https://www.westconcomstor.com/content/dam/wcgcom/Global/Cloud/Vendors/Microsoft/HomePage_MicrosoftLogo_FeatureVendor.png

All About Azure

Simple and reliable cloud integrated backup as a service

* Unified solution to protect data on-premises and in the cloud
* 99.9% availability guaranteed
* Reliable offsite backup target
* Efficient incremental backups
* Secure—data is encrypted in transit and at rest
* Geo-replicated backup store

Azure Backup is the Azure-based service you can use to back up (or protect) and restore your data in the Microsoft cloud. Azure Backup replaces your existing on-premises or off-site backup solution with a cloud-based solution that is reliable, secure, and cost-competitive. Azure Backup offers multiple components that you download and deploy on the appropriate computer, server, or in the cloud. The component, or agent, that you deploy depends on what you want to protect. All Azure Backup components (no matter whether you're protecting data on-premises or in the cloud) can be used to back up data to a Backup vault in Azure. See the [Azure Backup components table](https://docs.microsoft.com/en-us/azure/backup/backup-introduction-to-azure-backup#which-azure-backup-components-should-i-use) (later in this article) for information about which component to use to protect specific data, applications, or workloads.

## Why use Azure Backup?

Traditional backup solutions have evolved to treat the cloud as an endpoint, or static storage destination, similar to disks or tape. While this approach is simple, it is limited and doesn't take full advantage of an underlying cloud platform, which translates to an expensive, inefficient solution. Other solutions are expensive because you end up paying for the wrong type of storage, or storage that you don't need. Other solutions are often inefficient because they don't offer you the type or amount of storage you need, or administrative tasks require too much time. In contrast, Azure Backup delivers these key benefits:

**Automatic storage management** - Hybrid environments often require heterogeneous storage - some on-premises and some in the cloud. With Azure Backup, there is no cost for using on-premises storage devices. Azure Backup automatically allocates and manages backup storage, and it uses a pay-as-you-use model. Pay-as-you-use means that you only pay for the storage that you consume. For more information, see the [Azure pricing article](https://azure.microsoft.com/pricing/details/backup).

**Unlimited scaling** - Azure Backup uses the underlying power and unlimited scale of the Azure cloud to deliver high-availability - with no maintenance or monitoring overhead. You can set up alerts to provide information about events, but you don't need to worry about high-availability for your data in the cloud.

**Multiple storage options** - An aspect of high-availability is storage replication. Azure Backup offers two types of replication: [locally redundant storage](https://docs.microsoft.com/en-us/azure/storage/storage-redundancy#locally-redundant-storage) and [geo-redundant storage](https://docs.microsoft.com/en-us/azure/storage/storage-redundancy#geo-redundant-storage). Choose the backup storage option based on need:

* Locally redundant storage (LRS) replicates your data three times (it creates three copies of your data) in a paired datacenter in the same region. LRS is a low-cost option for protecting your data from local hardware failures.
* Geo-redundant storage (GRS) replicates your data to a secondary region (hundreds of miles away from the primary location of the source data). GRS costs more than LRS, but GRS provides a higher level of durability for your data, even if there is a regional outage.

**Unlimited data transfer** - Azure Backup does not limit the amount of inbound or outbound data you transfer. Azure Backup also does not charge for the data that is transferred. However, if you use the Azure Import/Export service to import large amounts of data, there is a cost associated with inbound data. For more information about this cost, see [Offline-backup workflow in Azure Backup](https://docs.microsoft.com/en-us/azure/backup/backup-azure-backup-import-export). Outbound data refers to data transferred from a Backup vault during a restore operation.

**Data encryption** - Data encryption allows for secure transmission and storage of your data in the public cloud. You store the encryption passphrase locally, and it is never transmitted or stored in Azure. If it is necessary to restore any of the data, only you have encryption passphrase, or key.

**Application-consistent backup** - Whether backing up a file server, virtual machine, or SQL database, you need to know that a recovery point has all required data to restore the backup copy. Azure Backup provides application-consistent backups, which ensured additional fixes are not needed to restore the data. Restoring application consistent data reduces the restoration time, allowing you to quickly return to a running state.

**Long-term retention** - Instead of switching backup copies from disk to tape and moving the tape to an off-site location, you can use Azure for short-term and long-term retention. Azure doesn't limit the length of time data remains in a Backup or Recovery Services vault. You can keep data in a vault for as long as you like. Azure Backup has a limit of 9999 recovery points per protected instance. See the [Backup and retention](https://docs.microsoft.com/en-us/azure/backup/backup-introduction-to-azure-backup#backup-and-retention)section in this article for an explanation of how this limit may impact your backup needs.

## Which Azure Backup components should I use?

If you aren't sure which Azure Backup component works for your needs, see the following table for information about what you can protect with each component. The Azure portal provides a wizard, which is built into the portal, to guide you through choosing the component to download and deploy. The wizard, which is part of the Recovery Services vault creation, leads you through the steps for selecting a backup goal, and choosing the data or application to protect.

## Which Azure Backup components should I use?

If you aren't sure which Azure Backup component works for your needs, see the following table for information about what you can protect with each component. The Azure portal provides a wizard, which is built into the portal, to guide you through choosing the component to download and deploy. The wizard, which is part of the Recovery Services vault creation, leads you through the steps for selecting a backup goal, and choosing the data or application to protect.

| Component | Benefits | Limits | What is protected? | Where are backups stored? |
| --- | --- | --- | --- | --- |
| Azure Backup (MARS) agent |  Back up files and folders on physical or virtual Windows OS (VMs can be on-premises or in Azure)   No separate backup server required. |  Backup 3x per day   Not application aware; file, folder, and volume-level restore only,   No support for Linux. |  Files,   Folders | Azure Backup vault |
| System Center DPM |  Application-aware snapshots (VSS)   Full flexibility for when to take backups   Recovery granularity (all)   Can use Azure Backup vault   Linux support on Hyper-V and VMware VMs   Back up and restore VMware VMs using DPM 2012 R2 | Cannot back up Oracle workload. |  Files,   Folders,    Volumes,   VMs,    Applications,    Workloads |  Azure Backup vault,    Locally attached disk,   Tape (on-premises only) |
| Azure Backup Server |  App aware snapshots (VSS)   Full flexibility for when to take backups   Recovery granularity (all)   Can use Azure Backup vault   Linux support on Hyper-V and VMware VMs   Back up and restore VMware VMs   Does not require a System Center license |  Cannot back up Oracle workload.   Always requires live Azure subscription   No support for tape backup |  Files,   Folders,    Volumes,   VMs,    Applications,    Workloads |  Azure Backup vault,    Locally attached disk |
| Azure IaaS VM Backup |  Native backups for Windows/Linux   No specific agent installation required   Fabric-level backup with no backup infrastructure needed |  Back up VMs once-a-day   Restore VMs only at disk level   Cannot back up on-premises |  VMs,   All disks (using PowerShell) | Azure Backup vault1 |

## What are the deployment scenarios for each component?

| Component | Can be deployed in Azure? | Can be deployed on-premises? | Target storage supported |
| --- | --- | --- | --- |
| Azure Backup (MARS) agent | **Yes**  The Azure Backup agent can be deployed on any Windows Server VM that runs in Azure. | **Yes**  The Backup agent can be deployed on any Windows Server VM or physical machine.1 | Azure Backup vault |
| System Center DPM | **Yes**  Learn more about [how to protect workloads in Azure by using System Center DPM](https://docs.microsoft.com/en-us/azure/backup/backup-azure-dpm-introduction). | **Yes**  Learn more about [how to protect workloads and VMs in your datacenter](https://technet.microsoft.com/en-us/system-center-docs/dpm/data-protection-manager). | Locally attached disk,  Azure Backup vault,  tape (on-premises only) |
| Azure Backup Server | **Yes**  Learn more about [how to protect workloads in Azure by using Azure Backup Server](https://docs.microsoft.com/en-us/azure/backup/backup-azure-microsoft-azure-backup). | **Yes**  Learn more about [how to protect workloads in Azure by using Azure Backup Server](https://docs.microsoft.com/en-us/azure/backup/backup-azure-microsoft-azure-backup). | Locally attached disk,  Azure Backup vault |
| Azure IaaS VM Backup | **Yes**  Part of Azure fabric  Specialized for [backup of Azure infrastructure as a service (IaaS) virtual machines](https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-introduction). | **No**  Use System Center DPM to back up virtual machines in your datacenter. | Azure Backup vault |

## Which applications and workloads can be backed up?

The following table provides a matrix of the data and workloads that can be protected using Azure Backup. The Azure Backup solution column has links to the deployment documentation for that solution. Each Azure Backup component can be deployed in a Classic (Service Manager-deployment) or Resource Manager-deployment model environment.

##### **Important**

Before you work with Azure resources, get familiar with the deployment models: [Resource Manager, and classic](https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-deployment-model).

| Data or Workload | Source environment | Azure Backup solution |
| --- | --- | --- |
| Files and folders | Windows Server | [Azure Backup agent](https://docs.microsoft.com/en-us/azure/backup/backup-configure-vault),1  [System Center DPM](https://docs.microsoft.com/en-us/azure/backup/backup-azure-dpm-introduction) (+ the Azure Backup agent),  [Azure Backup Server](https://docs.microsoft.com/en-us/azure/backup/backup-azure-microsoft-azure-backup) (includes the Azure Backup agent) |
| Files and folders | Windows computer | [Azure Backup agent](https://docs.microsoft.com/en-us/azure/backup/backup-configure-vault),  [System Center DPM](https://docs.microsoft.com/en-us/azure/backup/backup-azure-dpm-introduction) (+ the Azure Backup agent),  [Azure Backup Server](https://docs.microsoft.com/en-us/azure/backup/backup-azure-microsoft-azure-backup) (includes the Azure Backup agent) |
| Hyper-V virtual machine (Windows) | Windows Server | [System Center DPM](https://docs.microsoft.com/en-us/azure/backup/backup-azure-backup-sql) (+ the Azure Backup agent),  [Azure Backup Server](https://docs.microsoft.com/en-us/azure/backup/backup-azure-microsoft-azure-backup) (includes the Azure Backup agent) |
| Hyper-V virtual machine (Linux) | Windows Server | [System Center DPM](https://docs.microsoft.com/en-us/azure/backup/backup-azure-backup-sql) (+ the Azure Backup agent),  [Azure Backup Server](https://docs.microsoft.com/en-us/azure/backup/backup-azure-microsoft-azure-backup) (includes the Azure Backup agent) |
| Microsoft SQL Server | Windows Server | [System Center DPM](https://docs.microsoft.com/en-us/azure/backup/backup-azure-backup-sql) (+ the Azure Backup agent),  [Azure Backup Server](https://docs.microsoft.com/en-us/azure/backup/backup-azure-microsoft-azure-backup) (includes the Azure Backup agent) |
| Microsoft SharePoint | Windows Server | [System Center DPM](https://docs.microsoft.com/en-us/azure/backup/backup-azure-backup-sql) (+ the Azure Backup agent),  [Azure Backup Server](https://docs.microsoft.com/en-us/azure/backup/backup-azure-microsoft-azure-backup) (includes the Azure Backup agent) |
| Microsoft Exchange | Windows Server | [System Center DPM](https://docs.microsoft.com/en-us/azure/backup/backup-azure-backup-sql) (+ the Azure Backup agent),  [Azure Backup Server](https://docs.microsoft.com/en-us/azure/backup/backup-azure-microsoft-azure-backup) (includes the Azure Backup agent) |
| Azure IaaS VMs (Windows) | running in Azure | [Azure Backup (VM extension)](https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-introduction) |
| Azure IaaS VMs (Linux) | running in Azure | [Azure Backup (VM extension)](https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-introduction) |

## Linux support

The following table shows the Azure Backup components that have support for Linux.

| Component | Linux (Azure endorsed) Support |
| --- | --- |
| Azure Backup (MARS) agent | No (Only Windows based agent) |
| System Center DPM | File-consistent backup on Hyper-V only (not available for Azure VM) |
| Azure Backup Server | File-consistent backup on Hyper-V only (not available for Azure VM) |
| Azure IaaS VM Backup | Yes (application consistent backup using [pre-script and post-script framework](https://docs.microsoft.com/azure/backup/backup-azure-linux-app-consistent)) |

## Using Premium Storage VMs with Azure Backup

Azure Backup protects Premium Storage VMs. Azure Premium Storage is solid-state drive (SSD)-based storage designed to support I/O-intensive workloads. Premium Storage is attractive for virtual machine (VM) workloads. For more information about Premium Storage, see the article, [Premium Storage: High-Performance Storage for Azure Virtual Machine Workloads](https://docs.microsoft.com/en-us/azure/storage/storage-premium-storage).

### Back up Premium Storage VMs

While backing up Premium Storage VMs, the Backup service creates a temporary staging location, named "AzureBackup-", in the Premium Storage account. The staging location is equal to the size of the recovery point snapshot. Be sure there is free space in the storage account to accommodate the temporary staging location. For more information, see the article, [premium storage limitations](https://docs.microsoft.com/en-us/azure/storage/storage-premium-storage#premium-storage-scalability-and-performance-targets). Once the backup job finishes, the staging location is deleted. The price of storage used for the staging location is consistent with all [Premium storage pricing](https://docs.microsoft.com/en-us/azure/storage/storage-premium-storage#pricing-and-billing).

##### **Note**

Do not modify or edit the staging location.

### Restore Premium Storage VMs

Premium Storage VMs can be restored to either Premium Storage or to normal storage. Restoring a Premium Storage VM recovery point back to Premium Storage is the typical process of restoration. However, it can be cost effective to restore a Premium Storage VM recovery point to standard storage. This type of restoration can be used if you need a subset of files from the VM.

## Using managed disk VMs with Azure Backup

Azure Backup protects managed disk VMs. Managed disks free you from managing storage accounts of virtual machines and greatly simplify VM provisioning.

### Back up managed disk VMs

Backing up VMs on managed disks is no different than backing up Resource Manager VMs. In the Azure portal, you can configure the backup job directly from the Virtual Machine view or from the Recovery Services vault view. You can back up VMs on managed disks through RestorePoint collections built on top of managed disks. Azure Backup currently doesn't support backing up managed disk VMs encrypted using Azure Disk encryption(ADE).

### Restore managed disk VMs

Azure Backup allows you to restore a complete VM with managed disks or restore managed disks to a Resource Manager storage account. Azure manages the managed disks during the restore process. You (the customer) manage the storage account created as part of the restore process.

## What are the features of each Backup component?

The following sections provide tables that summarize the availability or support of various features in each Azure Backup component. See the information following each table for additional support or details.

### Storage

| Feature | Azure Backup agent | System Center DPM | Azure Backup Server | Azure IaaS VM Backup |
| --- | --- | --- | --- | --- |
| Azure Backup vault | Yes | Yes | Yes | Yes |
| Disk storage |  | Yes | Yes |  |
| Tape storage |  | Yes |  |  |
| Compression  (in Backup vault) | Yes | Yes | Yes |  |
| Incremental backup | Yes | Yes | Yes | Yes |
| Disk deduplication |  | Partially | Partially |  |

table key

The Backup vault is the preferred storage target across all components. System Center DPM and Azure Backup Server also provide the option to have a local disk copy. However, only System Center DPM provides the option to write data to a tape storage device.

#### **Compression**

Backups are compressed to reduce the required storage space. The only component that does not use compression is the VM extension. The VM extension copies all backup data from your storage account to the Backup vault in the same region. No compression is used when transferring the data. Transferring the data without compression slightly inflates the storage used. However, storing the data without compression allows for faster restoration, should you need that recovery point.

#### **Disk Deduplication**

You can take advantage of deduplication when you deploy System Center DPM or Azure Backup Server [on a Hyper-V virtual machine](http://blogs.technet.com/b/dpm/archive/2015/01/06/deduplication-of-dpm-storage-reduce-dpm-storage-consumption.aspx). Windows Server performs data deduplication (at the host level) on virtual hard disks (VHDs) that are attached to the virtual machine as backup storage.

##### **Note**

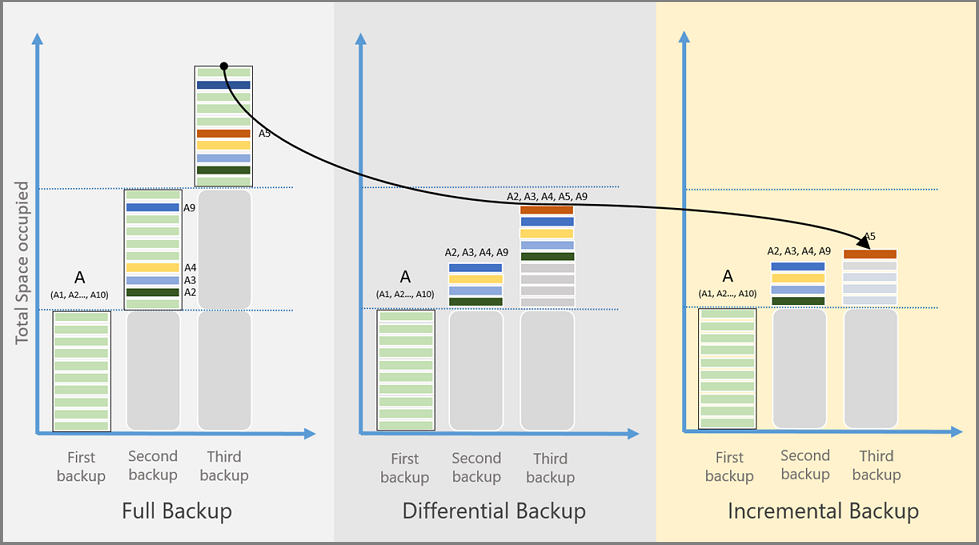
Deduplication is not available in Azure for any Backup component. When System Center DPM and Backup Server are deployed in Azure, the storage disks attached to the VM cannot be deduplicated.

### Incremental backup explained

Every Azure Backup component supports incremental backup regardless of the target storage (disk, tape, backup vault). Incremental backup ensures that backups are storage and time efficient, by transferring only those changes made since the last backup.

#### **Comparing Full, Differential and Incremental backup**

Storage consumption, recovery time objective (RTO), and network consumption varies for each type of backup method. To keep the backup total cost of ownership (TCO) down, you need to understand how to choose the best backup solution. The following image compares Full Backup, Differential Backup, and Incremental Backup. In the image, data source A is composed of 10 storage blocks A1-A10, which are backed up monthly. Blocks A2, A3, A4, and A9 change in the first month, and block A5 changes in the next month.



With **Full Backup**, each backup copy contains the entire data source. Full backup consumes a large amount of network bandwidth and storage, each time a backup copy is transferred.

**Differential backup** stores only the blocks that changed since the initial full backup, which results in a smaller amount of network and storage consumption. Differential backups don't retain redundant copies of unchanged data. However, because the data blocks that remain unchanged between subsequent backups are transferred and stored, differential backups are inefficient. In the second month, changed blocks A2, A3, A4, and A9 are backed up. In the third month, these same blocks are backed up again, along with changed block A5. The changed blocks continue to be backed up until the next full backup happens.

**Incremental Backup** achieves high storage and network efficiency by storing only the blocks of data that changed since the previous backup. With incremental backup, there is no need to take regular full backups. In the example, after the full backup is taken for the first month, changed blocks A2, A3, A4, and A9 are marked as changed and transferred for the second month. In the third month, only changed block A5 is marked and transferred. Moving less data saves storage and network resources, which decreases TCO.

### Security

| Feature | Azure Backup agent | System Center DPM | Azure Backup Server | Azure IaaS VM Backup |
| --- | --- | --- | --- | --- |
| Network security (to Azure) | Yes | Yes | Yes | Partially |
| Data security (in Azure) | Yes | Yes | Yes | Partially |

table key

#### **Network security**

All backup traffic from your servers to the Backup vault is encrypted using Advanced Encryption Standard 256. The backup data is sent over a secure HTTPS link. The backup data is also stored in the Backup vault in encrypted form. Only you, the Azure customer, have the passphrase to unlock this data. Microsoft cannot decrypt the backup data at any point.

##### **Warning**

Once you establish the Backup vault, only you have access to the encryption key. Microsoft never maintains a copy of your encryption key, and does not have access to the key. If the key is misplaced, Microsoft cannot recover the backup data.

#### **Data security**

Backing up Azure VMs requires setting up encryption within the virtual machine. Use BitLocker on Windows virtual machines and **dm-crypt** on Linux virtual machines. Azure Backup does not automatically encrypt backup data that comes through this path.

### Network

| Feature | Azure Backup agent | System Center DPM | Azure Backup Server | Azure IaaS VM Backup |
| --- | --- | --- | --- | --- |
| Network compression  (to **backup server**) |  | Yes | Yes |  |
| Network compression  (to **backup vault**) | Yes | Yes | Yes |  |
| Network protocol  (to **backup server**) |  | TCP | TCP |  |
| Network protocol  (to **backup vault**) | HTTPS | HTTPS | HTTPS | HTTPS |

table key

The VM extension (on the IaaS VM) reads the data directly from the Azure storage account over the storage network, so it is not necessary to compress this traffic.

If you are backing up data to a System Center DPM or Azure Backup Server, compress data going from the primary server to the backup server. Compressing data before backing it up to DPM or Azure Backup Server, saves bandwidth.

#### **Network Throttling**

The Azure Backup agent offers network throttling, which allows you to control how network bandwidth is used during data transfer. Throttling can be helpful if you need to back up data during work hours but do not want the backup process to interfere with other internet traffic. Throttling for data transfer applies to back up and restore activities.

## Backup and retention

Azure Backup has a limit of 9999 recovery points, also known as backup copies or snapshots, per protected instance. A protected instance is a computer, server (physical or virtual), or workload configured to back up data to Azure. For more information, see the section, [What is a protected instance](https://docs.microsoft.com/en-us/azure/backup/backup-introduction-to-azure-backup#what-is-a-protected-instance). An instance is protected once a backup copy of data has been saved. The backup copy of data is the protection. If the source data was lost or became corrupt, the backup copy could restore the source data. The following table shows the maximum backup frequency for each component. Your backup policy configuration determines how quickly you consume the recovery points. For example, if you create a recovery point each day, then you can retain recovery points for 27 years before you run out. If you take a monthly recovery point, you can retain recovery points for 833 years before you run out. The Backup service does not set an expiration time limit on a recovery point.

|  | Azure Backup agent | System Center DPM | Azure Backup Server | Azure IaaS VM Backup |
| --- | --- | --- | --- | --- |
| Backup frequency (to Backup vault) | Three backups per day | Two backups per day | Two backups per day | One backup per day |
| Backup frequency (to disk) | Not applicable |  Every 15 minutes for SQL Server   Every hour for other workloads |  Every 15 minutes for SQL Server   Every hour for other workloads | Not applicable |
| Retention options | Daily, weekly, monthly, yearly | Daily, weekly, monthly, yearly | Daily, weekly, monthly, yearly | Daily, weekly, monthly, yearly |
| Maximum recovery points per protected instance | 9999 | 9999 | 9999 | 9999 |
| Maximum retention period | Depends on backup frequency | Depends on backup frequency | Depends on backup frequency | Depends on backup frequency |
| Recovery points on local disk | Not applicable |  64 for File Servers,   448 for Application Servers |  64 for File Servers,   448 for Application Servers | Not applicable |
| Recovery points on tape | Not applicable | Unlimited | Not applicable | Not applicable |

## What is a protected instance

A protected instance is a generic reference to a Windows computer, a server (physical or virtual), or SQL database that has been configured to back up to Azure. An instance is protected once you configure a backup policy for the computer, server, or database, and create a backup copy of the data. Subsequent copies of the backup data for that protected instance (which are called recovery points), increase the amount of storage consumed. You can create up to 9999 recovery points for a protected instance. If you delete a recovery point from storage, it does not count against the 9999 recovery point total. Some common examples of protected instances are virtual machines, application servers, databases, and personal computers running the Windows operating system. For example:

* A virtual machine running the Hyper-V or Azure IaaS hypervisor fabric. The guest operating systems for the virtual machine can be Windows Server or Linux.
* An application server: The application server can be a physical or virtual machine running Windows Server and workloads with data that needs to be backed up. Common workloads are Microsoft SQL Server, Microsoft Exchange server, Microsoft SharePoint server, and the File Server role on Windows Server. To back up these workloads you need System Center Data Protection Manager (DPM) or Azure Backup Server.
* A personal computer, workstation, or laptop running the Windows operating system.

## What is the vault credential file?

The vault credentials file is a certificate generated by the portal for each Backup vault. The portal then uploads the public key to the Access Control Service (ACS). The private key is provided to you when downloading the credentials. Use it to register the computers you protect. The private key is what allows you to authenticate the servers or computers to send backup data to a particular Backup vault.1

You only use the vault credential to register the servers or computers. However, take care with the vault credentials, if it is lost or obtained by others, the vault credentials can be used to register other machines against the same vault. Since the backup data is encrypted using a passphrase, that only you can access, existing backup data cannot be compromised. Vault credentials expire after 48 hours. While you can download the Backup vault's vault credentials as often as you like, only the latest credentials can be used for registration.

## How does Azure Backup differ from Azure Site Recovery?

Azure Backup and Azure Site Recovery are related in that both services back up data and can restore that data. However, these services have different value propositions.

Azure Backup protects data on-premises and in the cloud. Azure Site Recovery coordinates virtual-machine and physical-server replication, failover, and failback. Both services are important because your disaster recovery solution needs to keep your data safe and recoverable (Backup) and keep your workloads available (Site Recovery) when outages occur.

The following concepts can help you make important decisions around backup and disaster recovery.

| Concept | Details | Backup | Disaster recovery (DR) |
| --- | --- | --- | --- |
| Recovery point objective (RPO) | The amount of acceptable data loss if a recovery needs to be done. | Backup solutions have wide variability in their acceptable RPO. Virtual machine backups usually have an RPO of one day, while database backups have RPOs as low as 15 minutes. | Disaster recovery solutions have low RPOs. The DR copy can be behind by a few seconds or a few minutes. |
| Recovery time objective (RTO) | The amount of time that it takes to complete a recovery or restore. | Because of the larger RPO, the amount of data that a backup solution needs to process is typically much higher, which leads to longer RTOs. For example, it can take days to restore data from tapes, depending on the time it takes to transport the tape from an off-site location. | Disaster recovery solutions have smaller RTOs because they are more in sync with the source. Fewer changes need to be processed. |
| Retention | How long data needs to be stored | For scenarios that require operational recovery (data corruption, inadvertent file deletion, OS failure), backup data is typically retained for 30 days or less. From a compliance standpoint, data might need to be stored for months or even years. Backup data is ideally suited for archiving in such cases. | Disaster recovery needs only operational recovery data, which typically takes a few hours or up to a day. Because of the fine-grained data capture used in DR solutions, using DR data for long-term retention is not recommended. |

## Next steps

Use one of the following tutorials for detailed, step-by-step, instructions for protecting data on Windows Server, or protecting a virtual machine (VM) in Azure:

* [Back up Files and Folders](https://docs.microsoft.com/en-us/azure/backup/backup-try-azure-backup-in-10-mins)
* [Backup Azure Virtual Machines](https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-first-look-arm)

For details about protecting other workloads, try one of these articles:

* [Back up your Windows Server](https://docs.microsoft.com/en-us/azure/backup/backup-configure-vault)
* [Back up application workloads](https://docs.microsoft.com/en-us/azure/backup/backup-azure-microsoft-azure-backup)
* [Backup Azure IaaS VMs](https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-prepare)