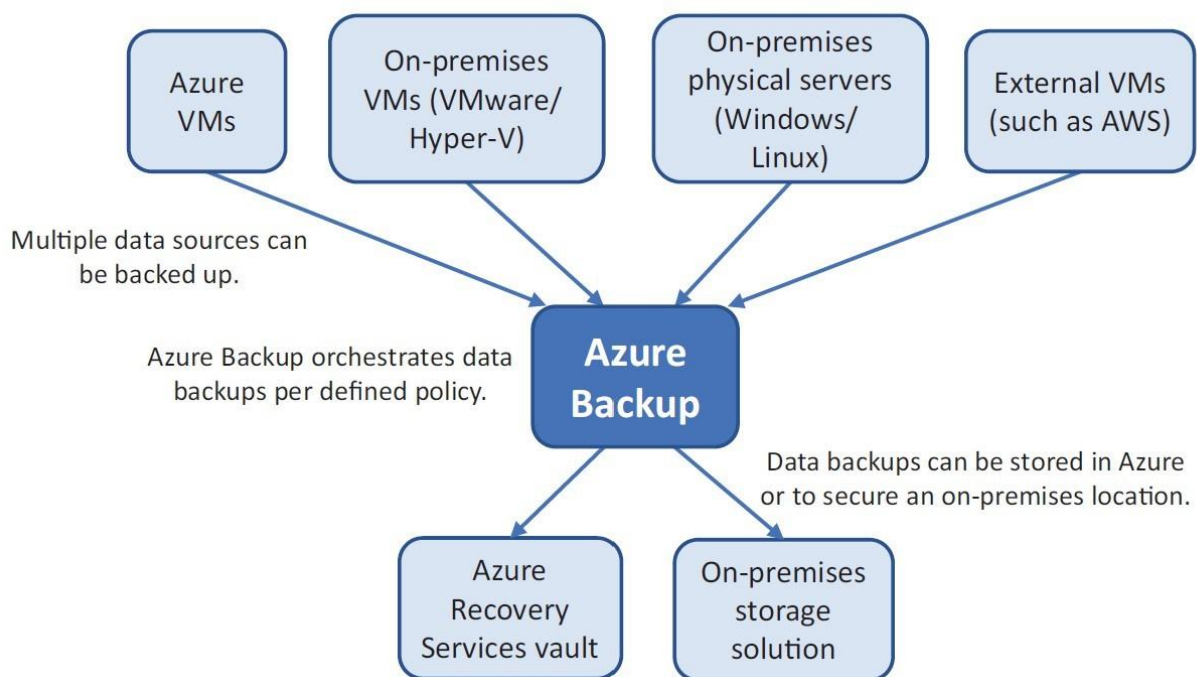


What is azure Backup?

The Azure Backup service backs up data to the Microsoft Azure cloud. You can back up on-premises machines and workloads, and Azure virtual machines (VMs).

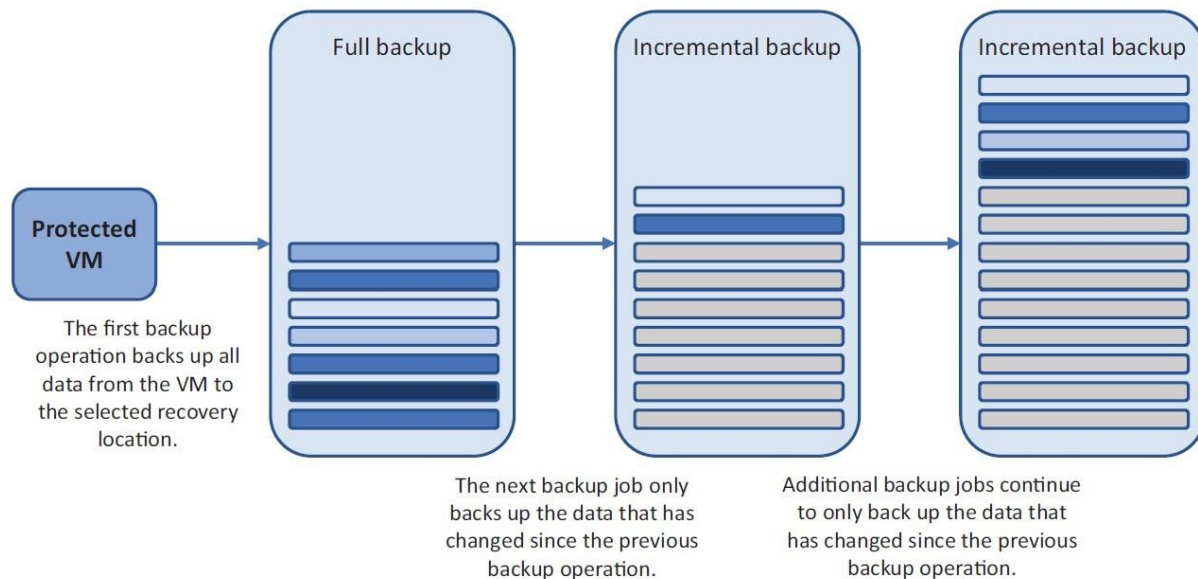
One of the cool things about Azure Backup is that it's both a service and a big bucket of storage for the actual backups. Azure Backup can protect VMs in Azure, on-premises VMs or physical servers, and even VMs in other providers such as Amazon Web Services (AWS). The data backups can be stored on your own on-premises storage arrays or within an Azure recovery vault. In my below, shows how the Azure Backup service can protect and orchestrate all of your backup needs.



At its core, Azure Backup manages backup schedules and data retention, and orchestrates the backup or restore jobs. To back up Azure VMs, there's no server component to install and no agent to manually install. All the backup and restore operations are built into the Azure platform. To back up on-premises VMs or physical servers, or VMs in other providers such as AWS, you install a small agent that enables secure communication back and forth with Azure. This secure communication ensures that your data is encrypted during transfer. For data stored in Azure, the backups are encrypted using an encryption key that you create and retain sole access to. Only you have access to those encrypted backups. You can also back up encrypted VMs, which we look at in the next chapter, to really make sure your data backups are safe. There's no charge for the network traffic flow to back up or restore data. You only pay for each protected instance, and then however much storage you consume in Azure. If you use an on-premises storage location, the cost to use Azure Backup is minimal, because there are no Azure Storage or network traffic costs.

Policies and retention

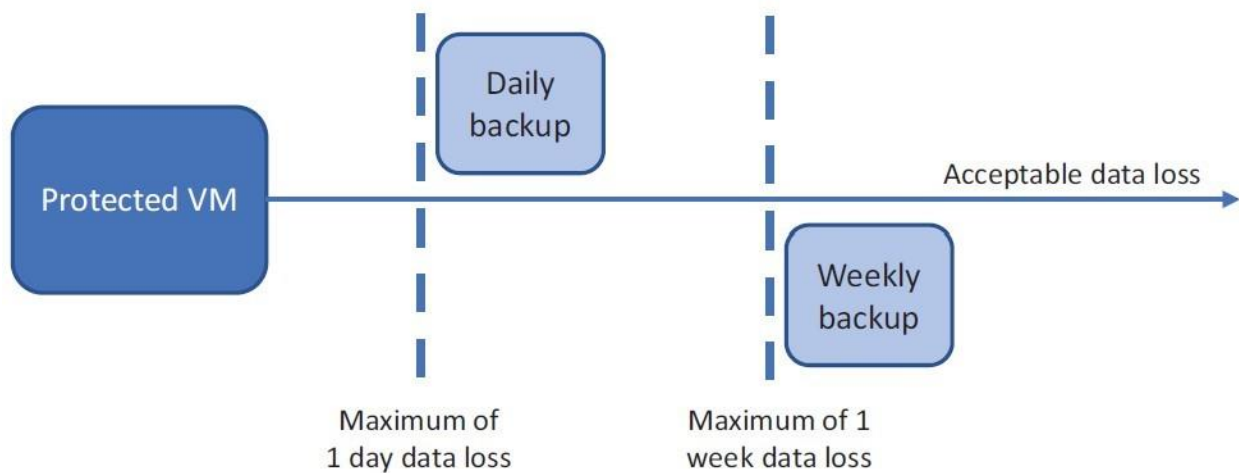
Azure Backup uses an incremental backup model. When you protect an instance, the first backup operation performs a full backup of the data. After that, each backup operation performs an incremental backup of the data. Each of these backups is called a recovery point. Incremental backups are a time-efficient approach that optimizes the storage and network bandwidth usage. Only data that has changed since the previous backup is securely transferred to the destination backup location. In my below details how incremental backups work.



With Azure Backup, you can store up to 9,999 recovery points for each instance that you protect. For some context, if you made a regular daily backup, you'd be set for over 27 years. And you could keep weekly backups for almost 200 years. I think that would cover most audit situations! You can choose to retain backups on a daily, weekly, monthly, or yearly basis, which is typically in line with most existing backup policies. To implement the optimal backup strategy for your workload, you need to understand and determine your acceptable recovery point objective (RPO) and recovery time objective (RTO).

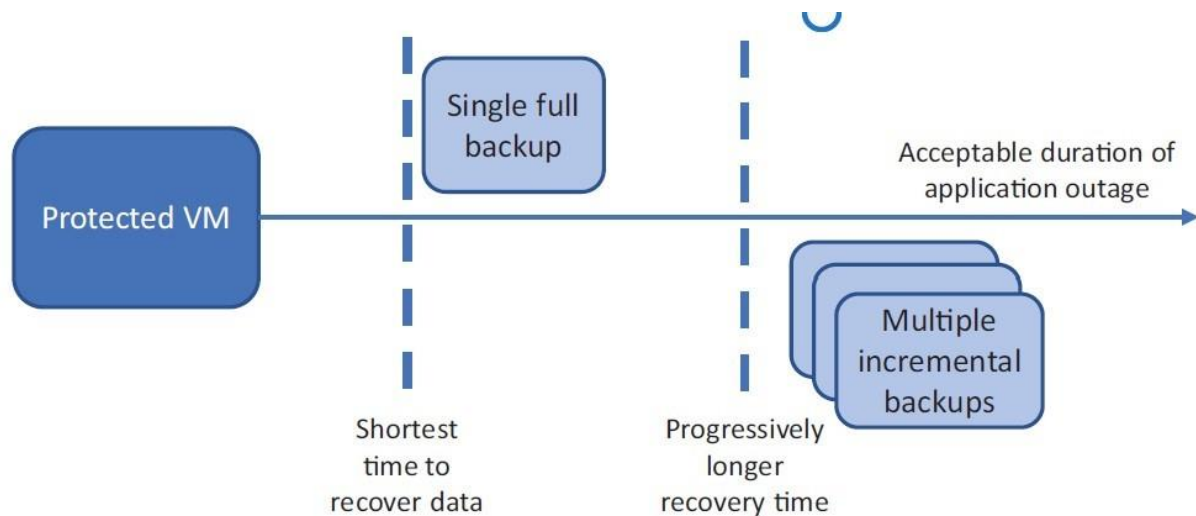
RECOVERY POINT OBJECTIVE

The RPO defines the point that your latest backup allows you to restore. By default, Azure Backup makes a daily backup. You then define retention policies as to how many days, weeks, months, or years you wish to keep these recovery points. Although the RPO is typically used to define the maximum amount of acceptable data loss, you should also consider how far back in time you may wish to go. Given Picture shows how the RPO defines the amount of acceptable data loss.



RECOVERY TIME OBJECTIVE

The RTO dictates how quickly you can restore your data. If you choose to back up Azure VMs and store the recovery points in an on-premises storage solution, it takes much longer to restore those backups than if they were housed directly in Azure Storage. The inverse would be true if you backed up on-premises VMs or physical servers to Azure Storage. Given Picture outlines the RTO.



Backup schedules

Try it now

All your Azure backups are stored in a Recovery Services vault. To create a vault and backup policy, complete the following steps.

1. Open the Azure portal, and select Create a Resource at upper left in the menu.
2. Search for and select Backup and Site Recovery (OMS), and then choose Create.
3. Provide a name, such as azuremol, and then choose Create New Resource Group. Enter a resource group name, such as azuremolchapter13.
4. Select a location, and then choose Create.
5. Select Resource Groups from the menu at left in the portal, and then choose the resource group you created.
6. Select your Recovery Services vault from the list of available resources, choose Backup Policies from the menu at left, and then select Add a Policy.
7. Select the Azure Virtual Machine policy type, and then provide a name for your new policy, such as molpolicy. By default, a backup is created each day. Select the most appropriate time zone from the drop-down menu. By default, Azure uses Universal Coordinated Time (UTC). If you wish, review and adjust the retention policies for daily, weekly, monthly, and yearly. The previous section on backup schedules detailed these retention values; these options typically vary as you create and apply backup policies to protect your VM instances.
8. When you're ready, select Create.

Create policy

* Policy name ⓘ

MOL-Policy ✓

Backup frequency

Daily

6:30 PM

(UTC) Coordinated Universal Time

Retention range

☒ Retention of daily backup point.

* At

For

6:30 PM

180 ✓

Day(s)

☒ Retention of weekly backup point.

* On

* At

For

Sunday

6:30 PM

104 ✓

Week(s)

☒ Retention of monthly backup point.

Week Based

Day Based

* On

* Day

* At

For

First

Sunday

6:30 PM

60

Month(s)

☒ Retention of yearly backup point.

Week Based

Day Based

* In

* On

* Day

* At

For

January

First

Sunday

6:30 PM

10 ✓

Year(s)

Create


To back up a VM with your defined policy, complete the following steps.

1. Select Resource Groups from the menu at left in the portal. Choose the resource group and then the VM you created.
2. Under Operations, select Backup.
3. Make sure your Recovery Services vault is selected, and then choose your backup policy from the drop-down menu. Review the schedule and retention options, and then choose Enable Backup, as shown in the figure below.


- It takes a few seconds for the backup policy to be applied. Once it's enabled, go back to the backup settings. The VM status reports "Warning (Initial backup pending)." To create the first backup, choose the Backup Now button, as shown in Below

Enable backup


molvm

**Welcome to Azure Backup**
Simple and reliable server backup to the cloud. [Learn more](#). Charges are based on the number and size of VMs being protected. [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

Choose backup policy 

BACKUP FREQUENCY

Daily at 1:00 AM Pacific Standard Time

RETENTION RANGE

Retention of daily backup point

Retain backup taken every day at 1:00 AM for 180 Day(s)

Retention of weekly backup point

Retain backup taken every week on Sunday at 1:00 AM for 104 Week(s)

Retention of monthly backup point

Retain backup taken every month on First Sunday at 1:00 AM for 60 Month(s)

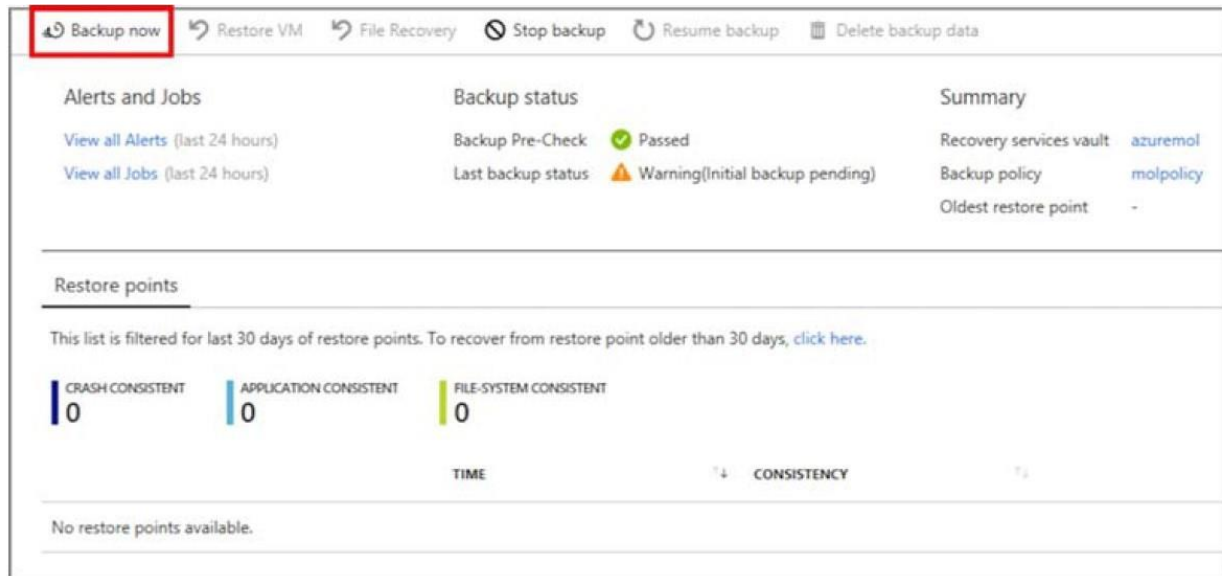
Retention of yearly backup point

Retain backup taken every year in January on First Sunday at 1:00 AM for 10 Year(s)

Or

[Create \(or edit\) a new policy](#)

Enable Backup



Restoring a VM

Azure Backup allows you to restore a complete VM or perform a file-level restore. In all my years, file-level restore operations were the more common of the two. This type of restore job is usually performed when files are deleted or accidentally overwritten. File-level restores usually determine the retention policies for your backups. The more important the data, the more likely you want to retain backups for longer, in case you get a late-night call to restore a file from six months ago. A complete VM restore, as you might expect, restores the entire VM. Rarely have I performed a complete VM restore to bring a deleted VM back online. A great use case for a complete VM restore is to provide a test VM, functionally equivalent to the original. You can restore a VM and then test a software upgrade or other maintenance procedure. This can help you identify potential problems and create a plan for how to handle the real, production VM. It's also important to regularly test your backups. Don't wait until a situation arises when you need to restore data in a real-world scenario. Trust in Azure Backup, but verify that you know how and where to restore the data when needed!

FILE-LEVEL RESTORE

A file-level restore is a pretty cool process in Azure Backup. To give you flexibility in how and where you restore files, Azure creates a recovery script that you download and run. This recovery script is protected with a password so that only you can execute the recovery process. When you run the recovery script, you're prompted to enter the password before you can continue. The window for downloading the recovery script is shown in figure When you run the recovery script, your recovery point is connected as a local filesystem on your computer. For Windows VMs, a PowerShell script is generated, and a local volume is connected, such as F:. For Linux VMs, the recovery point is mounted as a data disk, such as /dev/sdc1 in your home volume. In both cases, the recovery script clearly indicates where you can find your files. Once you've finished restoring files from the recovery vault, you return to the Azure portal and select the Unmount Disks option. This process detaches the disks from your local computer and returns them for use in the recovery vault. Don't worry if you forget to perform this unmount process in

the heat of the moment when you need to quickly restore files for a production VM! Azure automatically detaches any attached recovery points after 12 hours.

File Recovery

molvm



✓ Step 1: Select recovery point

11/17/2017, 8:13:32 PM [Latest] (FileSy... ▼

✓ Step 2: Download script to browse and recover files

This script will mount the disks from the selected recovery point as local drives on the machine where it is run. These drives will remain mounted for 12 hours.

Download Script *

✔ Download completed.

Password to run the script

db30af2a6dac41a



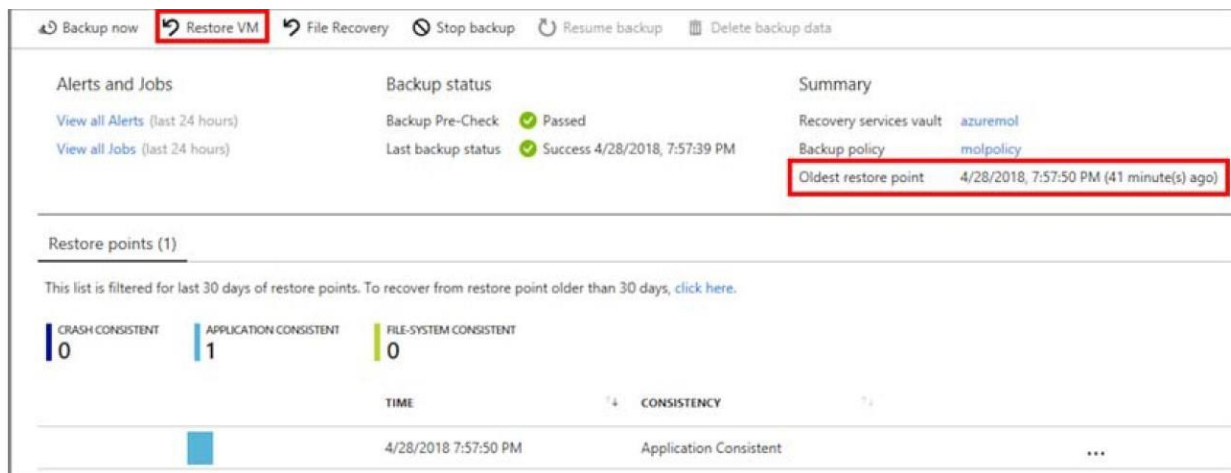
→ Step 3: Unmount the disks after recovery

Unmount disks and close the connection to the recovery point.

Unmount Disks

To restore a complete VM, complete the following steps.

1. From your resource group, select the VM that you backed up in the previous exercise.
2. Select the Backup option from the menu at left in the VM. The backup overview should report that a recovery point has been created, as shown in Bellow. If not, wait a few minutes and then come back to this exercise. Or, just read through what the process entails.



3. Select the Restore VM button. Choose a restore point from the list, and then select OK.
4. Choose a Restore Type. You can choose Create Virtual Machine or Restore Disks. When you choose to restore disks, the disks are restored to the specified storage account. You can then attach these restored disks to an existing VM and obtain the data you need. If you restore a complete VM, a new VM instance is created, connected to the virtual network, and the disks are reattached. For this exercise, choose Create Virtual Machine, as shown in Given Picture. Provide a name for the restored VM, such as restoredvm, and then review the settings for virtual network and storage. In production, you typically connect the restored VM to a segregated virtual network so you don't impact production traffic.
5. Select OK and then Restore. It takes a few minutes to connect the recovery point and create a restored VM with the previous disks attached. At this point, you could connect to the restored VM to test software upgrades or restore large amounts of data as needed. You can also back up a web app, so this isn't just a VM approach. The process is a little different, but the concepts are the same. Moving your application model to a PaaS solution like a web app doesn't mean you can forget the basics of data backups and retention!