**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.

**What can we back up?**

* **On-premises** - Back up files, folders, system state using the Microsoft Azure Recovery Services (MARS) agent. Or use the DPM or Azure Backup Server (MABS) agent to protect on-premises VMs (Hyper-V and VMware) and other on-premises workloads
* **Azure VMs** - Back up entire Windows/Linux VMs (using backup extensions) or back up files, folders, and system state using the MARS agent.
* **Azure Managed Disks** - Back up Azure Managed Disks
* **Azure Files shares** - Back up Azure File shares to a storage account
* **SQL Server in Azure VMs** - Back up SQL Server databases running on Azure VMs
* **SAP HANA** databases in Azure VMs - Backup SAP HANA databases running on Azure VMs
* **Azure Database for PostgreSQL servers** - Back up Azure PostgreSQL databases and retain the backups for up to 10 years
* **Azure Blobs** - Overview of operational backup for Azure Blobs

**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 doesn't limit the amount of inbound or outbound data you transfer, or charge for the data that's transferred.
* **Multiple storage options:** An aspect of high-availability is storage replication
  + Locally redundant storage
  + [Geo-redundant storage]
* **Data encryption:** Azure Backup provides solutions for securing data in transit and at rest..
* **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
* **Multiple storage options** - Azure Backup offers three types of replication (LRS/ZRS/GRS) to keep your storage/data highly available.
* **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. * 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. * 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. |

**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.
* Recovery Services vaults support System Center DPM, Windows Server, Azure Backup Server, and more. Recovery Services vaults make it easy to organize your backup data, while minimizing management overhead.
* 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.

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

|  |  |
| --- | --- |
| **Azure IaaS VM Backup using Recovery Service Agent (Only for Azure VM)**  **Benefits**   * Native backups for Windows/Linux * No specific agent installation required * Fabric-level backup with no backup infrastructure needed.   **Limits**   * Back up VMs once-a-day * Restore VMs only at disk level * Cannot back up on-premises   **What is protected?**   * VMs * All disks (using PowerShell)   **Where are backups stored?**   * Recovery Services vault | **Microsoft Azure Backup Server (MABS)**  (can be deployed in Azure and on-premises)  **Benefits**   * App aware snapshots (VSS) * Full flexibility for when to take backups * Linux support on Hyper-V and VMware VMs   **Limits**   * Cannot back up Oracle workload * Always requires live Azure subscription * No support for tape backup   **What is protected?**   * File * Folders * Volumes * VMs * Applications * System State   **Where are backups stored?**   * Recovery Services vault * Locally attached disk |

**Azure IaaS VM Backup**

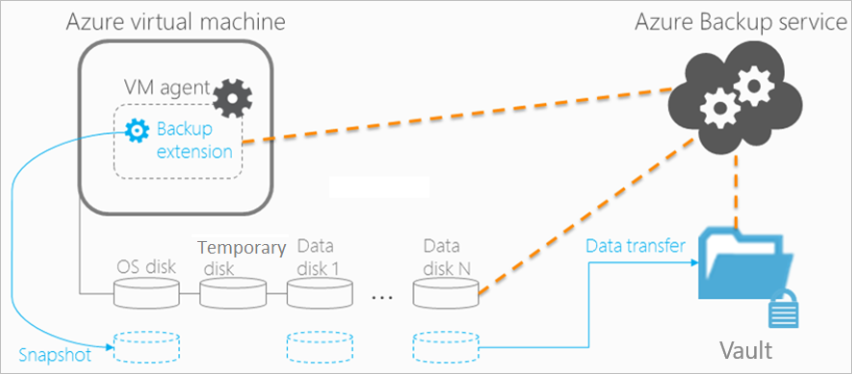
* Backups are stored in a Recovery Services vault with built-in management of recovery points.

## **Azure VM Backup Architecture:**

1. Azure Backup starts a backup job according to the backup schedule you specify.
2. During the first backup, a backup extension is installed on VM if it's running.
   * For Windows VMs, the [VMSnapshot extension](https://learn.microsoft.com/en-us/azure/virtual-machines/extensions/vmsnapshot-windows) is installed.
   * For Linux VMs, the [VMSnapshotLinux extension](https://learn.microsoft.com/en-us/azure/virtual-machines/extensions/vmsnapshot-linux) is installed.
3. For Windows VMs that are running, Backup coordinates with Windows Volume Shadow Copy Service (VSS) to take an app-consistent snapshot of the VM.
   * By default, Backup takes full VSS backups.
   * If Backup can't take an app-consistent snapshot, then it takes a file-consistent snapshot of the underlying storage (because no application writes occur while the VM is stopped).

For Linux VMs, Backup takes a file-consistent backup. For app-consistent snapshots, you need to manually customize pre/post scripts.

1. After Backup takes the snapshot, it transfers the data to the vault.
   * The backup is optimized by backing up each VM disk in parallel.
   * For each disk that's being backed up, Azure Backup reads the blocks on the disk and identifies and transfers only the data blocks that changed (the delta) since the previous backup.
   * Snapshot data might not be immediately copied to the vault. It might take some hours at peak times. Total backup time for a VM will be less than 24 hours for daily backup policies.



Note: Changes made to a Windows VM after Azure Backup is enabled on it are:

1. Microsoft Visual C++ 2013 Redistributable(x64) - 12.0.40660 is installed in the VM
2. Startup type of Volume Shadow Copy service (VSS) changed to automatic from manual
3. IaaSVmProvider Windows service is added

**Note about encryption:**

* The recovery services vault has encryption enabled via server-side encryption (SSE), so the backup is encrypted at rest and is protected while in transit.
* When you secure your data via Azure Disk Encryption (ADE), given keys and are also backed up via Azure Backup.

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.**

**Create a Recovery Services vault**

1. Search Backup center 🡪 **+ Vault** 🡪 Select **Recovery Service Vault** 🡪 Continue
   * Vault name = Demo-vault
   * Location (must be same as VM location)
   * Review + Create 🡪 Create

**Configure the backup job**

1. Select Demo-vault 🡪 **Properties** 🡪 Click **Update** under **Backup Configuration** 🡪 Choose the appropriate **storage replication** = LRS 🡪 Save
2. Select Demo-vault 🡪 Overview 🡪 **+ Backup**,
   * **Where is your workload running = Azure,**
   * **What do you want to backup = Virtual Machine**
   * **Configure**
3. **Configure backup**
   * Backup Policy = **Default Policy**
   * Add 🡪 **Select the VM** to backup 🡪 OK

Note: If error is reported changed to Enhanced Policy.

1. 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.

1. Select Demo-vault 🡪 **Backup Items**  🡪 Click Azure Virtual Machine.
2. On the **Backup Items** list, click the ellipses **...** to open the Context menu 🡪 **Backup now**
3. Provide **Retain Backup** **Till** = <Date> 🡪 Click OK button
4. To view or track the status of the initial backup,
   * Demo-vault 🡪 **Backup Jobs (Monitoring Section)** tile click **In progress.**

# **Use Azure portal to restore virtual machines**

## **Restore a recovery point**

1. Select Demo-vault 🡪 **Backup Items**  🡪 click **Azure Virtual Machines**.
2. From the list, select a VM, **View Details**. The Backup Item dashboard opens to the Monitoring area, which **contains the Restore points** tile.
3. click **Restore VM**
4. 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.
5. On the **Restore** blade, **Restore configuration** opens automatically after restore point is set.
6. Restore Type = **Create Virtual machine** and provide other details for creating a VM 🡪 OK
7. Restore
8. 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 extentions fails to create, please drop that and recreate the Extension using the below Powershell command

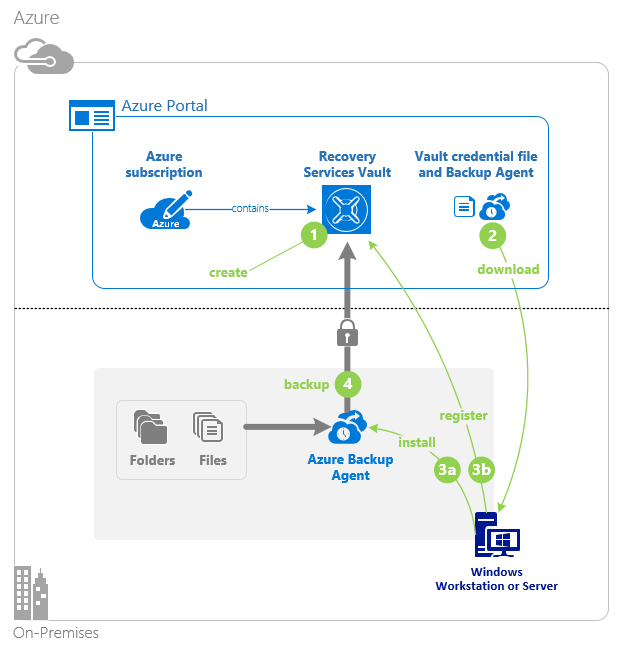
Set-AzVMSqlServerExtension -ResourceGroupName "DemoRG" -VMName "SqlServer" -Name "SqlIaasExtension" -Version "2.0" -Location "East US"

**Backup a Windows Server (Files and Folders) to Azure using Azure Backup**

Azure Backup uses the MARS agent to back up files, folders, and system state from on-premises machines and Azure VMs. Those backups are stored in a Recovery Services vault in Azure. You can run the agent:

* Directly on on-premises Windows machines. These machines can back up directly to a Recovery Services vault in Azure.
* On Azure VMs that run Windows side by side with the Azure VM backup extension. The agent backs up specific files and folders on the VM.
* On a Microsoft Azure Backup Server (MABS) instance or a System Center Data Protection Manager (DPM) server. In this scenario, machines and workloads back up to MABS or Data Protection Manager. Then MABS or Data Protection Manager uses the MARS agent to back up to a vault in Azure.

The data that's available for backup depends on where the agent is installed.



**Step1: Recovery Services vault**

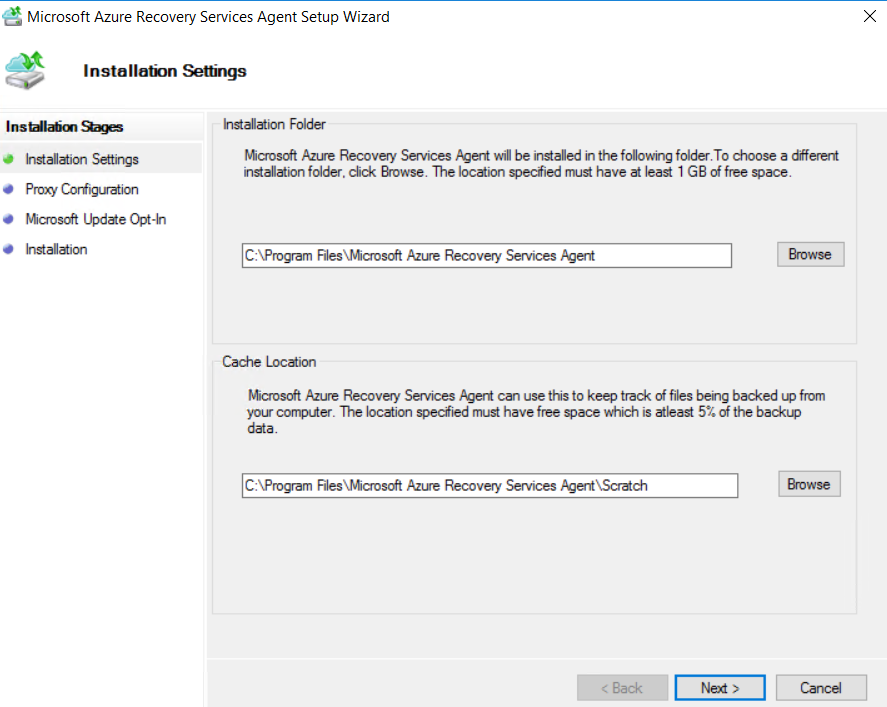
1. Create a Recovery Service Vault
2. Recovery Service Vault 🡪 Backup Infrastructure 🡪 Backup Configuration
3. Select the Storage **Replication Type** = Locally-redundant / [Geo Redundant]

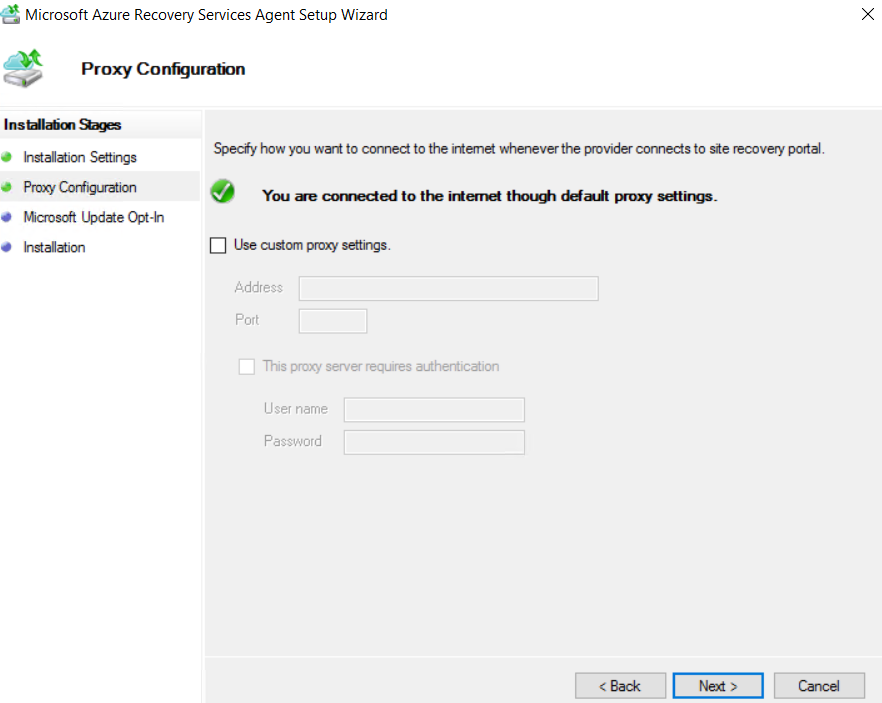
**Step2: Configure the Vault**

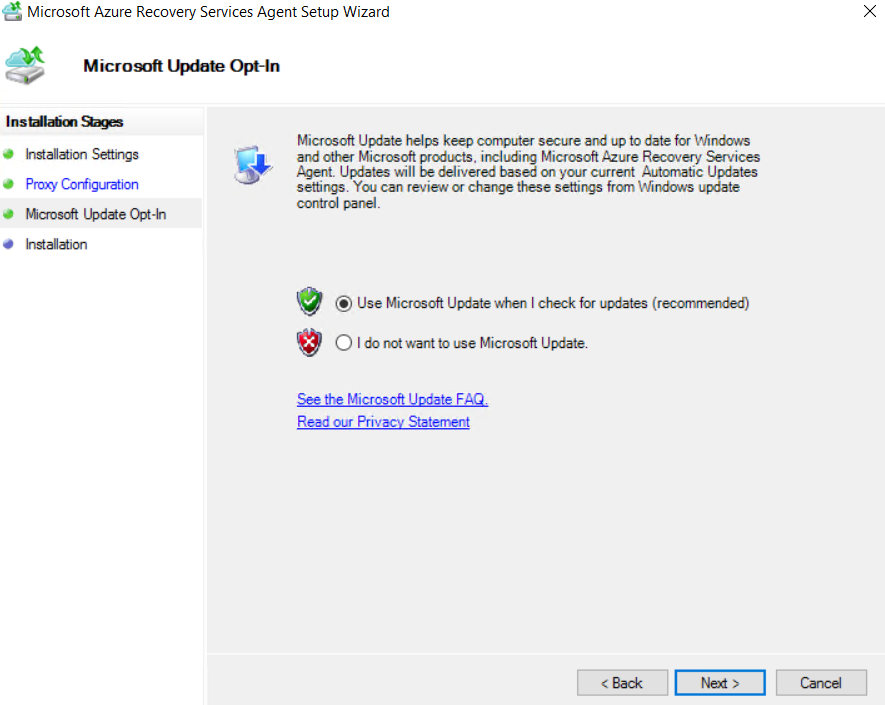
1. Recovery Service Vault 🡪 **Backup**,
2. Where is your workload running = **On-premise**, What do you want to backup = **Files and Folders**
3. Click on **Prepare Infrastructure**
4. Copy the “***Download Agent for Windows Server or Windows Client***” Link
5. Click **Download** to download the Vault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

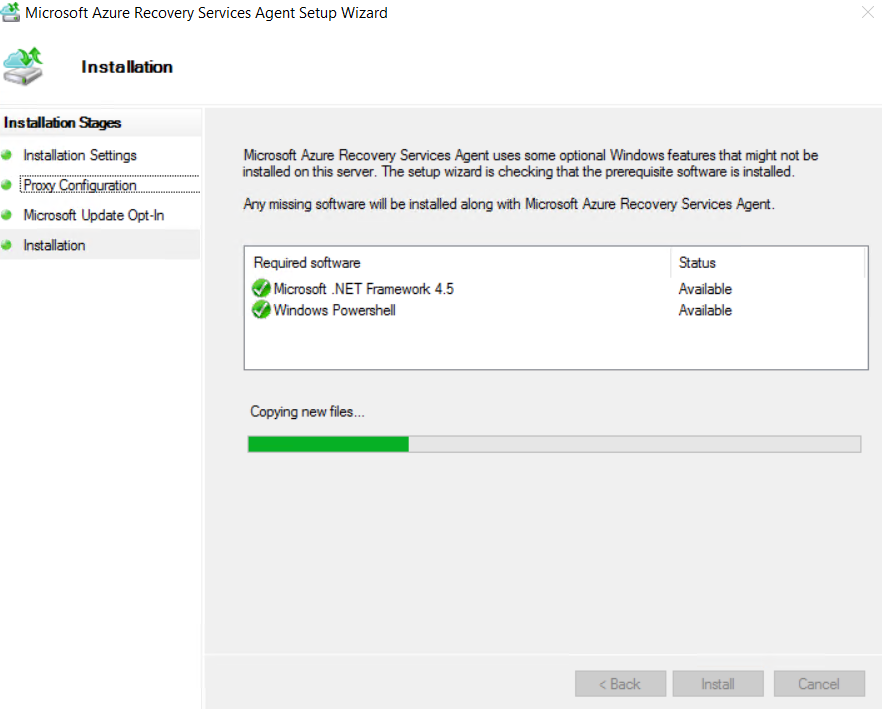
**Step3: Install and Register Agent on VM**

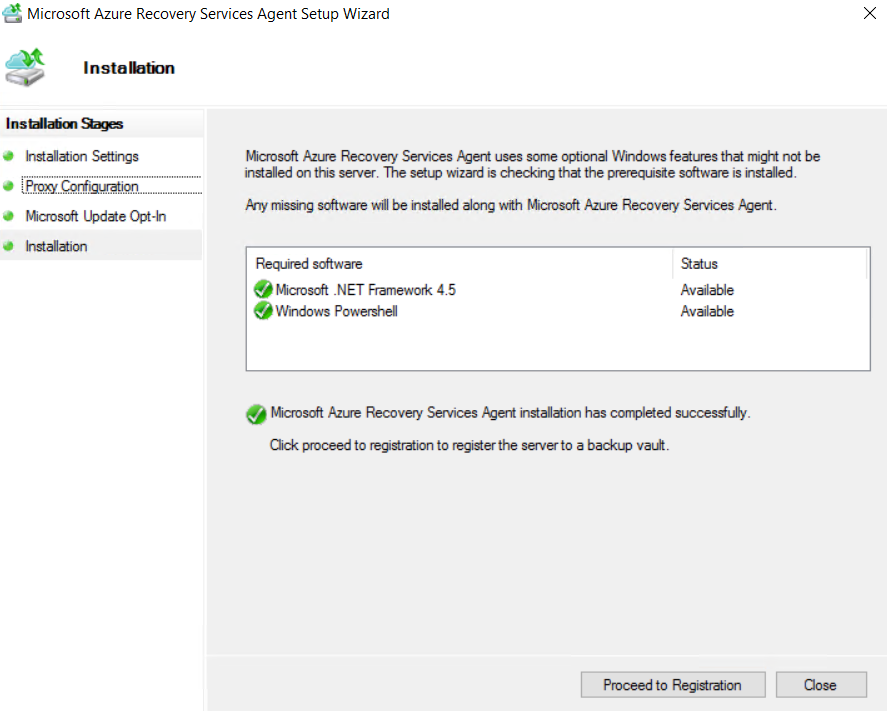
1. RDP to VM
2. **Copy** the Downloaded **Vault Credentials** **file** to this VM
3. Open browser 🡪 Visit link copied earlier 🡪 **Install Agent** **(MARSAgentInstaller.exe)**



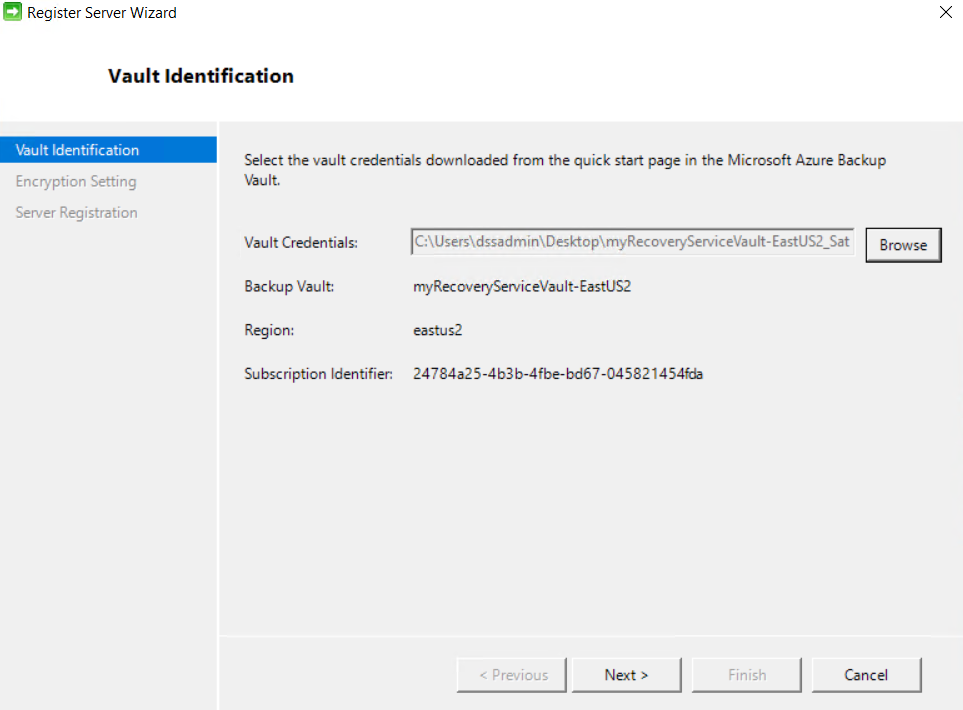




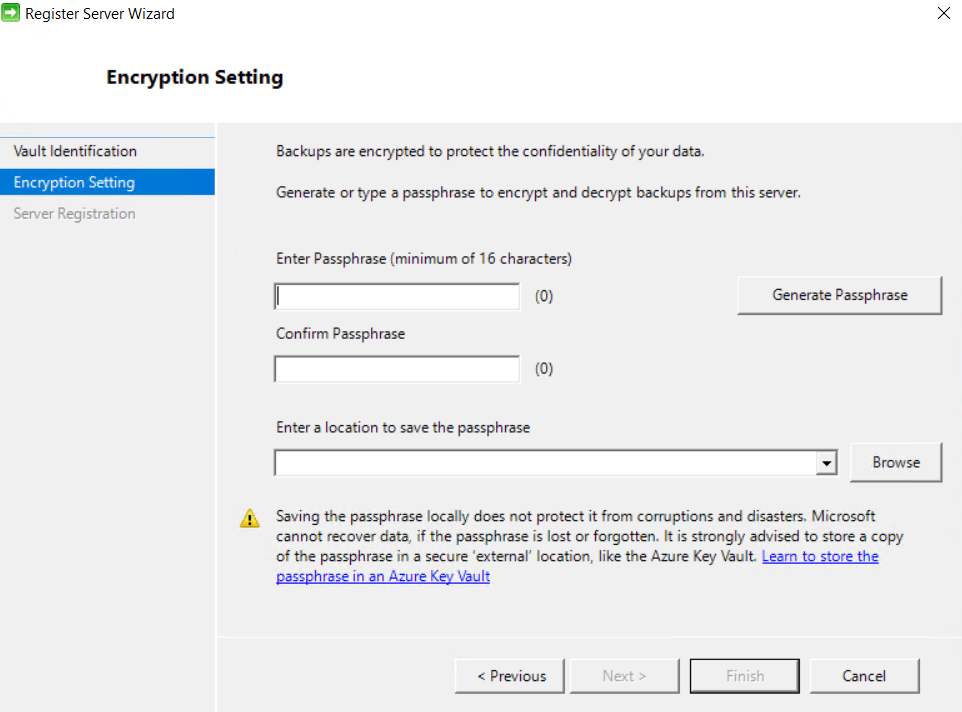




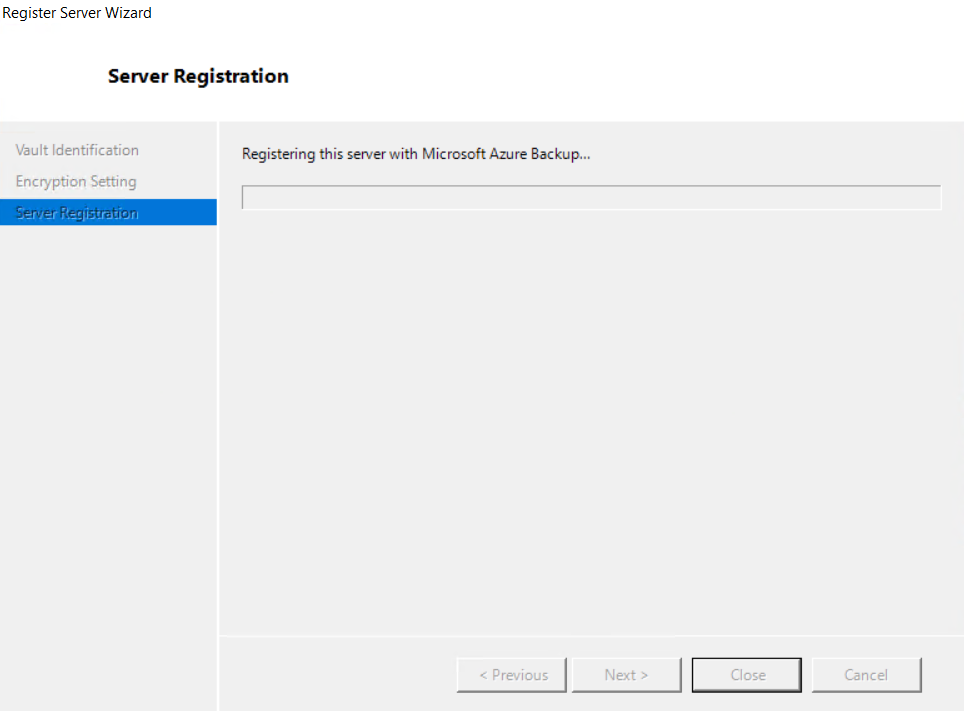
1. Click on Proceed to Registration and Complete the Setup Wizard by providing the **Vault Credential file**.

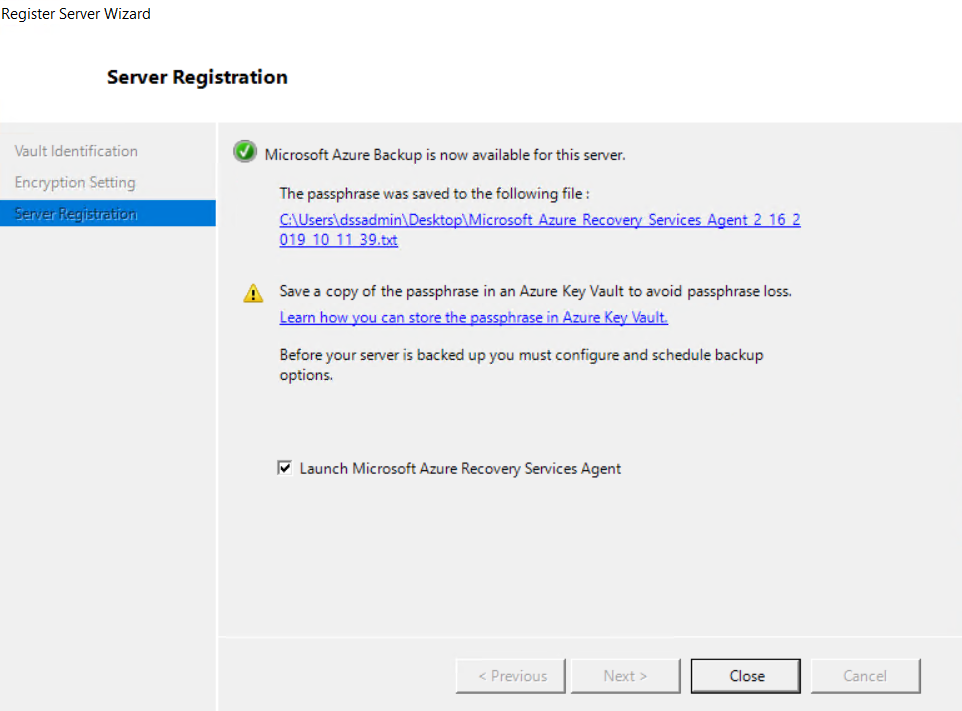


1. Click on Generate Passphrase and specify local folder for saving the same.



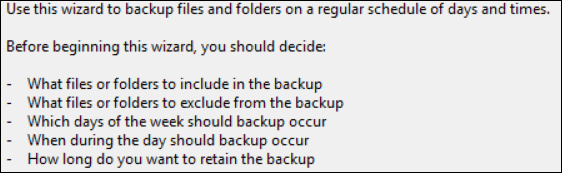
1. Now wait for Registering the server.



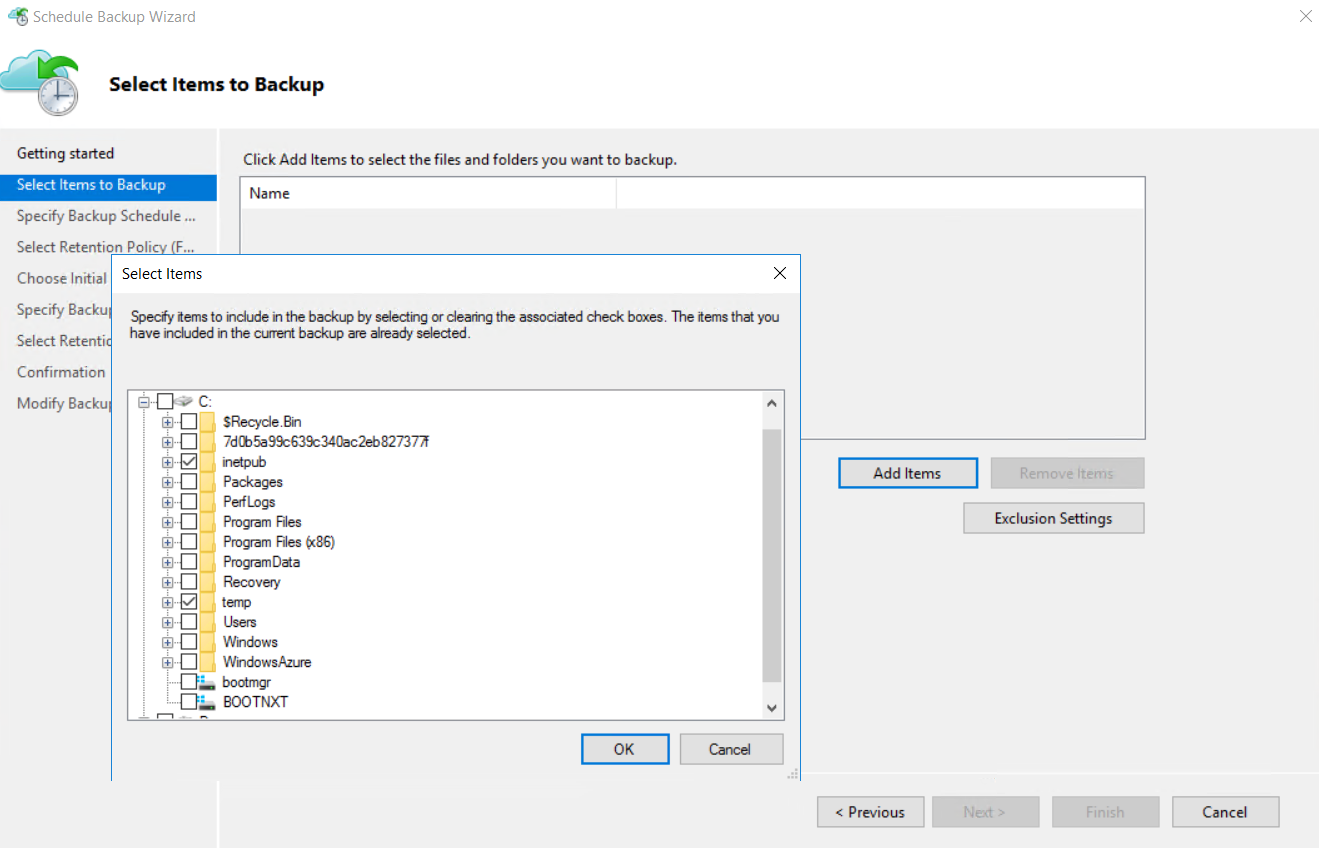


**Step4: Create the backup policy**

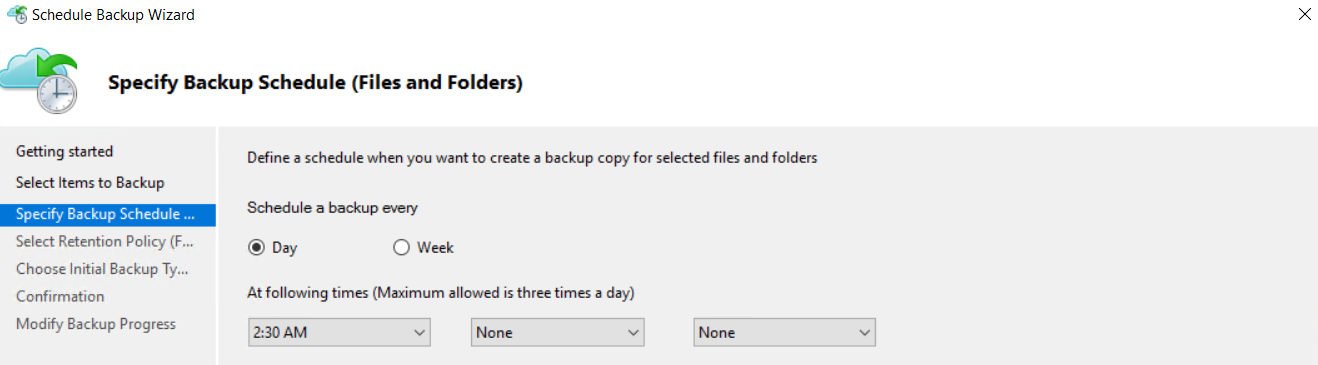
1. In VM 🡪 Open **Microsoft Azure Backup** application
2. Actions pane 🡪 **Schedule Backup**.



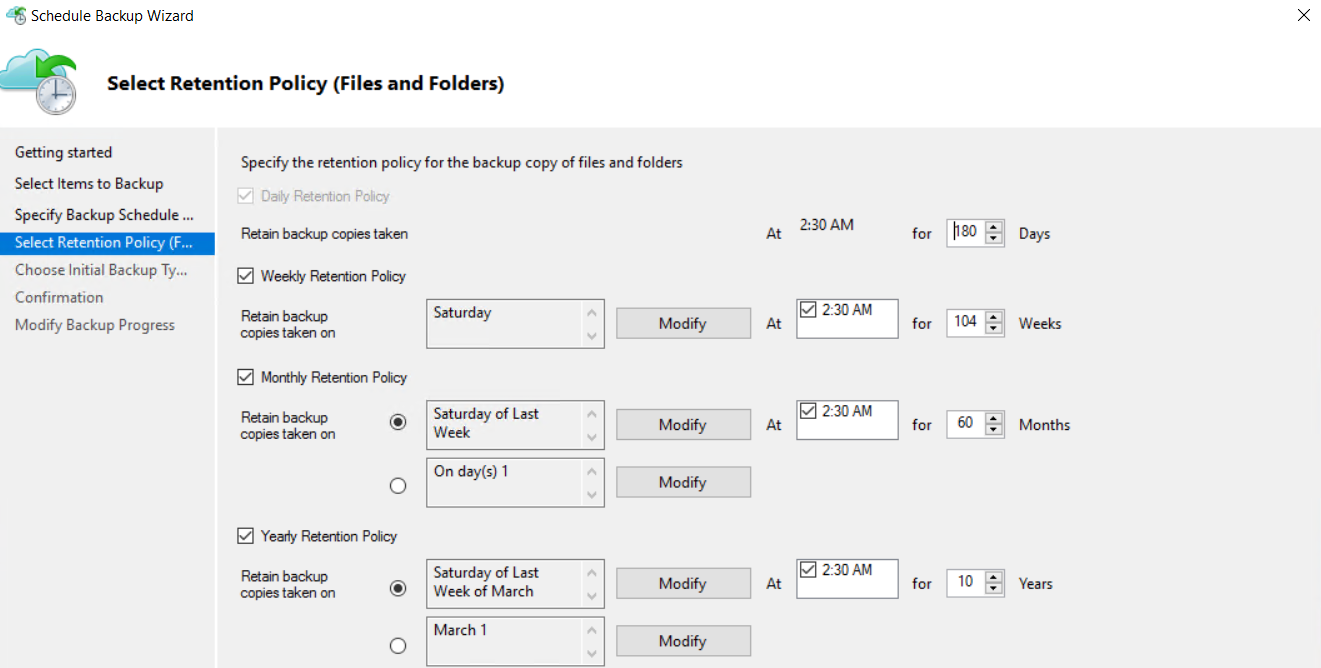
1. **Select Items to Backup** page, click **Add Items** 🡪 Select the files and folders that you want to protect, and then click **OK** 🡪 Next



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

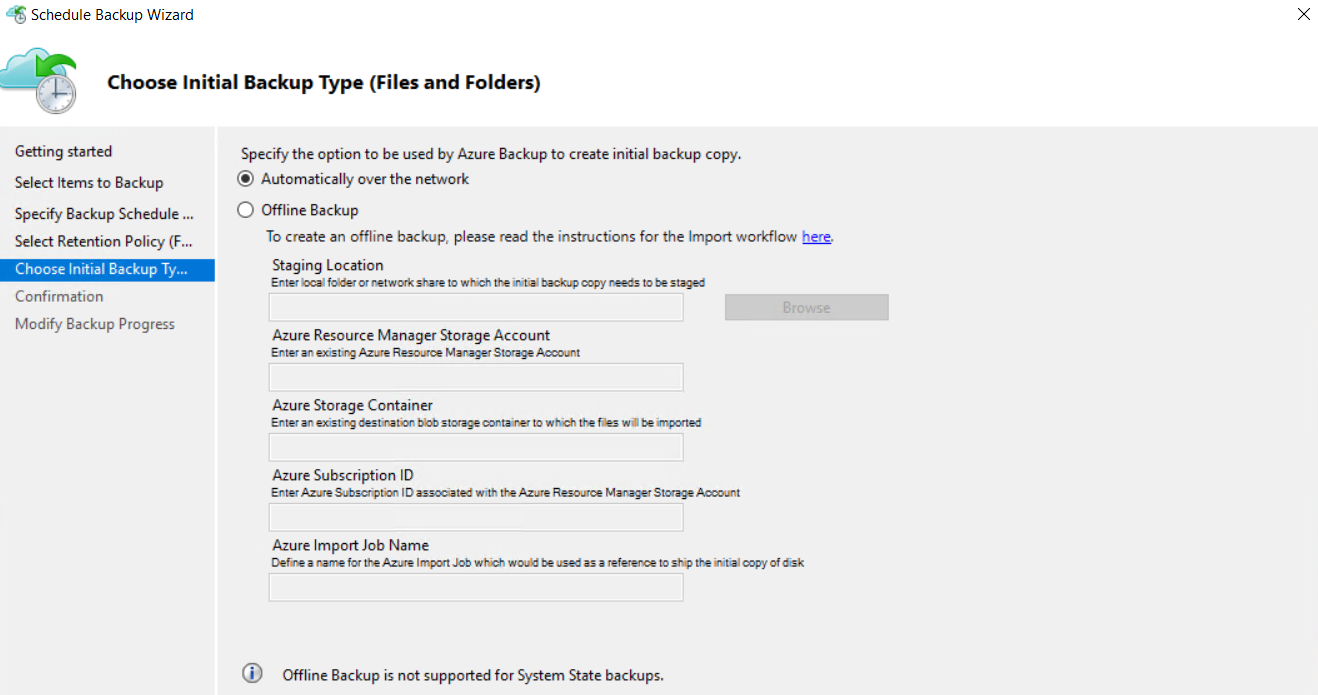


1. On the **Select Retention Policy** page, choose the specific retention policies the for the backup copy and click **Next**.

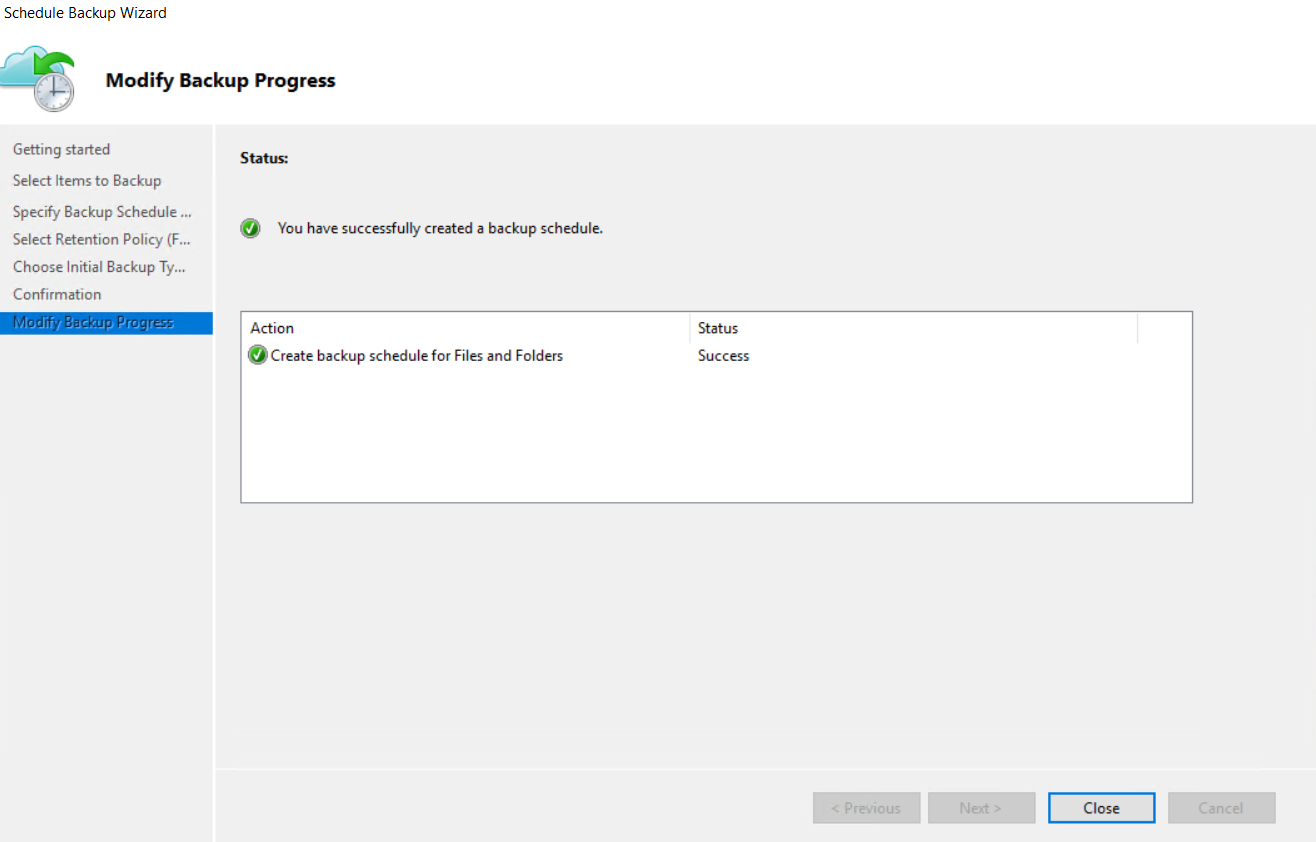


Note: The retention policy specifies the duration which the backup is stored. Rather than just specifying a “flat policy” for all backup points, you can specify different retention policies based on when the backup occurs. You can modify the daily, weekly, monthly, and yearly retention policies to meet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

1. Choose Initial Backup Type = Automatically over the Internet

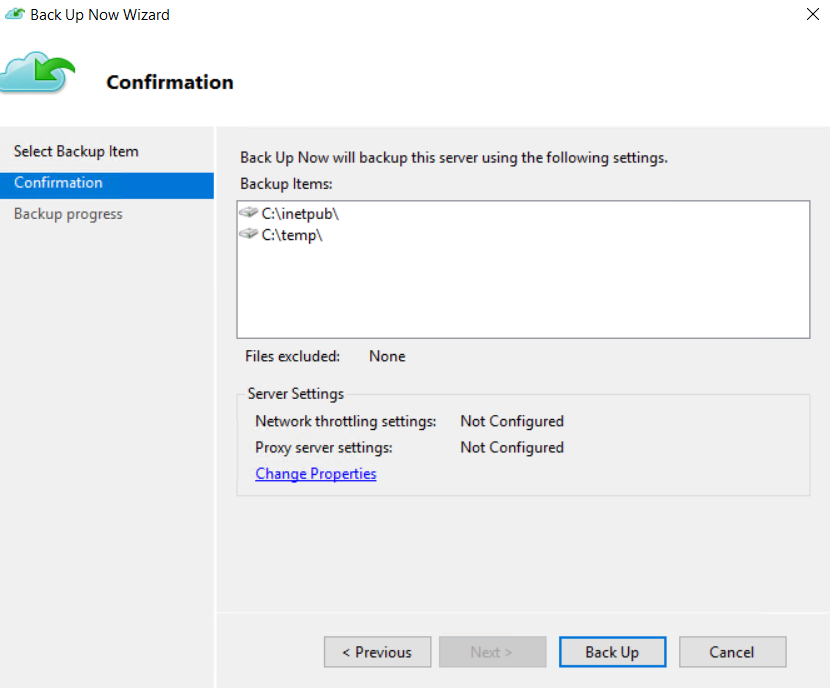


1. Click Finish to get the below screen



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

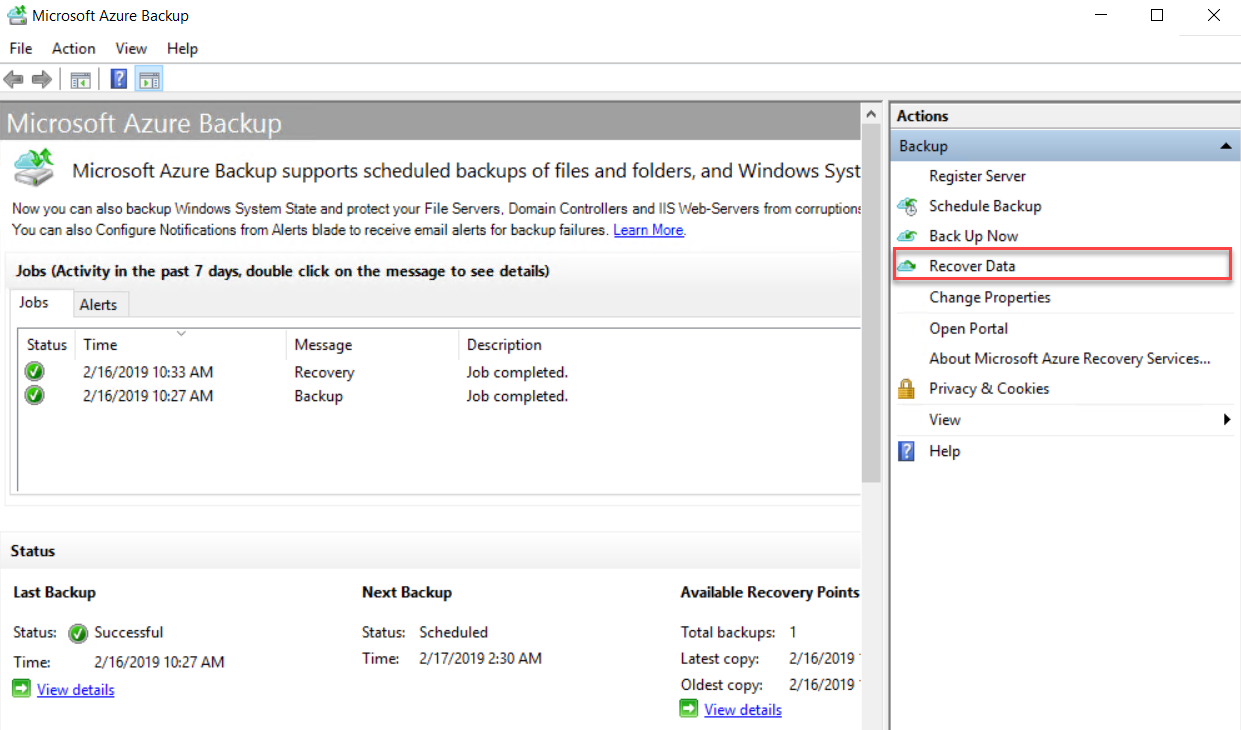
1. Actions pane 🡪 **Backup Now**
2. On the Confirmation page, review the settings that the Back Up Now Wizard will use to back up the machine. Then click **Back Up**.



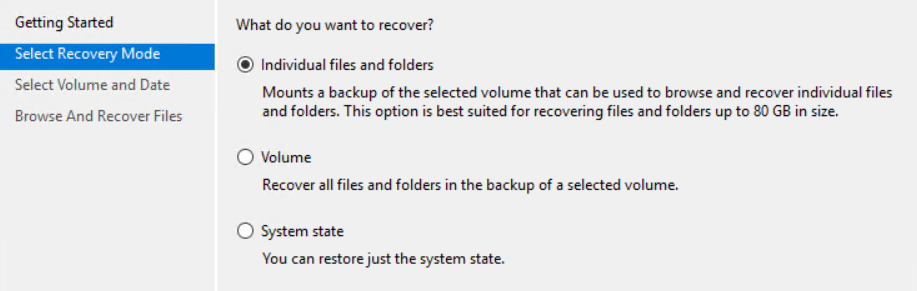
1. After the initial backup is completed, the **Job completed** status appears in the Backup console.

**Restore files from Azure to a Windows Server**

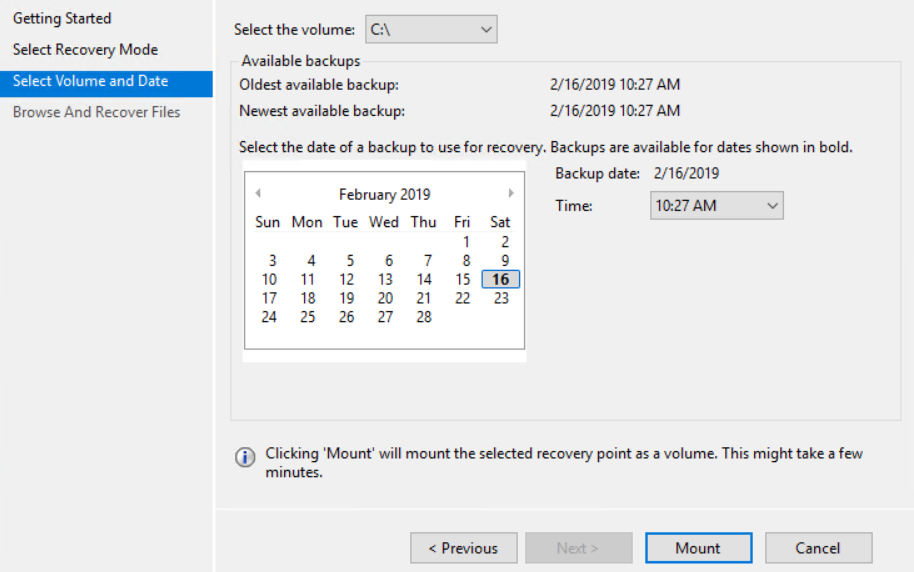
1. Open the **Microsoft Azure Backup** snap-in
2. click **Recover Data** in the **Actions Pane**



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



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



1. 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.
2. Note that when you click **Mount**, Azure Backup makes the recovery point available as a disk. Browse and recover files from the disk.
3. Once the recovery volume is mounted, click **Browse** to open Windows Explorer and find the files and folders you wish to recover.
4. 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**

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