

Domain 6: Monitor and back up Azure resources

Introduction to Azure Backup

1. Introduction

<https://learn.microsoft.com/en-us/training/modules/intro-to-azure-backup/1-introduction>

Introduction

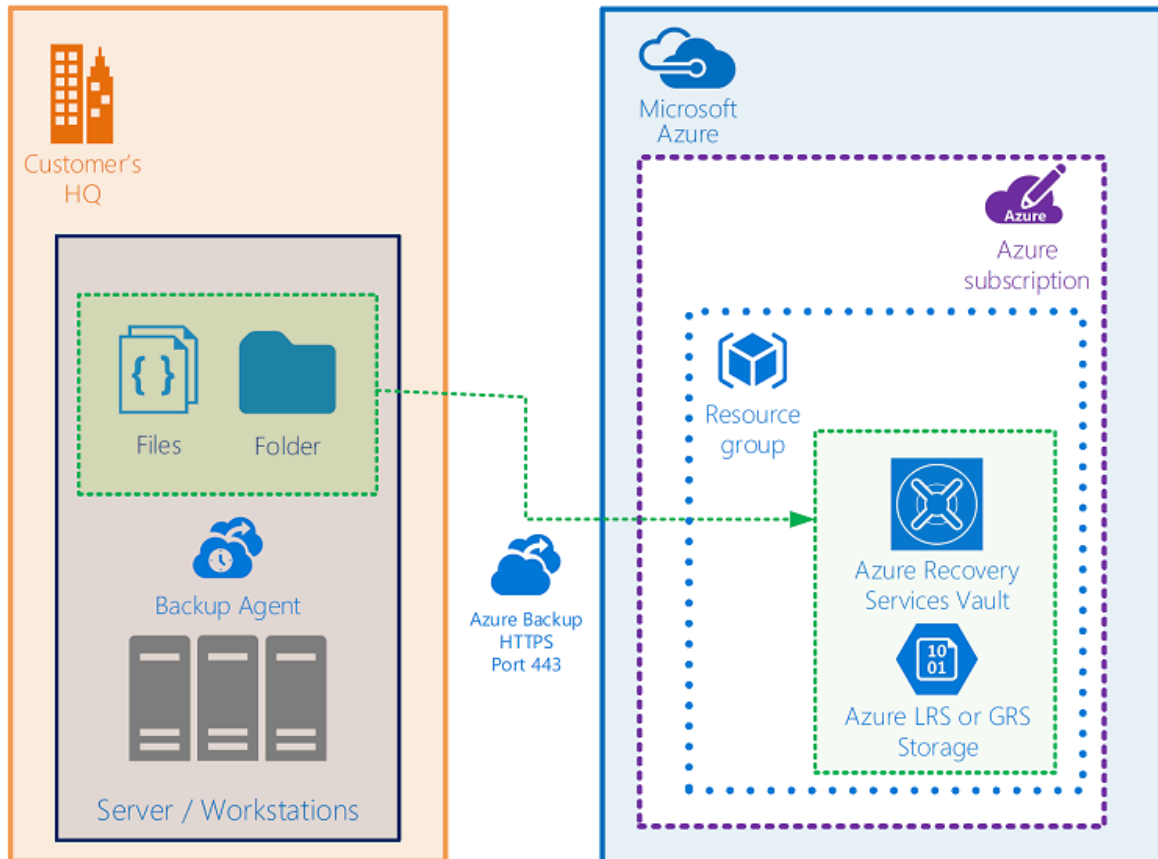
Completed

Information technology workers understand the importance of data to the organization. The need to protect that data drives decisions around storage, backups, and security. Many companies implement policies that dictate backup specifications for frequency, duration of backup storage, and restore policies.

For on-premises scenarios, backup solutions might have included local redundant storage solutions or off-site storage. Scenarios using backup to tape drives and storing offsite come with the resulting delay in restoring the data (because of the need to transport the tapes back to the server rooms and from performing the restore operation). This can result in significant downtime.

These backup solutions might not always address some of the most important considerations, such as security of the backups, the potential for the company to be impacted by a ransomware attack, or human error in the backup and restore operations. An ideal solution would be cost-effective, simple to use, and secure. This is where Azure Backup comes in.

Azure Backup: Back up on-premises Windows files/folders to Azure

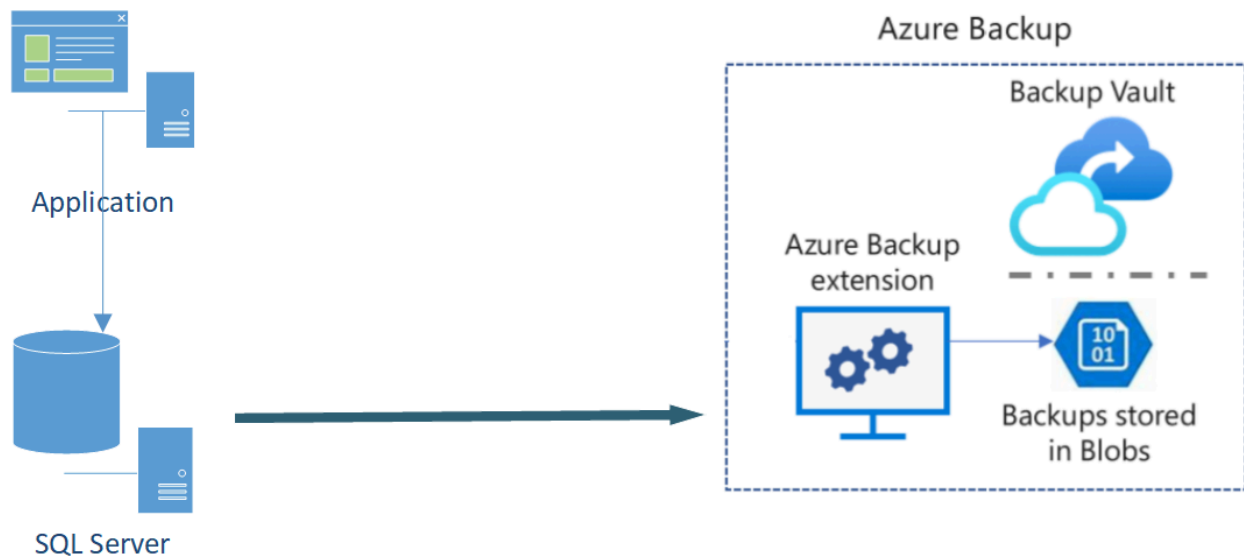


Azure Backup can also address scenarios for your Azure environments, with support for:

- Azure VMs
- Azure Managed Disks
- Azure Files
- SQL Server in Azure VMs
- SAP HANA databases in Azure VMs
- Azure Database for PostgreSQL servers
- Azure Blobs
- Azure Database for PostgreSQL - Flexible servers
- Azure Database for MySQL - Flexible servers
- Azure Kubernetes cluster

Example scenario

You're running an application powered by SQL Server. The database is running in an always-on availability group across three Azure VMs. You want to back up the databases using an Azure native backup service. You're looking to store the backup for 10 years in cheaper storage for your audit and compliance needs. You'd like to monitor the backup jobs daily for all such databases.



What will we be doing?

We'll evaluate the features and capabilities of Azure Backup to help decide if:

- Azure Backup can offer a solution for your backup needs.
- You can back up and restore the data you need for your organization.
- Azure Backup offers secure storage of your data.

What is the main goal?

By the end of this session, you'll be able to decide if Azure Backup is the right solution to consider for your data-protection needs.

2. What is Azure Backup?

<https://learn.microsoft.com/en-us/training/modules/intro-to-azure-backup/2-what-is-azure-backup>

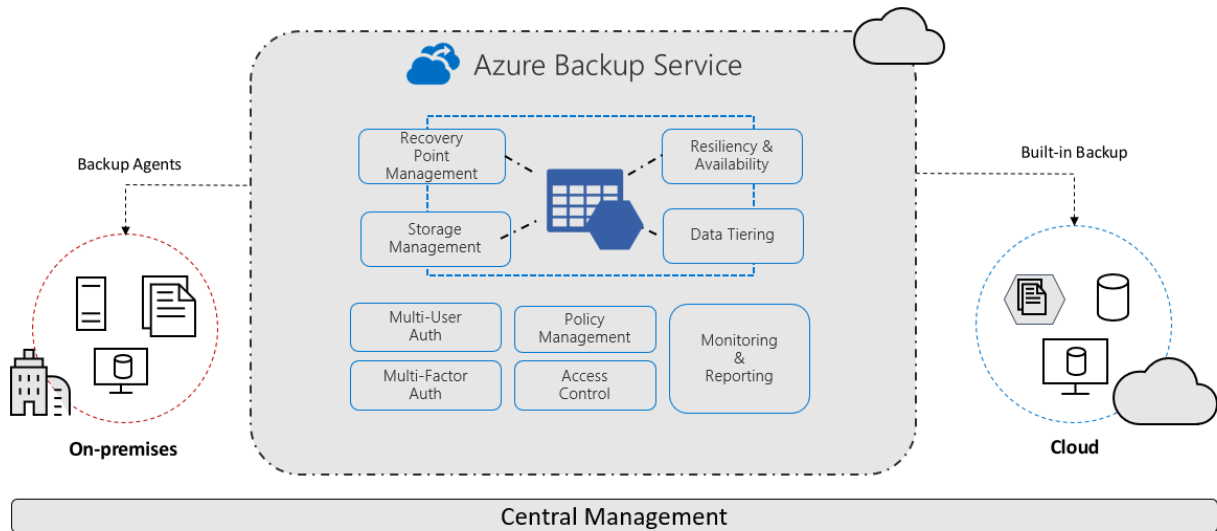
What is Azure Backup?

Completed

Let's start by defining Azure Backup and taking a quick tour of the core features. This overview should help you decide whether Azure Backup might be a good fit for your data-protection needs.

What is Azure Backup?

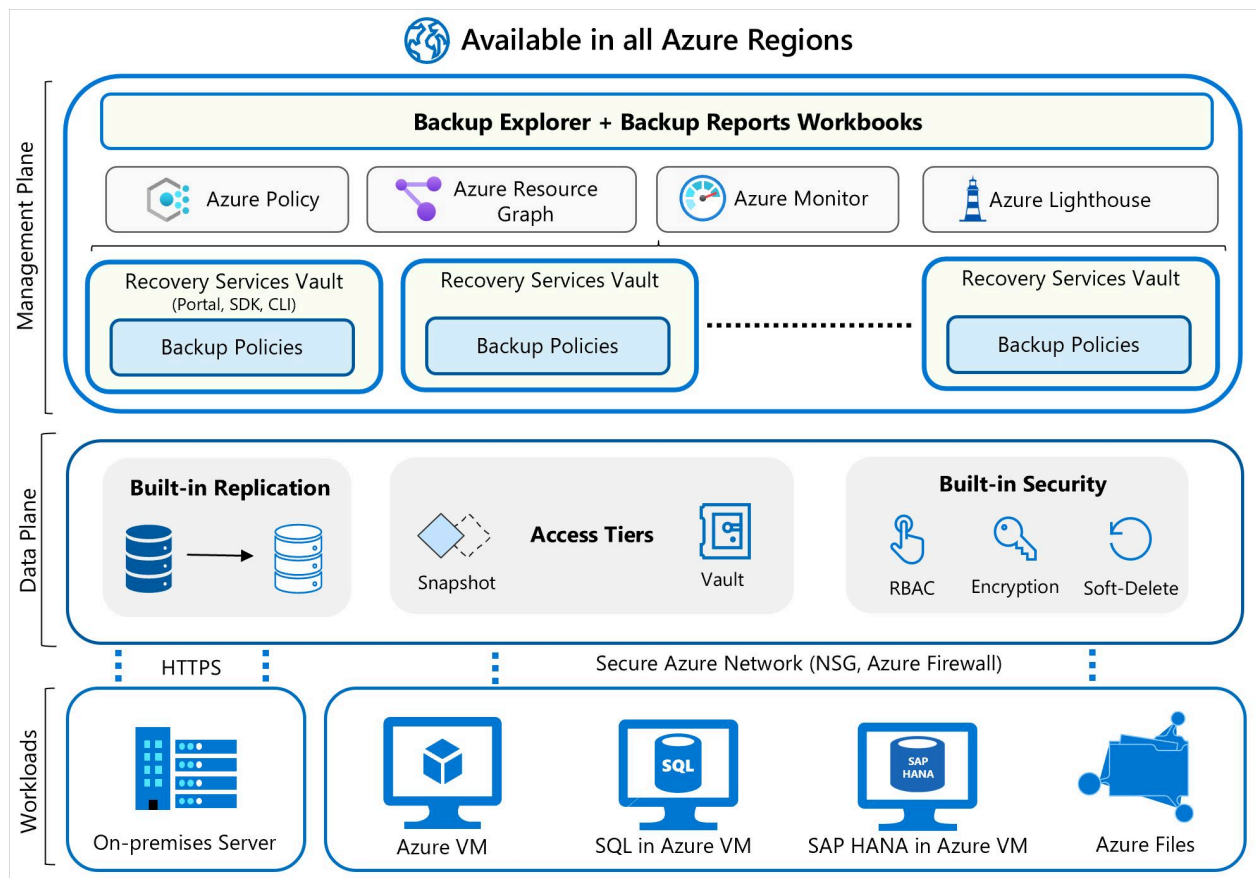
The Azure Backup service provides simple, secure, and cost-effective solutions to back up your data and recover it from the Microsoft Azure cloud.



Azure Backup definition

Azure Backup is an Azure service that provides cost effective, secure, and zero-infrastructure backup solutions for all Azure-managed data assets.

The centralized management interface makes it easy to define backup policies and protect a wide range of enterprise workloads, including Azure Virtual Machines, Azure Disks, SQL and SAP databases, Azure file shares, and blobs.



When to use Azure Backup

As the IT admin of your organization, you're responsible for meeting the compliance needs for all the data assets of the firm, and backup is a critical aspect. There are also various application admins in your company who need to do self-service backup and restore to take care of issues like data corruption or rogue-admin scenarios. You're looking for an enterprise-class backup solution to protect all your workloads and manage them from a central place.

Azure Backup can provide backup services for the following data assets:

- On-premises files, folders, and system state
- Azure Virtual Machines (VMs)
- Azure Managed Disks
- Azure Files Shares
- SQL Server in Azure VMs
- SAP HANA (High-performance Analytic Appliance) databases in Azure VMs
- Azure Database for PostgreSQL servers
- Azure Blobs
- Azure Database for PostgreSQL - Flexible servers
- Azure Database for MySQL - Flexible servers
- Azure Kubernetes cluster

Backup center | Backup jobs

Microsoft

Search (Ctrl+J)

Refresh

Select columns

Overview

Getting started

Community

Manage

Backup instances

Backup policies

Vaults

Monitoring + reporting

Backup jobs

Backup reports

Policy and compliance

Backup compliance

Azure policies for backup

Protectable datasources

Support + troubleshooting

New support request

Datasource subscription == 12 selected

Datasource resource group == All

Datasource location == All

Datasource type == Azure Virtual machines

Vault == All

Time range : Last 24 hours

Status == All

Operation == All

Filter by backup instance

1-11 of 11 items

Backup instance	Datasource subs...	Datasource reso...	Datasource locat...	Operation	Status	Vault	Start time	Duration	
CH1-JBOXVM00	Contoso Hotels Tena...	CH1-OpsRG-Pri	East US	Scheduled Backup	Completed	CH1-RV-Pri	3/8/2021, 7:24:04 AM	02:21:14	...
CH1-DCVM01	Contoso Hotels Tena...	CH1-InfraRG-Pri	East US	Scheduled Backup	Completed	CH1-RV-Pri	3/8/2021, 7:22:23 AM	02:21:14	...
CH1-AppBEVM01	Contoso Hotels Tena...	CH1-RetailRG-Pri	East US	Scheduled Backup	Completed	CH1-RV-Pri	3/8/2021, 7:21:46 AM	02:21:17	...
CH1-SQLVM01	Contoso Hotels Tena...	CH1-RetailRG-Pri	East US	Scheduled Backup	Completed	CH1-RV-Pri	3/8/2021, 7:20:21 AM	02:51:18	...
CH1-AppBEVM00	Contoso Hotels Tena...	CH1-RetailRG-Pri	East US	Scheduled Backup	Completed	CH1-RV-Pri	3/8/2021, 7:17:36 AM	02:26:17	...
CH1-SQLVM00	Contoso Hotels Tena...	CH1-RetailRG-Pri	East US	Scheduled Backup	Completed	CH1-RV-Pri	3/8/2021, 7:15:45 AM	02:51:18	...
CH1-DCVM00	Contoso Hotels Tena...	CH1-InfraRG-Pri	East US	Scheduled Backup	Completed	CH1-RV-Pri	3/8/2021, 7:15:23 AM	02:51:14	...
CH1-JBOXVM10	Contoso Hotels Tena...	CH1-OpsRG-Sec	West US 2	Scheduled Backup	Completed	CH1-RV-Sec	3/8/2021, 7:07:28 AM	02:21:12	...
CH1-SQLVM12	Contoso Hotels Tena...	CH1-RetailRG-Sec	West US 2	Scheduled Backup	Completed	CH1-RV-Sec	3/8/2021, 7:07:00 AM	02:31:17	...
CH1-DCVM11	Contoso Hotels Tena...	CH1-InfraRG-Sec	West US 2	Scheduled Backup	Completed	CH1-RV-Sec	3/8/2021, 7:04:54 AM	02:21:13	...
CH1-DCVM10	Contoso Hotels Tena...	CH1-InfraRG-Sec	West US 2	Scheduled Backup	Completed	CH1-RV-Sec	3/8/2021, 7:01:17 AM	02:21:14	...

< Previous

1

Next >

Key features

Let's look at some key features of Azure Backup.

Feature	Description	Usage
Zero-infrastructure backup solution	Unlike conventional backup solutions, no backup server or infrastructure is needed. Similarly, no backup storage needs to be deployed, because Azure Backup automatically manages and scales it.	Zero-infrastructure solution eliminates capital expenses and reduces operational expenses. It increases ease of use by automating storage management.
At-scale management	Natively manage your entire backup estate from a central console called Backup Center. Use APIs, PowerShell, and Azure CLI to automate Backup policy and security configurations.	Backup center simplifies data protection management at-scale by enabling you to discover, govern, monitor, operate, and optimize backup management from one unified console, which helps you to drive operational efficiency with Azure.
Security	Azure Backup provides built-in security to your backup environment, both when your data is in transit and at rest by using capabilities encryption, private endpoints, alerts, and so on.	Your backups are automatically secured against ransomware, malicious admins, and accidental deletions.

How do Recovery Time Objective and Recovery Point Objective work?

Recovery Time Objective (RTO) is the target time within which a business process must be restored after a disaster occurs to avoid unacceptable consequences. For instance, if a critical application goes

down due to a server failure and the business can only tolerate a maximum of four hours of downtime, then the RTO is four hours.

Recovery Point Objective (RPO) is the maximum amount of data loss, measured in time, that your organization can sustain during an event.

The following example scenario describes both the RPO and RTO concepts:

Your organization has an RPO of one hour for your customer database, which means you perform backups every hour. If a data-loss incident occurs, you lose not more than one hour of data. When you set RTO to three hours, then if a system failure occurs, you aim to restore access to the database within three hours to minimize the impact on operations.

3. How Azure Backup works

<https://learn.microsoft.com/en-us/training/modules/intro-to-azure-backup/3-how-azure-backup-works>

How Azure Backup works

Completed

Let's take a look at how Azure Backup works to provide the data protection you need. Particularly, let's look at how the different aspects of the backup service make it easy to back up various types of data, and how it offers security for your backups as well. In this unit, we cover the following aspects of the Azure Backup Service:

- **Workload integration layer - Backup Extension:** Integration with the actual workload, such as Azure virtual machines (VMs) or Azure Blobs, happens at this layer.
- **Data Plane - Access Tiers:** There are three access tiers where the backups could be stored:
 - Snapshot tier
 - Standard tier
 - Archive tier
- **Data Plane - Availability and Security:** The backup data is replicated across zones or regions, based on the redundancy the user specifies.
- **Management Plane – Recovery Services vault/Backup vault and Backup center:** The vault provides an interface for the user to interact with the backup service.

What data is backed up and how?

The simplest explanation of Azure Backup is that it backs up data, machine state, and workloads running on on-premises machines and VM instances to the Azure cloud. Azure Backup stores the backed-up data in Recovery Services vaults and Backup vaults.

For on-premises Windows machines, you can back up directly to Azure with the Azure Backup Microsoft Azure Recovery Services (MARS) agent. Alternatively, you can back up these Windows machines to a backup server, perhaps a System Center Data Protection Manager (DPM) or Microsoft Azure Backup Server (MABS). You can then back that server up to a Recovery Services vault in Azure.

If you're using Azure VMs, you can back them up directly. Azure Backup installs a backup extension to the Azure VM agent that's running on the VM, which allows you to back up the entire VM. If you only want to back up the files and folders on the VM, you can do so by running the MARS agent.

Azure Backup stores backed-up data in vaults: Recovery Services vaults and Backup vaults. A vault is an online-storage entity in Azure that's used to hold data such as backup copies, recovery points, and backup policies.

Supported backup types

Azure Backup supports full backups and incremental backups. Your initial backup is a full backup. DPM/MABS use the incremental backup for disk backups, and all backups to Azure also use incremental backups. As the name suggests, incremental backups only focus on the blocks of data that changed since the previous backup.

Azure Backup also supports SQL Server backup types. The following table outlines the support for SQL Server type backups:

Type	Description	Usage
Full	A full database backup backs up the entire database. It contains all the data in a specific database or in a set of filegroups or files. A full backup also contains enough logs to recover that data.	At most, you can trigger one full backup per day. You can choose to make a full backup on a daily or weekly interval.
Differential	A differential backup is based on the most recent full-data backup. It captures only the data that changed since the full backup.	At most, you can trigger one differential backup per day. You can't configure a full backup and a differential backup on the same day.
Multiple backups per day	Back up Azure VMs hourly with a minimum recovery point objective (RPO) of 4 hours and a maximum of 24 hours.	You can use Enhanced backup policy to set the backup schedule to 4, 6, 8, 12, and 24 hours (respectively) for new Azure offerings, such as Trusted Launch VM.
Selective disk backup	Selectively back up a subset of the data disks that are attached to your VM, then restore a subset of the disks that are available in a recovery point, both from instant restore and vault tier. Selective disk backup 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.	Azure Backup provides Selective Disk backup and restore capability using Enhanced backup policy.

Type	Description	Usage
Transaction Log	A log backup enables point-in-time restoration up to a specific second.	At most, you can configure transactional log backups every 15 minutes.

Workload integration layer - Backup Extension

A backup extension specific to each workload is installed on the source VM or a worker VM. At the time of backup (as defined by the user in the Backup Policy) the backup extension generates the backup, which could be:

- **Storage:** Snapshots when using an Azure VM or Azure Files.
- **Stream backup:** For databases like SQL or High-performance Analytic Appliance (HANA) running in VMs.

The backup data is eventually transferred to Azure Backup managed storage in the data plane by using secure Azure networks Network Security Groups (NSG), Firewalls, or more sophisticated private endpoints.

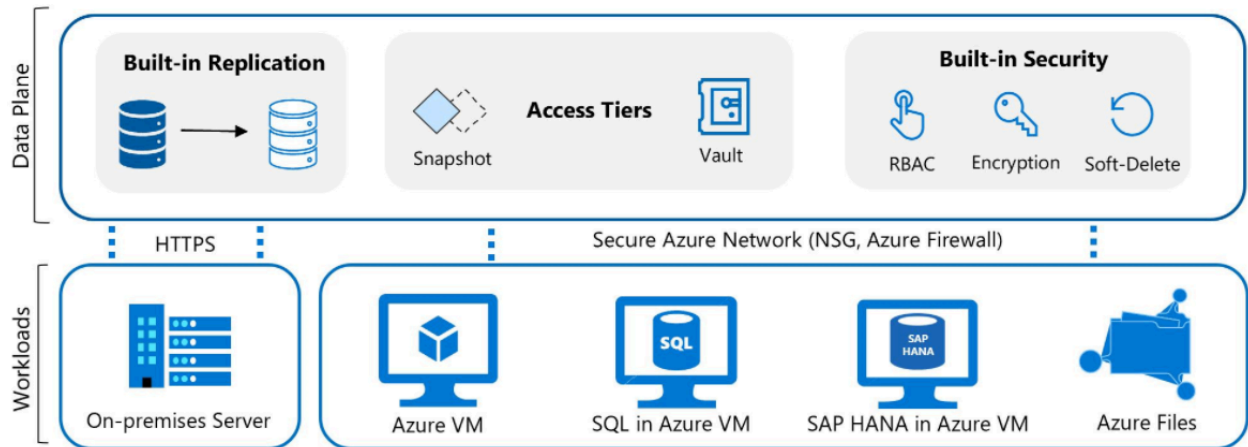
Data Plane - Access Tiers

There are three access tiers where the backups can be stored:

- **Snapshot tier:** (Workload-specific term) In the first phase of a virtual machine backup, the snapshot is taken and stored along with the disk. This form of storage is referred to as a snapshot tier. Restoring a snapshot tier is faster than restoring from a vault, because it eliminates the wait time for snapshots to be copied from the vault before triggering the restore operation. The snapshots of the VM/Azure Files/Azure Blobs/and so on are retained in the customer's subscription in a specified resource group. This container ensures that restores are quick, because the backup/snapshot is available locally to the customer.
- **Vault-standard tier:** Backup data for all workloads supported by Azure Backup is stored in vaults, which hold backup storage, an autoscaling set of storage accounts managed by Azure Backup. The Vault-standard tier is an online storage tier that allows you to store an isolated copy of backup data in a Microsoft-managed tenant, thus creating an extra layer of protection. For workloads where snapshot tier is supported, there's a copy of the backup data in both the snapshot tier and the Vault-standard tier. The Vault-standard tier ensures that backup data is available even if the data source being backed up is deleted or compromised.
- **Archive tier:** Customers rely on Azure Backup for storing backup data, including their Long-Term Retention (LTR) backup data, with retention needs defined in the organization's compliance rules. In most cases, the older backup data is rarely accessed and is only stored for compliance needs.

Azure Backup supports backup of long-term retention points in the archive tier.

All tiers offer different recovery time objectives (RTO) and are priced differently.



Data Plane - Availability and Security

The backup data is replicated across zones or regions, based on the redundancy you specify. You can choose from locally redundant storage (LRS), Geo-redundant storage (GRS), or zone-redundant storage (ZRS). These options provide you with highly available data storage capabilities.

The data is kept safe by encrypting it and implementing Azure role-based access control (RBAC). You choose who can perform backup and restore operations. Azure Backup also provides protection against malicious deletion of your backup by using soft-delete operations. A deleted backup is stored for 14 days, free of charge, which allows you to recover the backup if needed.

Azure Backup also supports a backup data lifecycle-management scenario that allows you to comply with retention policies.

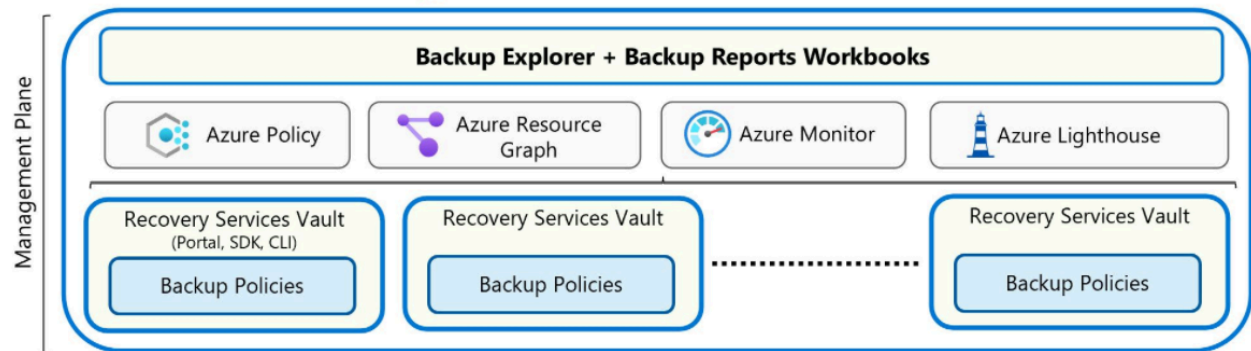


Management Plane – Recovery Services vault/Backup vault and Backup center

Azure Backup uses Recovery Services vaults and Backup vaults to orchestrate and manage backups. It also uses vaults to store backed-up data. The vault provides an interface for the user to interact with

the backup service. Azure Backup Policies within each vault define when the backups should get triggered and how long they need to be retained.

You can use a single vault or multiple vaults to organize and manage your backup. If you manage your workloads with a single subscription and single resource, you can use a single vault to monitor and manage your backup estate. If your workloads are spread across multiple subscriptions, you can create multiple vaults with one or more vaults per subscription.



Backup center allows you to have a single pane of glass to manage all tasks related to backups. Backup center is designed to function well across a large and distributed Azure environment. You can use Backup center to efficiently manage backups spanning multiple workload types, vaults, subscriptions, regions, and Azure Lighthouse tenants.

Home > Backup center

Search (Ctrl+/) « + Backup Restore + Policy + Vault Refresh

Overview Getting started Community

Manage Backup instances Backup policies Vaults Monitoring + reporting Backup jobs Backup reports Policy and compliance Backup compliance Azure policies for backup Protectable datasources Support + troubleshooting New support request

Datasource subscription == Account Datasource resource group == All Datasource location == All Datasource type == Azure Virtual machines Vault == All

Datasource type: Azure Virtual machines

Overview of Jobs and Backup instances

Jobs (last 24 Hours) View all

Operation	Failed	In progress	Completed
Scheduled backup	0	0	0
On-demand backup	0	0	0
Restore	0	0	0

Backup instances

Azure Virtual machines

0	Protection configured	0
	Protection stopped	0
	Soft deleted	0

0 out of 0 Backup instances with the underlying datasource not found

4. When to use Azure Backup

When to use Azure Backup

Completed

Here, we discuss how you can decide if Azure Backup is the right choice for your data-protection needs. In this unit, we highlight common backup scenarios where Azure Backup provides benefits, such as:

- Ensuring availability of your data.
- Protecting your Azure workloads.
- Securing your data.

Decision criteria

Azure Backup is an Azure service that provides secure and zero-infrastructure backup solutions for all Azure-managed data assets. It protects a wide range of enterprise workloads. Including, Azure Virtual Machines (VMs), Azure Disks, SQL and SAP databases, and Azure file shares and blobs.

The main criteria that we're evaluating are outlined in the following table. The table contains some key areas where Azure Backup can provide services to you for data protection.

Criteria	Consideration
Azure workloads	Azure VMs, Azure Disks, SQL Server in Azure VMs, SAP HANA databases in Azure VMs, Azure Blobs, Azure Files shares, Azure Database for PostgreSQL.
Compliance	Customer-defined backup policy with long-term retention across multiple zones or regions.
Operational recoveries	With self-service backup and restores, the application administrator can take care of issues that might arise such as accidental deletion or data corruption.

Apply the criteria

In the introduction, we presented a scenario where your organization might have an application that relies on data from a back-end SQL Server installation. SQL Server is running on three Azure VMs. The data in the backup must be retained for up to 10 years to meet compliance requirements. You also want to be able to monitor the backups.

Before we dive into how Azure Backup can help meet these needs, it's important to understand what isn't currently supported. If your three Azure VMs are deployed across multiple subscriptions or regions, you should note that Azure Backup doesn't support cross-region backup for most workloads. However, it does support cross-region restore in a paired secondary region.

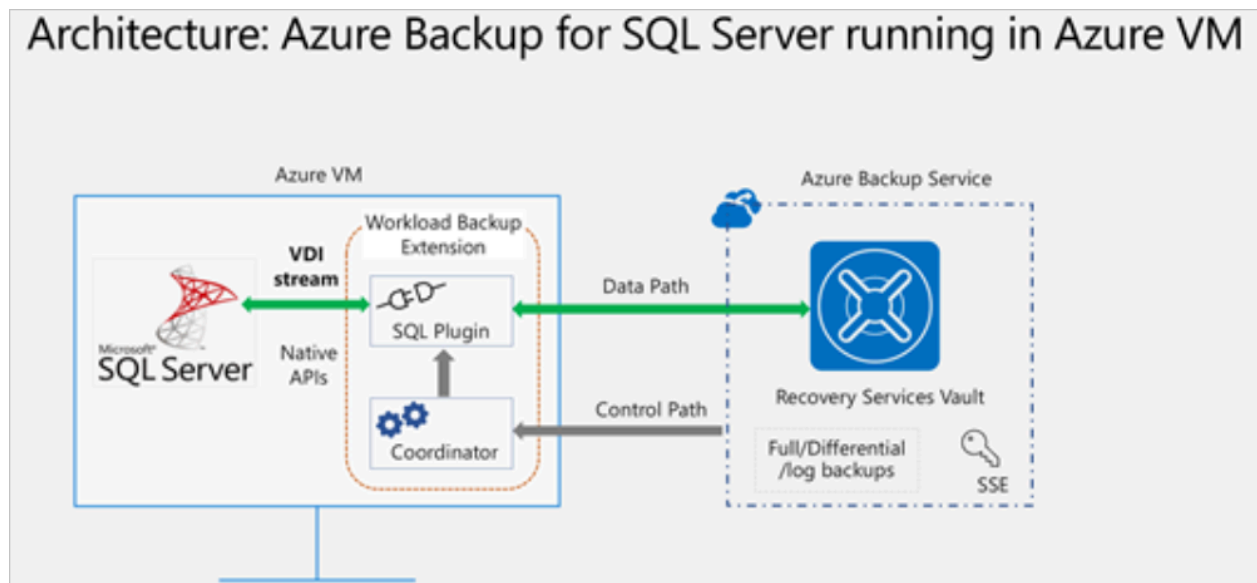
Can Azure Backup protect the Azure VMs hosting the SQL Server instances?

Azure Backup is able to back up entire Windows and Linux VMs using backup extensions. As a result, you can back up the entire VM that hosts SQL Server. If you only want to back up the files, folders, and system state on the Azure VMs, you can use the Microsoft Azure Recovery Services (MARS) agent.

If your main concern is to only back up the SQL Server data, Azure Backup provides support for that as well. Azure Backup offers a stream-based, specialized solution to back up SQL Servers running in Azure VMs. This solution aligns with Azure Backup's benefits of zero-infrastructure backup, long-term retention, and central management.

Additionally, Azure Backup provides the following advantages specifically for SQL Server:

- Workload aware backups that support all backup types: full, differential, and log
- 15-minute recovery point objective (RPO) with frequent log backups
- Point-in-time recovery up to a second
- Individual database-level backup and restore



Does Azure Backup help with compliance?

You can implement required access-control mechanisms for your backups. Vaults (Recovery Services and Backup vaults) provide the management capabilities and are accessible via the Azure portal, Backup Center, Vault dashboards, SDK, CLI, and even REST APIs. It's also an Azure role-based access control (Azure RBAC) boundary, providing you with the option to restrict access to backups only to authorized Backup Admins.

Short-term retention can be *minutes* or *daily*. Retention for *weekly*, *monthly*, or *yearly* backup points is referred to as *Long-term retention*.

Long-term retention can be:

- **Planned (compliance requirements):** If you know in advance that data is required years from the current time, use Long-term retention.
- **Unplanned (on-demand requirement):** If you don't know in advance, then you can use on-demand backup with specific custom retention settings. Your policy settings don't impact these custom retention settings.
- **On-demand backup with custom retention:** If you need to take a backup not scheduled via backup policy, then you can use an on-demand backup. It can be useful for taking backups that don't fit your scheduled backup or for taking granular backup (for example, multiple IaaS VM backups per day since scheduled backup permits only one backup per day). It's important to note that the retention policy defined in scheduled policy doesn't apply to on-demand backups.

You can also implement policy management to help with compliance. Azure Backup Policies within each vault define when the backups should be triggered and how long they need to be retained. You can also manage these policies and apply them across multiple items.

Does Azure Backup simplify monitoring and administration?

Azure Backup integrates with Log Analytics for monitoring and reporting and provides reports via Workbooks.

Azure Backup provides in-built job monitoring for operations such as configuring backup, backing up, restoring, deleting backups, and so on. Azure Backup is scoped to the vault, making it ideal for monitoring a single vault.

If you need to monitor operational activities at scale, Backup Explorer provides an aggregated view of your entire backup estate, enabling detailed drill-down analysis and troubleshooting. It's a built-in Azure Monitor workbook that provides a single, central location to help you monitor operational activities across the entire backup estate on Azure, spanning tenants, locations, subscriptions, resource groups, and vaults.

5. Module assessment

<https://learn.microsoft.com/en-us/training/modules/intro-to-azure-backup/5-knowledge-check>

Module assessment

Completed

6. Summary

Summary

Completed

Our goal was to help you evaluate whether Azure Backup would offer the features and capabilities you need to help you protect your data. During the module, we explored how Azure Backup might address:

- Ensuring availability of your data.
- Protecting your Azure workloads.
- Securing your data.

We applied the criteria to a scenario where your company was hosting an application that used a SQL Server database instance running on multiple Azure VMs. We noted how Azure Backup could provide data protection by backing up our Azure VMs or the files, folders, and system state on those VMs.

We also saw how Azure Backup helps with compliance by offering retention options for the data and security with encryption and RBAC. Using Backup center, we showed how easy it is to manage these backups.

Backup center simplifies data protection management at-scale by allowing you to discover, govern, monitor, operate, and optimize backup management, all from one unified console. This helps you to drive operational efficiency with Azure. Your backups are automatically secured against ransomware, malicious admins, and accidental deletions.

References

- [Azure Backup website](#)
- [Azure Backup compliance standards](#)

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 for 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 on 6/21/2020 at 6:01:37 AM), and a Summary section (listing Recovery services vault as ShopKartDemoVault, Backup policy as DefaultPolicy, and Oldest restore point as 4/5/2020 at 6:14:48 AM). Below these is a 'Restore points (4)' section, which includes a filter for the last 30 days and a table of restore points. The table has columns for Time, Consistency, Recovery Type, and a menu icon. The restore points listed are: 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), and 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.

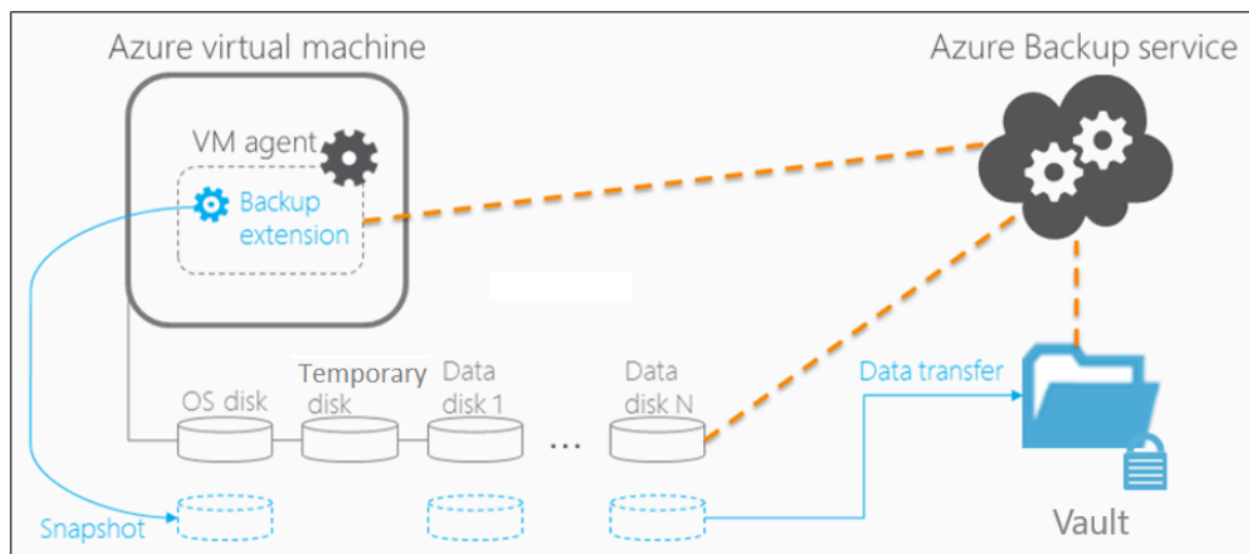
Snapshot tier: All the snapshots are stored locally for a maximum period of five days, in what is called the snapshot tier. For all types of operation recoveries, we recommended that you restore from the snapshots because it's faster to do so. This capability is called **instant restore**.

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.

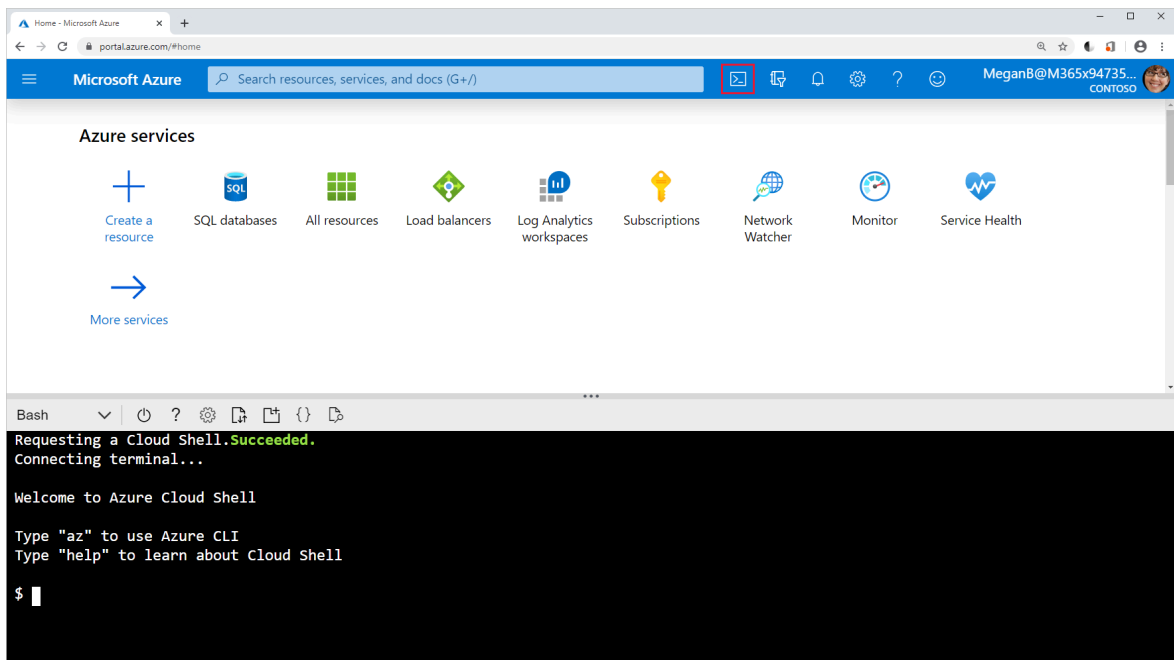
Note

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

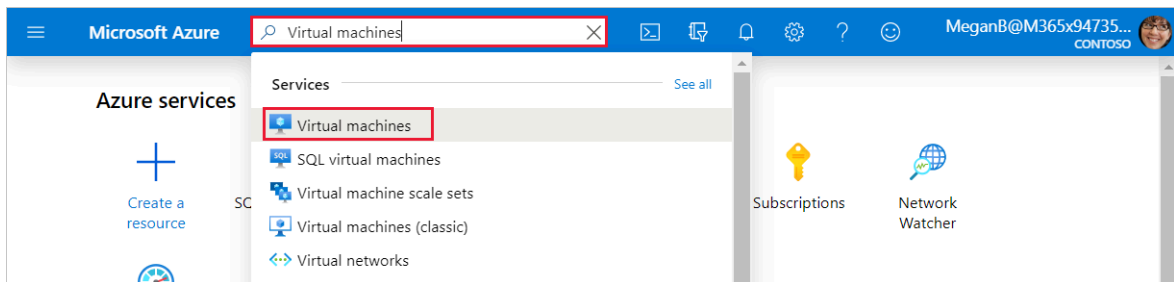
If you get a `securityProfile.securityType is invalid` error running the preceding command, run the following commands to register `UseStandardSecurityType`, then re-run the preceding command.

```
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.

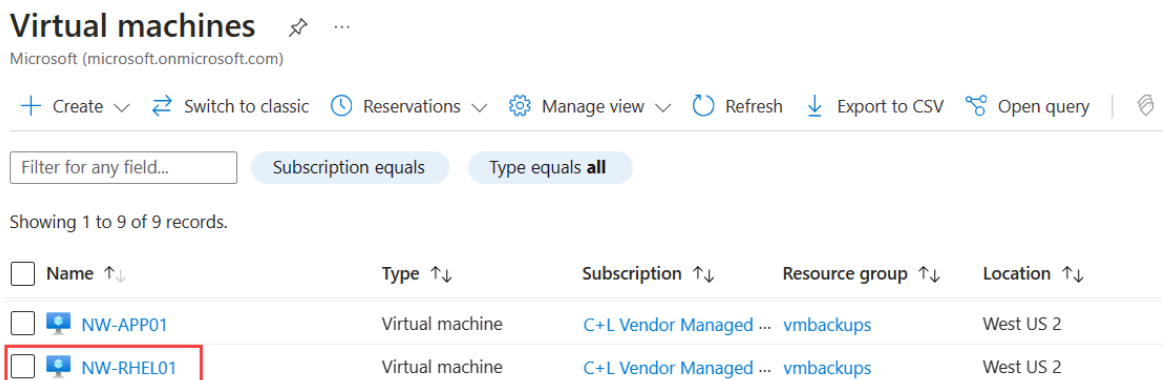
Enable backup for a virtual machine by using the Azure portal

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.

NW-RHEL01 | Backup ☆ ...

Virtual machine

Search

Network manager

Settings

Disks

Extensions + applications

Configuration

Advisor recommendations

Properties

Locks

Availability + scale

Size

Availability + scaling

Security

Identity

Microsoft Defender for Cloud

Backup + disaster recovery

Backup

Disaster recovery

Operations

Auto-shutdown

Welcome to Azure Backup for Azure VMs

Simple and reliable VM backup to the Azure. [Learn more](#). You are charged an instance fee based on the size of the VM and for backup data retained in Snapshots and the Recovery Services Vault. [Learn more about pricing](#).

Review the following information and click on 'Enable backup' to start protecting your VM.

Recovery Services vault ⓘ ☒ Create new ☐ Select existing

Backup vault * vault751 ✓

Resource group vmbackups

Policy sub type *

☒ Standard

- ✓ Once a day backup
- ✓ 1-5 days operational tier
- ✓ Vault tier
- ZRS resilient snapshot tier
- Support for Trusted Azure VM

☐ Enhanced

- ✓ Multiple backups per day
- ✓ 1-30 days operational tier
- ✓ Vault tier
- ✓ ZRS resilient snapshot tier
- ✓ Support for Trusted Azure VM

Choose backup policy * ⓘ (new) DailyPolicy-lqxwxm5x

[Edit this policy](#)

Enable backup Cancel

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
```

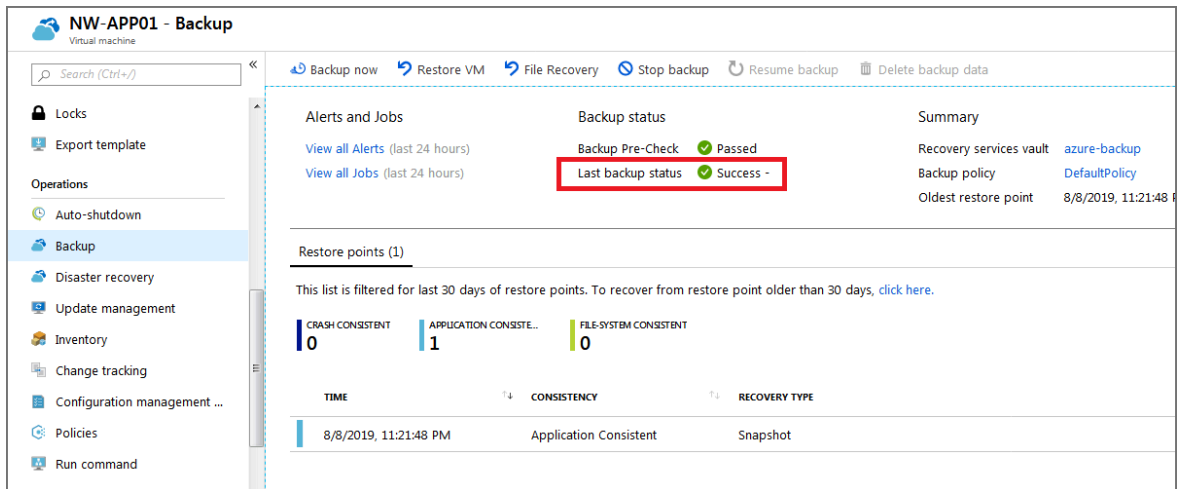
There's no need to wait for the backup to finish, because the next section shows you how to monitor the progress in the portal.

Monitor backups in the portal

View the status of a backup for a single virtual machine

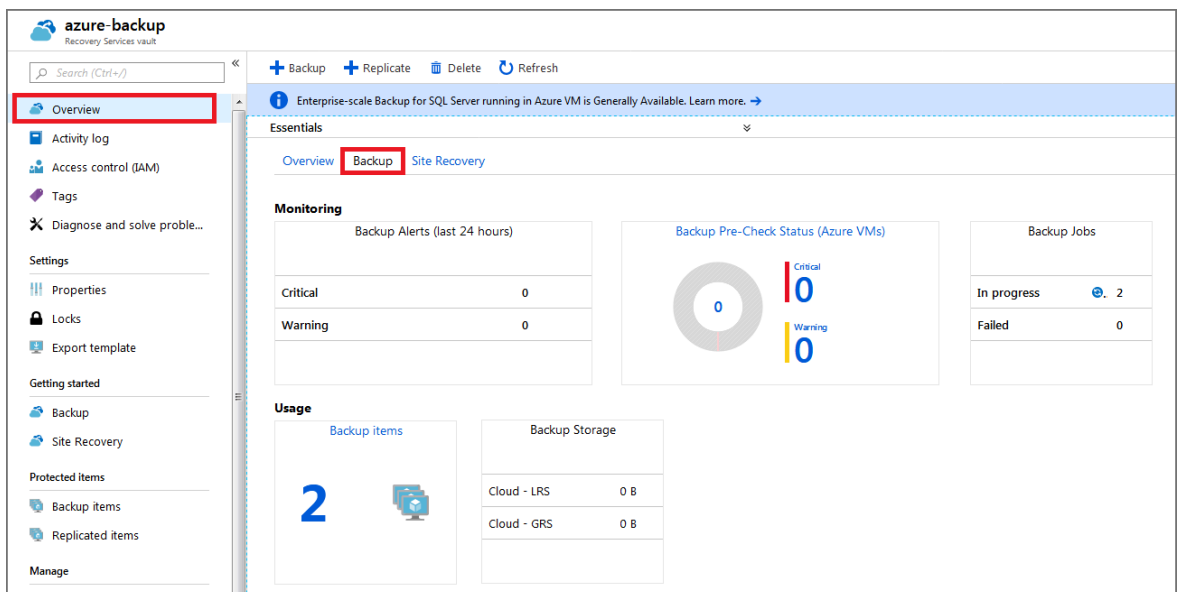
1. On the Azure portal menu or from the **Home** page, select **All resources**.
2. Enter *Virtual machines* in the search field at the top of the page and select **Virtual machines** from the results.
3. Select the **NW-APP01** virtual machine. The *NW-APP01* virtual machine pane appears.
4. In the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

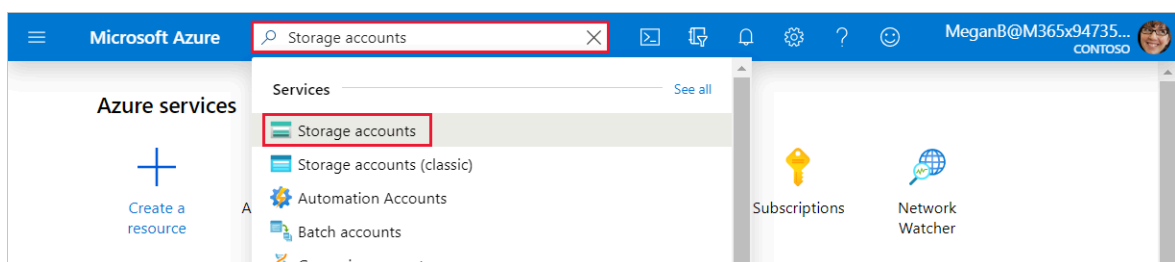
A few days after you backed up your first Azure virtual machine (VM), the server had issues. The VM needs to be restored from a backup. You want to restore the VM's disk and attach it to the problematic live server, and then track the restore to ensure that it finished successfully.

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 * <Subscription name placeholder>

Resource group * vmbackups
[Create new](#)

Instance details

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

Storage account name ⓘ * <Storage account name placeholder>

Region ⓘ * (US) West US 2

Performance ⓘ *

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

☐ Premium: Recommended for scenarios that require low latency.

Redundancy ⓘ *

Geo-redundant storage (GRS)

☒ 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' window in the Azure portal. On the left, there's a red banner indicating 'Validation failed. Click here for more details.' Below this, there 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)'. On the right, 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

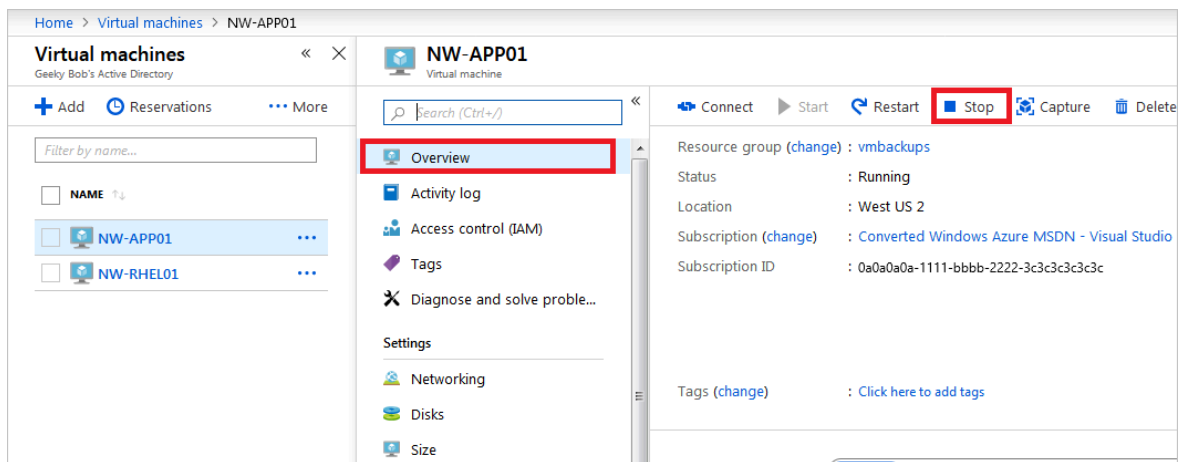
To prevent this error, follow these steps:

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

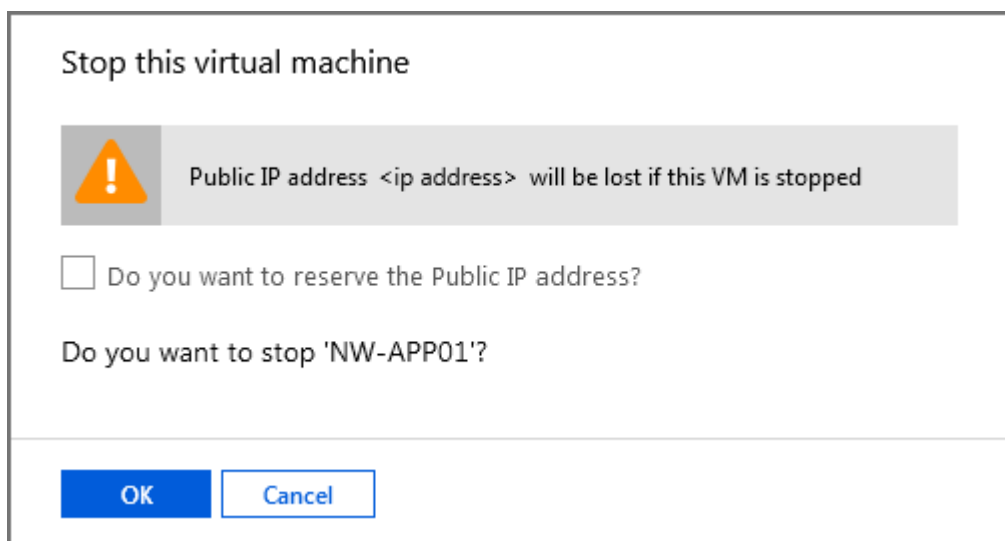
The screenshot shows the 'Virtual machines' page in the Azure portal. The 'NW-APP01' virtual machine is selected and highlighted with a red box. The right-hand pane shows the 'Overview' tab for the selected VM, displaying details like Resource group, Status (Running), Location (West US 2), Subscription, and Subscription ID.

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

Operations

- Locks
- Bastion
- Auto-shutdown
- Backup**
- Disaster recovery
- Guest + host updates
- Inventory
- Change tracking
- Configuration management (Preview)
- Policies
- Run command
- Monitoring

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](#).

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

- To restore the virtual machine, in the menu bar, select **Restore VM**. The **Restore Virtual Machine** pane for **NW-APP01** appears.
- Under the **Restore point** text box, choose **Select**. The **Select restore point** pane appears.
- 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.

- 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 ?](#)

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 \(MABS\)](#)

Monitor your Azure virtual machines with Azure Monitor

1. Introduction

<https://learn.microsoft.com/en-us/training/modules/monitor-azure-vm-using-diagnostic-data/1-introduction>

Introduction

Completed

Suppose you're the IT administrator for a musical group's website hosted on Azure virtual machines (VMs). The website runs mission-critical services for the group, including ticket booking, venue information, and tour updates. The website must respond quickly and remain accessible during frequent updates and spikes in traffic.

You need to maintain sufficient VM size and memory to effectively host the website without incurring unnecessary costs. You also need to proactively prevent and quickly respond to any access, security, and performance issues. To help achieve these objectives, you want to quickly and easily monitor your VMs' traffic, health, performance, and events.

Azure Monitor provides built-in and customizable monitoring abilities. You can use these to track the health, performance, and behavior of the VM host and the operating system, workloads, and applications running on your VM. This learning module shows you how to view VM host monitoring data, set up recommended alert rules, and use VM insights and custom data collection rules (DCRs) to collect and analyze monitoring data from inside your VMs.

Prerequisites

To complete this module, you need the following prerequisites:

- Familiarity with virtualization, Azure portal navigation, and Azure VMs.
- Access to an Azure subscription with at least **Contributor** role. If you don't have an Azure subscription, create a [free account](#) and add a subscription before you begin. If you're a student, you can take advantage of the [Azure for students](#) offer.

Learning objectives

- Understand which monitoring data you need to collect from your VM.
- Enable and view recommended alerts and diagnostics.
- Use Azure Monitor to collect and analyze VM host data.
- Use Azure Monitor Agent to collect VM client performance metrics and event logs.

2. Monitoring for Azure VMs

<https://learn.microsoft.com/en-us/training/modules/monitor-azure-vm-using-diagnostic-data/2-monitor-vm-health>

Monitoring for Azure VMs

Completed

3. Monitor VM host data

<https://learn.microsoft.com/en-us/training/modules/monitor-azure-vm-using-diagnostic-data/3-exercise-create-virtual-machine>

Monitor VM host data

Completed

4. Use Metrics Explorer to view detailed host metrics

<https://learn.microsoft.com/en-us/training/modules/monitor-azure-vm-using-diagnostic-data/4-view-host-metrics>

Use Metrics Explorer to view detailed host metrics

Completed

5. Collect client performance counters by using VM insights

<https://learn.microsoft.com/en-us/training/modules/monitor-azure-vm-using-diagnostic-data/5-enable-vm-insights>

Collect client performance counters by using VM insights

Completed

6. Collect VM client event logs

<https://learn.microsoft.com/en-us/training/modules/monitor-azure-vm-using-diagnostic-data/6-collect-log-data>

Collect VM client event logs

Completed

7. Summary

Summary

Completed

Azure Monitor helps you collect, analyze, and alert on various types of host and client monitoring data from your Azure VMs.

- Azure Monitor provides a set of VM host logs and performance and usage metrics for all Azure VMs.
- You can enable recommended alert rules when you create VMs or afterwards to alert on important VM host metrics.
- Azure Monitor Metrics Explorer lets you graph and analyze metrics for Azure VMs and other resources.
- VM insights provides a simple way to monitor important VM client performance counters and processes running on your VM.
- You can create data collection rules to collect other metrics and logs from your VM client.
- You can use Log Analytics to query and analyze log data.

Now that you understand these tools, you're confident that Azure Monitor can effectively monitor your Azure VMs and help you keep your website running effectively.

Clean up resources

In this module, you created a VM in your Azure subscription. To prevent further charges for this VM, you can delete it or the resource group that contains it.

To delete the resource group that contains the VM and its resources:

1. Select the **Resource group** link at the top of the **Essentials** section on the VM's **Overview** page.
2. At the top of the resource group page, select **Delete resource group**.
3. On the delete screen, select the checkbox next to **Apply force delete for selected virtual machines and virtual machine scale sets**. Enter the resource group name in the field, and then select **Delete**.

Learn more

To learn more about monitoring your VMs with Azure Monitor, see the following resources:

- [Azure Monitor documentation](#)
- [Monitor virtual machines with Azure Monitor](#)

- [Supported metrics with Azure Monitor](#)
- [Send Azure Monitor Activity log data](#)
- [Supported metrics for Microsoft.Compute/virtualMachines](#)
- [Overview of VM insights](#)
- [Create interactive reports with VM insights workbooks](#)
- [Use the Map feature of VM insights to understand application components](#)
- [Azure Monitor Agent overview](#)
- [Collect data with Azure Monitor Agent](#)
- [Tutorial: Collect guest logs and metrics from an Azure virtual machine](#)