

Protect your virtual machines by using Azure Backup

1. Introduction

<https://learn.microsoft.com/en-us/training/modules/protect-virtual-machines-with-azure-backup/1-introduction>

Introduction

Completed

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

Azure Backup is a service that allows you to back up Azure virtual machines, on-premises servers, Azure file shares, and SQL Server or SAP HANA (High-performance Analytic Appliance) running on Azure VMs, and other application workloads.

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

Learning objectives

In this module, you:

- 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 need use your own subscription to complete the optional exercises. A trial subscription or a subscription that you already have access to works for these exercises.

2. Azure Backup features and scenarios

<https://learn.microsoft.com/en-us/training/modules/protect-virtual-machines-with-azure-backup/2-azure-backup-features-scenarios>

Azure Backup features and scenarios

Completed

Your company's business continuity and disaster recovery (BCDR) plan requires a full backup and restore capability for all of your high-risk servers. You're asked to enable and test the backup and restore functionality for these critical Windows and Linux assets.

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

What is Azure Backup?

Azure Backup is a built-in Azure service that provides secure backup for all Azure-managed data assets. It uses zero-infrastructure solutions to enable self-service backups and restores, with at-scale management at a lower and predictable cost. Azure Backup currently offers specialized backup solutions for Azure and on-premises virtual machines (VMs). Azure Backup also gives workloads like SQL Server or SAP HANA (High-performance Analytic Appliance) running in Azure VMs enterprise-class backup and restore options.

In contrast to traditional backup solutions that can take considerable effort to set up, Azure Backup is easily managed through the Azure portal.

Azure Backup versus Azure Site Recovery

Both Azure Backup and Azure Site Recovery aim to make the system more resilient to faults and failures, but they use two different approaches. The primary goal of Backup is to maintain copies of stateful data that allow you to go back in time. Site Recovery, however, replicates the data in almost real time and allows for a failover.

In that sense, if there are issues like network or power outages, you can use availability zones. For a region-wide disaster (such as natural disasters), Site Recovery is used. Backups are used in cases of accidental data loss, data corruption, or ransomware attacks.

Additionally, the choice of a recovery approach depends on the criticality of the application, recovery point objective (RPO) and recovery time objective (RTO) requirements, and the cost implications.

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:

Zero-infrastructure backup: Azure Backup eliminates the need to deploy and manage any backup infrastructure or storage. There's no overhead in maintaining backup servers or scaling the storage up or down as the needs vary.

Long-term retention: Meet rigorous compliance and audit needs by retaining backups for many years, after which the built-in lifecycle management capability prunes the recovery points automatically.

Security: Azure Backup provides security to your backup environment, both when your data is in transit and at rest:

- **Azure role-based access control:** Role-based access control allows you to segregate duties within your team and grant only the amount of access to users necessary to do their jobs.
- **Encryption of backups:** Backup data is automatically encrypted using Microsoft-managed keys. Alternatively, you can encrypt your backed-up data using customer-managed keys stored in the Azure Key Vault.
- **No internet connectivity required:** When you use Azure VMs, all the data transfer happens only on the Azure backbone network without needing to access your virtual network. So no access to any IPs or fully qualified domain names (FQDNs) is required.
- **Soft delete:** With soft delete, the backup data is retained for 14 more days even after the deletion of the backup item. This retention protects against accidental deletion or malicious deletion scenarios, allowing the recovery of those backups with no data loss. Azure Backup also provides **Enhanced soft delete** that enables you to retain a deleted item in the *soft deleted* state for a longer duration.

Azure Backup also offers the ability to back up VMs encrypted with Azure Disk Encryption.

High availability: Azure Backup offers three types of replication:

- **Locally redundant storage (LRS):** The lowest-cost option with basic protection against server rack and drive failures. We recommend it for noncritical scenarios.
- **Geo-redundant storage (GRS):** The intermediate option has failover capabilities in a secondary region. We recommend it for backup scenarios.
- **Zone-redundant storage (ZRS):** This option protects against datacenter-level failures by replicating your storage account synchronously across three Azure availability zones. We recommend it for high-availability scenarios.

Centralized monitoring and management: Azure Backup provides built-in monitoring and alerting capabilities in a Recovery Services vault. These capabilities are available without any other management infrastructure.

Azure Backup supported scenarios

Azure Backup supports the following scenarios:

- **Azure VMs** - Back up Windows or Linux Azure VMs
Azure Backup provides independent and isolated backups to guard against unintended destruction of the data on your VMs. Backups are stored in a Recovery Services vault with built-in management of recovery points. Configuration and scaling are simple, backups are optimized, and you can easily restore as needed.
- **On-premises** - Back up files, folders, and system state using the [Microsoft Azure Recovery Services \(MARS\) agent](#). Or use [Microsoft Azure Backup Server \(MABS\)](#) or [Data Protection Manager \(DPM\) server](#) to protect on-premises VMs (Hyper-V and VMware) and other on-premises workloads.
- **Azure Files shares** - Azure Files provides snapshot management by Azure Backup.
- **SQL Server in Azure VMs** and **SAP HANA databases in Azure VMs** - Azure Backup offers stream-based, specialized solutions to back up SQL Server, or SAP HANA running in Azure VMs. These solutions take workload-aware backups that support different backup types such as full, differential and log, 15-minute RPO, and point-in-time recovery.

3. Back up an Azure virtual machine by using Azure Backup

<https://learn.microsoft.com/en-us/training/modules/protect-virtual-machines-with-azure-backup/3-back-up-azure-virtual-machine>

Back up an Azure virtual machine by using Azure Backup

Completed

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 (VMs).

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

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

Azure VMs are backed up by taking snapshots of the underlying disks at user-defined intervals and transferring those snapshots to the Recovery Services vault as per the customer-defined policy.

Recovery Services vault

Azure Backup uses a Recovery Services vault to manage and store the backup data. A vault is a storage-management entity, which provides a simple experience to carry out and monitor backup and restore operations. With Azure Backup, you don't need to worry about deploying or managing storage accounts. In fact, all you need to specify is the vault that you want to back up the virtual machine (VM) to. The backup data is transferred to the Azure Backup storage accounts (in a separate fault domain) in the background. The vault also acts as a role-based access control boundary to allow secure access to the data.

The screenshot shows the Azure Backup console for a virtual machine named 'ShopKartEmp'. The interface includes a left-hand navigation pane with sections like 'Operations' (Bastion, Auto-shutdown, Backup, Disaster recovery, Update management, Inventory, Change tracking, Configuration management, Policies, Run command) and 'Monitoring' (Insights, Alerts, Metrics). The main content area is divided into several sections: 'Alerts and Jobs' with links to view alerts and jobs; 'Backup status' showing 'Backup Pre-Check' as 'Passed' and 'Last backup status' as 'Success 6/21/2020, 6:01:37 AM'; a 'Summary' section showing the recovery services vault as 'ShopKartDemoVault', backup policy as 'DefaultPolicy', and oldest restore point as '4/5/2020, 6:14:48 AM (2 month(s) ago)'; and a 'Restore points (4)' section. Below the restore points, there are three bar charts for 'CRASH CONSISTENT' (0), 'APPLICATION CONSISTENT' (4), and 'FILE-SYSTEM CONSISTENT' (0). A table lists the restore points with columns for Time, Consistency, Recovery Type, and a menu icon. The table shows four restore points, all of which are 'Application Consistent' and stored in the 'Vault'.

Time	Consistency	Recovery Type	
6/21/2020, 6:01:44 AM	Application Consistent	Snapshot and Vault	...
6/14/2020, 6:08:11 AM	Application Consistent	Vault	...
6/7/2020, 6:06:58 AM	Application Consistent	Vault	...
5/31/2020, 6:04:07 AM	Application Consistent	Vault	...

Snapshots

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

Extension	OS	Description
VM Snapshot	Windows	The extension works with Volume Shadow Copy Service (VSS) to take a copy of the data on disk and in memory.
VM SnapshotLinux	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 VM 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 need to write custom pre or post scripts per app to capture the application state.
 - You can get complete consistency for the VM and all running applications.
- **File system consistent**
 - If VSS fails on Windows, or the pre and post scripts fail on Linux, Azure Backup still creates 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 VM 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.

Backup policy

You can define the backup frequency and retention duration for your backups. Currently, the VM backup can be triggered daily or weekly, and can be stored for multiple years. The backup policy supports two access tiers: *snapshot tier* and the *vault tier*. By using the Enhanced policy, you can trigger hourly backups.

Selective disk backup: Azure Backup provides **Selective Disk backup and restore** capability using **Enhanced policy**. By using this capability, you can selectively back up a subset of the data disks that are attached to your VM. Then, you can restore a subset of the disks that are available in a recovery point, both from instant restore and vault tier. It helps you manage critical data in a subset of the VM disks and use database backup solutions when you want to back up only their OS disk to reduce cost.

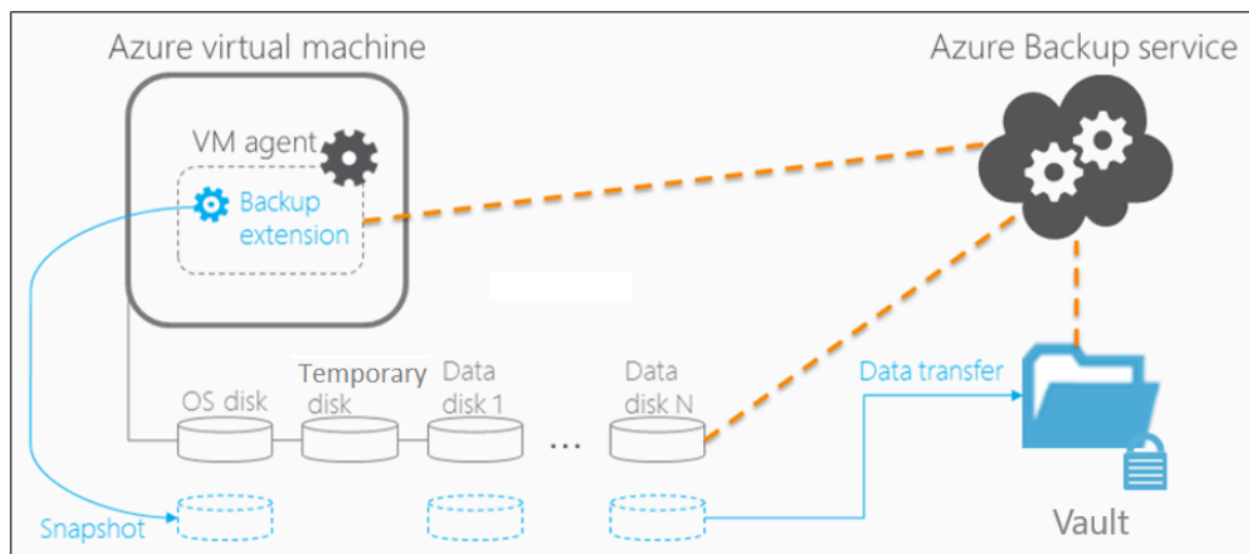
Snapshot tier: All the snapshots are stored locally for a maximum period of five days, in what is called the snapshot tier. For all types of operation recoveries, we recommended that you restore from the snapshots because it's faster to do so. This capability is called **instant restore**.

Vault tier: All snapshots are additionally transferred to the vault for more security and longer retention. At this point, the recovery point type changes to "snapshot and vault."

Backup process for an Azure virtual machine

Here's how Azure Backup completes a backup for Azure VMs:

1. For Azure VMs that are selected for backup, Azure Backup starts a backup job according to the backup frequency you specify in the backup policy.
2. During the first backup, a backup extension is installed on the VM, if the VM is running:
 - For Windows VMs, the VM Snapshot extension is installed.
 - For Linux VMs, the VM SnapshotLinux extension is installed.
3. After the snapshot is taken, the data is stored locally and transferred to the vault.
 - The backup is optimized by backing up each VM disk in parallel.
 - For each disk that's being backed up, Azure Backup reads the blocks on the disk and identifies and transfers only the data blocks that changed (the delta) since the previous backup.
 - Snapshot data might not be immediately copied to the vault. It might take several hours at peak times. Total backup time for a VM is less than 24 hours for daily backup policies.



You can additionally enable [vault encryption with customer-managed keys \(CMK\)](#). By using **Enhanced soft delete** for a Recovery Services vault, you can protect backups from deletion. You can also keep Enhanced soft delete *always on* to prevent turning it off, thus protecting your backups from accidental deletion or from malware attacks.

4. Exercise - Back up an Azure virtual machine

<https://learn.microsoft.com/en-us/training/modules/protect-virtual-machines-with-azure-backup/4-exercise-back-up-azure-virtual-machine>

Exercise - Back up an Azure virtual machine

Completed

Your company runs a combination of Windows and Linux workloads. You're asked to prove that Azure Backup is a good fit for both kinds of virtual machines (VMs). By using a combination of the Azure CLI and the Azure portal, you 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 by using PowerShell commands.

In this exercise, you create a virtual machine (VM), set up a backup, and start a backup.

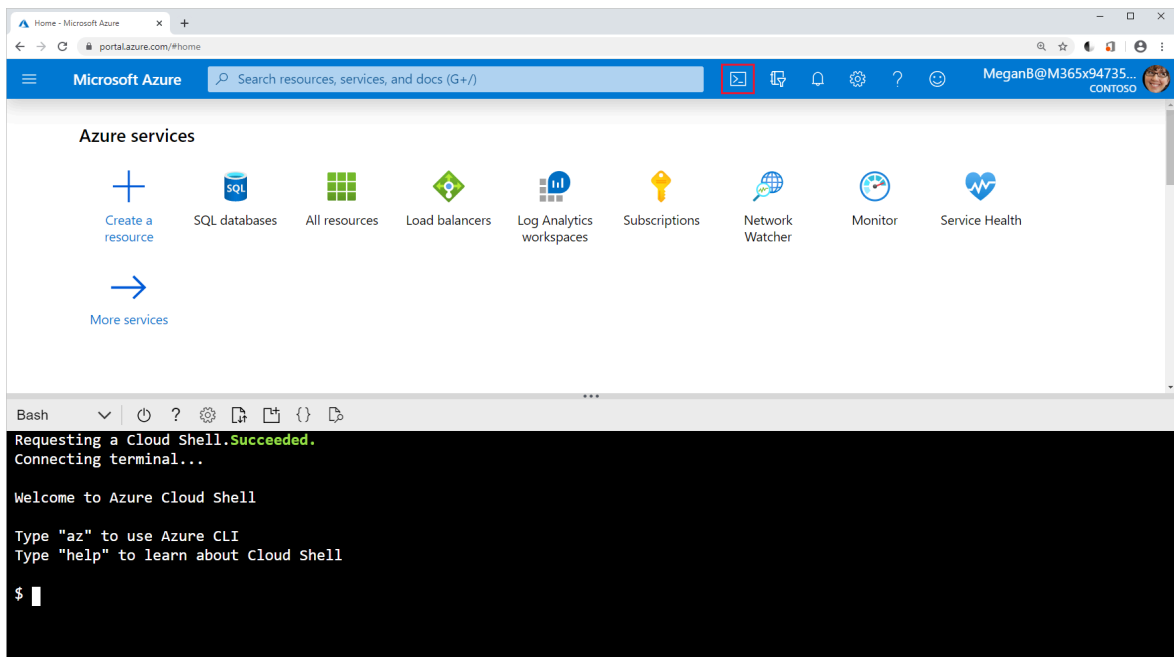
Note

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 virtual machines by 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 account, create a [free account](#) before you begin.

Create a backup for Azure virtual machines

Set up the environment

1. Sign in to the [Azure portal](#), and select the icon to open Azure Cloud Shell.



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

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


3. Use Cloud Shell to create the **NorthwindInternal** virtual network and the **NorthwindInternal1** subnet.

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

Create a Windows virtual machine by using the Azure CLI

Create the *NW-APP01* virtual machine by running the following command. Replace `<password>` with a password of your choice, enclosed in double quotes. For example, `--admin-password "PassWord123!"`.

```
az vm create \  
  --resource-group $RGROUP \  
  --name NW-APP01 \  
  --size Standard_DS1_v2 \  
  --public-ip-sku Standard \  
  --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 running the following command.

```
az vm create \  
  --resource-group $RGROUP \  
  --name NW-RHEL01 \  
  --size Standard_DS1_v2 \  
  --image RedHat:RHEL:8-gen2:latest \  
  --authentication-type ssh \  
  --generate-ssh-keys \  
  --vnet-name NorthwindInternal \  
  --subnet NorthwindInternal1
```

Note

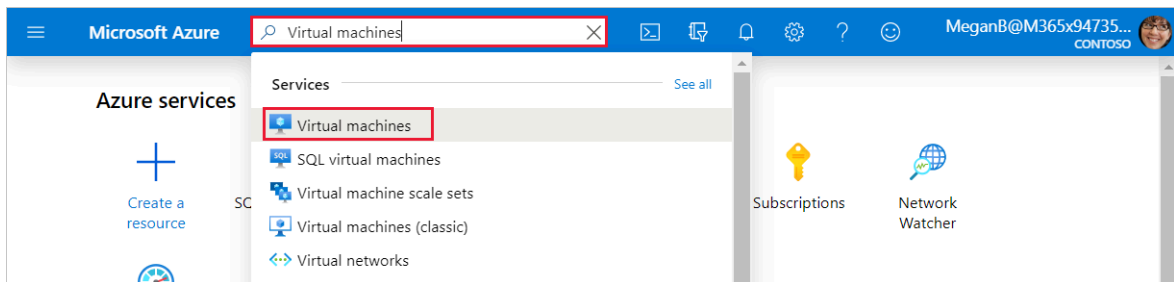
If you get a `securityProfile.securityType is invalid` error running the preceding command, run the following commands to register `UseStandardSecurityType`, then re-run the preceding command.

```
az feature register --name UseStandardSecurityType --namespace Microsoft.Compute
az feature show --name UseStandardSecurityType --namespace Microsoft.Compute
```

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

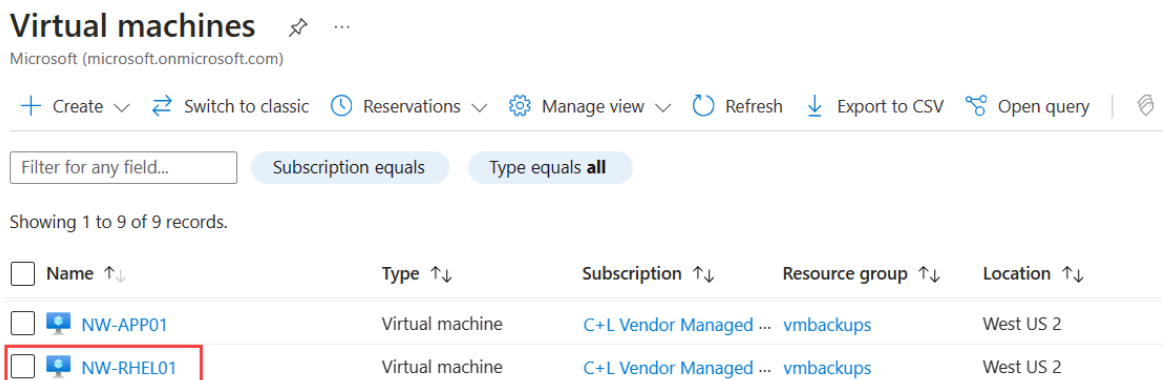
Enable backup for a virtual machine by using the Azure portal

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



The **Virtual machines** pane appears.

2. From the list, select the **NW-RHEL01** virtual machine that you created.



The **NW-RHEL01** virtual machine pane appears.

3. In the middle menu pane, select the **Capabilities** tab, then scroll down to and select **Backup**. The **Backup** pane for the *NW-RHEL01* virtual machine appears.
4. Select the radio button for **Standard**. You can accept the defaults for the following options:
 - **Backup vault:** **vaultXXX** for the name.
 - **Backup policy:** **DailyPolicy-xxxxxxxxx**, which creates a daily backup at 12:00 PM UTC with a retention range of 180 days.

5. Select the **Enable backup** button.

6. Once deployment completes, go back to the **NW-RHEL01** virtual machine, select the **Capabilities** tab, then scroll down to and select **Backup**. The **Backup** pane for the *NW-RHEL01* virtual machine appears.

7. To perform the first backup for this server, in the top menu bar, select **Backup now**.

The **Backup Now** pane for *NW-RHEL01* appears.

8. Select **OK**.

Enable a backup by using the Azure CLI

1. First, create the azure-backup vault by using Cloud Shell:

```
az backup vault create \
  --resource-group vmbackups \
  --location westus2 \
  --name azure-backup
```

2. Using Cloud Shell, enable a backup for the *NW-APP01* virtual machine.

```
az backup protection enable-for-vm \
  --resource-group vmbackups \
  --vault-name azure-backup \
```

```
--vm NW-APP01 \  
--policy-name EnhancedPolicy
```

3. Monitor the progress of the setup using the 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` is finished.

Name	Operation	Status	Item Name
a3df79b4-be4f-4cc9-8b2c-a5ead44a6a12	ConfigureBackup	Completed	NW-APP01
5e1531a9-8b3d-4983-a642-86ee982f7036	Backup	InProgress	NW-RHEL01
860d4dca-9603-4a4e-9f3b-93f242a0a64d	ConfigureBackup	Completed	NW-RHEL01

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

```
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 \  
  --backup-management-type AzureIaaSVM
```

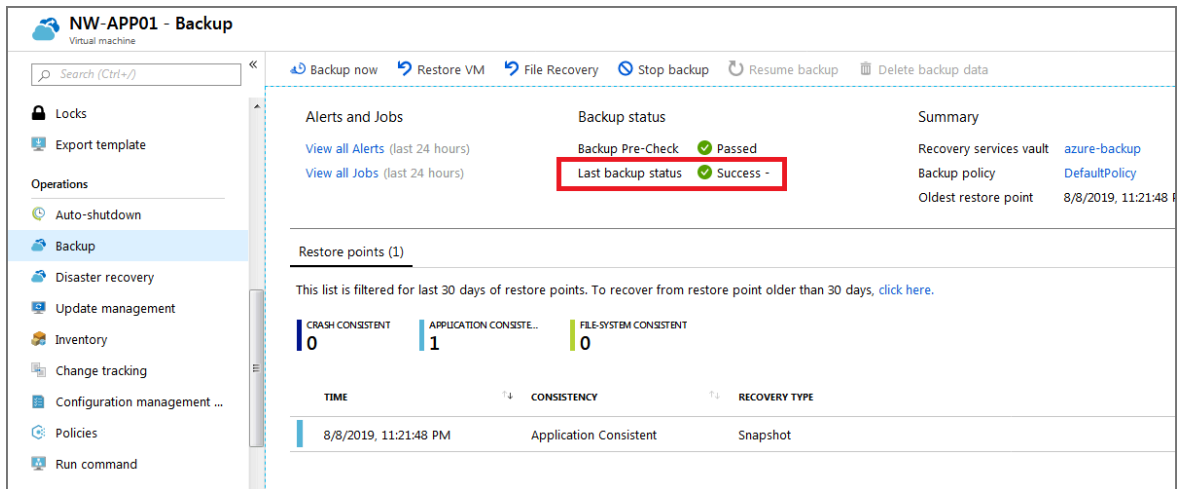
There's no need to wait for the backup to finish, because the next section shows you how to monitor the progress in the portal.

Monitor backups in the portal

View the status of a backup for a single virtual machine

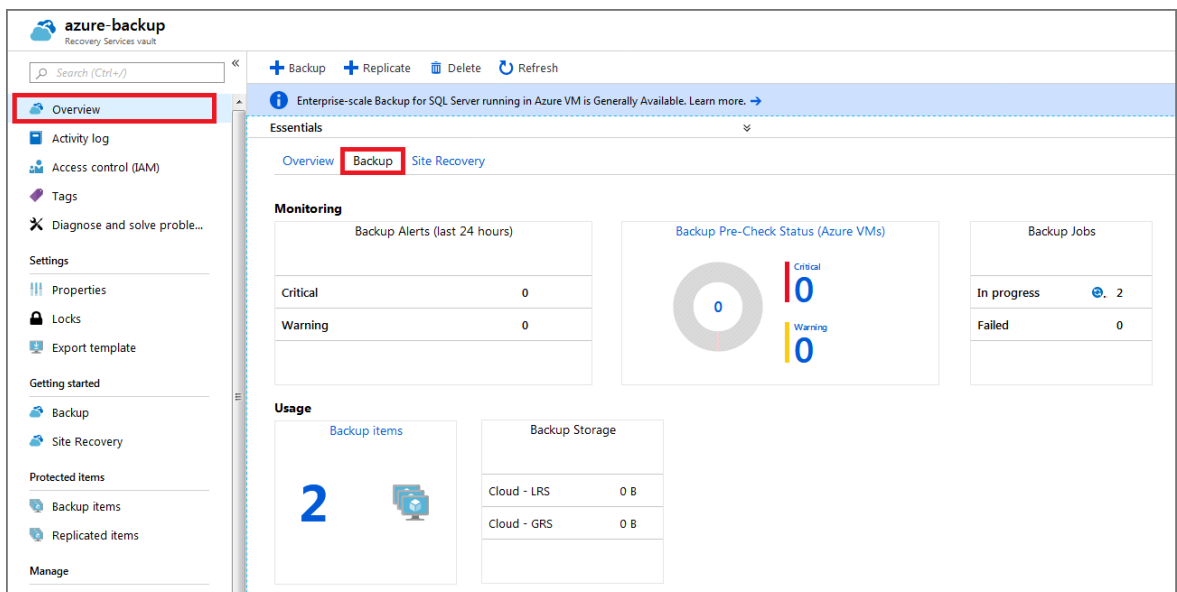
1. On the Azure portal menu or from the **Home** page, select **All resources**.
2. Enter *Virtual machines* in the search field at the top of the page and select **Virtual machines** from the results.
3. Select the **NW-APP01** virtual machine. The *NW-APP01* virtual machine pane appears.
4. In the middle menu pane, select the **Capabilities** tab, then scroll to and select **Backup**. The **Backup** pane for the *NW-APP01* virtual machine appears.

Under the **Backup status** section, the **Last backup status** field displays the current status of the backup.



View the status of backups in the Recovery Services vault

1. On the Azure portal menu or from the **Home** page, select **All resources**.
2. Sort the list by *Type*, and then select the **azure-backup** Recovery Services vault. The **Azure-backup** recovery services vault pane appears.
3. On the **Overview** pane, select the interior **Backup** tab to display a summary of all the backup items, the storage being used, and the current status of any backup jobs.



5. Restore virtual machine data

<https://learn.microsoft.com/en-us/training/modules/protect-virtual-machines-with-azure-backup/5-restore-virtual-machine-data>

Restore virtual machine data

Completed

6. Exercise - Restore Azure virtual machine data

<https://learn.microsoft.com/en-us/training/modules/protect-virtual-machines-with-azure-backup/6-exercise-restore-virtual-machine-data>

Exercise - Restore Azure virtual machine data

Completed

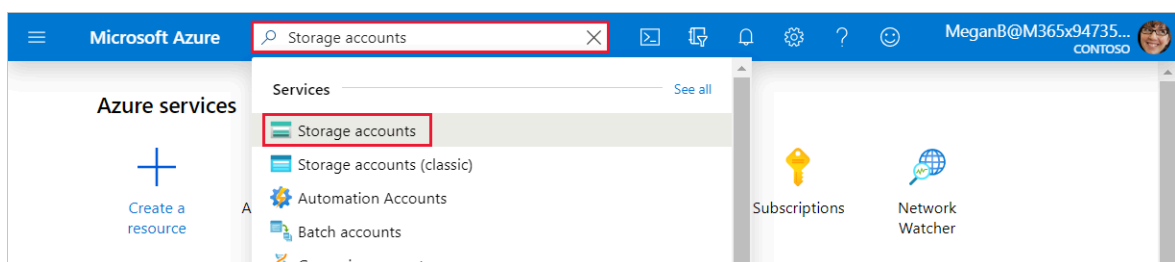
A few days after you backed up your first Azure virtual machine (VM), the server had issues. The VM needs to be restored from a backup. You want to restore the VM's disk and attach it to the problematic live server, and then track the restore to ensure that it finished successfully.

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

Restore a virtual machine in the Azure portal

Create a storage account to use as a staging location

1. If you closed Azure, sign in to the [Azure portal](#) by using the same account that you used in the previous exercise.
2. In the Azure portal, enter **Storage accounts** in the top search bar, and then select it.



The **Storage accounts** pane appears.

3. In the menu bar, select **Create**. The **Create a storage account** pane appears.

4. On the **Basics** tab, enter the following values for each setting to create a storage account.

Setting	Value
Resource group	From the dropdown list, select vmbackups .
Instance details	
Storage account name	Enter a unique name like restorestagingYYYYMMDD , where YYYYMMDD is replaced with today's date.
Region	From the dropdown list, select (US) West US 2 .

[Home](#) > [Storage accounts](#) >

Create a storage account

Basics Advanced Networking Data protection Tags Review + create

Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription *

Resource group * [Create new](#)

Instance details

If you need to create a legacy storage account type, please click [here](#).

Storage account name ⓘ *

Region ⓘ *

Performance ⓘ *

☒ Standard: Recommended for most scenarios (general-purpose v2 account)

☐ Premium: Recommended for scenarios that require low latency.

Redundancy ⓘ *

☒ Make read access to data available in the event of regional unavailability.

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

5. Select **Review + create**.

6. After validation passes, select **Create**.

Wait for the storage account to be deployed.

Stop the virtual machine

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

The screenshot shows the 'Restore configuration' pane on the left and the 'Error details' pane on the right. The 'Restore configuration' pane has a red banner indicating 'Validation failed. Click here for more details.' Below this are buttons for 'Create new' and 'Replace existing'. A message states: 'The disk(s) from the selected restore point will replace the disk(s) in your existing VM. [Learn more about In-Place Restore](#).' The 'Restore Type' dropdown is set to 'Replace Disk(s)'. The 'Error details' pane shows the following information:

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

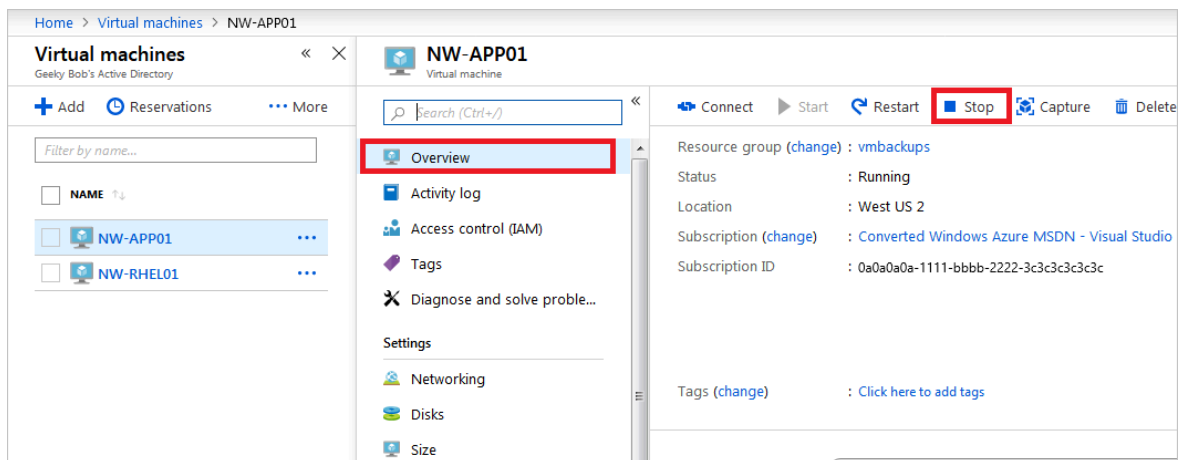
To prevent this error, follow these steps:

1. In the top left of the Azure portal, select **Home**, select **Virtual Machines**, and then select **NW-APP01**.

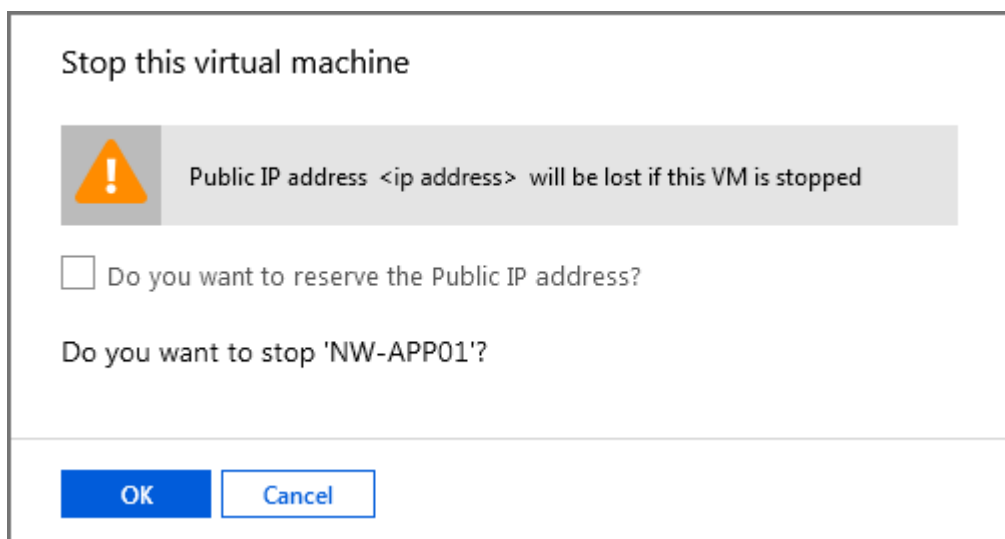
The screenshot shows the 'Virtual machines' page in the Azure portal. The breadcrumb navigation is 'Home > Virtual machines > NW-APP01'. The page title is 'Virtual machines' with a subtitle 'Demo Microsoft Entra ID'. There are buttons for '+ Add', 'Reservations', and 'More'. A search bar is present. A list of virtual machines is shown, with 'NW-APP01' highlighted and a red box around it. The 'NW-RHEL01' VM is also listed. The right pane shows the 'Overview' tab for 'NW-APP01', displaying details such as 'Resource group (change)', 'Status: Running', 'Location: West US 2', 'Subscription (change)', and 'Subscription ID: 0a0a0a0a-1111-bbbb-2222-3c3c3c3c3c'. There are also buttons for 'Connect', 'Start', 'Restart', 'Stop', 'Capture', and 'Delete'.

The *NW-APP01* virtual machine pane appears.

2. In the menu bar, select **Stop**.



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



Restore the virtual machine

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. In the menu pane, scroll to **Operations**, and select **Backup**.

NW-APP01 | Backup

Virtual machine

Search (Ctrl+/)

Backup now | Restore VM | File Recovery | Stop backup | Resume backup | Delete backup data | Restore to Secondary Region | Undelete

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 7/18/2021, 8:32:17 PM

Summary

Recovery services vault: [azure-backup](#)
Backup policy: [DefaultPolicy](#)
Oldest restore point: 7/17/2021, 10:36:18 AM (1 day(s) ago)

Restore points (4)

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

CRASH CONSISTENT: 0 | APPLICATION CONSISTENT: 4 | FILE-SYSTEM CONSISTENT: 0

Time	Consistency	Recovery Type
7/19/2021, 9:34:15 AM	Application Consistent	Snapshot
7/18/2021, 8:32:21 PM	Application Consistent	Snapshot and Vault-Standard
7/17/2021, 8:35:46 PM	Application Consistent	Snapshot and Vault-Standard
7/17/2021, 10:36:18 AM	Application Consistent	Snapshot and Vault-Standard

2. To restore the virtual machine, in the menu bar, select **Restore VM**. The **Restore Virtual Machine** pane for **NW-APP01** appears.
3. Under the **Restore point** text box, choose **Select**. The **Select restore point** pane appears.
4. By default, the start and end date are set for a two week range. Set the **Start date** to an appropriate date for our restore points (**07/05/2021**), select the restore point to use for the recovery, and then select **OK**.

Select restore point

×

nw-app01

Start Date

07/05/2021

End Date

07/19/2021

Recovery point type

All restore points

CRASH CONSISTENT

APPLICATION CONSISTENT

FILE-SYSTEM CONSISTENT

Time	Consistency	Recovery Type
7/19/2021, 9:34:15 AM	Application Consistent	Snapshot
7/18/2021, 8:32:21 PM	Application Consistent	Snapshot and Vault-Standard
7/17/2021, 8:35:46 PM	Application Consistent	Snapshot and Vault-Standard
7/17/2021, 10:36:18 AM	Application Consistent	Snapshot and Vault-Standard

OK

Cancel

The **Restore Virtual Machine** pane for *NW-APP01* appears.

5. Configure the restore point using the following values for each setting.

Setting	Value
Restore Configuration	
Replace existing	Select this option.
Staging Location	From the dropdown list, select the storage account that you previously created.

Home > Virtual machines > NW-APP01 >

Restore Virtual Machine ...

nw-app01

Restore allows you to restore VM/disks from a selected Restore Point.

Restore point *
[Select](#)

Data Store

Restore Configuration

☐ Create new ☒ Replace existing

i 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 ⓘ

Staging Location * ⓘ

[Can't find your storage account ?](#)

Restore

6. Select **Restore**. The **Backup** pane for the *NW-APP01* virtual machine appears. Notice the notifications in the top right of the toolbar. The latest notification shows **Triggering restore for NW-APP01**

Track a restore

1. In the **Alerts and Jobs** section, select **View all Jobs**. The **Backup Jobs** pane appears.

NW-APP01 | Backup Virtual machine

Search (Ctrl+/) « Backup now Restore VM File Recovery Stop backup Resume backup Delete backup data Restore to Secondary Region Undelete

Configuration

- Identity
- Properties
- Locks

Operations

- Bastion
- Auto-shutdown
- Backup**
- Disaster recovery
- Guest + host updates
- Inventory
- Change tracking
- Configuration management (Preview)
- 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 ✓ Success 7/18/2021, 8:32:17 PM

Summary

Recovery services vault [azure-backup](#)

Backup policy [DefaultPolicy](#)

Oldest restore point 7/17/2021, 10:36:18 AM (1 day(s) ago)

Restore points (4)

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

CRASH CONSISTENT 0 APPLICATION CONSISTENT 4 FILE-SYSTEM CONSISTENT 0

Time	Consistency	Recovery Type
7/19/2021, 9:34:15 AM	Application Consistent	Snapshot
7/18/2021, 8:32:21 PM	Application Consistent	Snapshot and Vault-Standard
7/17/2021, 8:35:46 PM	Application Consistent	Snapshot and Vault-Standard
7/17/2021, 10:36:18 AM	Application Consistent	Snapshot and Vault-Standard

2. In the **Details** column, select **View details** for the **Restore** job.

Home > Virtual machines > NW-APP01 > Backup Jobs

Choose columns Filter Export jobs Refresh

Filtered by: Item Type - All, Operation - All, Status - All, Start Time - 7/18/2021, 10:30:35 AM, End Time - 7/19/2021, 10:30:35 AM

Having issues? [Click here](#)

All data fetched from the service.

Filter items ...

Workload name ↑↓	Operation	Status	Type	Start time ↑↓	Duration ↑↓	Details
nw-app01	Backup	In progress	Azure Virtual machine	7/19/2021, 10:25:27 AM	00:05:09	View details
nw-app01	Restore	In progress	Azure Virtual machine	7/19/2021, 10:25:26 AM	00:05:09	View details
nw-app01	Backup	In progress	Azure Virtual machine	7/19/2021, 9:34:13 AM	00:56:23	View details
NW-RHEL01	Backup	In progress	Azure Virtual machine	7/19/2021, 9:27:05 AM	01:03:31	View details
nw-app01	Backup	Completed	Azure Virtual machine	7/18/2021, 8:32:17 PM	01:31:13	View details
NW-RHEL01	Backup	Completed	Azure Virtual machine	7/18/2021, 12:40:49 PM	01:51:12	View details

< Previous Page 1 of 1 Next >

The **Restore** pane appears for **NW-APP01**.

3. You can monitor the progress of the VM restore job:

- **Job details:** Details about the restore job you launched for this VM.
- **Job status:** Real-time progress of the restore job.
- **Sub tasks:** Name and status of the tasks within the job.

Home > Virtual machines > NW-APP01 > Backup Jobs >

Restore

nw-app01

 Refresh  Cancel  Deploy Template

Job details

Job Type	Replace disks
Target VM Name	
Target Storage Account Name	<Storage account name placeholder>
Recovery point time	7/19/2021 4:34:15 PM
Target resource group	vmbackups
Activity ID	<Activity ID placeholder>

Job status

Job progress



Sub tasks

Name	Status
Transfer data from vault	 In progress
Update the virtual machine	 Not started

7. Summary

<https://learn.microsoft.com/en-us/training/modules/protect-virtual-machines-with-azure-backup/7-summary>

Summary

Completed

In this module, you learned the importance of having a tested backup and recovery strategy for your organization. You learned about the different types of Azure backups, and the reasons why you would choose one backup type versus another depending on your scenario.

You learned that you can back up Azure virtual machines or on-premises machines. In addition, you learned how to back up an Azure virtual machine (VM). You then restored it by using the various

options available to you, and you were able to monitor the progress.

You can now use Azure Backup to help protect your environment against data loss or disk corruption. You can restore services according to your business continuity and disaster recovery plan.

Important

In this module you created resources using your Azure subscription. You want to clean up these resources so that you will not continue to be charged for them. You can delete resources individually or delete the resource group to delete the entire set of resources.

Learn more

For more information about Azure Backup, see the following articles:

- [Latest Azure Backup pricing and availability](#)
- [Documentation for the Azure Backup service](#)
- [Support matrix for Azure VM backup](#)
- [Security features in Azure Backup](#)
- [Built-in monitoring and alerting capabilities](#)
- [Azure Files - Snapshot management by Azure Backup](#)
- [Back up SQL Server databases running on Azure VMs](#)
- [Backup SAP HANA \(High-performance Analytic Appliance\) databases running on Azure VMs](#)
- [Azure Data Protection Manager \(DPM\) and Azure Backup Server \(MABS\)](#)