

Introduction to Azure Backup

1. Introduction

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

Introduction

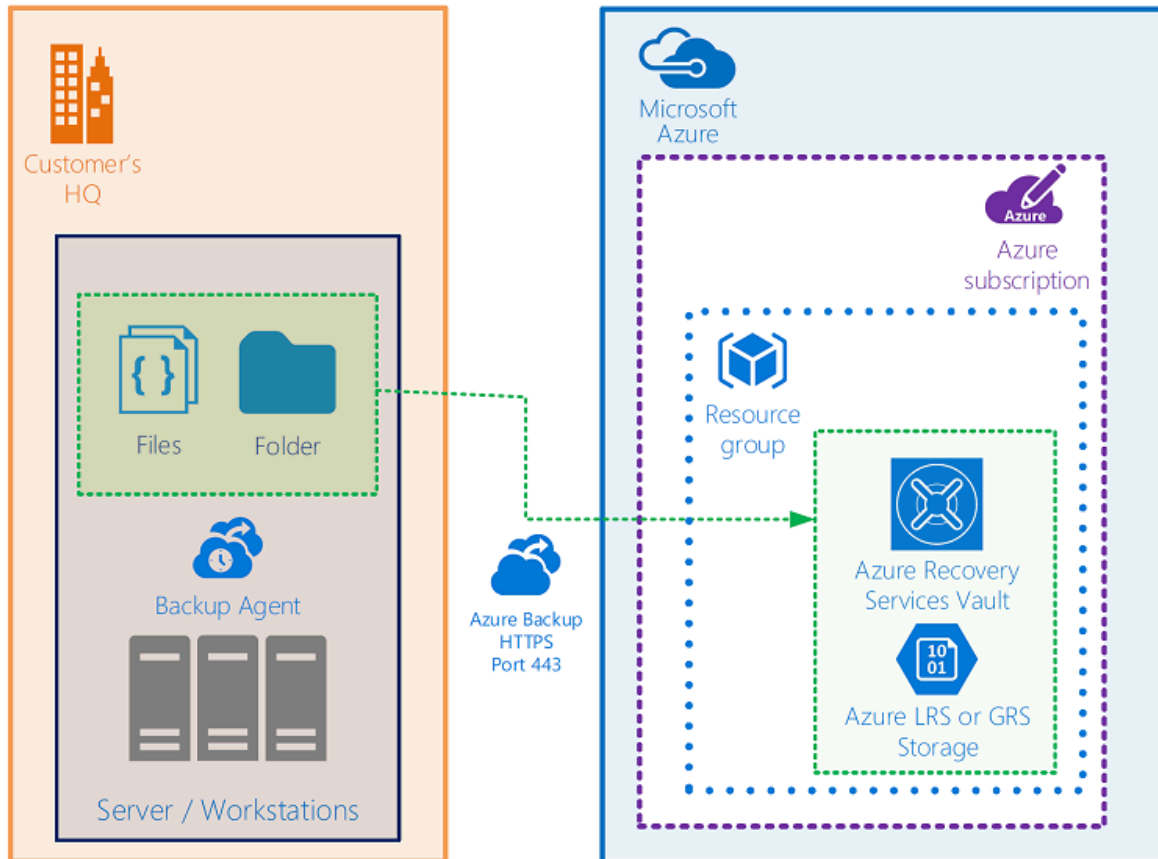
Completed

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

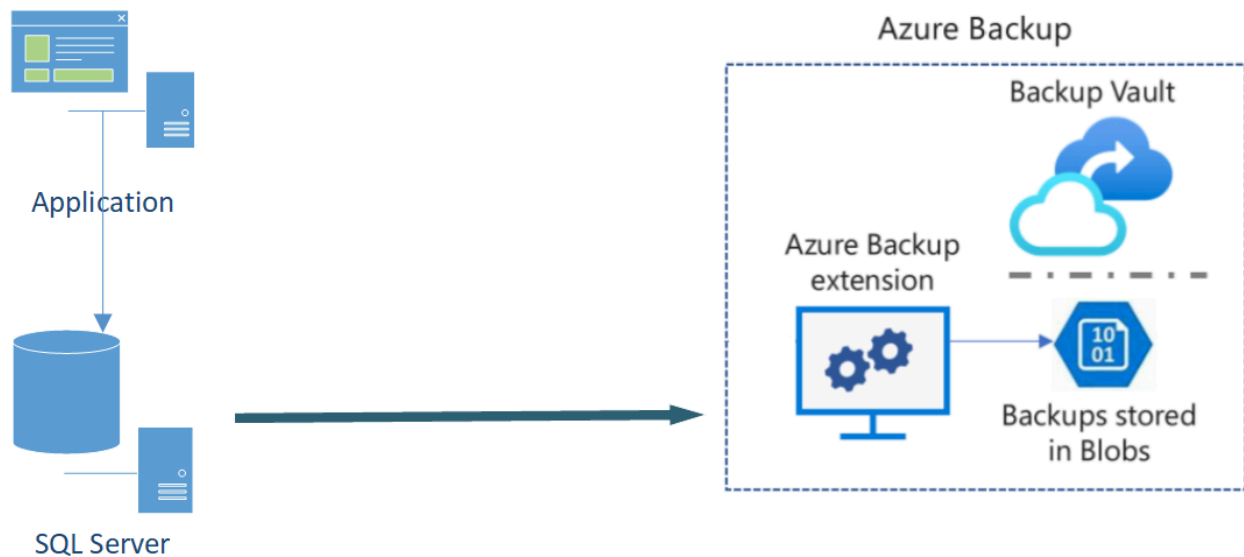


Azure Backup can also address scenarios for your Azure environments, with support for:

- 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>

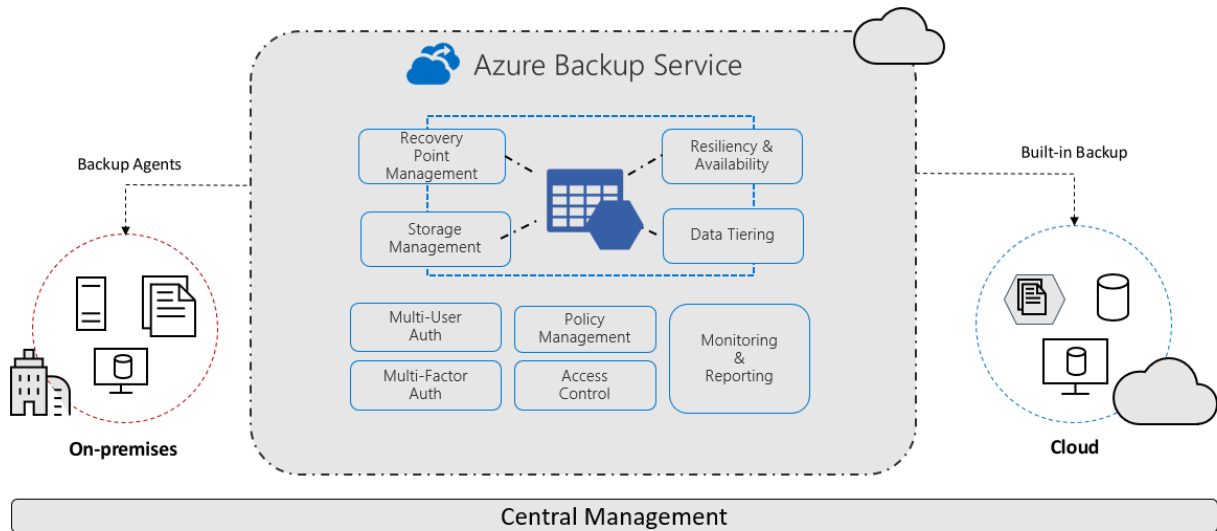
What is Azure Backup?

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?

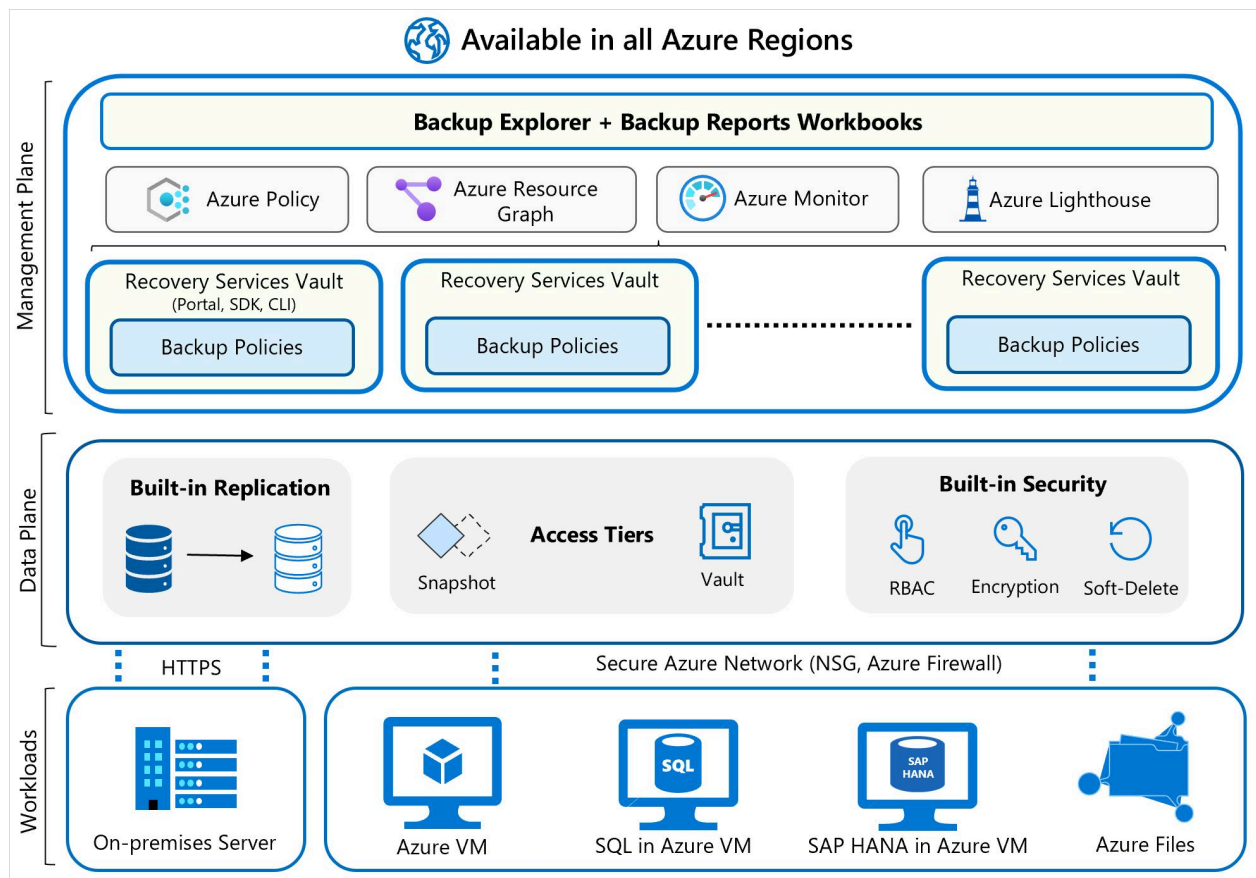
The Azure Backup service provides simple, secure, and cost-effective solutions to back up your data and recover it from the Microsoft Azure cloud.



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

Microsoft

Backup center | Backup jobs

...

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.

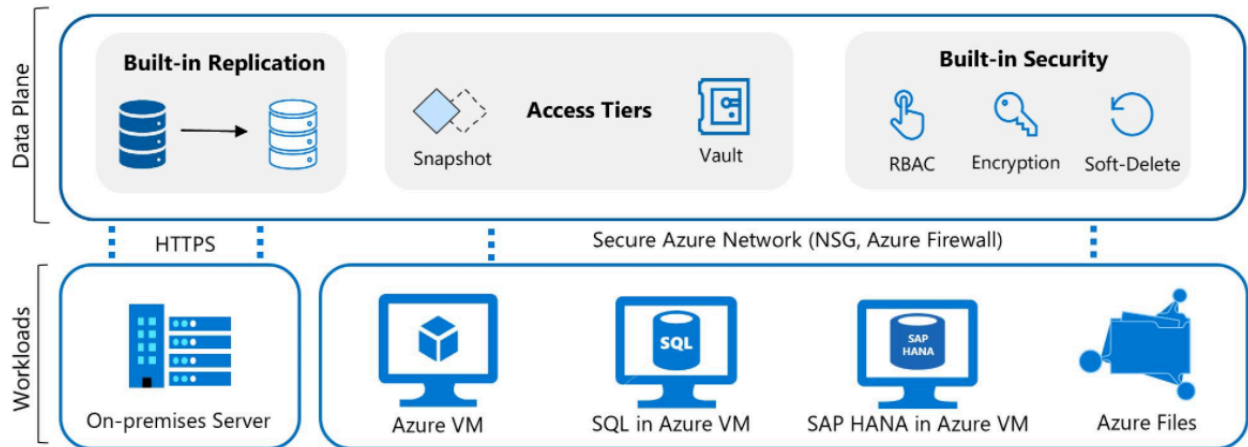
Data Plane - Access Tiers

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.

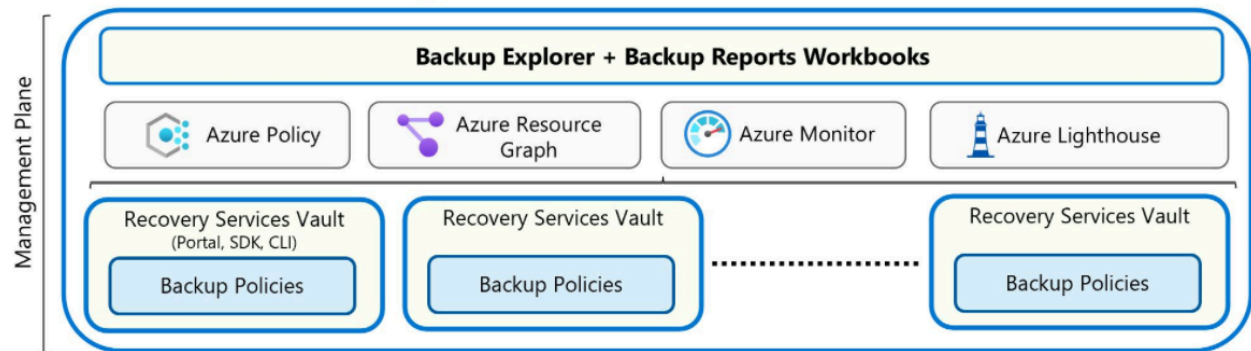


Management Plane – Recovery Services vault/Backup vault and Backup center

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.

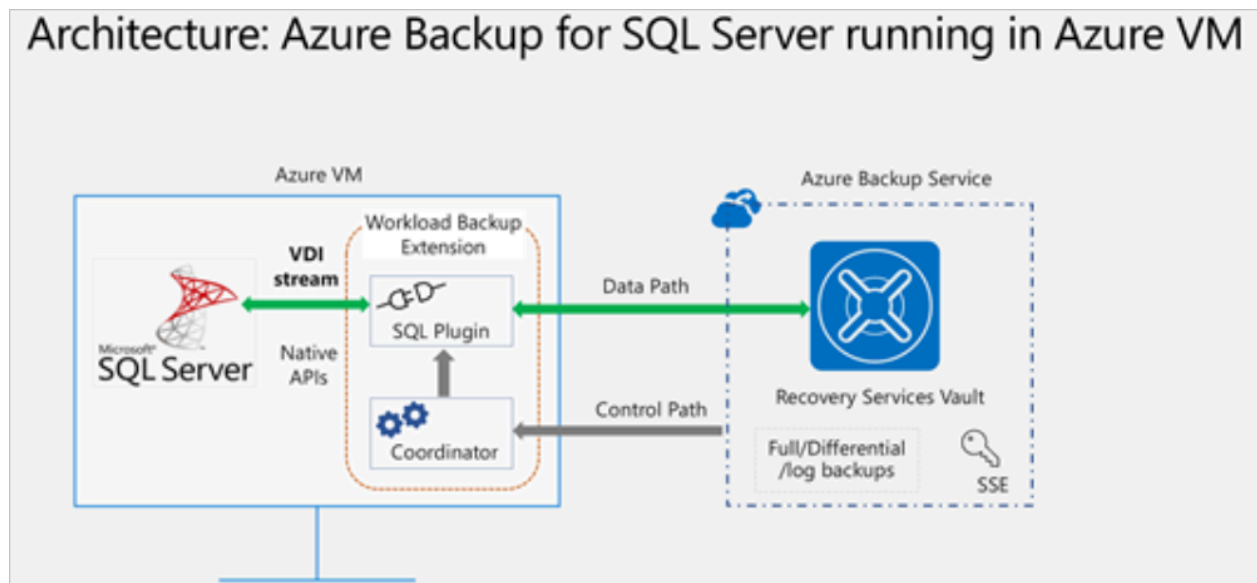
Can Azure Backup protect the Azure VMs hosting the SQL Server instances?

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](#)