

Azure Backup features and scenarios

5 minutes

Azure Backup is a suite of components that make it easy to back up machines and workloads in Azure or on-premises. Azure Backup also enables workloads like SQL Server or SharePoint to have additional backup and restore options.

To address your company's business continuity and disaster recovery (BCDR) plan, there must be a full backup and restore capability for all of your high-risk servers. You've been asked to enable and test backup and restore functionality for these critical Windows and Linux assets.

In this unit, you'll look at how Azure Backup works, and study some of the supported use cases for Azure Backup.

What is Azure Backup?

Azure Backup provides cloud-based backup and restore services for both Azure and on-premises virtual machines. Data, workloads, and machine state can all be backed up automatically at a granular level. Azure Backup offers integration with Microsoft-specific applications such as SQL Server, SharePoint, and Exchange.

In contrast to traditional backup solutions that can take considerable effort to set up, Azure Backup is easily managed through the Azure portal. Backups are stored in an Azure Recovery Services vault after you set up the appropriate component on the target machine.

Azure Backup versus Azure Site Recovery

The Azure Backup and Azure Site Recovery services both provide system recovery, but they have their differences:

- **Azure Site Recovery** Replicates virtual machine workloads to secondary locations for failover if a disaster affects a whole site.
- **Azure Backup** Recovers data more granularly. For example, it recovers virtual machine disks, or files and folders that became corrupted or were accidentally deleted by users.

Why use Azure Backup?

Traditional backup solutions, such as disk and tape, don't offer the highest level of integration with cloud-based solutions. Azure Backup has several benefits over more traditional backup solutions:

- **Automatic storage management** You can maintain a fully Azure-based backup solution, or a heterogeneous solution where data is backed up and stored both on-premises and in Azure. Using on-premises storage devices is free, and storing within Azure uses a pay-as-you-go model.
- **High availability** Because the service is cloud based, it's redundant and highly available by nature. The service doesn't need to be maintained, upgraded, or patched as a traditional solution would be.
- **Unlimited data transfer** Inbound and outbound backup traffic to your Azure subscription is unlimited.
- **Data security** The service uses AES 256-bit encryption for on-premises virtual machines and Storage Service Encryption for Azure virtual machines. Data is secured at rest on the Azure platform, and then decrypted when an authorized person or service accesses it.
- **No-limit retention times** Long-term and short-term options are available to keep your data, depending on your data retention policy.
- **Highly available storage** Two types of storage help ensure that data is always available
 - Locally redundant storage (LRS): Replicates data three times within the same region.
 - Geo-redundant storage (GRS): Replicates data to another region within the geography. This is the default. We recommend this option in most cases, because it uses LRS in a primary region and a secondary region.

Azure Backup types

Azure Backup supports several backup scenarios, for both virtual machines and on-premises machines. Each scenario requires a combination of backup type and agent to make the backup happen.

Location	OS	Environment	Level	Notes
On-premises	Windows	Virtual	Files, folders, volumes, system state, and app data	Uses System Center Data Protection Manager (DPM) or Microsoft Azure Backup Server (MABS). This scenario supports app-aware snapshots.

Location	OS	Environment	Level	Notes
On-premises	Windows	Physical	Files, folders, volumes, system state, and app data	Uses DPM or MABS. This scenario supports app-aware snapshots.
On-premises	Windows	Both	Direct backup of files, folders, and system state	Uses the Microsoft Azure Recovery Services (MARS) agent. This is <i>not</i> an app-aware backup.
On-premises	Linux	Virtual	Direct backup of files	Not supported with MARS.
On-premises	Linux	Physical	Direct backup of files	Not supported with MARS.
On-premises	Linux	Virtual	Files, folders, volumes, system state, and app data	Uses DPM or MABS. This scenario supports app-aware snapshots.
On-premises	Linux	Physical	Files, folders, volumes, system state, and app data	Not supported.
Azure	Windows	Virtual	Entire virtual machine	Uses the Azure Backup virtual machine extension. This scenario provides app-aware backups.
Azure	Windows	Virtual	Files, folders, and system state	Uses the virtual machine extension and MARS. This scenario provides app-aware backups.
Azure	Linux	Virtual	Entire virtual machine	Uses the Azure Backup virtual machine extension. This scenario provides file-consistent backups.
Azure	Linux	Virtual	Files, folders, volumes, system state, and app data	Uses DPM or MARS. This scenario provides app-aware snapshots.

SQL Server backups


If you need to back up SQL Server workloads, other options are available. Azure Backup can install a workload backup extension on a SQL Server instance on Windows to support the following options:

- **Full:** Backs up the entire database and file groups. It also contains enough logs to do a restore. Transaction logs hold records of the most recent additions or removals of records in the database. Recent transaction logs are needed to perform an up-to-date restore of a database.
- **Differential:** Based on the last full backup that was performed, and captures only blocks of data that changed since the last full backup.
- **Transaction log:** Allows a point-in-time restoration of a database.

SQL Server on Linux does not currently integrate with Azure Backup.

Check your knowledge

1. Which is the best way to back up an entire Azure virtual machine that's running Linux?

- ☒ Use the Azure Backup extension 
- Azure Backup works on Azure virtual machines without the need to install an agent. It meets the goal of a disk-level backup.**
- ☐ Use the MABS or DPM agent
- ☐ Use the MARS agent

2. Why would you use MABS or DPM instead of the MARS agent to do backups?

- ☐ File-level and folder-level backups are required.
- ☐ Physical Windows and Linux backups are required.
- ☒ Backup of running apps is required. 
- Only MABS and DPM support app-aware backups.**

Next unit: Back up an Azure virtual machine by using Azure Backup

Back up an Azure virtual machine by using Azure Backup

5 minutes

You want to ensure that the backup and restore jobs you put in place offer a way to recover your company's servers. With this requirement in mind, you want to investigate the best way to implement backup for your virtual machines.

Virtual machines that are hosted on Azure can take advantage of Azure Backup. You can easily back up and restore machines without installing additional software.

In this unit, you'll explore all the methods of backing up Azure virtual machines provided by Azure Backup and make a decision on which to implement.

Snapshots

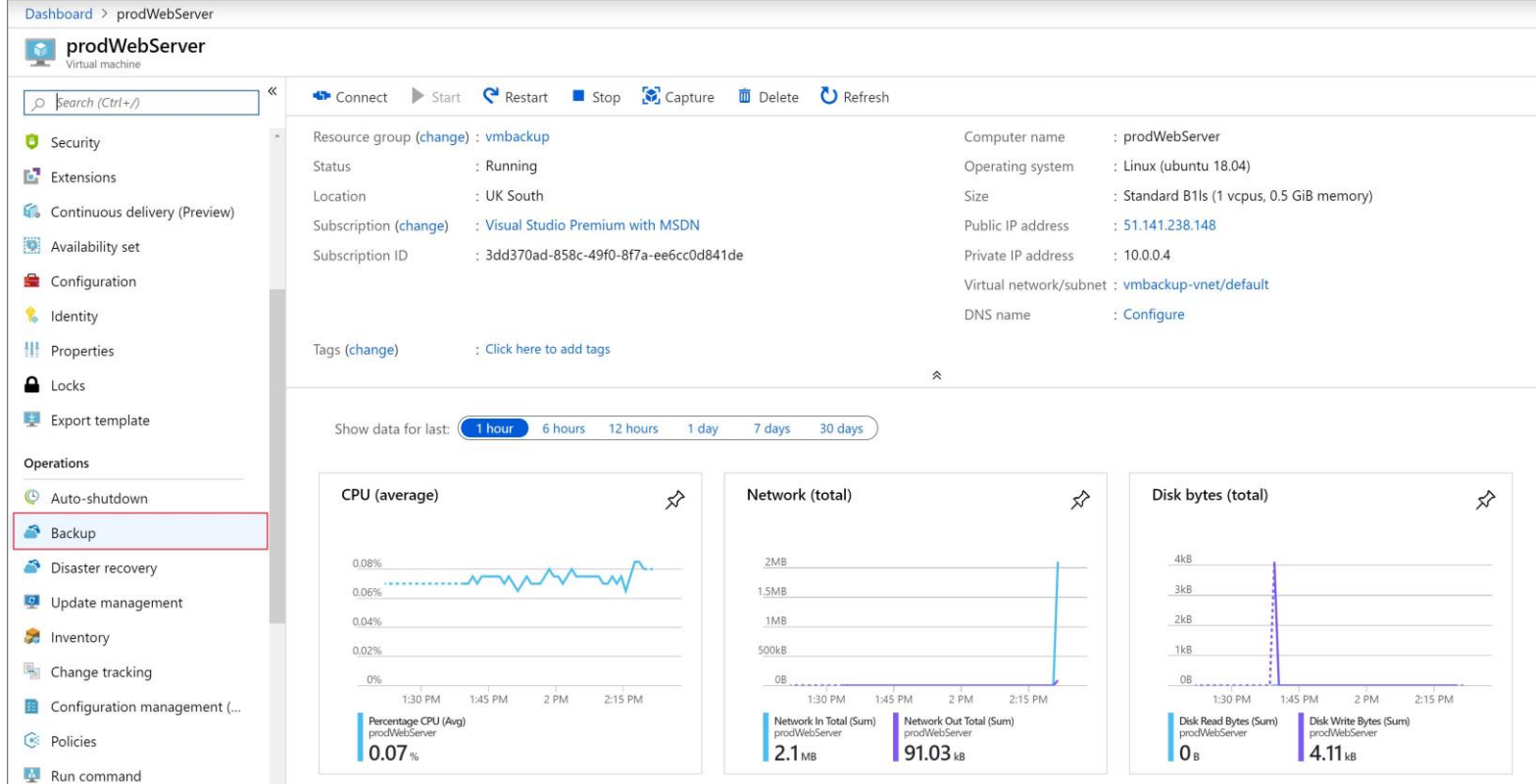
A snapshot is a point-in-time backup of all disks on the virtual machine. For Azure virtual machines, Azure Backup uses different extensions for each supporting operating system:

Extension	OS	Description
VMSnapshot	Windows	The extension works with Volume Shadow Copy Service (VSS) to take a copy of the data on disk and in memory.
VMSnapshotLinux	Linux	The snapshot is a copy of the disk.

Depending on how the snapshot is taken and what it includes, you can achieve different levels of consistency:

- **Application consistent**
 - The snapshot captures the virtual machine as a whole. It uses VSS writers to capture the content of the machine memory and any pending I/O operations.
 - For Linux machines, you'll need to write custom pre or post scripts per app to capture the application state.
 - You can get complete consistency for the virtual machine and all running applications.
- **File system consistent**
 - If VSS fails on Windows, or the pre and post scripts fail on Linux, Azure Backup will still create a file-system-consistent snapshot.
 - During a recovery, no corruption occurs within the machine. But installed applications need to do their own cleanup during startup to become consistent.
- **Crash consistent**
 - This level of consistency typically occurs if the virtual machine is shut down at the time of the backup.
 - No I/O operations or memory contents are captured during this type of backup. This method doesn't guarantee data consistency for the OS or app.

Recovery Services vault



You use a Recovery Services vault to manage and store the backup data in Azure. Typically a vault consists of data copies, configuration information for virtual machines, a server, and workstation workloads. You can also use Recovery Services vaults to hold backup data for infrastructure-as-a-service (IaaS) virtual machines.

The vault provides a single place to manage your backups. It's accessible in context to the resource that it helps protect. For example, with the vault, you can:

- Monitor Azure virtual machine backups. Hybrid scenarios are also supported, so on-premises machines protected with Azure Backup can also be monitored.
- Manage backup jobs and their properties.
- Take advantage of access management control, which allows fine-tuned permissions for administrators.
- Quickly restore files or folders within virtual machines instead of recovering the whole machine.
- Be assured that all data located in a Recovery Services vault is secured while at rest.

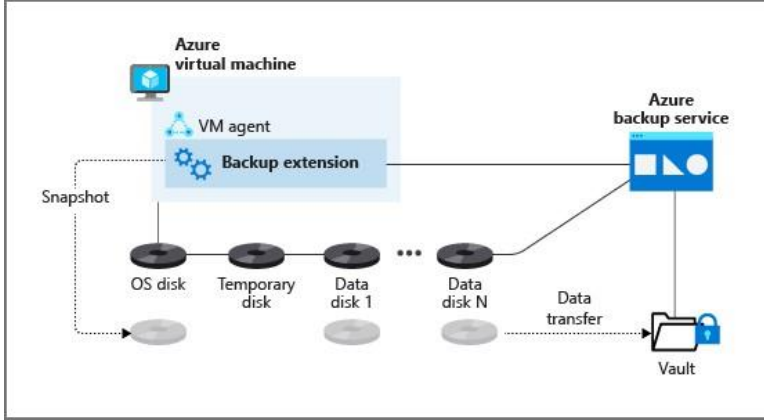
Cost considerations

There's a cost for every virtual machine backed up, and it starts as soon as the first backup is completed. The pricing is based on the size of the backed-up data, because the cost is based on the size of the allocated disk space. For SQL Server backups, cost is based on the size of the database backup file.

Backup agents

Azure Backup uses agents to support a variety of backup scenarios. The agents can be installed directly on physical or virtual machines, or be part of a dedicated backup server. The agent that you choose will differ slightly depending on whether you need to back up an entire virtual machine, files and folders, or running apps.

Azure Backup virtual machine extension

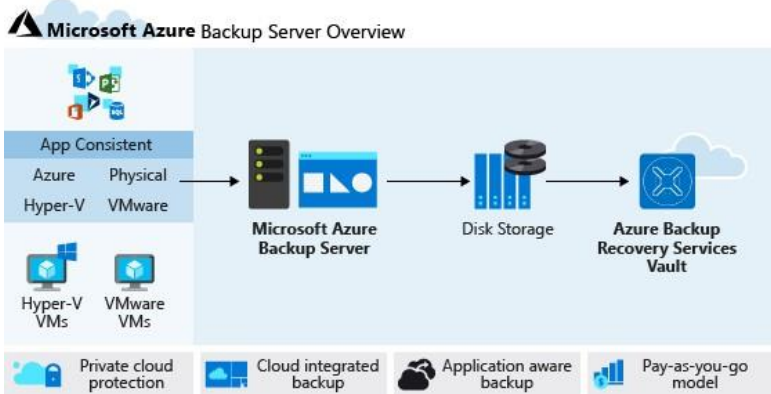


The Azure Backup extension is the default backup choice, because it's the most simple and straightforward method to quickly back up an Azure virtual machine. The administrator doesn't need to take any action other than to configure the backup job.

During the first backup, a *VMSnapshot* (for Windows) or *VMSnapshotLinux* (for Linux) extension is installed. These extensions take snapshots of the virtual machine's entire disk, which means they don't enable file-level or folder-level restores. The snapshots are created and stored in a Recovery Services vault.

If your company's virtual machines are in Azure, and you don't require file-level restores, your company should use the Azure Backup extension.

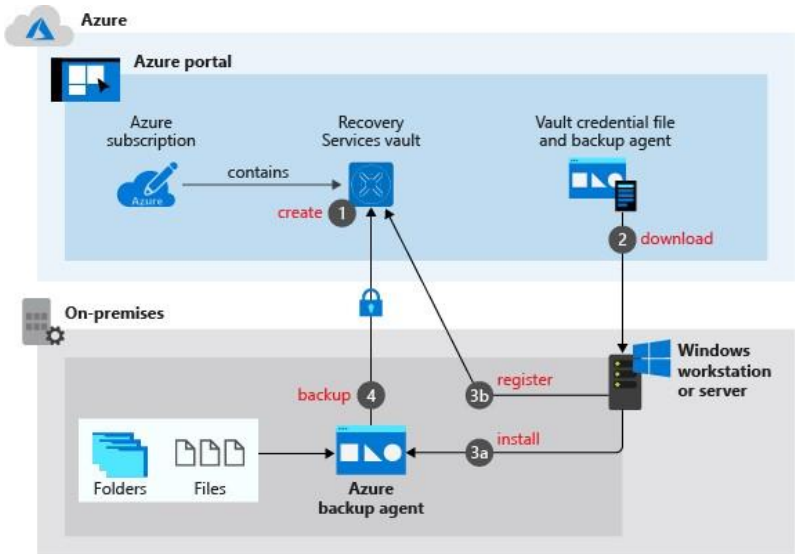
Microsoft Azure Backup Server protection agent



The Microsoft Azure Backup Server (MABS) agent installed on an Azure or on-premises virtual machine allows that machine to back up to an Azure Backup server. The MABS agent can back up and restore SQL and other application services. You can also support workloads like Exchange and SharePoint by using the *AzureBackupWindowsWorkload* extension.

Machines and workloads are backed up to an Azure Backup server, although this doesn't move these backups to a Recovery Services vault. If you need to move your backups to a Recovery Services vault, install the Microsoft Azure Recovery Services (MARS) agent.

Microsoft Azure Recovery Services agent



Azure Backup uses the MARS agent to back up Windows files, folders, and system state data to a Recovery Services vault. The agent is installed manually on the machines that you're backing up.

The MARS agent enhances the levels of backup if it's installed alongside the Azure Backup extension on an Azure virtual machine. MARS enables on-premises Windows machines to be backed up directly to a Recovery Services vault.

When the MARS agent is used in conjunction with an Azure Backup server, it will copy the snapshots from the server into a vault.

Backup process for an Azure virtual machine

1. The first stage of the backup job is installing the extension automatically. The *VMSnapshot* extension is for Windows machines, and the *VMSnapshotLinux* extension is for Linux virtual machines.

In a Windows environment, Azure Backup uses the Volume Shadow Copy Service to take app-consistent snapshots of the virtual machine that's used for the backup procedure.

In a Linux environment, Azure Backup takes file-consistent snapshots that are used for the backup procedure.
2. The snapshot is transferred to your Recovery Services vault in Azure.

Each disk for the selected virtual machine is backed up in parallel for optimization purposes.

After the first full backup, Azure Backup will identify the blocks of data that have changed. It will back up only that information, rather than the whole virtual machine a second time.
3. Snapshots can take up to 24 hours to transfer to the Recovery Services vault in Azure. When the transfer finishes, the service will remove the snapshot and create a recovery point for the machine.

Security

Azure Backup offers the ability to back up virtual machines encrypted with Azure Disk Encryption. Azure Storage also encrypts your backed-up data at rest by using Storage Service Encryption. Your data is automatically decrypted when it's retrieved.

Here are more details about the encryption types:

- Azure Disk Encryption encrypts your operating system and data disks. It works with BitLocker encryption keys (BEKs), which are safeguarded in a key vault as secrets. It also works with Azure Key Vault encryption keys (KEKs).

During the backup procedure, both BEKs and KEKs are backed up and encrypted. Users who have appropriate permissions can then restore the keys and secrets if needed, and also recover an encrypted virtual machine.
- Storage Service Encryption encrypts your backups when it's at rest after it has been copied to the vault. When a restore operation is called for the backed-up data, it's automatically decrypted and ready for use.

Next unit: Exercise - Back up an Azure virtual machine

Continue 

Exercise - Back up an Azure virtual machine

10 minutes

Your company is running a combination of Windows and Linux workloads. You've been asked to prove that Azure Backup is a good fit for your virtual machines. By using a combination of the Azure CLI and the Azure portal, you'll help protect both kinds of virtual machines with Azure Backup.

Azure Backup can be quickly enabled for virtual machines in Azure. You can enable Azure Backup from the portal, from the Azure CLI, or from PowerShell commands.

In this exercise, you'll create a virtual machine, set up a backup, and start a backup.

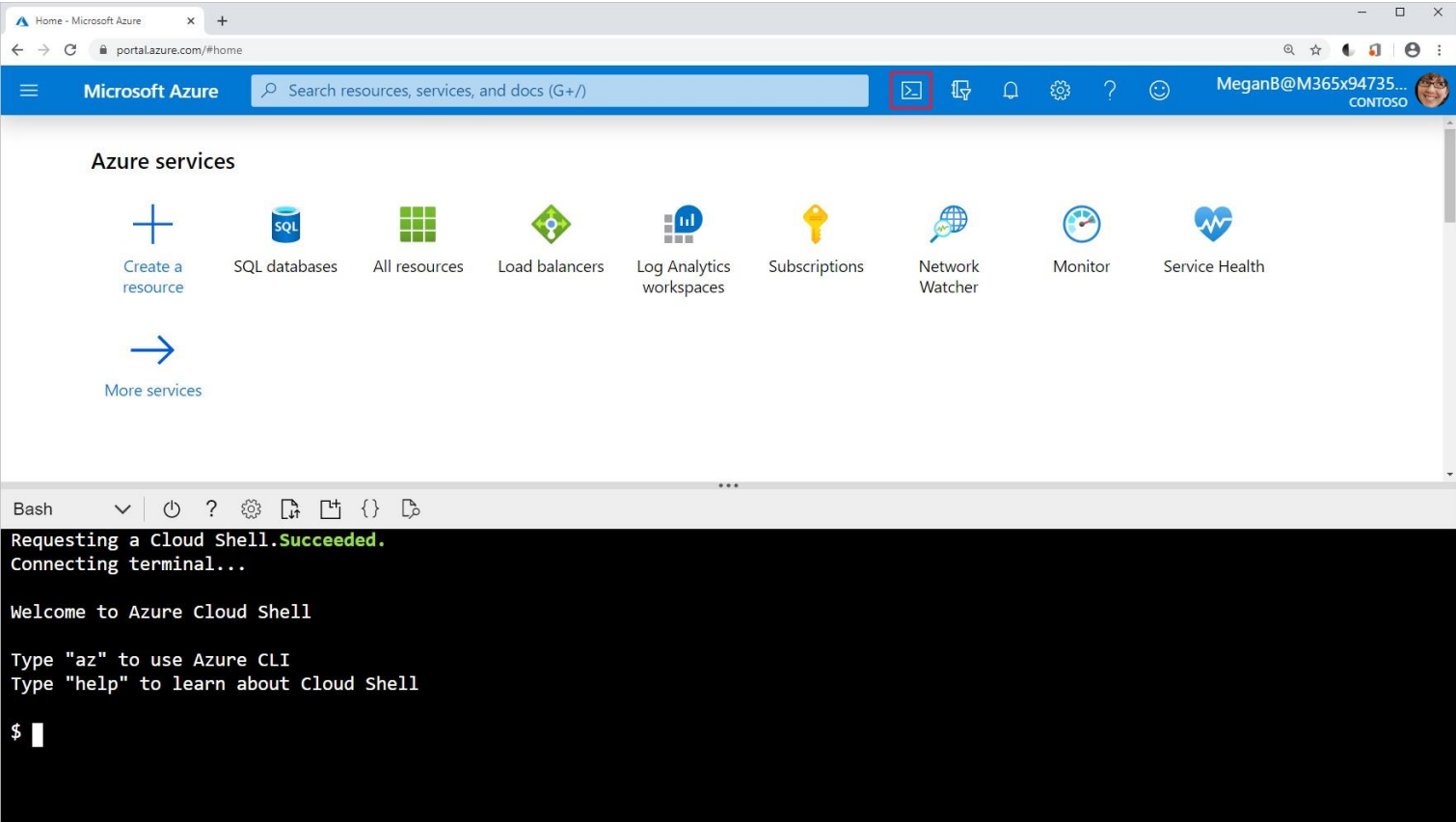
Not

This exercise is optional. If you don't have an Azure account, you can read through the instructions so you understand how to back up your virtual machines using Azure Backup. If you want to complete this exercise, but you don't have an Azure subscription or you prefer not to use your own subscription, you can use a free Azure account before you begin.

Create a backup for Azure virtual machines

Set up the environment

1. Sign in to the Azure portal and open Azure Cloud Shell.



2. Create a resource group to contain all the resources for this exercise.

Azure CLI

Copy

```
RGROUP=$(az group create --name vmbackups --location westus2 --output tsv --query name)
```

3. Use Cloud Shell to create a Northwind virtual network and a NorthwindInternalNet.

Azure CLI

Copy


```
az network vnet create \      --resource-group $RGROUP \      --name NorthwindInternal \
--address-prefix 10.0.0.0/16 \
--subnet-name NorthwindInternal1 \
--subnet-prefix 10.0.0.0/24
```

Create a Windows virtual machine by using the Azure CLI

Create the **NW-APP01** virtual machine by using the following command. Replace `<password>` with a password of your choice.

Azure CLI

```
az vm create \
  --resource-group $RGROUP \
  --name NW-APP01 \
  --size Standard_DS1_v2 \
  --vnet-name NorthwindInternal \
  --subnet NorthwindInternal1 \
  --image Win2016Datacenter \      --admin-
username admin123 \
  --no-wait \
  --admin-password <password>
```

Create a Linux virtual machine by using the Azure CLI

Create the **NW-RHEL01** virtual machine by using the following command.

Azure CLI

```
az vm create \
  --resource-group $RGROUP \
  --name NW-RHEL01 \
  --size Standard_DS1_v2 \
  --image RedHat:RHEL:7-RAW:latest \
  --authentication-type ssh \
  --generate-ssh-keys \
  --vnet-name NorthwindInternal \
  --subnet NorthwindInternal1
```

The command can take a few minutes to finish. Wait for it to finish before you move on to the next step.

Enable backup for a virtual machine by using the Azure portal

1. In the Azure portal, search for and select **Virtual machines**.

Home > Virtual machines

Virtual machines

Bob's Active Directory

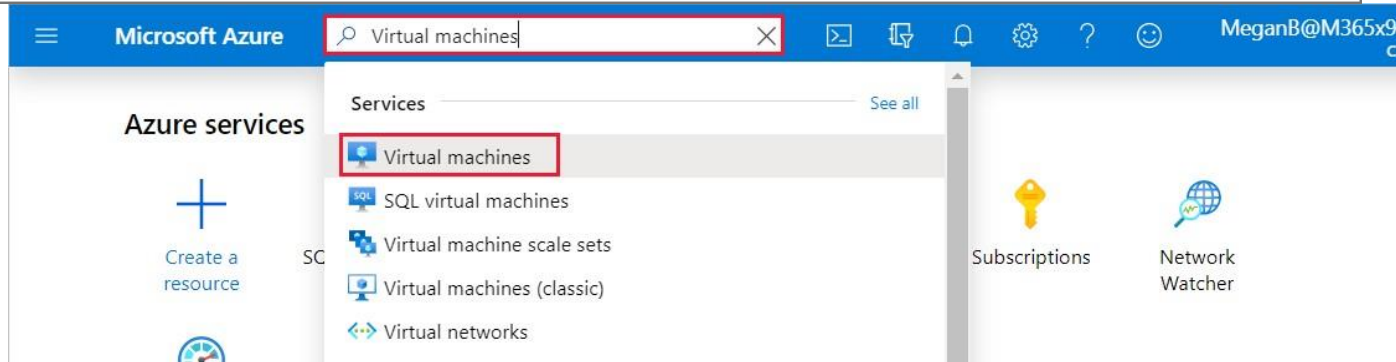
+ Add Reservations Edit columns Refresh Assign tags Start Restart Stop Delete Services

Subscriptions: All 2 selected – Don't see a subscription? Open Directory + Subscription settings

Filter by name... All subscriptions All resource groups All types All locations All tags

2 items

	NAME ↑↓	TYPE ↑↓	STATUS	RESOURCE GROUP ↑↓	LOCATION ↑↓	MAINTENANCE
<input type="checkbox"/>	NW-APP01	Virtual machine	Running	vmbackups	West US 2	-
<input type="checkbox"/>	NW-RHEL01	Virtual machine	Running	vmbackups	West US 2	-



- From the list, select the **NW-RHEL01** virtual machine that you created.
- In the sidebar, scroll down to **Operations**, select **Backup**, and then use the following information to create a backup:

Recovery Services vault

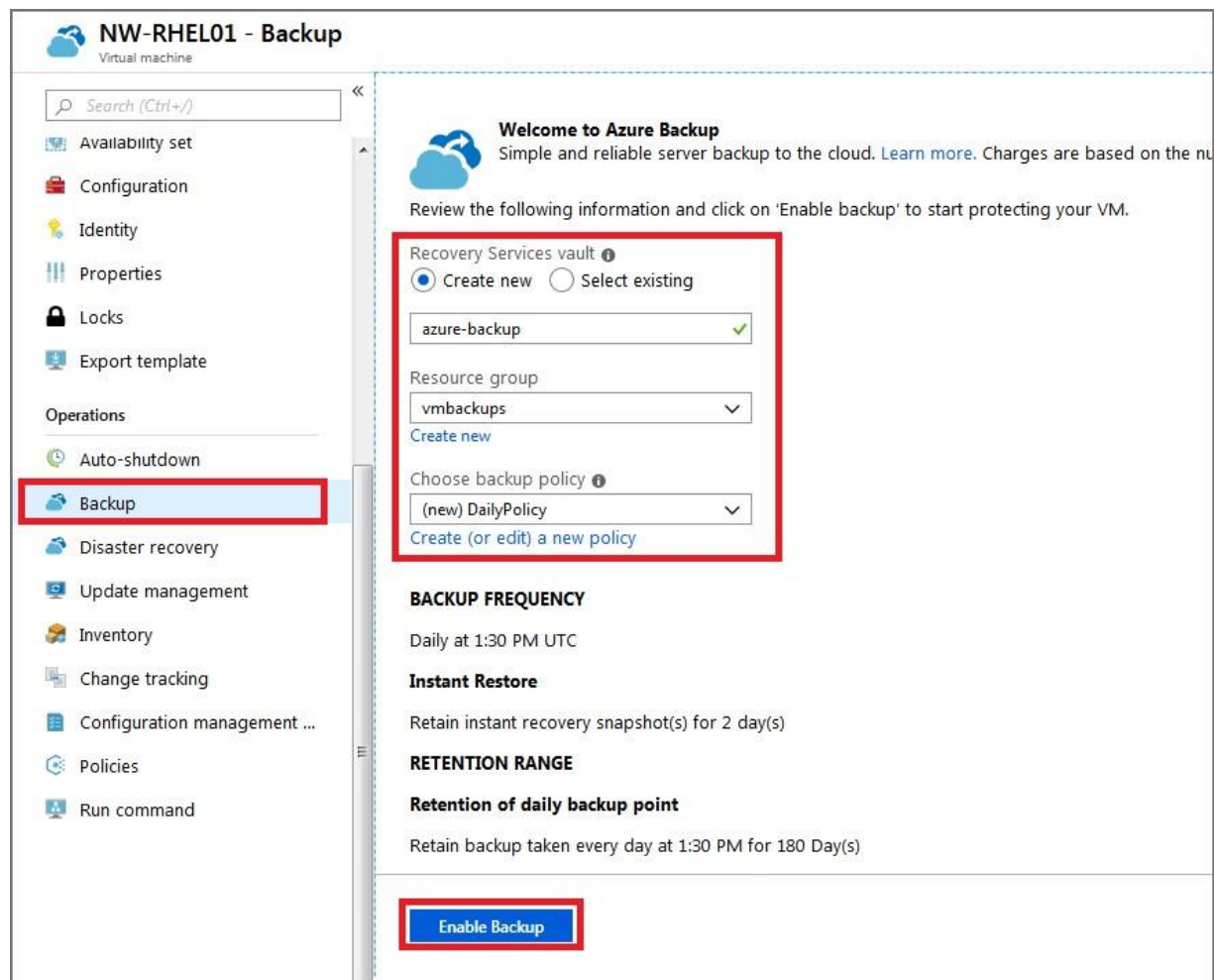
Select **Create new**, and enter **azure-backup** for the name.

Resource group

Select the **vmbackups** resource group that you created earlier.

Choose a backup policy

Select **(new) DailyPolicy**, which is a daily backup at 12:00 PM UTC, and a retention range of 180 days.



4. Select **Enable Backup**.
5. After the deployment finishes, select **NW-RHEL01** from the list of virtual machines.
6. You can access backup settings from the virtual machine menu by scrolling down to **Operations** and selecting **Backup**.
7. To perform the first backup for this server, select **Backup now**.
8. On the **Backup Now** page, select **OK**.

Enable a backup by using the Azure CLI

1. By using Cloud Shell, enable a backup for the **NW-APP01** virtual machine.

Azure CLI

NW-RHEL01 - Backup
Virtual machine

Search (Ctrl+/) << **Backup now** Restore VM File Recovery Stop backup Resume backup Delete backup data

Locks

Export template

Operations

Auto-shutdown

Backup

Disaster recovery

Update management

Inventory

Change tracking

Configuration management ...

Policies

Run command

Alerts and Jobs

[View all Alerts](#) (last 24 hours)

[View all Jobs](#) (last 24 hours)

Backup status

Backup Pre-Check ✓ Passed

Last backup status ⚠ Warning(Initial backup pending)

Summary

Recovery services vault [azure-backup](#)

Backup policy [DailyPolicy](#)

Oldest restore point -

Restore points

This list is filtered for last 30 days of restore points. To recover from restore point older than 30 days, [click here](#).

CRASH CONSISTENT 0 APPLICATION CONSISTENT 0 FILE-SYSTEM CONSISTENT 0

TIME	CONSISTENCY	RECOVERY TYPE
No restore points available.		

```
az backup protection enable-for-vm \
  --resource-group vmbackups \
  --vault-name azure-backup \
  -vm NW-APP01 \
  --policy-name DefaultPolicy
```

2. Monitor the progress of the setup by using the Azure CLI.

Azure CLI

```
az backup job list \
  --resource-group vmbackups \
  --vault-name azure-backup \
  --output table
```

Keep running the preceding command until you see that `ConfigureBackup` has finished:

output

Name	Operation	Status	Item Name	Start Time UTC	Duration
4cc9-8b2c-a5ead44a6a12	ConfigureBackup	Completed	NW-APP01	2019-08-01T06:19:12.101048+00:00	0:00:31.305975
a642-86ee982f7036	Backup	InProgress	NW-RHEL01	2019-08-01T06:18:35.955118+00:00	0:01:22.734182
860d4dca-9603-4a4e-9f3b-93f242a0a64d	ConfigureBackup	Completed	NW-RHEL01	2019-08-01T06:13:33.860598+00:00	0:00:31.256773

3. Do an initial backup of the virtual machine, instead of waiting for the schedule to run it.

Azure CLI

```
az backup protection backup-now \
  --resource-group vmbackups \
  --vault-name azure-backup \
  --container-name NW-APP01 \
  --item-name NW-APP01 \
  --retain-until 18-10-2030
```

There's no need to wait for the backup to finish, because you'll see how to monitor the progress in the portal next.

Monitor backups in the portal

View the status of a backup for a single virtual machine

1. Sign in to the [Azure portal](#).
2. On the Azure portal menu or from the **Home** page, select **All resources**.
3. Select the **NW-APP01** virtual machine.
4. Under **Operations**, select **Backup**.

The screenshot displays the 'NW-APP01 - Backup' page in the Azure portal. The left sidebar shows the 'Operations' menu with 'Backup' selected. The main content area includes a search bar, action buttons (Backup now, Restore VM, File Recovery, Stop backup, Resume backup, Delete backup data), and a 'Backup status' section. The 'Backup status' section shows 'Backup Pre-Check' as 'Passed' and 'Last backup status' as 'Success', with the latter highlighted by a red rectangle. Below this, there is a 'Restore points (1)' section with a filter for the last 30 days. A summary table shows 'CRASH CONSISTENT' as 0, 'APPLICATION CONSISTENT' as 1, and 'FILE-SYSTEM CONSISTENT' as 0. A table at the bottom lists restore points with columns for TIME, CONSISTENCY, and RECOVERY TYPE. The first entry is dated 8/8/2019, 11:21:48 PM, with Application Consistent consistency and Snapshot recovery type.

TIME	CONSISTENCY	RECOVERY TYPE
8/8/2019, 11:21:48 PM	Application Consistent	Snapshot

Last backup status displays the current status of the backup.

View the status of backups in the Recovery Services vault

1. Sign in to the [Azure portal](#).
2. On the Azure portal menu or from the **Home** page, select **All resources**.
3. Select the **azure-backup** Recovery Services vault.
4. Select the **Backup** tab on the **Overview** page to see a summary of all the backup items, the storage being used, and the current status of any backup jobs.

azure-backup

Recovery Services vault

Search (Ctrl+ /)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve proble...

Settings

Properties

Locks

Export template

Getting started

Backup

Site Recovery

Protected items

Backup items

Replicated items

Manage

+ Backup + Replicate Delete Refresh

Enterprise-scale Backup for SQL Server running in Azure VM is Generally Available. Learn more. →

Essentials

Overview Backup Site Recovery

Monitoring

Backup Alerts (last 24 hours)

Critical	0
Warning	0

Backup Pre-Check Status (Azure VMs)

0

Critical0

Warning0

Usage

Backup items

2

Backup Storage

Cloud - LRS	0 B
Cloud - GRS	0 B

Exercise - Restore Azure virtual machine data

6 minutes

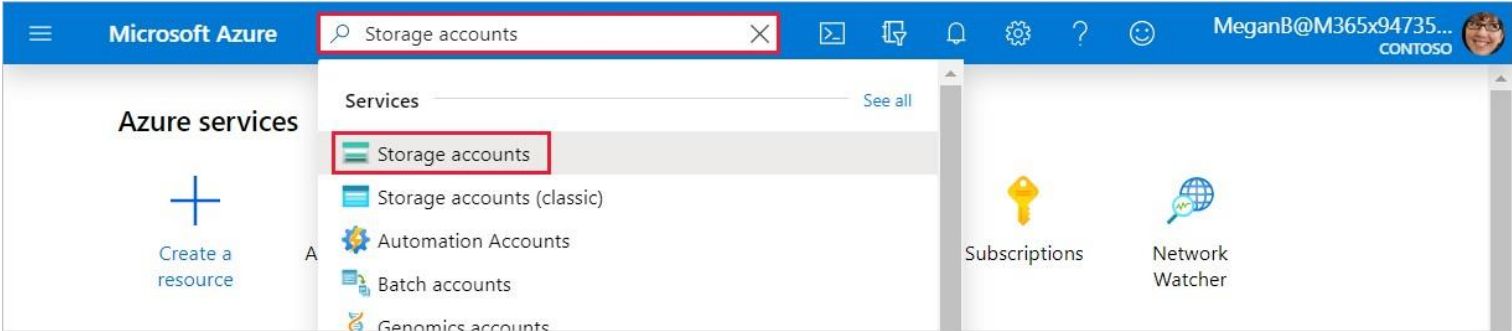
A few days after you backed up your first Azure virtual machine, the server had issues. It needs to be restored from a backup. You want to restore the virtual machine's disk and attach it to the problematic live server, and then track the restore to ensure that it has finished successfully.

In this exercise, you'll see how to restore a successful backup to replace a VM that has become corrupted, and monitor its progress.

Restore a virtual machine in the Azure portal

Create a storage account to use as a staging location

1. Sign in to the [Azure portal](#) by using the same account that you used in the previous exercise.
2. In the Azure portal, search for and select **Storage accounts**



3. Select + **Add**, and then use the following information to create a storage account:

Resource group	Select vmbackups .
Storage account name	Enter a unique name like restorestagingYYYYMMDD , where YYYYMMDD is replaced with today's date.
Location	Select (US) West US 2 .

Home > Storage accounts > Create storage account

Create storage account

Basics Advanced Tags Review + create

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. [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 Converted Windows Azure MSDN - Visual Studio Ultimate

* Resource group vmbackups
Create new

Instance details

The default deployment model is Resource Manager, which supports the latest Azure features. You may choose to deploy using the classic deployment model instead. [Choose classic deployment model](#)

* Storage account name restorestaging20190801

* Location (US) West US 2

Performance ☒ Standard ☐ Premium

Account kind StorageV2 (general purpose v2)

Replication Read-access geo-redundant storage (RA-GRS)

Access tier (default) ☐ Cool ☒ Hot

[Review + create](#) < Previous Next : Advanced >

4. Select **Review + create**
5. On the **Create storage account** page, select **Create**.
6. Wait for the storage account to be deployed.

Stop the VM to allow for the restore

A backup can't be restored if the VM is allocated and running. If you forget to stop the VM, you'll see an error that's similar to the following example.

... > azure-backup - Backup items > Backup Items (Azure Virtual Machine) > NW-APP01 > Restore > Restore configuration > Error details

Restore configuration

Validation failed. Click here for more details.

Create new Replace existing

The disk(s) from the selected restore point will replace the disk(s) in your existing VM. [Learn more about In-Place Restore](#).

Restore Type Replace Disk(s)

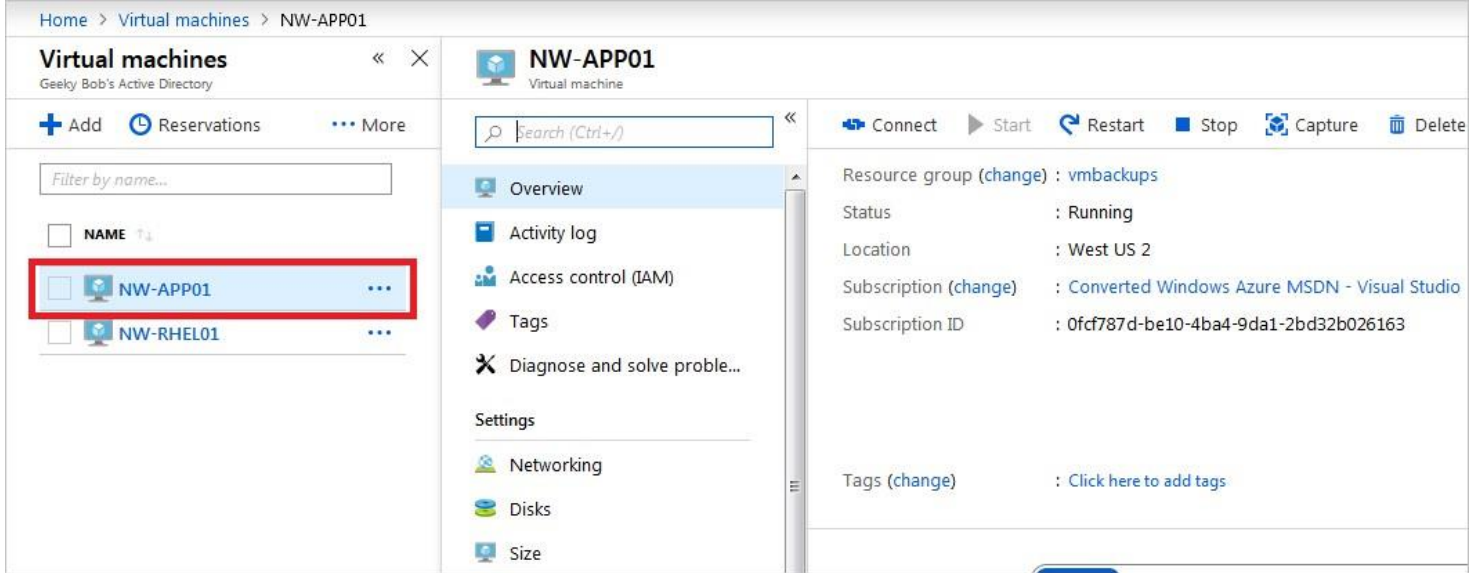
Error details

laasVM restore validation errors

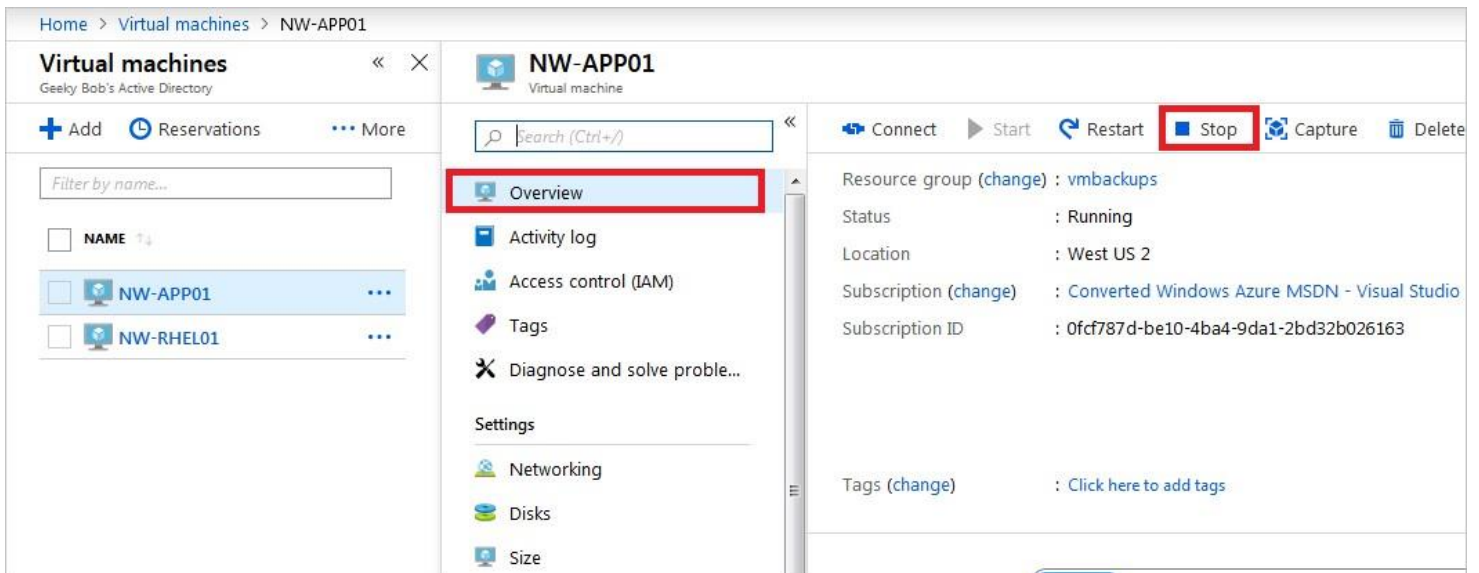
Error Code	UserErrorVmNotShutDown
Error Message	VM needs to be in deallocated state for performing replace disks operation
Recommended Action	Please shut down the VM, and retry

To prevent this error, use the following steps:

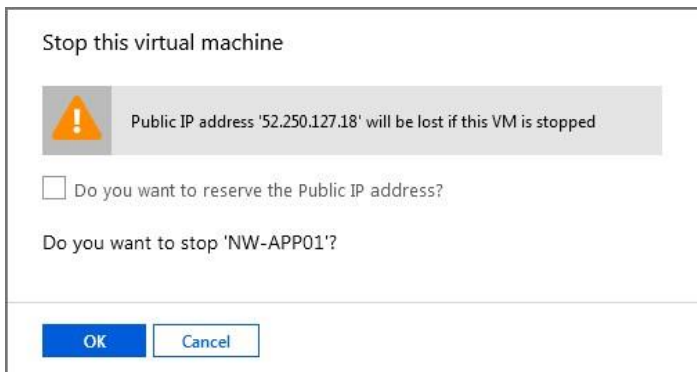
1. In the Azure portal, search for and select **Virtual machines** and then select **NW-APP01**.



2. Select **Stop** to shut down the VM.



3. In the **Stop this virtual machine** dialog box, select **OK**.



Restore the VM

The Recovery Services vaults are accessible at the subscription level. When you're viewing the VM, Azure provides a quick link to the specific vault under **Operations**

1. On the left menu, under **Operations**, select **Backup**.

NW-APP01 - Backup

Virtual machine

Search (Ctrl+/)

- Locks
- Export template
- Operations**
 - Auto-shutdown
 - Backup**
 - Disaster recovery
 - Update management
 - Inventory
 - Change tracking
 - Configuration management ...
 - Policies
 - Run command

Backup now Restore VM File Recovery Stop backup Resume backup Delete backup data

Alerts and Jobs

[View all Alerts](#) (last 24 hours)

[View all Jobs](#) (last 24 hours)

Backup status

Backup Pre-Check ✓ Passed

Last backup status ✓ Success -

Summary

Recovery services vault

Backup policy

Oldest restore point

Restore points (1)

This list is filtered for last 30 days of restore points. To recover from restore point older than 30 days, [click here](#).

CRASH CONSISTENT

0

APPLICATION CONSISTE...

1

FILE-SYSTEM CONSISTENT

0

TIME	CONSISTENCY	RECOVERY TYPE
8/8/2019, 11:21:48 PM	Application Consistent	Snapshot

2. To restore the virtual machine, select **Restore VM**

NW-APP01 - Backup

Virtual machine

Search (Ctrl+/)

- Locks
- Export template
- Operations
 - Auto-shutdown
 - Backup**
 - Disaster recovery
 - Update management
 - Inventory
 - Change tracking
 - Configuration management ...
 - Policies
 - Run command

Backup now **Restore VM** File Recovery Stop backup Resume backup Delete backup data

Alerts and Jobs

[View all Alerts](#) (last 24 hours)

[View all Jobs](#) (last 24 hours)

Backup status

Backup Pre-Check ✓ Passed

Last backup status ✓ Success -

Summary

Recovery services vault

Backup policy

Oldest restore point

Restore points (1)

This list is filtered for last 30 days of restore points. To recover from restore point older than 30 days, [click here](#).

CRASH CONSISTENT

0

APPLICATION CONSISTE...

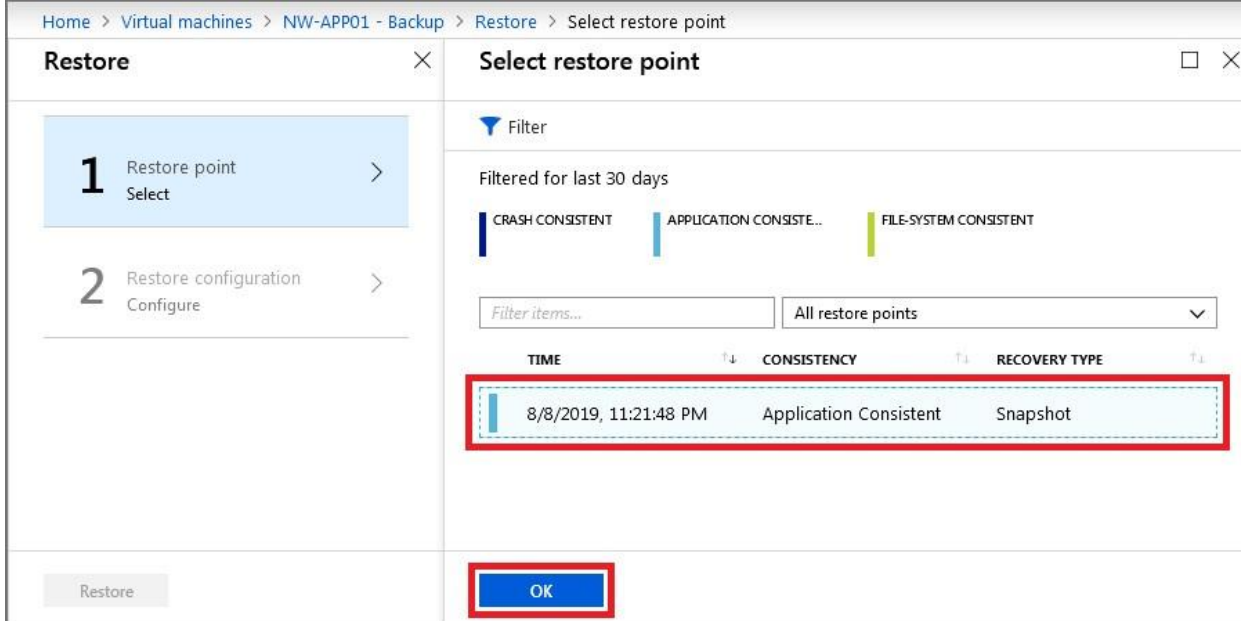
1

FILE-SYSTEM CONSISTENT

0

TIME	CONSISTENCY	RECOVERY TYPE
8/8/2019, 11:21:48 PM	Application Consistent	Snapshot

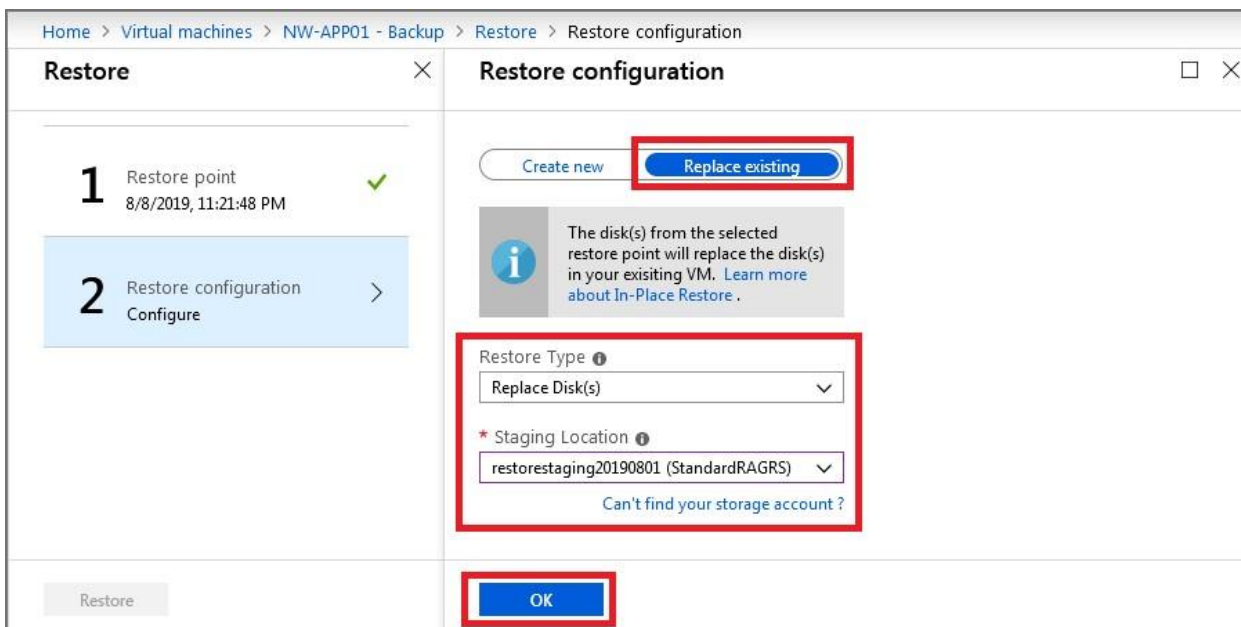
3. Select the restore point to use for the recovery, and then select **OK**



4. In the **Restore Configuration** window, select **Replace Existing** and use the following information to configure the restore:

Restore Type Select **Replace Disk(s)**. This is the restore point that will be used to replace the existing VM's disks.

Staging Location Select the storage account that you created previously.



5. Select **OK**.

6. On the confirmation screen, select **Restore**.

Track a restore

1. At the top of the page, select **View all Jobs**

Introduction

2 minutes

Your company has several critical virtual machine workloads running on Azure. As the lead solution architect, you've been asked to ensure that the company can recover these virtual machines if there's data loss or corruption. You've been asked to use the built-in capabilities of Azure Backup to help protect these virtual machines.

Azure Backup is a service that allows you to back up Azure virtual machines, on-premises virtual machines, SQL databases, and other application workloads. Every backup is encrypted at rest and can be kept for a user-defined retention period.

In this module, you'll learn about Azure Backup. And you'll see how you can use the Azure portal to back up and restore a machine.

Learning objectives

In this module, you'll:

- Identify the scenarios for which Azure Backup provides backup and restore capabilities
- Back up and restore an Azure virtual machine

Prerequisites

- Basic knowledge of Azure virtual machines
- Basic knowledge of disk storage for virtual machines

Note

For this module, you'll need use your own subscription to complete the optional exercises. A trial subscription or a subscription that you already have access to will work for these exercises.

Next unit: Azure Backup features and scenarios

Continue



900 XP ▶

Protect your virtual machines by using Azure Backup

35 min • Module • 7 Units

V V V V W 4.6 (325)

Rate it

Beginner Solutions Architect Administrator Azure Virtual Machines Backup

Use Azure Backup to help protect the data for on-premises servers, virtual machines, virtualized workloads, SQL Server, Azure Files, and more.

In this module, you'll:

- Identify the scenarios for which Azure Backup provides backup and restore capabilities
- Back up and restore an Azure virtual machine

- Basic knowledge of Azure virtual machines
- Basic knowledge of disk storage for virtual machines

This module is part of these learning paths

Architect migration, business continuity, and disaster recovery in Azure

Introduction

2 min

Azure Backup features and scenarios

5 min

Back up an Azure virtual machine by using Azure

Backup 5 min

Exercise - Back up an Azure virtual machine

10 min

Restore virtual machine data

5 min

Exercise - Restore Azure virtual machine data

6 min

Summary

2 min



Restore virtual machine data

5 minutes

Companies that have a business continuity and disaster recovery (BCDR) plan typically schedule test runs to ensure that the business can successfully recover from disasters. Now that you have successfully backed up your VMs, you want to explore the options available for restoring them as part of your BCDR testing.

In this unit, you'll learn about the options for restoring an Azure VM from a previous backup.

Restore options

You have three options when you're restoring a machine from backup:

- **Create a new VM**
 - This is the quickest method to get a virtual machine up and running with default settings from a restore point.
 - You can choose the name, resource group, virtual network, and storage type before doing the restore.
- **Restore disk**
 - Restore the backed-up disk so that it can be used to create a new virtual machine. The portal provides a template to help you customize the new machine.
 - The restore copies the virtual hard disk (VHD) to your chosen storage account. The VHD should be in the same location as the Recovery Services vault you're using. You can also attach the restored disk to an existing virtual machine.
- **Replace existing**
 - Restore a disk and use it to replace the disk on an existing virtual machine.
 - Azure Backup takes a snapshot of the virtual machine before the recovered disk is attached. It stores the snapshot in a staging location that you specify. The Recovery Services vault stores the snapshot according to your retention policy.
 - This option supports only unencrypted managed virtual machines.

Each of these restore options can be useful in certain situations. For example:

- **Create a new VM** can be used to quickly create a development server from the live version's backup.
- **Restore disk** can be used to create a new virtual machine. This option allows for customization of the virtual machine before it's created. You can add configuration settings, like extra network adapters or an increased memory size. Using this option also allows for customization through PowerShell.
- **Replace existing** allows a disk to be restored and replaced on an existing virtual machine. This option can be useful if an operating system disk has failed during an update operation and can be recovered only with a restore.

Recover files from a backup

Files and folders are available for recovery from Azure virtual machines if the backup was created with the Microsoft Azure Recovery Services (MARS) agent. You can restore data to the same machine that it was originally backed up from, or to a different machine in your subscription.

Use **Instant Restore** to restore data on the target machine by using the Azure Backup snap-in. After the snap-in is loaded, you can select the original server where the backup was created. Then, specify whether to restore individual files, folders, or a whole volume.

If you need to restore the data to the same server where it was backed up, select **This server**. If it's a different server, choose that machine instead.

To mount the recovery point as a drive on the local machine, select the date to restore, and then select **Mount**. You can copy the data to a new location.

Restore an encrypted virtual machine

Azure Backup supports the backup and restore of machines encrypted through Azure Disk Encryption. Disk Encryption works with Azure Key Vault to manage the relevant secrets that are associated with the encrypted disk. For an additional layer of security, you can use **key vault encryption keys (KEKs)** to encrypt the secrets before they're written to the key vault.

Certain limitations apply when you restore encrypted virtual machines:

- Virtual machines can be backed up and restored only to the same subscription and region that they're a member of. The subscription and region have to be the same as the Recovery Services vault that you use.
- Azure Backup supports only standalone key encryption. Any key that's part of a certificate isn't supported currently.
- File-level or folder-level restores are not supported with encrypted virtual machines. To restore to that level of granularity, the whole virtual machine has to be restored. You can then manually copy the file or folders.

- The **Replace existing VM** option isn't available for encrypted virtual machines.

Check your knowledge

1. Which restore type should you select if you want to replace a disk on an existing virtual machine?

- ☐ Create a new VM
- ☐ Restore disk
- ☒ Replace existing

Selecting this option allows for a disk to be restored and then used to replace a disk on an existing VM.

2. You want to replace a disk on an existing VM but receive an error. What's the possible reason?

- ☒ The existing VM has been deleted and is no longer available

If the VM was deleted, the disk can't be restored.

- ☐ The existing VM is part of a different resource group in your Azure subscription
- ☐ The existing VM is turned off

Next unit: Exercise - Restore Azure virtual machine data

Continue ↗