

**Agenda: Azure Backup and Restore**

- Overview of Azure Backup
- Configure VM backup
- Create Recovery Services Vault
- Define and Implement backup policies
- Perform VM restore
- Perform backup operation
- Configure and review backup reports

**Overview of Azure Backup**

- Azure Backup is the Azure-based service you can use to back up (or protect) and restore your data, machine state and workloads running on on-premise and Azure VMs 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.

[Watch a video overview of Azure Backup](#)

**Azure Backup delivers these key benefits:**

- **Automatic storage management:** Azure Backup automatically allocates and manages **backup storage**, and it uses a **pay-as-you-use** model.
- **Unlimited scaling:** You don't need to worry about **high-availability** for your data in the cloud.
- **Unlimited data transfer:** Azure Backup does not limit the amount of **inbound or outbound** data you transfer.
- **Multiple storage options:** An aspect of high-availability is storage replication
  - Locally redundant storage
  - [Geo-redundant storage]
- **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.
- **Long-term retention:** Azure doesn't limit the length of time data can remain in a Recovery Services vault.
- **Data integrity verified in the cloud:** Backed up data is also automatically checked for integrity once the backup is complete. As a result, any corruptions due to data transfer are automatically identified and repair is attempted in the next backup

- **Block level incremental backups:** Automatic incremental backups track file and block level changes, only transferring the changed blocks, hence reducing the storage and bandwidth utilization
- **Application-consistent backup:** Azure Backup provides application-consistent backups, which ensure additional fixes are not required to restore the data.

#### Crash-consistent snapshots

- A crash consistent snapshot captures data that was on the disk when the snapshot was taken. It doesn't include anything in memory.
- It contains the equivalent of the on-disk data that would be present if the VM crashed or the power cord was pulled from the server at the instant that the snapshot was taken.
- A crash-consistent doesn't guarantee data consistency for the operating system, or for apps on the VM.
- Site Recovery creates crash-consistent recovery points every five minutes by default. This setting can't be modified.
- Crash-consistent recovery points are usually sufficient for the replication of operating systems, and apps such as DHCP servers and print servers.

#### App-consistent snapshots

- App-consistent recovery points are created from app-consistent snapshots.
- An app-consistent snapshot contains all the information in a crash-consistent snapshot, plus all the data in memory and transactions in progress.
- App-consistent snapshots use the Volume Shadow Copy Service (VSS):
  - 1) When a snapshot is initiated, VSS perform a copy-on-write (COW) operation on the volume.
  - 2) Before it performs the COW, VSS informs every app on the machine that it needs to flush its memory-resident data to disk.
  - 3) VSS then allows the backup/disaster recovery app (in this case Site Recovery) to read the snapshot data and proceed.
- They're more complex and take longer to complete than crash-consistent snapshots.
- They affect the performance of apps running on a VM enabled for replication.

**Azure Backup Components:** These can be used to back up data to a Recovery Services vault in Azure.

1. Azure IaaS VM Backup
2. Azure Backup [Microsoft Azure Recovery Service (MARS)] agent

3. System Center Data Protection Manager (DPM)
4. Microsoft Azure Backup Server (MABS)

Component	Benefits	Limits	What is protected?	Where are backups stored?
<b>Azure Backup Server</b> (can be deployed in Azure and on-premises)	<ul style="list-style-type: none"> <li>• App aware snapshots (VSS)</li> <li>• Full flexibility for when to take backups</li> <li>• Recovery granularity (all)</li> <li>• Can use Recovery Services vault</li> <li>• Linux support on Hyper-V and VMware VMs</li> <li>• Back up and restore VMware VMs</li> <li>• Does not require a System Center license</li> </ul>	<ul style="list-style-type: none"> <li>• Cannot back up Oracle workload.</li> <li>• Always requires live Azure subscription</li> <li>• No support for tape backup</li> </ul>	<ul style="list-style-type: none"> <li>• Files,</li> <li>• Folders,</li> <li>• Volumes,</li> <li>• VMs,</li> <li>• Applications,</li> <li>• Workloads,</li> <li>• System State</li> </ul>	<ul style="list-style-type: none"> <li>• Recovery Services vault,</li> <li>• Locally attached disk</li> </ul>
<b>Azure IaaS VM Backup</b>	<ul style="list-style-type: none"> <li>• Native backups for Windows/Linux</li> <li>• No specific agent installation required</li> <li>• Fabric-level backup with no backup infrastructure needed</li> </ul>	<ul style="list-style-type: none"> <li>• Back up VMs once-a-day</li> <li>• Restore VMs only at disk level</li> <li>• Cannot back up on-premises</li> </ul>	<ul style="list-style-type: none"> <li>• VMs,</li> <li>• All disks (using PowerShell)</li> </ul>	Recovery Services vault

Note: All Components can be deployed in Azure and except Azure IaaS VM Backup, all components can be deployed in on-premises.

### How does Azure Backup work?

The way in which Azure Backup takes a backup depends on the scenario.

1. **Directly backup Azure VMs:** Azure VM extension is installed on the VM the first time a back up runs for the VM.
2. **Directly backup on-premises machines:** Azure Backup uses the Microsoft Azure Recovery Services (MARS) agent. This agent runs on individual on-premises Windows Servers to back up files, folders, and system state.
3. **Backup machines and apps protected by DPM or MABS:** The machine/app is first backed up to DPM or MABS local storage using MARS agent. Then, the data in DPM/MABS is backed up to the vault by Azure Backup. On-premises machines can be protected by DPM/MABS running on-premises. Azure VMs can be protected by DPM/MABS running in Azure.

### Backup Types:

1. **Full:** A backup contains the entire data source. Full backup takes more network bandwidth. Used for initial backup.
2. **Differential:** Stores the blocks that **changed since the initial full backup**. **Not used by Azure Backup.**
3. **Incremental:** High storage and network efficiency. Stores only blocks of data that **changed since the previous backup**. Used by DPM/MABS for disk backups, and used in all backups to Azure.

#### Which applications and workloads can be backed up?

Data or Workload	Source Environment	Azure Backup solution
Azure IaaS VMs	Running in Azure	Azure Backup Extension (VM Extension)
Files and folders	Windows Server	Azure Backup Agent, System Center DPM, Azure Backup Server
Hyper-V virtual machine	Windows Server Unix Server	System Center DPM Azure Backup Server
VMware virtual machine	Windows Server Unix Server	System Center DPM Azure Backup Server
Microsoft SQL Server	Windows Server	System Center DPM Azure Backup Server
Microsoft SharePoint	Windows Server	System Center DPM Azure Backup Server
Microsoft Exchange	Windows Server	System Center DPM Azure Backup Server

### Backup and Restore of Azure VM

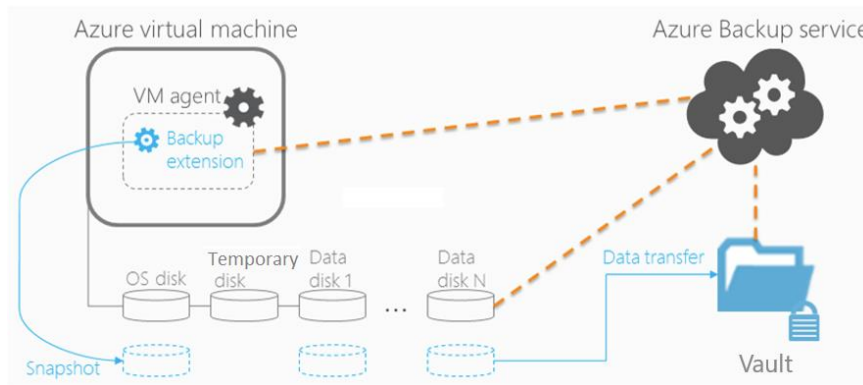
#### Where is data backed up?

##### Recovery Services Vault

- A Recovery Services vault is a **logical container** that stores the backup data for each protected resource, such as Azure VMs and Azure SQL databases.
- When the backup job for a protected resource runs, it creates a **recovery point** inside the Recovery Services vault. You can then use one of these recovery points to **restore** data to a given **point in time**.
- Within an Azure subscription, you can create up to 500 Recovery Services vaults.

**Architecture:**

1. When you enable backup for an Azure VM, a backup runs in accordance with the schedule you specify.
2. During the first backup, a backup extension (VMSnapshot) is installed on VM if it's running.
3. The extension takes a storage level **app-consistent snapshot** of the VM. If Backup is unable to take an app-consistent snapshot, then it takes a file-consistent snapshot.
4. After the snapshot is taken, only blocks of data that have changed since the last backup are transferred to the vault. Total backup time for a VM will be less than 24 hours for daily backup policies.
5. After data has been sent to the vault, the snapshot is removed, and a recovery point is created.



Note: Backing up virtual machines is a local process. **You cannot back up a virtual machine from one location to a Recovery Services vault in another location.**

**WALKTHROUGH:**

Create a VM and install some software or create some files in it.

**Configure the backup job from the Recovery Services vault**

1. New Services → **Backup and Site Recovery**
2. Click Add and provide the required details including Name, Subscription, Location **(must be same as VM location)** → Create
3. Select vault → Settings → **Properties** → **Backup Configuration** → Choose the appropriate **storage replication** option for your vault.
4. Select Vault → Settings → Overview → **+ Backup**, The Backup and Backup Goal blades open.
  - Set Where is your workload running = **Azure**, What do you want to backup = **Virtual Machine**
  - Set Backup Policy Select → **Default Policy**

- Items to backup Select → **Select the VM** to backup → OK

5. Click **Enable Backup**

**Initial Backup:**

You have enabled backup for the Recovery Services vaults, but an initial backup has not been created. It is a disaster recovery best practice to trigger the first backup, so that your data is protected.

6. Select Vault → **Backup Items** blade → Click Azure Virtual Machine.
7. On the **Backup Items** list, click the ellipses ... to open the Context menu → **Backup now**
8. Provide **Retain Backup Till** = <Date> → Click OK button
9. To view or track the status of the initial backup, on the vault dashboard, on the **Backup Jobs (Monitoring Section)** tile click **In progress**.

**Alternative: Configure the backup job from the VM management blade**

1. Select the VM
2. On the VM management blade, in the **Settings** section, click **Backup**.
3. In Enable backup blade → Create New vault and provide Backup Policy → OK → **Enable Backup**
4. Select VM → Settings → Backup → Click on Backup now (Menu).

Note: Until the initial backup has completed, **Last backup status** shows as **Warning (Initial backup pending)**.

5. In Backup Now blade provide Retain backup Till = <Date> → Backup

**Use Azure portal to restore virtual machines**

**Restore a recovery point**

6. Browse → Recovery Services vaults
7. Select vault → In the vault dashboard. On the **Backup Items** tile, click **Azure Virtual Machines** to display the VMs associated with the vault.
8. From the list, select a VM to open the dashboard. The VM dashboard opens to the Monitoring area, which **contains the Restore points** tile.
9. On the VM dashboard menu, click **Restore VM**
10. Select Restore Point, by default, the dialog displays all restore points from the last 30 days. Use the **Filter** to alter the time range of the restore points displayed. By default, restore points of all consistency are displayed.
11. Choose a Restore point and click **OK**.
12. On the **Restore** blade, **Restore configuration** opens automatically after restore point is set.

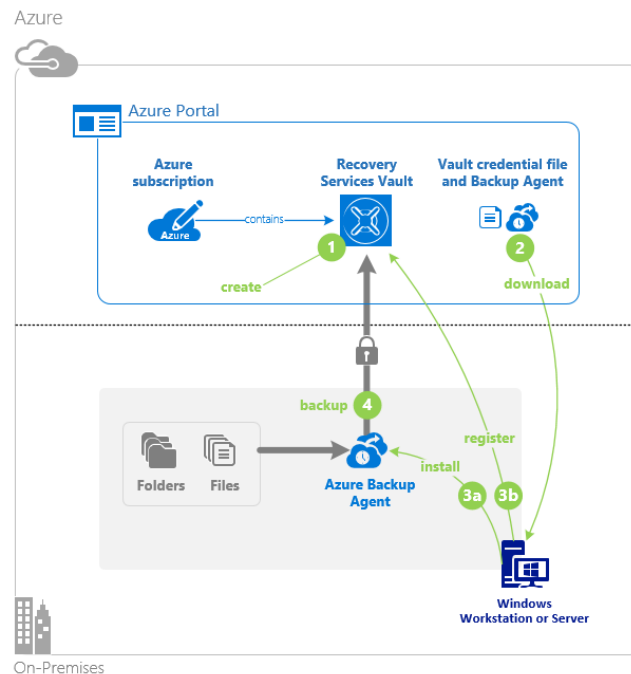
13. In the **Restore configuration** blade, Restore Type = **Create Virtual machine** and provide other details for creating a VM → OK
14. Click Restore (Once you trigger the restore operation, the Backup service creates a job for tracking the restore operation.)
15. To **Track the restore operation**, Select the vault → Vault Dashboard → **Backup Jobs tile** → click the Azure Virtual Machine

#### For SQL Server on Azure VM following Extension must be installed

If the default extensions fails to create, please drop that and recreate the Extension using the below Powershell command

```
Set-AzVMSqlServerExtension -ResourceGroupName "DemoRG" -VMName "SqlServer" -Name "SqlIaaSExtension" -Version "2.0" -Location "East US"
```

### Backup a Windows Server (Files and Folders) to Azure



#### Step1: Recovery Services vault

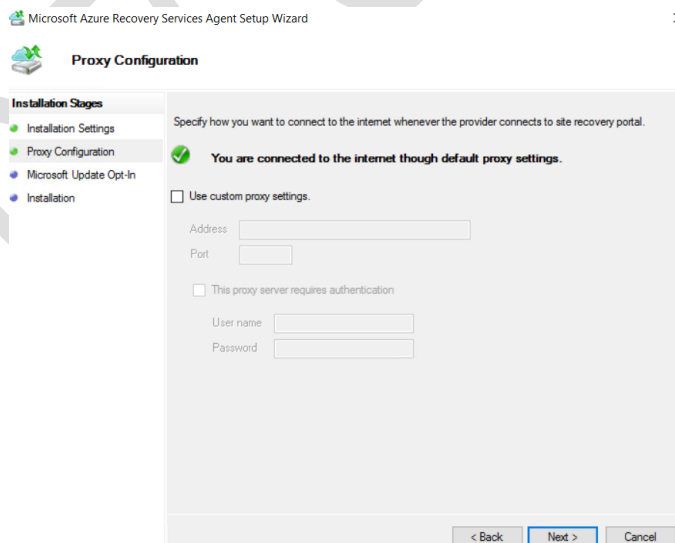
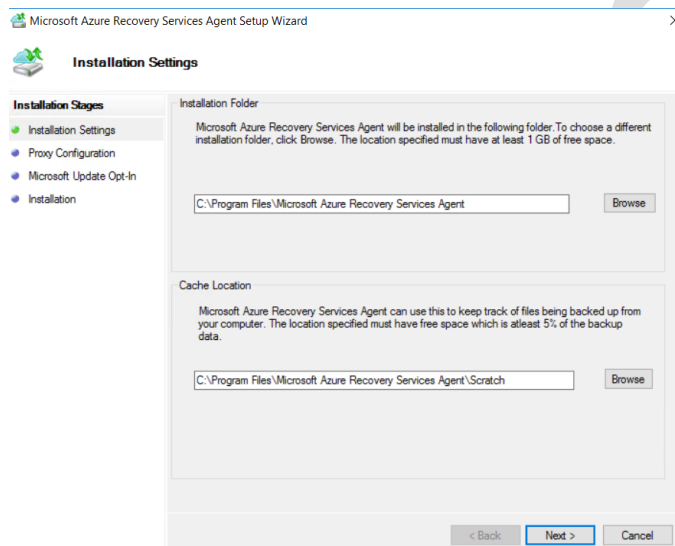
1. Create a Recovery Service Vault
2. Recovery Service Vault → Backup Infrastructure → Backup Configuration
3. Select the Storage **Replication Type** = Locally-redundant / [Geo Redundant]

**Step2: Configure the Vault**

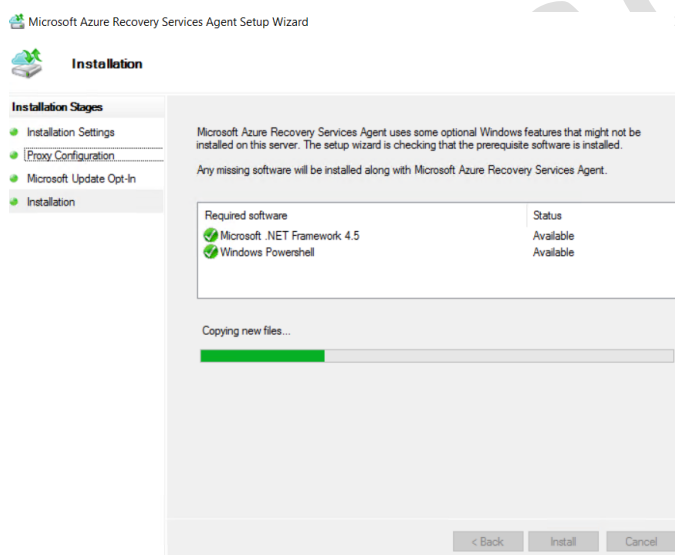
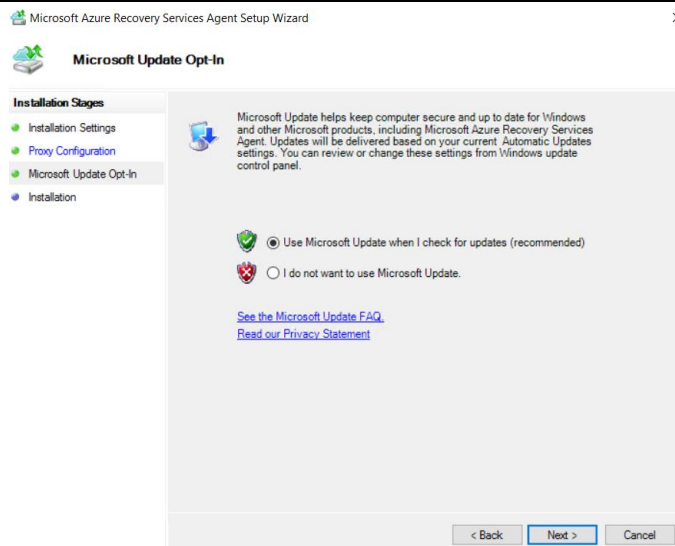
4. Recovery Service Vault → **Backup**,
5. Where is your workload running = **On-premise**, What do you want to backup = **Files and Folders**
6. Click on **Prepare Infrastructure**
7. Copy the “**Download Agent for Windows Server or Windows Client**” Link
8. Click **Download** to download the Vault Credentials and save the file locally.

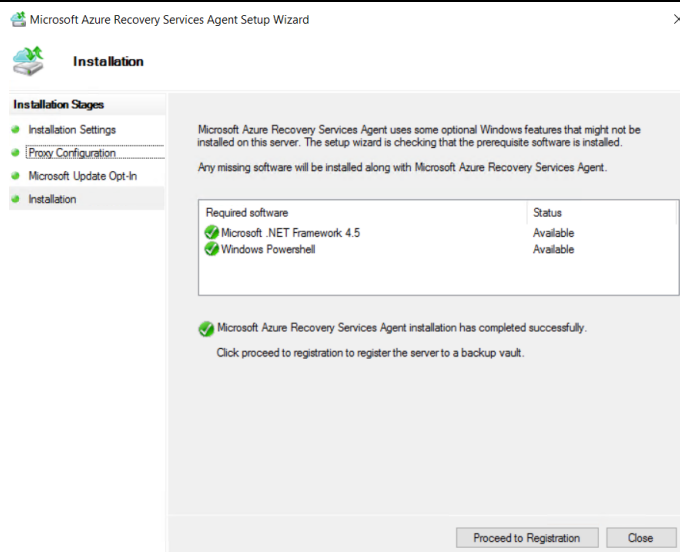
**Step3: Install and Register Agent on VM**

9. RDP to VM
10. **Copy** the Downloaded **Vault Credentials** file to this VM
11. Open browser → Visit link copied earlier → **Install Agent** (MARSAgentInstaller.exe)

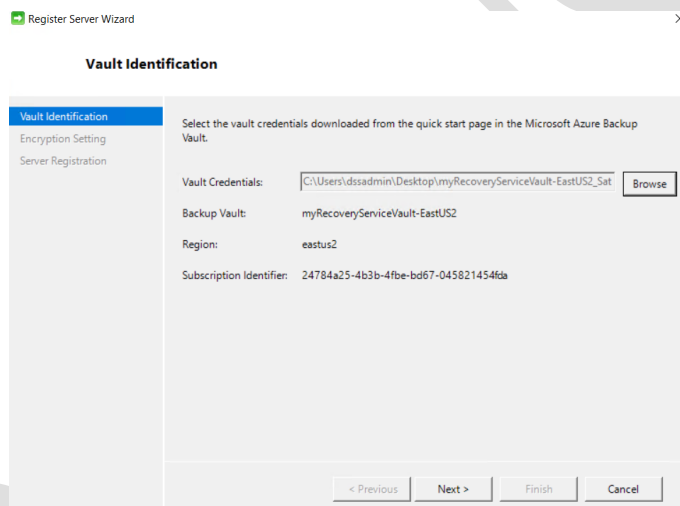








12. Click on Proceed to Registration and Complete the Setup Wizard by providing the **Vault Credential file**.



13. Click on Generate Passphrase and specify local folder for saving the same.

Register Server Wizard

### Encryption Setting


Vault Identification  
Encryption Setting  
Server Registration

Backups are encrypted to protect the confidentiality of your data.  
Generate or type a passphrase to encrypt and decrypt backups from this server.

Enter Passphrase (minimum of 16 characters)  
 (0)

Confirm Passphrase  
 (0)

Enter a location to save the passphrase

 Saving the passphrase locally does not protect it from corruptions and disasters. Microsoft cannot recover data, if the passphrase is lost or forgotten. It is strongly advised to store a copy of the passphrase in a secure 'external' location, like the Azure Key Vault. [Learn to store the passphrase in an Azure Key Vault](#)

< Previous Next > Finish Cancel

#### 14. Now wait for Registering the server.

Register Server Wizard

### Server Registration

Vault Identification  
Encryption Setting  
Server Registration


Registering this server with Microsoft Azure Backup...

< Previous Next > Close Cancel


Register Server Wizard

### Server Registration

Vault Identification  
Encryption Setting  
Server Registration

 Microsoft Azure Backup is now available for this server.

The passphrase was saved to the following file:  
[C:\Users\dssadmin\Desktop\Microsoft Azure Recovery Services Agent 2\\_16\\_2019\\_10\\_11\\_39.txt](#)

 Save a copy of the passphrase in an Azure Key Vault to avoid passphrase loss.  
[Learn how you can store the passphrase in Azure Key Vault.](#)

Before your server is backed up you must configure and schedule backup options.

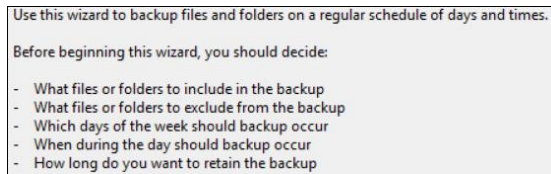
☒ Launch Microsoft Azure Recovery Services Agent

< Previous Next > Close Cancel

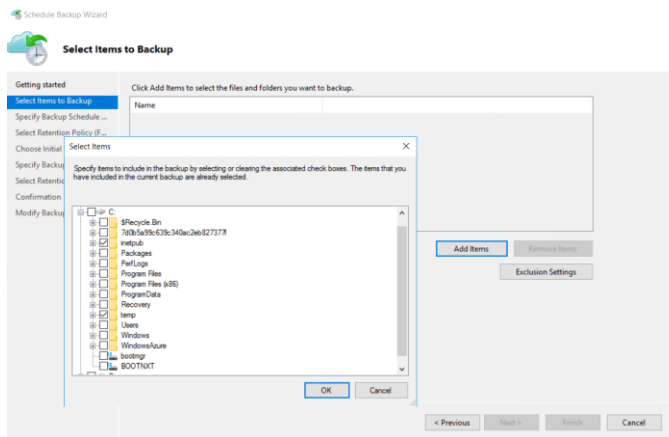
**Step4: Create the backup policy**

15. In VM → Open **Microsoft Azure Backup** application

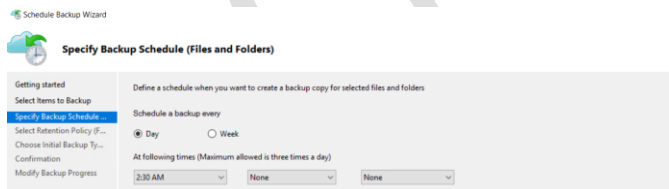
16. Actions pane → **Schedule Backup**.



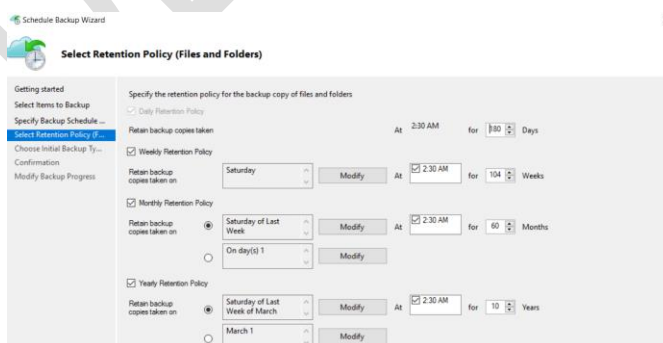
17. Select **Items to Backup** page, click **Add Items** → Select the files and folders that you want to protect, and then click **OK** → Next



18. Specify Backup Schedule = **Day / Week**

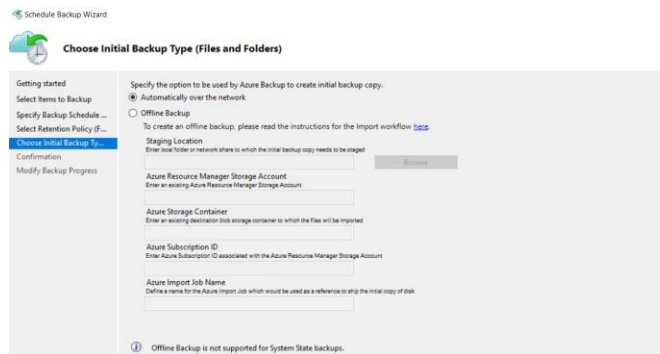


19. On the **Select Retention Policy** page, choose the specific retention policies the for the backup copy and click **Next**.

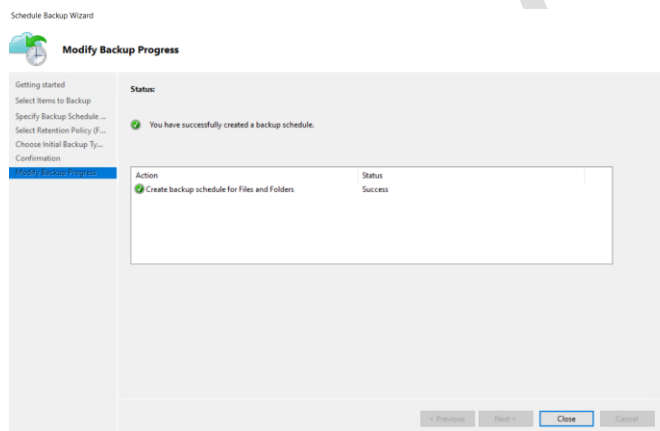


Note: The retention policy specifies the duration which the backup is stored. Rather than just specifying a “flat policy” for all backup points, you can specify different retention policies based on when the backup occurs. You can modify the daily, weekly, monthly, and yearly retention policies to meet your needs.

20. Choose Initial Backup Type = Automatically over the Internet



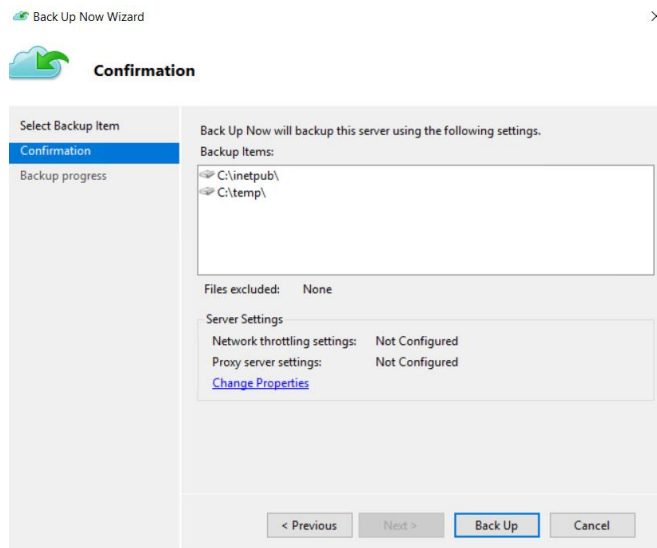
21. Click Finish to get the below screen



**Step5: To back up files and folders for the first time**

22. Actions pane → **Backup Now**

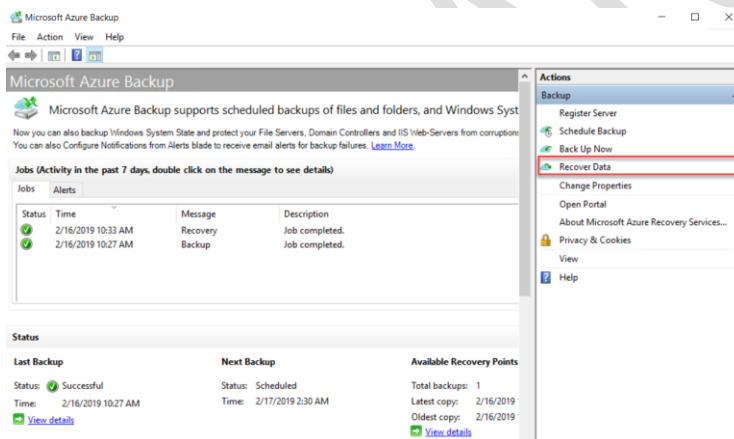
23. On the Confirmation page, review the settings that the Back Up Now Wizard will use to back up the machine. Then click **Back Up**.



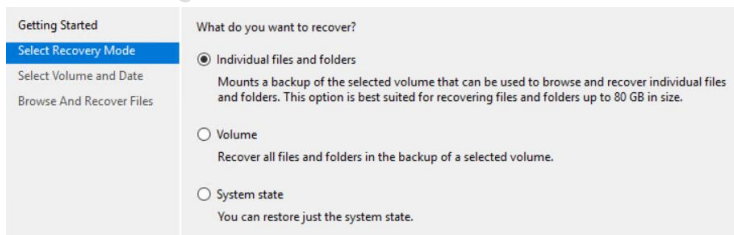
24. After the initial backup is completed, the **Job completed** status appears in the Backup console.

### Restore files from Azure to a Windows Server

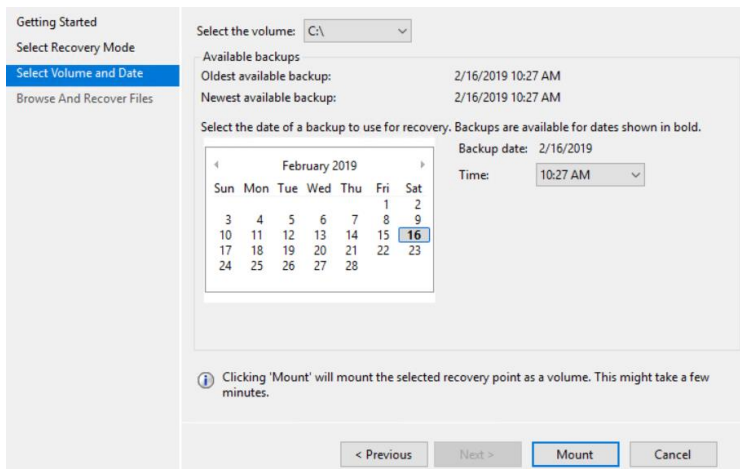
1. Open the **Microsoft Azure Backup** snap-in
2. click **Recover Data** in the **Actions Pane**



3. **Getting Started** page, select **This server (server name)** and click **Next**
4. On the **Select Recovery Mode** page, select **Individual files and folders** and then click **Next**



- On the **Select Volume and Date** page, select the volume that contains the files or folders you want to restore, and click **Mount**.



- Select a date, and select a time from the drop-down menu that corresponds to a recovery point. Dates in **bold** indicate the availability of at least one recovery point on that day.
- Note that when you click **Mount**, Azure Backup makes the recovery point available as a disk. Browse and recover files from the disk.
- Once the recovery volume is mounted, click **Browse** to open Windows Explorer and find the files and folders you wish to recover.
- In Windows Explorer, copy the files and/or folders you want to restore and paste them to any desired location on the server.

### Unmount the Drive

- When you are finished restoring the files and/or folders, on the **Browse and Recovery Files** page of the **Recover Data** wizard, click **Unmount**.
- Once the snapshot is unmounted, **Job Completed** appears in the **Jobs** pane in the agent console.