# AZ-104T00A – Administer Data Protection

After Kubernetes topic, today we are going to cover protection in Azure. It means Backup and replication.

## Configure File and Folder Backups

Azure Backup, as you might expect, is Microsoft’s cloud-based backup solution that requires no infrastructure to implement. Azure Backup allows you to perform one-off backups and scheduled backups through the use of backup policies. You can use Azure Backup to protect many different workloads, including Azure VMs, Azure Managed Disks, SQL Server in Azure VMs, and SAP HANA databases in Azure VMs. You can also use Azure Backup to protect Azure Files Shares, Azure Blobs, and on-prem files, folders, and system state. Because it’s a zero-infrastructure backup solution, Azure Backup requires no capital expenditures. Its single pane of glass streamlines backups by allowing you to discover, govern, monitor, and manage backups right from the backup portal. Over the next few lessons, we’ll take a look at some of the key aspects of the Azure Backup offering.

Describe Azure Backup Benefits

When you're thinking about backup and recovery, there are number of outcomes that come to mind. They include things like recovering files and folders, restoring a single or multiple virtual machines, this could be a physical server failure or a full OS corruption, recovering a site‑wide disaster, such as a datacenter fire or an Azure region going down. Along with these outcomes, you need to decide what tolerance your business has for data recovery. Do you need to recover to the minute or just last night? Do you have to have backups going back years for compliance or just a few quarters? This is referred to as the recovery point objective, RPO, or what point do you need to recover from? How quickly your application needs to be back in service is important as well. This is the recovery time objective, or RTO. This is the target for when services need to be back up and running. How you plan for these is referred to as business continuity and disaster recovery planning, or BCDR. Having a good plan is critical for all organizations. While we won't go into how our organization decides its particular needs in a BCDR plan, you'll learn how to use the tools in Azure to implement a BCDR plan for your organization. Azure Backup offers different benefits like:

|  |  |
| --- | --- |
| **Offload on-premises backup** | Azure Backup offers a simple solution for backing up your on-premises resources to the cloud. Get short and long-term backup without the need to deploy complex on-premises backup solutions. |
| **Back up Azure IaaS VMs** | Azure Backup provides independent and isolated backups to guard against accidental destruction of original data. Backups are stored in an Azure Recovery Services vault with built-in management of recovery points. Configuration and scalability are simple, backups are optimized, and you can easily restore as needed. |
| **Get unlimited data transfer** | Azure Backup doesn't limit the amount of inbound or outbound data you transfer, or charge for the data that's transferred. Outbound data refers to data transferred from a Recovery Services vault during a restore operation. If you perform an offline initial backup by using the Azure Import/Export service to import large amounts of data, there's a cost associated with inbound data. |
| **Keep data secure** | Data encryption allows for secure transmission and storage of your data in the public cloud. You store the encryption passphrase locally, and it's never transmitted or stored in Azure. If it's necessary to restore any of the data, only you have encryption passphrase, or key. |
| **Get app-consistent backups** | An application-consistent backup means a recovery point has all required data to restore the backup copy. Azure Backup provides application-consistent backups, which ensure extra fixes aren't required to restore the data. Restoring application-consistent data reduces the restoration time, allowing you to quickly return to a running state. |
| **Retain short and long-term data** | You can use Azure Recovery Services vaults for short-term and long-term data retention. Azure doesn't limit the length of time data can remain in a Recovery Services vault. You can keep it for as long as you like. Azure Backup has a limit of 9,999 recovery points per protected instance. |
| **Automatic storage management** | Hybrid environments often require heterogeneous storage with some on-premises instances and some instances in the cloud. With Azure Backup, there's no cost for implementing on-premises storage devices. Azure Backup automatically allocates and manages backup storage. The service uses a pay-as-you-use model, so you only pay for the storage you consume. |
| **Multiple storage options** | Azure Backup offers two types of replication to keep your storage and data highly available.   Locally redundant storage (LRS) replicates your data three times (it creates three copies of your data) in a storage scale unit in a datacenter. All copies of the data exist within the same region. LRS is a low-cost option for protecting your data from local hardware failures.   Geo-redundant storage (GRS) is the default and recommended replication option. 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's a regional outage. |

Implement Backup center for Azure Backup

Backup center for Azure Backup provides a single unified management experience in Azure. Enterprises can govern, monitor, operate, and analyze their backups at scale. The Backup center interface is consistent with Azure's native management experiences. Azure Backup Center is designed to be a single pane of glass where organizations can manage their backups at scale. It’s designed in a way that makes it especially useful in large and distributed Azure environments. The Backup Center allows you to manage backups for many different workload types, vaults, subscriptions, regions, and even Azure Lighthouse tenants. Because of its Datasource-centric design, Backup center can provide views and filters that focus on data sources that are being backed up. For example, if you make use of resource tags in your Azure environment, you can filter your views in Backup center so that you see the backup information for only the resources that are tagged with a specific resource tag. This helps filter out “noise”. Now, I do need to mention here that the Backup Center only supports certain resource backups. The resource backups supported include Azure VM backups, SQL in Azure VM backups, SAP HANA in Azure VM backups, Azure Files backups, Azure Blobs backups, Azure Managed Disks backups, and Azure Database for PostgreSQL Server backups.

**DEMO – Show Backup Center in Azure Portal**

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 tenants. Backup center provides views and filters that are centered on the datasources that you're backing up like virtual machines and databases. A resource owner or backup administrator can manage backup items across different vaults. The admin can also filter views by datasource-specific properties, including datasource subscription, resource group, and tags. Backup center provides native integrations to existing Azure services that enable management at scale. Backup center uses the Azure Policy experience to help you govern your backups. It uses the Azure Workbooks of Azure Monitor and Azure Monitor Logs (Log Analytics) to help you view detailed reports on backups. You don't need to learn new principles to use the varied features that Backup center offers. You can also discover community resources from the Backup center.

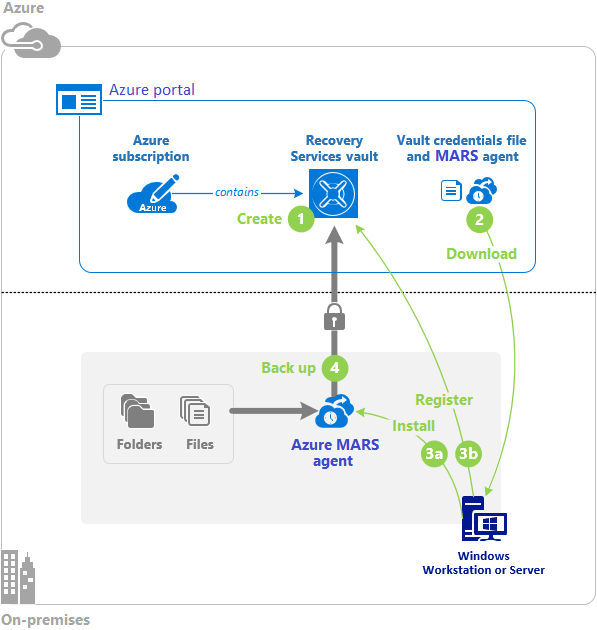
Setup Recovery Services Vault Backup Options – Files

At the center of Azure Backup and recovery is the Recovery Services vault. A Recovery Services vault is a storage object in Azure designed for backup and recovery of Azure Resources. Azure Virtual Machines and Azure Files are two of the common services that we'll find. RSVs provide a central place for organizing and managing your backup continuity and disaster recovery strategy using Azure Backup and Azure Site Recovery. Backup, restore, site replication, and management tasks like reporting are handled through the RSV. While the focus of this course and the exam is on Azure Virtual Machines and Azure file shares, you should know that RSVs can serve as on‑prem workloads, along with workloads in AWS. When you're creating an RSV it's important to remember a Recovery Services vault can only back up Azure data that's in the same region as the RSV. So, if you have resources distributed across multiple regions, you'll need multiple resource vaults. When creating an RSV for Azure Site Recovery, it needs to be in a separate region than the source data. That's because the RSV will hold replicated data and is designed for when the region goes down. This is an important distinction from Azure Backup. So basically, rhe **Recovery Services vault** is a storage entity in Azure that stores data. Recovery Services vaults make it easy to organize your backup data, while minimizing management overhead.

Demonstration – Backup Azure File Shares

Follow this guide <https://learn.microsoft.com/en-us/azure/backup/backup-azure-files?tabs=backup-center>

Configure On-Premises File and Folder Backup

The following diagram shows the high-level steps to use the MARS agent for Azure Backup

1 – The first step is to create a Recovery Services vault for your backups. The vault must be created within your Azure subscription

2 – On the Backup center dashboard, the Recovery Services vault page provides a link to download the MARS agent (Recovery Services Agent). To complete the MARS agent installation, you also need to download the vault credentials file.

3 – The MARS agent installer provides a wizard to configure the installation location, proxy server, and passphrase information. The downloaded credentials file is used to register the agent. The MARS agent is installed on your local machine.

4 - Now you're ready to use the MARS agent to create a backup policy. You can specify when to do the backup, what data to back up, how long to retain the backup items, and other settings such as network throttling.

Demonstration – Backup Files and Folders

**Create a Recovery Services vault**

1. In the Azure portal, type Recovery Services and click **Recovery Services vaults**.

2. Click **Add**.

3. Provide a **Name, Subscription, Resource group, and Location**.

4. Click **Create**. It can take several minutes for the Recovery Services vault to be created. Monitor the status notifications in the upper right-hand area of the portal. Once your vault is created, it appears in the list of Recovery Services vaults.

5. If after several minutes you don't observe your vault, click **Refresh**.

**Configure the vault**

1. For your recovery services vault, click **Backup**.

2. From the **Where is your workload running?** drop-down menu, select **On-premises**

3. From the **What do you want to backup?** menu, select **Files and folders**. Notice your other choices.

4. Click **Prepare infrastructure**.

5. Click **Download Agent for Windows Server or Windows Client**. A pop-up menu prompts you to run or **save** MARSAgentInstaller.exe.

6. By default, the MARSagentinstaller.exe file is saved to your **Downloads** folder. When the installer completes, a pop-up asking if you want to run the installer, or open the folder. You **don't need** to install the agent yet. You can install the agent after you have downloaded the vault credentials.

7. Return to your recovery services vault, check the box **Already downloaded or using the latest recovery services agent.**

8. Click **Download.** After the vault credentials finish downloading, a pop-up asking if you want to open or **save** the credentials. Click **Save**. If you accidentally click **Open**, let the dialog that attempts to open the vault credentials, fail. You cannot open the vault credentials. Proceed to the next step. The vault credentials are in the **Downloads** folder.

**Install and register the agent**

1. Locate and double-click the **MARSagentinstaller.exe** from the **Downloads** folder (or other saved location). The installer provides a series of messages as it extracts, installs, and registers the Recovery Services agent.

* 1. 2. To complete the wizard, you need to: o Choose a location for the installation and cache folder.
* Provide your proxy server info if you use a proxy server to connect to the internet.
* Provide your user name and password details if you use an authenticated proxy.
* If prompted, install any missing software.
* Provide the downloaded vault credentials
* Enter and save the encryption passphrase in a secure location.
  1. 3. Wait for the server registration to complete. This could take a couple of minutes.
  2. 4. The agent is now installed and your machine is registered to the vault. You're ready to configure and schedule your backup.

**Create the backup policy**

1. Open the **Microsoft Azure Recovery Services** agent. You can find it by searching your machine for Microsoft Azure Recovery Services.

2. If this is the first time you are using the agent there will be a **Warning** to create a backup policy. The backup policy is the schedule when recovery points are taken, and the length of time the recovery points are retained.

* + 3. Click **Schedule Backup** to launch the Schedule Backup Wizard.
* Read the **Getting Started** page.
* **Add items** to include files and folders that you want to protect. Select just a few sample files. Notice you can exclude files from the backup.
* Specify the **backup schedule**. You can schedule daily (at a maximum rate of three times per day) or weekly backups.
* Select your **retention policy** settings. The retention policy specifies the duration for which the backup is stored. Rather than just specifying a “flat policy” for all backup points, you can specify different retention policies based on when the backup occurs. You can modify the daily, weekly, monthly, and yearly retention policies to meet your needs.
* Choose your **initial backup type page** as **Automatically**. Notice there is a choice for offline backup.
* **Confirm** your choices and **Finish** the wizard.

**Backup files and folders**

1. Click **Back Up Now** to complete the initial sending over the network.

2. In the wizard, confirm your settings, and then click **Back Up**.

3. You may **Close** the wizard. It will continue to run in the background.

4. The **Status** of your backup will show on the first page of the agent.

5. You can **View Details** for more information.

**Explore the recover settings**

1. Click **Recover data**.

2. Walkthrough the wizard making selections based on your backup settings.

3. Notice your choices to restore from the current server or another server.

4. Notice you can backup individual files and folders or an entire volume.

5. Select a volume and **Mount** the drive. This can take a couple of minutes.

6. Verify the mounted volume can be accessed in **File Explorer** and that your backup files are available.

7. **Unmount** the drive.

**Explore the backup properties**

1. Click **Change Properties**.

2. Explore the different tabs.

3. On the **Encryption** tab you can change the passphrase.

4. On the **Proxy Configuration** tab you can add proxy information.

5. On the **Throttling** tab you can enable internet bandwidth usage throttling. Throttling controls how network bandwidth is used during data transfer. This control 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 applies to back up and restore activities.

**Delete your backup schedule**

1. Click **Schedule Backup**.

2. In the wizard, select **Stop using this backup schedule and delete all the stored backups.**

3. Verify your choices and click **Finish**.

4. You will be prompted for a recovery services vault security pin.

5. In the Azure portal locate your recovery services vault.

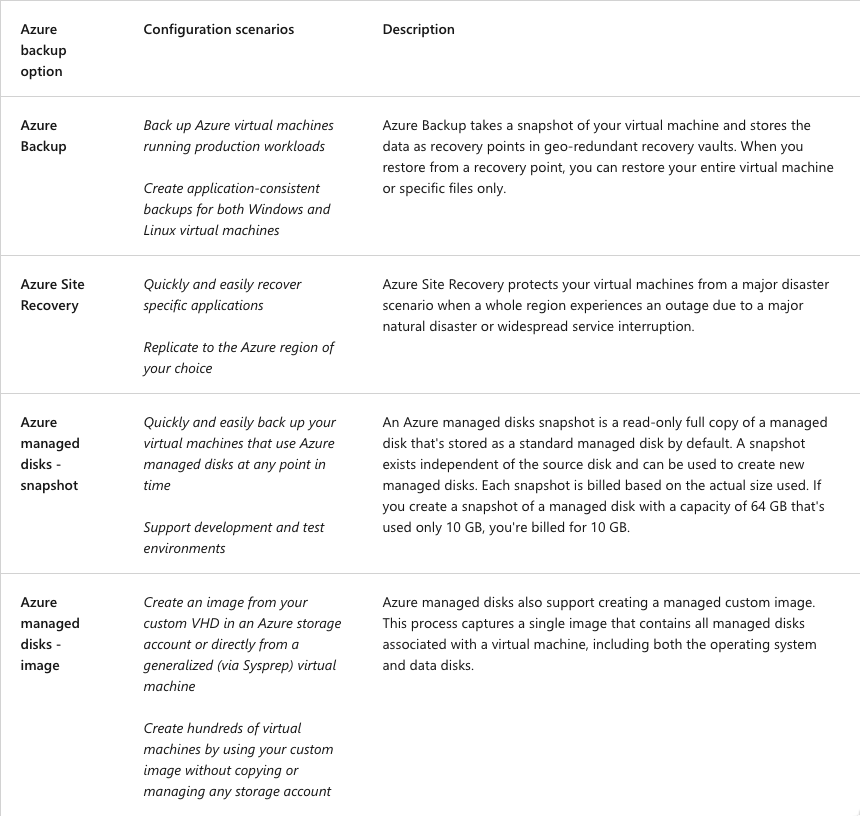
6. Select **Properties** and then Security PIN **Generate**.

7. Copy the PIN into the Backup agent to finish deleting the schedule.

## Configure Virtual Machine Backups

Azure Backup provides independent and isolated backups to guard against unintended destruction of the data on your virtual machines. Administrators can implement Azure services to support their backup requirements, including the Microsoft Azure Recovery Services (MARS) agent for Azure Backup, the Microsoft Azure Backup Server (MABS), Azure managed disks snapshots, and Azure Site Recovery.

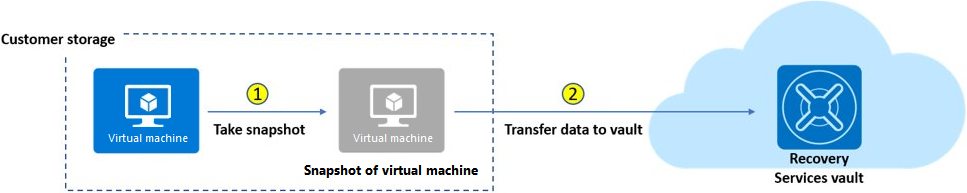
Protect Virtual Machine Data

We have 4 options for backing up our virtual machines. Azure Backup, Azure Site Recovery and Azure managed disks snapshots and images.

It’s important to understand the differences and benefits of creating an image and a snapshot backup of an Azure managed disk. **Consider images**. With Azure managed disks, you can take an image of a generalized virtual machine that's been deallocated. The image includes all of the disks attached to the virtual machine. You can use the image to create a virtual machine that includes all of the disks. **Consider snapshots**. A snapshot is a copy of a disk at the point in time the snapshot is taken. The snapshot applies to one disk only, and doesn't have awareness of any disk other than the one it contains. Snapshot backups are problematic for configurations that require the coordination of multiple disks, such as striping. In this case, the snapshots need to coordinate with each other, but this functionality isn't currently supported. **Consider operating disk backups.** If you have a virtual machine with only one disk (the operating system disk), you can take a snapshot or an image of the disk. You can create a virtual machine from either a snapshot or an image.

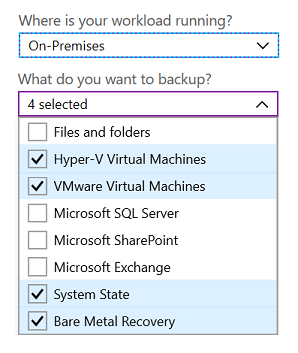
Create Virtual Machine Snapshots

An Azure Backup job creates a snapshot for your virtual machine in two phases: Phase 1: Take a snapshot of the virtual machine data. Phase 2: Transfer the snapshot to an Azure Recovery Service Vault.



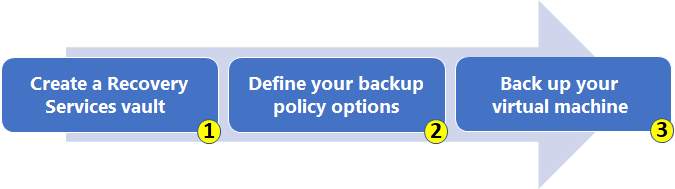
By default, Azure Backup keeps snapshots for two days to reduce backup and restore times. The local retention reduces the time required to transform and copy data back from an Azure Recovery Services vault. You can set the default snapshot retention value from one and five days. Incremental snapshots are stored as Azure page blobs (Azure Disks). Recovery points for a virtual machine snapshot are available only after both phases of the Azure Backup job are complete. Recovery points are listed for the virtual machine snapshot in the Azure portal and are labeled with a recovery point type. After a snapshot is first taken, the recovery points are identified with the **snapshot** recovery point type. After the snapshot is transferred to an Azure Recovery Services vault, the recovery point type changes to **snapshot and vault**.

Setup Recovery Services Vault Backup Options – VMs

As we said before, an Azure Recovery Services vault is a storage entity in Azure that houses data. The data is typically copies of data, or configuration information for virtual machines, workloads, servers, or workstations.

You can use Recovery Services vaults to organize your backup data and minimize your management overhead. In this slide you can see that a Recovery Services vault can be used to back up your on-premises virtual machines, such as Hyper-V, VMware, System State, and Bare Metal Recovery

Backup Virtual Machines



To use Azure Backup to protect your Azure virtual machines, you follow a simple three-step process: create a vault, define your backup options, and trigger the backup job.

1. The first step is to create an Azure Recovery Services vault for your virtual machine backups. The vault must be created within your Azure subscription, and in the region where you want to store the data. You also need to specify how you want your storage replicated, either geo-redundant (default) or locally redundant.

* **Geo-redundant** (GRS): (Default) Use GRS when Azure is your primary backup storage endpoint.
* **Locally redundant** (LRS): If Azure **isn't** your primary backup storage endpoint, use LRS to reduce your storage costs.

1. After you create your vault, you need to define your backup policy. The policy specifies when to take the data snapshots, and how long to keep the snapshots. Your virtual machine is protected by taking snapshots of your data at defined intervals. The snapshots produce recovery points that are stored in your Recovery Services vault. If it becomes necessary to repair or rebuild your virtual machine, you can restore your machine by using your saved recovery points. In your backup policy, you can specify to trigger a backup from one to five times per day.
2. The last step is to run the Azure Backup job process and create your backups. To run the backup job, the Azure Backup extension requires the Microsoft Azure Virtual Machine Agent to be present on your Azure virtual machine.

* If your virtual machine was created from the Azure gallery, the agent is installed by default on your machine.
* If your virtual machine was migrated from an on-premises data center, you need to manually install the agent on your machine.

Restore Virtual Machines

After you back up your virtual machine, the backup snapshots and recovery points are stored in your Recovery Services vault. You can recover your machine by accessing the snapshot, or restore data to a specific point-in-time by using recovery points.

Demonstration Virtual Machine Backups

Follow this guide <https://learn.microsoft.com/en-us/azure/backup/tutorial-backup-vm-at-scale>

Implement Azure Backup Server

Azure Backup Server is a standalone service that you install on a Windows Server operating system that stores the backed-up data in a Recovery Services Vault. Azure Backup Server inherits much of the workload backup functionality from Data Protection Manager (DPM). Though Azure Backup Server shares much of the same functionality as DPM, Azure Backup Server does not back up to tape, and it does not integrate with System Center. You should consider using Azure Backup server when you need to back up the following supported workloads: Windows Client, Windows Server, Linux Servers (running on Hyper-v or VMware), VMware VMs, Exchange, Sharepoint, SQL Server, System State and Bare Metal Recovery.



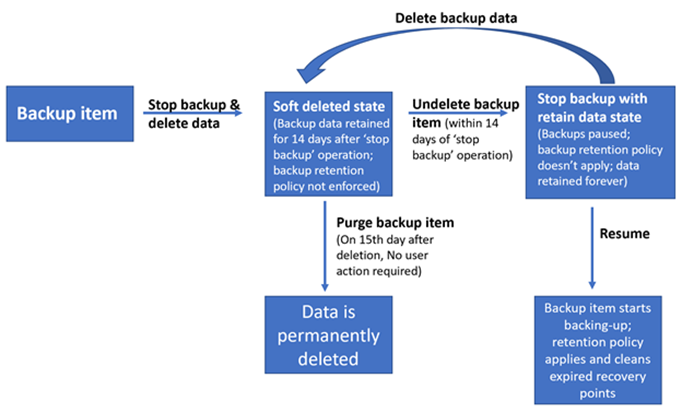
When you set up protection for a machine or application by using System Center DPM or MABS, you select to back up to the MABS or DPM local disk for short-term storage, and to Azure for online protection. You specify when to run the backup to the local DPM or MABS storage, and when to run the online backup to Azure. To protect your on-premises machines, the System Center DPM or MABS instance must be located on-premises. To protect your Azure virtual machines, the MABS instance must run as an Azure virtual machine and located in Azure. The System Center DPM / MABS protection agent must be installed on each machine you want to protect. The machines that you want to back up must be added to a [System Center DPM protection grou](https://learn.microsoft.com/en-us/system-center/dpm/create-dpm-protection-groups)p. When the backup triggers, the disk of the protected workload is backed up to the local MABS or DPM disks, according to the schedule you specified. The DPM and MABS disks are then backed up to the Recovery Services vault by the MARS agent running on the DPM or MABS instance. There are several advantages to choosing System Center DPM or MABS for your backup solution. **Consider optimized app-aware backups**. Back up your data to MABS or System Center DPM to enable app-aware backups that are optimized for common apps. Apps can include SQL Server, Exchange, and SharePoint. The optimization can be achieved for file/folder/volume backups, and machine-state backups. The machine-state backups can be bare-metal, or system-state. **Consider simplified backups for on-premises machines**. Implement System Center DPM or MABS implementation to avoid installing the Microsoft Azure Recovery Services (MARS) agent on each on-premises machine to back up. Your on-premises machines automatically run the System Center DPM (and MABS) **protection** agent. The MARS agent runs only on the MABS or DPM instance. **Consider flexibility and scheduling**. Configure System Center DPM or MABS to gain flexibility and more granular scheduling options for running your backups. **Consider consolidated management**. Manage backups for multiple machines by gathering them into protection groups in a single console. Grouping machines is useful when apps are tiered over multiple machines and you want to back them up at the same time.

Compare Backup Options

There are advantages and limits to using the different Azure backup components. In this section, we compare the Microsoft Azure Recovery Services (MARS) backup agent and Microsoft Azure Backup Server, which uses the System Center DPM protection agent. This slide summarizes features and restrictions and identifies what data is protected by the backup and where the backups are stored in the configuration.

Manage Soft Delete

Azure Storage now offers the soft delete option for Azure Blob objects. With this feature, you can more easily recover your data when it's erroneously modified or deleted by an application or other storage account user. Soft delete for virtual machines protects backups of your virtual machines from unintended deletion. Even after the backups are deleted, they're preserved in the soft-delete state for 14 more days. Soft delete only protects deleted backup data. If a virtual machine is deleted without a backup, the soft-delete feature won't preserve the data. All resources should be protected with Azure Backup to ensure full resilience.

**Stop backup job**. Before you can delete or retain backup data for your virtual machine, you must stop the active backup job. After you stop the backup job in the Azure portal, you can choose to delete or retain your backup data.

**Apply soft-delete state**. Prevent your virtual machine backup data from being permanently deleted by selecting **Delete backup data** followed by **Stop backup**. The soft-delete state is applied to your backup data, and the data is retained for 14 days. If you apply the state to a virtual machine, the machine is referred to as soft-deleted.

**View soft-delete data in the vault**. During the 14 day retention period, the Recovery Services vault shows your soft-deleted virtual machine with a red **soft-delete** icon.

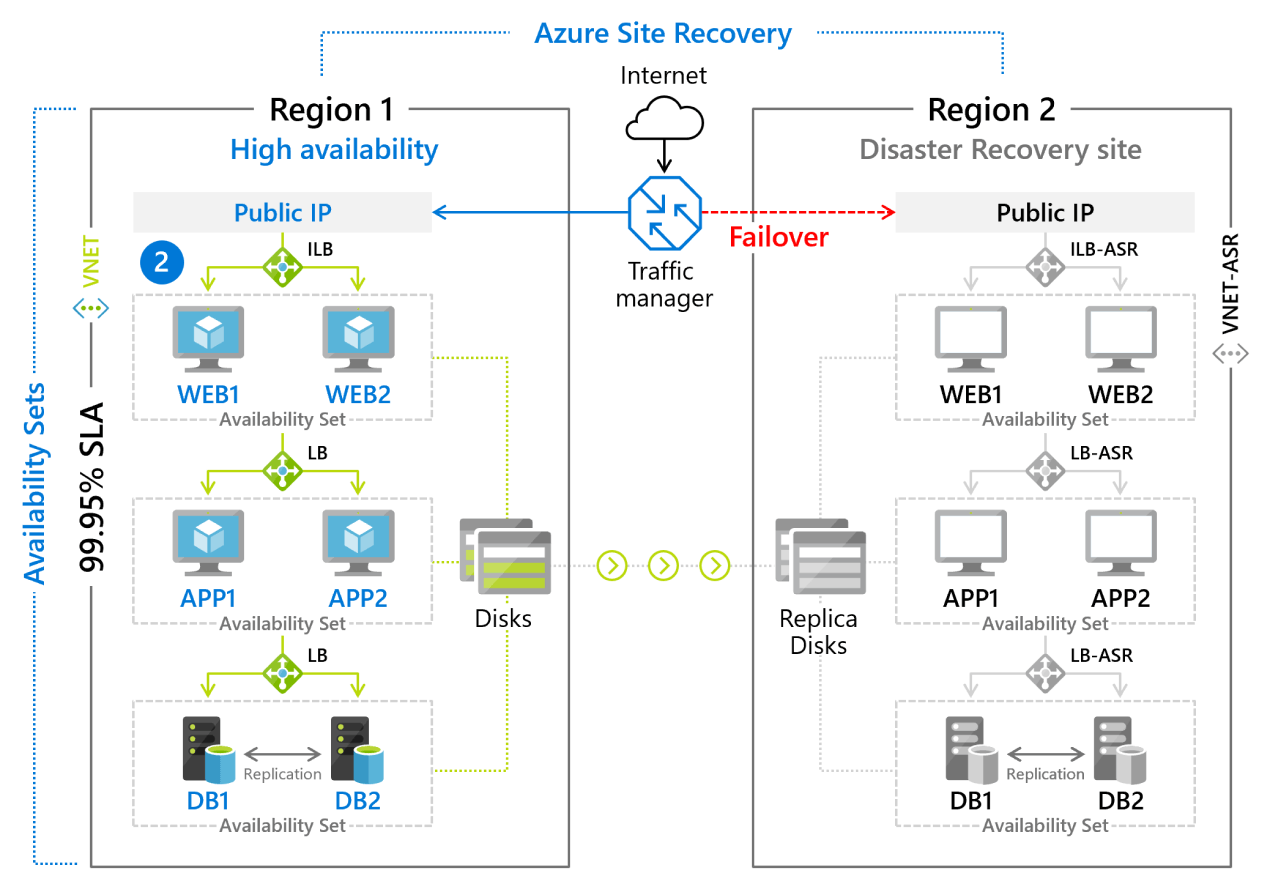
**Undelete backup items**. Before you can restore a soft-deleted virtual machine, you must undelete the backup data.

**Restore items**. After you undelete the backup item, you can restore your virtual machine by selecting **Restore virtual machine** from the chosen recovery point in the backup.

**Resume backups**. When the undelete process completes, the backup job status returns to **Stop backup with retain data**, and you can choose **Resume backup**. The resume operation retrieves the backup item in the active state according to the backup policy selected by the user. The policy defines the backup and retention schedules.

Implement Azure Site Recovery

Now that you have an understanding of the Recovery Services vault and Azure Backup, it's time to look at the other recovery tool in the vault, Azure Site Recovery. Site Recovery helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines from a primary site to a secondary location. When an outage occurs at the primary site, you fail over to the secondary location and access the apps and data from there. After the primary location is running again, you can fail back to it. When you're setting up ASR, you need to make sure to create the Recovery Services vault in any region other than the source region. So if your VMS are located in East US, West US is a good choice for your ASR vault. This is different than Azure Backup requirements. It's important to understand what makes up Azure Site Recovery, so let's take a look at its general topology.

When you enable replication for an azure VM within a Recovery Services vault, the following happens. The Site Recovery Mobility Services extension is automatically installed on the VM. The extension registers the VM with Site Recovery. Continuous replication begins for the VM. Disk rights are immediately transferred to the cached storage account in the source location. Site Recovery processes the data in the cache and sends it to the target storage account or to the replica managed disks. After the data is processed, crash‑consistent recovery points are generated every 5 minutes. App‑consistent recovery points are generated according to the settings specified in the replication policy when you set up ASR. When a failover occurs, the Recovery Services vault builds out the VMs using the replica disks, places them in the virtual network in the secondary region, and brings the VMs online. Depending on your network security and domain naming requirements, you may need to use a service like Traffic Manager to ensure custom domain name transfers automatically. Otherwise, these things can be done manually.