RandomReads\_8K. Select the corresponding specification when running the test scenario.

An example of access specifications for maximum Write IOPS scenario is shown below,

**Edit Access Specification**

|                                                                                                                                |                                                                                |                                                                                                                                    |
|--------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Name<br>RandomWrites                                                                                                           | Default Assignment<br>None                                                     |                                                                                                                                    |
| Size<br>0MB 8KB 0B                                                                                                             | % Access 100 % Read 0 % Random 100 Delay 0 Burst 1 Alignment sector Reply none |                                                                                                                                    |
| <input type="button" value="Insert Before"/> <input type="button" value="Insert After"/> <input type="button" value="Delete"/> |                                                                                |                                                                                                                                    |
| Transfer Request Size<br><br>Megabytes 0 Kilobytes 8 Bytes 0                                                                   | Percent of Access Specification<br><br>100 Percent                             | Percent Read/Write Distribution<br><br>100% Write 0% Read                                                                          |
| Percent Random/Sequential Distribution<br><br>0% Sequential 100% Random                                                        | Burstiness<br><br>Transfer Delay 0 ms Burst Length 1 I/Os                      | Align I/Os on<br><br><input checked="" type="radio"/> Sector Boundaries<br><input type="radio"/> Megabytes 0 Kilobytes 0 Bytes 512 |
| Reply Size<br><br><input checked="" type="radio"/> No Reply<br><input type="radio"/> Megabytes 0 Kilobytes 8 Bytes 0           | <input type="button" value="OK"/> <input type="button" value="Cancel"/>        |                                                                                                                                    |

#### Maximum IOPS test specifications

To demonstrate maximum IOPs, use smaller request size. Use 8K request size and create specifications for Random Writes and Reads.

| ACCESS SPECIFICATION | REQUEST SIZE | RANDOM % | READ % |
|----------------------|--------------|----------|--------|
| RandomWrites_8K      | 8K           | 100      | 0      |
| RandomReads_8K       | 8K           | 100      | 100    |

#### Maximum throughput test specifications

To demonstrate maximum Throughput, use larger request size. Use 64 K request size and create specifications for Random Writes and Reads.

| ACCESS SPECIFICATION | REQUEST SIZE | RANDOM % | READ % |
|----------------------|--------------|----------|--------|
| RandomWrites_64K     | 64 K         | 100      | 0      |
| RandomReads_64K      | 64 K         | 100      | 100    |

#### Run the Iometer test

Perform the steps below to warm up cache

1. Create two access specifications with values shown below,

| NAME             | REQUEST SIZE | RANDOM % | READ % |
|------------------|--------------|----------|--------|
| RandomWrites_1MB | 1 MB         | 100      | 0      |
| RandomReads_1MB  | 1 MB         | 100      | 100    |

2. Run the lometer test for initializing cache disk with following parameters. Use three worker threads for the target volume and a queue depth of 128. Set the "Run time" duration of the test to 2 hrs on the "Test Setup" tab.

| SCENARIO              | TARGET VOLUME | NAME             | DURATION |
|-----------------------|---------------|------------------|----------|
| Initialize Cache Disk | CacheReads    | RandomWrites_1MB | 2 hrs    |

3. Run the lometer test for warming up cache disk with following parameters. Use three worker threads for the target volume and a queue depth of 128. Set the "Run time" duration of the test to 2 hrs on the "Test Setup" tab.

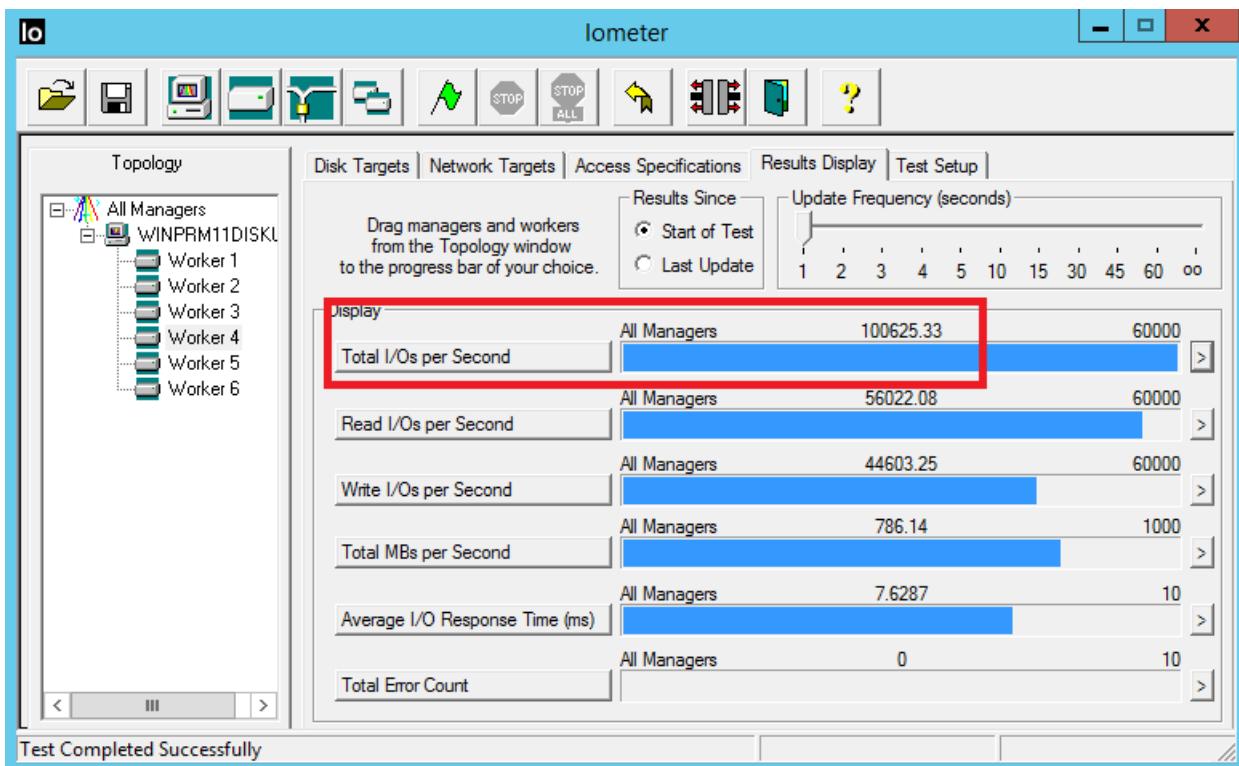
| SCENARIO           | TARGET VOLUME | NAME            | DURATION |
|--------------------|---------------|-----------------|----------|
| Warm up Cache Disk | CacheReads    | RandomReads_1MB | 2 hrs    |

After cache disk is warmed up, proceed with the test scenarios listed below. To run the lometer test, use at least three worker threads for **each** target volume. For each worker thread, select the target volume, set queue depth and select one of the saved test specifications, as shown in the table below, to run the corresponding test scenario. The table also shows expected results for IOPS and Throughput when running these tests. For all scenarios, a small IO size of 8 KB and a high queue depth of 128 is used.

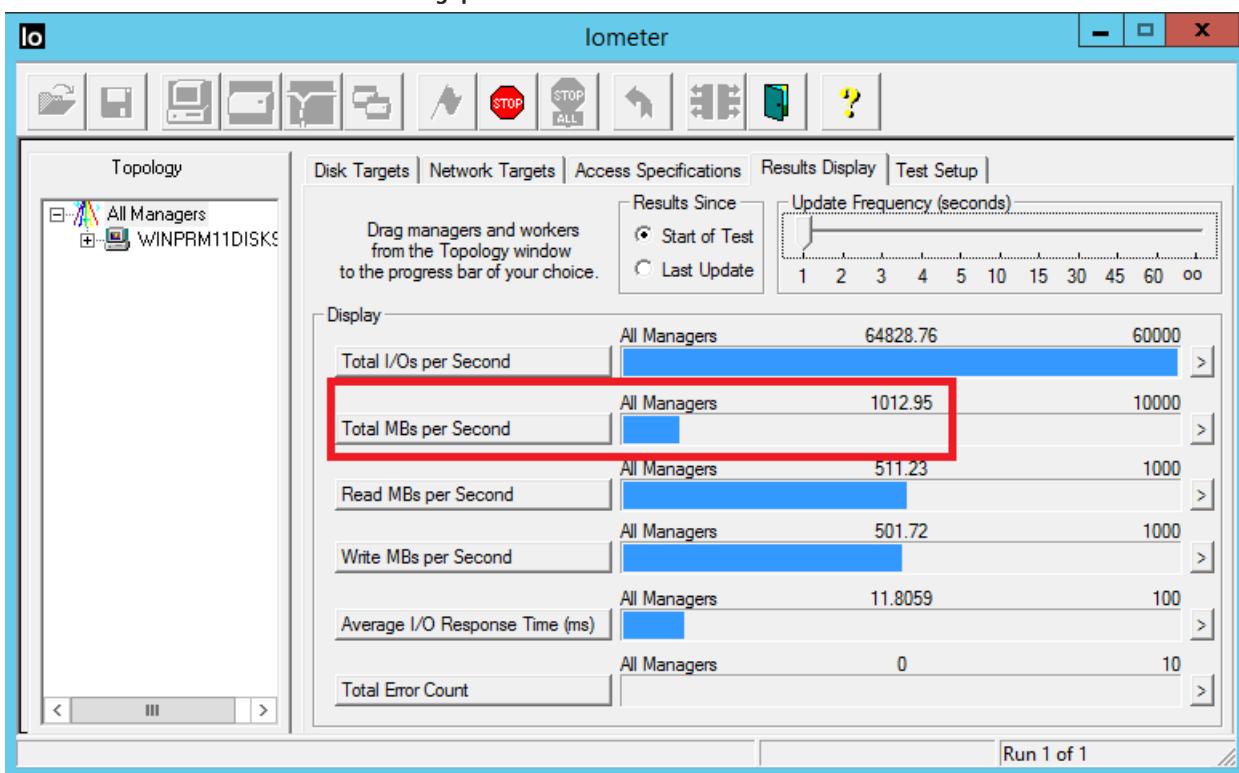
| TEST SCENARIO      | TARGET VOLUME   | NAME             | RESULT       |
|--------------------|-----------------|------------------|--------------|
| Max. Read IOPS     | CacheReads      | RandomWrites_8K  | 50,000 IOPS  |
| Max. Write IOPS    | NoCacheWrites   | RandomReads_8K   | 64,000 IOPS  |
| Max. Combined IOPS | CacheReads      | RandomWrites_8K  | 100,000 IOPS |
| NoCacheWrites      | RandomReads_8K  |                  |              |
| Max. Read MB/sec   | CacheReads      | RandomWrites_64K | 524 MB/sec   |
| Max. Write MB/sec  | NoCacheWrites   | RandomReads_64K  | 524 MB/sec   |
| Combined MB/sec    | CacheReads      | RandomWrites_64K | 1000 MB/sec  |
| NoCacheWrites      | RandomReads_64K |                  |              |

Below are screenshots of the lometer test results for combined IOPS and Throughput scenarios.

#### Combined reads and writes maximum IOPS



Combined reads and writes maximum throughput



## FIO

FIO is a popular tool to benchmark storage on the Linux VMs. It has the flexibility to select different IO sizes, sequential or random reads and writes. It spawns worker threads or processes to perform the specified I/O operations. You can specify the type of I/O operations each worker thread must perform using job files. We created one job file per scenario illustrated in the examples below. You can change the specifications in these job files to benchmark different workloads running on Premium Storage. In the examples, we are using a Standard DS 14 VM running **Ubuntu**. Use the same setup described in the beginning of the Benchmarking section and warm up the cache before running the benchmarking tests.

Before you begin, [download FIO](#) and install it on your virtual machine.

Run the following command for Ubuntu,

```
apt-get install fio
```

We use four worker threads for driving Write operations and four worker threads for driving Read operations on the disks. The Write workers are driving traffic on the "nocache" volume, which has 10 disks with cache set to "None". The Read workers are driving traffic on the "readcache" volume, which has one disk with cache set to "ReadOnly".

#### Maximum write IOPS

Create the job file with following specifications to get maximum Write IOPS. Name it "fiowrite.ini".

```
[global]
size=30g
direct=1
iodepth=256
ioengine=libaio
bs=8k

[writer1]
rw=randwrite
directory=/mnt/nocache
[writer2]
rw=randwrite
directory=/mnt/nocache
[writer3]
rw=randwrite
directory=/mnt/nocache
[writer4]
rw=randwrite
directory=/mnt/nocache
```

Note the follow key things that are in line with the design guidelines discussed in previous sections. These specifications are essential to drive maximum IOPS,

- A high queue depth of 256.
- A small block size of 8 KB.
- Multiple threads performing random writes.

Run the following command to kick off the FIO test for 30 seconds,

```
sudo fio --runtime 30 fiowrite.ini
```

While the test runs, you are able to see the number of write IOPS the VM and Premium disks are delivering. As shown in the sample below, the DS14 VM is delivering its maximum write IOPS limit of 50,000 IOPS.

```
demo@DS-VM-Linux-Demo:~$ sudo fio --runtime 30 fiowrite.ini
[sudo] password for demo:
writer1: (g=0): rw=randwrite, bs=8K-8K/8K-8K/8K-8K, ioengine=libaio, iodepth=256
writer2: (g=0): rw=randwrite, bs=8K-8K/8K-8K/8K-8K, ioengine=libaio, iodepth=256
writer3: (g=0): rw=randwrite, bs=8K-8K/8K-8K/8K-8K, ioengine=libaio, iodepth=256
writer4: (g=0): rw=randwrite, bs=8K-8K/8K-8K/8K-8K, ioengine=libaio, iodepth=256
fio-2.1.11
Starting 4 processes
Jobs: 4 (f=4): [w(4)] [63.3% done] [0KB/396.4MB/0KB /s] [0/50.8K/0 iops] [eta 00m:11s]
```

#### Maximum read IOPS

Create the job file with following specifications to get maximum Read IOPS. Name it "ioread.ini".

```

[global]
size=30g
direct=1
iodepth=256
ioengine=libaio
bs=8k

[reader1]
rw=randread
directory=/mnt/readcache
[reader2]
rw=randread
directory=/mnt/readcache
[reader3]
rw=randread
directory=/mnt/readcache
[reader4]
rw=randread
directory=/mnt/readcache

```

Note the follow key things that are in line with the design guidelines discussed in previous sections. These specifications are essential to drive maximum IOPS,

- A high queue depth of 256.
- A small block size of 8 KB.
- Multiple threads performing random writes.

Run the following command to kick off the FIO test for 30 seconds,

```
sudo fio --runtime 30 fioread.ini
```

While the test runs, you are able to see the number of read IOPS the VM and Premium disks are delivering. As shown in the sample below, the DS14 VM is delivering more than 64,000 Read IOPS. This is a combination of the disk and the cache performance.

```

demo@DS-VM-Linux-Demo:~$ sudo fio --runtime 30 fioread.ini
[sudo] password for demo:
reader1: (g=0): rw=randread, bs=8K-8K/8K-8K/8K-8K, ioengine=libaio, iodepth=256
reader2: (g=0): rw=randread, bs=8K-8K/8K-8K/8K-8K, ioengine=libaio, iodepth=256
reader3: (g=0): rw=randread, bs=8K-8K/8K-8K/8K-8K, ioengine=libaio, iodepth=256
reader4: (g=0): rw=randread, bs=8K-8K/8K-8K/8K-8K, ioengine=libaio, iodepth=256
fio-2.1.11
Starting 4 processes
Jobs: 4 (f=4): [r(4)] [70.0% done] [514.8MB/0KB/0KB /s] [65.9K/0/0 iops] [eta 00m:09s]
```

#### **Maximum read and write IOPS**

Create the job file with following specifications to get maximum combined Read and Write IOPS. Name it "fioreadwrite.ini".

```

[global]
size=30g
direct=1
iodepth=128
ioengine=libaio
bs=4k

[reader1]
rw=randread
directory=/mnt/readcache
[reader2]
rw=randread
directory=/mnt/readcache
[reader3]
rw=randread
directory=/mnt/readcache
[reader4]
rw=randread
directory=/mnt/readcache

[writer1]
rw=randwrite
directory=/mnt/nocache
rate_iops=12500
[writer2]
rw=randwrite
directory=/mnt/nocache
rate_iops=12500
[writer3]
rw=randwrite
directory=/mnt/nocache
rate_iops=12500
[writer4]
rw=randwrite
directory=/mnt/nocache
rate_iops=12500

```

Note the follow key things that are in line with the design guidelines discussed in previous sections. These specifications are essential to drive maximum IOPS,

- A high queue depth of 128.
- A small block size of 4 KB.
- Multiple threads performing random reads and writes.

Run the following command to kick off the FIO test for 30 seconds,

```
sudo fio --runtime 30 fioreadwrite.ini
```

While the test runs, you are able to see the number of combined read and write IOPS the VM and Premium disks are delivering. As shown in the sample below, the DS14 VM is delivering more than 100,000 combined Read and Write IOPS. This is a combination of the disk and the cache performance.

```

demo@DS-VM-Linux-Demo:~$ sudo fio --runtime 30 fioreadwrite.ini
reader1: (g=0): rw=randread, bs=4K-4K/4K-4K/4K-4K, ioengine=libaio, iodepth=128
reader2: (g=0): rw=randread, bs=4K-4K/4K-4K/4K-4K, ioengine=libaio, iodepth=128
reader3: (g=0): rw=randread, bs=4K-4K/4K-4K/4K-4K, ioengine=libaio, iodepth=128
reader4: (g=0): rw=randread, bs=4K-4K/4K-4K/4K-4K, ioengine=libaio, iodepth=128
writer1: (g=0): rw=randwrite, bs=4K-4K/4K-4K/4K-4K, ioengine=libaio, iodepth=128
writer2: (g=0): rw=randwrite, bs=4K-4K/4K-4K/4K-4K, ioengine=libaio, iodepth=128
writer3: (g=0): rw=randwrite, bs=4K-4K/4K-4K/4K-4K, ioengine=libaio, iodepth=128
writer4: (g=0): rw=randwrite, bs=4K-4K/4K-4K/4K-4K, ioengine=libaio, iodepth=128
fio-2.1.11
Starting 8 processes
Jobs: 8 (f=8), CR=50000/0 IOPS: [r(4),w(4)] [22.6% done] [251.2MB/183.3MB/0KB /s] [64.3K/46.1K/0 iops] [eta 00m:24s]
```

#### Maximum combined throughput

To get the maximum combined Read and Write Throughput, use a larger block size and large queue depth with

multiple threads performing reads and writes. You can use a block size of 64 KB and queue depth of 128.

## Next steps

Proceed to our article on [designing for high performance](#).

In that article, you create a checklist similar to your existing application for the prototype. Using Benchmarking tools you can simulate the workloads and measure performance on the prototype application. By doing so, you can determine which disk offering can match or surpass your application performance requirements. Then you can implement the same guidelines for your production application.

# Optimize your Linux VM on Azure

2/28/2020 • 7 minutes to read • [Edit Online](#)

Creating a Linux virtual machine (VM) is easy to do from the command line or from the portal. This tutorial shows you how to ensure you have set it up to optimize its performance on the Microsoft Azure platform. This topic uses an Ubuntu Server VM, but you can also create Linux virtual machine using [your own images as templates](#).

## Prerequisites

This topic assumes you already have a working Azure subscription ([free trial signup](#)) and have already provisioned a VM into your Azure subscription. Make sure that you have the latest [Azure CLI](#) installed and logged in to your Azure subscription with [az login](#) before you [create a VM](#).

## Azure OS Disk

Once you create a Linux VM in Azure, it has two disks associated with it. **/dev/sda** is your OS disk, **/dev/sdb** is your temporary disk. Do not use the main OS disk (**/dev/sda**) for anything except the operating system as it is optimized for fast VM boot time and does not provide good performance for your workloads. You want to attach one or more disks to your VM to get persistent and optimized storage for your data.

## Adding Disks for Size and Performance targets

Based on the VM size, you can attach up to 16 additional disks on an A-Series, 32 disks on a D-Series and 64 disks on a G-Series machine - each up to 32 TB in size. You add extra disks as needed per your space and IOps requirements. Each disk has a performance target of 500 IOps for Standard Storage and up to 20,000 IOps per disk for Premium Storage.

To achieve the highest IOps on Premium Storage disks where their cache settings have been set to either **ReadOnly** or **None**, you must disable **barriers** while mounting the file system in Linux. You do not need barriers because the writes to Premium Storage backed disks are durable for these cache settings.

- If you use **reiserFS**, disable barriers using the mount option `barrier=none` (For enabling barriers, use `barrier=flush`)
- If you use **ext3/ext4**, disable barriers using the mount option `barrier=0` (For enabling barriers, use `barrier=1`)
- If you use **XFS**, disable barriers using the mount option `nobarrier` (For enabling barriers, use the option `barrier`)

## Unmanaged storage account considerations

The default action when you create a VM with the Azure CLI is to use Azure Managed Disks. These disks are handled by the Azure platform and do not require any preparation or location to store them. Unmanaged disks require a storage account and have some additional performance considerations. For more information about managed disks, see [Azure Managed Disks overview](#). The following section outlines performance considerations only when you use unmanaged disks. Again, the default and recommended storage solution is to use managed disks.

If you create a VM with unmanaged disks, make sure that you attach disks from storage accounts residing in the same region as your VM to ensure close proximity and minimize network latency. Each Standard storage account has a maximum of 20k IOps and a 500 TB size capacity. This limit works out to approximately 40 heavily used disks including both the OS disk and any data disks you create. For Premium Storage accounts, there is no Maximum

IOps limit but there is a 32 TB size limit.

When dealing with high IOps workloads and you have chosen Standard Storage for your disks, you might need to split the disks across multiple storage accounts to make sure you have not hit the 20,000 IOps limit for Standard Storage accounts. Your VM can contain a mix of disks from across different storage accounts and storage account types to achieve your optimal configuration.

## Your VM Temporary drive

By default when you create a VM, Azure provides you with an OS disk (**/dev/sda**) and a temporary disk (**/dev/sdb**). All additional disks you add show up as **/dev/sdc**, **/dev/sdd**, **/dev/sde** and so on. All data on your temporary disk (**/dev/sdb**) is not durable, and can be lost if specific events like VM Resizing, redeployment, or maintenance forces a restart of your VM. The size and type of your temporary disk is related to the VM size you chose at deployment time. All of the premium size VMs (DS, G, and DS\_V2 series) the temporary drive are backed by a local SSD for additional performance of up to 48k IOps.

## Linux Swap Partition

If your Azure VM is from an Ubuntu or CoreOS image, then you can use CustomData to send a cloud-config to cloud-init. If you [uploaded a custom Linux image](#) that uses cloud-init, you also configure swap partitions using cloud-init.

On Ubuntu Cloud Images, you must use cloud-init to configure the swap partition. For more information, see [AzureSwapPartitions](#).

For images without cloud-init support, VM images deployed from the Azure Marketplace have a VM Linux Agent integrated with the OS. This agent allows the VM to interact with various Azure services. Assuming you have deployed a standard image from the Azure Marketplace, you would need to do the following to correctly configure your Linux swap file settings:

Locate and modify two entries in the **/etc/waagent.conf** file. They control the existence of a dedicated swap file and size of the swap file. The parameters you need to verify are `ResourceDisk.EnableSwap` and `ResourceDisk.SwapSizeMB`

To enable a properly enabled disk and mounted swap file, ensure the parameters have the following settings:

- `ResourceDisk.EnableSwap=Y`
- `ResourceDisk.SwapSizeMB={size in MB to meet your needs}`

Once you have made the change, you need to restart the waagent or restart your Linux VM to reflect those changes. You know the changes have been implemented and a swap file has been created when you use the `free` command to view free space. The following example has a 512MB swap file created as a result of modifying the **waagent.conf** file:

```
azuseruser@myVM:~$ free
 total used free shared buffers cached
Mem: 3525156 804168 2720988 408 8428 633192
 -/+ buffers/cache: 162548 3362608
Swap: 524284 0 524284
```

## I/O scheduling algorithm for Premium Storage

With the 2.6.18 Linux kernel, the default I/O scheduling algorithm was changed from Deadline to CFQ (Completely fair queuing algorithm). For random access I/O patterns, there is negligible difference in performance differences between CFQ and Deadline. For SSD-based disks where the disk I/O pattern is predominantly sequential,

switching back to the NOOP or Deadline algorithm can achieve better I/O performance.

## View the current I/O scheduler

Use the following command:

```
cat /sys/block/sda/queue/scheduler
```

You see following output, which indicates the current scheduler.

```
noop [deadline] cfq
```

## Change the current device (/dev/sda) of I/O scheduling algorithm

Use the following commands:

```
azureuser@myVM:~$ sudo su -
root@myVM:~# echo "noop" >/sys/block/sda/queue/scheduler
root@myVM:~# sed -i 's/GRUB_CMDLINE_LINUX=""/GRUB_CMDLINE_LINUX_DEFAULT="quiet splash elevator=noop"/g' /etc/default/grub
root@myVM:~# update-grub
```

### NOTE

Applying this setting for **/dev/sda** alone is not useful. Set on all data disks where sequential I/O dominates the I/O pattern.

You should see the following output, indicating that **grub.cfg** has been rebuilt successfully and that the default scheduler has been updated to NOOP.

```
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-3.13.0-34-generic
Found initrd image: /boot/initrd.img-3.13.0-34-generic
Found linux image: /boot/vmlinuz-3.13.0-32-generic
Found initrd image: /boot/initrd.img-3.13.0-32-generic
Found memtest86+ image: /memtest86+.elf
Found memtest86+ image: /memtest86+.bin
done
```

For the Red Hat distribution family, you only need the following command:

```
echo 'echo noop >/sys/block/sda/queue/scheduler' >> /etc/rc.local
```

## Using Software RAID to achieve higher I/Ops

If your workloads require more IOps than a single disk can provide, you need to use a software RAID configuration of multiple disks. Because Azure already performs disk resiliency at the local fabric layer, you achieve the highest level of performance from a RAID-0 striping configuration. Provision and create disks in the Azure environment and attach them to your Linux VM before partitioning, formatting and mounting the drives. More details on configuring a software RAID setup on your Linux VM in azure can be found in the [Configuring Software RAID on Linux](#) document.

As an alternative to a traditional RAID configuration, you can also choose to install Logical Volume Manager (LVM) in order to configure a number of physical disks into a single striped logical storage volume. In this configuration, reads and writes are distributed to multiple disks contained in the volume group (similar to RAID0). For

performance reasons, it is likely you will want to stripe your logical volumes so that reads and writes utilize all your attached data disks. More details on configuring a striped logical volume on your Linux VM in Azure can be found in the [Configure LVM on a Linux VM in Azure](#) document.

## Next Steps

Remember, as with all optimization discussions, you need to perform tests before and after each change to measure the impact the change has. Optimization is a step by step process that has different results across different machines in your environment. What works for one configuration may not work for others.

Some useful links to additional resources:

- [Azure Linux Agent User Guide](#)
- [Configure Software RAID on Linux](#)

# Configure Software RAID on Linux

11/26/2019 • 5 minutes to read • [Edit Online](#)

It's a common scenario to use software RAID on Linux virtual machines in Azure to present multiple attached data disks as a single RAID device. Typically this can be used to improve performance and allow for improved throughput compared to using just a single disk.

## Attaching data disks

Two or more empty data disks are needed to configure a RAID device. The primary reason for creating a RAID device is to improve performance of your disk IO. Based on your IO needs, you can choose to attach disks that are stored in our Standard Storage, with up to 500 IO/ps per disk or our Premium storage with up to 5000 IO/ps per disk. This article does not go into detail on how to provision and attach data disks to a Linux virtual machine. See the Microsoft Azure article [attach a disk](#) for detailed instructions on how to attach an empty data disk to a Linux virtual machine on Azure.

### IMPORTANT

Do not mix disks of different sizes, doing so would result in performance of the raidset to be limited to that of the slowest disk.

## Install the mdadm utility

- **Ubuntu**

```
sudo apt-get update
sudo apt-get install mdadm
```

- **CentOS & Oracle Linux**

```
sudo yum install mdadm
```

- **SLES and openSUSE**

```
zypper install mdadm
```

## Create the disk partitions

In this example, we create a single disk partition on /dev/sdc. The new disk partition will be called /dev/sdc1.

1. Start `fdisk` to begin creating partitions

```
sudo fdisk /dev/sdc
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF disklabel
Building a new DOS disklabel with disk identifier 0xa34cb70c.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.

WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
 switch off the mode (command 'c') and change display units to
 sectors (command 'u').
```

2. Press 'n' at the prompt to create a **new** partition:

```
Command (m for help): n
```

3. Next, press 'p' to create a **primary** partition:

```
Command action
e extended
p primary partition (1-4)
```

4. Press '1' to select partition number 1:

```
Partition number (1-4): 1
```

5. Select the starting point of the new partition, or press **<enter>** to accept the default to place the partition at the beginning of the free space on the drive:

```
First cylinder (1-1305, default 1):
Using default value 1
```

6. Select the size of the partition, for example type '+10G' to create a 10 gigabyte partition. Or, press **<enter>** create a single partition that spans the entire drive:

```
Last cylinder, +cylinders or +size{K,M,G} (1-1305, default 1305):
Using default value 1305
```

7. Next, change the ID and **type** of the partition from the default ID '83' (Linux) to ID 'fd' (Linux raid auto):

```
Command (m for help): t
Selected partition 1
Hex code (type L to list codes): fd
```

8. Finally, write the partition table to the drive and exit fdisk:

```
Command (m for help): w
The partition table has been altered!
```

## Create the RAID array

1. The following example will "stripe" (RAID level 0) three partitions located on three separate data disks (`sdc1`, `sdd1`, `sde1`). After running this command a new RAID device called **/dev/md127** is created. Also

note that if these data disks were previously part of another defunct RAID array it may be necessary to add the `--force` parameter to the `mdadm` command:

```
sudo mdadm --create /dev/md127 --level 0 --raid-devices 3 \
/dev/sdc1 /dev/sdd1 /dev/sde1
```

## 2. Create the file system on the new RAID device

### **CentOS, Oracle Linux, SLES 12, openSUSE, and Ubuntu**

```
sudo mkfs -t ext4 /dev/md127
```

### **SLES 11**

```
sudo mkfs -t ext3 /dev/md127
```

### **SLES 11** - enable boot.md and create mdadm.conf

```
sudo -i chkconfig --add boot.md
sudo echo 'DEVICE /dev/sd*[0-9]' >> /etc/mdadm.conf
```

#### **NOTE**

A reboot may be required after making these changes on SUSE systems. This step is *not* required on SLES 12.

## Add the new file system to /etc/fstab

#### **IMPORTANT**

Improperly editing the `/etc/fstab` file could result in an unbootable system. If unsure, refer to the distribution's documentation for information on how to properly edit this file. It is also recommended that a backup of the `/etc/fstab` file is created before editing.

### 1. Create the desired mount point for your new file system, for example:

```
sudo mkdir /data
```

### 2. When editing `/etc/fstab`, the **UUID** should be used to reference the file system rather than the device name. Use the `blkid` utility to determine the UUID for the new file system:

```
sudo /sbin/blkid
.....
/dev/md127: UUID="aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeee" TYPE="ext4"
```

### 3. Open `/etc/fstab` in a text editor and add an entry for the new file system, for example:

```
UUID=aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeee /data ext4 defaults 0 2
```

Or on **SLES 11**:

```
/dev/disk/by-uuid/aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeee /data ext3 defaults 0 2
```

Then, save and close /etc/fstab.

#### 4. Test that the /etc/fstab entry is correct:

```
sudo mount -a
```

If this command results in an error message, please check the syntax in the /etc/fstab file.

Next run the `mount` command to ensure the file system is mounted:

```
mount
.....
/dev/md127 on /data type ext4 (rw)
```

#### 5. (Optional) Failsafe Boot Parameters

##### **fstab configuration**

Many distributions include either the `nobootwait` or `nofail` mount parameters that may be added to the /etc/fstab file. These parameters allow for failures when mounting a particular file system and allow the Linux system to continue to boot even if it is unable to properly mount the RAID file system. Refer to your distribution's documentation for more information on these parameters.

Example (Ubuntu):

```
UUID=aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeee /data ext4 defaults,nobootwait 0 2
```

##### **Linux boot parameters**

In addition to the above parameters, the kernel parameter "`bootdegraded=true`" can allow the system to boot even if the RAID is perceived as damaged or degraded, for example if a data drive is inadvertently removed from the virtual machine. By default this could also result in a non-bootable system.

Please refer to your distribution's documentation on how to properly edit kernel parameters. For example, in many distributions (CentOS, Oracle Linux, SLES 11) these parameters may be added manually to the "`/boot/grub/menu.lst`" file. On Ubuntu this parameter can be added to the `GRUB_CMDLINE_LINUX_DEFAULT` variable on "`/etc/default/grub`".

## TRIM/UNMAP support

Some Linux kernels support TRIM/UNMAP operations to discard unused blocks on the disk. These operations are primarily useful in standard storage to inform Azure that deleted pages are no longer valid and can be discarded. Discarding pages can save cost if you create large files and then delete them.

##### **NOTE**

RAID may not issue discard commands if the chunk size for the array is set to less than the default (512KB). This is because the unmap granularity on the Host is also 512KB. If you modified the array's chunk size via mdadm's `--chunk=` parameter, then TRIM/unmap requests may be ignored by the kernel.

There are two ways to enable TRIM support in your Linux VM. As usual, consult your distribution for the

recommended approach:

- Use the `discard` mount option in `/etc/fstab`, for example:

```
UUID=aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeee /data ext4 defaults,discard 0 2
```

- In some cases the `discard` option may have performance implications. Alternatively, you can run the `fstrim` command manually from the command line, or add it to your crontab to run regularly:

### **Ubuntu**

```
sudo apt-get install util-linux
sudo fstrim /data
```

### **RHEL/CentOS**

```
sudo yum install util-linux
sudo fstrim /data
```

# Configure LVM on a Linux VM in Azure

1/16/2020 • 4 minutes to read • [Edit Online](#)

This document will discuss how to configure Logical Volume Manager (LVM) in your Azure virtual machine. LVM may be used on the OS disk or data disks in Azure VMs, however, by default most cloud images will not have LVM configured on the OS disk. The steps below will focus on configuring LVM for your data disks.

## Linear vs. striped logical volumes

LVM can be used to combine a number of physical disks into a single storage volume. By default LVM will usually create linear logical volumes, which means that the physical storage is concatenated together. In this case read/write operations will typically only be sent to a single disk. In contrast, we can also create striped logical volumes where reads and writes are distributed to multiple disks contained in the volume group (similar to RAID0). For performance reasons, it is likely you will want to stripe your logical volumes so that reads and writes utilize all your attached data disks.

This document will describe how to combine several data disks into a single volume group, and then create a striped logical volume. The steps below are generalized to work with most distributions. In most cases the utilities and workflows for managing LVM on Azure are not fundamentally different than other environments. As usual, also consult your Linux vendor for documentation and best practices for using LVM with your particular distribution.

## Attaching data disks

One will usually want to start with two or more empty data disks when using LVM. Based on your IO needs, you can choose to attach disks that are stored in our Standard Storage, with up to 500 IO/ps per disk or our Premium storage with up to 5000 IO/ps per disk. This article will not go into detail on how to provision and attach data disks to a Linux virtual machine. See the Microsoft Azure article [attach a disk](#) for detailed instructions on how to attach an empty data disk to a Linux virtual machine on Azure.

## Install the LVM utilities

- **Ubuntu**

```
sudo apt-get update
sudo apt-get install lvm2
```

- **RHEL, CentOS & Oracle Linux**

```
sudo yum install lvm2
```

- **SLES 12 and openSUSE**

```
sudo zypper install lvm2
```

- **SLES 11**

```
sudo zypper install lvm2
```

On SLES11, you must also edit `/etc/sysconfig/lvm` and set `LVM_ACTIVATED_ON_DISCOVERED` to "enable":

```
LVM_ACTIVATED_ON_DISCOVERED="enable"
```

## Configure LVM

In this guide we will assume you have attached three data disks, which we'll refer to as `/dev/sdc`, `/dev/sdd` and `/dev/sde`. These paths may not match the disk path names in your VM. You can run '`sudo fdisk -l`' or similar command to list your available disks.

1. Prepare the physical volumes:

```
sudo pvcreate /dev/sd[cde]
Physical volume "/dev/sdc" successfully created
Physical volume "/dev/sdd" successfully created
Physical volume "/dev/sde" successfully created
```

2. Create a volume group. In this example we are calling the volume group `data-vg01`:

```
sudo vgcreate data-vg01 /dev/sd[cde]
Volume group "data-vg01" successfully created
```

3. Create the logical volume(s). The command below we will create a single logical volume called `data-lv01` to span the entire volume group, but note that it is also feasible to create multiple logical volumes in the volume group.

```
sudo lvcreate --extents 100%FREE --stripes 3 --name data-lv01 data-vg01
Logical volume "data-lv01" created.
```

4. Format the logical volume

```
sudo mkfs -t ext4 /dev/data-vg01/data-lv01
```

**NOTE**

With SLES11 use `-t ext3` instead of ext4. SLES11 only supports read-only access to ext4 filesystems.

## Add the new file system to `/etc/fstab`

**IMPORTANT**

Improperly editing the `/etc/fstab` file could result in an unbootable system. If unsure, refer to the distribution's documentation for information on how to properly edit this file. It is also recommended that a backup of the `/etc/fstab` file is created before editing.

1. Create the desired mount point for your new file system, for example:

```
sudo mkdir /data
```

## 2. Locate the logical volume path

```
lvdisplay
--- Logical volume ---
LV Path /dev/data-vg01/data-lv01
....
```

## 3. Open `/etc/fstab` in a text editor and add an entry for the new file system, for example:

```
/dev/data-vg01/data-lv01 /data ext4 defaults 0 2
```

Then, save and close `/etc/fstab`.

## 4. Test that the `/etc/fstab` entry is correct:

```
sudo mount -a
```

If this command results in an error message check the syntax in the `/etc/fstab` file.

Next run the `mount` command to ensure the file system is mounted:

```
mount
.....
/dev/mapper/data--vg01-data--lv01 on /data type ext4 (rw)
```

## 5. (Optional) Failsafe boot parameters in `/etc/fstab`

Many distributions include either the `nobootwait` or `nofail` mount parameters that may be added to the `/etc/fstab` file. These parameters allow for failures when mounting a particular file system and allow the Linux system to continue to boot even if it is unable to properly mount the RAID file system. Refer to your distribution's documentation for more information on these parameters.

Example (Ubuntu):

```
/dev/data-vg01/data-lv01 /data ext4 defaults,nobootwait 0 2
```

## TRIM/UNMAP support

Some Linux kernels support TRIM/UNMAP operations to discard unused blocks on the disk. These operations are primarily useful in standard storage to inform Azure that deleted pages are no longer valid and can be discarded. Discarding pages can save cost if you create large files and then delete them.

There are two ways to enable TRIM support in your Linux VM. As usual, consult your distribution for the recommended approach:

- Use the `discard` mount option in `/etc/fstab`, for example:

```
/dev/data-vg01/data-lv01 /data ext4 defaults,discard 0 2
```

- In some cases the `discard` option may have performance implications. Alternatively, you can run the

`fstrim` command manually from the command line, or add it to your crontab to run regularly:

## Ubuntu

```
sudo apt-get install util-linux
sudo fstrim /datadrive
```

## RHEL, CentOS & Oracle Linux

```
sudo yum install util-linux
sudo fstrim /datadrive
```

# Find and delete unattached Azure managed and unmanaged disks

11/13/2019 • 2 minutes to read • [Edit Online](#)

When you delete a virtual machine (VM) in Azure, by default, any disks that are attached to the VM aren't deleted. This feature helps to prevent data loss due to the unintentional deletion of VMs. After a VM is deleted, you will continue to pay for unattached disks. This article shows you how to find and delete any unattached disks and reduce unnecessary costs.

## Managed disks: Find and delete unattached disks

The following script looks for unattached [managed disks](#) by examining the value of the **ManagedBy** property. When a managed disk is attached to a VM, the **ManagedBy** property contains the resource ID of the VM. When a managed disk is unattached, the **ManagedBy** property is null. The script examines all the managed disks in an Azure subscription. When the script locates a managed disk with the **ManagedBy** property set to null, the script determines that the disk is unattached.

### IMPORTANT

First, run the script by setting the **deleteUnattachedDisks** variable to 0. This action lets you find and view all the unattached managed disks.

After you review all the unattached disks, run the script again and set the **deleteUnattachedDisks** variable to 1. This action lets you delete all the unattached managed disks.

```
Set deleteUnattachedDisks=1 if you want to delete unattached Managed Disks
Set deleteUnattachedDisks=0 if you want to see the Id of the unattached Managed Disks
deleteUnattachedDisks=0

unattachedDiskIds=$(az disk list --query '[?managedBy==`null`].[id]' -o tsv)
for id in ${unattachedDiskIds[@]}
do
 if (($deleteUnattachedDisks == 1))
 then
 echo "Deleting unattached Managed Disk with Id: \"$id"
 az disk delete --ids $id --yes
 echo "Deleted unattached Managed Disk with Id: \"$id"
 else
 echo $id
 fi
done
```

## Unmanaged disks: Find and delete unattached disks

Unmanaged disks are VHD files that are stored as [page blobs](#) in [Azure storage accounts](#). The following script looks for unattached unmanaged disks (page blobs) by examining the value of the **LeaseStatus** property. When an unmanaged disk is attached to a VM, the **LeaseStatus** property is set to **Locked**. When an unmanaged disk is unattached, the **LeaseStatus** property is set to **Unlocked**. The script examines all the unmanaged disks in all the Azure storage accounts in an Azure subscription. When the script locates an unmanaged disk with a **LeaseStatus**

property set to **Unlocked**, the script determines that the disk is unattached.

#### IMPORTANT

First, run the script by setting the **deleteUnattachedVHDs** variable to 0. This action lets you find and view all the unattached unmanaged VHDs.

After you review all the unattached disks, run the script again and set the **deleteUnattachedVHDs** variable to 1. This action lets you delete all the unattached unmanaged VHDs.

```
Set deleteUnattachedVHDs=1 if you want to delete unattached VHDs
Set deleteUnattachedVHDs=0 if you want to see the details of the unattached VHDs
deleteUnattachedVHDs=0

storageAccountIds=$(az storage account list --query [].[id] -o tsv)

for id in ${storageAccountIds[@]}
do
 connectionString=$(az storage account show-connection-string --ids $id --query connectionString -o tsv)
 containers=$(az storage container list --connection-string $connectionString --query [].[name] -o tsv)

 for container in ${containers[@]}
 do

 blobs=$(az storage blob list -c $container --connection-string $connectionString --query "[?properties.blobType=='PageBlob' && ends_with(name,'.vhd')].[name]" -o tsv)

 for blob in ${blobs[@]}
 do
 leaseStatus=$(az storage blob show -n $blob -c $container --connection-string $connectionString --query "properties.lease.status" -o tsv)

 if ["$leaseStatus" == "unlocked"]
 then

 if (($deleteUnattachedVHDs == 1))
 then

 echo "Deleting VHD: \"$blob\" in container: \"$container\" in storage account: \"$id"
 az storage blob delete --delete-snapshots include -n $blob -c $container --connection-string $connectionString

 echo "Deleted VHD: \"$blob\" in container: \"$container\" in storage account: \"$id"
 else
 echo "StorageAccountId: \"$id\" container: \"$container\" VHD: \"$blob"
 fi

 fi
 done
 done
done
```

## Next steps

[Delete storage account](#)

# Mount Azure File storage on Linux VMs using SMB

11/13/2019 • 3 minutes to read • [Edit Online](#)

This article shows you how to use the Azure File storage service on a Linux VM using an SMB mount with the Azure CLI. Azure File storage offers file shares in the cloud using the standard SMB protocol.

File storage offers file shares in the cloud that use the standard SMB protocol. You can mount a file share from any OS that supports SMB 3.0. When you use an SMB mount on Linux, you get easy backups to a robust, permanent archiving storage location that is supported by an SLA.

Moving files from a VM to an SMB mount that's hosted on File storage is a great way to debug logs. The same SMB share can be mounted locally to your Mac, Linux, or Windows workstation. SMB isn't the best solution for streaming Linux or application logs in real time, because the SMB protocol is not built to handle such heavy logging duties. A dedicated, unified logging layer tool such as Fluentd would be a better choice than SMB for collecting Linux and application logging output.

This guide requires that you're running the Azure CLI version 2.0.4 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install the Azure CLI](#).

## Create a resource group

Create a resource group named *myResourceGroup* in the *East US* location.

```
az group create --name myResourceGroup --location eastus
```

## Create a storage account

Create a new storage account, within the resource group that you created, using [az storage account create](#). This example creates a storage account named *mySTORAGEACCT<random number>* and puts the name of that storage account in the variable **STORAGEACCT**. Storage account names must be unique, using `$RANDOM` appends a number to the end to make it unique.

```
STORAGEACCT=$(az storage account create \
 --resource-group "myResourceGroup" \
 --name "mystorageacct$RANDOM" \
 --location eastus \
 --sku Standard_LRS \
 --query "name" | tr -d '')
```

## Get the storage key

When you create a storage account, the account keys are created in pairs so that they can be rotated without any service interruption. When you switch to the second key in the pair, you create a new key pair. New storage account keys are always created in pairs, so you always have at least one unused storage account key ready to switch to.

View the storage account keys using [az storage account keys list](#). This example stores the value of key 1 in the **STORAGEKEY** variable.

```
STORAGEKEY=$(az storage account keys list \
--resource-group "myResourceGroup" \
--account-name $STORAGEACCT \
--query "[0].value" | tr -d '')
```

## Create a file share

Create the File storage share using [az storage share create](#).

Share names need to be all lower case letters, numbers, and single hyphens but can't start with a hyphen. For complete details about naming file shares and files, see [Naming and Referencing Shares, Directories, Files, and Metadata](#).

This example creates a share named *myshare* with a 10-GiB quota.

```
az storage share create --name myshare \
--quota 10 \
--account-name $STORAGEACCT \
--account-key $STORAGEKEY
```

## Create a mount point

To mount the Azure file share on your Linux computer, you need to make sure you have the **cifs-utils** package installed. For installation instructions, see [Install the cifs-utils package for your Linux distribution](#).

Azure Files uses SMB protocol, which communicates over TCP port 445. If you're having trouble mounting your Azure file share, make sure your firewall is not blocking TCP port 445.

```
mkdir -p /mnt/MyAzureFileShare
```

## Mount the share

Mount the Azure file share to the local directory.

```
sudo mount -t cifs //${STORAGEACCT}.file.core.windows.net/myshare /mnt/MyAzureFileShare -o
vers=3.0,username=${STORAGEACCT},password=${STORAGEKEY},dir_mode=0777,file_mode=0777,serverino
```

The above command uses the [mount](#) command to mount the Azure file share and options specific to [cifs](#). Specifically, the `file_mode` and `dir_mode` options set files and directories to permission `0777`. The `0777` permission gives read, write, and execute permissions to all users. You can change these permissions by replacing the values with other [chmod permissions](#). You can also use other [cifs](#) options such as `gid` or `uid`.

## Persist the mount

When you reboot the Linux VM, the mounted SMB share is unmounted during shutdown. To remount the SMB share on boot, add a line to the Linux `/etc/fstab`. Linux uses the `fstab` file to list the file systems that it needs to mount during the boot process. Adding the SMB share ensures that the File storage share is a permanently mounted file system for the Linux VM. Adding the File storage SMB share to a new VM is possible when you use `cloud-init`.

```
//myaccountname.file.core.windows.net/mystorageshare /mnt/mymountpoint cifs
vers=3.0,username=mystorageaccount,password=myStorageAccountKeyEndingIn==,dir_mode=0777,file_mode=0777
```

For increased security in production environments, you should store your credentials outside of fstab.

## Next steps

- [Using cloud-init to customize a Linux VM during creation](#)
- [Add a disk to a Linux VM](#)
- [Azure Disk Encryption for Linux VMs](#)

# Frequently asked questions about Azure IaaS VM disks and managed and unmanaged premium disks

12/10/2019 • 21 minutes to read • [Edit Online](#)

This article answers some frequently asked questions about Azure Managed Disks and Azure Premium SSD disks.

## Managed Disks

### **What is Azure Managed Disks?**

Managed Disks is a feature that simplifies disk management for Azure IaaS VMs by handling storage account management for you. For more information, see the [Managed Disks overview](#).

### **If I create a standard managed disk from an existing VHD that's 80 GB, how much will that cost me?**

A standard managed disk created from an 80-GB VHD is treated as the next available standard disk size, which is an S10 disk. You're charged according to the S10 disk pricing. For more information, see the [pricing page](#).

### **Are there any transaction costs for standard managed disks?**

Yes. You're charged for each transaction. For more information, see the [pricing page](#).

### **For a standard managed disk, will I be charged for the actual size of the data on the disk or for the provisioned capacity of the disk?**

You're charged based on the provisioned capacity of the disk. For more information, see the [pricing page](#).

### **How is pricing of premium managed disks different from unmanaged disks?**

The pricing of premium managed disks is the same as unmanaged premium disks.

### **Can I change the storage account type (Standard or Premium) of my managed disks?**

Yes. You can change the storage account type of your managed disks by using the Azure portal, PowerShell, or the Azure CLI.

### **Can I use a VHD file in an Azure storage account to create a managed disk with a different subscription?**

Yes.

### **Can I use a VHD file in an Azure storage account to create a managed disk in a different region?**

No.

### **Are there any scale limitations for customers that use managed disks?**

Managed Disks eliminates the limits associated with storage accounts. However, the maximum limit is 50,000 managed disks per region and per disk type for a subscription.

### **Can I take an incremental snapshot of a managed disk?**

No. The current snapshot capability makes a full copy of a managed disk.

### **Can VMs in an availability set consist of a combination of managed and unmanaged disks?**

No. The VMs in an availability set must use either all managed disks or all unmanaged disks. When you create an availability set, you can choose which type of disks you want to use.

## **Is Managed Disks the default option in the Azure portal?**

Yes.

## **Can I create an empty managed disk?**

Yes. You can create an empty disk. A managed disk can be created independently of a VM, for example, without attaching it to a VM.

## **What is the supported fault domain count for an availability set that uses Managed Disks?**

Depending on the region where the availability set that uses Managed Disks is located, the supported fault domain count is 2 or 3.

## **How is the standard storage account for diagnostics set up?**

You set up a private storage account for VM diagnostics.

## **What kind of Role-Based Access Control support is available for Managed Disks?**

Managed Disks supports three key default roles:

- Owner: Can manage everything, including access
- Contributor: Can manage everything except access
- Reader: Can view everything, but can't make changes

## **Is there a way that I can copy or export a managed disk to a private storage account?**

You can generate a read-only shared access signature (SAS) URI for the managed disk and use it to copy the contents to a private storage account or on-premises storage. You can use the SAS URI using the Azure portal, Azure PowerShell, the Azure CLI, or [AzCopy](#)

## **Can I create a copy of my managed disk?**

Customers can take a snapshot of their managed disks and then use the snapshot to create another managed disk.

## **Are unmanaged disks still supported?**

Yes, both unmanaged and managed disks are supported. We recommend that you use managed disks for new workloads and migrate your current workloads to managed disks.

## **Can I co-locate unmanaged and managed disks on the same VM?**

No.

## **If I create a 128-GB disk and then increase the size to 130 gibibytes (GiB), will I be charged for the next disk size (256 GiB)?**

Yes.

## **Can I create locally redundant storage, geo-redundant storage, and zone-redundant storage managed disks?**

Azure Managed Disks currently supports only locally redundant storage managed disks.

## **Can I shrink or downsize my managed disks?**

No. This feature is not supported currently.

## **Can I break a lease on my disk?**

No. This is not supported currently as a lease is present to prevent accidental deletion when the disk is being used.

## **Can I change the computer name property when a specialized (not created by using the System Preparation tool or generalized) operating system disk is used to provision a VM?**

No. You can't update the computer name property. The new VM inherits it from the parent VM, which was used to create the operating system disk.

## **Where can I find sample Azure Resource Manager templates to create VMs with managed disks?**

- [List of templates using Managed Disks](#)
- <https://github.com/chagarw/MDPP>

## **When creating a disk from a blob, is there any continually existing relationship with that source blob?**

No, when the new disk is created it is a full standalone copy of that blob at that time and there is no connection between the two. If you like, once you've created the disk, the source blob may be deleted without affecting the newly created disk in any way.

## **Can I rename a managed or unmanaged disk after it has been created?**

For managed disks you cannot rename them. However, you may rename an unmanaged disk as long as it is not currently attached to a VHD or VM.

## **Can I use GPT partitioning on an Azure Disk?**

Generation 1 images can only use GPT partitioning on data disks, not OS disks. OS disks must use the MBR partition style.

[Generation 2 images](#) can use GPT partitioning on the OS disk as well as the data disks.

## **What disk types support snapshots?**

Premium SSD, standard SSD, and standard HDD support snapshots. For these three disk types, snapshots are supported for all disk sizes (including disks up to 32 TiB in size). Ultra disks do not support snapshots.

**What are Azure disk reservations?** Disk reservation is the option to purchase one year of disk storage in advance, reducing your total cost. For details regarding Azure disk reservations, see our article on the subject: [Understand how your reservation discount is applied to Azure Disk](#).

**What options does Azure disk reservation offer?** Azure disk reservation provides the option to purchase Premium SSDs in the specified SKUs from P30 (1 TiB) up to P80 (32 TiB) for a one-year term. There is no limitation on the minimum amount of disks necessary to purchase a disk reservation. Additionally, you can choose to pay with a single, upfront payment or monthly payments. There is no additional transactional cost applied for Premium SSD Managed Disks.

Reservations are made in the form of disks, not capacity. In other words, when you reserve a P80 (32 TiB) disk, you get a single P80 disk, you cannot then divide that specific reservation up into two smaller P70 (16 TiB) disks. You can, of course, reserve as many or as few disks as you like, including two separate P70 (16 TiB) disks.

**How is Azure disk reservation applied?** Disks reservation follows a model similar to reserved virtual machine (VM) instances. The difference being that a disk reservation cannot be applied to different SKUs, while a VM instance can. See [Save costs with Azure Reserved VM Instances](#) for more information on VM instances.

**Can I use my data storage purchased through Azure disks reservation across multiple regions?** Azure disks reservation are purchased for a specific region and SKU (like P30 in East US 2), and therefore cannot be used outside these constructs. You can always purchase an additional Azure Disks Reservation for your disk storage needs in other regions or SKUs.

**What happens when my Azure disks reservation expires?** You will receive email notifications 30 days prior to expiration and again on the expiration date. Once the reservation expires, deployed disks will continue to run and will be billed with the latest [pay-as-you-go rates](#).

## Azure shared disks

### Is the shared disks feature supported for unmanaged disks or page blobs?

No, it is only supported for premium SSD managed disks.

### What regions support shared disks?

Currently only West Central US.

### Can shared disks be used as an OS disk?

No, shared disks are only supported for data disks.

### What disk sizes support shared disks?

Only premium SSDs that are P15 or greater support shared disks.

### If I have an existing premium SSD, can I enable shared disks on it?

All managed disks created with API version 2019-07-01 or higher can enable shared disks. To do this, you need to unmount the disk from all VMs that it is attached to. Next, edit the `maxShares` property on the disk.

### If I no longer want to use a disk in shared mode, how do I disable it?

Unmount the disk from all VMs that it is attached to. Then edit the `maxShare` property on the disk to 1.

### Can you resize a shared disk?

Yes.

### Can I enable write accelerator on a disk that also has shared disks enabled?

No.

### Can I enable host caching for a disk that has shared disk enabled?

The only supported host caching option is 'None'.

## Ultra disks

**What should I set my ultra disk throughput to?** If you are unsure what to set your disk throughput to, we recommend you start by assuming an IO size of 16 KiB and adjust the performance from there as you monitor your application. The formula is: Throughput in MBps = # of IOPS \* 16 / 1000.

**I configured my disk to 40000 IOPS but I'm only seeing 12800 IOPS, why am I not seeing the performance of the disk?** In addition to the disk throttle, there is an IO throttle that gets imposed at the VM level. Please ensure that the VM size you are using can support the levels that are configured on your disks. For details regarding IO limits imposed by your VM, see [Sizes for Windows virtual machines in Azure](#).

**Can I use caching levels with an ultra disk?** No, ultra disks do not support the different caching methods that are supported on other disk types. Set the disk caching to None.

**Can I attach an ultra disk to my existing VM?** Maybe, your VM has to be in a region and availability zone pair that supports Ultra disks. See [getting started with ultra disks](#) for details.

**Can I use an ultra disk as the OS disk for my VM?** No, ultra Disks are only supported as data disks and are only supported as 4K native disks.

**Can I convert an existing disk to an ultra disk?** No, but you can migrate the data from an existing disk to an ultra disk. To migrate an existing disk to an ultra Disk, attach both disks to the same VM, and copy the disk's data from one disk to the other or leverage a 3rd party solution for data migration.

**Can I create snapshots for ultra disks?** No, snapshots are not yet available.

**Is Azure Backup available for ultra disks?** No, Azure Backup support is not yet available.

**Can I attach an ultra disk to a VM running in an availability set?** No, this is not yet supported.

**Can I enable Azure Site Recovery for VMs using ultra disks?** No, Azure Site Recovery is not yet supported for ultra disks.

## Uploading to a managed disk

**Can I upload data to an existing managed disk?**

No, upload can only be used during the creation of a new empty disk with the **ReadyToUpload** state.

**How do I upload to a managed disk?**

Create a managed disk with the `createOption` property of `creationData` set to "Upload", then you can upload data to it.

**Can I attach a disk to a VM while it is in an upload state?**

No.

**Can I take a snapshot of a manged disk in an upload state?**

No.

## Standard SSD disks

**What are Azure Standard SSD disks?** Standard SSD disks are standard disks backed by solid-state media, optimized as cost effective storage for workloads that need consistent performance at lower IOPS levels.

**What are the regions currently supported for Standard SSD disks?** All Azure regions now support Standard SSD disks.

**Is Azure Backup available when using Standard SSDs?** Yes, Azure Backup is now available.

**How do I create Standard SSD disks?** You can create Standard SSD disks using Azure Resource Manager templates, SDK, PowerShell, or CLI. Below are the parameters needed in the Resource Manager template to create Standard SSD Disks:

- `apiVersion` for Microsoft.Compute must be set as `2018-04-01` (or later)
- Specify `managedDisk.storageAccountType` as `StandardSSD_LRS`

The following example shows the `properties.storageProfile.osDisk` section for a VM that uses Standard SSD Disks:

```
"osDisk": {
 "osType": "Windows",
 "name": "myOsDisk",
 "caching": "ReadWrite",
 "createOption": "FromImage",
 "managedDisk": {
 "storageAccountType": "StandardSSD_LRS"
 }
}
```

For a complete template example of how to create a Standard SSD disk with a template, see [Create a VM from a Windows Image with Standard SSD Data Disks](#).

**Can I convert my existing disks to Standard SSD?** Yes, you can. Refer to [Convert Azure managed disks storage](#)

from standard to premium, and vice versa for the general guidelines for converting Managed Disks. And, use the following value to update the disk type to Standard SSD. -AccountType StandardSSD\_LRS

**What is the benefit of using Standard SSD disks instead of HDD?** Standard SSD disks deliver better latency, consistency, availability, and reliability compared to HDD disks. Application workloads run a lot more smoothly on Standard SSD because of that. Note, Premium SSD disks are the recommended solution for most IO-intensive production workloads.

**Can I use Standard SSDs as Unmanaged Disks?** No, Standard SSDs disks are only available as Managed Disks.

**Do Standard SSD Disks support "single instance VM SLA"?** No, Standard SSDs do not have single instance VM SLA. Use Premium SSD disks for single instance VM SLA.

## Migrate to Managed Disks

### **Is there any impact of migration on the Managed Disks performance?**

Migration involves movement of the Disk from one Storage location to another. This is orchestrated via background copy of data, which can take several hours to complete, typically less than 24 Hrs depending on the amount of data in the disks. During that time your application can experience higher than usual read latency as some reads can get redirected to the original location, and can take longer to complete. There is no impact on write latency during this period.

### **What changes are required in a pre-existing Azure Backup service configuration prior/after migration to Managed Disks?**

No changes are required.

### **Will my VM backups created via Azure Backup service before the migration continue to work?**

Yes, backups work seamlessly.

### **What changes are required in a pre-existing Azure Disks Encryption configuration prior/after migration to Managed Disks?**

No changes are required.

### **Is automated migration of an existing virtual machine scale set from unmanaged disks to Managed Disks supported?**

No. You can create a new scale set with Managed Disks using the image from your old scale set with unmanaged disks.

### **Can I create a Managed Disk from a page blob snapshot taken before migrating to Managed Disks?**

No. You can export a page blob snapshot as a page blob and then create a Managed Disk from the exported page blob.

### **Can I fail over my on-premises machines protected by Azure Site Recovery to a VM with Managed Disks?**

Yes, you can choose to failover to a VM with Managed Disks.

### **Is there any impact of migration on Azure VMs protected by Azure Site Recovery via Azure to Azure replication?**

No. Azure Site Recovery Azure to Azure protection for VMs with Managed Disks is available.

### **Can I migrate VMs with unmanaged disks that are located on storage accounts that are or were previously encrypted to managed disks?**

Yes

## Managed Disks and Storage Service Encryption

### **Is Azure Storage Service Encryption enabled by default when I create a managed disk?**

Yes.

### **Is the boot volume encrypted by default on a managed disk?**

Yes. By default, all managed disks are encrypted, including the OS disk.

### **Who manages the encryption keys?**

Microsoft manages the encryption keys.

### **Can I disable Storage Service Encryption for my managed disks?**

No.

### **Is Storage Service Encryption only available in specific regions?**

No. It's available in all the regions where Managed Disks are available. Managed Disks is available in all public regions and Germany. It is also available in China, however, only for Microsoft managed keys, not customer managed keys.

### **How can I find out if my managed disk is encrypted?**

You can find out the time when a managed disk was created from the Azure portal, the Azure CLI, and PowerShell. If the time is after June 9, 2017, then your disk is encrypted.

### **How can I encrypt my existing disks that were created before June 10, 2017?**

As of June 10, 2017, new data written to existing managed disks is automatically encrypted. We are also planning to encrypt existing data, and the encryption will happen asynchronously in the background. If you must encrypt existing data now, create a copy of your disk. New disks will be encrypted.

- [Copy managed disks by using the Azure CLI](#)
- [Copy managed disks by using PowerShell](#)

### **Are managed snapshots and images encrypted?**

Yes. All managed snapshots and images created after June 9, 2017, are automatically encrypted.

### **Can I convert VMs with unmanaged disks that are located on storage accounts that are or were previously encrypted to managed disks?**

Yes

### **Will an exported VHD from a managed disk or a snapshot also be encrypted?**

No. But if you export a VHD to an encrypted storage account from an encrypted managed disk or snapshot, then it's encrypted.

## Premium disks: Managed and unmanaged

### **If a VM uses a size series that supports Premium SSD disks, such as a DSv2, can I attach both premium and standard data disks?**

Yes.

### **Can I attach both premium and standard data disks to a size series that doesn't support Premium SSD**

## **disks, such as D, Dv2, G, or F series?**

No. You can attach only standard data disks to VMs that don't use a size series that supports Premium SSD disks.

## **If I create a premium data disk from an existing VHD that was 80 GB, how much will that cost?**

A premium data disk created from an 80-GB VHD is treated as the next-available premium disk size, which is a P10 disk. You're charged according to the P10 disk pricing.

## **Are there transaction costs to use Premium SSD disks?**

There is a fixed cost for each disk size, which comes provisioned with specific limits on IOPS and throughput. The other costs are outbound bandwidth and snapshot capacity, if applicable. For more information, see the [pricing page](#).

## **What are the limits for IOPS and throughput that I can get from the disk cache?**

The combined limits for cache and local SSD for a DS series are 4,000 IOPS per core and 33 MiB per second per core. The GS series offers 5,000 IOPS per core and 50 MiB per second per core.

## **Is the local SSD supported for a Managed Disks VM?**

The local SSD is temporary storage that is included with a Managed Disks VM. There is no extra cost for this temporary storage. We recommend that you do not use this local SSD to store your application data because it isn't persisted in Azure Blob storage.

## **Are there any repercussions for the use of TRIM on premium disks?**

There is no downside to the use of TRIM on Azure disks on either premium or standard disks.

# New disk sizes: Managed and unmanaged

## **What regions support bursting capability for applicable premium SSD disk size?**

The bursting capability is currently supported in Azure West Central US.

## **What regions are 4/8/16 GiB Managed Disk sizes (P1/P2/P3, E1/E2/E3) supported in?**

These new disk sizes are currently supported in Azure West Central US.

## **Are P1/P2/P3 disk sizes supported for unmanaged disks or page blobs?**

No, it is only supported on premium SSD managed disks.

## **Are E1/E2/E3 disk sizes supported for unmanaged disks or page blobs?**

No, standard SSD managed disks of any size cannot be used with unmanaged disks or page blobs.

## **What is the largest Managed disk size supported for operating system and data disks?**

The partition type that Azure supports for an operating system disk is the master boot record (MBR). The MBR format supports a disk size up to 2 TiB. The largest size that Azure supports for an operating system disk is 2 TiB. Azure supports up to 32 TiB for managed data disks.

## **What is the largest Unmanaged Disk size supported for operating system and data disks?**

The partition type that Azure supports for an operating system disk is the master boot record (MBR). The MBR format supports a disk size up to 2 TiB. The largest size that Azure supports for an operating system Unmanaged disk is 2 TiB. Azure supports up to 4 TiB for data Unmanaged disks.

## **What is the largest page blob size that's supported?**

The largest page blob size that Azure supports is 8 TiB (8,191 GiB). The maximum page blob size when attached to

a VM as data or operating system disks is 4 TiB (4,095 GiB).

## **Do I need to use a new version of Azure tools to create, attach, resize, and upload disks larger than 1 TiB?**

You don't need to upgrade your existing Azure tools to create, attach, or resize disks larger than 1 TiB. To upload your VHD file from on-premises directly to Azure as a page blob or unmanaged disk, you need to use the latest tool sets listed below. We only support VHD uploads of up to 8 TiB.

| AZURE TOOLS      | SUPPORTED VERSIONS                                |
|------------------|---------------------------------------------------|
| Azure PowerShell | Version number 4.1.0: June 2017 release or later  |
| Azure CLI v1     | Version number 0.10.13: May 2017 release or later |
| Azure CLI v2     | Version number 2.0.12: July 2017 release or later |
| AzCopy           | Version number 6.1.0: June 2017 release or later  |

## **Are P4 and P6 disk sizes supported for unmanaged disks or page blobs?**

P4 (32 GiB) and P6 (64 GiB) disk sizes are not supported as the default disk tiers for unmanaged disks and page blobs. You need to explicitly [set the Blob Tier](#) to P4 and P6 to have your disk mapped to these tiers. If you deploy a unmanaged disk or page blob with the disk size or content length less than 32 GiB or between 32 GiB to 64 GiB without setting the Blob Tier, you will continue to land on P10 with 500 IOPS and 100 MiB/s and the mapped pricing tier.

## **If my existing premium managed disk less than 64 GiB was created before the small disk was enabled (around June 15, 2017), how is it billed?**

Existing small premium disks less than 64 GiB continue to be billed according to the P10 pricing tier.

## **How can I switch the disk tier of small premium disks less than 64 GiB from P10 to P4 or P6?**

You can take a snapshot of your small disks and then create a disk to automatically switch the pricing tier to P4 or P6 based on the provisioned size.

## **Can you resize existing Managed Disks from sizes fewer than 4 tebibytes (TiB) to new newly introduced disk sizes up to 32 TiB?**

Yes.

## **What are the largest disk sizes supported by Azure Backup and Azure Site Recovery service?**

The largest disk size supported by Azure Backup is 32 TiB (4 TiB for encrypted disks). The largest disk size supported by Azure Site Recovery is 8 TiB. Support for the larger disks up to 32 TiB is not yet available in Azure Site Recovery.

## **What are the recommended VM sizes for larger disk sizes (>4 TiB) for Standard SSD and Standard HDD disks to achieve optimized disk IOPS and Bandwidth?**

To achieve the disk throughput of Standard SSD and Standard HDD large disk sizes (>4 TiB) beyond 500 IOPS and 60 MiB/s, we recommend you deploy a new VM from one of the following VM sizes to optimize your performance: B-series, DSv2-series, Dsv3-Series, ESv3-Series, Fs-series, Fsv2-series, M-series, GS-series, NCv2-series, NCv3-series, or Ls-series VMs. Attaching large disks to existing VMs or VMs that are not using the recommended sizes above may experience lower performance.

## **How can I upgrade my disks (>4 TiB) which were deployed during the larger disk sizes preview in order to get the higher IOPS & bandwidth at GA?**

You can either stop and start the VM that the disk is attached to or, detach and re-attach your disk. The performance targets of larger disk sizes have been increased for both premium SSDs and standard SSDs at GA.

### **What regions are the managed disk sizes of 8 TiB, 16 TiB, and 32 TiB supported in?**

The 8 TiB, 16 TiB, and 32 TiB disk SKUs are supported in all regions under global Azure, Microsoft Azure Government, and Azure China 21Vianet.

### **Do we support enabling Host Caching on all disk sizes?**

We support Host Caching of ReadOnly and Read/Write on disk sizes less than 4 TiB. For disk sizes more than 4 TiB, we don't support setting caching option other than None. We recommend leveraging caching for smaller disk sizes where you can expect to observe better performance boost with data cached to the VM.

## **What if my question isn't answered here?**

If your question isn't listed here, let us know and we'll help you find an answer. You can post a question at the end of this article in the comments. To engage with the Azure Storage team and other community members about this article, use the MSDN [Azure Storage forum](#).

To request features, submit your requests and ideas to the [Azure Storage feedback forum](#).

2 minutes to read

# Open ports and endpoints to a Linux VM with the Azure CLI

12/23/2019 • 2 minutes to read • [Edit Online](#)

You open a port, or create an endpoint, to a virtual machine (VM) in Azure by creating a network filter on a subnet or VM network interface. You place these filters, which control both inbound and outbound traffic, on a Network Security Group attached to the resource that receives the traffic. Let's use a common example of web traffic on port 80. This article shows you how to open a port to a VM with the Azure CLI.

To create a Network Security Group and rules you need the latest [Azure CLI](#) installed and logged in to an Azure account using [az login](#).

In the following examples, replace example parameter names with your own values. Example parameter names include *myResourceGroup*, *myNetworkSecurityGroup*, and *myVnet*.

## Quickly open a port for a VM

If you need to quickly open a port for a VM in a dev/test scenario, you can use the [az vm open-port](#) command. This command creates a Network Security Group, adds a rule, and applies it to a VM or subnet. The following example opens port 80 on the VM named *myVM* in the resource group named *myResourceGroup*.

```
az vm open-port --resource-group myResourceGroup --name myVM --port 80
```

For more control over the rules, such as defining a source IP address range, continue with the additional steps in this article.

## Create a Network Security Group and rules

Create the network security group with [az network nsg create](#). The following example creates a network security group named *myNetworkSecurityGroup* in the *eastus* location:

```
az network nsg create \
--resource-group myResourceGroup \
--location eastus \
--name myNetworkSecurityGroup
```

Add a rule with [az network nsg rule create](#) to allow HTTP traffic to your webserver (or adjust for your own scenario, such as SSH access or database connectivity). The following example creates a rule named *myNetworkSecurityGroupRule* to allow TCP traffic on port 80:

```
az network nsg rule create \
--resource-group myResourceGroup \
--nsg-name myNetworkSecurityGroup \
--name myNetworkSecurityGroupRule \
--protocol tcp \
--priority 1000 \
--destination-port-range 80
```

## Apply Network Security Group to VM

Associate the Network Security Group with your VM's network interface (NIC) with [az network nic update](#). The following example associates an existing NIC named *myNic* with the Network Security Group named *myNetworkSecurityGroup*:

```
az network nic update \
--resource-group myResourceGroup \
--name myNic \
--network-security-group myNetworkSecurityGroup
```

Alternatively, you can associate your Network Security Group with a virtual network subnet with [az network vnet subnet update](#) rather than just to the network interface on a single VM. The following example associates an existing subnet named *mySubnet* in the *myVnet* virtual network with the Network Security Group named *myNetworkSecurityGroup*:

```
az network vnet subnet update \
--resource-group myResourceGroup \
--vnet-name myVnet \
--name mySubnet \
--network-security-group myNetworkSecurityGroup
```

## More information on Network Security Groups

The quick commands here allow you to get up and running with traffic flowing to your VM. Network Security Groups provide many great features and granularity for controlling access to your resources. You can read more about [creating a Network Security Group and ACL rules here](#).

For highly available web applications, you should place your VMs behind an Azure Load Balancer. The load balancer distributes traffic to VMs, with a Network Security Group that provides traffic filtering. For more information, see [How to load balance Linux virtual machines in Azure to create a highly available application](#).

## Next steps

In this example, you created a simple rule to allow HTTP traffic. You can find information on creating more detailed environments in the following articles:

- [Azure Resource Manager overview](#)
- [What is a Network Security Group \(NSG\)?](#)

# Create a virtual machine with a static public IP address using the Azure CLI

1/16/2020 • 2 minutes to read • [Edit Online](#)

You can create a virtual machine with a static public IP address. A public IP address enables you to communicate to a virtual machine from the internet. Assign a static public IP address, rather than a dynamic address, to ensure that the address never changes. Learn more about [static public IP addresses](#). To change a public IP address assigned to an existing virtual machine from dynamic to static, or to work with private IP addresses, see [Add, change, or remove IP addresses](#). Public IP addresses have a [nominal charge](#), and there is a [limit](#) to the number of public IP addresses that you can use per subscription.

## Create a virtual machine

You can complete the following steps from your local computer or by using the Azure Cloud Shell. To use your local computer, ensure you have the [Azure CLI installed](#). To use the Azure Cloud Shell, select **Try It** in the top right corner of any command box that follows. The Cloud Shell signs you into Azure.

1. If using the Cloud Shell, skip to step 2. Open a command session and sign into Azure with `az login`.
2. Create a resource group with the `az group create` command. The following example creates a resource group in the East US Azure region:

```
az group create --name myResourceGroup --location eastus
```

3. Create a virtual machine with the `az vm create` command. The `--public-ip-address-allocation=static` option assigns a static public IP address to the virtual machine. The following example creates an Ubuntu virtual machine with a static, basic SKU public IP address named *myPublicIpAddress*:

```
az vm create \
 --resource-group myResourceGroup \
 --name myVM \
 --image UbuntuLTS \
 --admin-username azureuser \
 --generate-ssh-keys \
 --public-ip-address myPublicIpAddress \
 --public-ip-address-allocation static
```

If the public IP address must be a standard SKU, add `--public-ip-sku Standard` to the previous command. Learn more about [Public IP address SKUs](#). If the virtual machine will be added to the back-end pool of a public Azure Load Balancer, the SKU of the virtual machine's public IP address must match the SKU of the load balancer's public IP address. For details, see [Azure Load Balancer](#).

4. View the public IP address assigned and confirm that it was created as a static, basic SKU address, with `az network public-ip show`:

```
az network public-ip show \
 --resource-group myResourceGroup \
 --name myPublicIpAddress \
 --query [ipAddress,publicIpAllocationMethod,sku] \
 --output table
```

Azure assigned a public IP address from addresses used in the region you created the virtual machine in. You can download the list of ranges (prefixes) for the Azure [Public](#), [US government](#), [China](#), and [Germany](#) clouds.

#### WARNING

Do not modify the IP address settings within the virtual machine's operating system. The operating system is unaware of Azure public IP addresses. Though you can add private IP address settings to the operating system, we recommend not doing so unless necessary, and not until after reading [Add a private IP address to an operating system](#).

## Clean up resources

When no longer needed, you can use `az group delete` to remove the resource group and all of the resources it contains:

```
az group delete --name myResourceGroup --yes
```

## Next steps

- Learn more about [public IP addresses](#) in Azure
- Learn more about all [public IP address settings](#)
- Learn more about [private IP addresses](#) and assigning a [static private IP address](#) to an Azure virtual machine
- Learn more about creating [Linux](#) and [Windows](#) virtual machines

# How to create a Linux virtual machine in Azure with multiple network interface cards

12/23/2019 • 6 minutes to read • [Edit Online](#)

This article details how to create a VM with multiple NICs with the Azure CLI.

## Create supporting resources

Install the latest [Azure CLI](#) and log in to an Azure account using [az login](#).

In the following examples, replace example parameter names with your own values. Example parameter names included *myResourceGroup*, *mystorageaccount*, and *myVM*.

First, create a resource group with [az group create](#). The following example creates a resource group named *myResourceGroup* in the *eastus* location:

```
az group create --name myResourceGroup --location eastus
```

Create the virtual network with [az network vnet create](#). The following example creates a virtual network named *myVnet* and subnet named *mySubnetFrontEnd*:

```
az network vnet create \
 --resource-group myResourceGroup \
 --name myVnet \
 --address-prefix 10.0.0.0/16 \
 --subnet-name mySubnetFrontEnd \
 --subnet-prefix 10.0.1.0/24
```

Create a subnet for the back-end traffic with [az network vnet subnet create](#). The following example creates a subnet named *mySubnetBackEnd*:

```
az network vnet subnet create \
 --resource-group myResourceGroup \
 --vnet-name myVnet \
 --name mySubnetBackEnd \
 --address-prefix 10.0.2.0/24
```

Create a network security group with [az network nsg create](#). The following example creates a network security group named *myNetworkSecurityGroup*:

```
az network nsg create \
 --resource-group myResourceGroup \
 --name myNetworkSecurityGroup
```

## Create and configure multiple NICs

Create two NICs with [az network nic create](#). The following example creates two NICs, named *myNic1* and *myNic2*, connected the network security group, with one NIC connecting to each subnet:

```
az network nic create \
--resource-group myResourceGroup \
--name myNic1 \
--vnet-name myVnet \
--subnet mySubnetFrontEnd \
--network-security-group myNetworkSecurityGroup
az network nic create \
--resource-group myResourceGroup \
--name myNic2 \
--vnet-name myVnet \
--subnet mySubnetBackEnd \
--network-security-group myNetworkSecurityGroup
```

## Create a VM and attach the NICs

When you create the VM, specify the NICs you created with `--nics`. You also need to take care when you select the VM size. There are limits for the total number of NICs that you can add to a VM. Read more about [Linux VM sizes](#).

Create a VM with [az vm create](#). The following example creates a VM named *myVM*:

```
az vm create \
--resource-group myResourceGroup \
--name myVM \
--image UbuntuLTS \
--size Standard_DS3_v2 \
--admin-username azureuser \
--generate-ssh-keys \
--nics myNic1 myNic2
```

Add routing tables to the guest OS by completing the steps in [Configure the guest OS for multiple NICs](#).

## Add a NIC to a VM

The previous steps created a VM with multiple NICs. You can also add NICs to an existing VM with the Azure CLI. Different [VM sizes](#) support a varying number of NICs, so size your VM accordingly. If needed, you can [resize a VM](#).

Create another NIC with [az network nic create](#). The following example creates a NIC named *myNic3* connected to the back-end subnet and network security group created in the previous steps:

```
az network nic create \
--resource-group myResourceGroup \
--name myNic3 \
--vnet-name myVnet \
--subnet mySubnetBackEnd \
--network-security-group myNetworkSecurityGroup
```

To add a NIC to an existing VM, first deallocate the VM with [az vm deallocate](#). The following example deallocates the VM named *myVM*:

```
az vm deallocate --resource-group myResourceGroup --name myVM
```

Add the NIC with [az vm nic add](#). The following example adds *myNic3* to *myVM*:

```
az vm nic add \
--resource-group myResourceGroup \
--vm-name myVM \
--nics myNic3
```

Start the VM with [az vm start](#):

```
az vm start --resource-group myResourceGroup --name myVM
```

Add routing tables to the guest OS by completing the steps in [Configure the guest OS for multiple NICs](#).

## Remove a NIC from a VM

To remove a NIC from an existing VM, first deallocate the VM with [az vm deallocate](#). The following example deallocates the VM named *myVM*:

```
az vm deallocate --resource-group myResourceGroup --name myVM
```

Remove the NIC with [az vm nic remove](#). The following example removes *myNic3* from *myVM*:

```
az vm nic remove \
--resource-group myResourceGroup \
--vm-name myVM \
--nics myNic3
```

Start the VM with [az vm start](#):

```
az vm start --resource-group myResourceGroup --name myVM
```

## Create multiple NICs using Resource Manager templates

Azure Resource Manager templates use declarative JSON files to define your environment. You can read an [overview of Azure Resource Manager](#). Resource Manager templates provide a way to create multiple instances of a resource during deployment, such as creating multiple NICs. You use *copy* to specify the number of instances to create:

```
"copy": {
 "name": "multiplenics",
 "count": "[parameters('count')]"
}
```

Read more about [creating multiple instances using copy](#).

You can also use a `copyIndex()` to then append a number to a resource name, which allows you to create `myNic1`, `myNic2`, etc. The following shows an example of appending the index value:

```
"name": "[concat('myNic', copyIndex())]",
```

You can read a complete example of [creating multiple NICs using Resource Manager templates](#).

Add routing tables to the guest OS by completing the steps in [Configure the guest OS for multiple NICs](#).

# Configure guest OS for multiple NICs

The previous steps created a virtual network and subnet, attached NICs, then created a VM. A public IP address and network security group rules that allow SSH traffic were not created. To configure the guest OS for multiple NICs, you need to allow remote connections and run commands locally on the VM.

To allow SSH traffic, create a network security group rule with [az network nsg rule create](#) as follows:

```
az network nsg rule create \
 --resource-group myResourceGroup \
 --nsg-name myNetworkSecurityGroup \
 --name allow_ssh \
 --priority 101 \
 --destination-port-ranges 22
```

Create a public IP address with [az network public-ip create](#) and assign it to the first NIC with [az network nic ip-config update](#):

```
az network public-ip create --resource-group myResourceGroup --name myPublicIP

az network nic ip-config update \
 --resource-group myResourceGroup \
 --nic-name myNic1 \
 --name ipconfig1 \
 --public-ip myPublicIP
```

To view the public IP address of the VM, use [az vm show](#) as follows::

```
az vm show --resource-group myResourceGroup --name myVM -d --query publicIps -o tsv
```

Now SSH to the public IP address of your VM. The default username provided in a previous step was *azureuser*. Provide your own username and public IP address:

```
ssh azureuser@137.117.58.232
```

To send to or from a secondary network interface, you have to manually add persistent routes to the operating system for each secondary network interface. In this article, *eth1* is the secondary interface. Instructions for adding persistent routes to the operating system vary by distro. See documentation for your distro for instructions.

When adding the route to the operating system, the gateway address is *.1* for whichever subnet the network interface is in. For example, if the network interface is assigned the address *10.0.2.4*, the gateway you specify for the route is *10.0.2.1*. You can define a specific network for the route's destination, or specify a destination of *0.0.0.0*, if you want all traffic for the interface to go through the specified gateway. The gateway for each subnet is managed by the virtual network.

Once you've added the route for a secondary interface, verify that the route is in your route table with [route -n](#). The following example output is for the route table that has the two network interfaces added to the VM in this article:

| Kernel IP routing table |          |                 |       |        |     |     |       |
|-------------------------|----------|-----------------|-------|--------|-----|-----|-------|
| Destination             | Gateway  | Genmask         | Flags | Metric | Ref | Use | Iface |
| 0.0.0.0                 | 10.0.1.1 | 0.0.0.0         | UG    | 0      | 0   | 0   | eth0  |
| 0.0.0.0                 | 10.0.2.1 | 0.0.0.0         | UG    | 0      | 0   | 0   | eth1  |
| 10.0.1.0                | 0.0.0.0  | 255.255.255.0   | U     | 0      | 0   | 0   | eth0  |
| 10.0.2.0                | 0.0.0.0  | 255.255.255.0   | U     | 0      | 0   | 0   | eth1  |
| 168.63.129.16           | 10.0.1.1 | 255.255.255.255 | UGH   | 0      | 0   | 0   | eth0  |
| 169.254.169.254         | 10.0.1.1 | 255.255.255.255 | UGH   | 0      | 0   | 0   | eth0  |

Confirm that the route you added persists across reboots by checking your route table again after a reboot. To test connectivity, you can enter the following command, for example, where *eth1* is the name of a secondary network interface:

```
ping bing.com -c 4 -I eth1
```

## Next steps

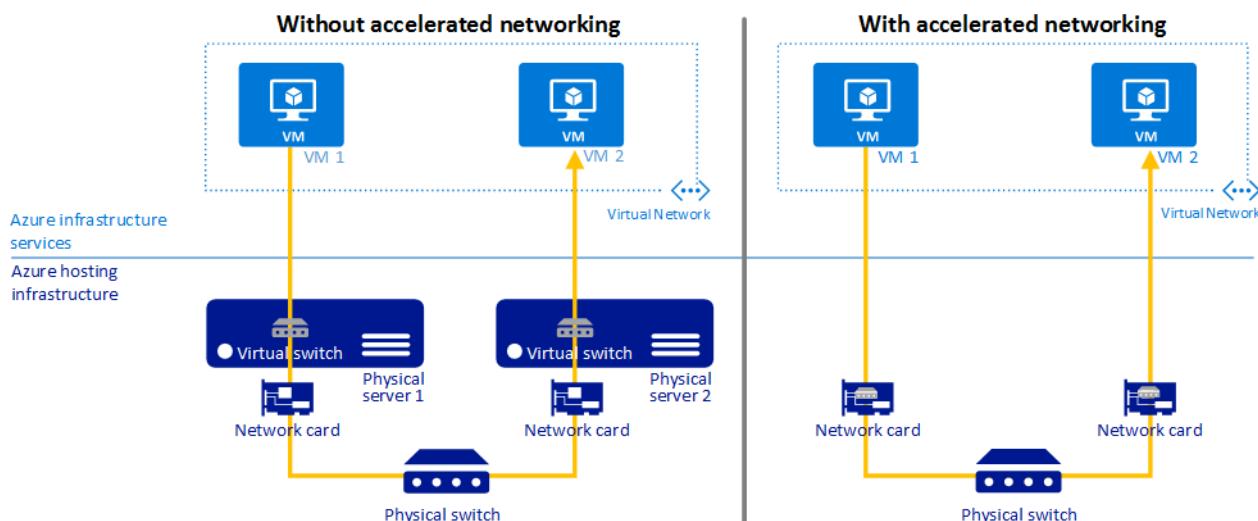
Review [Linux VM sizes](#) when trying to creating a VM with multiple NICs. Pay attention to the maximum number of NICs each VM size supports.

To further secure your VMs, use just in time VM access. This feature opens network security group rules for SSH traffic when needed, and for a defined period of time. For more information, see [Manage virtual machine access using just in time](#).

# Create a Linux virtual machine with Accelerated Networking using Azure CLI

12/3/2019 • 10 minutes to read • [Edit Online](#)

In this tutorial, you learn how to create a Linux virtual machine (VM) with Accelerated Networking. To create a Windows VM with Accelerated Networking, see [Create a Windows VM with Accelerated Networking](#). Accelerated networking enables single root I/O virtualization (SR-IOV) to a VM, greatly improving its networking performance. This high-performance path bypasses the host from the datapath, reducing latency, jitter, and CPU utilization, for use with the most demanding network workloads on supported VM types. The following picture shows communication between two VMs with and without accelerated networking:



Without accelerated networking, all networking traffic in and out of the VM must traverse the host and the virtual switch. The virtual switch provides all policy enforcement, such as network security groups, access control lists, isolation, and other network virtualized services to network traffic. To learn more about virtual switches, read the [Hyper-V network virtualization and virtual switch](#) article.

With accelerated networking, network traffic arrives at the virtual machine's network interface (NIC), and is then forwarded to the VM. All network policies that the virtual switch applies are now offloaded and applied in hardware. Applying policy in hardware enables the NIC to forward network traffic directly to the VM, bypassing the host and the virtual switch, while maintaining all the policy it applied in the host.

The benefits of accelerated networking only apply to the VM that it is enabled on. For the best results, it is ideal to enable this feature on at least two VMs connected to the same Azure virtual network (VNet). When communicating across VNets or connecting on-premises, this feature has minimal impact to overall latency.

## Benefits

- **Lower Latency / Higher packets per second (pps):** Removing the virtual switch from the datapath removes the time packets spend in the host for policy processing and increases the number of packets that can be processed inside the VM.
- **Reduced jitter:** Virtual switch processing depends on the amount of policy that needs to be applied and the workload of the CPU that is doing the processing. Offloading the policy enforcement to the hardware removes that variability by delivering packets directly to the VM, removing the host to VM communication and all software interrupts and context switches.
- **Decreased CPU utilization:** Bypassing the virtual switch in the host leads to less CPU utilization for

processing network traffic.

## Supported operating systems

The following distributions are supported out of the box from the Azure Gallery:

- **Ubuntu 14.04 with the linux-azure kernel**
- **Ubuntu 16.04 or later**
- **SLES12 SP3 or later**
- **RHEL 7.4 or later**
- **CentOS 7.4 or later**
- **CoreOS Linux**
- **Debian "Stretch" with backports kernel**
- **Oracle Linux 7.4 and later with Red Hat Compatible Kernel (RHCK)**
- **Oracle Linux 7.5 and later with UEK version 5**
- **FreeBSD 10.4, 11.1 & 12.0**

## Limitations and Constraints

### Supported VM instances

Accelerated Networking is supported on most general purpose and compute-optimized instance sizes with 2 or more vCPUs. These supported series are: D/DSv2 and F/Fs

On instances that support hyperthreading, Accelerated Networking is supported on VM instances with 4 or more vCPUs. Supported series are: D/Dsv3, E/Esv3, Fsv2, Lsv2, Ms/Mms and Ms/Mmsv2.

For more information on VM instances, see [Linux VM sizes](#).

### Custom Images

If you are using a custom image, and your image supports Accelerated Networking, please make sure to have the required drivers to work with Mellanox ConnectX-3 and ConnectX-4 Lx NICs on Azure.

### Regions

Available in all public Azure regions as well as Azure Government Clouds.

### Enabling Accelerated Networking on a running VM

A supported VM size without accelerated networking enabled can only have the feature enabled when it is stopped and deallocated.

### Deployment through Azure Resource Manager

Virtual machines (classic) cannot be deployed with Accelerated Networking.

## Create a Linux VM with Azure Accelerated Networking

### Portal creation

Though this article provides steps to create a virtual machine with accelerated networking using the Azure CLI, you can also [create a virtual machine with accelerated networking using the Azure portal](#). When creating a virtual machine in the portal, in the **Create a virtual machine** blade, choose the **Networking** tab. In this tab, there is an option for **Accelerated networking**. If you have chosen a [supported operating system](#) and [VM size](#), this option will automatically populate to "On." If not, it will populate the "Off" option for Accelerated Networking and give the user a reason why it is not be enabled.

- *Note:* Only supported operating systems can be enabled through the portal. If you are using a custom image,

and your image supports Accelerated Networking, please create your VM using CLI or Powershell.

After the virtual machine is created, you can confirm Accelerated Networking is enabled by following the instructions in the [Confirm that accelerated networking is enabled](#).

## CLI creation

### Create a virtual network

Install the latest [Azure CLI](#) and log in to an Azure account using [az login](#). In the following examples, replace example parameter names with your own values. Example parameter names included *myResourceGroup*, *myNic*, and *myVm*.

Create a resource group with [az group create](#). The following example creates a resource group named *myResourceGroup* in the *centralus* location:

```
az group create --name myResourceGroup --location centralus
```

Select a supported Linux region listed in [Linux accelerated networking](#).

Create a virtual network with [az network vnet create](#). The following example creates a virtual network named *myVnet* with one subnet:

```
az network vnet create \
 --resource-group myResourceGroup \
 --name myVnet \
 --address-prefix 192.168.0.0/16 \
 --subnet-name mySubnet \
 --subnet-prefix 192.168.1.0/24
```

### Create a network security group

Create a network security group with [az network nsg create](#). The following example creates a network security group named *myNetworkSecurityGroup*:

```
az network nsg create \
 --resource-group myResourceGroup \
 --name myNetworkSecurityGroup
```

The network security group contains several default rules, one of which disables all inbound access from the Internet. Open a port to allow SSH access to the virtual machine with [az network nsg rule create](#):

```
az network nsg rule create \
 --resource-group myResourceGroup \
 --nsg-name myNetworkSecurityGroup \
 --name Allow-SSH-Internet \
 --access Allow \
 --protocol Tcp \
 --direction Inbound \
 --priority 100 \
 --source-address-prefix Internet \
 --source-port-range "*" \
 --destination-address-prefix "*" \
 --destination-port-range 22
```

### Create a network interface with accelerated networking

Create a public IP address with [az network public-ip create](#). A public IP address isn't required if you don't plan to

access the virtual machine from the Internet, but to complete the steps in this article, it is required.

```
az network public-ip create \
--name myPublicIp \
--resource-group myResourceGroup
```

Create a network interface with [az network nic create](#) with accelerated networking enabled. The following example creates a network interface named *myNic* in the *mySubnet* subnet of the *myVnet* virtual network and associates the *myNetworkSecurityGroup* network security group to the network interface:

```
az network nic create \
--resource-group myResourceGroup \
--name myNic \
--vnet-name myVnet \
--subnet mySubnet \
--accelerated-networking true \
--public-ip-address myPublicIp \
--network-security-group myNetworkSecurityGroup
```

## Create a VM and attach the NIC

When you create the VM, specify the NIC you created with `--nics`. Select a size and distribution listed in [Linux accelerated networking](#).

Create a VM with [az vm create](#). The following example creates a VM named *myVM* with the UbuntuLTS image and a size that supports Accelerated Networking (*Standard\_DS4\_v2*):

```
az vm create \
--resource-group myResourceGroup \
--name myVM \
--image UbuntuLTS \
--size Standard_DS4_v2 \
--admin-username azureuser \
--generate-ssh-keys \
--nics myNic
```

For a list of all VM sizes and characteristics, see [Linux VM sizes](#).

Once the VM is created, output similar to the following example output is returned. Take note of the **publicIpAddress**. This address is used to access the VM in subsequent steps.

```
{
 "fqdns": "",
 "id": "/subscriptions/<ID>/resourceGroups/myResourceGroup/providers/Microsoft.Compute/virtualMachines/myVM",
 "location": "centralus",
 "macAddress": "00-0D-3A-23-9A-49",
 "powerState": "VM running",
 "privateIpAddress": "192.168.0.4",
 "publicIpAddress": "40.68.254.142",
 "resourceGroup": "myResourceGroup"
}
```

## Confirm that accelerated networking is enabled

Use the following command to create an SSH session with the VM. Replace `<your-public-ip-address>` with the public IP address assigned to the virtual machine you created, and replace *azureuser* if you used a different value for `--admin-username` when you created the VM.

```
ssh azureuser@<your-public-ip-address>
```

From the Bash shell, enter `uname -r` and confirm that the kernel version is one of the following versions, or greater:

- **Ubuntu 16.04:** 4.11.0-1013
- **SLES SP3:** 4.4.92-6.18
- **RHEL:** 7.4.2017120423
- **CentOS:** 7.4.20171206

Confirm the Mellanox VF device is exposed to the VM with the `lspci` command. The returned output is similar to the following output:

```
0000:00:00.0 Host bridge: Intel Corporation 440BX/ZX/DX - 82443BX/ZX/DX Host bridge (AGP disabled) (rev 03)
0000:00:07.0 ISA bridge: Intel Corporation 82371AB/EB/MB PIIX4 ISA (rev 01)
0000:00:07.1 IDE interface: Intel Corporation 82371AB/EB/MB PIIX4 IDE (rev 01)
0000:00:07.3 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 02)
0000:00:08.0 VGA compatible controller: Microsoft Corporation Hyper-V virtual VGA
0001:00:02.0 Ethernet controller: Mellanox Technologies MT27500/MT27520 Family [ConnectX-3/ConnectX-3 Pro
Virtual Function]
```

Check for activity on the VF (virtual function) with the `ethtool -S eth0 | grep vf_` command. If you receive output similar to the following sample output, accelerated networking is enabled and working.

```
vf_rx_packets: 992956
vf_rx_bytes: 2749784180
vf_tx_packets: 2656684
vf_tx_bytes: 1099443970
vf_tx_dropped: 0
```

Accelerated Networking is now enabled for your VM.

## Handle dynamic binding and revocation of virtual function

Applications must run over the synthetic NIC that is exposed in VM. If the application runs directly over the VF NIC, it doesn't receive **all** packets that are destined to the VM, since some packets show up over the synthetic interface. If you run an application over the synthetic NIC, it guarantees that the application receives **all** packets that are destined to it. It also makes sure that the application keeps running, even if the VF is revoked when the host is being serviced. Applications binding to the synthetic NIC is a **mandatory** requirement for all applications taking advantage of **Accelerated Networking**.

## Enable Accelerated Networking on existing VMs

If you have created a VM without Accelerated Networking, it is possible to enable this feature on an existing VM. The VM must support Accelerated Networking by meeting the following prerequisites that are also outlined above:

- The VM must be a supported size for Accelerated Networking
- The VM must be a supported Azure Gallery image (and kernel version for Linux)
- All VMs in an availability set or VMSS must be stopped/deallocated before enabling Accelerated Networking on any NIC

### Individual VMs & VMs in an availability set

First stop/deallocate the VM or, if an Availability Set, all the VMs in the Set:

```
az vm deallocate \
--resource-group myResourceGroup \
--name myVM
```

Important, please note, if your VM was created individually, without an availability set, you only need to stop/deallocate the individual VM to enable Accelerated Networking. If your VM was created with an availability set, all VMs contained in the availability set will need to be stopped/deallocated before enabling Accelerated Networking on any of the NICs.

Once stopped, enable Accelerated Networking on the NIC of your VM:

```
az network nic update \
--name myNic \
--resource-group myResourceGroup \
--accelerated-networking true
```

Restart your VM or, if in an Availability Set, all the VMs in the Set and confirm that Accelerated Networking is enabled:

```
az vm start --resource-group myResourceGroup \
--name myVM
```

## VMSS

VMSS is slightly different but follows the same workflow. First, stop the VMs:

```
az vmss deallocate \
--name myvmss \
--resource-group myrg
```

Once the VMs are stopped, update the Accelerated Networking property under the network interface:

```
az vmss update --name myvmss \
--resource-group myrg \
--set
virtualMachineProfile.networkProfile.networkInterfaceConfigurations[0].enableAcceleratedNetworking=true
```

Please note, a VMSS has VM upgrades that apply updates using three different settings, automatic, rolling and manual. In these instructions the policy is set to automatic so that the VMSS will pick up the changes immediately after restarting. To set it to automatic so that the changes are immediately picked up:

```
az vmss update \
--name myvmss \
--resource-group myrg \
--set upgradePolicy.mode="automatic"
```

Finally, restart the VMSS:

```
az vmss start \
--name myvmss \
--resource-group myrg
```

Once you restart, wait for the upgrades to finish but once completed, the VF will appear inside the VM. (Please make sure you are using a supported OS and VM size.)

## **Resizing existing VMs with Accelerated Networking**

VMs with Accelerated Networking enabled can only be resized to VMs that support Accelerated Networking.

A VM with Accelerated Networking enabled cannot be resized to a VM instance that does not support Accelerated Networking using the resize operation. Instead, to resize one of these VMs:

- Stop/Deallocate the VM or if in an availability set/VMSS, stop/deallocate all the VMs in the set/VMSS.
- Accelerated Networking must be disabled on the NIC of the VM or if in an availability set/VMSS, all VMs in the set/VMSS.
- Once Accelerated Networking is disabled, the VM/availability set/VMSS can be moved to a new size that does not support Accelerated Networking and restarted.

# Create a fully qualified domain name in the Azure portal for a Linux VM

12/23/2019 • 2 minutes to read • [Edit Online](#)

When you create a virtual machine (VM) in the [Azure portal](#), a public IP resource for the virtual machine is automatically created. You use this IP address to remotely access the VM. Although the portal does not create a [fully qualified domain name](#), or FQDN, you can add one once the VM is created. This article demonstrates the steps to create a DNS name or FQDN.

## Create a FQDN

This article assumes that you have already created a VM. If needed, you can [create a VM in the portal](#) or [with the Azure CLI](#). Follow these steps once your VM is up and running:

1. Select your VM in the portal. Under **DNS name**, click **Configure**.

The screenshot shows the Azure portal interface for a virtual machine named 'myVM'. The left sidebar lists navigation options like Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The main content area displays VM details under 'myResourceGroup':

| Setting                | Value                                    |
|------------------------|------------------------------------------|
| Computer name          | myVM                                     |
| Operating system       | Linux                                    |
| Size                   | Standard DS1 v2 (1 vcpus, 3.5 GB memory) |
| Public IP address      | 40.76.54.250                             |
| Virtual network/subnet | myVMNET/myVMSubnet                       |
| DNS name               | <a href="#">Configure</a> (button)       |

Below the main content, there's a note about tags: 'Tags (change) Click here to add tags'.

2. Enter the desired DNS name and then select **Save**.

The screenshot shows the 'Configuration' dialog for a VM named 'myVMPublicIP'. The dialog has tabs for 'Save' and 'Discard'. The 'Assignment' section shows 'Dynamic' selected for IP address. The 'IP address' field contains '40.76.54.250'. The 'Idle timeout (minutes)' slider is set to 4. The 'DNS name label (optional)' field is highlighted with a red border and contains '.eastus.cloudapp.azure.com'. At the bottom, there's a note: 'Prefer to use your own domain name? Try Azure DNS now'.

3. To return to the VM overview blade, close the *Public IP address* blade. Verify that the *DNS name* is now shown.

You can now connect remotely to the VM using this DNS name such as with

```
ssh azureuser@mydns.westus.cloudapp.azure.com .
```

## Next steps

Now that your VM has a public IP and DNS name, you can deploy common application frameworks or services such as nginx, MongoDB, Docker, etc.

You can also read more about [using Resource Manager](#) for tips on building your Azure deployments.

# How to find and delete unattached network interface cards (NICs) for Azure VMs

11/13/2019 • 2 minutes to read • [Edit Online](#)

When you delete a virtual machine (VM) in Azure, the network interface cards (NICs) are not deleted by default. If you create and delete multiple VMs, the unused NICs continue to use the internal IP address leases. As you create other VM NICs, they may be unable to obtain an IP lease in the address space of the subnet. This article shows you how to find and delete unattached NICs.

## Find and delete unattached NICs

The *virtualMachine* property for a NIC stores the ID and resource group of the VM the NIC is attached to. The following script loops through all the NICs in a subscription and checks if the *virtualMachine* property is null. If this property is null, the NIC is not attached to a VM.

To view all the unattached NICs, it's highly recommend to first run the script with the *deleteUnattachedNics* variable to 0. To delete all the unattached NICs after you review the list output, run the script with *deleteUnattachedNics* to 1.

```
Set deleteUnattachedNics=1 if you want to delete unattached NICs
Set deleteUnattachedNics=0 if you want to see the Id(s) of the unattached NICs
deleteUnattachedNics=0

unattachedNicsIds=$(az network nic list --query '[?virtualMachine==`null`].[id]' -o tsv)
for id in ${unattachedNicsIds[@]}
do
 if (($deleteUnattachedNics == 1))
 then
 echo "Deleting unattached NIC with Id: \"$id"
 az network nic delete --ids $id
 echo "Deleted unattached NIC with Id: \"$id"
 else
 echo $id
 fi
done
```

## Next steps

For more information on how to create and manage virtual networks in Azure, see [create and manage VM networks](#).

# DNS Name Resolution options for Linux virtual machines in Azure

8/28/2019 • 7 minutes to read • [Edit Online](#)

Azure provides DNS name resolution by default for all virtual machines that are in a single virtual network. You can implement your own DNS name resolution solution by configuring your own DNS services on your virtual machines that Azure hosts. The following scenarios should help you choose the one that works for your situation.

- [Name resolution that Azure provides](#)
- [Name resolution using your own DNS server](#)

The type of name resolution that you use depends on how your virtual machines and role instances need to communicate with each other.

The following table illustrates scenarios and corresponding name resolution solutions:

| SCENARIO                                                                                               | SOLUTION                                                                                                                                                                                                                         | SUFFIX                                         |
|--------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| Name resolution between role instances or virtual machines in the same virtual network                 | Name resolution that Azure provides                                                                                                                                                                                              | hostname or fully-qualified domain name (FQDN) |
| Name resolution between role instances or virtual machines in different virtual networks               | Customer-managed DNS servers that forward queries between virtual networks for resolution by Azure (DNS proxy). See <a href="#">Name resolution using your own DNS server</a> .                                                  | FQDN only                                      |
| Resolution of on-premises computers and service names from role instances or virtual machines in Azure | Customer-managed DNS servers (for example, on-premises domain controller, local read-only domain controller, or a DNS secondary synced by using zone transfers). See <a href="#">Name resolution using your own DNS server</a> . | FQDN only                                      |
| Resolution of Azure hostnames from on-premises computers                                               | Forward queries to a customer-managed DNS proxy server in the corresponding virtual network. The proxy server forwards queries to Azure for resolution. See <a href="#">Name resolution using your own DNS server</a> .          | FQDN only                                      |
| Reverse DNS for internal IPs                                                                           | <a href="#">Name resolution using your own DNS server</a>                                                                                                                                                                        | n/a                                            |

## Name resolution that Azure provides

Along with resolution of public DNS names, Azure provides internal name resolution for virtual machines and role instances that are in the same virtual network. In virtual networks that are based on Azure Resource Manager, the DNS suffix is consistent across the virtual network; the FQDN is not needed. DNS names can be assigned to both network interface cards (NICs) and virtual machines. Although the name resolution that Azure provides does not require any configuration, it is not the appropriate choice for all deployment scenarios, as seen on the preceding

table.

## Features and considerations

### Features:

- No configuration is required to use name resolution that Azure provides.
- The name resolution service that Azure provides is highly available. You don't need to create and manage clusters of your own DNS servers.
- The name resolution service that Azure provides can be used along with your own DNS servers to resolve both on-premises and Azure hostnames.
- Name resolution is provided between virtual machines in virtual networks without need for the FQDN.
- You can use hostnames that best describe your deployments rather than working with auto-generated names.

### Considerations:

- The DNS suffix that Azure creates cannot be modified.
- You cannot manually register your own records.
- WINS and NetBIOS are not supported.
- Hostnames must be DNS-compatible. Names must use only 0-9, a-z, and '-', and they cannot start or end with a '-'. See RFC 3696 Section 2.
- DNS query traffic is throttled for each virtual machine. Throttling shouldn't impact most applications. If request throttling is observed, ensure that client-side caching is enabled. For more information, see [Getting the most from name resolution that Azure provides](#).

## Getting the most from name resolution that Azure provides

### Client-side caching:

Some DNS queries are not sent across the network. Client-side caching helps reduce latency and improve resilience to network inconsistencies by resolving recurring DNS queries from a local cache. DNS records contain a Time-To-Live (TTL), which enables the cache to store the record for as long as possible without impacting record freshness. As a result, client-side caching is suitable for most situations.

Some Linux distributions do not include caching by default. We recommend that you add a cache to each Linux virtual machine after you check that there isn't a local cache already.

Several different DNS caching packages, such as dnsmasq, are available. Here are the steps to install dnsmasq on the most common distributions:

### Ubuntu (uses resolvconf)

- Install the dnsmasq package ("sudo apt-get install dnsmasq").

### SUSE (uses netconf):

1. Install the dnsmasq package ("sudo zypper install dnsmasq").
2. Enable the dnsmasq service ("systemctl enable dnsmasq.service").
3. Start the dnsmasq service ("systemctl start dnsmasq.service").
4. Edit "/etc/sysconfig/network/config", and change NETCONFIG\_DNS\_FORWARDER="" to "dnsmasq".
5. Update resolv.conf ("netconfig update") to set the cache as the local DNS resolver.

### CentOS by Rogue Wave Software (formerly OpenLogic; uses NetworkManager)

1. Install the dnsmasq package ("sudo yum install dnsmasq").
2. Enable the dnsmasq service ("systemctl enable dnsmasq.service").
3. Start the dnsmasq service ("systemctl start dnsmasq.service").
4. Add "prepend domain-name-servers 127.0.0.1;" to "/etc/dhclient-eth0.conf".

5. Restart the network service ("service network restart") to set the cache as the local DNS resolver

**NOTE**

: The 'dnsmasq' package is only one of the many DNS caches that are available for Linux. Before you use it, check its suitability for your needs and that no other cache is installed.

### Client-side retries

DNS is primarily a UDP protocol. Because the UDP protocol doesn't guarantee message delivery, the DNS protocol itself handles retry logic. Each DNS client (operating system) can exhibit different retry logic depending on the creator's preference:

- Windows operating systems retry after one second and then again after another two, four, and another four seconds.
- The default Linux setup retries after five seconds. You should change this to retry five times at one-second intervals.

To check the current settings on a Linux virtual machine, 'cat /etc/resolv.conf', and look at the 'options' line, for example:

```
options timeout:1 attempts:5
```

The resolv.conf file is auto-generated and should not be edited. The specific steps that add the 'options' line vary by distribution:

#### **Ubuntu** (uses resolvconf)

1. Add the options line to '/etc/resolvconf/resolv.conf.d/head'.
2. Run 'resolvconf -u' to update.

#### **SUSE** (uses netconfig)

1. Add 'timeout:1 attempts:5' to the NETCONFIG\_DNS\_RESOLVER\_OPTIONS="" parameter in '/etc/sysconfig/network/config'.
2. Run 'netconfig update' to update.

#### **CentOS by Rogue Wave Software (formerly OpenLogic)** (uses NetworkManager)

1. Add 'RES\_OPTIONS="timeout:1 attempts:5"' to '/etc/sysconfig/network'.
2. Run 'service network restart' to update.

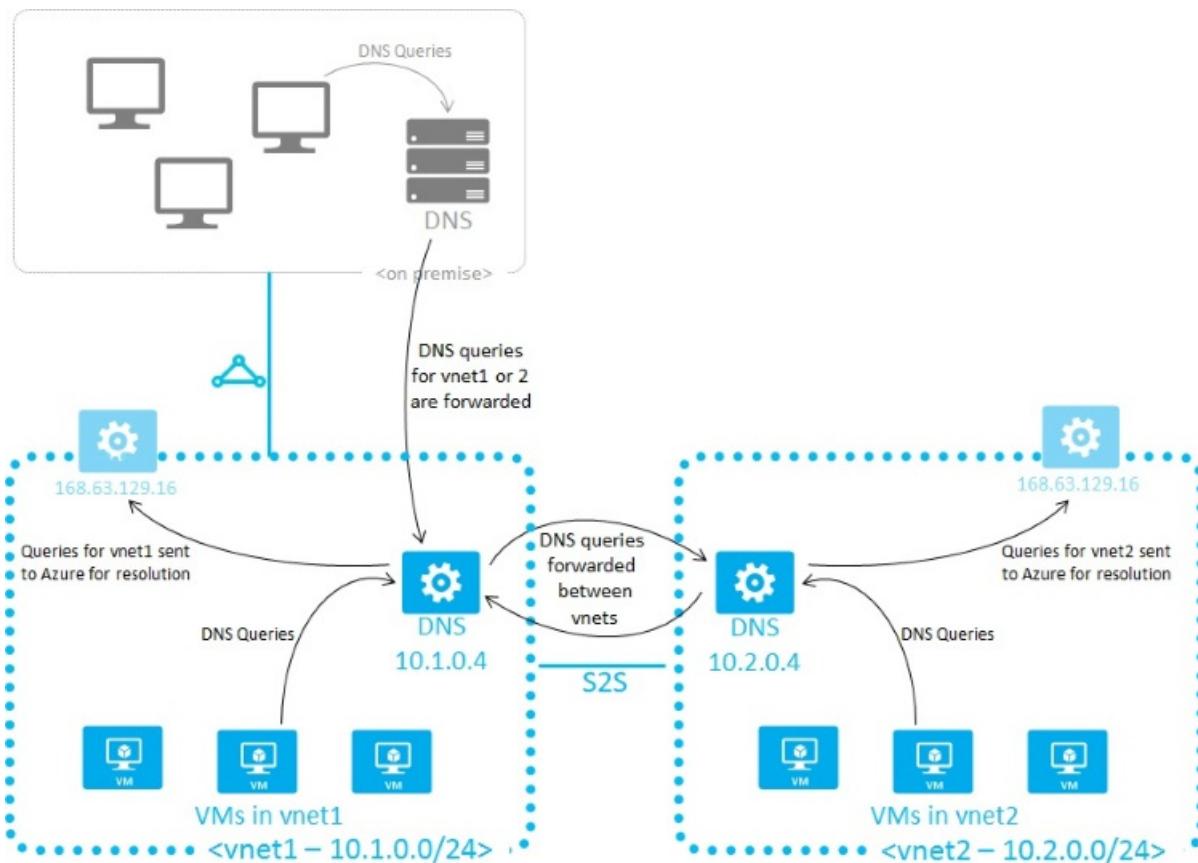
## Name resolution using your own DNS server

Your name resolution needs may go beyond the features that Azure provides. For example, you might require DNS resolution between virtual networks. To cover this scenario, you can use your own DNS servers.

DNS servers within a virtual network can forward DNS queries to recursive resolvers of Azure to resolve hostnames that are in the same virtual network. For example, a DNS server that runs in Azure can respond to DNS queries for its own DNS zone files and forward all other queries to Azure. This functionality enables virtual machines to see both your entries in your zone files and hostnames that Azure provides (via the forwarder). Access to the recursive resolvers of Azure is provided via the virtual IP 168.63.129.16.

DNS forwarding also enables DNS resolution between virtual networks and enables your on-premises machines to resolve hostnames that Azure provides. To resolve a virtual machine's hostname, the DNS server virtual machine must reside in the same virtual network and be configured to forward hostname queries to Azure.

Because the DNS suffix is different in each virtual network, you can use conditional forwarding rules to send DNS queries to the correct virtual network for resolution. The following image shows two virtual networks and an on-premises network doing DNS resolution between virtual networks by using this method:



When you use name resolution that Azure provides, the internal DNS suffix is provided to each virtual machine by using DHCP. When you use your own name resolution solution, this suffix is not supplied to virtual machines because the suffix interferes with other DNS architectures. To refer to machines by FQDN or to configure the suffix on your virtual machines, you can use PowerShell or the API to determine the suffix:

- For virtual networks that are managed by Azure Resource Manager, the suffix is available via the [network interface card](#) resource. You can also run the `azurerm network public-ip show <resource group> <ip name>` command to display the details of your public IP, which includes the FQDN of the NIC.

If forwarding queries to Azure doesn't suit your needs, you need to provide your own DNS solution. Your DNS solution needs to:

- Provide appropriate hostname resolution, for example via [DDNS](#). If you use DDNS, you might need to disable DNS record scavenging. DHCP leases of Azure are very long and scavenging may remove DNS records prematurely.
- Provide appropriate recursive resolution to allow resolution of external domain names.
- Be accessible (TCP and UDP on port 53) from the clients it serves and be able to access the Internet.
- Be secured against access from the Internet to mitigate threats posed by external agents.

#### NOTE

For best performance, when you use virtual machines in Azure DNS servers, disable IPv6 and assign an [Instance-Level Public IP](#) to each DNS server virtual machine.

# Create virtual network interface cards and use internal DNS for VM name resolution on Azure

11/13/2019 • 5 minutes to read • [Edit Online](#)

This article shows you how to set static internal DNS names for Linux VMs using virtual network interface cards (vNics) and DNS label names with the Azure CLI. Static DNS names are used for permanent infrastructure services like a Jenkins build server, which is used for this document, or a Git server.

The requirements are:

- [an Azure account](#)
- [SSH public and private key files](#)

## Quick commands

If you need to quickly accomplish the task, the following section details the commands needed. More detailed information and context for each step can be found in the rest of the document, [starting here](#). To perform these steps, you need the latest [Azure CLI](#) installed and logged in to an Azure account using [az login](#).

Pre-Requirements: Resource Group, virtual network and subnet, Network Security Group with SSH inbound.

### Create a virtual network interface card with a static internal DNS name

Create the vNic with [az network nic create](#). The `--internal-dns-name` CLI flag is for setting the DNS label, which provides the static DNS name for the virtual network interface card (vNic). The following example creates a vNic named `myNic`, connects it to the `myVnet` virtual network, and creates an internal DNS name record called `jenkins`:

```
az network nic create \
 --resource-group myResourceGroup \
 --name myNic \
 --vnet-name myVnet \
 --subnet mySubnet \
 --internal-dns-name jenkins
```

### Deploy a VM and connect the vNic

Create a VM with [az vm create](#). The `--nics` flag connects the vNic to the VM during the deployment to Azure. The following example creates a VM named `myVM` with Azure Managed Disks and attaches the vNic named `myNic` from the preceding step:

```
az vm create \
 --resource-group myResourceGroup \
 --name myVM \
 --nics myNic \
 --image UbuntuLTS \
 --admin-username azureuser \
 --ssh-key-value ~/.ssh/id_rsa.pub
```

## Detailed walkthrough

A full continuous integration and continuous deployment (CiCd) infrastructure on Azure requires certain servers to

be static or long-lived servers. It is recommended that Azure assets like the virtual networks and Network Security Groups are static and long lived resources that are rarely deployed. Once a virtual network has been deployed, it can be reused by new deployments without any adverse affects to the infrastructure. You can later add a Git repository server or a Jenkins automation server delivers CiCd to this virtual network for your development or test environments.

Internal DNS names are only resolvable inside an Azure virtual network. Because the DNS names are internal, they are not resolvable to the outside internet, providing additional security to the infrastructure.

In the following examples, replace example parameter names with your own values. Example parameter names include `myResourceGroup`, `myNic`, and `myVM`.

## Create the resource group

First, create the resource group with [az group create](#). The following example creates a resource group named `myResourceGroup` in the `westus` location:

```
az group create --name myResourceGroup --location westus
```

## Create the virtual network

The next step is to build a virtual network to launch the VMs into. The virtual network contains one subnet for this walkthrough. For more information on Azure virtual networks, see [Create a virtual network](#).

Create the virtual network with [az network vnet create](#). The following example creates a virtual network named `myVnet` and subnet named `mySubnet`:

```
az network vnet create \
 --resource-group myResourceGroup \
 --name myVnet \
 --address-prefix 192.168.0.0/16 \
 --subnet-name mySubnet \
 --subnet-prefix 192.168.1.0/24
```

## Create the Network Security Group

Azure Network Security Groups are equivalent to a firewall at the network layer. For more information about Network Security Groups, see [How to create NSGs in the Azure CLI](#).

Create the network security group with [az network nsg create](#). The following example creates a network security group named `myNetworkSecurityGroup`:

```
az network nsg create \
 --resource-group myResourceGroup \
 --name myNetworkSecurityGroup
```

## Add an inbound rule to allow SSH

Add an inbound rule for the network security group with [az network nsg rule create](#). The following example creates a rule named `myRuleAllowSSH`:

```
az network nsg rule create \
--resource-group myResourceGroup \
--nsg-name myNetworkSecurityGroup \
--name myRuleAllowSSH \
--protocol tcp \
--direction inbound \
--priority 1000 \
--source-address-prefix '*' \
--source-port-range '*' \
--destination-address-prefix '*' \
--destination-port-range 22 \
--access allow
```

## Associate the subnet with the Network Security Group

To associate the subnet with the Network Security Group, use [az network vnet subnet update](#). The following example associates the subnet name `mySubnet` with the Network Security Group named `myNetworkSecurityGroup`:

```
az network vnet subnet update \
--resource-group myResourceGroup \
--vnet-name myVnet \
--name mySubnet \
--network-security-group myNetworkSecurityGroup
```

## Create the virtual network interface card and static DNS names

Azure is very flexible, but to use DNS names for VM name resolution, you need to create virtual network interface cards (vNics) that include a DNS label. vNics are important as you can reuse them by connecting them to different VMs over the infrastructure lifecycle. This approach keeps the vNic as a static resource while the VMs can be temporary. By using DNS labeling on the vNic, we are able to enable simple name resolution from other VMs in the VNet. Using resolvable names enables other VMs to access the automation server by the DNS name `Jenkins` or the Git server as `gitrepo`.

Create the vNic with [az network nic create](#). The following example creates a vNic named `myNic`, connects it to the `myVnet` virtual network named `myVnet`, and creates an internal DNS name record called `jenkins`:

```
az network nic create \
--resource-group myResourceGroup \
--name myNic \
--vnet-name myVnet \
--subnet mySubnet \
--internal-dns-name jenkins
```

## Deploy the VM into the virtual network infrastructure

We now have a virtual network and subnet, a Network Security Group acting as a firewall to protect our subnet by blocking all inbound traffic except port 22 for SSH, and a vNic. You can now deploy a VM inside this existing network infrastructure.

Create a VM with [az vm create](#). The following example creates a VM named `myVM` with Azure Managed Disks and attaches the vNic named `myNic` from the preceding step:

```
az vm create \
--resource-group myResourceGroup \
--name myVM \
--nics myNic \
--image UbuntuLTS \
--admin-username azureuser \
--ssh-key-value ~/.ssh/id_rsa.pub
```

By using the CLI flags to call out existing resources, we instruct Azure to deploy the VM inside the existing network. To reiterate, once a VNet and subnet have been deployed, they can be left as static or permanent resources inside your Azure region.

## Next steps

- [Create your own custom environment for a Linux VM using Azure CLI commands directly](#)
- [Create a Linux VM on Azure using templates](#)

# Azure virtual machine extensions and features

11/13/2019 • 3 minutes to read • [Edit Online](#)

Azure virtual machine (VM) extensions are small applications that provide post-deployment configuration and automation tasks on Azure VMs, you can use existing images and then customize them as part of your deployments, getting you out of the business of custom image building.

The Azure platform hosts many extensions that range from VM configuration, monitoring, security, and utility applications. Publishers take an application, then wrap it into an extension, and simplify the installation, so all you need to do is provide mandatory parameters.

There is a large choice of first and third party extensions, if the application in the extension repository does not exist, then you can use the Custom Script extension and configure your VM with your own scripts and commands.

Examples of key scenarios that extensions are used for:

- VM configuration, you can use Powershell DSC (Desired State Configuration), Chef, Puppet and Custom Script Extensions to install VM configuration agents and configure your VM.
- AV products, such as Symantec, ESET.
- VM vulnerability tool, such as Qualys, Rapid7, HPE.
- VM and App monitoring tooling, such as DynaTrace, Azure Network Watcher, Site24x7, and Stackify.

Extensions can be bundled with a new VM deployment. For example, they can be part of a larger deployment, configuring applications on VM provision, or run against any supported extension operated systems post deployment.

## How can I find What extensions are available?

You can view available extensions in the VM blade in the Portal, under extensions, this represents just a small amount, for the full list, you can use the CLI tools, see [Discovering VM Extensions for Linux](#) and [Discovering VM Extensions for Windows](#).

## How can I install an extension?

Azure VM extensions can be managed using either the Azure CLI, Azure PowerShell, Azure Resource Manager templates, and the Azure portal. To try an extension, you can go to the Azure portal, select the Custom Script Extension, then pass in a command / script and run the extensions.

If you want to same extension you added in the portal by CLI or Resource Manager template, see different extension documentation, such as [Windows Custom Script Extension](#) and [Linux Custom Script Extension](#).

## How do I manage extension application lifecycle?

You do not need to connect to a VM directly to install or delete the extension. As the Azure extension application lifecycle is managed outside of the VM and integrated into the Azure platform, you also get integrated status of the extension.

## Anything else I should be thinking about for extensions?

Extensions install applications, like any applications there are some requirements, for extensions there is a list of supported Windows and Linux OSes, and you need to have the Azure VM agents installed. Some individual VM

extension applications may have their own environmental prerequisites, such as access to an endpoint.

## Troubleshoot extensions

Troubleshooting information for each extension can be found in the **Troubleshoot and support** section in the overview for the extension. Here is a list of the troubleshooting information available:

| NAMESPACE                                                         | TROUBLESHOOTING                                         |
|-------------------------------------------------------------------|---------------------------------------------------------|
| microsoft.azure.monitoring.dependencyagent.dependencyagentlinux   | <a href="#">Azure Monitor Dependency for Linux</a>      |
| microsoft.azure.monitoring.dependencyagent.dependencyagentwindows | <a href="#">Azure Monitor Dependency for Windows</a>    |
| microsoft.azure.security.azurediskencryptionforlinux              | <a href="#">Azure Disk Encryption for Linux</a>         |
| microsoft.azure.security.azurediskencryption                      | <a href="#">Azure Disk Encryption for Windows</a>       |
| microsoft.compute.customscriptextension                           | <a href="#">Custom Script for Windows</a>               |
| microsoft.ostcextensions.customscriptforlinux                     | <a href="#">Desired State Configuration for Linux</a>   |
| microsoft.powershell.dsc                                          | <a href="#">Desired State Configuration for Windows</a> |
| microsoft.hpccompute.nvidiagpudriverlinux                         | <a href="#">NVIDIA GPU Driver Extension for Linux</a>   |
| microsoft.hpccompute.nvidiagpudriverwindows                       | <a href="#">NVIDIA GPU Driver Extension for Windows</a> |
| microsoft.azure.security.iaasantimalware                          | <a href="#">Antimalware Extension for Windows</a>       |
| microsoft.enterprisecloud.monitoring.omsagentforlinux             | <a href="#">Azure Monitor for Linux</a>                 |
| microsoft.enterprisecloud.monitoring.microsoftmonitoringagent     | <a href="#">Azure Monitor for Windows</a>               |
| stackify.linuxagent.extension.stackifylinuxagentextension         | <a href="#">Stackify Retrace for Linux</a>              |
| vmaccessforlinux.microsoft.ostcextensions                         | <a href="#">Reset password (VMAccess) for Linux</a>     |
| microsoft.recoveryservices.vmsnapshot                             | <a href="#">Snapshot for Linux</a>                      |
| microsoft.recoveryservices.vmsnapshot                             | <a href="#">Snapshot for Windows</a>                    |

## Next steps

- For more information about how the Linux Agent and Extensions work, see [Azure VM extensions and features for Linux](#).
- For more information about how the Windows Guest Agent and Extensions work, see [Azure VM extensions and features for Windows](#).
- To install the Windows Guest Agent, see [Azure Windows Virtual Machine Agent Overview](#).
- To install the Linux Agent, see [Azure Linux Virtual Machine Agent Overview](#).

# Move a Linux VM to another subscription or resource group

1/14/2020 • 3 minutes to read • [Edit Online](#)

This article walks you through how to move a Linux virtual machine (VM) between resource groups or subscriptions. Moving a VM between subscriptions can be handy if you created a VM in a personal subscription and now want to move it to your company's subscription.

## IMPORTANT

You cannot move Azure Managed Disks at this time.

New resource IDs are created as part of the move. After the VM has been moved, you will need to update your tools and scripts to use the new resource IDs.

## Use the Azure CLI to move a VM

Before you can move your VM by using the Azure CLI, you need to make sure the source and destination subscriptions exist within the same tenant. To check that both subscriptions have the same tenant ID, use [az account show](#).

```
az account show --subscription mySourceSubscription --query tenantId
az account show --subscription myDestinationSubscription --query tenantId
```

If the tenant IDs for the source and destination subscriptions are not the same, you must contact [support](#) to move the resources to a new tenant.

To successfully move a VM, you need to move the VM and all its supporting resources. Use the [az resource list](#) command to list all the resources in a resource group and their IDs. It helps to pipe the output of this command to a file so you can copy and paste the IDs into later commands.

```
az resource list --resource-group "mySourceResourceGroup" --query "[].{Id:id}" --output table
```

To move a VM and its resources to another resource group, use [az resource move](#). The following example shows how to move a VM and the most common resources it requires. Use the **-ids** parameter and pass in a comma-separated list (without spaces) of IDs for the resources to move.

```

vm=/subscriptions/mySourceSubscriptionID/resourceGroups/mySourceResourceGroup/providers/Microsoft.Compute/virtualMachines/myVM
nic=/subscriptions/mySourceSubscriptionID/resourceGroups/mySourceResourceGroup/providers/Microsoft.Network/networkInterfaces/myNIC
nsg=/subscriptions/mySourceSubscriptionID/resourceGroups/mySourceResourceGroup/providers/Microsoft.Network/networkSecurityGroups/myNSG
pip=/subscriptions/mySourceSubscriptionID/resourceGroups/mySourceResourceGroup/providers/Microsoft.Network/publicIPAddresses/myPublicIPAddress
vnet=/subscriptions/mySourceSubscriptionID/resourceGroups/mySourceResourceGroup/providers/Microsoft.Network/virtualNetworks/myVNet
diag=/subscriptions/mySourceSubscriptionID/resourceGroups/mySourceResourceGroup/providers/Microsoft.Storage/storageAccounts/mydiagnosticstorageaccount
storage=/subscriptions/mySourceSubscriptionID/resourceGroups/mySourceResourceGroup/providers/Microsoft.Storage/storageAccounts/mystorageaccountname

az resource move \
 --ids $vm,$nic,$nsg,$pip,$vnet,$storage,$diag \
 --destination-group "myDestinationResourceGroup"

```

If you want to move the VM and its resources to a different subscription, add the **--destination-subscriptionId** parameter to specify the destination subscription.

When you are asked to confirm that you want to move the specified resources, enter **Y** to confirm.

## Use the Azure portal to move a VM to a different subscription

You can move a VM and its associated resources to a different subscription by using the Azure portal.

1. Go to the [Azure portal](#) to manage the resource group containing the VM to move. Search for and select **Resource groups**.
2. Choose the resource group containing the VM that you would like to move.
3. At the top of the page for the resource group, select **Move** and then select **Move to another subscription**. The **Move resources** page opens.
4. Select each of the resources to move. In most cases, you should move all of the related resources that are listed.
5. Select the **Subscription** where you want the VM to be moved.
6. Select an existing **Resource group**, or enter a name to have a new resource group created.
7. When you are done, select that you understand that new resource IDs will be created and that the new IDs will need to be used with the VM after it is moved, and then select **OK**.

## Use the Azure portal to move a VM to another resource group

You can move a VM and its associated resources to another resource group by using the Azure portal.

1. Go to the [Azure portal](#) to manage the resource group containing the VM to move. Search for and select **Resource groups**.
2. Choose the resource group containing the VM that you would like to move.
3. At the top of the page for the resource group, select **Move** and then select **Move to another resource group**. The **Move resources** page opens.
4. Select each of the resources to move. In most cases, you should move all of the related resources that are listed.
5. Select an existing **Resource group**, or enter a name to have a new resource group created.
6. When you are done, select that you understand that new resource IDs will be created and that the new IDs will need to be used with the VM after it is moved, and then select **OK**.

## Next steps

You can move many different types of resources between resource groups and subscriptions. For more

information, see [Move resources to a new resource group or subscription](#).

# Move Azure VMs to another region

11/12/2019 • 6 minutes to read • [Edit Online](#)

There are various scenarios in which you'd want to move your existing Azure IaaS virtual machines (VMs) from one region to another. For example, you want to improve reliability and availability of your existing VMs, to improve manageability, or to move for governance reasons. For more information, see the [Azure VM move overview](#).

You can use the [Azure Site Recovery](#) service to manage and orchestrate disaster recovery of on-premises machines and Azure VMs for business continuity and disaster recovery (BCDR). You can also use Site Recovery to manage the move of Azure VMs to a secondary region.

In this tutorial, you will:

- Verify prerequisites for the move
- Prepare the source VMs and the target region
- Copy the data and enable replication
- Test the configuration and perform the move
- Delete the resources in the source region

## NOTE

This tutorial shows you how to move Azure VMs from one region to another as is. If you need to improve availability by moving VMs in an availability set to zone pinned VMs in a different region, see the [Move Azure VMs into Availability Zones tutorial](#).

## Prerequisites

- Make sure that the Azure VMs are in the Azure region from which you want to move.
- Verify that your choice of [source region - target region combination is supported](#), and make an informed decision about the target region.
- Make sure that you understand the [scenario architecture and components](#).
- Review the [support limitations and requirements](#).
- Verify account permissions. If you created your free Azure account, you're the administrator of your subscription. If you're not the subscription administrator, work with the administrator to assign the permissions that you need. To enable replication for a VM and essentially copy data by using Azure Site Recovery, you must have:
  - Permissions to create a VM in Azure resources. The Virtual Machine Contributor built-in role has these permissions, which include:
  - Permission to create a VM in the selected resource group
  - Permission to create a VM in the selected virtual network
  - Permission to write to the selected storage account
  - Permissions to manage Azure Site Recovery operations. The Site Recovery Contributor role has all the permissions that are required to manage Site Recovery operations in a Recovery Services vault.

- Make sure that all the latest root certificates are on the Azure VMs that you want to move. If the latest root certificates aren't on the VM, security constraints will prevent the data copy to the target region.
- For Windows VMs, install all the latest Windows updates on the VM, so that all the trusted root certificates are on the machine. In a disconnected environment, follow the standard Windows Update and certificate update processes for your organization.
- For Linux VMs, follow the guidance provided by your Linux distributor to get the latest trusted root certificates and certificate revocation list on the VM.
- Make sure that you're not using an authentication proxy to control network connectivity for VMs that you want to move.
- If the VM that you're trying to move doesn't have access to the internet, or it's using a firewall proxy to control outbound access, [check the requirements](#).
- Identify the source networking layout and all the resources that you're currently using. This includes but isn't limited to load balancers, network security groups (NSGs), and public IPs.
- Verify that your Azure subscription allows you to create VMs in the target region that's used for disaster recovery. Contact support to enable the required quota.
- Make sure that your subscription has enough resources to support VMs with sizes that match your source VMs. If you're using Site Recovery to copy data to the target, Site Recovery chooses the same size or the closest possible size for the target VM.
- Make sure that you create a target resource for every component that's identified in the source networking layout. This step is important to ensure that your VMs have all the functionality and features in the target region that you had in the source region.

**NOTE**

Azure Site Recovery automatically discovers and creates a virtual network when you enable replication for the source VM. You can also pre-create a network and assign it to the VM in the user flow for enable replication. As mentioned later, you need to manually create any other resources in the target region.

To create the most commonly used network resources that are relevant for you based on the source VM configuration, see the following documentation:

- [Network security groups](#)
- [Load balancers](#)
- [Public IP](#)
- For any other networking components, see the [networking documentation](#).

## Prepare

The following steps shows how to prepare the virtual machine for the move using Azure Site Recovery as a solution.

### Create the vault in any region, except the source region

1. Sign in to the [Azure portal](#) > **Recovery Services**.
2. Select **Create a resource** > **Management Tools** > **Backup and Site Recovery**.
3. In **Name**, specify the friendly name **ContosoVMVault**. If you have more than one subscription, select the appropriate one.
4. Create the resource group **ContosoRG**.

- Specify an Azure region. To check supported regions, see geographic availability in [Azure Site Recovery pricing details](#).
- In **Recovery Services vaults**, select **Overview > ContosoVMVault > +Replicate**.
- In **Source**, select **Azure**.
- In **Source location**, select the source Azure region where your VMs are currently running.
- Select the Resource Manager deployment model. Then select the **Source subscription** and **Source resource group**.
- Select **OK** to save the settings.

#### **Enable replication for Azure VMs and start copying the data**

Site Recovery retrieves a list of the VMs that are associated with the subscription and resource group.

- In the next step, select the VM that you want to move, then select **OK**.
- In **Settings**, select **Disaster recovery**.
- In **Configure disaster recovery > Target region**, select the target region to which you'll replicate.
- For this tutorial, accept the other default settings.
- Select **Enable replication**. This step starts a job to enable replication for the VM.

The screenshot shows the 'Configure settings' dialog box with the following configuration:

- Resource group, Network, Storage and Availability sets**: Includes a 'Customize' link. Description: By default Azure Site Recovery(ASR) will mirror the source site configuration to target site by creating/using the required resource groups, storage accounts, virtual network and availability sets as below. Click 'Customize' above to change the configuration. The resources created by ASR are appended with "asr" suffix.
- Target resource group**: ContosoRG
- Target virtual network**: A2ATest2-vnet-asr(new)
- Cache storage accounts**: a2atest2disks86cacheasr(new)
- Target storage accounts**: a2atest2disks864asr(new)
- Target availability sets**: (empty)
- Replication Policy**: Includes a 'Customize' link. Details: **Name:** 24-hour-retention-policy, **Recovery point retention:** 24 hour(s), **App consistent snapshot frequency:** 4 hour(s)

## Move

The following steps shows how to perform the move to the target region.

- Go to the vault. In **Settings > Replicated items**, select the VM, and then select **Failover**.
- In **Failover**, select **Latest**.

3. Select **Shut down machine before beginning failover**. Site Recovery attempts to shut down the source VM before triggering the failover. Failover continues even if shutdown fails. You can follow the failover progress on the **Jobs** page.
4. After the job is finished, check that the VM appears in the target Azure region as expected.

## Discard

In case you checked the moved VM and need to make changes to point of failover or want to go back to a previous point, in the **Replicated items**, right-select the VM > **Change recovery point**. This step provides you the option to specify a different recovery point and failover to that one.

## Commit

Once you have checked the moved VM and are ready to commit the change, in the **Replicated items**, right-select the VM > **Commit**. This step finishes the move process to the target region. Wait until the commit job finishes.

## Clean up

The following steps will guide you through how to clean up the source region as well as related resources that were used for the move.

For all resources that were used for the move:

- Go to the VM. Select **Disable Replication**. This step stops the process from copying the data for the VM.

### IMPORTANT

It's important to perform this step to avoid being charged for Azure Site Recovery replication.

If you have no plans to reuse any of the source resources, complete these additional steps:

1. Delete all the relevant network resources in the source region that you identified in [prerequisites](#).
2. Delete the corresponding storage account in the source region.

## Next steps

In this tutorial, you moved an Azure VM to a different Azure region. Now you can configure disaster recovery for the VM that you moved.

[Set up disaster recovery after migration](#)

# Move Azure VMs into Availability Zones

11/6/2019 • 7 minutes to read • [Edit Online](#)

Availability Zones in Azure help protect your applications and data from datacenter failures. Each Availability Zone is made up of one or more datacenters 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 helps protect applications and data from datacenter failures. With Availability Zones, Azure offers a service-level agreement (SLA) of 99.99% for uptime of virtual machines (VMs). Availability Zones are supported in select regions, as mentioned in [What are Availability Zones in Azure?](#).

In a scenario where your VMs are deployed as *single instance* into a specific region, and you want to improve your availability by moving these VMs into an Availability Zone, you can do so by using Azure Site Recovery. This action can further be categorized into:

- Move single-instance VMs into Availability Zones in a target region
- Move VMs in an availability set into Availability Zones in a target region

## IMPORTANT

Currently, Azure Site Recovery supports moving VMs from one region to another but doesn't support moving within a region.

## Check prerequisites

- Check whether the target region has [support for Availability Zones](#). Check that your choice of [source region/target region combination is supported](#). Make an informed decision on the target region.
- Make sure that you understand the [scenario architecture and components](#).
- Review the [support limitations and requirements](#).
- Check account permissions. If you just created your free Azure account, you're the admin of your subscription. If you aren't the subscription admin, work with the admin to assign the permissions you need. To enable replication for a VM and eventually copy data to the target by using Azure Site Recovery, you must have:
  1. Permission to create a VM in Azure resources. The *Virtual Machine Contributor* built-in role has these permissions, which include:
    - Permission to create a VM in the selected resource group
    - Permission to create a VM in the selected virtual network
    - Permission to write to the selected storage account
  2. Permission to manage Azure Site Recovery tasks. The *Site Recovery Contributor* role has all permissions required to manage Site Recovery actions in a Recovery Services vault.

## Prepare the source VMs

1. Your VMs should use managed disks if you want to move them to an Availability Zone by using Site Recovery. You can convert existing Windows VMs that use unmanaged disks to use managed disks. Follow the steps at [Convert a Windows virtual machine from unmanaged disks to managed disks](#). Ensure that the availability set is configured as *managed*.

2. Check that all the latest root certificates are present on the Azure VMs you want to move. If the latest root certificates aren't present, the data copy to the target region can't be enabled because of security constraints.
3. For Windows VMs, install all the latest Windows updates on the VM, so that all the trusted root certificates are on the machine. In a disconnected environment, follow the standard Windows update and certificate update processes for your organization.
4. For Linux VMs, follow the guidance provided by your Linux distributor to get the latest trusted root certificates and certificate revocation list on the VM.
5. Make sure you don't use an authentication proxy to control network connectivity for VMs that you want to move.
6. If the VM you're trying to move doesn't have access to the internet and uses a firewall proxy to control outbound access, check the requirements at [Configure outbound network connectivity](#).
7. Identify the source networking layout and the resources you currently use for verification, including load balancers, NSGs, and public IP.

## Prepare the target region

1. Check that your Azure subscription lets you create VMs in the target region used for disaster recovery. If necessary, contact support to enable the required quota.
2. Make sure your subscription has enough resources to support VMs with sizes that match your source VMs. If you use Site Recovery to copy data to the target, it picks the same size or the closest possible size for the target VM.
3. Create a target resource for every component identified in the source networking layout. This action ensures that after you cut over to the target region, your VMs have all the functionality and features that you had in the source.

### NOTE

Azure Site Recovery automatically discovers and creates a virtual network and storage account when you enable replication for the source VM. You can also pre-create these resources and assign to the VM as part of the enable replication step. But for any other resources, as mentioned later, you need to manually create them in the target region.

The following documents tell how to create the most commonly used network resources that are relevant to you, based on the source VM configuration.

- [Network security groups](#)
- [Load balancers](#)
- [Public IP](#)

For any other networking components, refer to the networking [documentation](#).

### IMPORTANT

Ensure that you use a zone-redundant load balancer in the target. You can read more at [Standard Load Balancer and Availability Zones](#).

4. Manually [create a non-production network](#) in the target region if you want to test the configuration before you cut over to the target region. We recommend this approach because it causes minimal interference with the production environment.

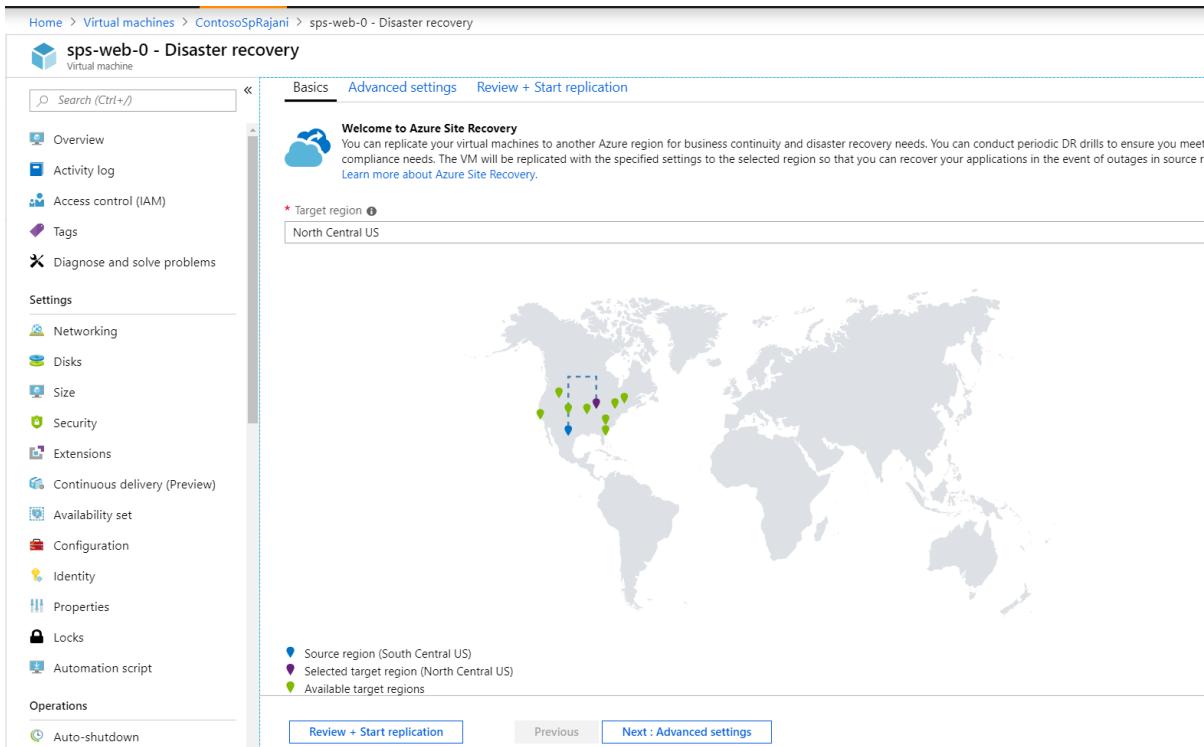
# Enable replication

The following steps will guide you when using Azure Site Recovery to enable replication of data to the target region, before you eventually move them into Availability Zones.

## NOTE

These steps are for a single VM. You can extend the same to multiple VMs. Go to the Recovery Services vault, select + **Replicate**, and select the relevant VMs together.

1. In the Azure portal, select **Virtual machines**, and select the VM you want to move into Availability Zones.
2. In **Operations**, select **Disaster recovery**.
3. In **Configure disaster recovery > Target region**, select the target region to which you'll replicate. Ensure this region [supports](#) Availability Zones.



4. Select **Next: Advanced settings**.
5. Choose the appropriate values for the target subscription, target VM resource group, and virtual network.
6. In the **Availability** section, choose the Availability Zone into which you want to move the VM.

## NOTE

If you don't see the option for availability set or Availability Zone, ensure that the [prerequisites](#) are met and the [preparation](#) of source VMs is complete.

The screenshot shows the 'Review + Start replication' step in the Azure portal. Under the 'Availability' section, a red box highlights the 'Availability zone' dropdown which lists three options: 1, 2, and 3. Other sections like 'Storage settings', 'Replication settings', and 'Extension settings' are also visible.

- Select **Enable Replication**. This action starts a job to enable replication for the VM.

## Check settings

After the replication job has finished, you can check the replication status, modify replication settings, and test the deployment.

- In the VM menu, select **Disaster recovery**.
- You can check replication health, the recovery points that have been created and the source, and target regions on the map.

The screenshot shows the 'Disaster recovery' blade for a specific VM. The left sidebar has 'Disaster recovery' selected. The main area shows replication settings (Active location: East US, Target location: South Central US), replication health (Healthy), and latest recovery points (Crash-consistent: 8/21/2018, 3:23:56 PM; App-consistent: 8/21/2018, 3:23:56 PM). A world map on the right shows the geographical distribution of recovery points.

## Test the configuration

- In the virtual machine menu, select **Disaster recovery**.

2. Select the **Test Failover** icon.
3. In **Test Failover**, select a recovery point to use for the failover:
  - **Latest processed:** Fails the VM over to the latest recovery point that was processed by the Site Recovery service. The time stamp is shown. With this option, no time is spent processing data, so it provides a low recovery time objective (RTO).
  - **Latest app-consistent:** This option fails over all VMs to the latest app-consistent recovery point. The time stamp is shown.
  - **Custom:** Select any recovery point.
4. Select the test target Azure virtual network to which you want to move the Azure VMs to test the configuration.

#### IMPORTANT

We recommend that you use a separate Azure VM network for the test failure, and not the production network in the target region into which you want to move your VMs.

5. To start testing the move, select **OK**. To track progress, select the VM to open its properties. Or, you can select the **Test Failover** job in the vault name > **Settings** > **Jobs** > **Site Recovery jobs**.
6. After the failover finishes, the replica Azure VM appears in the Azure portal > **Virtual Machines**. Make sure that the VM is running, sized appropriately, and connected to the appropriate network.
7. If you want to delete the VM created as part of testing the move, select **Cleanup test failover** on the replicated item. In **Notes**, record and save any observations associated with the test.

## Move to the target region and confirm

1. In the virtual machine menu, select **Disaster recovery**.
2. Select the **Failover** icon.
3. In **Failover**, select **Latest**.
4. Select **Shut down machine before beginning failover**. Site Recovery attempts to shut down the source VM before triggering the failover. Failover continues even if shutdown fails. You can follow the failover progress on the **Jobs** page.
5. After the job is finished, check that the VM appears in the target Azure region as expected.
6. In **Replicated items**, right-click the VM > **Commit**. This finishes the move process to the target region. Wait until the commit job is finished.

## Discard the resource in the source region

Go to the VM. Select **Disable Replication**. This action stops the process of copying the data for the VM.

#### IMPORTANT

Do the preceding step to avoid getting charged for Site Recovery replication after the move. The source replication settings are cleaned up automatically. Note that the Site Recovery extension that is installed as part of the replication isn't removed and needs to be removed manually.

## Next steps

In this tutorial, you increased the availability of an Azure VM by moving into an availability set or Availability Zone. Now you can set disaster recovery for the moved VM.

[Set up disaster recovery after migration](#)

# Migrate from Amazon Web Services (AWS) and other platforms to Managed Disks in Azure

11/13/2019 • 4 minutes to read • [Edit Online](#)

You can upload VHD files from AWS or on-premises virtualization solutions to Azure to create VMs that take advantage of Managed Disks. Azure Managed Disks removes the need to manage storage accounts for Azure IaaS VMs. You have to only specify the type (Premium or Standard) and size of disk you need, and Azure creates and manages the disk for you.

You can upload either generalized and specialized VHDs.

- **Generalized VHD** - has had all of your personal account information removed using Sysprep.
- **Specialized VHD** - maintains the user accounts, applications, and other state data from your original VM.

## IMPORTANT

Before uploading any VHD to Azure, you should follow [Prepare a Windows VHD or VHDX to upload to Azure](#)

| SCENARIO                                                                                                                | DOCUMENTATION                                                                   |
|-------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| You have existing AWS EC2 instances that you would like to migrate to Azure VMs using managed disks                     | <a href="#">Move a VM from Amazon Web Services (AWS) to Azure</a>               |
| You have a VM from another virtualization platform that you would like to use as an image to create multiple Azure VMs. | <a href="#">Upload a generalized VHD and use it to create a new VM in Azure</a> |
| You have a uniquely customized VM that you would like to recreate in Azure.                                             | <a href="#">Upload a specialized VHD to Azure and create a new VM</a>           |

## Overview of Managed Disks

Azure Managed Disks simplifies VM management by removing the need to manage storage accounts. Managed Disks also benefit from better reliability of VMs in an Availability Set. It ensures that the disks of different VMs in an Availability Set are sufficiently isolated from each other to avoid a single point of failure. It automatically places disks of different VMs in an Availability Set in different Storage scale units (stamps) which limits the impact of single Storage scale unit failures caused due to hardware and software failures. Based on your needs, you can choose from four types of storage options. To learn about the available disk types, see our article [Select a disk type](#).

## Plan for the migration to Managed Disks

This section helps you to make the best decision on VM and disk types.

If you are planning on migrating from unmanaged disks to managed disks, you should be aware that users with the [Virtual Machine Contributor](#) role will not be able to change the VM size (as they could pre-conversion). This is because VMs with managed disks require the user to have the Microsoft.Compute/disks/write permission on the OS disks.

### Location

Pick a location where Azure Managed Disks are available. If you are migrating to Premium Managed Disks, also

ensure that Premium storage is available in the region where you are planning to migrate to. See [Azure Services by Region](#) for up-to-date information on available locations.

## VM sizes

If you are migrating to Premium Managed Disks, you have to update the size of the VM to Premium Storage capable size available in the region where VM is located. Review the VM sizes that are Premium Storage capable. The Azure VM size specifications are listed in [Sizes for virtual machines](#). Review the performance characteristics of virtual machines that work with Premium Storage and choose the most appropriate VM size that best suits your workload. Make sure that there is sufficient bandwidth available on your VM to drive the disk traffic.

## Disk sizes

### Premium Managed Disks

There are seven types of premium managed disks that can be used with your VM and each has specific IOPs and throughput limits. Take into consideration these limits when choosing the Premium disk type for your VM based on the needs of your application in terms of capacity, performance, scalability, and peak loads.

| PREMIUM DISKS TYPE  | P4               | P6               | P10               | P15               | P20               | P30               | P40               | P50               |
|---------------------|------------------|------------------|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|
| Disk size           | 32 GB            | 64 GB            | 128 GB            | 256 GB            | 512 GB            | 1024 GB (1 TB)    | 2048 GB (2 TB)    | 4095 GB (4 TB)    |
| IOPS per disk       | 120              | 240              | 500               | 1100              | 2300              | 5000              | 7500              | 7500              |
| Throughput per disk | 25 MB per second | 50 MB per second | 100 MB per second | 125 MB per second | 150 MB per second | 200 MB per second | 250 MB per second | 250 MB per second |

### Standard Managed Disks

There are seven types of standard managed disks that can be used with your VM. Each of them have different capacity but have same IOPS and throughput limits. Choose the type of Standard Managed disks based on the capacity needs of your application.

| STANDARD DISK TYPE  | S4               | S6               | S10              | S15              | S20              | S30              | S40              | S50              |
|---------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|------------------|
| Disk size           | 30 GB            | 64 GB            | 128 GB           | 256 GB           | 512 GB           | 1024 GB (1 TB)   | 2048 GB (2TB)    | 4095 GB (4 TB)   |
| IOPS per disk       | 500              | 500              | 500              | 500              | 500              | 500              | 500              | 500              |
| Throughput per disk | 60 MB per second |

## Disk caching policy

### Premium Managed Disks

By default, disk caching policy is *Read-Only* for all the Premium data disks, and *Read-Write* for the Premium operating system disk attached to the VM. This configuration setting is recommended to achieve the optimal performance for your application's IOs. For write-heavy or write-only data disks (such as SQL Server log files),

disable disk caching so that you can achieve better application performance.

## Pricing

Review the [pricing for Managed Disks](#). Pricing of Premium Managed Disks is same as the Premium Unmanaged Disks. But pricing for Standard Managed Disks is different than Standard Unmanaged Disks.

## Next Steps

- Before uploading any VHD to Azure, you should follow [Prepare a Windows VHD or VHDX to upload to Azure](#)

# Move a Windows VM from Amazon Web Services (AWS) to an Azure virtual machine

11/13/2019 • 2 minutes to read • [Edit Online](#)

If you are evaluating Azure virtual machines for hosting your workloads, you can export an existing Amazon Web Services (AWS) EC2 Windows VM instance then upload the virtual hard disk (VHD) to Azure. Once the VHD is uploaded, you can create a new VM in Azure from the VHD.

This article covers moving a single VM from AWS to Azure. If you want to move VMs from AWS to Azure at scale, see [Migrate virtual machines in Amazon Web Services \(AWS\) to Azure with Azure Site Recovery](#).

## Prepare the VM

You can upload both generalized and specialized VHDs to Azure. Each type requires that you prepare the VM before exporting from AWS.

- **Generalized VHD** - a generalized VHD has had all of your personal account information removed using Sysprep. If you intend to use the VHD as an image to create new VMs from, you should:
  - [Prepare a Windows VM](#).
  - Generalize the virtual machine using Sysprep.
- **Specialized VHD** - a specialized VHD maintains the user accounts, applications and other state data from your original VM. If you intend to use the VHD as-is to create a new VM, ensure the following steps are completed.
  - [Prepare a Windows VHD to upload to Azure](#). **Do not** generalize the VM using Sysprep.
  - Remove any guest virtualization tools and agents that are installed on the VM (i.e. VMware tools).
  - Ensure the VM is configured to pull its IP address and DNS settings via DHCP. This ensures that the server obtains an IP address within the VNet when it starts up.

## Export and download the VHD

Export the EC2 instance to a VHD in an Amazon S3 bucket. Follow the steps in the Amazon documentation article [Exporting an Instance as a VM Using VM Import/Export](#) and run the `create-instance-export-task` command to export the EC2 instance to a VHD file.

The exported VHD file is saved in the Amazon S3 bucket you specify. The basic syntax for exporting the VHD is below, just replace the placeholder text in <brackets> with your information.

```
aws ec2 create-instance-export-task --instance-id <instanceID> --target-environment Microsoft \
--export-to-s3-task DiskImageFormat=VHD,ContainerFormat=ova,S3Bucket=<bucket>,S3Prefix=<prefix>
```

Once the VHD has been exported, follow the instructions in [How Do I Download an Object from an S3 Bucket?](#) to download the VHD file from the S3 bucket.

### IMPORTANT

AWS charges data transfer fees for downloading the VHD. See [Amazon S3 Pricing](#) for more information.

## Next steps

Now you can upload the VHD to Azure and create a new VM.

- If you ran Sysprep on your source to **generalize** it before exporting, see [Upload a generalized VHD and use it to create a new VMs in Azure](#)
- If you did not run Sysprep before exporting, the VHD is considered **specialized**, see [Upload a specialized VHD to Azure and create a new VM](#)

# Create a Linux VM from a custom disk with the Azure CLI

12/23/2019 • 4 minutes to read • [Edit Online](#)

This article shows you how to upload a customized virtual hard disk (VHD), and how to copy an existing VHD in Azure. The newly created VHD is then used to create new Linux virtual machines (VMs). You can install and configure a Linux distro to your requirements and then use that VHD to create a new Azure virtual machine.

To create multiple VMs from your customized disk, first create an image from your VM or VHD. For more information, see [Create a custom image of an Azure VM by using the CLI](#).

You have two options to create a custom disk:

- Upload a VHD
- Copy an existing Azure VM

## Requirements

To complete the following steps, you'll need:

- A Linux virtual machine that has been prepared for use in Azure. The [Prepare the VM](#) section of this article covers how to find distro-specific information on installing the Azure Linux Agent (waagent), which is needed for you to connect to a VM with SSH.
- The VHD file from an existing [Azure-endorsed Linux distribution](#) (or see [information for non-endorsed distributions](#)) to a virtual disk in the VHD format. Multiple tools exist to create a VM and VHD:
  - Install and configure [QEMU](#) or [KVM](#), taking care to use VHD as your image format. If needed, you can [convert an image](#) with `qemu-img convert`.
  - You can also use Hyper-V [on Windows 10](#) or [on Windows Server 2012/2012 R2](#).

### NOTE

The newer VHDX format is not supported in Azure. When you create a VM, specify VHD as the format. If needed, you can convert VHDX disks to VHD with [qemu-img convert](#) or the [Convert-VHD](#) PowerShell cmdlet. Azure does not support uploading dynamic VHDs, so you'll need to convert such disks to static VHDs before uploading. You can use tools such as [Azure VHD Utilities for GO](#) to convert dynamic disks during the process of uploading them to Azure.

- Make sure that you have the latest [Azure CLI](#) installed and you are signed in to an Azure account with [az login](#).

In the following examples, replace example parameter names with your own values, such as `myResourceGroup`, `mystorageaccount`, and `mydisks`.

## Prepare the VM

Azure supports various Linux distributions (see [Endorsed Distributions](#)). The following articles describe how to prepare the various Linux distributions that are supported on Azure:

- [CentOS-based Distributions](#)
- [Debian Linux](#)
- [Oracle Linux](#)
- [Red Hat Enterprise Linux](#)

- [SLES & openSUSE](#)
- [Ubuntu](#)
- [Others: Non-Endorsed Distributions](#)

Also see the [Linux Installation Notes](#) for more general tips on preparing Linux images for Azure.

#### NOTE

The [Azure platform SLA](#) applies to VMs running Linux only when one of the endorsed distributions is used with the configuration details as specified under "Supported Versions" in [Linux on Azure-Endorsed Distributions](#).

## Option 1: Upload a VHD

You can now upload VHD straight into a managed disk. For instructions, see [Upload a VHD to Azure using Azure CLI](#).

## Option 2: Copy an existing VM

You can also create a customized VM in Azure and then copy the OS disk and attach it to a new VM to create another copy. This is fine for testing, but if you want to use an existing Azure VM as the model for multiple new VMs, create an *image* instead. For more information about creating an image from an existing Azure VM, see [Create a custom image of an Azure VM by using the CLI](#).

If you want to copy an existing VM to another region, you might want to use azcopy to [create a copy of a disk in another region](#).

Otherwise, you should take a snapshot of the VM and then create a new OS VHD from the snapshot.

### Create a snapshot

This example creates a snapshot of a VM named *myVM* in resource group *myResourceGroup* and creates a snapshot named *osDiskSnapshot*.

```
osDiskId=$(az vm show -g myResourceGroup -n myVM --query "storageProfile.osDisk.managedDisk.id" -o tsv)
az snapshot create \
 -g myResourceGroup \
 --source "$osDiskId" \
 --name osDiskSnapshot
```

### Create the managed disk

Create a new managed disk from the snapshot.

Get the ID of the snapshot. In this example, the snapshot is named *osDiskSnapshot* and it is in the *myResourceGroup* resource group.

```
snapshotId=$(az snapshot show --name osDiskSnapshot --resource-group myResourceGroup --query [id] -o tsv)
```

Create the managed disk. In this example, we will create a managed disk named *myManagedDisk* from our snapshot, where the disk is in standard storage and sized at 128 GB.

```
az disk create \
 --resource-group myResourceGroup \
 --name myManagedDisk \
 --sku Standard_LRS \
 --size-gb 128 \
 --source $snapshotId
```

## Create the VM

Create your VM with [az vm create](#) and attach (--attach-os-disk) the managed disk as the OS disk. The following example creates a VM named *myNewVM* using the managed disk you created from your uploaded VHD:

```
az vm create \
 --resource-group myResourceGroup \
 --location eastus \
 --name myNewVM \
 --os-type linux \
 --attach-os-disk myManagedDisk
```

You should be able to SSH into the VM with the credentials from the source VM.

## Next steps

After you have prepared and uploaded your custom virtual disk, you can read more about [using Resource Manager and templates](#). You may also want to [add a data disk](#) to your new VMs. If you have applications running on your VMs that you need to access, be sure to [open ports and endpoints](#).

2 minutes to read

# Frequently asked question about Linux Virtual Machines

2/12/2020 • 3 minutes to read • [Edit Online](#)

This article addresses some common questions about Linux virtual machines created in Azure using the Resource Manager deployment model. For the Windows version of this topic, see [Frequently asked question about Windows Virtual Machines](#)

## What can I run on an Azure VM?

All subscribers can run server software on an Azure virtual machine. For more information, see [Linux on Azure-Endorsed Distributions](#)

## How much storage can I use with a virtual machine?

Each data disk can be up to 32,767 GiB. The number of data disks you can use depends on the size of the virtual machine. For details, see [Sizes for Virtual Machines](#).

Azure Managed Disks are the recommended disk storage offerings for use with Azure Virtual Machines for persistent storage of data. You can use multiple Managed Disks with each Virtual Machine. Managed Disks offer two types of durable storage options: Premium and Standard Managed Disks. For pricing information, see [Managed Disks Pricing](#).

Azure storage accounts can also provide storage for the operating system disk and any data disks. Each disk is a .vhd file stored as a page blob. For pricing details, see [Storage Pricing Details](#).

## How can I access my virtual machine?

Establish a remote connection to sign on to the virtual machine, using Secure Shell (SSH). See the instructions on how to connect [from Windows](#) or [from Linux and Mac](#). By default, SSH allows a maximum of 10 concurrent connections. You can increase this number by editing the configuration file.

If you're having problems, check out [Troubleshoot Secure Shell \(SSH\) connections](#).

## Can I use the temporary disk (/dev/sdb1) to store data?

Don't use the temporary disk (/dev/sdb1) to store data. It is only there for temporary storage. You risk losing data that can't be recovered.

## Can I copy or clone an existing Azure VM?

Yes. For instructions, see [How to create a copy of a Linux virtual machine in the Resource Manager deployment model](#).

## Why am I not seeing Canada Central and Canada East regions through Azure Resource Manager?

The two new regions of Canada Central and Canada East are not automatically registered for virtual machine creation for existing Azure subscriptions. This registration is done automatically when a virtual machine is deployed through the Azure portal to any other region using Azure Resource Manager. After a virtual machine is

deployed to any other Azure region, the new regions should be available for subsequent virtual machines.

## Can I add a NIC to my VM after it's created?

Yes, this is now possible. The VM first needs to be stopped deallocated. Then you can add or remove a NIC (unless it's the last NIC on the VM).

## Are there any computer name requirements?

Yes. The computer name can be a maximum of 64 characters in length. See [Naming conventions rules and restrictions](#) for more information around naming your resources.

## Are there any resource group name requirements?

Yes. The resource group name can be a maximum of 90 characters in length. See [Naming conventions rules and restrictions](#) for more information about resource groups.

## What are the username requirements when creating a VM?

Usernames should be 1 - 32 characters in length.

The following usernames are not allowed:

|               |         |                  |        |
|---------------|---------|------------------|--------|
| administrator | admin   | user             | user1  |
| test          | user2   | test1            | user3  |
| admin1        | 1       | 123              | a      |
| actuser       | adm     | admin2           | aspnet |
| backup        | console | david            | guest  |
| john          | owner   | root             | server |
| sql           | support | support_388945a0 | sys    |
| test2         | test3   | user4            | user5  |
| video         |         |                  |        |

## What are the password requirements when creating a VM?

There are varying password length requirements, depending on the tool you are using:

- Portal - between 12 - 72 characters
- PowerShell - between 8 - 123 characters
- CLI - between 12 - 123

Passwords must also meet 3 out of the following 4 complexity requirements:

- Have lower characters

- Have upper characters
- Have a digit
- Have a special character (Regex match [\W\_])

The following passwords are not allowed:

|            |            |           |             |            |
|------------|------------|-----------|-------------|------------|
| abc@123    | P@\$\$w0rd | P@ssw0rd  | P@ssword123 | Pa\$\$word |
| pass@word1 | Password!  | Password1 | Password22  | iloveyou!  |