

Contents

[Azure Backup documentation](#)

Overview

[Overview of Azure Backup](#)

[Pricing](#)

Quickstarts

[Back up a VM - Portal](#)

[Back up a VM - PowerShell](#)

[Back up a VM - CLI](#)

[Back up a VM - Resource Manager template](#)

Tutorials

[Back up Azure VMs at scale](#)

[Back up Azure VMs with PowerShell](#)

[Restore a disk](#)

[Restore individual files](#)

[Back up SQL Server on Azure VM](#)

[Back up SAP HANA databases in Azure VMs](#)

[Back up Azure Files file shares](#)

[Back up Windows Server](#)

[Restore files to Windows Server](#)

[SAP HANA databases on Azure VMs – using CLI](#)

[Backup SAP HANA databases - CLI](#)

[Restore SAP HANA databases - CLI](#)

[Manage backed up SAP HANA databases - CLI](#)

Concepts

[Support matrices](#)

[Azure Backup support matrix](#)

[Azure VM backup support matrix](#)

[DPM/Azure Backup Server \(MABS\) support matrix](#)

[MARS agent support matrix](#)

[SAP HANA Backup support matrix](#)

[Supported VM SKUs for Azure Policy](#)

[Frequently asked questions \(FAQ\)](#)

[FAQ-Recovery Services vaults](#)

[FAQ-Azure VM backup](#)

[FAQ-MARS agent](#)

[FAQ-Back up Azure Files](#)

[FAQ-Back up SQL Server databases on Azure VMs](#)

[FAQ-Back up SAP HANA databases on Azure VMs](#)

[FAQ-Azure Backup Server and DPM](#)

[FAQ-Azure Backup monitor alert](#)

[Backup architecture](#)

[How to guides](#)

[Recovery Services vault](#)

[Overview](#)

[Create](#)

[Delete](#)

[Move](#)

[Manage](#)

[Azure VM backup](#)

[Overview](#)

[Backup](#)

[Back up and restore Azure VMs with Azure Backup Instant Restore](#)

[Enable backup when you create an Azure VM](#)

[Back up an Azure VM from VM settings](#)

[Set up a vault and enable backup for Azure VMs](#)

[Back up encrypted Azure VMs](#)

[Configure app-consistent backups of Azure VMs running Linux](#)

[Restore](#)

[Restore Azure VMs in the portal](#)

[Recover files from Azure VM backups](#)

[Restore encrypted VMs](#)

- [Restore keys and secret for encrypted VMs](#)
- [Manage](#)
 - [Manage Azure VM backups](#)
 - [SQL Server database on Azure VM backup](#)
 - [Overview](#)
 - [Backup](#)
 - [Restore](#)
 - [Manage](#)
 - [Windows backup using MARS agent](#)
 - [Overview](#)
 - [Backup](#)
 - [Back up Windows Server files and folders](#)
 - [Back up Windows Server System State](#)
 - [Restore](#)
 - [Recover files from Azure to Windows Server](#)
 - [Restore Windows Server System State](#)
 - [Manage](#)
 - [Azure File share backup](#)
 - [From the Azure portal](#)
 - [Backup](#)
 - [Restore](#)
 - [Manage](#)
 - [With Azure CLI](#)
 - [Backup](#)
 - [Restore](#)
 - [Manage](#)
 - [With PowerShell](#)
 - [Backup](#)
 - [Restore](#)
 - [Manage](#)
 - [With REST API](#)
 - [Backup](#)

[Restore](#)

[Manage](#)

SAP HANA database on Azure VM backup

[Overview](#)

[Backup](#)

[Restore](#)

[Manage](#)

Azure Backup Server (MABS)

[Azure Backup Server protection matrix](#)

[Install or upgrade](#)

[Install Azure Backup Server](#)

[Add storage](#)

[What's New in MABS](#)

[Release notes MABS V3](#)

[Unattended installation](#)

[Protect workloads](#)

[Back up Hyper-V virtual machines](#)

[VMware server](#)

[Exchange](#)

[SharePoint farm](#)

[SQL Server](#)

[Protect system state and bare metal recovery](#)

[Recover data from Azure Backup Server](#)

[Restore VMware VMs with Azure Backup Server](#)

Azure Backup Server on Azure Stack

[Install Azure Backup Server](#)

[Protect files and applications](#)

[Protect SharePoint farm](#)

[Protect SQL Server database](#)

Data Protection Manager (DPM)

[Prepare DPM workloads in the Azure portal](#)

[Use DPM to back up Exchange server](#)

[Recover data to alternate DPM server](#)

[Use DPM to back up SQL Server workloads](#)

[Use DPM to back up a SharePoint farm](#)

[Replace your tape library](#)

[Offline backup](#)

[Overview](#)

[Offline Backup with Azure Data Box](#)

[Offline Backup with Import/Export \(MARS\)](#)

[Offline Backup with Import/Export \(DPM/MABS\)](#)

[Monitor and Alerts](#)

[Using Backup Explorer](#)

[Using the Azure portal](#)

[Using Azure Monitor](#)

[Reports](#)

[Configure Azure Backup reports](#)

[Configure Azure Backup reports](#)

[Configure Diagnostics Events for Recovery Services Vaults](#)

[Using Diagnostics Settings for Recovery Services Vaults](#)

[Log Analytics Data Model for Resource Specific Diagnostics Events](#)

[Log Analytics Data Model for Azure Backup \(Azure Diagnostics mode\)](#)

[Automation](#)

[Built-in Azure Policy for Azure Backup](#)

[Auto-Enable Backup on VM Creation using Azure Policy](#)

[Configure vault diagnostics settings at scale](#)

[PowerShell](#)

[Azure VMs in the Azure portal](#)

[DPM in the Azure portal](#)

[Windows Server in the Azure portal](#)

[SQL in Azure VM backups](#)

[Azure PowerShell Samples](#)

[Use Azure Backup REST API](#)

[Create Recovery Services vault](#)

[Update Recovery Services vault configurations](#)

[Create and update backup policy](#)

[Back up Azure VMs](#)

[Restore Azure VMs](#)

[Manage Azure Backup jobs](#)

[Resource Manager templates](#)

Security

[Role-Based Access Control](#)

[Security for cloud workloads](#)

[Security for hybrid backups](#)

[Built-in security controls](#)

Troubleshoot

[Azure VM](#)

[Azure Backup agent or VM extension timed out](#)

[Files and folders backup is slow](#)

[Azure Backup Server](#)

[System Center DPM](#)

[Azure Backup agent](#)

[Azure File share](#)

[SQL Server](#)

[SAP HANA backup in Azure VMs](#)

[System State](#)

Reference

[.NET](#)

[Azure CLI](#)

[PowerShell](#)

[REST - Backup](#)

[REST - Recovery Services vault](#)

[Resource Manager template](#)

Resources

[Azure Roadmap](#)

[MSDN forum](#)

[Pricing calculator](#)

[Service updates](#)

[Videos](#)

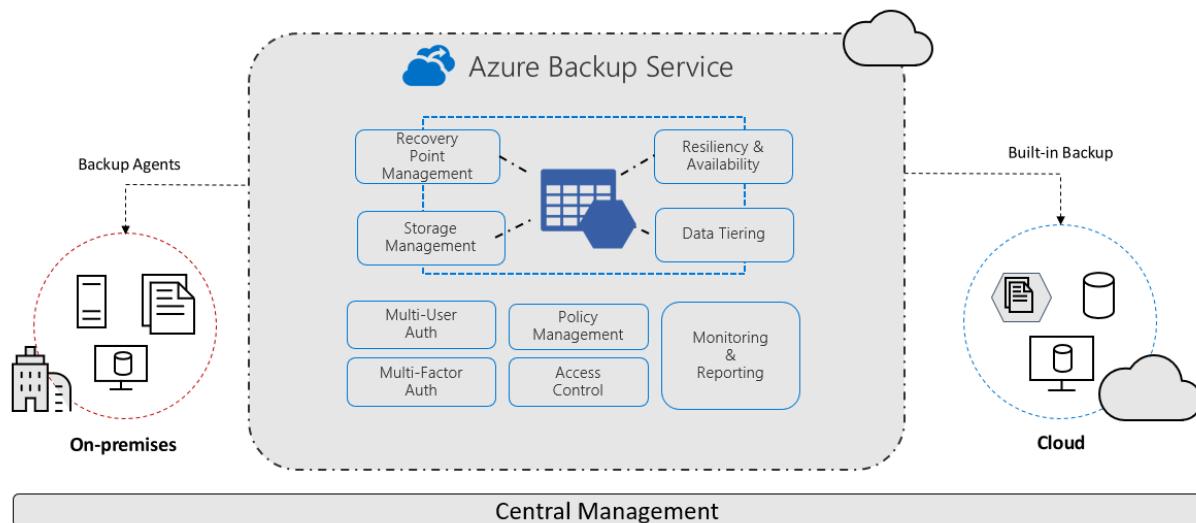
What is the Azure Backup service?

1/20/2020 • 3 minutes to read • [Edit Online](#)

The Azure Backup service provides simple, secure, and cost-effective solutions to back up your data and recover it from the Microsoft Azure cloud.

What can I 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 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



Why use Azure Backup?

Azure Backup delivers these key benefits:

- **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 a 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.
- **Scale easily** - Azure Backup uses the underlying power and unlimited scale of the Azure cloud to deliver high-availability with no maintenance or monitoring overhead.
- **Get unlimited data transfer:** Azure Backup doesn't limit the amount of inbound or outbound data you transfer, or charge for the data that is transferred.

- Outbound data refers to data transferred from a Recovery Services vault during a restore operation.
- If you perform an offline initial backup using the Azure Import/Export service to import large amounts of data, there's a cost associated with inbound data. [Learn more](#).
- **Keep data secure:** Azure Backup provides solutions for securing data [in transit](#) and [at rest](#).
- **Centralized monitoring and management:** Azure Backup provides [built-in monitoring and alerting capabilities](#) in a Recovery Services vault. These capabilities are available without any additional management infrastructure. You can also increase the scale of your monitoring and reporting by [using Azure Monitor](#).
- **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 additional 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 [Recovery Services vaults](#) for short-term and long-term data retention.
- **Automatic storage management** - Hybrid environments often require heterogeneous storage - some on-premises and some in the cloud. With Azure Backup, there's 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. So you only pay for the storage you consume. [Learn more](#) about pricing.
- **Multiple storage options** - Azure Backup offers two types of replication to keep your storage/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.

Next steps

- [Review](#) the architecture and components for different backup scenarios.
- [Verify](#) support requirements and limitations for backup, and for [Azure VM backup](#).

Back up a virtual machine in Azure

2/6/2020 • 3 minutes to read • [Edit Online](#)

Azure backups can be created through the Azure portal. This method provides a browser-based user interface to create and configure Azure backups and all related resources. You can protect your data by taking backups at regular intervals. Azure Backup creates recovery points that can be stored in geo-redundant recovery vaults. This article details how to back up a virtual machine (VM) with the Azure portal.

This quickstart enables backup on an existing Azure VM. If you need to create a VM, you can [create a VM with the Azure portal](#).

Sign in to Azure

Sign in to the [Azure portal](#).

Select a VM to back up

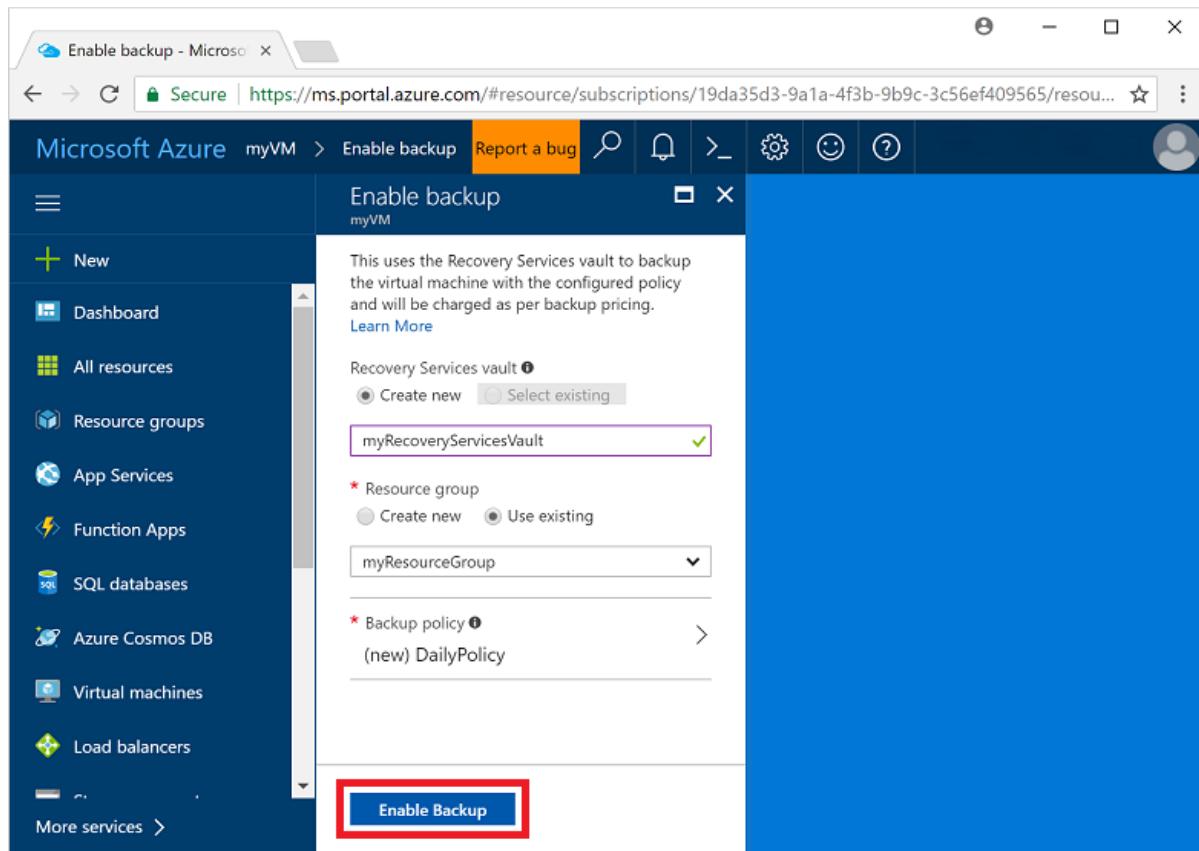
Create a simple scheduled daily backup to a Recovery Services Vault.

1. In the menu on the left, select **Virtual machines**.
2. From the list, choose a VM to back up. If you used the sample VM quickstart commands, the VM is named *myVM* in the *myResourceGroup* resource group.
3. In the **Operations** section, choose **Backup**. The **Enable backup** window opens.

Enable backup on a VM

A Recovery Services vault is a logical container that stores the backup data for each protected resource, such as Azure VMs. 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.

1. Select **Create new** and provide a name for the new vault, such as *myRecoveryServicesVault*.
2. If not already selected, choose **Use existing**, then select the resource group of your VM from the drop-down menu.



By default, the vault is set for Geo-Redundant storage. To further protect your data, this storage redundancy level ensures that your backup data is replicated to a secondary Azure region that is hundreds of miles away from the primary region.

You create and use policies to define when a backup job runs and how long the recovery points are stored. The default protection policy runs a backup job each day and retains recovery points for 30 days. You can use these default policy values to quickly protect your VM.

3. To accept the default backup policy values, select **Enable Backup**.

It takes a few moments to create the Recovery Services vault.

Start a backup job

You can start a backup now rather than wait for the default policy to run the job at the scheduled time. This first backup job creates a full recovery point. Each backup job after this initial backup creates incremental recovery points. Incremental recovery points are storage and time-efficient, as they only transfer changes made since the last backup.

1. On the **Backup** window for your VM, select **Backup now**.

The screenshot shows the Azure portal interface for a virtual machine named 'myVM'. The main header bar includes 'myVM - Backup' and 'Virtual machine' along with standard window controls. Below the header is a search bar labeled 'Search (Ctrl+ /)'. The top navigation bar contains 'Settings', 'Backup now' (which is highlighted with a red box), 'Restore VM', 'File Recovery', and 'Stop backup'. On the left side, there's a navigation menu with sections like 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'SETTINGS' (with 'Networking', 'Disks', 'Size', 'Availability set'), 'Configuration', and 'Backup' (which is highlighted with a red box). Under 'Backup', there's also an 'Extensions' option. The main content area is titled 'Essentials' and shows details about the recovery services vault ('myRecoveryServicesVault'), subscription name ('Visual Studio Enterprise'), subscription ID, item type ('Azure virtual machine'), last backup status ('Warning(Initial backup pending)'), and backup policy ('DailyPolicy'). It also displays 'Restore points' with counts for 'Last 30 days' (0) and 'Last 7 days' (0).

2. To accept the backup retention policy of 30 days, leave the default **Retain Backup Till** date. To start the job, select **Backup**.

Monitor the backup job

In the **Backup** window for your VM, the status of the backup and number of completed restore points are shown. Once the VM backup job is complete, information on the **Last backup time**, **Latest restore point**, and **Oldest restore point** is shown on the right-hand side of the **Overview** window.

Clean up deployment

When no longer needed, you can disable protection on the VM, remove the restore points and Recovery Services vault, then delete the resource group and associated VM resources

If you are going to continue on to a Backup tutorial that explains how to restore data for your VM, skip the steps in this section and go to [Next steps](#).

1. Select the **Backup** option for your VM.
2. Select **...More** to show additional options, then choose **Stop backup**.

The screenshot shows the 'myRecoveryServicesVault' settings page. At the top, there are buttons for 'Backup now', 'Restore VM', 'File Recovery', and 'More'. A red box highlights the 'More' button. Below it, under 'Essentials', there are several items:

- Subscription name: Visual Studio Enterprise
- Subscription ID
- Item type: Azure virtual machine
- Last backup status: Success
- Last backup: 9/18/2017, 9:01:00 PM (16 minute(s) ago)
- Latest restore point: 9/18/2017, 9:01:00 PM (16 minute(s) ago)
- Oldest restore point: 9/18/2017, 9:01:00 PM (16 minute(s) ago)
- Backup policy: DailyPolicy
- Backup Pre-Check: Passed

On the right side, there are buttons for 'Stop backup', 'Resume backup', and 'Delete backup data', with the 'Delete backup data' button also highlighted by a red box.

3. Select **Delete Backup Data** from the drop-down menu.
4. In the **Type the name of the Backup item** dialog, enter your VM name, such as *myVM*. Select **Stop Backup**.

Once the VM backup has been stopped and recovery points removed, you can delete the resource group. If you used an existing VM, you may wish to leave the resource group and VM in place.

5. In the menu on the left, select **Resource groups**.
6. From the list, choose your resource group. If you used the sample VM quickstart commands, the resource group is named *myResourceGroup*.
7. Select **Delete resource group**. To confirm, enter the resource group name, then select **Delete**.

The screenshot shows the 'myResourceGroup' blade. On the left, there's a navigation bar with 'Overview' selected. At the top, there are buttons for 'Add', 'Assign Tags', 'Columns', and a red box highlighting 'Delete resource group'. Below that, there's an 'Essentials' section with information about the subscription and deployments. At the bottom, there are filters for 'Filter by name...', 'All types', 'All locations', and 'No grouping'.

Next steps

In this quickstart, you created a Recovery Services vault, enabled protection on a VM, and created the initial recovery point. To learn more about Azure Backup and Recovery Services, continue to the tutorials.

[Back up multiple Azure VMs](#)

Back up a virtual machine in Azure with PowerShell

11/18/2019 • 4 minutes to read • [Edit Online](#)

The [Azure PowerShell AZ](#) module is used to create and manage Azure resources from the command line or in scripts.

[Azure Backup](#) backs up on-premises machines and apps, and Azure VMs. This article shows you how to back up an Azure VM with the AZ module. Alternatively, you can back up a VM using the [Azure CLI](#), or in the [Azure portal](#).

This quickstart enables backup on an existing Azure VM. If you need to create a VM, you can [create a VM with Azure PowerShell](#).

This quickstart requires the Azure PowerShell AZ module version 1.0.0 or later. Run `Get-Module -ListAvailable Az` to find the version. If you need to install or upgrade, see [Install Azure PowerShell module](#).

NOTE

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

Sign in and register

1. Sign in to your Azure subscription with the `Connect-AzAccount` command and follow the on-screen directions.

```
Connect-AzAccount
```

2. The first time you use Azure Backup, you must register the Azure Recovery Service provider in your subscription with [Register-AzResourceProvider](#), as follows:

```
Register-AzResourceProvider -ProviderNamespace "Microsoft.RecoveryServices"
```

Create a Recovery Services vault

A [Recovery Services vault](#) is a logical container that stores backup data for protected resources, such as Azure VMs. When a backup job 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.

When you create the vault:

- For the resource group and location, specify the resource group and location of the VM you want to back up.
- If you used this [sample script](#) to create the VM, the resource group is **myResourceGroup**, the VM is ***myVM**, and the resources are in the **WestEurope** region.
- Azure Backup automatically handles storage for backed up data. By default the vault uses [Geo-Redundant Storage \(GRS\)](#). Geo-redundancy ensures that backed up data is replicated to a secondary Azure region, hundreds of miles away from the primary region.

Now create a vault:

1. Use the [New-AzRecoveryServicesVault](#) to create the vault:

```
New-AzRecoveryServicesVault `  
    -ResourceGroupName "myResourceGroup" `  
    -Name "myRecoveryServicesVault" `  
    -Location "WestEurope"
```

2. Set the vault context with [Set-AzRecoveryServicesVaultContext](#), as follows:

```
Get-AzRecoveryServicesVault `  
    -Name "myRecoveryServicesVault" | Set-AzRecoveryServicesVaultContext
```

3. Change the storage redundancy configuration (LRS/GRS) of the vault with [Set-AzRecoveryServicesBackupProperty](#), as follows:

```
Get-AzRecoveryServicesVault `  
    -Name "myRecoveryServicesVault" | Set-AzRecoveryServicesBackupProperty -BackupStorageRedundancy  
LocallyRedundant/GeoRedundant
```

NOTE

Storage Redundancy can be modified only if there are no backup items protected to the vault.

Enable backup for an Azure VM

You enable backup for an Azure VM, and specify a backup policy.

- The policy defines when backups run, and how long recovery points created by the backups should be retained.
- The default protection policy runs a backup once a day for the VM, and retains the created recovery points for 30 days. You can use this default policy to quickly protect your VM.

Enable backup as follows:

1. First, set the default policy with [Get-AzRecoveryServicesBackupProtectionPolicy](#):

```
$policy = Get-AzRecoveryServicesBackupProtectionPolicy -Name "DefaultPolicy"
```

2. Enable VM backup with [Enable-AzRecoveryServicesBackupProtection](#). Specify the policy, the resource group, and the VM name.

```
Enable-AzRecoveryServicesBackupProtection `  
    -ResourceGroupName "myResourceGroup" `  
    -Name "myVM" `  
    -Policy $policy
```

Start a backup job

Backups run according to the schedule specified in the backup policy. You can also run an on-demand backup:

- The first initial backup job creates a full recovery point.
- After the initial backup, each backup job creates incremental recovery points.

- Incremental recovery points are storage and time-efficient, as they only transfer changes made since the last backup.

To run an on-demand backup, you use the [Backup-AzRecoveryServicesBackupItem](#).

- You specify a container in the vault that holds your backup data with [Get-AzRecoveryServicesBackupContainer](#).
- Each VM to back up is treated as an item. To start a backup job, you obtain information about the VM with [Get-AzRecoveryServicesBackupItem](#).

Run an on-demand backup job as follows:

1. Specify the container, obtain VM information, and run the backup.

```
$backupcontainer = Get-AzRecoveryServicesBackupContainer ` 
    -ContainerType "AzureVM" ` 
    -FriendlyName "myVM"

$item = Get-AzRecoveryServicesBackupItem ` 
    -Container $backupcontainer ` 
    -WorkloadType "AzureVM"

Backup-AzRecoveryServicesBackupItem -Item $item
```

2. You might need to wait up to 20 minutes, since the first backup job creates a full recovery point. Monitor the job as described in the next procedure.

Monitor the backup job

1. Run [Get-AzRecoveryServicesBackupJob](#) to monitor the job status.

```
Get-AzRecoveryServicesBackupJob
```

Output is similar to the following example, which shows the job as **InProgress**:

WorkloadName	Operation	Status	StartTime	EndTime	JobID
myvm	Backup	InProgress	9/18/2017 9:38:02 PM		9f9e8f14
myvm	ConfigureBackup	Completed	9/18/2017 9:33:18 PM	9/18/2017 9:33:51 PM	fe79c739

2. When the job status is **Completed**, the VM is protected and has a full recovery point stored.

Clean up the deployment

If you no longer need to back up the VM, you can clean it up.

- If you want to try out restoring the VM, skip the clean-up.
- If you used an existing VM, you can skip the final [Remove-AzResourceGroup](#) cmdlet to leave the resource group and VM in place.

Disable protection, remove the restore points and vault. Then delete the resource group and associated VM resources, as follows:

```
Disable-AzRecoveryServicesBackupProtection -Item $item -RemoveRecoveryPoints
$vault = Get-AzRecoveryServicesVault -Name "myRecoveryServicesVault"
Remove-AzRecoveryServicesVault -Vault $vault
Remove-AzResourceGroup -Name "myResourceGroup"
```

Next steps

In this quickstart, you created a Recovery Services vault, enabled protection on a VM, and created the initial recovery point.

- [Learn how](#) to back up VMs in the Azure portal.
- [Learn how](#) to quickly restore a VM

Back up a virtual machine in Azure with the CLI

11/18/2019 • 5 minutes to read • [Edit Online](#)

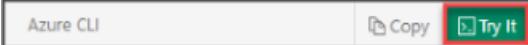
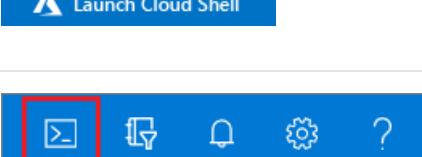
The Azure CLI is used to create and manage Azure resources from the command line or in scripts. You can protect your data by taking backups at regular intervals. Azure Backup creates recovery points that can be stored in geo-redundant recovery vaults. This article details how to back up a virtual machine (VM) in Azure with the Azure CLI. You can also perform these steps with [Azure PowerShell](#) or in the [Azure portal](#).

This quickstart enables backup on an existing Azure VM. If you need to create a VM, you can [create a VM with the Azure CLI](#).

Use Azure Cloud Shell

Azure hosts Azure Cloud Shell, an interactive shell environment that you can use through your browser. You can use either Bash or PowerShell with Cloud Shell to work with Azure services. You can use the Cloud Shell preinstalled commands to run the code in this article without having to install anything on your local environment.

To start Azure Cloud Shell:

OPTION	EXAMPLE/LINK
Select Try It in the upper-right corner of a code block. Selecting Try It doesn't automatically copy the code to Cloud Shell.	
Go to https://shell.azure.com , or select the Launch Cloud Shell button to open Cloud Shell in your browser.	
Select the Cloud Shell button on the menu bar at the upper right in the Azure portal .	

To run the code in this article in Azure Cloud Shell:

1. Start Cloud Shell.
2. Select the **Copy** button on a code block to copy the code.
3. Paste the code into the Cloud Shell session by selecting **Ctrl+Shift+V** on Windows and Linux or by selecting **Cmd+Shift+V** on macOS.
4. Select **Enter** to run the code.

To install and use the CLI locally, you must run Azure CLI version 2.0.18 or later. To find the CLI version, run `az --version`. If you need to install or upgrade, see [Install the Azure CLI](#).

Create a recovery services vault

A Recovery Services vault is a logical container that stores the backup data for each protected resource, such as Azure VMs. 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.

Create a Recovery Services vault with [az backup vault create](#). Specify the same resource group and location as the VM you wish to protect. If you used the [VM quickstart](#), then you created:

- a resource group named *myResourceGroup*,
- a VM named *myVM*,
- resources in the *eastus* location.

```
az backup vault create --resource-group myResourceGroup \
--name myRecoveryServicesVault \
--location eastus
```

By default, the Recovery Services vault is set for Geo-Redundant storage. Geo-Redundant storage ensures your backup data is replicated to a secondary Azure region that is hundreds of miles away from the primary region. If the storage redundancy setting needs to be modified, use [az backup vault backup-properties set](#) cmdlet.

```
az backup vault backup-properties set \
--name myRecoveryServicesVault \
--resource-group myResourceGroup \
--backup-storage-redundancy "LocallyRedundant/GeoRedundant"
```

Enable backup for an Azure VM

Create a protection policy to define: when a backup job runs, and how long the recovery points are stored. The default protection policy runs a backup job each day and retains recovery points for 30 days. You can use these default policy values to quickly protect your VM. To enable backup protection for a VM, use [az backup protection enable-for-vm](#). Specify the resource group and VM to protect, then the policy to use:

```
az backup protection enable-for-vm \
--resource-group myResourceGroup \
--vault-name myRecoveryServicesVault \
--vm myVM \
--policy-name DefaultPolicy
```

NOTE

If the VM is not in the same resource group as that of vault, then *myResourceGroup* refers to the resource group where vault was created. Instead of VM name, provide the VM ID as indicated below.

```
az backup protection enable-for-vm \
--resource-group myResourceGroup \
--vault-name myRecoveryServicesVault \
--vm $(az vm show -g VMResourceGroup -n MyVm --query id | tr -d '') \
--policy-name DefaultPolicy
```

IMPORTANT

While using CLI to enable backup for multiple VMs at once, ensure that a single policy doesn't have more than 100 VMs associated with it. This is a [recommended best practice](#). Currently, the PS client doesn't explicitly block if there are more than 100 VMs but the check is planned to be added in the future.

Start a backup job

To start a backup now rather than wait for the default policy to run the job at the scheduled time, use [az backup protection backup-now](#). This first backup job creates a full recovery point. Each backup job after this initial backup

creates incremental recovery points. Incremental recovery points are storage and time-efficient, as they only transfer changes made since the last backup.

The following parameters are used to back up the VM:

- `--container-name` is the name of your VM
- `--item-name` is the name of your VM
- `--retain-until` value should be set to the last available date, in UTC time format (**dd-mm-yyyy**), that you wish the recovery point to be available

The following example backs up the VM named *myVM* and sets the expiration of the recovery point to October 18, 2017:

```
az backup protection backup-now \
    --resource-group myResourceGroup \
    --vault-name myRecoveryServicesVault \
    --container-name myVM \
    --item-name myVM \
    --retain-until 18-10-2017
```

Monitor the backup job

To monitor the status of backup jobs, use [az backup job list](#):

```
az backup job list \
    --resource-group myResourceGroup \
    --vault-name myRecoveryServicesVault \
    --output table
```

The output is similar to the following example, which shows the backup job is *InProgress*:

Name	Operation	Status	Item Name	Start Time UTC	Duration
a0a8e5e6	Backup	InProgress	myvm	2017-09-19T03:09:21	0:00:48.718366
fe5d0414	ConfigureBackup	Completed	myvm	2017-09-19T03:03:57	0:00:31.191807

When the *Status* of the backup job reports *Completed*, your VM is protected with Recovery Services and has a full recovery point stored.

Clean up deployment

When no longer needed, you can disable protection on the VM, remove the restore points and Recovery Services vault, then delete the resource group and associated VM resources. If you used an existing VM, you can skip the final [az group delete](#) command to leave the resource group and VM in place.

If you want to try a Backup tutorial that explains how to restore data for your VM, go to [Next steps](#).

```
az backup protection disable \
--resource-group myResourceGroup \
--vault-name myRecoveryServicesVault \
--container-name myVM \
--item-name myVM \
--delete-backup-data true
az backup vault delete \
--resource-group myResourceGroup \
--name myRecoveryServicesVault \
az group delete --name myResourceGroup
```

Next steps

In this quickstart, you created a Recovery Services vault, enabled protection on a VM, and created the initial recovery point. To learn more about Azure Backup and Recovery Services, continue to the tutorials.

[Back up multiple Azure VMs](#)

Back up a virtual machine in Azure with Resource Manager template

1/14/2020 • 2 minutes to read • [Edit Online](#)

Azure Backup backs up on-premises machines and apps, and Azure VMs. This article shows you how to back up an Azure VM with Resource Manager template and Azure PowerShell. This quickstart focuses on the process of deploying a Resource Manager template to create a Recover Services vault. For more information on developing Resource Manager templates, see [Resource Manager documentation](#) and the [template reference](#).

Alternatively, you can back up a VM using [Azure PowerShell](#), the [Azure CLI](#), or in the [Azure portal](#).

Create a VM and Recovery Services vault

A [Recovery Services vault](#) is a logical container that stores backup data for protected resources, such as Azure VMs. When a backup job 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.

The template used in this quickstart is from [Azure quickstart templates](#). This template allows you to deploy simple Windows VM and Recovery Services Vault configured with the DefaultPolicy for Protection.

To deploy the template, select **Try it** to open the Azure Cloud shell, and then paste the following PowerShell script into the shell window. To paste the code, right-click the shell window and then select **Paste**.

```
$projectName = Read-Host -Prompt "Enter a project name (limited to eight characters) that is used to generate Azure resource names"
$location = Read-Host -Prompt "Enter the location (i.e. centralus)"
$adminUsername = Read-Host -Prompt "Enter the administrator username for the virtual machine"
$adminPassword = Read-Host -Prompt "Enter the administrator password for the virtual machine" -AsSecureString
$dnsPrefix = Read-Host -Prompt "Enter the unique DNS Name for the Public IP used to access the virtual machine"

$resourceGroupName = "${projectName}rg"
$templateUri = "https://raw.githubusercontent.com/Azure/azure-quickstart-templates/master/101-recovery-services-create-vm-and-configure-backup/azuredeploy.json"

New-AzResourceGroup -Name $resourceGroupName -Location $location
New-AzResourceGroupDeployment -ResourceGroupName $resourceGroupName -TemplateUri $templateUri - projectName
$projectName -adminUsername $adminUsername -adminPassword $adminPassword -dnsLabelPrefix $dnsPrefix
```

Azure PowerShell is used to deploy the Resource Manager template in this quickstart. The [Azure portal](#), [Azure CLI](#), and [Rest API](#) can also be used to deploy templates.

Start a backup job

The template creates a VM and enables back on the VM. After you deploy the template, you need to start a backup job. For more information, see [Start a backup job](#).

Monitor the backup job

To monitor the backup job, see [Monitor the backup job](#).

Clean up the deployment

If you no longer need to back up the VM, you can clean it up.

- If you want to try out restoring the VM, skip the cleanup.
- If you used an existing VM, you can skip the final `Remove-AzResourceGroup` cmdlet to leave the resource group and VM in place.

Disable protection, remove the restore points and vault. Then delete the resource group and associated VM resources, as follows:

```
Disable-AzRecoveryServicesBackupProtection -Item $item -RemoveRecoveryPoints  
$vault = Get-AzRecoveryServicesVault -Name "myRecoveryServicesVault"  
Remove-AzRecoveryServicesVault -Vault $vault  
Remove-AzResourceGroup -Name "myResourceGroup"
```

Next steps

In this quickstart, you created a Recovery Services vault, enabled protection on a VM, and created the initial recovery point.

- [Learn how](#) to back up VMs in the Azure portal.
- [Learn how](#) to quickly restore a VM

Use Azure portal to back up multiple virtual machines

11/18/2019 • 6 minutes to read • [Edit Online](#)

When you back up data in Azure, you store that data in an Azure resource called a Recovery Services vault. The Recovery Services vault resource is available from the Settings menu of most Azure services. The benefit of having the Recovery Services vault integrated into the Settings menu of most Azure services makes it easy to back up data. However, individually working with each database or virtual machine in your business is tedious. What if you want to back up the data for all virtual machines in one department, or in one location? It is easy to back up multiple virtual machines by creating a backup policy and applying that policy to the desired virtual machines. This tutorial explains how to:

- Create a Recovery Services vault
- Define a backup policy
- Apply the backup policy to protect multiple virtual machines
- Trigger an on-demand backup job for the protected virtual machines

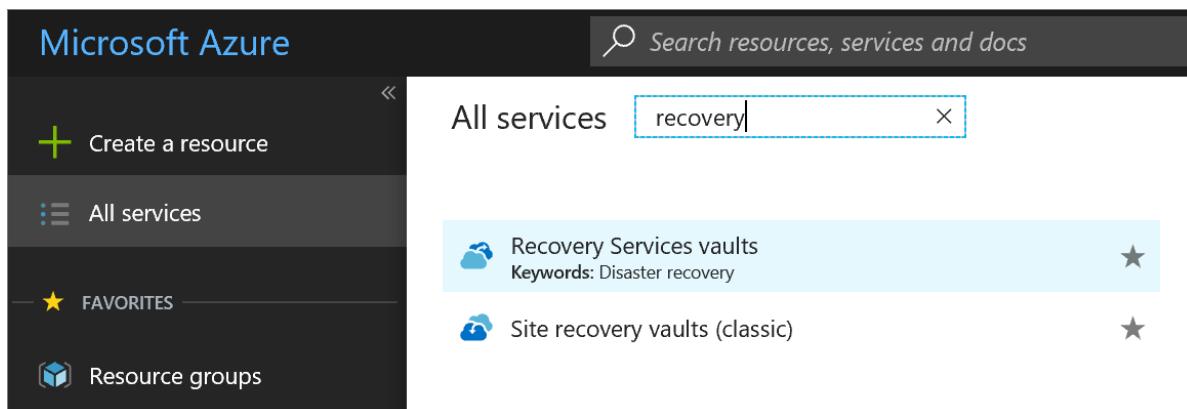
Sign in to the Azure portal

Sign in to the [Azure portal](#).

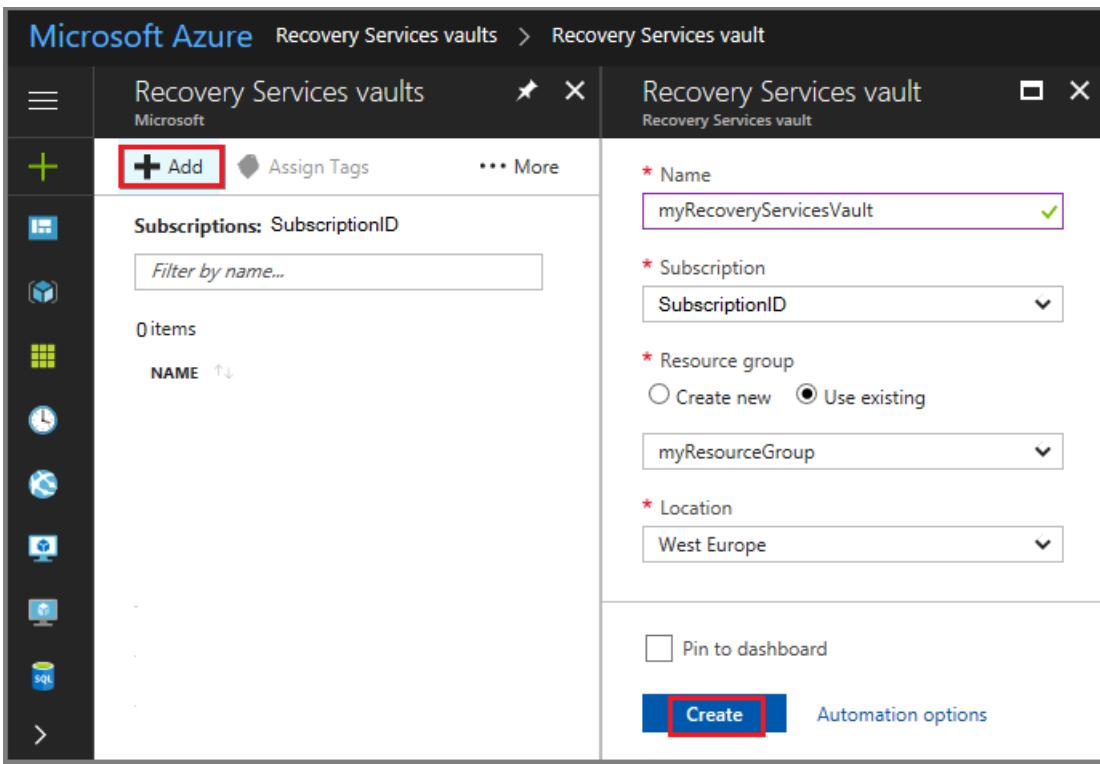
Create a Recovery Services vault

The Recovery Services vault contains the backup data, and the backup policy applied to the protected virtual machines. 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. So, for each Azure location that has virtual machines to be backed up, at least one Recovery Services vault must exist in that location.

1. On the left-hand menu, select **All services** and in the services list, type *Recovery Services*. As you type, the list of resources filters. When you see Recovery Services vaults in the list, select it to open the Recovery Services vaults menu.



2. In the **Recovery Services vaults** menu, click **Add** to open the Recovery Services vault menu.



3. In the Recovery Services vault menu,

- Type *myRecoveryServicesVault* in **Name**.
- The current subscription ID appears in **Subscription**. If you have additional subscriptions, you could choose another subscription for the new vault.
- For **Resource group**, select **Use existing** and choose *myResourceGroup*. If *myResourceGroup* doesn't exist, select **Create new** and type *myResourceGroup*.
- From the **Location** drop-down menu, choose *West Europe*.
- Click **Create** to create your Recovery Services vault.

A Recovery Services vault must be in the same location as the virtual machines being protected. If you have virtual machines in multiple regions, create a Recovery Services vault in each region. This tutorial creates a Recovery Services vault in *West Europe* because that is where *myVM* (the virtual machine created with the quickstart) was created.

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.

When you create a Recovery Services vault, by default the vault has geo-redundant storage. To provide data resiliency, geo-redundant storage replicates the data multiple times across two Azure regions.

Set backup policy to protect VMs

After creating the Recovery Services vault, the next step is to configure the vault for the type of data, and to set the backup policy. Backup policy is the schedule for how often and when recovery points are taken. Policy also includes the retention range for the recovery points. For this tutorial, let's assume your business is a sports complex with a hotel, stadium, and restaurants and concessions, and you are protecting the data on the virtual machines. The following steps create a backup policy for the financial data.

1. From the list of Recovery Services vaults, select **myRecoveryServicesVault** to open its dashboard.

The image shows two side-by-side Azure dashboard windows. The left window, titled 'Recovery Services vaults', lists 'myRecoveryServicesVault' and 'Contoso-vault'. The right window, titled 'myRecoveryServicesVault Recovery Services vault', has a 'Backup' button highlighted with a red box. It displays 'Resource group (change) myResourceGroup', 'Status Active', 'Location West Europe', and 'Subscription name (change) MSDNNonDallas'. The 'Backup items' section shows 0 backup items and 0 backup management servers. The 'Monitoring' section shows 0 critical and 0 warning backup alerts. A circular gauge indicates 0 total backup pre-check status.

2. On the vault dashboard menu, click **Backup** to open the Backup menu.
3. On the Backup Goal menu, in the **Where is your workload running?** drop-down menu, choose *Azure*. From the **What do you want to backup?** drop-down, choose *Virtual machine*, and click **Backup**.

These actions prepare the Recovery Services vault for interacting with a virtual machine. Recovery Services vaults have a default policy that creates a restore point each day, and retains the restore points for 30 days.

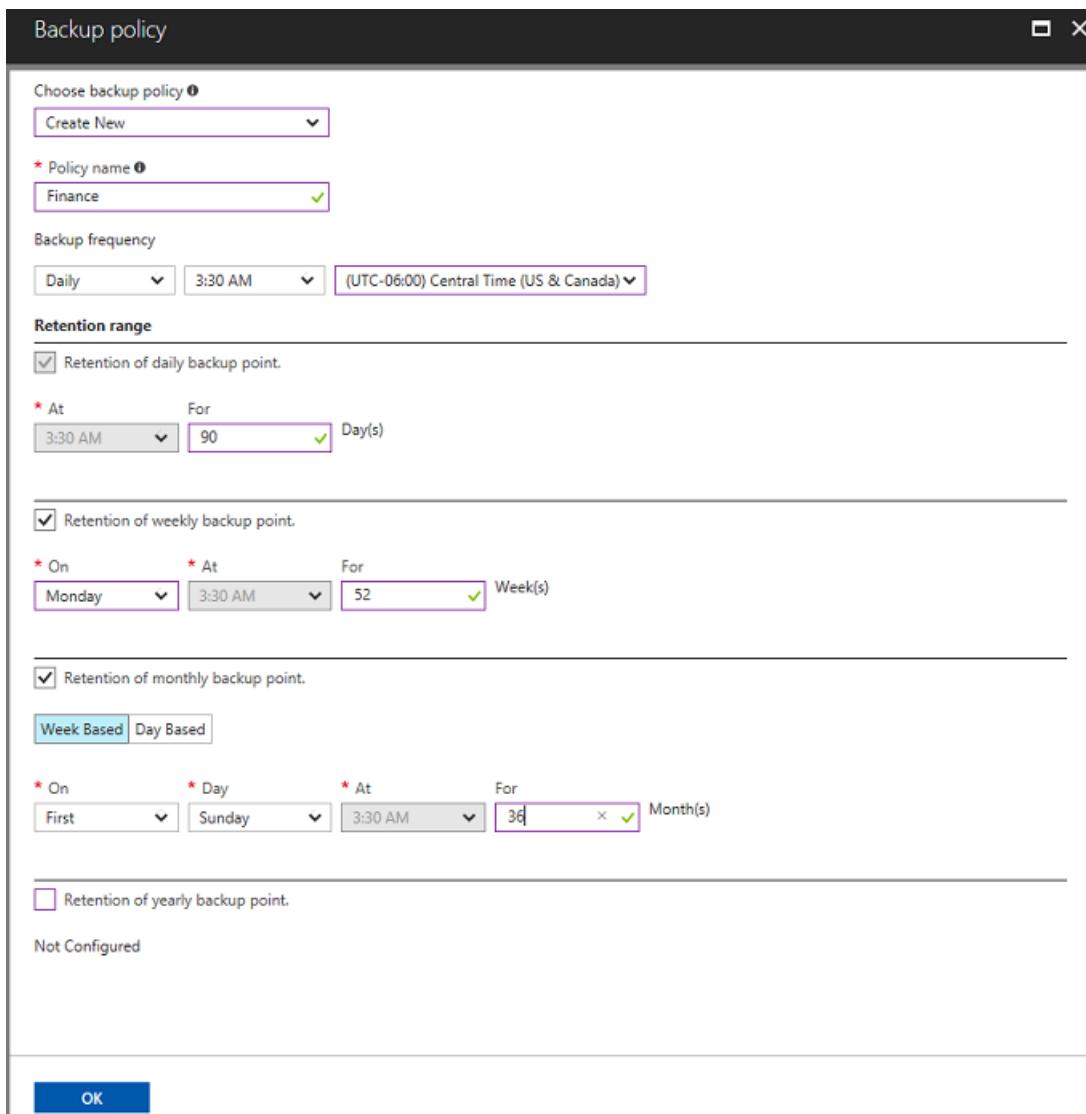
The 'Backup Goal' dialog shows 'Where is your workload running?' set to 'Azure' and 'What do you want to backup?' set to 'Virtual machine'. Below, under 'Step: Configure Backup', the 'Backup' button is highlighted with a red box.

4. To create a new policy, on the Backup policy menu, from the **Choose backup policy** drop-down menu, select *Create New*.

The 'Backup policy' dialog shows 'Choose backup policy' with 'DefaultPolicy' selected. Below, 'Create New' is highlighted with a red box. Under 'RETENTION RANGE', it says 'Daily at 1:00 AM'. In the 'Retention of daily backup point' section, it says 'Retain backup taken every day at 1:00 AM for 30 Day(s)'. At the bottom is an 'OK' button.

5. In the **Backup policy** menu, for **Policy Name** type *Finance*. Enter the following changes for the Backup policy:

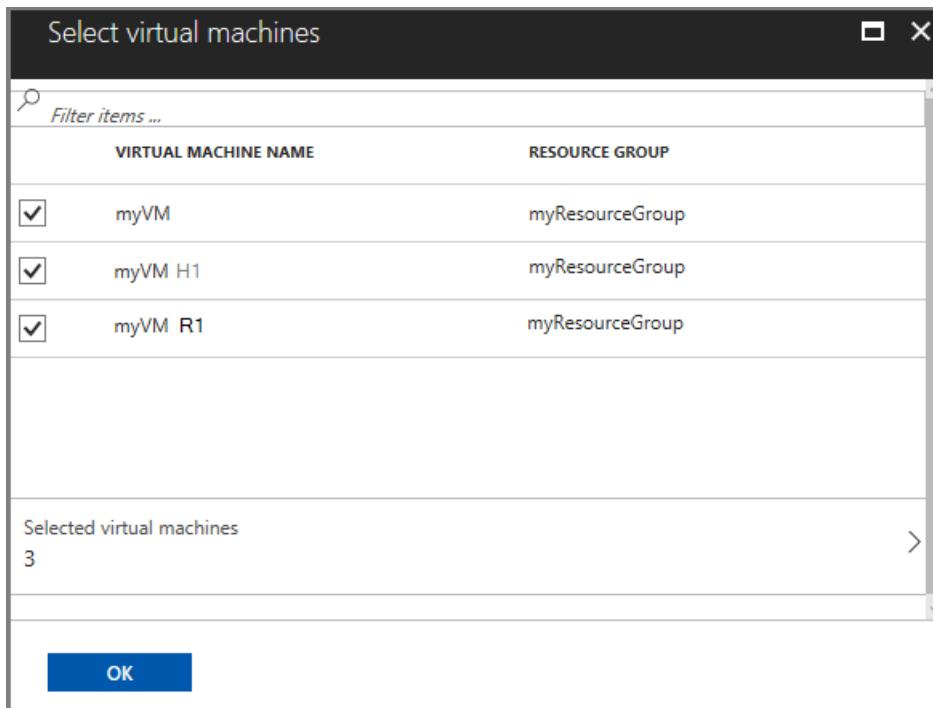
- For **Backup frequency** set the timezone for *Central Time*. Since the sports complex is in Texas, the owner wants the timing to be local. Leave the backup frequency set to Daily at 3:30AM.
- For **Retention of daily backup point**, set the period to 90 days.
- For **Retention of weekly backup point**, use the *Monday* restore point and retain it for 52 weeks.
- For **Retention of monthly backup point**, use the restore point from First Sunday of the month, and retain it for 36 months.
- Deselect the **Retention of yearly backup point** option. The leader of Finance doesn't want to keep data longer than 36 months.
- Click **OK** to create the backup policy.



After creating the backup policy, associate the policy with the virtual machines.

6. In the **Select virtual machines** dialog, select *myVM* and click **OK** to deploy the backup policy to the virtual machines.

All virtual machines that are in the same location, and are not already associated with a backup policy, appear. *myVMH1* and *myVMR1* are selected to be associated with the *Finance* policy.



When the deployment completes, you receive a notification that deployment successfully completed.

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.

To run an on-demand backup job:

1. On the vault dashboard, click **3** under **Backup Items**, to open the Backup Items menu.

The **Backup Items** menu opens.

2. On the **Backup Items** menu, click **Azure Virtual Machine** to open the list of virtual machines associated with the vault.

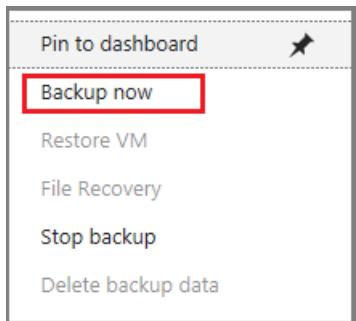
BACKUP MANAGEMENT TYPE	BACKUP ITEM COUNT
Azure Virtual Machine	3
Azure Backup Agent	0
Azure Backup Server	0

The **Backup Items** list opens.

NAME	RESOURCE GROUP	BACKUP PRE-CHECK	LAST BACKUP STATUS	LATEST RESTORE POINT	Context menu
myVM	myResourceGroup	Passed	Warning(Initial backu...)
buntu	rasquill-security	Passed	Warning(Initial backu...)
ops	rhelfiles	Passed	Warning(Initial backu...)

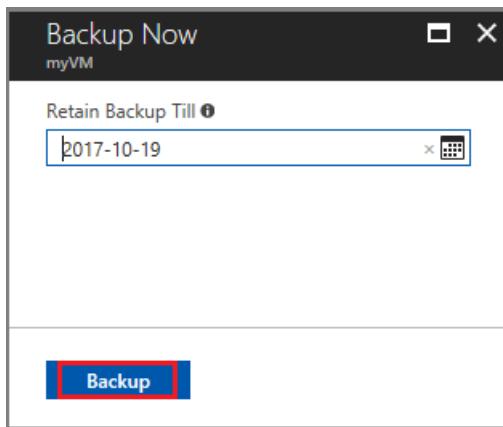
3. On the **Backup Items** list, click the ellipses **...** to open the Context menu.

4. On the Context menu, select **Backup now**.



The Backup Now menu opens.

5. On the Backup Now menu, enter the last day to retain the recovery point, and click **Backup**.



Deployment notifications let you know the backup job has been triggered, and that you can monitor the progress of the job on the Backup jobs page. Depending on the size of your virtual machine, creating the initial backup may take a while.

When the initial backup job completes, you can see its status in the Backup job menu. The on-demand backup job created the initial restore point for *myVM*. If you want to back up other virtual machines, repeat these steps for each virtual machine.

NAME	RESOURCE GROUP	BACKUP PRE-CHECK	LAST BACKUP STATUS	LATEST RESTORE POINT	...
myVM	myResourceGroup	Passed	Success	9/19/2017 6:52:32 PM	...

Clean up resources

If you plan to continue on to work with subsequent tutorials, do not clean up the resources created in this tutorial. If you do not plan to continue, use the following steps to delete all resources created by this tutorial in the Azure portal.

1. On the **myRecoveryServicesVault** dashboard, click **3** under **Backup Items**, to open the Backup Items menu.

The screenshot shows the Azure Recovery Services vault interface for 'myRecoveryServicesVault'. The left sidebar contains a navigation menu with various options such as Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Properties, Locks, Automation script, Backup, Site Recovery, Jobs, Alerts and Events, and Backup Reports. The main content area is titled 'Overview' and includes sections for 'Essentials' and 'Monitoring'. In the 'Essentials' section, it shows a resource group named 'myResourceGroup' with a status of 'Active', located in 'West Europe', and associated with a 'Subscription name' of 'subscriptionID'. It also displays 'Backup items' (3), 'Backup management servers' (0), and 'Replicated items' (0). The 'Monitoring' section provides a summary of backup alerts and pre-check status for Azure VMs, both of which show 0 critical and 0 warning levels.

2. On the **Backup Items** menu, click **Azure Virtual Machine** to open the list of virtual machines associated with the vault.

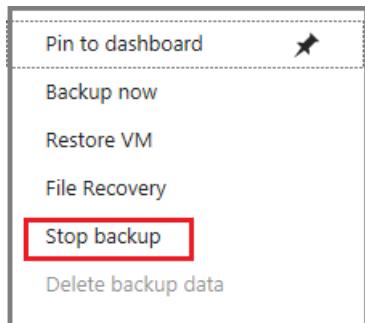
BACKUP MANAGEMENT TYPE	BACKUP ITEM COUNT
Azure Virtual Machine	3
Azure Backup Agent	0
Azure Backup Server	0

The **Backup Items** list opens.

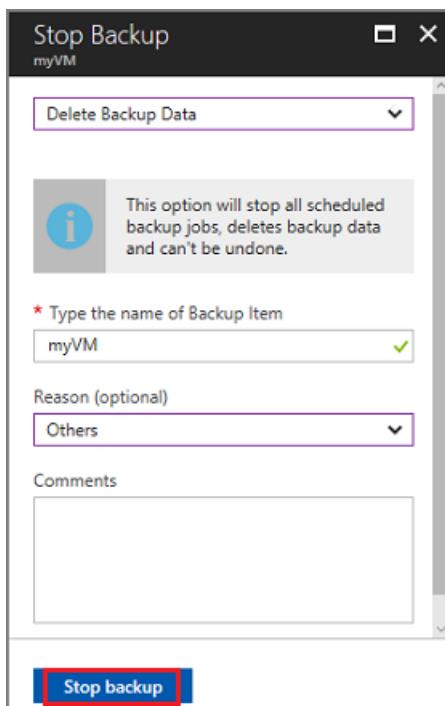
3. In the **Backup Items** menu, click the ellipsis to open the Context menu.

Backup Items (Azure Virtual Machine)						
myRecoveryServicesVault						
Actions		Items				
NAME	RESOURCE GROUP	BACKUP PRE-CHECK	LAST BACKUP STATUS	LATEST RESTORE POINT		
myVM	myResourceGroup	Passed	Success	9/19/2017 6:22:37 PM	...	
myVM H1	myResourceGroup	Passed	Success	9/19/2017 6:32:35 PM	...	
myVM R1	myResourceGroup	Passed	Success	9/19/2017 6:56:17 PM	...	

4. On the context menu, select **Stop backup** to open Stop Backup menu.



5. In the **Stop Backup** menu, select the upper drop-down menu and choose **Delete Backup Data**.
6. In the **Type the name of the Backup item** dialog, type *myVM*.
7. Once the backup item is verified (a check mark appears), **Stop backup** button is enabled. Click **Stop Backup** to stop the policy and delete the restore points.



8. In the **myRecoveryServicesVault** menu, click **Delete**.

The screenshot shows the Azure Recovery Services vault interface for 'myRecoveryServicesVault'. The 'Delete' button in the top navigation bar is highlighted with a red box. The main content area displays an 'Essentials' summary with the following data:

Resource group (change)	Backup items
myResourceGroup	0
Status	Backup management servers
Active	0

Once the vault is deleted, you return to the list of Recovery Services vaults.

Next steps

In this tutorial, you used the Azure portal to:

- Create a Recovery Services vault
- Set the vault to protect virtual machines
- Create a custom backup and retention policy
- Assign the policy to protect multiple virtual machines
- Trigger an on-demand back up for virtual machines

Continue to the next tutorial to restore an Azure virtual machine from disk.

[Restore VMs using CLI](#)

Back up Azure VMs with PowerShell

11/18/2019 • 3 minutes to read • [Edit Online](#)

NOTE

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

This tutorial describes how to deploy an [Azure Backup](#) Recovery Services vault to back up multiple Azure VMs using PowerShell.

In this tutorial you learn how to:

- Create a Recovery Services vault and set the vault context.
- Define a backup policy
- Apply the backup policy to protect multiple virtual machines
- Trigger an on-demand backup job for the protected virtual machines Before you can back up (or protect) a virtual machine, you must complete the [prerequisites](#) to prepare your environment for protecting your VMs.

IMPORTANT

This tutorial assumes you have already created a resource group and an Azure virtual machine.

Sign in and register

1. Sign in to your Azure subscription with the `Connect-AzAccount` command and follow the on-screen directions.

```
Connect-AzAccount
```

2. The first time you use Azure Backup, you must register the Azure Recovery Service provider in your subscription with [Register-AzResourceProvider](#). If you've already registered, skip this step.

```
Register-AzResourceProvider -ProviderNamespace "Microsoft.RecoveryServices"
```

Create a Recovery Services vault

A [Recovery Services vault](#) is a logical container that stores backup data for protected resources, such as Azure VMs. When a backup job 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.

- In this tutorial, you create the vault in the same resource group and location as the VM you want to back up.
- Azure Backup automatically handles storage for backed up data. By default the vault uses [Geo-Redundant Storage \(GRS\)](#). Geo-redundancy ensures that backed up data is replicated to a secondary Azure region, hundreds of miles away from the primary region.

Create the vault as follows:

1. Use the [New-AzRecoveryServicesVault](#)to create the vault. Specify the resource group name and location of the VM you want to back up.

```
New-AzRecoveryServicesVault -Name myRSVault -ResourceGroupName "myResourceGroup" -Location "EastUS"
```

2. Many Azure Backup cmdlets require the Recovery Services vault object as an input. For this reason, it is convenient to store the Backup Recovery Services vault object in a variable.

```
$vault1 = Get-AzRecoveryServicesVault -Name myRSVault
```

3. Set the vault context with [Set-AzRecoveryServicesVaultContext](#).

- The vault context is the type of data protected in the vault.
- Once the context is set, it applies to all subsequent cmdlets

```
Get-AzRecoveryServicesVault -Name "myRSVault" | Set-AzRecoveryServicesVaultContext
```

Back up Azure VMs

Backups run in accordance with the schedule specified in the backup policy. When you create a Recovery Services vault, it comes with default protection and retention policies.

- The default protection policy triggers a backup job once a day at a specified time.
- The default retention policy retains the daily recovery point for 30 days.

To enable and backup up the Azure VM in this tutorial, we do the following:

1. Specify a container in the vault that holds your backup data with [Get-AzRecoveryServicesBackupContainer](#).
2. Each VM for backup is an item. To start a backup job, you obtain information about the VM with [Get-AzRecoveryServicesBackupItem](#).
3. Run an on-demand backup with[Backup-AzRecoveryServicesBackupItem](#).
 - The first initial backup job creates a full recovery point.
 - After the initial backup, each backup job creates incremental recovery points.
 - Incremental recovery points are storage and time-efficient, as they only transfer changes made since the last backup.

Enable and run the backup as follows:

```
$namedContainer = Get-AzRecoveryServicesBackupContainer -ContainerType AzureVM -Status Registered -FriendlyName "V2VM"  
$item = Get-AzRecoveryServicesBackupItem -Container $namedContainer -WorkloadType AzureVM  
$job = Backup-AzRecoveryServicesBackupItem -Item $item
```

Troubleshooting

If you run into issues while backing up your virtual machine, review this [troubleshooting article](#).

Deleting a Recovery Services vault

If you need to delete a vault, first delete recovery points in the vault, and then unregister the vault, as follows:

```
$Cont = Get-AzRecoveryServicesBackupContainer -ContainerType AzureVM -Status Registered
$PI = Get-AzRecoveryServicesBackupItem -Container $Cont[0] -WorkloadType AzureVm
Disable-AzRecoveryServicesBackupProtection -RemoveRecoveryPoints $PI[0]
Unregister-AzRecoveryServicesBackupContainer -Container $namedContainer
Remove-AzRecoveryServicesVault -Vault $vault1
```

Next steps

- [Review](#) a more detailed walkthrough of backing up and restoring Azure VMs with PowerShell.
- [Manage and monitor Azure VMs](#)
- [Restore Azure VMs](#)

Restore a disk and create a recovered VM in Azure

2/10/2020 • 8 minutes to read • [Edit Online](#)

Azure Backup creates recovery points that are stored in geo-redundant recovery vaults. When you restore from a recovery point, you can restore the whole VM or individual files. This article explains how to restore a complete VM using CLI. In this tutorial you learn how to:

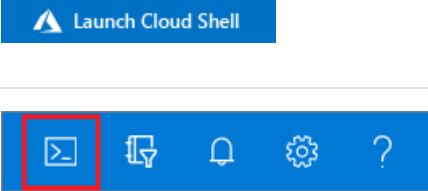
- List and select recovery points
- Restore a disk from a recovery point
- Create a VM from the restored disk

For information on using PowerShell to restore a disk and create a recovered VM, see [Back up and restore Azure VMs with PowerShell](#).

Use Azure Cloud Shell

Azure hosts Azure Cloud Shell, an interactive shell environment that you can use through your browser. You can use either Bash or PowerShell with Cloud Shell to work with Azure services. You can use the Cloud Shell preinstalled commands to run the code in this article without having to install anything on your local environment.

To start Azure Cloud Shell:

OPTION	EXAMPLE/LINK
Select Try It in the upper-right corner of a code block. Selecting Try It doesn't automatically copy the code to Cloud Shell.	
Go to https://shell.azure.com , or select the Launch Cloud Shell button to open Cloud Shell in your browser.	
Select the Cloud Shell button on the menu bar at the upper right in the Azure portal .	

To run the code in this article in Azure Cloud Shell:

1. Start Cloud Shell.
2. Select the **Copy** button on a code block to copy the code.
3. Paste the code into the Cloud Shell session by selecting **Ctrl+Shift+V** on Windows and Linux or by selecting **Cmd+Shift+V** on macOS.
4. Select **Enter** to run the code.

If you choose to install and use the CLI locally, this tutorial requires that you are running the Azure CLI version 2.0.18 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install the Azure CLI](#).

Prerequisites

This tutorial requires a Linux VM that has been protected with Azure Backup. To simulate an accidental VM deletion and recovery process, you create a VM from a disk in a recovery point. If you need a Linux VM that has

been protected with Azure Backup, see [Back up a virtual machine in Azure with the CLI](#).

Backup overview

When Azure initiates a backup, the backup extension on the VM takes a point-in-time snapshot. The backup extension is installed on the VM when the first backup is requested. Azure Backup can also take a snapshot of the underlying storage if the VM is not running when the backup takes place.

By default, Azure Backup takes a file system consistent backup. Once Azure Backup takes the snapshot, the data is transferred to the Recovery Services vault. To maximize efficiency, Azure Backup identifies and transfers only the blocks of data that have changed since the previous backup.

When the data transfer is complete, the snapshot is removed and a recovery point is created.

List available recovery points

To restore a disk, you select a recovery point as the source for the recovery data. As the default policy creates a recovery point each day and retains them for 30 days, you can keep a set of recovery points that allows you to select a particular point in time for recovery.

To see a list of available recovery points, use `az backup recoverypoint list`. The recovery point **name** is used to recover disks. In this tutorial, we want the most recent recovery point available. The `--query [0].name` parameter selects the most recent recovery point name as follows:

```
az backup recoverypoint list \
--resource-group myResourceGroup \
--vault-name myRecoveryServicesVault \
--backup-management-type AzureIaaSVM \
--container-name myVM \
--item-name myVM \
--query [0].name \
--output tsv
```

Restore a VM disk

IMPORTANT

It is very strongly recommended to use Az CLI version 2.0.74 or later to get all the benefits of a quick restore including managed disk restore. It is best if user always uses the latest version.

Managed disk restore

If the backed up VM has managed disks and if the intent is to restore managed disks from the recovery point, you first provide an Azure storage account. This storage account is used to store the VM configuration and the deployment template that can be later used to deploy the VM from the restored disks. Then, you also provide a target resource group for the managed disks to be restored into.

1. To create a storage account, use `az storage account create`. The storage account name must be all lowercase, and be globally unique. Replace *mystorageaccount* with your own unique name:

```
az storage account create \
--resource-group myResourceGroup \
--name mystorageaccount \
--sku Standard_LRS
```

2. Restore the disk from your recovery point with `az backup restore restore-disks`. Replace *mystorageaccount*

with the name of the storage account you created in the preceding command. Replace *myRecoveryPointName* with the recovery point name you obtained in the output from the previous [az backup recoverypoint list](#) command. **Also provide the target resource group to which the managed disks are restored into.**

```
az backup restore restore-disks \
--resource-group myResourceGroup \
--vault-name myRecoveryServicesVault \
--container-name myVM \
--item-name myVM \
--storage-account mystorageaccount \
--rp-name myRecoveryPointName \
--target-resource-group targetRG
```

WARNING

If target-resource-group is not provided then the managed disks will be restored as unmanaged disks to the given storage account. This will have significant consequences to the restore time since the time taken to restore the disks entirely depends on the given storage account.

Unmanaged disks restore

If the backed up VM has unmanaged disks and if the intent is to restore disks from the recovery point, you first provide an Azure storage account. This storage account is used to store the VM configuration and the deployment template that can be later used to deploy the VM from the restored disks. By default, the unmanaged disks will be restored to their original storage accounts. If user wishes to restore all unmanaged disks to one single place, then the given storage account can also be used as a staging location for those disks too.

In additional steps, the restored disk is used to create a VM.

1. To create a storage account, use [az storage account create](#). The storage account name must be all lowercase, and be globally unique. Replace *mystorageaccount* with your own unique name:

```
az storage account create \
--resource-group myResourceGroup \
--name mystorageaccount \
--sku Standard_LRS
```

2. Restore the disk from your recovery point with [az backup restore restore-disks](#). Replace *mystorageaccount* with the name of the storage account you created in the preceding command. Replace *myRecoveryPointName* with the recovery point name you obtained in the output from the previous [az backup recoverypoint list](#) command:

```
az backup restore restore-disks \
--resource-group myResourceGroup \
--vault-name myRecoveryServicesVault \
--container-name myVM \
--item-name myVM \
--storage-account mystorageaccount \
--rp-name myRecoveryPointName
```

As mentioned above, the unmanaged disks will be restored to their original storage account. This provides the best restore performance. But if all unmanaged disks need to be restored to given storage account, then use the relevant flag as shown below.

```

az backup restore restore-disks \
--resource-group myResourceGroup \
--vault-name myRecoveryServicesVault \
--container-name myVM \
--item-name myVM \
--storage-account mystorageaccount \
--rp-name myRecoveryPointName
--restore-to-staging-storage-account
```
Monitor the restore job

To monitor the status of restore job, use [az backup job list]
(https://docs.microsoft.com/cli/azure/backup/job?view=azure-cli-latest#az-backup-job-list):

```azurecli-interactive
az backup job list \
--resource-group myResourceGroup \
--vault-name myRecoveryServicesVault \
--output table
```

```

The output is similar to the following example, which shows the restore job is *InProgress*:

| Name     | Operation       | Status     | Item Name | Start Time UTC      | Duration       |
|----------|-----------------|------------|-----------|---------------------|----------------|
| 7f2ad916 | Restore         | InProgress | myvm      | 2017-09-19T19:39:52 | 0:00:34.520850 |
| a0a8e5e6 | Backup          | Completed  | myvm      | 2017-09-19T03:09:21 | 0:15:26.155212 |
| fe5d0414 | ConfigureBackup | Completed  | myvm      | 2017-09-19T03:03:57 | 0:00:31.191807 |

When the *Status* of the restore job reports *Completed*, the necessary information (VM configuration and the deployment template) has been restored to the storage account.

## Create a VM from the restored disk

The final step is to create a VM from the restored disks. You can use the deployment template downloaded to the given storage account to create the VM.

### Fetch the Job details

The resultant job details give the template URI that can be queried and deployed. Use the job show command to get more details for the triggered restored job.

```

az backup job show \
-v myRecoveryServicesVault \
-g myResourceGroup \
-n 1fc2d55d-f0dc-4ca6-ad48-aca0fe5d0414

```

The output of this query will give all details but we are interested only in the storage account contents. We can use the [query capability](#) of Azure CLI to fetch the relevant details

```

az backup job show \
-v myRecoveryServicesVault \
-g myResourceGroup \
-n 1fc2d55d-f0dc-4ca6-ad48-aca0fe5d0414 \
--query properties.extendedInfo.propertyBag

{
 "Config Blob Container Name": "myVM-daa1931199fd4a22ae601f46d8812276",
 "Config Blob Name": "config-myVM-1fc2d55d-f0dc-4ca6-ad48-aca0fe5d0414.json",
 "Config Blob Uri": "https://mystorageaccount.blob.core.windows.net/myVM-
daa1931199fd4a22ae601f46d8812276/config-appvm8-1fc2d55d-f0dc-4ca6-ad48-aca0519c0232.json",
 "Job Type": "Recover disks",
 "Recovery point time": "12/25/2019 10:07:11 PM",
 "Target Storage Account Name": "mystorageaccount",
 "Target resource group": "mystorageaccountRG",
 "Template Blob Uri": "https://mystorageaccount.blob.core.windows.net/myVM-
daa1931199fd4a22ae601f46d8812276/azuredeploy1fc2d55d-f0dc-4ca6-ad48-aca0519c0232.json"
}

```

## Fetch the deployment template

The template is not directly accessible since it is under a customer's storage account and the given container. We need the complete URL (along with a temporary SAS token) to access this template.

First, extract the template blob Uri from job details

```

az backup job show \
-v myRecoveryServicesVault \
-g myResourceGroup \
-n 1fc2d55d-f0dc-4ca6-ad48-aca0fe5d0414 \
--query properties.extendedInfo.propertyBag."Template Blob Uri"

"https://mystorageaccount.blob.core.windows.net/myVM-daa1931199fd4a22ae601f46d8812276/azuredeploy1fc2d55d-
f0dc-4ca6-ad48-aca0519c0232.json"

```

The template blob Uri will be of this format and extract the template name

```
https://<storageAccountName.blob.core.windows.net>/<containerName>/<templateName>
```

So, the template name from the above example will be `azuredeploy1fc2d55d-f0dc-4ca6-ad48-aca0519c0232.json` and the container name is `myVM-daa1931199fd4a22ae601f46d8812276`

Now get the SAS token for this container and template as detailed [here](#)

```
expiretime=$(date -u -d '30 minutes' +%Y-%m-%dT%H:%MZ)
connection=$(az storage account show-connection-string \
 --resource-group mystorageaccountRG \
 --name mystorageaccount \
 --query connectionString)
token=$(az storage blob generate-sas \
 --container-name myVM-daa1931199fd4a22ae601f46d8812276 \
 --name azuredploy1fc2d55d-f0dc-4ca6-ad48-aca0519c0232.json \
 --expiry $expiretime \
 --permissions r \
 --output tsv \
 --connection-string $connection)
url=$(az storage blob url \
 --container-name myVM-daa1931199fd4a22ae601f46d8812276 \
 --name azuredploy1fc2d55d-f0dc-4ca6-ad48-aca0519c0232.json \
 --output tsv \
 --connection-string $connection)
```

## Deploy the template to create the VM

Now deploy the template to create the VM as explained [here](#).

```
az group deployment create \
 --resource-group ExampleGroup \
 --template-uri $url?$token
```

To confirm that your VM has been created from your recovered disk, list the VMs in your resource group with [az vm list](#) as follows:

```
az vm list --resource-group myResourceGroup --output table
```

## Next steps

In this tutorial, you restored a disk from a recovery point and then created a VM from the disk. You learned how to:

- List and select recovery points
- Restore a disk from a recovery point
- Create a VM from the restored disk

Advance to the next tutorial to learn about restoring individual files from a recovery point.

[Restore files to a virtual machine in Azure](#)

# Restore files to a virtual machine in Azure

11/18/2019 • 6 minutes to read • [Edit Online](#)

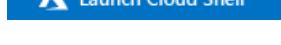
Azure Backup creates recovery points that are stored in geo-redundant recovery vaults. When you restore from a recovery point, you can restore the whole VM or individual files. This article details how to restore individual files. In this tutorial you learn how to:

- List and select recovery points
- Connect a recovery point to a VM
- Restore files from a recovery point

## Use Azure Cloud Shell

Azure hosts Azure Cloud Shell, an interactive shell environment that you can use through your browser. You can use either Bash or PowerShell with Cloud Shell to work with Azure services. You can use the Cloud Shell preinstalled commands to run the code in this article without having to install anything on your local environment.

To start Azure Cloud Shell:

| OPTION                                                                                                                                                    | EXAMPLE/LINK                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Select <b>Try It</b> in the upper-right corner of a code block.<br>Selecting <b>Try It</b> doesn't automatically copy the code to Cloud Shell.            |  |
| Go to <a href="https://shell.azure.com">https://shell.azure.com</a> , or select the <b>Launch Cloud Shell</b> button to open Cloud Shell in your browser. |  |
| Select the <b>Cloud Shell</b> button on the menu bar at the upper right in the <a href="#">Azure portal</a> .                                             |  |

To run the code in this article in Azure Cloud Shell:

1. Start Cloud Shell.
2. Select the **Copy** button on a code block to copy the code.
3. Paste the code into the Cloud Shell session by selecting **Ctrl+Shift+V** on Windows and Linux or by selecting **Cmd+Shift+V** on macOS.
4. Select **Enter** to run the code.

If you choose to install and use the CLI locally, this tutorial requires that you are running the Azure CLI version 2.0.18 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install the Azure CLI](#).

## Prerequisites

This tutorial requires a Linux VM that has been protected with Azure Backup. To simulate an accidental file deletion and recovery process, you delete a page from a web server. If you need a Linux VM that runs a webserver and has been protected with Azure Backup, see [Back up a virtual machine in Azure with the CLI](#).

## Backup overview

When Azure initiates a backup, the backup extension on the VM takes a point-in-time snapshot. The backup extension is installed on the VM when the first backup is requested. Azure Backup can also take a snapshot of the underlying storage if the VM is not running when the backup takes place.

By default, Azure Backup takes a file system consistent backup. Once Azure Backup takes the snapshot, the data is transferred to the Recovery Services vault. To maximize efficiency, Azure Backup identifies and transfers only the blocks of data that have changed since the previous backup.

When the data transfer is complete, the snapshot is removed and a recovery point is created.

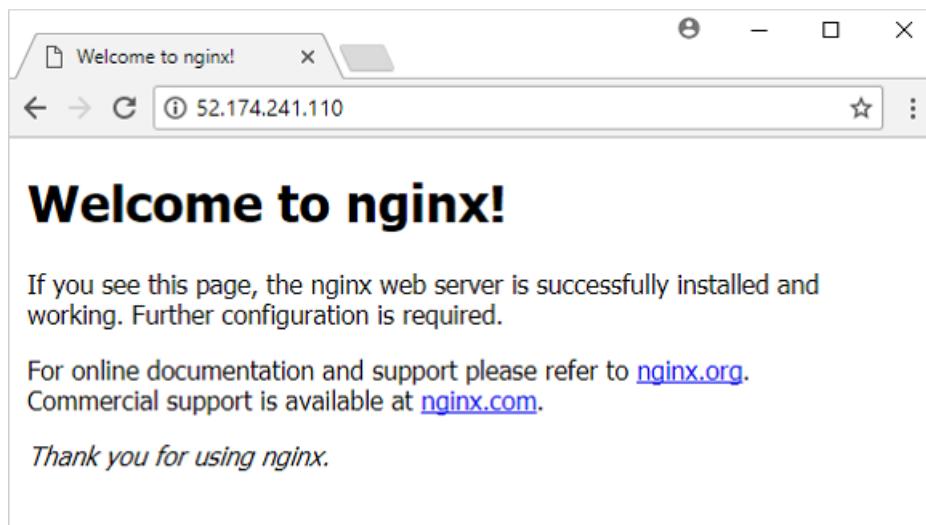
## Delete a file from a VM

If you accidentally delete or make changes to a file, you can restore individual files from a recovery point. This process allows you to browse the files backed up in a recovery point and restore only the files you need. In this example, we delete a file from a web server to demonstrate the file-level recovery process.

1. To connect to your VM, obtain the IP address of your VM with [az vm show](#):

```
az vm show --resource-group myResourceGroup --name myVM -d --query [publicIps] --o tsv
```

2. To confirm that your web site currently works, open a web browser to the public IP address of your VM. Leave the web browser window open.



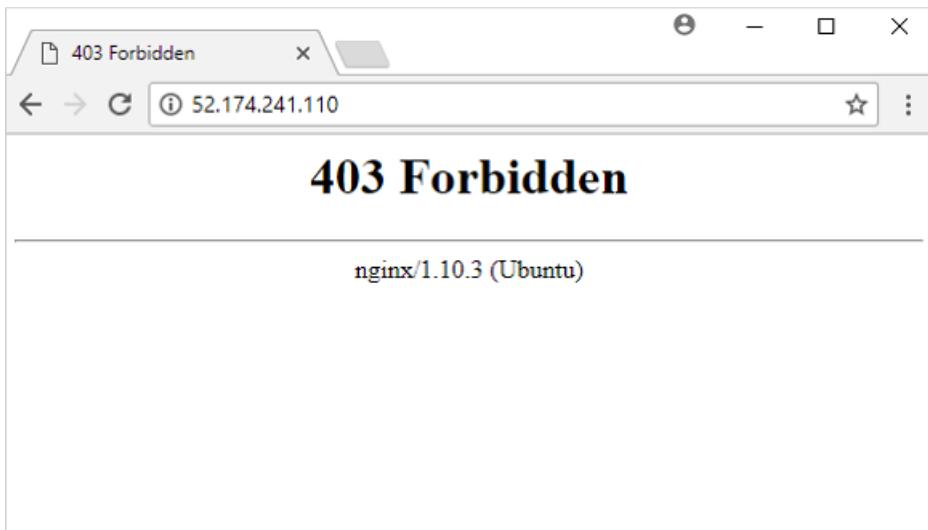
3. Connect to your VM with SSH. Replace *publicIpAddress* with the public IP address that you obtained in a previous command:

```
ssh publicIpAddress
```

4. Delete the default page from the web server at */var/www/html/index.nginx-debian.html* as follows:

```
sudo rm /var/www/html/index.nginx-debian.html
```

5. In your web browser, refresh the web page. The web site no longer loads the page, as shown in the following example:



6. Close the SSH session to your VM as follows:

```
exit
```

## Generate file recovery script

To restore your files, Azure Backup provides a script to run on your VM that connects your recovery point as a local drive. You can browse this local drive, restore files to the VM itself, then disconnect the recovery point. Azure Backup continues to back up your data based on the assigned policy for schedule and retention.

1. To list recovery points for your VM, use [az backup recoverypoint list](#). In this example, we select the most recent recovery point for the VM named *myVM* that is protected in *myRecoveryServicesVault*:

```
az backup recoverypoint list \
--resource-group myResourceGroup \
--vault-name myRecoveryServicesVault \
--container-name myVM \
--item-name myVM \
--query [0].name \
--output tsv
```

2. To obtain the script that connects, or mounts, the recovery point to your VM, use [az backup restore files mount-rp](#). The following example obtains the script for the VM named *myVM* that is protected in *myRecoveryServicesVault*.

Replace *myRecoveryPointName* with the name of the recovery point that you obtained in the preceding command:

```
az backup restore files mount-rp \
--resource-group myResourceGroup \
--vault-name myRecoveryServicesVault \
--container-name myVM \
--item-name myVM \
--rp-name myRecoveryPointName
```

The script is downloaded and a password is displayed, as in the following example:

```
File downloaded: myVM_we_1571974050985163527.sh. Use password c068a041ce12465
```

3. To transfer the script to your VM, use Secure Copy (SCP). Provide the name of your downloaded script, and

replace *publicIpAddress* with the public IP address of your VM. Make sure you include the trailing `:` at the end of the SCP command as follows:

```
scp myVM_we_1571974050985163527.sh 52.174.241.110:
```

## Restore file to your VM

With the recovery script copied to your VM, you can now connect the recovery point and restore files.

1. Connect to your VM with SSH. Replace *publicIpAddress* with the public IP address of your VM as follows:

```
ssh publicIpAddress
```

2. To allow your script to run correctly, add execute permissions with **chmod**. Enter the name of your own script:

```
chmod +x myVM_we_1571974050985163527.sh
```

3. To mount the recovery point, run the script. Enter the name of your own script:

```
./myVM_we_1571974050985163527.sh
```

As the script runs, you are prompted to enter a password to access the recovery point. Enter the password shown in the output from the previous [az backup restore files mount-rp](#) command that generated the recovery script.

The output from the script gives you the path for the recovery point. The following example output shows that the recovery point is mounted at `/home/azureuser/myVM-20170919213536/Volume1`:

```
Microsoft Azure VM Backup - File Recovery

Please enter the password as shown on the portal to securely connect to the recovery point. :
c068a041ce12465

Connecting to recovery point using ISCSI service...

Connection succeeded!

Please wait while we attach volumes of the recovery point to this machine...

***** Volumes of the recovery point and their mount paths on this machine *****

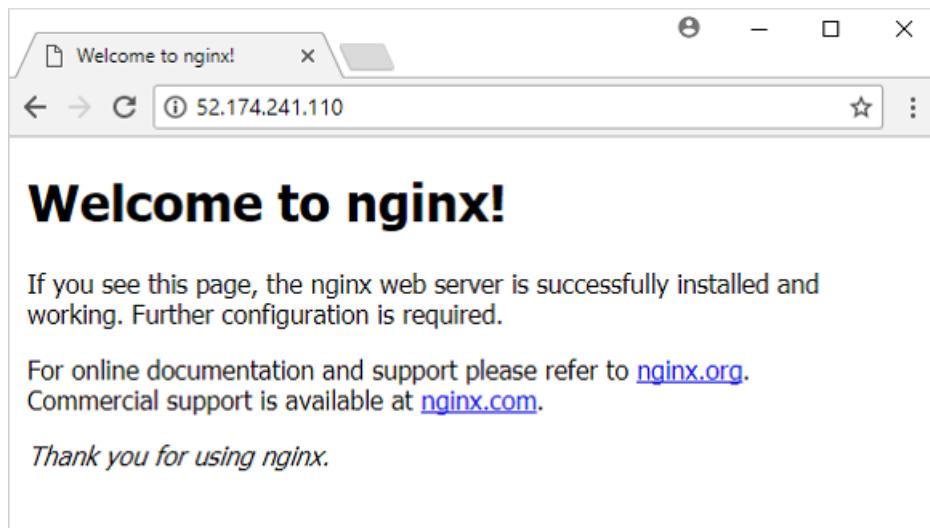
Sr.No. | Disk | Volume | MountPath
1) | /dev/sdc | /dev/sdc1 | /home/azureuser/myVM-20170919213536/Volume1

***** Open File Explorer to browse for files. *****
```

4. Use **cp** to copy the NGINX default web page from the mounted recovery point back to the original file location. Replace the `/home/azureuser/myVM-20170919213536/Volume1` mount point with your own location:

```
sudo cp /home/azureuser/myVM-20170919213536/Volume1/var/www/html/index.nginx-debian.html /var/www/html/
```

5. In your web browser, refresh the web page. The web site now loads correctly again, as shown in the following example:



6. Close the SSH session to your VM as follows:

```
exit
```

7. Unmount the recovery point from your VM with `az backup restore files unmount-rp`. The following example unmounts the recovery point from the VM named *myVM* in *myRecoveryServicesVault*.

Replace *myRecoveryPointName* with the name of your recovery point that you obtained in the previous commands:

```
az backup restore files unmount-rp \
--resource-group myResourceGroup \
--vault-name myRecoveryServicesVault \
--container-name myVM \
--item-name myVM \
--rp-name myRecoveryPointName
```

## Next steps

In this tutorial, you connected a recovery point to a VM and restored files for a web server. You learned how to:

- List and select recovery points
- Connect a recovery point to a VM
- Restore files from a recovery point

Advance to the next tutorial to learn about how to back up Windows Server to Azure.

[Back up Windows Server to Azure](#)

# Back up a SQL Server database in an Azure VM

11/18/2019 • 10 minutes to read • [Edit Online](#)

This tutorial shows you how to back up a SQL Server database running on an Azure VM to an Azure Backup Recovery Services vault. In this article, you learn how to:

- Create and configure a vault.
- Discover databases, and set up backups.
- Set up auto-protection for databases.
- Run an on-demand backup.

## Prerequisites

Before you back up your SQL Server database, check the following conditions:

1. Identify or [create](#) a Recovery Services vault in the same region or locale as the VM hosting the SQL Server instance.
2. [Check the VM permissions](#) needed to back up the SQL databases.
3. Verify that the VM has [network connectivity](#).
4. Check that the SQL Server databases are named in accordance with [naming guidelines](#) for Azure Backup.
5. Verify that you don't have any other backup solutions enabled for the database. Disable all other SQL Server backups before you set up this scenario. You can enable Azure Backup for an Azure VM along with Azure Backup for a SQL Server database running on the VM without any conflict.

### Establish network connectivity

For all operations, the SQL Server VM virtual machine needs connectivity to Azure public IP addresses. VM operations (database discovery, configure backups, schedule backups, restore recovery points, and so on) fail without connectivity to the public IP addresses. Establish connectivity with one of these options:

- **Allow the Azure datacenter IP ranges:** Allow the [IP ranges](#) in the download. To access network security group (NSG), use the **Set-AzureNetworkSecurityRule** cmdlet.
- **Deploy an HTTP proxy server to route traffic:** When you back up a SQL Server database on an Azure VM, the backup extension on the VM uses the HTTPS APIs to send management commands to Azure Backup, and data to Azure Storage. The backup extension also uses Azure Active Directory (Azure AD) for authentication. Route the backup extension traffic for these three services through the HTTP proxy. The extensions are the only component that's configured for access to the public internet.

Each option has advantages and disadvantages

| OPTION          | ADVANTAGES           | DISADVANTAGES                                                                                                                       |
|-----------------|----------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Allow IP ranges | No additional costs. | Complex to manage because the IP address ranges change over time.<br>Provides access to the whole of Azure, not just Azure Storage. |

| OPTION            | ADVANTAGES                                                                                                                                                            | DISADVANTAGES                                         |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| Use an HTTP proxy | <p>Granular control in the proxy over the storage URLs is allowed.</p> <p>Single point of internet access to VMs.</p> <p>Not subject to Azure IP address changes.</p> | Additional costs to run a VM with the proxy software. |

## Set VM permissions

Azure Backup does a number of things when you configure backup for a SQL Server database:

- Adds the **AzureBackupWindowsWorkload** extension.
- To discover databases on the virtual machine, Azure Backup creates the account **NT SERVICE\AzureWLBackupPluginSvc**. This account is used for backup and restore, and requires SQL sysadmin permissions.
- Azure Backup leverages the **NT AUTHORITY\SYSTEM** account for database discovery/inquiry, so this account need to be a public login on SQL.

If you didn't create the SQL Server VM from the Azure Marketplace, you might receive an error

**UserErrorSQLNoSysadminMembership**. If this occurs [follow these instructions](#).

## Verify database naming guidelines for Azure Backup

Avoid the following for database names:

- Trailing/Leading spaces
- Trailing '!'
- Close square bracket ']'
- Databases names starting with 'F:\'

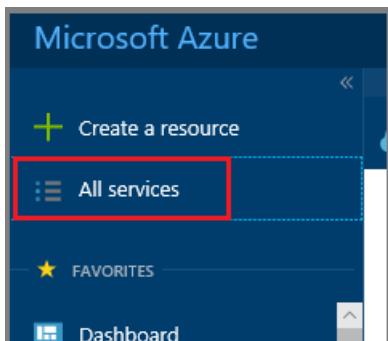
We do have aliasing for Azure table unsupported characters, but we recommend avoiding them. [Learn more](#).

## Create a Recovery Services vault

A Recovery Services vault is an entity that stores backups and recovery points created over time. The Recovery Services vault also contains the backup policies that are associated with the protected virtual machines.

To create a Recovery Services vault, follow these steps.

1. Sign in to your subscription in the [Azure portal](#).
2. On the left menu, select **All services**.



3. In the **All services** dialog box, enter *Recovery Services*. The list of resources filters according to your input. In the list of resources, select **Recovery Services vaults**.

The list of Recovery Services vaults in the subscription appears.

4. On the **Recovery Services vaults** dashboard, select **Add**.

The **Recovery Services vault** dialog box opens. Provide values for the **Name**, **Subscription**, **Resource group**, and **Location**.

The dialog box has the following fields:

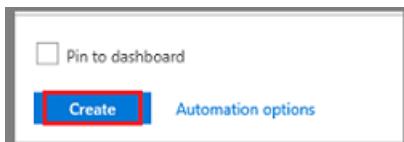
- Name:** Enter the name (e.g., "Enter the name")
- Subscription:** <subscription> (dropdown menu)
- Resource group:** Create new (radio button) or Use existing (radio button, selected)
- Location:** West US (dropdown menu)
- Pin to dashboard:** (checkbox)
- Create** (button)
- Automation options** (link)

- **Name:** Enter a friendly name to identify the vault. The name must be unique to the Azure subscription. Specify a name that has at least 2 but not more than 50 characters. The name must start with a letter and consist only of letters, numbers, and hyphens.
- **Subscription:** Choose the subscription to use. If you're a member of only one subscription, you'll see that name. If you're not sure which subscription to use, use the default (suggested) subscription. There are multiple choices only if your work or school account is associated with more than one Azure subscription.
- **Resource group:** Use an existing resource group or create a new one. To see the list of available resource groups in your subscription, select **Use existing**, and then select a resource from the dropdown list. To create a new resource group, select **Create new** and enter the name. For more information about resource groups, see [Azure Resource Manager overview](#).
- **Location:** Select the geographic region for the vault. To create a vault to protect virtual machines, the vault *must* be in the same region as the virtual machines.

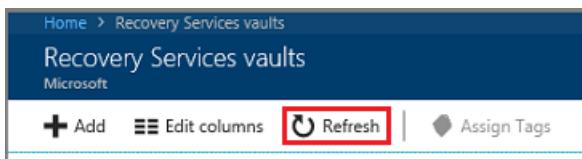
### IMPORTANT

If you're not sure of the location of your VM, close the dialog box. Go to the list of virtual machines in the portal. If you have virtual machines in several regions, create a Recovery Services vault in each region. Create the vault in the first location, before you create the vault for another location. There's no need to specify storage accounts to store the backup data. The Recovery Services vault and Azure Backup handle that automatically.

- When you're ready to create the Recovery Services vault, select **Create**.



It can take a while to create the Recovery Services vault. Monitor the status notifications in the **Notifications** area at the upper-right corner of the portal. After your vault is created, it's visible in the list of Recovery Services vaults. If you don't see your vault, select **Refresh**.



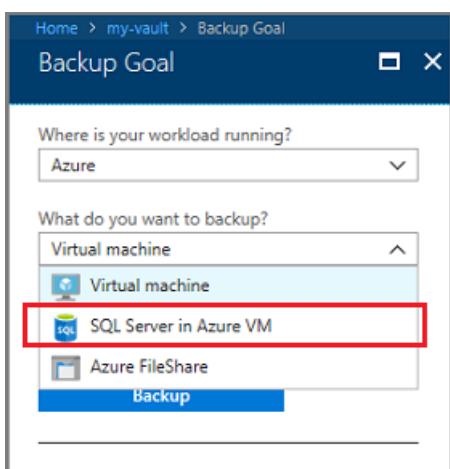
## Discover SQL Server databases

Discover databases running on the VM.

- In the [Azure portal](#), open the Recovery Services vault you use to back up the database.
- On the **Recovery Services vault** dashboard, select **Backup**.

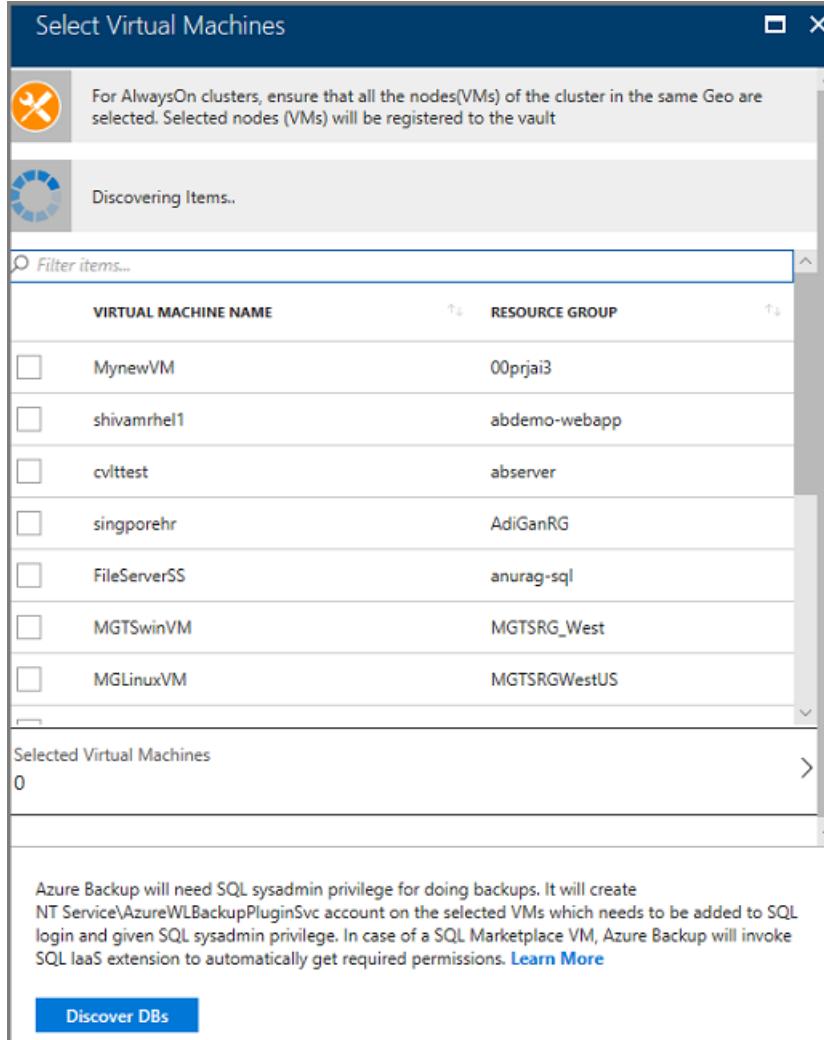


- In **Backup Goal**, set **Where is your workload running** to **Azure** (the default).
- In **What do you want to backup**, select **SQL Server in Azure VM**.



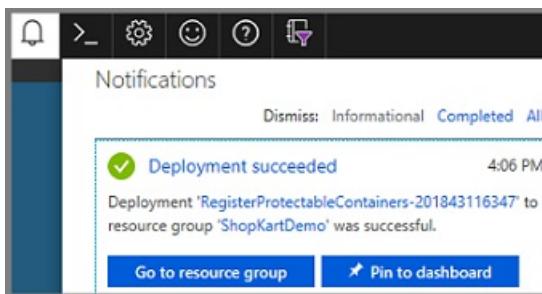
5. In **Backup Goal > Discover DBs in VMs**, select **Start Discovery** to search for unprotected VMs in the subscription. It can take a while, depending on the number of unprotected virtual machines in the subscription.

- Unprotected VMs should appear in the list after discovery, listed by name and resource group.
- If a VM isn't listed as you expect, check whether it's already backed up in a vault.
- Multiple VMs can have the same name but they'll belong to different resource groups.



6. In the VM list, select the VM running the SQL Server database > **Discover DBs**.

7. Track database discovery in the **Notifications** area. It can take a while for the job to complete, depending on how many databases are on the VM. When the selected databases are discovered, a success message appears.



8. Azure Backup discovers all SQL Server databases on the VM. During discovery the following occurs in the background:

- Azure Backup register the VM with the vault for workload backup. All databases on the registered

VM can only be backed up to this vault.

- Azure Backup installs the **AzureBackupWindowsWorkload** extension on the VM. No agent is installed on the SQL database.
- Azure Backup creates the service account **NT Service\AzureWLBackupPluginSvc** on the VM.
  - All backup and restore operations use the service account.
  - **NT Service\AzureWLBackupPluginSvc** needs SQL sysadmin permissions. All SQL Server VMs created in the Azure Marketplace come with the **SqlIaaSExtension** installed. The **AzureBackupWindowsWorkload** extension uses the **SQLIaaSExtension** to automatically get the required permissions.
- If you didn't create the VM from the marketplace, then the VM doesn't have the **SqlIaaSExtension** installed, and the discovery operation fails with the error message **UserErrorSQLNoSysAdminMembership**. Follow the [instructions](#) to fix this issue.

The screenshot shows two windows side-by-side. The left window is titled 'Protected Servers' and shows a list of VMs. One VM, 'ShopKartHR', is highlighted with a red box and has a status of 'Not Ready' with an 'Error' icon. The right window is titled 'Error details' and shows the error code 'UserErrorSQLNoSysAdminMembership' and the message 'Azure Backup service creates a service account "NTService\AzureWLBackupPluginSvc" for all operations and this account needs SQL sysadmin privilege.' It also includes a 'Recommended Action' to 'Please provide Sys Admin privileges to AzureWLBackupPluginSvc.'

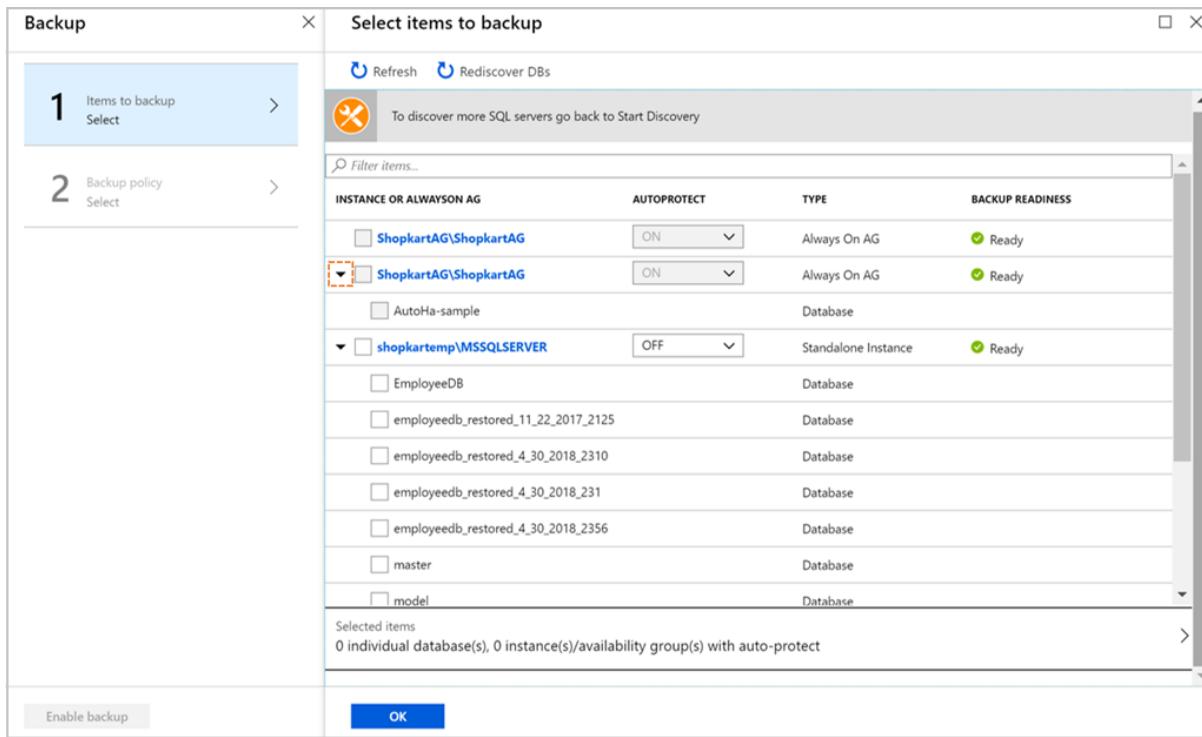
## Configure backup

Configure backup as follows:

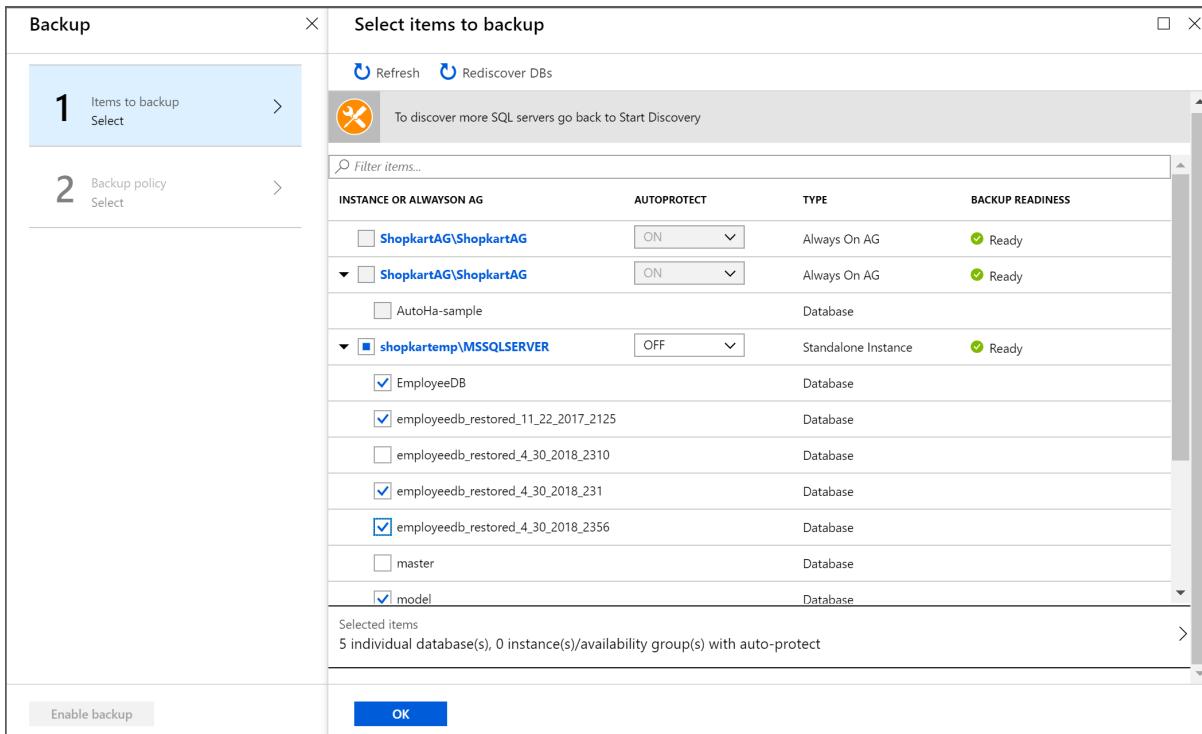
1. In **Backup Goal**, select **Configure Backup**.

The screenshot shows the 'Backup Goal' configuration blade. It asks 'Where is your workload running?' (set to 'Azure') and 'What do you want to backup?' (set to 'SQL Server in Azure VM'). It has two main sections: 'Step 1: Discover DBs in VMs' with a 'Start Discovery' button, and 'Step 2: Configure Backup' with a 'Configure Backup' button. The 'Configure Backup' button is highlighted with a red box.

2. Click **Configure Backup**, the **Select items to backup** blade appears. This lists all the registered availability groups and standalone SQL Servers. Expand the chevron to the left of the row to see all the unprotected databases in that instance or Always on AG.



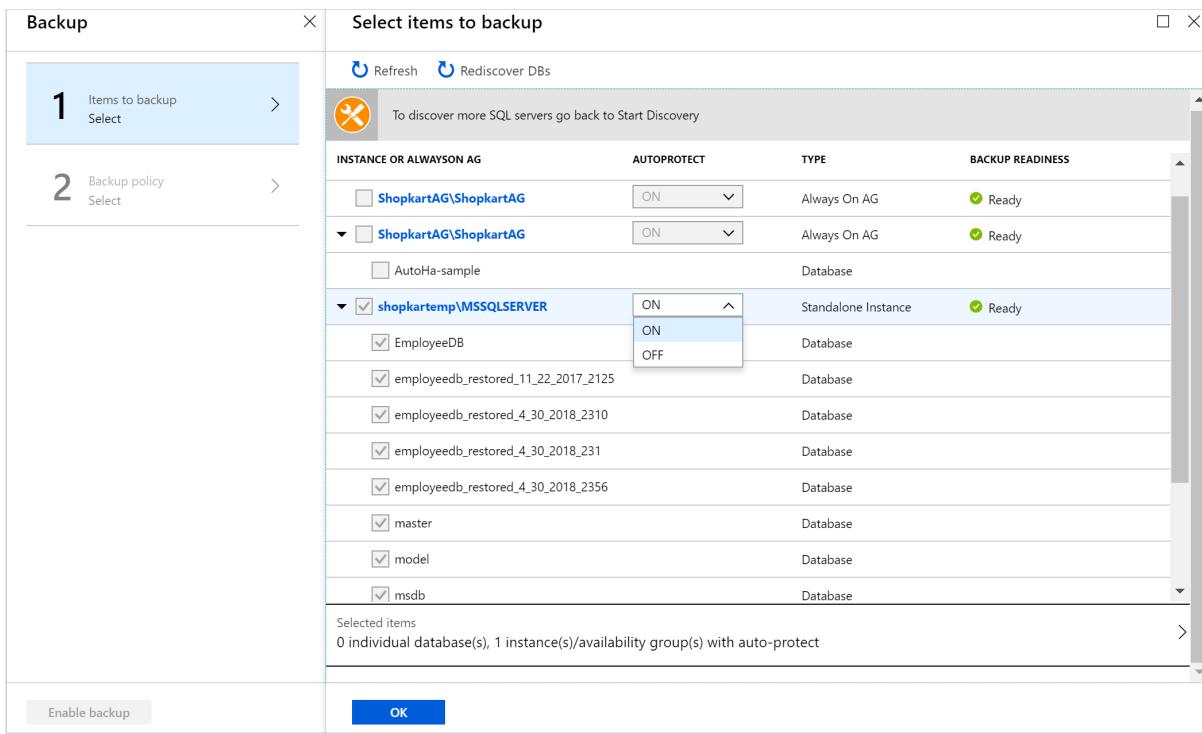
3. Select all the databases you want to protect > **OK**.



To optimize backup loads, Azure Backup sets a maximum number of databases in one backup job to 50.

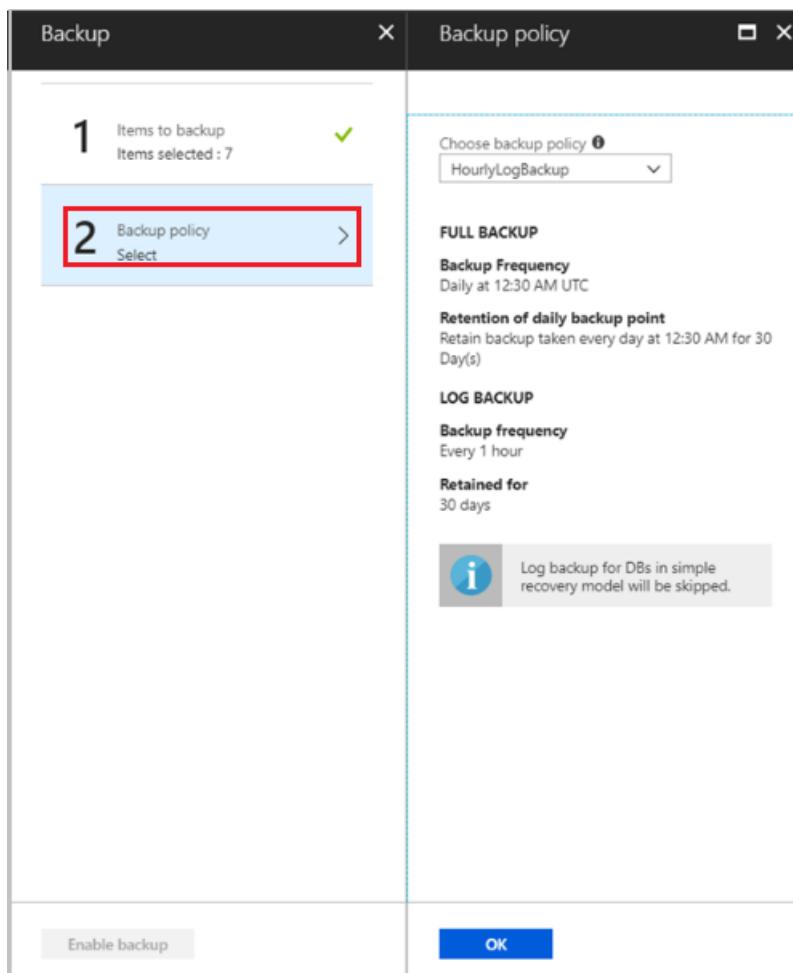
- Alternatively, you can enable auto-protection on the entire instance or Always On Availability group by selecting the **ON** option in the corresponding dropdown in the **AUTOPROTECT** column. The auto-protection feature not only enables protection on all the existing databases in one go but also automatically protects any new databases that will be added to that instance or the availability group in future.

4. Click **OK** to open the **Backup policy** blade.

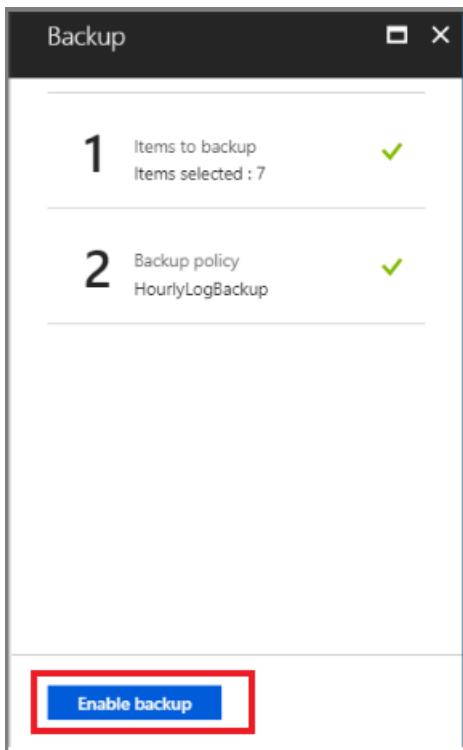


5. In **Choose backup policy**, select a policy, then click **OK**.

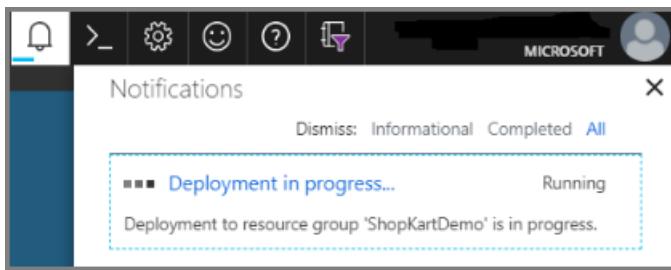
- Select the default policy: HourlyLogBackup.
- Choose an existing backup policy previously created for SQL.
- Define a new policy based on your RPO and retention range.



6. On **Backup** menu, select **Enable backup**.



7. Track the configuration progress in the **Notifications** area of the portal.



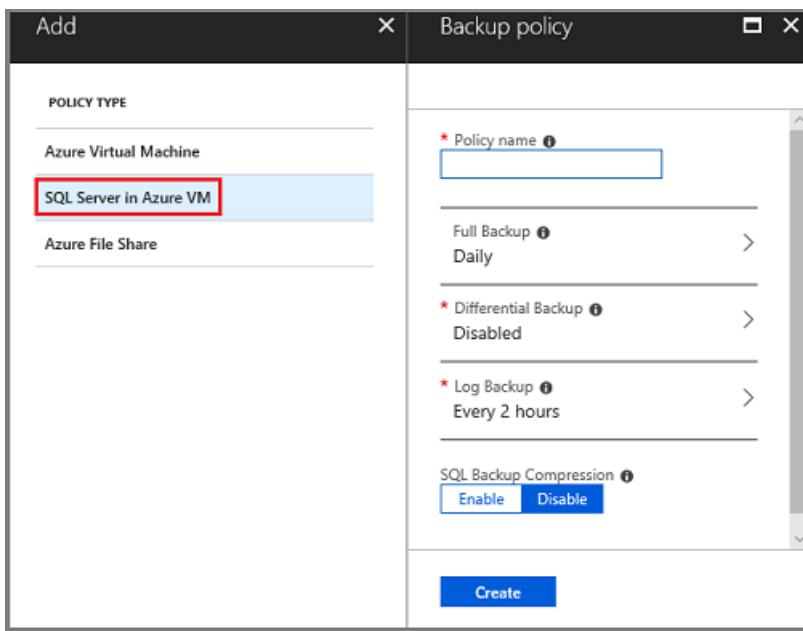
### Create a backup policy

A backup policy defines when backups are taken and how long they're retained.

- A policy is created at the vault level.
- Multiple vaults can use the same backup policy, but you must apply the backup policy to each vault.
- When you create a backup policy, a daily full backup is the default.
- You can add a differential backup, but only if you configure full backups to occur weekly.
- [Learn about](#) different types of backup policies.

To create a backup policy:

1. In the vault, click **Backup policies** > **Add**.
2. In **Add** menu, click **SQL Server in Azure VM** to define the policy type.



3. In **Policy name**, enter a name for the new policy.
4. In **Full Backup policy**, select a **Backup Frequency**, choose **Daily** or **Weekly**.

- For **Daily**, select the hour and time zone when the backup job begins.
- You must run a full backup as you can't turn off the **Full Backup** option.
- Click **Full Backup** to view the policy.
- You can't create differential backups for daily full backups.

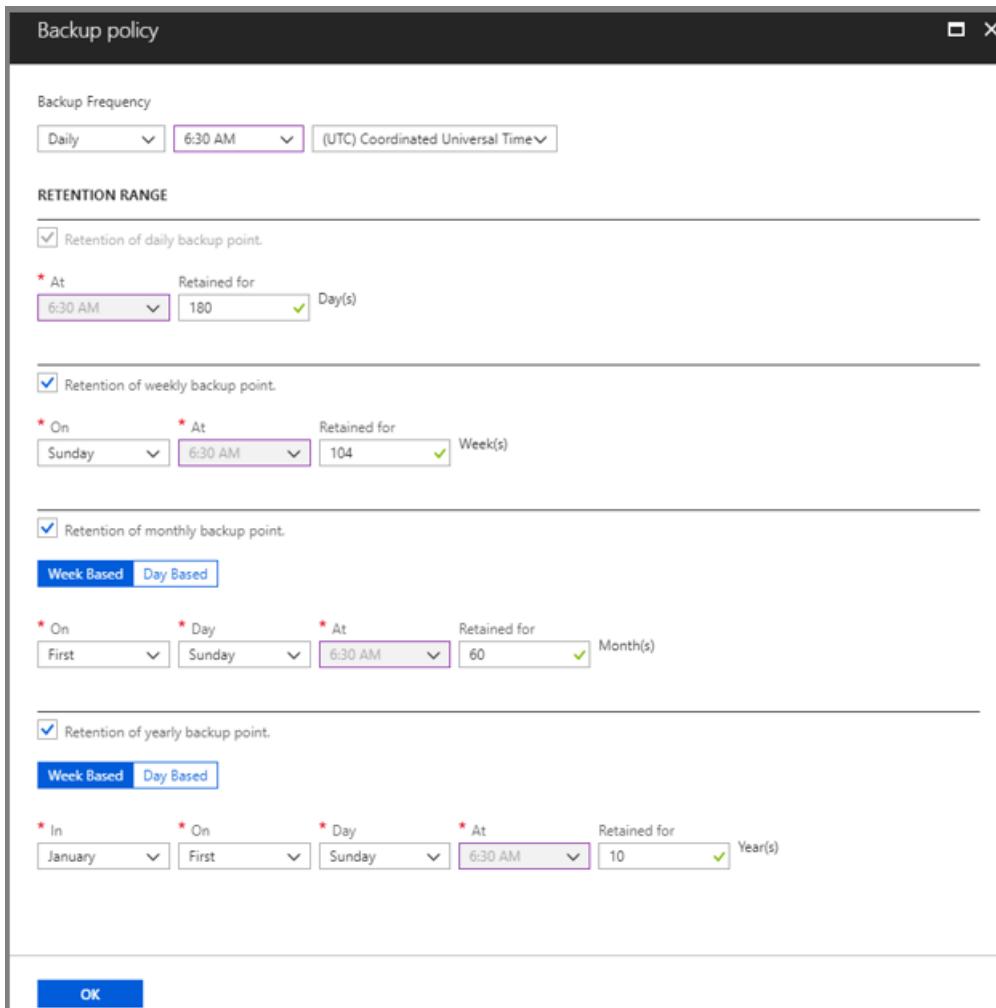
- For **Weekly**, select the day of the week, hour, and time zone when the backup job begins.

The screenshot shows the 'Backup Frequency' configuration dialog box. It includes sections for 'Backup Frequency' (set to Daily at 12:00 AM UTC), 'Retention Range' (with options for daily, weekly, monthly, and yearly retention), and tabs for 'Week Based' and 'Day Based'. The 'Day Based' tab is selected for all categories. Buttons for 'OK' and 'Cancel' are at the bottom.

| Retention Type                    | On       | At       | Retained for |             |            |
|-----------------------------------|----------|----------|--------------|-------------|------------|
| Retention of daily backup point   | 12:00 AM | 180      | Day(s)       |             |            |
| Retention of weekly backup point  | Sunday   | 12:00 AM | 104 Week(s)  |             |            |
| Retention of monthly backup point | First    | Sunday   | 12:00 AM     | 60 Month(s) |            |
| Retention of yearly backup point  | January  | First    | Sunday       | 12:00 AM    | 10 Year(s) |

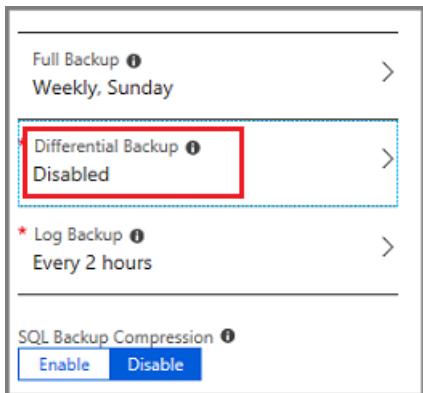
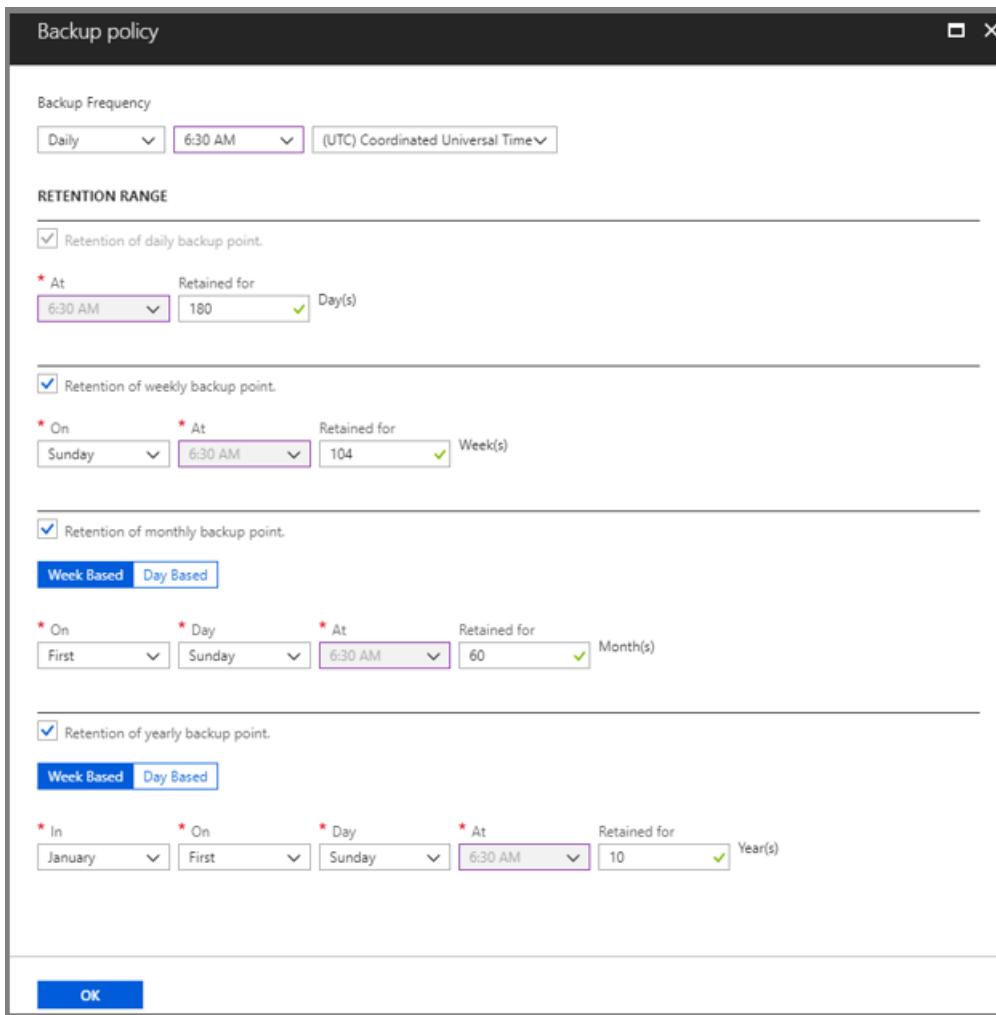
5. For **Retention Range**, by default all options are selected. Clear any undesired retention range limits you don't want to use, and set the intervals to use.

- Minimum retention period for any type of backup (full/differential/log) is seven days.
- Recovery points are tagged for retention based on their retention range. For example, if you select a daily full backup, only one full backup is triggered each day.
- The backup for a specific day is tagged and retained based on the weekly retention range and your weekly retention setting.
- The monthly and yearly retention ranges behave in a similar way.

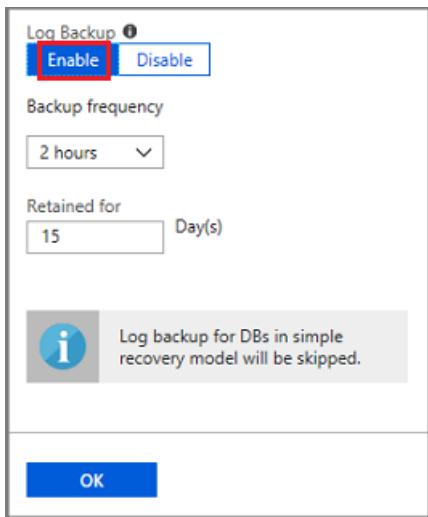


6. In the **Full Backup policy** menu, select **OK** to accept the settings.

7. To add a differential backup policy, select **Differential Backup**.



8. In **Differential Backup policy**, select **Enable** to open the frequency and retention controls.
  - At most, you can trigger one differential backup per day.
  - Differential backups can be retained for a maximum of 180 days. If you need longer retention, you must use full backups.
9. Select **OK** to save the policy and return to the main **Backup policy** menu.
10. To add a transactional log backup policy, select **Log Backup**.
11. In **Log Backup**, select **Enable**, and then set the frequency and retention controls. Log backups can occur as often as every 15 minutes, and can be retained for up to 35 days.
12. Select **OK** to save the policy and return to the main **Backup policy** menu.



13. On the **Backup policy** menu, choose whether to enable **SQL Backup Compression**.

- Compression is disabled by default.
- On the back end, Azure Backup uses SQL native backup compression.

14. After you complete the edits to the backup policy, select **OK**.

## Run an on-demand backup

1. In your Recovery Services vault, choose Backup items.
2. Click on "SQL in Azure VM".
3. Right click on a database, and choose "Backup now".
4. Choose the Backup Type (Full/Differential/Log/Copy Only Full) and Compression (Enable/Disable)
5. Select OK to begin the backup.
6. Monitor the backup job by going to your Recovery Services vault and choosing "Backup Jobs".

## Next steps

In this tutorial, you used the Azure portal to:

- Create and configure a vault.
- Discover databases, and set up backups.
- Set up auto-protection for databases.
- Run an on-demand backup.

Continue to the next tutorial to restore an Azure virtual machine from disk.

[Restore SQL Server databases on Azure VMs](#)

# Tutorial: Back up SAP HANA databases in an Azure VM

2/27/2020 • 9 minutes to read • [Edit Online](#)

This tutorial shows you how to back up SAP HANA databases running on Azure VMs to an Azure Backup Recovery Services vault. In this article you'll learn how to:

- Create and configure a vault
- Discover databases
- Configure backups

[Here](#) are all the scenarios that we currently support.

## Prerequisites

Make sure you do the following before configuring backups:

- Allow connectivity from the VM to the internet, so that it can reach Azure, as described in the [set up network connectivity](#) procedure below.
- A key should exist in the **hdbuserstore** that fulfills the following criteria:
  - It should be present in the default **hdbuserstore**
  - For MDC, the key should point to the SQL port of **NAMESERVER**. In the case of SDC it should point to the SQL port of **INDEXSERVER**
  - It should have credentials to add and delete users
- Run the SAP HANA backup configuration script (pre-registration script) in the virtual machine where HANA is installed, as the root user. [This script](#) gets the HANA system ready for backup. Refer to the [What the pre-registration script does](#) section to understand more about the pre-registration script.

## Set up network connectivity

For all operations, the SAP HANA VM requires connectivity to Azure public IP addresses. VM operations (database discovery, configure backups, schedule backups, restore recovery points, and so on) fail without connectivity to Azure public IP addresses.

Establish connectivity by using one of the following options:

### Allow the Azure datacenter IP ranges

This option allows the [IP ranges](#) in the downloaded file. To access a network security group (NSG), use the `Set-AzureNetworkSecurityRule` cmdlet. If your safe recipients list only includes region-specific IPs, you'll also need to update the safe recipients list the Azure Active Directory (Azure AD) service tag to enable authentication.

### Allow access using NSG tags

If you use NSG to restrict connectivity, then you should use AzureBackup service tag to allow outbound access to Azure Backup. In addition, you should also allow connectivity for authentication and data transfer by using [rules](#) for Azure AD and Azure Storage. This can be done from the Azure portal or via PowerShell.

To create a rule using the portal:

1. In **All Services**, go to **Network security groups** and select the network security group.
2. Select **Outbound security rules** under **Settings**.

3. Select **Add**. Enter all the required details for creating a new rule as described in [security rule settings](#). Ensure the option **Destination** is set to **Service Tag** and **Destination service tag** is set to **AzureBackup**.
4. Click **Add**, to save the newly created outbound security rule.

To create a rule using PowerShell:

1. Add Azure account credentials and update the national clouds

```
Add-AzureRmAccount
```

2. Select the NSG subscription

```
Select-AzureRmSubscription "<Subscription Id>"
```

3. Select the NSG

```
$nsg = Get-AzureRmNetworkSecurityGroup -Name "<NSG name>" -ResourceGroupName "<NSG resource group name>"
```

4. Add allow outbound rule for Azure Backup service tag

```
Add-AzureRmNetworkSecurityRuleConfig -NetworkSecurityGroup $nsg -Name "AzureBackupAllowOutbound" -Access Allow -Protocol * -Direction Outbound -Priority <priority> -SourceAddressPrefix * -SourcePortRange * -DestinationAddressPrefix "AzureBackup" -DestinationPortRange 443 -Description "Allow outbound traffic to Azure Backup service"
```

5. Add allow outbound rule for Storage service tag

```
Add-AzureRmNetworkSecurityRuleConfig -NetworkSecurityGroup $nsg -Name "StorageAllowOutbound" -Access Allow -Protocol * -Direction Outbound -Priority <priority> -SourceAddressPrefix * -SourcePortRange * -DestinationAddressPrefix "Storage" -DestinationPortRange 443 -Description "Allow outbound traffic to Azure Backup service"
```

6. Add allow outbound rule for AzureActiveDirectory service tag

```
Add-AzureRmNetworkSecurityRuleConfig -NetworkSecurityGroup $nsg -Name "AzureActiveDirectoryAllowOutbound" -Access Allow -Protocol * -Direction Outbound -Priority <priority> -SourceAddressPrefix * -SourcePortRange * -DestinationAddressPrefix "AzureActiveDirectory" -DestinationPortRange 443 -Description "Allow outbound traffic to AzureActiveDirectory service"
```

7. Save the NSG

```
Set-AzureRmNetworkSecurityGroup -NetworkSecurityGroup $nsg
```

**Allow access by using Azure Firewall tags.** If you're using Azure Firewall, create an application rule by using the AzureBackup [FQDN tag](#). This allows outbound access to Azure Backup.

**Deploy an HTTP proxy server to route traffic.** When you back up an SAP HANA database on an Azure VM, the backup extension on the VM uses the HTTPS APIs to send management commands to Azure Backup and data to Azure Storage. The backup extension also uses Azure AD for authentication. Route the backup extension traffic for these three services through the HTTP proxy. The extensions are the only component that's configured for access to the public internet.

Connectivity options include the following advantages and disadvantages:

| OPTION               | ADVANTAGES                                                                               | DISADVANTAGES                                                           |
|----------------------|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| Allow IP ranges      | No additional costs<br><br>Provides access to the whole of Azure, not just Azure Storage | Complex to manage because the IP address ranges change over time        |
| Use NSG service tags | Easier to manage as range changes are automatically merged<br><br>No additional costs    | Can be used with NSGs only<br><br>Provides access to the entire service |

| OPTION                       | ADVANTAGES                                                                                                                                                  | DISADVANTAGES                                        |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| Use Azure Firewall FQDN tags | Easier to manage as the required FQDNs are automatically managed                                                                                            | Can be used with Azure Firewall only                 |
| Use an HTTP proxy            | Granular control in the proxy over the storage URLs is allowed<br><br>Single point of internet access to VMs<br><br>Not subject to Azure IP address changes | Additional costs to run a VM with the proxy software |

## What the pre-registration script does

Running the pre-registration script performs the following functions:

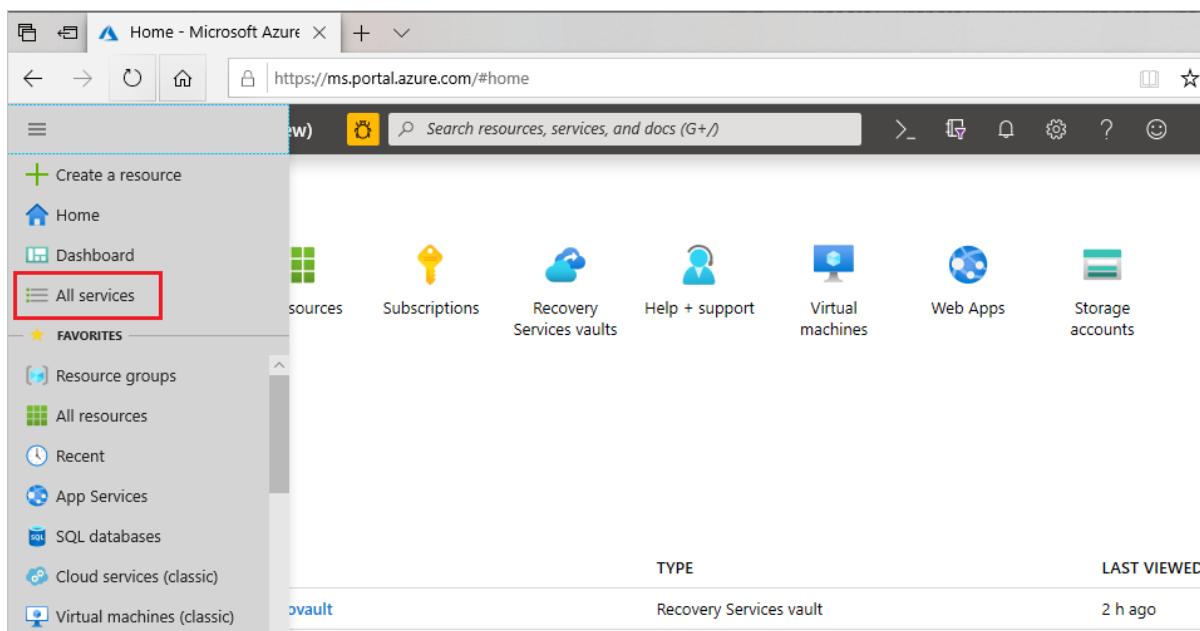
- It installs or updates any necessary packages required by the Azure Backup agent on your distribution.
- It performs outbound network connectivity checks with Azure Backup servers and dependent services like Azure Active Directory and Azure Storage.
- It logs into your HANA system using the user key listed as part of the [prerequisites](#). This key is used to create a backup user (AZUREWLBACKUPHANAUSER) in the HANA system and can be deleted after the pre-registration script runs successfully. This backup user (AZUREWLBACKUPHANAUSER) will allow the backup agent to discover, backup and restore databases in your HANA system.

## Create a Recovery Service vault

A Recovery Services vault is an entity that stores the backups and recovery points created over time. The Recovery Services vault also contains the backup policies that are associated with the protected virtual machines.

To create a Recovery Services vault:

1. Sign in to your subscription in the [Azure portal](#).
2. On the left menu, select **All services**



The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the 'Home - Microsoft Azure' title, a search bar, and various icons. The left sidebar features a 'Create a resource' button and a 'FAVORITES' section with links to 'Resource groups', 'All resources', 'Recent', 'App Services', 'SQL databases', 'Cloud services (classic)', and 'Virtual machines (classic)'. A red box highlights the 'All services' link under the 'FAVORITES' section. The main content area displays several service icons: 'sources', 'Subscriptions', 'Recovery Services vaults', 'Help + support', 'Virtual machines', 'Web Apps', and 'Storage accounts'. Below this, a table lists a single resource: 'Recovery Services vault' under 'TYPE' and '2 h ago' under 'LAST VIEWED'.

| TYPE                    | LAST VIEWED |
|-------------------------|-------------|
| Recovery Services vault | 2 h ago     |

3. In the **All services** dialog box, enter **Recovery Services**. The list of resources filters according to your input. In the list of resources, select **Recovery Services vaults**.

- On the **Recovery Services** vaults dashboard, select **Add**.

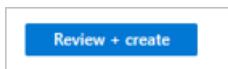
The **Recovery Services vault** dialog box opens. Provide values for the **Name**, **Subscription**, **Resource group**, and **Location**

- Name:** The name is used to identify the recovery services vault and must be unique to the Azure subscription. Specify a name that has at least two, but not more than 50 characters. The name must start with a letter and consist only of letters, numbers, and hyphens. For this tutorial, we've used the name **SAPHanaVault**.
- Subscription:** Choose the subscription to use. If you're a member of only one subscription, you'll see that name. If you're not sure which subscription to use, use the default (suggested) subscription. There are multiple choices only if your work or school account is associated with more than one Azure subscription. Here, we have used the **SAP HANA solution lab subscription** subscription.
- Resource group:** Use an existing resource group or create a new one. Here, we have used **SAPHANADemo**.

To see the list of available resource groups in your subscription, select **Use existing**, and then select a resource from the drop-down list box. To create a new resource group, select **Create new** and enter the name. For complete information about resource groups, see [Azure Resource Manager overview](#).

- **Location:** Select the geographic region for the vault. The vault must be in the same region as the Virtual Machine running SAP HANA. We have used **East US 2**.

## 5. Select **Review + Create**.



The Recovery services vault is now created.

## Discover the databases

1. In the vault, in **Getting Started**, click **Backup**. In **Where is your workload running?**, select **SAP HANA in Azure VM**.
2. Click **Start Discovery**. This initiates discovery of unprotected Linux VMs in the vault region. You will see the Azure VM that you want to protect.
3. In **Select Virtual Machines**, click the link to download the script that provides permissions for the Azure Backup service to access the SAP HANA VMs for database discovery.
4. Run the script on the VM hosting SAP HANA database(s) that you want to back up.
5. After running the script on the VM, in **Select Virtual Machines**, select the VM. Then click **Discover DBs**.
6. Azure Backup discovers all SAP HANA databases on the VM. During discovery, Azure Backup registers the VM with the vault, and installs an extension on the VM. No agent is installed on the database.

The screenshot shows two windows. On the left is the main 'ReadyDemoVault - Backup' dashboard under 'Recovery Services vault'. It has a sidebar with 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'SETTINGS' (Properties, Locks, Automation script), 'GETTING STARTED' (Backup, Site Recovery), and 'MONITORING AND REPORTS'. A red box highlights the 'Backup' link in 'GETTING STARTED'. On the right is a 'Select Virtual Machines' dialog titled 'Discovering Items...'. It lists several VMs: Prtestvmsea (Resource Group Test1), UtBkpVM1, UtBkpVMRes1, myManagedDiskVM, aruna-rest-demo, and arunavm. A red box highlights the dropdown 'What do you want to backup?' set to 'SAP HANA in Azure VM'. Below the list is a note: 'Azure backup requires permissions to able to discover SAP HANA DBs and perform backup and restore operations. Run this script on the SAP HANA VMs to provide these permissions to Azure Backup service. Learn More'. A red box highlights the 'Discover DBs' button at the bottom of the dialog.

## Configure backup

Now that the databases we want to back up are discovered, let's enable backup.

1. Click **Configure Backup**.

The screenshot shows the 'Backup Goal' page. At the top, there's a breadcrumb navigation: Home > ignitedemovault > Backup Goal. Below it, the title 'Backup Goal' is displayed. A section asks 'Where is your workload running?' with a dropdown menu set to 'Azure'. Another section asks 'What do you want to backup?' with a dropdown menu set to 'SAP HANA in Azure VM (Preview)'. The page is divided into two main steps: 'Step 1: Discover DBs in VMs' and 'Step 2: Configure Backup'. The 'Configure Backup' button in Step 2 is highlighted with a red border.

2. In **Select items to back up**, select one or more databases that you want to protect, and then click **OK**.

The screenshot shows the 'Select items to backup' dialog box. It has two main sections: 'Items to backup' and 'Backup policy'. The 'Items to backup' section shows '1 Items to backup' and a 'Select' button. The 'Backup policy' section shows '2 Backup policy' and a 'Select' button. The right side of the dialog shows a list of databases under 'HANA System' with columns for 'TYPE' and 'BACKUP READINESS'. The database 'HANADemoIDC3\H22' is selected, showing it's a 'Standalone Instance' and 'Ready'. Other databases listed are 'H22 IGNITE\_BOOTH', 'H22 IGNITEBOOTH', 'H22 RESTORE', and 'HANADemoIDC4\H21'. At the bottom, it says 'Selected items 0 database(s)'. There are 'Enable backup' and 'OK' buttons at the bottom.

| HANA System                                          |                     |                                            | TYPE | BACKUP READINESS |
|------------------------------------------------------|---------------------|--------------------------------------------|------|------------------|
| <input checked="" type="checkbox"/> HANADemoIDC3\H22 | Standalone Instance | <span style="color: green;">✓ Ready</span> |      |                  |
| <input type="checkbox"/> H22 IGNITE_BOOTH            | Database            |                                            |      |                  |
| <input type="checkbox"/> H22 IGNITEBOOTH             | Database            |                                            |      |                  |
| <input type="checkbox"/> H22 RESTORE                 | Database            |                                            |      |                  |
| <input type="checkbox"/> HANADemoIDC4\H21            | Standalone Instance | <span style="color: green;">✓ Ready</span> |      |                  |

3. In **Backup Policy > Choose backup policy**, create a new backup policy for the database(s), in accordance with the instructions in the next section.

**Backup**

**Backup policy**

**Choose backup policy** DailyFullLog2

**FULL BACKUP**  
Backup Frequency: Daily at 2:30 AM UTC  
Retention of daily backup point: Retain backup taken every day at 2:30 AM for 180 Day(s)

**Retention of weekly backup point**: Retain backup taken every week on Sunday at 2:30 AM for 104 Week(s)

**Retention of monthly backup point**: Retain backup taken every month on First Sunday at 2:30 AM for 60 Month(s)

**Retention of yearly backup point**: Retain backup taken every year in January on First Sunday at 2:30 AM for 10 Year(s)

**LOG BACKUP**

**Enable backup**

**OK**

4. After creating the policy, on the **Backup menu**, click **Enable backup**.

**Backup**

**1 Items to backup**  
1 database(s)

**2 Backup policy**  
DailyFullLog2

**Enable backup**

5. Track the backup configuration progress in the **Notifications** area of the portal.

## Creating a backup policy

A backup policy defines when backups are taken, and how long they're retained.

- A policy is created at the vault level.
- Multiple vaults can use the same backup policy, but you must apply the backup policy to each vault.

Specify the policy settings as follows:

1. In **Policy name**, enter a name for the new policy. In this case, enter **SAPHANA**.

|                        |   |
|------------------------|---|
| Add                    | X |
| <b>Policy Type</b>     |   |
| Azure Virtual Machine  |   |
| SAP HANA in Azure VM   |   |
| SQL Server in Azure VM |   |
| Azure File Share       |   |

|                        |   |
|------------------------|---|
| Backup policy          | X |
| <b>Policy name *</b> ⓘ |   |
| Full Backup ⓘ          | > |
| Daily                  |   |
| *Differential Backup ⓘ | > |
| Disabled               |   |
| *Log Backup ⓘ          | > |
| Every 2 hours          |   |
| <b>Create</b>          |   |

2. In **Full Backup policy**, select a **Backup Frequency**. You can choose **Daily** or **Weekly**. For this tutorial, we chose the **Daily** backup.

## Full Backup Policy

### Backup Frequency

Daily  11:30 AM  (UTC) Coordinated Univers...

### RETENTION RANGE

Retention of daily backup point.

At \*  Retained for  
11:30 AM  180 Day(s)

Retention of weekly backup point.

On \*  At \*  Retained for  
Sunday  11:30 AM  104 Week(s)

Retention of monthly backup point.

Week Based  Day Based

On \*  Day \*  At \*  Retained for  
First  Sunday  11:30 AM  60 Month(s)

Retention of yearly backup point.

Week Based  Day Based

In \*  On \*  Day \*  At \*  Retained for  
January  First  Sunday  11:30 AM  10 Year(s)

OK

3. In **Retention Range**, configure retention settings for the full backup.

- By default, all options are selected. Clear any retention range limits you don't want to use and set those that you do.
- The minimum retention period for any type of backup (full/differential/log) is seven days.
- Recovery points are tagged for retention based on their retention range. For example, if you select a daily full backup, only one full backup is triggered each day.
- The backup for a specific day is tagged and retained based on the weekly retention range and setting.
- The monthly and yearly retention ranges behave in a similar way.

4. In the **Full Backup policy** menu, click **OK** to accept the settings.

5. Then select **Differential Backup** to add a differential policy.

6. In **Differential Backup policy**, select **Enable** to open the frequency and retention controls. We have enabled a differential backup every **Sunday at 2:00 AM**, which is retained for **30 days**.

### Differential Backup Policy

Differential Backup ⓘ

Enable    Disable

Backup Frequency

Sunday    2:00 AM    (UTC) Coordinated  
Universal Time

Retained for

30 Day(s)

**NOTE**

Incremental backups aren't currently supported.

7. Click **OK** to save the policy and return to the main **Backup policy** menu.
8. Select **Log Backup** to add a transactional log backup policy,
  - **Log Backup** is by default set to **Enable**. This cannot be disabled as SAP HANA manages all log backups.
  - We have set **2 hours** as the Backup schedule and **15 days** of retention period.

### Log Backup Policy

Log Backup ⓘ

Enable    Disable

Backup schedule

2 hours

Retained for

15 Day(s)

**NOTE**

Log backups only begin to flow after one successful full backup is completed.

9. Click **OK** to save the policy and return to the main **Backup policy** menu.
10. After you finish defining the backup policy, click **OK**.

You have now successfully configured backup(s) for your SAP HANA database(s).

## Next Steps

- Learn how to [run on-demand backups on SAP HANA databases running on Azure VMs](#)
- Learn how to [restore SAP HANA databases running on Azure VMs](#)
- Learn how to [manage SAP HANA databases that are backed up using Azure Backup](#)
- Learn how to [troubleshoot common issues when backing up SAP HANA databases](#)

# Back up Azure file shares in the Azure portal

1/20/2020 • 3 minutes to read • [Edit Online](#)

This tutorial explains how to use the Azure portal to back up [Azure file shares](#).

In this guide, you learn how to:

- Configure a Recovery Services vault to back up Azure Files
- Run an on-demand backup job to create a restore point

## Prerequisites

Before you can back up an Azure file share, ensure that it's present in one of the [supported Storage Account types](#).

Once you have verified this, you can protect your file shares.

## Limitations for Azure file share backup during preview

Backup for Azure file shares is in preview. Azure file shares in both general-purpose v1 and general-purpose v2 storage accounts are supported. The following backup scenarios aren't supported for Azure file shares:

- There is no CLI available for protecting Azure Files using Azure Backup.
- The maximum number of scheduled backups per day is one.
- The maximum number of on-demand backups per day is four.
- Use [resource locks](#) on the storage account to prevent accidental deletion of backups in your Recovery Services vault.
- Do not delete snapshots created by Azure Backup. Deleting snapshots can result in loss of recovery points and/or restore failures.
- Do not delete file shares that are protected by Azure Backup. The current solution will delete all snapshots taken by Azure Backup once the file share is deleted and hence lose all restore points

Back up for Azure File Shares in Storage Accounts with [zone redundant storage](#) (ZRS) replication is currently available only in Central US (CUS), East US (EUS), East US 2 (EUS2), North Europe (NE), SouthEast Asia (SEA), West Europe (WE) and West US 2 (WUS2).

## Configuring backup for an Azure file share

This tutorial assumes you already have established an Azure file share. To back up your Azure file share:

1. Create a Recovery Services vault in the same region as your file share. If you already have a vault, open your vault's Overview page and click **Backup**.

The screenshot shows the Azure Recovery Services vault interface for 'contosovault01'. At the top, there are buttons for '+ Backup', '+ Replicate', and 'Delete'. A message bar at the top right informs about new feature improvements for Linux VM backup. The main area is divided into sections: 'Monitoring' (Backup Alerts last 24 hours, showing 0 Critical and 0 Warning), 'Usage' (Backup items: 0, Backup Storage: Cloud - LRS: 0 B, Cloud - GRS: 0 B), and 'Backup Jobs' (In progress: 0, Failed: 0). On the left, a sidebar lists navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Properties, Locks, Automation script, Backup, Site Recovery, Jobs, Alerts and Events, and Backup Reports.

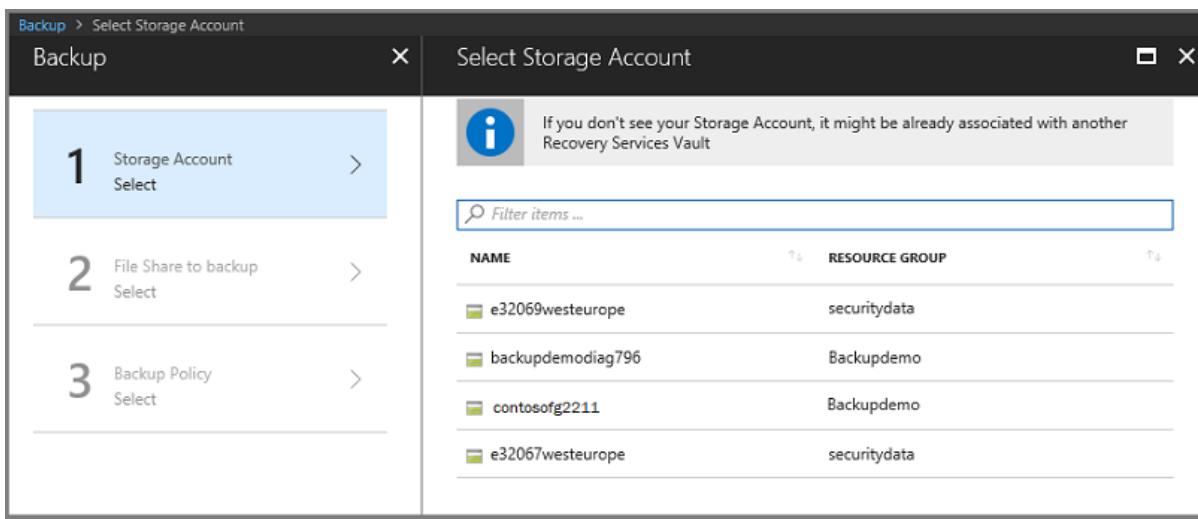
2. In the **Backup Goal** menu, from **What do you want to back up?**, choose Azure FileShare.

The screenshot shows the 'Backup Goal' configuration dialog. It asks 'Where is your workload running?' (set to 'Azure') and 'What do you want to backup?' (set to 'Virtual machine'). Below this, a list of options is shown: 'Virtual machine' (selected), 'Azure FileShare' (highlighted with a red box), and 'SQL Server in Azure VM'. At the bottom, a 'Backup' button is visible.

3. Click **Backup** to configure the Azure file share to your Recovery Services vault.

The screenshot shows the 'Backup Goal' configuration dialog again, but now it displays the 'Step: Configure Backup' step. The 'What do you want to backup?' dropdown is set to 'Azure FileShare'. At the bottom, a large blue 'Backup' button is highlighted with a red box.

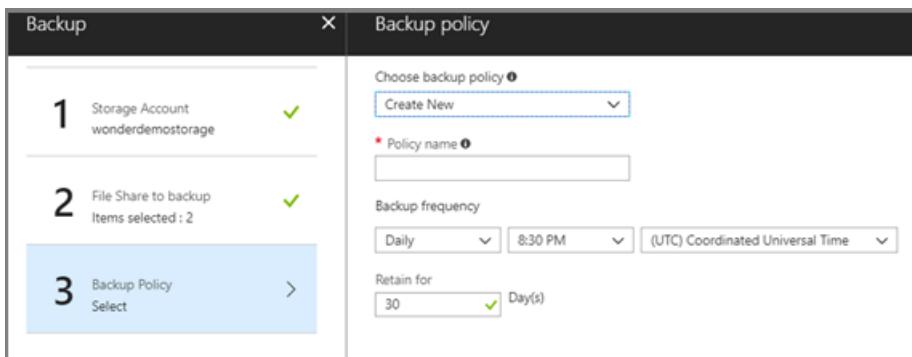
Once the vault is associated with the Azure file share, the Backup menu opens and prompts you to select a Storage account. The menu displays all supported Storage Accounts in the region where your vault exists that aren't already associated with a Recovery Services vault.



- In the list of Storage accounts, select an account, and click **OK**. Azure searches the storage account for files shares that can be backed up. If you recently added your file shares and do not see them in the list, allow a little time for the file shares to appear.



- From the **File Shares** list, select one or more of the file shares you want to back up, and click **OK**.
- After choosing your File Shares, the Backup menu switches to the **Backup policy**. From this menu either select an existing backup policy, or create a new one, and then click **Enable Backup**.



After establishing a backup policy, a snapshot of the File Shares will be taken at the scheduled time, and the recovery point is retained for the chosen period.

## Create an on-demand backup

After configuring the backup policy, you'll want to create an on-demand backup to ensure your data is protected until the next scheduled backup.

### To create an on-demand backup

- Open the Recovery Services vault that contains the file share recovery points, and click **Backup Items**. The list of Backup Item types appears.

| Backup Management Type      | Backup Item Count |
|-----------------------------|-------------------|
| SQL in Azure VM             | 4                 |
| Azure Backup Server         | 3                 |
| Azure Storage (Azure Files) | 3                 |
| Azure Virtual Machine       | 1                 |
| Azure Backup Agent          | 1                 |

2. From the list, select **Azure Storage (Azure Files)**. The list of Azure file shares appears.

| Backup Items (Azure Storage (Azure Files))                                                                              |                   |                |                      |                       |     |     |
|-------------------------------------------------------------------------------------------------------------------------|-------------------|----------------|----------------------|-----------------------|-----|-----|
| WonderDemoVault                                                                                                         |                   |                |                      |                       |     |     |
| <span>Refresh</span> <span>Add</span> <span>Filter</span>                                                               |                   |                |                      |                       |     |     |
|  Fetching data from service completed. |                   |                |                      |                       |     |     |
| NAME                                                                                                                    | STORAGE ACCOUNT   | RESOURCE GROUP | LAST BACKUP STATUS   | LAST BACKUP TIME      |     | ... |
| batshare                                                                                                                | wonderdemostorage | wonderdemorg   | <span>Success</span> | 15/2/2018, 6:02:58 AM | ... | ... |
| flashshare                                                                                                              | wonderdemostorage | wonderdemorg   | <span>Success</span> | 15/2/2018, 6:02:55 AM | ... | ... |

3. From the list of Azure file shares, select the desired file share. The Backup Item menu for the selected file share opens.

Dashboard > - Backup items > Backup Items (Azure Storage (Azure Files)) > dc-fileshare

### Wonderdemo

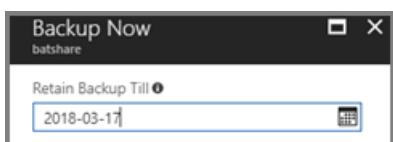
Backup Item

Backup now Restore Share File Recovery Resume backup Stop backup Delete backup data

Essentials ^

|                                        |                                            |
|----------------------------------------|--------------------------------------------|
| Recovery services vault<br>test-       | Last backup status<br>Success              |
| Subscription name<br>Subscription Name | Last backup time<br>9/18/2019, 10:00:41 AM |
| Subscription ID<br>Subscription ID     | Backup policy<br>FileSharePolicy           |
| Item type<br>Azure File Share          |                                            |
| Storage Account<br>Wonderdemostorage   |                                            |

4. From the Backup Item menu, click **Backup Now**. Because this is an on-demand backup job, there is no retention policy associated with the recovery point. The **Backup Now** dialog opens. Specify the last day you want to retain the recovery point.



## Next steps

In this tutorial, you used the Azure portal to:

- Configure a Recovery Services vault to back up Azure Files
- Run an on-demand backup job to create a restore point

Continue to the next article to restore from a backup of an Azure file share.

Restore from backup of Azure file shares

# Back up Windows Server to Azure

11/19/2019 • 4 minutes to read • [Edit Online](#)

You can use Azure Backup to protect your Windows Server from corruptions, attacks, and disasters. Azure Backup provides a lightweight tool known as the Microsoft Azure Recovery Services (MARS) agent. The MARS agent is installed on the Windows Server to protect files and folders, and server configuration info via Windows Server System State. This tutorial explains how you can use MARS Agent to back up your Windows Server to Azure. In this tutorial you learn how to:

- Download and set up the MARS Agent
- Configure back up times and retention schedule for your server's backups
- Perform an on-demand back up

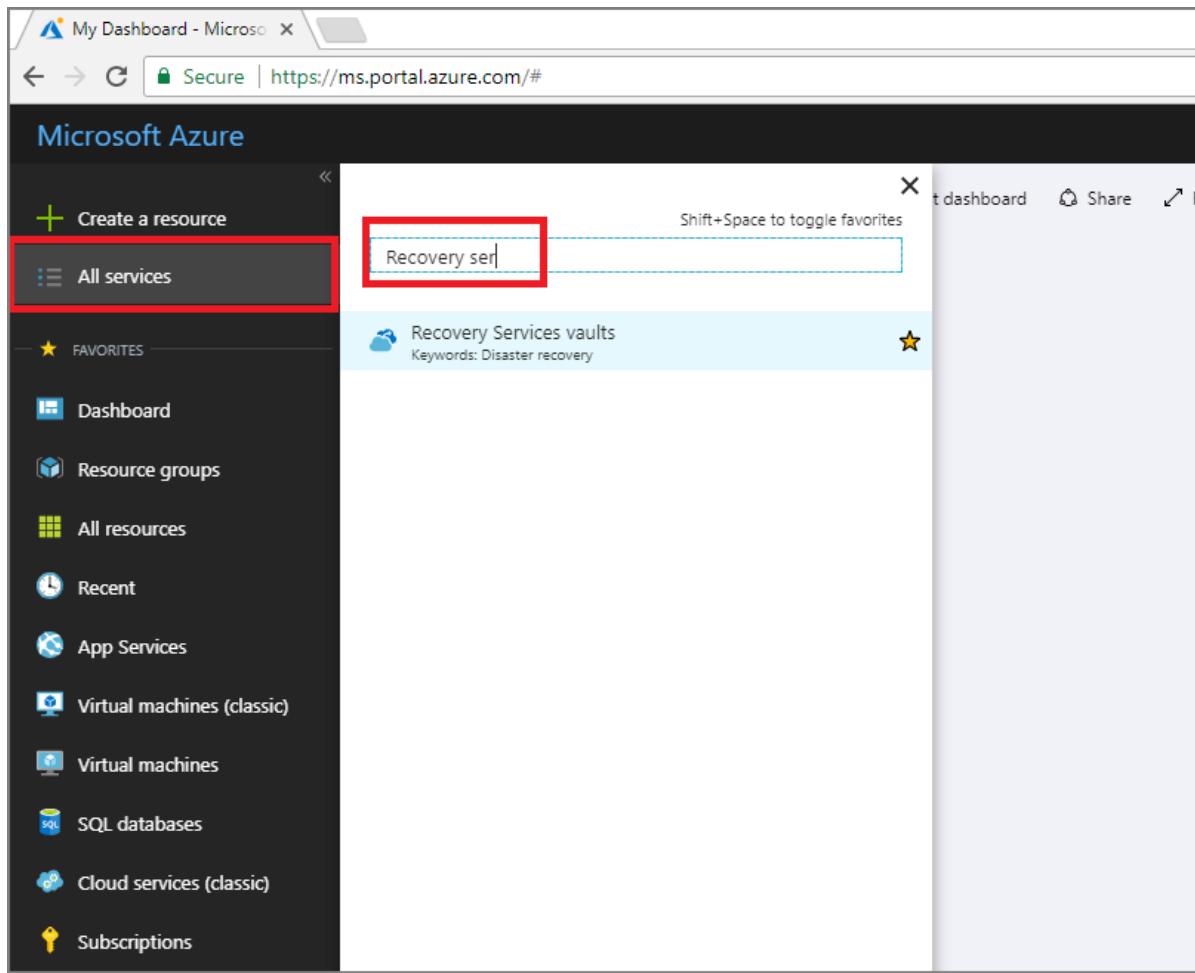
## Sign in to Azure

Sign in to the Azure portal at <https://portal.azure.com>.

## Create a Recovery Services vault

Before you can back up Windows Server, you must create a place for the backups, or restore points, to be stored. A [Recovery Services vault](#) is a container in Azure that stores the backups from your Windows Server. Follow the steps below to create a Recovery Services vault in the Azure portal.

1. On the left-hand menu, select **All services** and in the services list, type **Recovery Services**. Click **Recovery Services vaults**.



2. On the **Recovery Services vaults** menu, click **Add**.

A screenshot of the Microsoft Azure portal showing the 'Recovery Services vaults' blade. On the left, there's a sidebar with various icons. A red box highlights the '+ Add' button. The main content area shows a table with one row labeled 'SubscriptionID'. To the right, a 'Recovery Services vault' creation dialog is open. It contains fields for 'Name' (set to 'myRecoveryServicesVault'), 'Subscription' (set to 'SubscriptionID'), 'Resource group' (radio button selected for 'Use existing', value 'myResourceGroup'), and 'Location' (set to 'West Europe'). At the bottom, there's a 'Create' button highlighted with a red box and an 'Automation options' link.

3. In the **Recovery Services vault** menu,

- Type *myRecoveryServicesVault* in **Name**.
- The current subscription ID appears in **Subscription**.
- For **Resource group**, select **Use existing** and choose *myResourceGroup*. If *myResourceGroup* doesn't exist, select **Create New** and type *myResourceGroup*.

- From the **Location** drop-down menu, choose *West Europe*.
- Click **Create** to create your Recovery Services vault.

Once your vault is created, it appears in the list of Recovery Services vaults.

## Download Recovery Services agent

The Microsoft Azure Recovery Services (MARS) agent creates an association between Windows Server and your Recovery Services vault. The following procedure explains how to download the agent to your server.

- From the list of Recovery Services vaults, select **myRecoveryServicesVault** to open its dashboard.

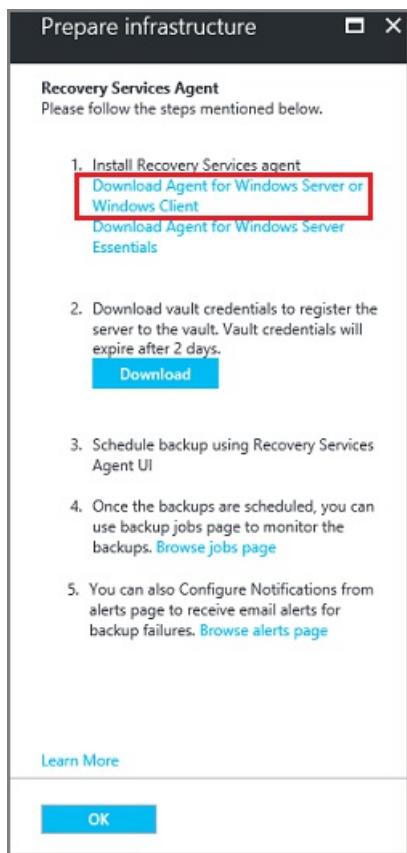
- On the vault dashboard menu, click **Backup**.

- On the **Backup Goal** menu:

| Backup Goal Settings            | Description                                           |
|---------------------------------|-------------------------------------------------------|
| Where is your workload running? | On-Premises                                           |
| What do you want to backup?     | 2 selected                                            |
|                                 | <input checked="" type="checkbox"/> Files and folders |
|                                 | <input type="checkbox"/> Hyper-V Virtual Machines     |
|                                 | <input type="checkbox"/> VMware Virtual Machines      |
|                                 | <input type="checkbox"/> Microsoft SQL Server         |
|                                 | <input type="checkbox"/> Microsoft SharePoint         |
|                                 | <input type="checkbox"/> Microsoft Exchange           |
|                                 | <input checked="" type="checkbox"/> System State      |
|                                 | <input type="checkbox"/> Bare Metal Recovery          |

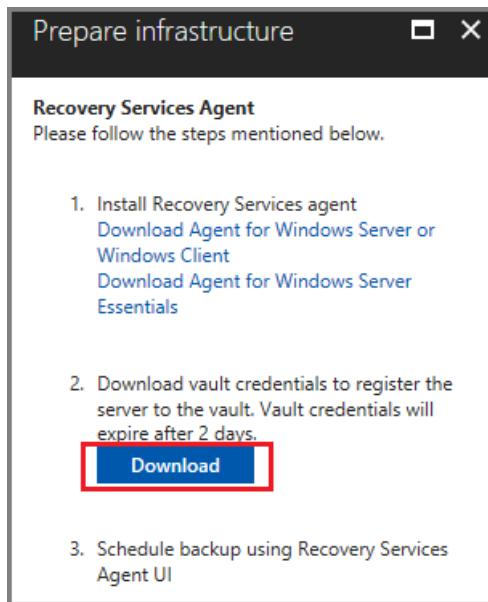
- Click **Prepare Infrastructure** to open the **Prepare infrastructure** menu.

- On the **Prepare infrastructure** menu, click **Download Agent for Windows Server or Windows Client** to download the *MARSAgentInstaller.exe*.



The installer opens a separate browser and downloads **MARSAgentInstaller.exe**.

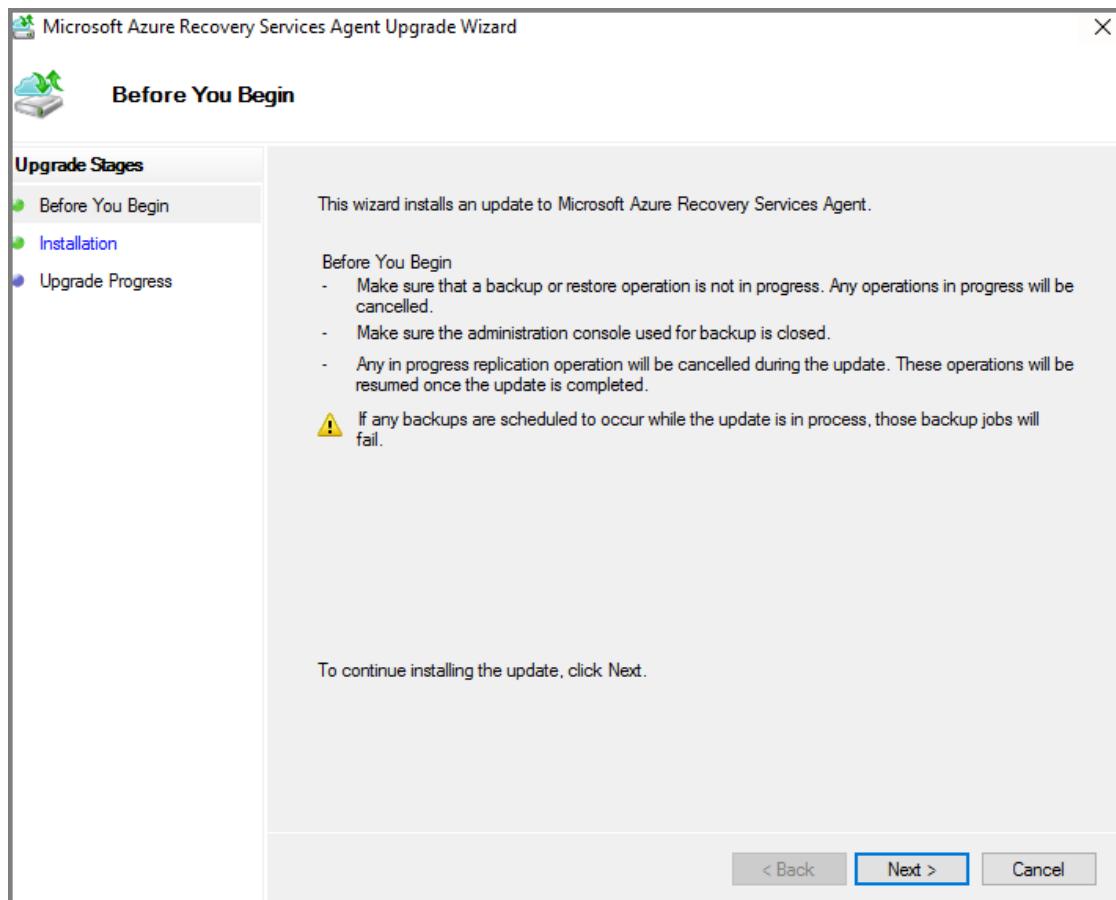
6. Before you run the downloaded file, on the Prepare infrastructure menu click **Download** and save the **Vault Credentials** file. Vault credentials are required to connect the MARS Agent with the Recovery Services vault.



## Install and register the agent

1. Locate and double-click the downloaded **MARSagentinstaller.exe**.
2. The **Microsoft Azure Recovery Services Agent Setup Wizard** appears. As you go through the wizard, provide the following information when prompted and click **Register**.
  - Location for the installation and cache folder.
  - Proxy server info if you use a proxy server to connect to the internet.

- Your user name and password details if you use an authenticated proxy.

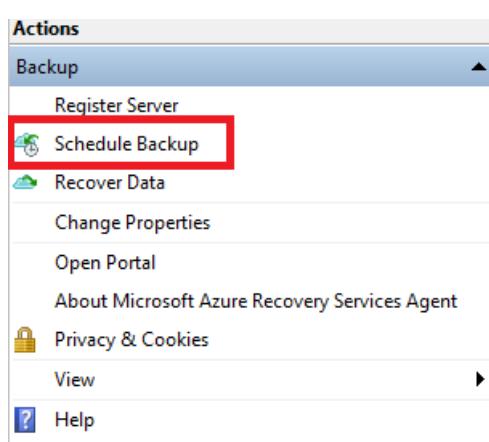


3. At the end of the wizard, click **Proceed to Registration** and provide the **Vault Credentials** file you downloaded in the previous procedure.
4. When prompted, provide an encryption passphrase to encrypt backups from Windows Server. Save the passphrase in a secure location as Microsoft cannot recover the passphrase if it is lost.
5. Click **Finish**.

## Configure Backup and Retention

You use the Microsoft Azure Recovery Services agent to schedule when backups to Azure, occur on Windows Server. Execute the following steps on the server where you downloaded the agent.

1. Open the Microsoft Azure Recovery Services agent. You can find it by searching your machine for **Microsoft Azure Backup**.
2. In the Recovery Services agent console, click **Schedule Backup** under the **Actions Pane**.

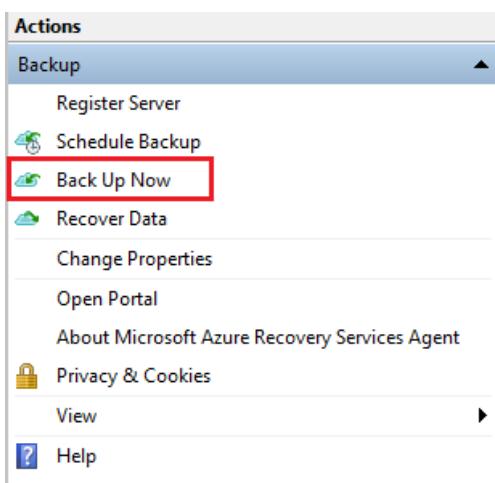


3. Click **Next** to navigate to the **Select Items to Back up** page.
4. Click **Add Items** and from the dialog box that opens, select **System State** and files or folders that you want to back up. Then click **OK**.
5. Click **Next**.
6. On the **Specify Backup Schedule (System State)** page, specify the time of the day, or week when backups need to be triggered for System State and click **Next**.
7. On the **Select Retention Policy (System State)** page, select the Retention Policy for the backup copy for System State and click **Next**.
8. Similarly, select the backup schedule and retention policy for selected files and folders.
9. On the **Choose Initial Back up Type** page, select **Automatically over the network**, and click **Next**.
10. On the **Confirmation** page, review the information, and click **Finish**.
11. After the wizard finishes creating the backup schedule, click **Close**.

## Perform an on-demand backup

You have established the schedule when backup jobs run. However, you have not backed up the server. It is a disaster recovery best practice to run an on-demand backup to ensure data resiliency for your server.

1. In the Microsoft Azure Recovery Services agent console, click **Back Up Now**.



2. On the **Back Up Now** wizard, select one from **Files and Folders** or **System State** that you want to back up and click **Next**.
3. On the **Confirmation** page, review the settings that the **Back Up Now** wizard uses to back up your server. Then click **Back Up**.
4. Click **Close** to close the wizard. If you close the wizard before the backup process finishes, the wizard continues to run in the background.
5. After the initial backup is completed, **Job completed** status appears in **Jobs** pane of the MARS agent console.

## Next steps

In this tutorial, you used the Azure portal to:

- Create a Recovery Services vault
- Download the Microsoft Azure Recovery Services agent

- Install the agent
- Configure backup for Windows Server
- Perform an on-demand backup

Continue to the next tutorial to recover files from Azure to Windows Server

[Restore files from Azure to Windows Server](#)

# Recover files from Azure to a Windows Server

11/18/2019 • 2 minutes to read • [Edit Online](#)

Azure Backup enables the recovery of individual items from backups of your Windows Server. Recovering individual files is helpful if you must quickly restore files that are accidentally deleted. This tutorial covers how you can use the Microsoft Azure Recovery Services Agent (MARS) agent to recover items from backups you have already performed in Azure. In this tutorial you learn how to:

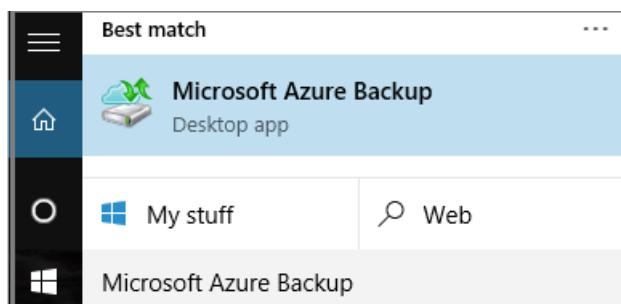
- Initiate recovery of individual items
- Select a recovery point
- Restore items from a recovery point

This tutorial assumes you have already performed the steps to [Back up a Windows Server to Azure](#) and have at least one backup of your Windows Server files in Azure.

## Initiate recovery of individual items

A helpful user interface wizard named Microsoft Azure Backup is installed with the Microsoft Azure Recovery Services (MARS) agent. The Microsoft Azure Backup wizard works with the Microsoft Azure Recovery Services (MARS) agent to retrieve backup data from recovery points stored in Azure. Use the Microsoft Azure Backup wizard to identify the files or folders you want to restore to Windows Server.

1. Open the **Microsoft Azure Backup** snap-in. You can find it by searching your machine for **Microsoft Azure Backup**.

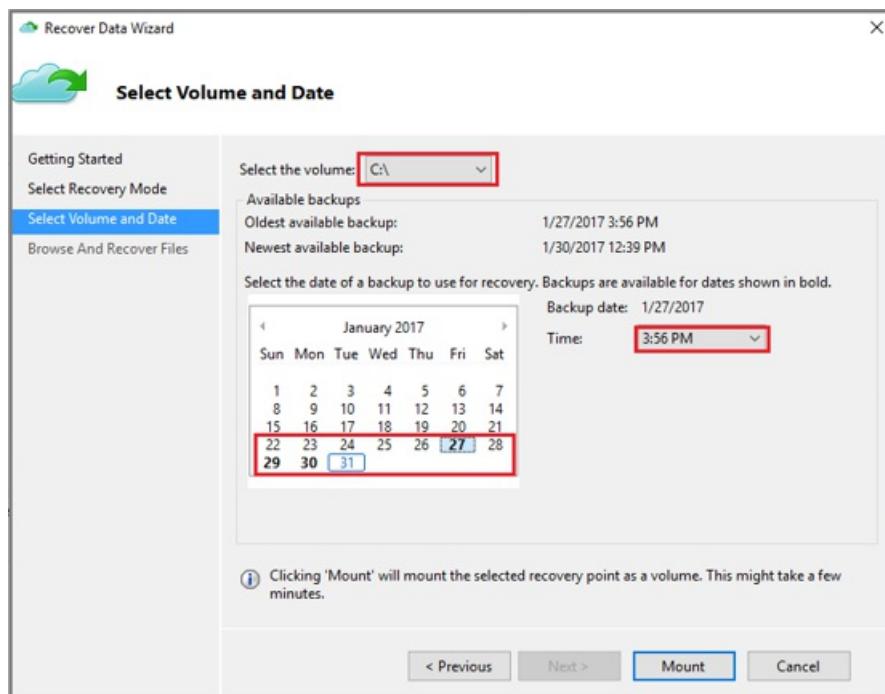


2. In the wizard, click **Recover Data** in the **Actions Pane** of the agent console to start the **Recover Data** wizard.



3. On the **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** to begin the recovery point selection process.

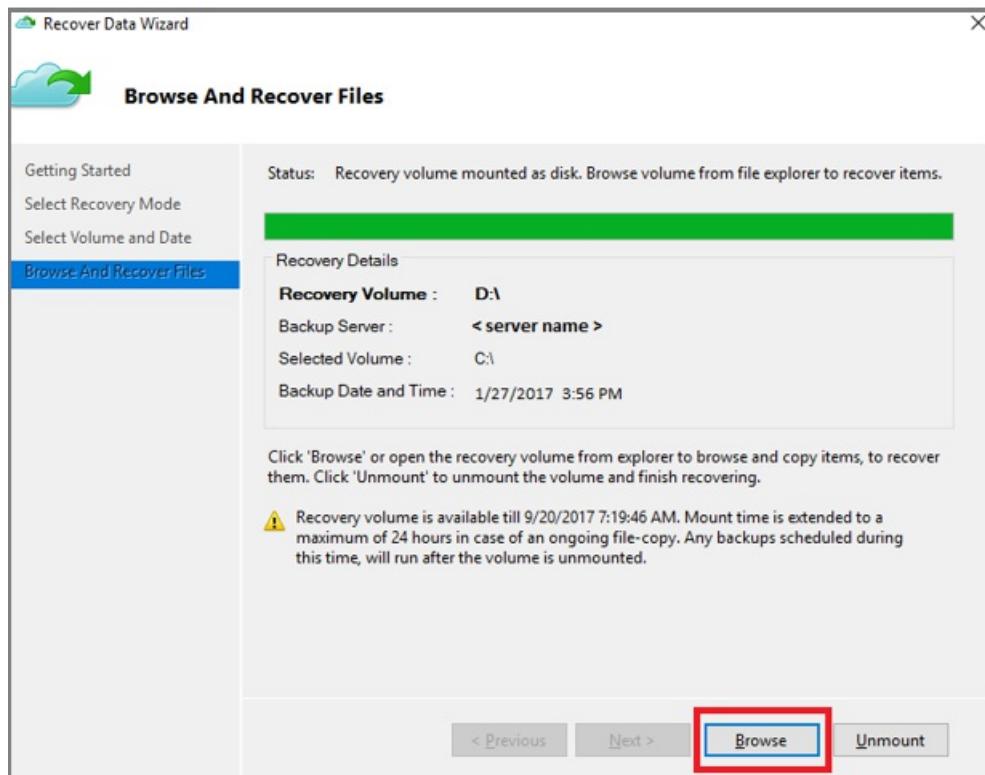
- On the **Select Volume and Date** page, select the volume that contains the files or folders you want to restore, and click **Mount**. Select a date, and select a time from the drop-down menu that corresponds to a recovery point. Dates in **bold** indicate the availability of at least one recovery point on that day.



When you click **Mount**, Azure Backup makes the recovery point available as a disk. Browse and recover files from the disk.

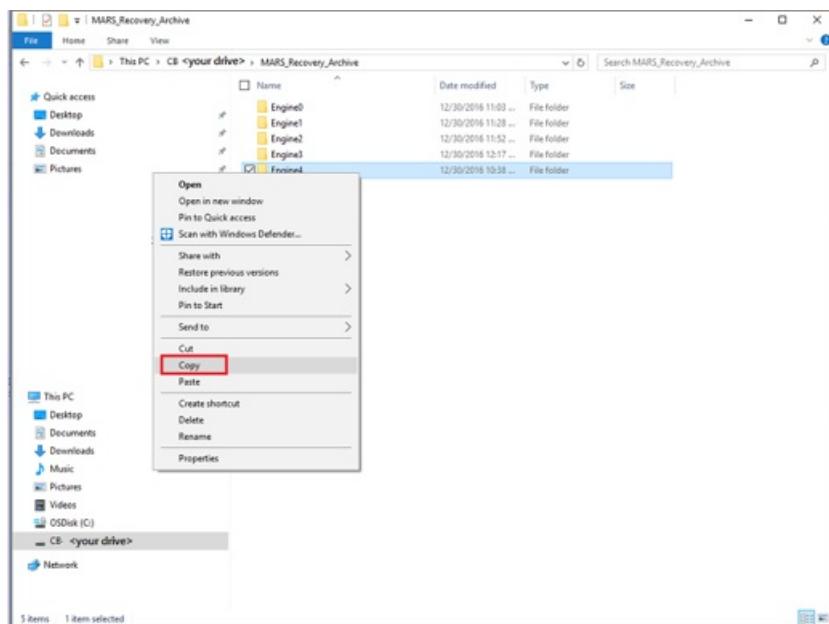
## Restore items from a recovery point

- Once the recovery volume is mounted, click **Browse** to open Windows Explorer and find the files and folders you wish to recover.

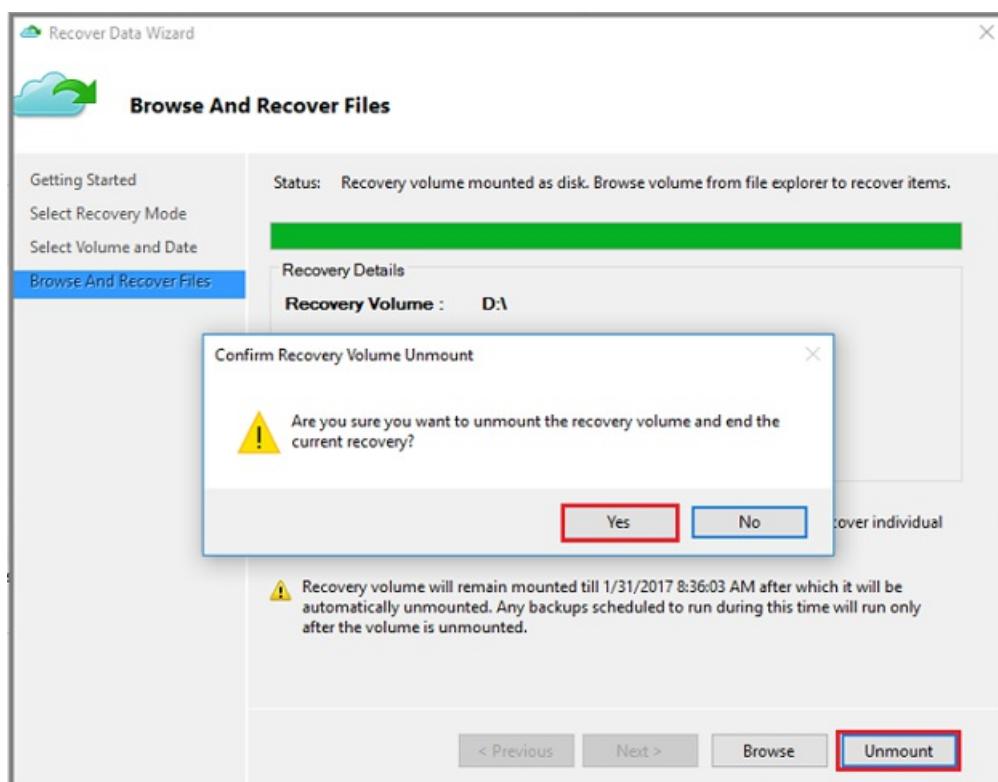


You can open the files directly from the recovery volume and verify the files.

2. In Windows Explorer, copy the files and/or folders you want to restore and paste them to any desired location on the server.



3. When you are finished restoring the files and/or folders, on the **Browse and Recovery Files** page of the **Recover Data** wizard, click **Unmount**.



4. Click **Yes** to confirm that you want to unmount the volume.

Once the snapshot is unmounted, **Job Completed** appears in the **Jobs** pane in the agent console.

## Next steps

This completes the tutorials on backing up and restoring Windows Server data to Azure. To learn more about Azure Backup, see the PowerShell sample for backing up encrypted virtual machines.

[Back up encrypted VM](#)

# Tutorial: Back up SAP HANA databases in an Azure VM using Azure CLI

12/23/2019 • 6 minutes to read • [Edit Online](#)

Azure CLI is used to create and manage Azure resources from the Command Line or through scripts. This documentation details how to back up an SAP HANA database and trigger on-demand backups - all using Azure CLI. You can also perform these steps using the [Azure portal](#).

This document assumes that you already have an SAP HANA database installed on an Azure VM. (You can also [create a VM using Azure CLI](#)). By the end of this tutorial, you'll be able to:

- Create a recovery services vault
- Register SAP HANA instance and discover database(s) on it
- Enable backup on an SAP HANA database
- Trigger an on-demand backup

Check out the [scenarios that we currently support](#) for SAP HANA.

## Use Azure Cloud Shell

Azure hosts Azure Cloud Shell, an interactive shell environment that you can use through your browser. You can use either Bash or PowerShell with Cloud Shell to work with Azure services. You can use the Cloud Shell preinstalled commands to run the code in this article without having to install anything on your local environment.

To start Azure Cloud Shell:

| OPTION                                                                                                                                                    | EXAMPLE/LINK                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Select <b>Try It</b> in the upper-right corner of a code block.<br>Selecting <b>Try It</b> doesn't automatically copy the code to Cloud Shell.            |  |
| Go to <a href="https://shell.azure.com">https://shell.azure.com</a> , or select the <b>Launch Cloud Shell</b> button to open Cloud Shell in your browser. |  |
| Select the <b>Cloud Shell</b> button on the menu bar at the upper right in the <a href="#">Azure portal</a> .                                             |  |

To run the code in this article in Azure Cloud Shell:

1. Start Cloud Shell.
2. Select the **Copy** button on a code block to copy the code.
3. Paste the code into the Cloud Shell session by selecting **Ctrl+Shift+V** on Windows and Linux or by selecting **Cmd+Shift+V** on macOS.
4. Select **Enter** to run the code.

To install and use the CLI locally, you must run Azure CLI version xx.xxx.x or later. To find the CLI version, run `az --version`. If you need to install or upgrade, see [Install the Azure CLI](#).

# Create a recovery services vault

A Recovery Services vault is a logical container that stores the backup data for each protected resource, such as Azure VMs or workloads running on Azure VMs - like SQL or HANA 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.

Create a Recovery Services vault with [az backup vault create](#). Specify the same resource group and location as the VM you wish to protect. Learn how to create a VM using Azure CLI with this [VM quickstart](#).

For this tutorial, we'll be using the following:

- a resource group named *saphanaResourceGroup*
- a VM named *saphanaVM*
- resources in the *westus2* location.

We'll be creating a vault named *saphanaVault*.

```
az backup vault create --resource-group saphanaResourceGroup \
--name saphanaVault \
--location westus2
```

By default, the Recovery Services vault is set for Geo-Redundant storage. Geo-Redundant storage ensures your backup data is replicated to a secondary Azure region that is hundreds of miles away from the primary region. If the storage redundancy setting needs to be modified, use the [az backup vault backup-properties set](#) cmdlet.

```
az backup vault backup-properties set \
--name saphanaVault \
--resource-group saphanaResourceGroup \
--backup-storage-redundancy "LocallyRedundant/GeoRedundant"
```

To see if your vault was successfully created, use the [az backup vault list](#) cmdlet. You'll see the following response:

| Location | Name         | ResourceGroup        |
|----------|--------------|----------------------|
| -----    | -----        | -----                |
| westus2  | saphanaVault | saphanaResourceGroup |

## Register and protect the SAP HANA instance

For the SAP HANA instance (the VM with SAP HANA installed on it) to be discovered by the Azure services, a [pre-registration script](#) must be run on the SAP HANA machine. Make sure that all the [prerequisites](#) are met before running the script. To learn more about what the script does, refer to the [setting up permissions](#) section.

Once the script is run, the SAP HANA instance can be registered with the recovery services vault we created earlier. To register the instance, use the [az backup container register](#) cmdlet. *VMResourceId* is the resource ID of the VM that you created to install SAP HANA.

```
az backup container register --resource-group saphanaResourceGroup \
--vault-name saphanaVault \
--location westus2 \
--workload-type SAPHANA \
--backup-management-type AzureWorkload \
--resource-id VMResourceId
```

#### NOTE

If the VM is not in the same resource group as the vault, then *saphanaResourceGroup* refers to the resource group where the vault was created.

Registering the SAP HANA instance automatically discovers all its current databases. However, to discover any new databases that may be added in the future refer to the [Discovering new databases added to the registered SAP HANA instance](#) section.

To check if the SAP HANA instance is successfully registered with your vault, use the [az backup container list](#) cmdlet. You'll see the following response:

| Name                                                                      | Friendly Name | Resource Group       | Type          |
|---------------------------------------------------------------------------|---------------|----------------------|---------------|
| Registration Status                                                       |               |                      |               |
| VMApplianceContainer;Compute;saphanaResourceGroup;saphanaVM<br>Registered | saphanaVM     | saphanaResourceGroup | AzureWorkload |

#### NOTE

The column "name" in the above output refers to the container name. This container name will be used in the next sections to enable backups and trigger them. Which in this case, is *VMApplianceContainer;Compute;saphanaResourceGroup;saphanaVM*.

## Enable backup on SAP HANA database

The [az backup protectable-item list](#) cmdlet lists out all the databases discovered on the SAP HANA instance that you registered in the previous step.

```
az backup protectable-item list --resource-group saphanaResourceGroup \
 --vault-name saphanaVault \
 --workload-type SAPHANA \
 --output table
```

You should find the database that you want to back up in this list, which will look as follows:

| Name                         | Protectable Item Type | ParentName | ServerName | IsProtected  |
|------------------------------|-----------------------|------------|------------|--------------|
| saphanasystem;hxe            | SAPHanaSystem         | HXE        | hxehost    | NotProtected |
| saphanadatabase;hxe;systemdb | SAPHanaDatabase       | HXE        | hxehost    | NotProtected |
| saphanadatabase;hxe;hxe      | SAPHanaDatabase       | HXE        | hxehost    | NotProtected |

As you can see from the above output, the SID of the SAP HANA system is HXE. In this tutorial, we'll configure backup for the *saphanadatabase;hxe;hxe* database that resides on the *hxehost* server.

To protect and configure backup on a database, one at a time, we use the [az backup protection enable-for-azurewl](#) cmdlet. Provide the name of the policy that you want to use. To create a policy using CLI, use the [az backup policy create](#) cmdlet. For this tutorial, we'll be using the *saphanaPolicy* policy.

```
az backup protection enable-for-azurewl --resource-group saphanaResourceGroup \
--policy-name saphanaPolicy \
--protectable-item-name saphanadatabase;hxe;hxe \
--protectable-item-type SAPHANADatabase \
--server-name hxehost \
--workload-type SAPHANA \
--output table
```

You can check if the above backup configuration is complete using the [az backup job list](#) cmdlet. The output will display as follows:

| Name                                 | Operation       | Status    | Item Name | Start Time UTC                |
|--------------------------------------|-----------------|-----------|-----------|-------------------------------|
| e0f15dae-7cac-4475-a833-f52c50e5b6c3 | ConfigureBackup | Completed | hxe       | 2019-12-03T03:09:210831+00:00 |

The [az backup job list](#) cmdlet lists out all the backup jobs (scheduled or on-demand) that have run or are currently running on the protected database, in addition to other operations like register, configure backup, delete backup data etc.

## Trigger an on-demand backup

While the above section details how to configure a scheduled backup, this section talks about triggering an on-demand backup. To do this, we use the [az backup protection backup-now](#) cmdlet.

### NOTE

The retention policy of an on-demand backup is determined by the underlying retention policy for the database.

```
az backup protection backup-now --resource-group saphanaResourceGroup \
--item-name saphanadatabase;hxe;hxe \
--vault-name saphanaVault \
--container-name VMAppContainer;Compute;saphanaResourceGroup;saphanaVM \
--backup-type Full \
--retain-until 01-01-2040 \
--output table
```

The output will display as follows:

| Name                                 | ResourceGroup        |
|--------------------------------------|----------------------|
| e0f15dae-7cac-4475-a833-f52c50e5b6c3 | saphanaResourceGroup |

The response will give you the job name. This job name can be used to track the job status using the [az backup job show](#) cmdlet.

### NOTE

In addition to scheduling a full or differential backup, they can also be currently triggered manually. Log backups are automatically triggered and managed by SAP HANA internally.

Incremental backups are not currently supported by Azure Backup.

## Next steps

- To learn how to restore an SAP HANA database in Azure VM using CLI, continue to the tutorial – [Restore an SAP HANA database in Azure VM using CLI](#)
- To learn how to back up an SAP HANA database running in Azure VM using Azure portal, refer to [Backup an SAP HANA databases on Azure VMs](#)

# Tutorial: Restore SAP HANA databases in an Azure VM using Azure CLI

12/23/2019 • 5 minutes to read • [Edit Online](#)

Azure CLI is used to create and manage Azure resources from the command line or through scripts. This documentation details how to restore a backed-up SAP HANA database on an Azure VM - using Azure CLI. You can also perform these steps using the [Azure portal](#).

Use [Azure Cloud Shell](#) to run CLI commands.

By the end of this tutorial you'll be able to:

- View restore points for a backed-up database
- Restore a database

This tutorial assumes you have an SAP HANA database running on Azure VM that is backed-up using Azure Backup. If you've used [Back up an SAP HANA database in Azure using CLI](#) to back up your SAP HANA database, then you're using the following resources:

- a resource group named *saphanaResourceGroup*
- a vault named *saphanaVault*
- protected container named *VMApContainer;Compute;saphanaResourceGroup;saphanaVM*
- backed-up database/item named *saphanadatabase;hxe;hxe*
- resources in the *westus2* region

## View restore points for a backed-up database

To view the list of all the recovery points for a database, use the [az backup recoverypoint list](#) cmdlet as follows:

```
az backup recoverypoint list --resource-group saphanaResourceGroup \
 --vault-name saphanaVault \
 --container-name VMApContainer;Compute;saphanaResourceGroup;saphanaVM \
 --item-name saphanadatabase;hxe;hxe \
 --output table
```

The list of recovery points will look as follows:

| Name                      | Time                             | BackupManagementType | Item Name               |
|---------------------------|----------------------------------|----------------------|-------------------------|
| RecoveryPointType         | -----                            | -----                | -----                   |
| 7660777527047692711       | 2019-12-10T04:00:32.346000+00:00 | AzureWorkload        | SAPHanaDatabase;hxe;hxe |
| Full                      |                                  |                      |                         |
| 7896624824685666836       | 2019-12-15T10:33:32.346000+00:00 | AzureWorkload        | SAPHanaDatabase;hxe;hxe |
| Differential              |                                  |                      |                         |
| DefaultRangeRecoveryPoint |                                  | AzureWorkload        | SAPHanaDatabase;hxe;hxe |
| Log                       |                                  |                      |                         |

As you can see, the list above contains three recovery points: one each for full, differential, and log backup.

#### NOTE

You can also view the start and end points of every unbroken log backup chain, using the [az backup recoverypoint show-log-chain](#) cmdlet.

## Prerequisites to restore a database

Ensure that the following prerequisites are met before restoring a database:

- You can restore the database only to an SAP HANA instance that is in the same region
- The target instance must be registered with the same vault as the source
- Azure Backup can't identify two different SAP HANA instances on the same VM. Therefore, restoring data from one instance to another on the same VM isn't possible.

## Restore a database

Azure Backup can restore SAP HANA databases that are running on Azure VMs as follows:

- Restore to a specific date or time (to the second) by using log backups. Azure Backup automatically determines the appropriate full, differential backups and the chain of log backups that are required to restore based on the selected time.
- Restore to a specific full or differential backup to restore to a specific recovery point.

To restore a database, use the [az restore restore-azurewl](#) cmdlet, which requires a recovery config object as one of the inputs. This object can be generated using the [az backup recoveryconfig show](#) cmdlet. The recovery config object contains all the details to perform a restore. One of them being the restore mode –

**OriginalWorkloadRestore** or **AlternateWorkloadRestore**.

#### NOTE

**OriginalWorkloadRestore** - Restore the data to the same SAP HANA instance as the original source. This option overwrites the original database.

**AlternateWorkloadRestore** - Restore the database to an alternate location and keep the original source database.

## Restore to alternate location

To restore a database to an alternate location, use **AlternateWorkloadRestore** as the restore mode. You must then choose the restore point, which could either be a previous point-in-time or any of the previous restore points.

In this tutorial, you'll restore to a previous restore point. [View the list of restore points](#) for the database and choose the point you want to restore to. This tutorial will use the restore point with the name `7660777527047692711`.

Using the above restore point name and the restore mode, let's create the recovery config object using the [az backup recoveryconfig show](#) cmdlet. Let's look at what each of the remaining parameters in this cmdlet mean:

- **--target-item-name** This is the name that the restored database will be using. In this case, we used the name `restored_database`.
- **--target-server-name** This is the name of an SAP HANA server that is successfully registered to a recovery services vault and lies in the same region as the database to be restored. For this tutorial, we'll restore the database to the same SAP HANA server that we have protected, named `hxehost`.
- **--target-server-type** For the restore of SAP HANA databases, **SapHanaDatabase** must be used.

```
az backup recoveryconfig show --resource-group saphanaResourceGroup \
--vault-name saphanaVault \
--container-name VMAppContainer;Compute;saphanaResourceGroup;saphanaVM \
--item-name saphanadatabase;hxe;hxe \
--restore-mode AlternateWorkloadRestore \
--rp-name 7660777527047692711 \
--target-item-name restored_database \
--target-server-name hxehost \
--target-server-type HANAInstance \
--workload-type SAPHANA \
--output json
```

The response to the above query will be a recovery config object that looks something like this:

```
{"\"restore_mode\": \"OriginalLocation\", \"container_uri\": \"VMAppContainer;Compute;saphanaResourceGroup;saphanaVM \", \"item_uri\": \"SAPHanaDatabase;hxe;hxe\", \"recovery_point_id\": \"DefaultRangeRecoveryPoint\", \"log_point_in_time\": \"28-11-2019-09:53:00\", \"item_type\": \"SAPHana\", \"source_resource_id\": \"/subscriptions/ef4ab5a7-c2c0-4304-af80-af49f48af3d1/resourceGroups/saphanaResourceGroup/providers/Microsoft.Compute/virtualMachines/saphanavm\", \"database_name\": null, \"container_id\": null, \"alternate_directory_paths\": null}"
```

Now, to restore the database run the [az restore restore-azurewl](#) cmdlet. To use this command, we will enter the above json output that is saved to a file named *recoveryconfig.json*.

```
az backup restore restore-azurewl --resource-group saphanaResourceGroup \
--vault-name saphanaVault \
--restore-config recoveryconfig.json \
--output table
```

The output will look like this:

| Name                                 | Resource |
|--------------------------------------|----------|
| 5b198508-9712-43df-844b-977e5dfc30ea | SAPHANA  |

The response will give you the job name. This job name can be used to track the job status using [az backup job show](#) cmdlet.

## Restore and overwrite

To restore to the original location, we'll use **OriginalWorkloadRestore** as the restore mode. You must then choose the restore point, which could either be a previous point-in-time or any of the previous restore points.

For this tutorial, we'll choose the previous point-in-time "28-11-2019-09:53:00" to restore to. You can provide this restore point in the following formats: dd-mm-yyyy, dd-mm-yyyy-hh:mm:ss. To choose a valid point-in-time to restore to, use the [az backup recoverypoint show-log-chain](#) cmdlet, which lists the intervals of unbroken log chain backups.

```
az backup recoveryconfig show --resource-group saphanaResourceGroup \
--vault-name saphanaVault \
--container-name VMAppContainer;Compute;saphanaResourceGroup;saphanaVM \
--item-name saphanadatabase;hxe;hxe \
--restore-mode OriginalWorkloadRestore \
--log-point-in-time 28-11-2019-09:53:00 \
--output json
```

The response to the above query will be a recovery config object that looks as follows:

```
{"\"restore_mode\": \"OriginalLocation\", \"container_uri\": \"VMAppContainer;Compute;saphanaResourceGroup;saphanaVM \", \"item_uri\": \"SAPHanaDatabase;hx;hx\", \"recovery_point_id\": \"DefaultRangeRecoveryPoint\", \"log_point_in_time\": \"28-11-2019-09:53:00\", \"item_type\": \"SAPHana\", \"source_resource_id\": \"/subscriptions/ef4ab5a7-c2c0-4304-af80-af49f48af3d1/resourceGroups/saphanaResourceGroup/providers/Microsoft.Compute/virtualMachines/saphanavm\", \"database_name\": null, \"container_id\": null, \"alternate_directory_paths\": null}"
```

Now, to restore the database run the [az restore restore-azurewl](#) cmdlet. To use this command, we will enter the above json output that is saved to a file named *recoveryconfig.json*.

```
az backup restore restore-azurewl --resource-group saphanaResourceGroup \
--vault-name saphanaVault \
--restore-config recoveryconfig.json \
--output table
```

The output will look like this:

| Name                                 | Resource |
|--------------------------------------|----------|
| 5b198508-9712-43df-844b-977e5dfc30ea | SAPHANA  |

The response will give you the job name. This job name can be used to track the job status using the [az backup job show](#) cmdlet.

## Next steps

- To learn how to manage SAP HANA databases that are backed up using Azure CLI, continue to the tutorial [Manage an SAP HANA database in Azure VM using CLI](#)
- To learn how to restore an SAP HANA database running in Azure VM using the Azure portal, refer to [Restore an SAP HANA databases on Azure VMs](#)

# Tutorial: Manage SAP HANA databases in an Azure VM using Azure CLI

12/23/2019 • 4 minutes to read • [Edit Online](#)

Azure CLI is used to create and manage Azure resources from the Command Line or through scripts. This documentation details how to manage a backed-up SAP HANA database on Azure VM - all using Azure CLI. You can also perform these steps using [the Azure portal](#).

Use [Azure Cloud Shell](#) to run CLI commands.

By the end of this tutorial, you'll be able to:

- Monitor backup and restore jobs
- Protect new databases added to an SAP HANA instance
- Change the policy
- Stop protection
- Resume protection

If you've used [Back up an SAP HANA database in Azure using CLI](#) to back up your SAP HANA database, then you're using the following resources:

- a resource group named *saphanaResourceGroup*
- a vault named *saphanaVault*
- protected container named *VMApContainer;Compute;saphanaResourceGroup;saphanaVM*
- backed-up database/item named *saphanadatabase;hxe;hxe*
- resources in the *westus2* region

Azure CLI makes it easy to manage an SAP HANA database running on an Azure VM that is backed-up using Azure Backup. This tutorial details each of the management operations.

## Monitor backup and restore jobs

To monitor completed or currently running jobs (backup or restore), use the [az backup job list](#) cmdlet. CLI also allows you to [suspend a currently running job](#) or [wait until a job completes](#).

```
az backup job list --resource-group saphanaResourceGroup \
--vault-name saphanaVault \
--output table
```

The output will look something like this:

| Name                                 | Operation             | Status    | Item Name     | Start Time UTC |
|--------------------------------------|-----------------------|-----------|---------------|----------------|
| e0f15dae-7cac-4475-a833-f52c50e5b6c3 | ConfigureBackup       | Completed | hxe           | 2019-12-       |
| 03T03:09:210831+00:00                |                       |           |               |                |
| ccdb4dce-8b15-47c5-8c46-b0985352238f | Backup (Full)         | Completed | hxe [hxehost] | 2019-12-       |
| 01T10:30:58.867489+00:00             |                       |           |               |                |
| 4980af91-1090-49a6-ab96-13bc905a5282 | Backup (Differential) | Completed | hxe [hxehost] | 2019-12-       |
| 01T10:36:00.563909+00:00             |                       |           |               |                |
| F7c68818-039f-4a0f-8d73-e0747e68a813 | Restore (Log)         | Completed | hxe [hxehost] | 2019-12-       |
| 03T05:44:51.081607+00:00             |                       |           |               |                |

## Change policy

To change the policy underlying the SAP HANA backup configuration, use the [az backup policy set cmdlet](#). The name parameter in this cmdlet refers to the backup item whose policy we want to change. For this tutorial, we'll be replacing the policy of our SAP HANA database `saphanadatabase;hxe;hxe` with a new policy `newsaphanaPolicy`. New policies can be created using the [az backup policy create cmdlet](#).

```
az backup item set policy --resource-group saphanaResourceGroup \
--vault-name saphanaVault \
--container-name VMAppContainer;Compute;saphanaResourceGroup;saphanaVM \
--policy-name newsaphanaPolicy \
--name saphanadatabase;hxe;hxe \
```

The output should look like this:

| Name                                 | Resource Group |
|--------------------------------------|----------------|
| cb110094-9b15-4c55-ad45-6899200eb8dd | SAPHANA        |

## Protect new databases added to an SAP HANA instance

[Registering an SAP HANA instance with a recovery services vault](#) automatically discovers all the databases on this instance.

However, in cases when new databases are added to the SAP HANA instance later, use the [az backup protectable-item initialize cmdlet](#). This cmdlet discovers the new databases added.

```
az backup protectable-item initialize --resource-group saphanaResourceGroup \
--vault-name saphanaVault \
--container-name VMAppContainer;Compute;saphanaResourceGroup;saphanaVM \
--workload-type SAPHANA
```

Then use the [az backup protectable-item list cmdlet](#) to list all the databases that have been discovered on your SAP HANA instance. This list, however, excludes those databases on which backup has already been configured. Once the database to be backed-up is discovered, refer to [Enable backup on SAP HANA database](#).

```
az backup protectable-item list --resource-group saphanaResourceGroup \
--vault-name saphanaVault \
--workload-type SAPHANA \
--output table
```

The new database that you want to back up will show up in this list, which will look as follows:

| Name                         | Protectable Item Type | ParentName | ServerName | IsProtected  |
|------------------------------|-----------------------|------------|------------|--------------|
| saphanasystem;hxe            | SAPHanaSystem         | HXE        | hxehost    | NotProtected |
| saphanadatabase;hxe;systemdb | SAPHanaDatabase       | HXE        | hxehost    | NotProtected |
| saphanadatabase;hxe;newhxe   | SAPHanaDatabase       | HXE        | hxehost    | NotProtected |

## Stop protection for an SAP HANA database

You can stop protecting an SAP HANA database in a couple of ways:

- Stop all future backup jobs and delete all recovery points.

- Stop all future backup jobs and leave the recovery points intact.

If you choose to leave recovery points, keep these details in mind:

- All recovery points will remain intact forever, all pruning shall stop at stop protection with retain data.
- You'll be charged for the protected instance and the consumed storage.
- If you delete a data source without stopping backups, new backups will fail.

Let's look at each of the ways to stop protection in more detail.

### Stop protection with retain data

To stop protection with retain data, use the [az backup protection disable](#) cmdlet.

```
az backup protection disable --resource-group saphanaResourceGroup \
--vault-name saphanaVault \
--container-name VMAppContainer;Compute;saphanaResourceGroup;saphanaVM \
--item-name saphanadatabase;hx;hxe \
--workload-type SAPHANA \
--output table
```

The output should look like this:

| Name                                 | ResourceGroup        |
|--------------------------------------|----------------------|
| <hr/>                                |                      |
| g0f15dae-7cac-4475-d833-f52c50e5b6c3 | saphanaResourceGroup |

To check the status of this operation, use the [az backup job show](#) cmdlet.

### Stop protection without retain data

To stop protection without retain data, use the [az backup protection disable](#) cmdlet.

```
az backup protection disable --resource-group saphanaResourceGroup \
--vault-name saphanaVault \
--container-name VMAppContainer;Compute;saphanaResourceGroup;saphanaVM \
--item-name saphanadatabase;hx;hxe \
--workload-type SAPHANA \
--delete-backup-data true \
--output table
```

The output should look like this:

| Name                                 | ResourceGroup        |
|--------------------------------------|----------------------|
| <hr/>                                |                      |
| g0f15dae-7cac-4475-d833-f52c50e5b6c3 | saphanaResourceGroup |

To check the status of this operation, use the [az backup job show](#) cmdlet.

## Resume protection

When you stop protection for the SAP HANA database with retain data, you can later resume protection. If you don't retain the backed-up data, you won't be able to resume protection.

To resume protection, use the [az backup protection resume](#) cmdlet.

```
az backup protection resume --resource-group saphanaResourceGroup \
--vault-name saphanaVault \
--container-name VMAppContainer;Compute;saphanaResourceGroup;saphanaVM \
--policy-name saphanaPolicy \
--output table
```

The output should look like this:

| Name                                 | ResourceGroup        |
|--------------------------------------|----------------------|
| b2a7f108-1020-4529-870f-6c4c43e2bb9e | saphanaResourceGroup |

To check the status of this operation, use the [az backup job show](#) cmdlet.

## Next steps

- To learn how to back up an SAP HANA database running on Azure VM using the Azure portal, refer to [Backup SAP HANA databases on Azure VMs](#)
- To learn how to manage a backed-up SAP HANA database running on Azure VM using the Azure portal, refer to [Manage Backed up SAP HANA databases on Azure VM](#)

# Support matrix for Azure Backup

2/20/2020 • 7 minutes to read • [Edit Online](#)

You can use [Azure Backup](#) to back up data to the Microsoft Azure cloud platform. This article summarizes the general support settings and limitations for Azure Backup scenarios and deployments.

Other support matrices are available:

- Support matrix for [Azure virtual machine \(VM\) backup](#)
- Support matrix for backup by using [System Center Data Protection Manager \(DPM\)/Microsoft Azure Backup Server \(MABS\)](#)
- Support matrix for backup by using the [Microsoft Azure Recovery Services \(MARS\) agent](#)

## NOTE

This service supports [Azure delegated resource management](#), which lets service providers sign in to their own tenant to manage subscriptions and resource groups that customers have delegated. For more info, see [Azure Lighthouse](#).

## Vault support

Azure Backup uses Recovery Services vaults to orchestrate and manage backups. It also uses vaults to store backed-up data.

The following table describes the features of Recovery Services vaults:

| FEATURE                              | DETAILS                                                                                                                                                                |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Vaults in subscription</b>        | Up to 500 Recovery Services vaults in a single subscription.                                                                                                           |
| <b>Machines in a vault</b>           | Up to 1,000 Azure VMs in a single vault.<br>Up to 50 MABS servers can be registered in a single vault.                                                                 |
| <b>Data sources in vault storage</b> | Maximum 54,400 GB. There's no limit for Azure VM backups.                                                                                                              |
| <b>Backups to vault</b>              | <b>Azure VMs:</b> Once a day.<br><b>Machines protected by DPM/MABS:</b> Twice a day.<br><b>Machines backed up directly by using the MARS agent:</b> Three times a day. |
| <b>Backups between vaults</b>        | Backup is within a region.<br>You need a vault in every Azure region that contains VMs you want to back up. You can't back up to a different region.                   |
| <b>Move vaults</b>                   | You can <a href="#">move vaults</a> across subscriptions or between resource groups in the same subscription. However, moving vaults across regions isn't supported.   |

| FEATURE                          | DETAILS                                                                                                                                                                                                                  |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Move data between vaults</b>  | Moving backed-up data between vaults isn't supported.                                                                                                                                                                    |
| <b>Modify vault storage type</b> | You can modify the storage replication type (either geo-redundant storage or locally redundant storage) for a vault before backups are stored. After backups begin in the vault, the replication type can't be modified. |

## On-premises backup support

Here's what's supported if you want to back up on-premises machines:

| MACHINE                                                 | WHAT'S BACKED UP                                | LOCATION                                                        | FEATURES                                                                                                                            |
|---------------------------------------------------------|-------------------------------------------------|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>Direct backup of Windows machine with MARS agent</b> | Files, folders, system state                    | Back up to Recovery Services vault.                             | Back up three times a day<br>No app-aware backup<br>Restore file, folder, volume                                                    |
| <b>Direct backup of Linux machine with MARS agent</b>   | Backup not supported                            |                                                                 |                                                                                                                                     |
| <b>Back up to DPM</b>                                   | Files, folders, volumes, system state, app data | Back up to local DPM storage. DPM then backs up to vault.       | App-aware snapshots<br>Full granularity for backup and recovery<br>Linux supported for VMs (Hyper-V/VMware)<br>Oracle not supported |
| <b>Back up to MABS</b>                                  | Files, folders, volumes, system state, app data | Back up to MABS local storage. MABS then backs up to the vault. | App-aware snapshots<br>Full granularity for backup and recovery<br>Linux supported for VMs (Hyper-V/VMware)<br>Oracle not supported |

## Azure VM backup support

### Azure VM limits

| LIMIT                          | DETAILS                                                                                                                                                                                         |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Azure VM data disks</b>     | Limit of 16<br>To sign up for the private preview of VMs with 16+ disks (up to 32 disks), write to us at <a href="mailto:AskAzureBackupTeam@microsoft.com">AskAzureBackupTeam@microsoft.com</a> |
| <b>Azure VM data disk size</b> | Individual disk size can be up to 32 TB and a maximum of 256 TB combined for all disks in a VM.                                                                                                 |

## Azure VM backup options

Here's what's supported if you want to back up Azure VMs:

| MACHINE                                      | WHAT'S BACKED UP                                | LOCATION                                                                                   | FEATURES                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------|-------------------------------------------------|--------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Azure VM backup by using VM extension</b> | Entire VM                                       | Back up to vault.                                                                          | <p>Extension installed when you enable backup for a VM.</p> <p>Back up once a day.</p> <p>App-aware backup for Windows VMs; file-consistent backup for Linux VMs. You can configure app-consistency for Linux machines by using custom scripts.</p> <p>Restore VM or disk.</p> <p>Can't back up an Azure VM to an on-premises location.</p> |
| <b>Azure VM backup by using MARS agent</b>   | Files, folders, system state                    | Back up to vault.                                                                          | <p>Back up three times a day.</p> <p>If you want to back up specific files or folders rather than the entire VM, the MARS agent can run alongside the VM extension.</p>                                                                                                                                                                     |
| <b>Azure VM with DPM</b>                     | Files, folders, volumes, system state, app data | Back up to local storage of Azure VM that's running DPM. DPM then backs up to vault.       | <p>App-aware snapshots.</p> <p>Full granularity for backup and recovery.</p> <p>Linux supported for VMs (Hyper-V/VMware).</p> <p>Oracle not supported.</p>                                                                                                                                                                                  |
| <b>Azure VM with MABS</b>                    | Files, folders, volumes, system state, app data | Back up to local storage of Azure VM that's running MABS. MABS then backs up to the vault. | <p>App-aware snapshots.</p> <p>Full granularity for backup and recovery.</p> <p>Linux supported for VMs (Hyper-V/VMware).</p> <p>Oracle not supported.</p>                                                                                                                                                                                  |

## Linux backup support

Here's what's supported if you want to back up Linux machines:

| BACKUP TYPE                                                      | LINUX (AZURE ENDORSED)                                                   |
|------------------------------------------------------------------|--------------------------------------------------------------------------|
| <b>Direct backup of on-premises machine that's running Linux</b> | Not supported. The MARS agent can be installed only on Windows machines. |

| BACKUP TYPE                                                           | LINUX (AZURE ENDORSED)                                                                                                                             |
|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Using agent extension to back up Azure VM that's running Linux</b> | App-consistent backup by using <a href="#">custom scripts</a> .<br>File-level recovery.<br>Restore by creating a VM from a recovery point or disk. |
| <b>Using DPM to back up on-premises machines running Linux</b>        | File-consistent backup of Linux Guest VMs on Hyper-V and VMWare.<br>VM restoration of Hyper-V and VMWare Linux Guest VMs.                          |
| <b>Using MABS to back up on-premises machines running Linux</b>       | File-consistent backup of Linux Guest VMs on Hyper-V and VMWare.<br>VM restoration of Hyper-V and VMWare Linux guest VMs.                          |
| <b>Using MABS or DPM to back up Linux Azure VMs</b>                   | Not supported.                                                                                                                                     |

## Daylight saving time support

Azure Backup doesn't support automatic clock adjustment for daylight saving time for Azure VM backups. Modify backup policies manually as required.

## Disk deduplication support

Disk deduplication support is as follows:

- Disk deduplication is supported on-premises when you use DPM or MABs to back up Hyper-V VMs that are running Windows. Windows Server performs data deduplication (at the host level) on virtual hard disks (VHDs) that are attached to the VM as backup storage.
- Deduplication isn't supported in Azure for any Backup component. When DPM and MABS are deployed in Azure, the storage disks attached to the VM can't be deduplicated.

## Security and encryption support

Azure Backup supports encryption for in-transit and at-rest data.

### Network traffic to Azure

- Backup traffic from servers to the Recovery Services vault is encrypted by using Advanced Encryption Standard 256.
- Backup data is sent over a secure HTTPS link.
- Backup data is stored in the Recovery Services vault in encrypted form.
- Only you have the passphrase to unlock this data. Microsoft can't decrypt the backup data at any point.

#### WARNING

After setting up the vault, only you have access to the encryption key. Microsoft never maintains a copy and doesn't have access to the key. If the key is misplaced, Microsoft can't recover the backup data.

### Data security

- When you're backing up Azure VMs, you need to set up encryption *within* the virtual machine.

- Azure Backup supports Azure Disk Encryption, which uses BitLocker on Windows virtual machines and **dm-crypt** on Linux virtual machines.
- On the back end, Azure Backup uses [Azure Storage Service Encryption](#), which protects data at rest.

| MACHINE                                                    | IN TRANSIT | AT REST |
|------------------------------------------------------------|------------|---------|
| <b>On-premises Windows machines without DPM/MABS</b>       |            |         |
| <b>Azure VMs</b>                                           |            |         |
| <b>On-premises Windows machines or Azure VMs with DPM</b>  |            |         |
| <b>On-premises Windows machines or Azure VMs with MABS</b> |            |         |

## Compression support

Backup supports the compression of backup traffic, as summarized in the following table.

- For Azure VMs, the VM extension reads the data directly from the Azure storage account over the storage network, so it isn't necessary to compress this traffic.
- If you're using DPM or MABS, you can save bandwidth by compressing the data before it's backed up.

| MACHINE                                                       | COMPRESS TO MABS/DPM (TCP) | COMPRESS TO VAULT (HTTPS) |
|---------------------------------------------------------------|----------------------------|---------------------------|
| <b>Direct backup of on-premises Windows machines</b>          | NA                         |                           |
| <b>Backup of Azure VMs by using VM extension</b>              | NA                         | NA                        |
| <b>Backup on on-premises/Azure machines by using MABS/DPM</b> |                            |                           |

## Retention limits

| SETTING                                                                 | LIMITS                                                              |
|-------------------------------------------------------------------------|---------------------------------------------------------------------|
| <b>Max recovery points per protected instance (machine or workload)</b> | 9,999                                                               |
| <b>Max expiry time for a recovery point</b>                             | No limit                                                            |
| <b>Maximum backup frequency to DPM/MABS</b>                             | Every 15 minutes for SQL Server<br>Once an hour for other workloads |

| SETTING                                  | LIMITS                                                                                                                                                      |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Maximum backup frequency to vault</b> | <b>On-premises Windows machines or Azure VMs running MARS:</b> Three per day<br><br><b>DPM/MABS:</b> Two per day<br><br><b>Azure VM backup:</b> One per day |
| <b>Recovery point retention</b>          | Daily, weekly, monthly, yearly                                                                                                                              |
| <b>Maximum retention period</b>          | Depends on backup frequency                                                                                                                                 |
| <b>Recovery points on DPM/MABS disk</b>  | 64 for file servers; 448 for app servers<br><br>Unlimited tape recovery points for on-premises DPM                                                          |

## Cross Region Restore

Azure Backup has added the Cross Region Restore feature to strengthen data availability and resiliency capability, giving customers full control to restore data to a secondary region. To configure this feature, visit [the Set Cross Region Restore article](#). This feature is supported for the following management types:

| BACKUP MANAGEMENT TYPE | SUPPORTED                                                                                   | SUPPORTED REGIONS |
|------------------------|---------------------------------------------------------------------------------------------|-------------------|
| Azure VM               | Yes. Public limited Preview Supported for encrypted VMs and VMs with lesser than 4-TB disks | West Central US   |
| MARS Agent/On premises | No                                                                                          | N/A               |
| SQL /SAP HANA          | No                                                                                          | N/A               |
| AFS                    | No                                                                                          | N/A               |

## Next steps

- [Review support matrix](#) for Azure VM backup.

# Support matrix for Azure VM backup

2/25/2020 • 16 minutes to read • [Edit Online](#)

You can use the [Azure Backup service](#) to back up on-premises machines and workloads, and Azure virtual machines (VMs). This article summarizes support settings and limitations when you back up Azure VMs with Azure Backup.

Other support matrices:

- [General support matrix for Azure Backup](#)
- [Support matrix for Azure Backup server/System Center Data Protection Manager \(DPM\) backup](#)
- [Support matrix for backup with the Microsoft Azure Recovery Services \(MARS\) agent](#)

## Supported scenarios

Here's how you can back up and restore Azure VMs with the Azure Backup service.

| SCENARIO                                  | BACKUP                                 | AGENT                                                                                                                                                                                | RESTORE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Direct backup of Azure VMs                | Back up the entire VM.                 | No additional agent is needed on the Azure VM. Azure Backup installs and uses an extension to the <a href="#">Azure VM agent</a> that is running on the VM.                          | <p>Restore as follows:</p> <ul style="list-style-type: none"><li>- <b>Create a basic VM.</b> This is useful if the VM has no special configuration such as multiple IP addresses.</li><li>- <b>Restore the VM disk.</b> Restore the disk. Then attach it to an existing VM, or create a new VM from the disk by using PowerShell.</li><li>- <b>Replace VM disk.</b> If a VM exists and it uses managed disks (unencrypted), you can restore a disk and use it to replace an existing disk on the VM.</li><li>- <b>Restore specific files/folders.</b> You can restore files/folders from a VM instead of from the entire VM.</li></ul> |
| Direct backup of Azure VMs (Windows only) | Back up specific files/folders/volume. | Install the <a href="#">Azure Recovery Services agent</a> . You can run the MARS agent alongside the backup extension for the Azure VM agent to back up the VM at file/folder level. | Restore specific folders/files.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

| SCENARIO                          | BACKUP                                                                                                                                                                                            | AGENT                                                                                     | RESTORE                                                                 |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| Back up Azure VM to backup server | <p>Back up files/folders/volumes; system state/bare metal files; app data to System Center DPM or to Microsoft Azure Backup Server (MABS).</p> <p>DPM/MABS then backs up to the backup vault.</p> | Install the DPM/MABS protection agent on the VM. The MARS agent is installed on DPM/MABS. | Restore files/folders/volumes; system state/bare metal files; app data. |

Learn more about backup using a [backup server](#) and about [support requirements](#).

#### NOTE

##### Azure Backup now supports selective disk backup and restore using the Azure Virtual Machine backup solution.

Today, Azure Backup supports backing up all the disks (Operating System and data) in a VM together using the Virtual Machine backup solution. With exclude-disk functionality, you get an option to backup one or a few from the many data disks in a VM. This provides an efficient and cost-effective solution for your backup and restore needs. Each recovery point contains data of the disks included in the backup operation, which further allows you to have a subset of disks restored from the given recovery point during the restore operation. This applies to restore both from the snapshot and the vault.

\*\*To sign up for the preview, write to us at [AskAzureBackupTeam@microsoft.com](mailto:AskAzureBackupTeam@microsoft.com)\*\*

## Supported backup actions

| ACTION                                           | SUPPORT                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable backup when you create a Windows Azure VM | <p>Supported for:</p> <ul style="list-style-type: none"> <li>- Windows Server 2019 (Datacenter/Datacenter Core/Standard)</li> <li>- Windows Server 2016 (Datacenter/Datacenter Core/Standard)</li> <li>- Windows Server 2012 R2 (Datacenter/Standard)</li> <li>- Windows Server 2008 R2 (RTM and SP1 Standard)</li> </ul>                                             |
| Enable backup when you create a Linux VM         | <p>Supported for:</p> <ul style="list-style-type: none"> <li>- Ubuntu Server: 18.04, 17.10, 17.04, 16.04 (LTS), 14.04 (LTS)</li> <li>- Red Hat: RHEL 6.7, 6.8, 6.9, 7.2, 7.3, 7.4</li> <li>- SUSE Linux Enterprise Server: 11 SP4, 12 SP2, 12 SP3, 15</li> <li>- Debian: 8, 9</li> <li>- CentOS: 6.9, 7.3</li> <li>- Oracle Linux: 6.7, 6.8, 6.9, 7.2, 7.3</li> </ul> |
| Back up a VM that's shutdown/offline VM          | <p>Supported.</p> <p>Snapshot is crash-consistent only, not app-consistent.</p>                                                                                                                                                                                                                                                                                       |

| ACTION                                                   | SUPPORT                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Back up disks after migrating to managed disks           | <p>Supported.</p> <p>Backup will continue to work. No action is required.</p>                                                                                                                                                                                                                               |
| Back up managed disks after enabling resource group lock | <p>Not supported.</p> <p>Azure Backup can't delete the older restore points, and backups will start to fail when the maximum limit of restore points is reached.</p>                                                                                                                                        |
| Modify backup policy for a VM                            | <p>Supported.</p> <p>The VM will be backed up by using the schedule and retention settings in new policy. If retention settings are extended, existing recovery points are marked and kept. If they're reduced, existing recovery points will be pruned in the next cleanup job and eventually deleted.</p> |
| Cancel a backup job                                      | <p>Supported during snapshot process.</p> <p>Not supported when the snapshot is being transferred to the vault.</p>                                                                                                                                                                                         |
| Back up the VM to a different region or subscription     | Not supported.                                                                                                                                                                                                                                                                                              |
| Backups per day (via the Azure VM extension)             | <p>One scheduled backup per day.</p> <p>The Azure Backup service supports up to nine on-demand backups per day, but Microsoft recommends no more than four daily on-demand backups to ensure best performance.</p>                                                                                          |
| Backups per day (via the MARS agent)                     | Three scheduled backups per day.                                                                                                                                                                                                                                                                            |
| Backups per day (via DPM/MABS)                           | Two scheduled backups per day.                                                                                                                                                                                                                                                                              |
| Monthly/yearly backup                                    | <p>Not supported when backing up with Azure VM extension. Only daily and weekly is supported.</p> <p>You can set up the policy to retain daily/weekly backups for monthly/yearly retention period.</p>                                                                                                      |
| Automatic clock adjustment                               | <p>Not supported.</p> <p>Azure Backup doesn't automatically adjust for daylight saving time changes when backing up a VM.</p> <p>Modify the policy manually as needed.</p>                                                                                                                                  |
| <a href="#">Security features for hybrid backup</a>      | Disabling security features isn't supported.                                                                                                                                                                                                                                                                |
| Back up the VM whose machine time is changed             | <p>Not supported.</p> <p>If the machine time is changed to a future date-time after enabling backup for that VM; However even if the time change is reverted, successful backup is not guaranteed.</p>                                                                                                      |

## Operating system support (Windows)

The following table summarizes the supported operating systems when backing up Windows Azure VMs.

| SCENARIO                              | OS SUPPORT                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Back up with Azure VM agent extension | <ul style="list-style-type: none"><li>- Windows 10 Client (64 bit only)</li><li>- Windows Server 2019 (Datacenter/Datacenter Core/Standard)</li><li>- Windows Server 2016 (Datacenter/Datacenter Core/Standard)</li><li>- Windows Server 2012 R2 (Datacenter/Standard)</li><li>- Windows Server 2008 R2 (RTM and SP1 Standard)</li><li>- Windows Server 2008 (64 bit only)</li></ul> |
| Back up with MARS agent               | <a href="#">Supported</a> operating systems.                                                                                                                                                                                                                                                                                                                                         |
| Back up with DPM/MABS                 | Supported operating systems for backup with <a href="#">MABS</a> and <a href="#">DPM</a> .                                                                                                                                                                                                                                                                                           |

Azure Backup doesn't support 32-bit operating systems.

## Support for Linux backup

Here's what's supported if you want to back up Linux machines.

| ACTION                                                | SUPPORT                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Back up Linux Azure VMs with the Linux Azure VM agent | <p>File consistent backup.</p> <p>App-consistent backup using <a href="#">custom scripts</a>.</p> <p>During restore, you can create a new VM, restore a disk and use it to create a VM, or restore a disk and use it to replace a disk on an existing VM. You can also restore individual files and folders.</p> |
| Back up Linux Azure VMs with MARS agent               | <p>Not supported.</p> <p>The MARS agent can only be installed on Windows machines.</p>                                                                                                                                                                                                                           |
| Back up Linux Azure VMs with DPM/MABS                 | Not supported.                                                                                                                                                                                                                                                                                                   |

## Operating system support (Linux)

For Azure VM Linux backups, Azure Backup supports the list of Linux [distributions endorsed by Azure](#). Note the following:

- Azure Backup doesn't support Core OS Linux.
- Azure Backup doesn't support 32-bit operating systems.
- Other bring-your-own Linux distributions might work as long as the [Azure VM agent for Linux](#) is available on the VM, and as long as Python is supported.

- Azure Backup doesn't support a proxy-configured Linux VM if it does not have Python version 2.7 installed.

## Backup frequency and retention

| SETTING                                                           | LIMITS                                                                                                   |
|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Maximum recovery points per protected instance (machine/workload) | 9999.                                                                                                    |
| Maximum expiry time for a recovery point                          | No limit.                                                                                                |
| Maximum backup frequency to vault (Azure VM extension)            | Once a day.                                                                                              |
| Maximum backup frequency to vault (MARS agent)                    | Three backups per day.                                                                                   |
| Maximum backup frequency to DPM/MABS                              | Every 15 minutes for SQL Server.<br>Once an hour for other workloads.                                    |
| Recovery point retention                                          | Daily, weekly, monthly, and yearly.                                                                      |
| Maximum retention period                                          | Depends on backup frequency.                                                                             |
| Recovery points on DPM/MABS disk                                  | 64 for file servers, and 448 for app servers.<br>Tape recovery points are unlimited for on-premises DPM. |

## Supported restore methods

| RESTORE OPTION         | DETAILS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Create a new VM</b> | <p>Quickly creates and gets a basic VM up and running from a restore point.</p> <p>You can specify a name for the VM, select the resource group and virtual network (VNet) in which it will be placed, and specify a storage account for the restored VM. The new VM must be created in the same region as the source VM.</p>                                                                                                                                                                                                                                                                                                                                    |
| <b>Restore disk</b>    | <p>Restores a VM disk, which can then be used to create a new VM.</p> <p>Azure Backup provides a template to help you customize and create a VM.</p> <p>The restore job generates a template that you can download and use to specify custom VM settings, and create a VM.</p> <p>The disks are copied to the Resource Group you specify.</p> <p>Alternatively, you can attach the disk to an existing VM, or create a new VM using PowerShell.</p> <p>This option is useful if you want to customize the VM, add configuration settings that weren't there at the time of backup, or add settings that must be configured using the template or PowerShell.</p> |

| RESTORE OPTION                         | DETAILS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Replace existing</b>                | <p>You can restore a disk, and use it to replace a disk on the existing VM.</p> <p>The current VM must exist. If it's been deleted, this option can't be used.</p> <p>Azure Backup takes a snapshot of the existing VM before replacing the disk, and stores it in the staging location you specify. Existing disks connected to the VM are replaced with the selected restore point.</p> <p>The snapshot is copied to the vault, and retained in accordance with the retention policy.</p> <p>After the replace disk operation, the original disk is retained in the resource group. You can choose to manually delete the original disks if they are not needed.</p> <p>Replace existing is supported for unencrypted managed VMs. It's not supported for unmanaged disks, <a href="#">generalized VMs</a>, or for VMs <a href="#">created using custom images</a>.</p> <p>If the restore point has more or less disks than the current VM, then the number of disks in the restore point will only reflect the VM configuration.</p> <p>Replace existing isn't supported for VMs with linked resources (like <a href="#">user-assigned managed-identity</a> or <a href="#">Key Vault</a>) because the backup client-app doesn't have permissions on these resources while performing the restore.</p> |
| <b>Cross Region (secondary region)</b> | <p>Cross Region restore can be used to restore Azure VMs in the secondary region, which is an <a href="#">Azure paired region</a>.</p> <p>You can restore all the Azure VMs for the selected recovery point if the backup is done in the secondary region.</p> <p>This feature is available for the options below:</p> <ul style="list-style-type: none"> <li>* <a href="#">Create a VM</a></li> <li>* <a href="#">Restore Disks</a></li> </ul> <p>We don't currently support the <a href="#">Replace existing disks</a> option.</p> <p>Permissions</p> <p>The restore operation on secondary region can be performed by Backup Admins and App admins.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## Support for file-level restore

| RESTORE                                  | SUPPORTED                                                                                                                                    |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Restoring files across operating systems | You can restore files on any machine that has the same (or compatible) OS as the backed-up VM. See the <a href="#">Compatible OS table</a> . |
| Restoring files on classic VMs           | Not supported.                                                                                                                               |
| Restoring files from encrypted VMs       | Not supported.                                                                                                                               |

| RESTORE                                                  | SUPPORTED                                                                               |
|----------------------------------------------------------|-----------------------------------------------------------------------------------------|
| Restoring files from network-restricted storage accounts | Not supported.                                                                          |
| Restoring files on VMs using Windows Storage Spaces      | Restore not supported on same VM.<br><br>Instead, restore the files on a compatible VM. |
| Restore files on Linux VM using LVM/raid arrays          | Restore not supported on same VM.<br><br>Restore on a compatible VM.                    |
| Restore files with special network settings              | Restore not supported on same VM.<br><br>Restore on a compatible VM.                    |

## Support for VM management

The following table summarizes support for backup during VM management tasks, such as adding or replacing VM disks.

| RESTORE                                                                              | SUPPORTED                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Restore across subscription/region/zone.                                             | Not supported.                                                                                                                                                                                                                  |
| Restore to an existing VM                                                            | Use replace disk option.                                                                                                                                                                                                        |
| Restore disk with storage account enabled for Azure Storage Service Encryption (SSE) | Not supported.<br><br>Restore to an account that doesn't have SSE enabled.                                                                                                                                                      |
| Restore to mixed storage accounts                                                    | Not supported.<br><br>Based on the storage account type, all restored disks will be either premium or standard, and not mixed.                                                                                                  |
| Restore VM directly to an availability set                                           | For managed disks, you can restore the disk and use the availability set option in the template.<br><br>Not supported for unmanaged disks. For unmanaged disks, restore the disk, and then create a VM in the availability set. |
| Restore backup of unmanaged VMs after upgrading to managed VM                        | Supported.<br><br>You can restore disks, and then create a managed VM.                                                                                                                                                          |
| Restore VM to restore point before the VM was migrated to managed disks              | Supported.<br><br>You restore to unmanaged disks (default), convert the restored disks to managed disk, and create a VM with the managed disks.                                                                                 |
| Restore a VM that's been deleted.                                                    | Supported.<br><br>You can restore the VM from a recovery point.                                                                                                                                                                 |

| RESTORE                                                                                     | SUPPORTED                                                                          |
|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Restore a domain controller (DC) VM that is part of a multi-DC configuration through portal | Supported if you restore the disk and create a VM by using PowerShell.             |
| Restore VM in different virtual network                                                     | Supported.<br><br>The virtual network must be in the same subscription and region. |

## VM compute support

| COMPUTE                                                                                                           | SUPPORT                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VM size                                                                                                           | Any Azure VM size with at least 2 CPU cores and 1-GB RAM.<br><br><a href="#">Learn more.</a>                                                                                                                                                                                                           |
| Back up VMs in <a href="#">availability sets</a>                                                                  | Supported.<br><br>You can't restore a VM in an available set by using the option to quickly create a VM. Instead, when you restore the VM, restore the disk and use it to deploy a VM, or restore a disk and use it to replace an existing disk.                                                       |
| Back up VMs that are deployed with <a href="#">Hybrid Use Benefit (HUB)</a>                                       | Supported.                                                                                                                                                                                                                                                                                             |
| Back up VMs that are deployed in a <a href="#">scale set</a>                                                      | Not supported.                                                                                                                                                                                                                                                                                         |
| Back up VMs that are deployed from the <a href="#">Azure Marketplace</a><br>(Published by Microsoft, third party) | Supported.<br><br>The VM must be running a supported operating system.<br><br>When recovering files on the VM, you can restore only to a compatible OS (not an earlier or later OS). We do not restore the Azure Marketplace VMs backed as VMs, as these needs purchase information but only as Disks. |
| Back up VMs that are deployed from a custom image (third-party)                                                   | Supported.<br><br>The VM must be running a supported operating system.<br><br>When recovering files on the VM, you can restore only to a compatible OS (not an earlier or later OS).                                                                                                                   |
| Back up VMs that are migrated to Azure                                                                            | Supported.<br><br>To back up the VM, the VM agent must be installed on the migrated machine.                                                                                                                                                                                                           |
| Back up Multi-VM consistency                                                                                      | Azure Backup does not provide data and application consistency across multiple VMs.                                                                                                                                                                                                                    |

| COMPUTE                                         | SUPPORT                                                                                                                                                                                                                                                 |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Backup with <a href="#">Diagnostic Settings</a> | <p>Unsupported.</p> <p>If the restore of the Azure VM with diagnostic settings is triggered using <a href="#">Create New</a> option, then the restore fails.</p>                                                                                        |
| Restore of Zone-pinned VMs                      | <p>Supported (for VM that is backed-up after Jan 2019 and where <a href="#">availability zone</a> are available).</p> <p>We currently support restoring to the same zone that is pinned in VMs. However, if the zone is unavailable, restore fails.</p> |
| Gen2 VMs                                        | <p>Supported</p> <p>Azure Backup supports backup and restore of <a href="#">Gen2 VMs</a>. When these VMs are restored from Recovery point, they are restored as <a href="#">Gen2 VMs</a>.</p>                                                           |

## VM storage support

| COMPONENT                            | SUPPORT                                                                                                                                                                                                                                                                                                          |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Azure VM data disks                  | <p>Back up a VM with 16 or fewer data disks.</p> <p>To sign up for the private preview of VMs with 16+ disks (up to 32 disks), write to us at <a href="mailto:AskAzureBackupTeam@microsoft.com">AskAzureBackupTeam@microsoft.com</a></p>                                                                         |
| Data disk size                       | Individual disk size can be up to 32 TB and a maximum of 256 TB combined for all disks in a VM.                                                                                                                                                                                                                  |
| Storage type                         | Standard HDD, Standard SSD, Premium SSD.                                                                                                                                                                                                                                                                         |
| Managed disks                        | Supported.                                                                                                                                                                                                                                                                                                       |
| Encrypted disks                      | <p>Supported.</p> <p>Azure VMs enabled with Azure Disk Encryption can be backed up (with or without the Azure AD app).</p> <p>Encrypted VMs can't be recovered at the file/folder level. You must recover the entire VM.</p> <p>You can enable encryption on VMs that are already protected by Azure Backup.</p> |
| Disks with Write Accelerator enabled | <p>Not supported.</p> <p>Azure backup automatically excludes the Disks with Write Accelerator enabled during backup. Since they are not backed up, you will not be able to Restore these disks from Recovery-Points of the VM.</p>                                                                               |

| COMPONENT                                | SUPPORT                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Back up & Restore deduplicated VMs/disks | <p>Azure Backup does not support deduplication. For more information, see this <a href="#">article</a></p> <ul style="list-style-type: none"> <li>- Azure Backup does not deduplicate across VMs in the Recovery Services vault</li> <li>- If there are VMs in deduplication state during restore, the files can't be restored as vault does not understand the format. However, you will be able to successfully perform the full VM restore.</li> </ul> |
| Add disk to protected VM                 | Supported.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Resize disk on protected VM              | Supported.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Shared storage                           | Backing up VMs using Cluster Shared Volume (CSV) or Scale-Out File Server is not supported. CSV writers are likely to fail during backup. On restore, disks containing CSV volumes might not come-up.                                                                                                                                                                                                                                                     |
| Shared disks                             | Not supported.                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## VM network support

| COMPONENT                           | SUPPORT                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Number of network interfaces (NICs) | <p>Up to maximum number of NICs supported for a specific Azure VM size.</p> <p>NICs are created when the VM is created during the restore process.</p> <p>The number of NICs on the restored VM mirrors the number of NICs on the VM when you enabled protection. Removing NICs after you enable protection doesn't affect the count.</p> |
| External/internal load balancer     | <p>Supported.</p> <p><a href="#">Learn more</a> about restoring VMs with special network settings.</p>                                                                                                                                                                                                                                    |
| Multiple reserved IP addresses      | <p>Supported.</p> <p><a href="#">Learn more</a> about restoring VMs with special network settings.</p>                                                                                                                                                                                                                                    |
| VMs with multiple network adapters  | <p>Supported.</p> <p><a href="#">Learn more</a> about restoring VMs with special network settings.</p>                                                                                                                                                                                                                                    |
| VMs with public IP addresses        | <p>Supported.</p> <p>Associate an existing public IP address with the NIC, or create an address and associate it with the NIC after restore is done.</p>                                                                                                                                                                                  |

| COMPONENT                                   | SUPPORT                                                                                                                                                                                                        |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network security group (NSG) on NIC/subnet. | Supported.                                                                                                                                                                                                     |
| Static IP address                           | <p>Not supported.</p> <p>A new VM that's created from a restore point is assigned a dynamic IP address.</p> <p>For classic VMs, you can't back up a VM with a reserved IP address and no defined endpoint.</p> |
| Dynamic IP address                          | <p>Supported.</p> <p>If the NIC on the source VM uses dynamic IP addressing, by default the NIC on the restored VM will use it too.</p>                                                                        |
| Azure Traffic Manager                       | <p>Supported.</p> <p>If the backed-up VM is in Traffic Manager, manually add the restored VM to the same Traffic Manager instance.</p>                                                                         |
| Azure DNS                                   | Supported.                                                                                                                                                                                                     |
| Custom DNS                                  | Supported.                                                                                                                                                                                                     |
| Outbound connectivity via HTTP proxy        | <p>Supported.</p> <p>An authenticated proxy isn't supported.</p>                                                                                                                                               |
| Virtual network service endpoints           | <p>Supported.</p> <p>Firewall and virtual network storage account settings should allow access from all networks.</p>                                                                                          |

## VM security and encryption support

Azure Backup supports encryption for in-transit and at-rest data:

Network traffic to Azure:

- Backup traffic from servers to the Recovery Services vault is encrypted by using Advanced Encryption Standard 256.
- Backup data is sent over a secure HTTPS link.
- The backup data is stored in the Recovery Services vault in encrypted form.
- Only you have the passphrase to unlock this data. Microsoft can't decrypt the backup data at any point.

### WARNING

After you set up the vault, only you have access to the encryption key. Microsoft never maintains a copy and doesn't have access to the key. If the key is misplaced, Microsoft can't recover the backup data.

Data security:

- When backing up Azure VMs, you need to set up encryption *within* the virtual machine.

- Azure Backup supports Azure Disk Encryption, which uses BitLocker on Windows virtual machines and uses **dm-crypt** on Linux virtual machines.
- On the back end, Azure Backup uses [Azure Storage Service encryption](#), which protects data at rest.

| MACHINE                                       | IN TRANSIT | AT REST |
|-----------------------------------------------|------------|---------|
| On-premises Windows machines without DPM/MABS |            |         |
| Azure VMs                                     |            |         |
| On-premises/Azure VMs with DPM                |            |         |
| On-premises/Azure VMs with MABS               |            |         |

## VM compression support

Backup supports the compression of backup traffic, as summarized in the following table. Note the following:

- For Azure VMs, the VM extension reads the data directly from the Azure storage account over the storage network. It is not necessary to compress this traffic.
- If you're using DPM or MABS, you can save bandwidth by compressing the data before it's backed up to DPM/MABS.

| MACHINE                                       | COMPRESS TO MABS/DPM (TCP) | COMPRESS TO VAULT (HTTPS) |
|-----------------------------------------------|----------------------------|---------------------------|
| On-premises Windows machines without DPM/MABS | NA                         |                           |
| Azure VMs                                     | NA                         | NA                        |
| On-premises/Azure VMs with DPM                |                            |                           |
| On-premises/Azure VMs with MABS               |                            |                           |

## Next steps

- [Back up Azure VMs](#).
- [Back up Windows machines directly](#), without a backup server.
- [Set up MABS](#) for backup to Azure, and then back up workloads to MABS.
- [Set up DPM](#) for backup to Azure, and then back up workloads to DPM.

# Support matrix for backup with Microsoft Azure Backup Server or System Center DPM

2/24/2020 • 9 minutes to read • [Edit Online](#)

You can use the [Azure Backup service](#) to back up on-premises machines and workloads, and Azure virtual machines (VMs). This article summarizes support settings and limitations for backing up machines by using Microsoft Azure Backup Server (MABS) or System Center Data Protection Manager (DPM), and Azure Backup.

## About DPM/MABS

[System Center DPM](#) is an enterprise solution that configures, facilitates, and manages backup and recovery of enterprise machines and data. It's part of the [System Center](#) suite of products.

MABS is a server product that can be used to back up on-premises physical servers, VMs, and apps running on them.

MABS is based on System Center DPM and provides similar functionality with a few differences:

- No System Center license is required to run MABS.
- For both MABS and DPM, Azure provides long-term backup storage. In addition, DPM allows you to back up data for long-term storage on tape. MABS doesn't provide this functionality.
- You can back up a primary DPM server with a secondary DPM server. The secondary server will protect the primary server database and the data source replicas stored on the primary server. If the primary server fails, the secondary server can continue to protect workloads that are protected by the primary server, until the primary server is available again. MABS doesn't provide this functionality.

You download MABS from the [Microsoft Download Center](#). It can be run on-premises or on an Azure VM.

DPM and MABS support backing up a wide variety of apps, and server and client operating systems. They provide multiple backup scenarios:

- You can back up at the machine level with system-state or bare-metal backup.
- You can back up specific volumes, shares, folders, and files.
- You can back up specific apps by using optimized app-aware settings.

## DPM/MABS backup

Backup using DPM/MABS and Azure Backup works as follows:

1. DPM/MABS protection agent is installed on each machine that will be backed up.
2. Machines and apps are backed up to local storage on DPM/MABS.
3. The Microsoft Azure Recovery Services (MARS) agent is installed on the DPM server/MABS.
4. The MARS agent backs up the DPM/MABS disks to a backup Recovery Services vault in Azure by using Azure Backup.

For more information:

- [Learn more](#) about MABS architecture.
- [Review what's supported](#) for the MARS agent.

## Supported scenarios

| SCENARIO                                      | AGENT                                                                                                                                                                                                                                                        | LOCATION                              |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| <b>Back up on-premises machines/workloads</b> | DPM/MABS protection agent runs on the machines that you want to back up.<br><br>The MARS agent on DPM/MABS server. The minimum version of the Microsoft Azure Recovery Services agent, or Azure Backup agent, required to enable this feature is 2.0.8719.0. | DPM/MABS must be running on-premises. |

## Supported deployments

DPM/MABS can be deployed as summarized in the following table.

| DEPLOYMENT                           | SUPPORT                                                        | DETAILS                                                                                                           |
|--------------------------------------|----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Deployed on-premises</b>          | Physical server<br><br>Hyper-V VM<br><br>VMware VM             | If DPM/MABS is installed as a VMware VM, it only backs up VMware VMs and workloads that are running on those VMs. |
| <b>Deployed as an Azure Stack VM</b> | MABS only                                                      | DPM can't be used to back up Azure Stack VMs.                                                                     |
| <b>Deployed as an Azure VM</b>       | Protects Azure VMs and workloads that are running on those VMs | DPM/MABS running in Azure can't back up on-premises machines.                                                     |

## Supported MABS and DPM operating systems

Azure Backup can back up DPM/MABS instances that are running any of the following operating systems.

Operating systems should be running the latest service packs and updates.

| SCENARIO                   | DPM/MABS                                                                                                                                                                                                                                                        |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>MABS on an Azure VM</b> | Windows 2016 Datacenter.<br><br>Windows 2019 Datacenter.<br><br>We recommend that you start with an image from the marketplace.<br><br>Minimum Standard_A4_v2 with four cores and 8-GB RAM.                                                                     |
| <b>DPM on an Azure VM</b>  | System Center 2012 R2 with Update 3 or later.<br><br>Windows operating system as <a href="#">required by System Center</a> .<br><br>We recommend that you start with an image from the marketplace.<br><br>Minimum Standard_A4_v2 with four cores and 8-GB RAM. |

| SCENARIO                | DPM/MABS                                                                                                                 |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>MABS on-premises</b> | MABS v3 and later: Windows Server 2016 or Windows Server 2019                                                            |
| <b>DPM on-premises</b>  | Physical server/Hyper-V VM: System Center 2012 SP1 or later.<br>VMware VM: System Center 2012 R2 with Update 5 or later. |

#### NOTE

Installing Azure Backup Server is not supported on Windows Server Core or Microsoft Hyper-V Server.

## Management support

| ISSUE               | DETAILS                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Installation</b> | <p>Install DPM/MABS on a single-purpose machine.</p> <p>Don't install DPM/MABS on a domain controller, on a machine with the Application Server role installation, on a machine that is running Microsoft Exchange Server or System Center Operations Manager, or on a cluster node.</p> <p><a href="#">Review all DPM system requirements</a>.</p>                                  |
| <b>Domain</b>       | DPM/MABS should be joined to a domain. Install first, and then join DPM/MABS to a domain. Moving DPM/MABS to a new domain after deployment isn't supported.                                                                                                                                                                                                                          |
| <b>Storage</b>      | Modern backup storage (MBS) is supported from DPM 2016/MABS v2 and later. It isn't available for MABS v1.                                                                                                                                                                                                                                                                            |
| <b>MABS upgrade</b> | You can directly install MABS v3, or upgrade to MABS v3 from MABS v2. <a href="#">Learn more</a> .                                                                                                                                                                                                                                                                                   |
| <b>Moving MABS</b>  | <p>Moving MABS to a new server while retaining the storage is supported if you're using MBS.</p> <p>The server must have the same name as the original. You can't change the name if you want to keep the same storage pool, and use the same MABS database to store data recovery points.</p> <p>You will need a backup of the MABS database because you'll need to restore it.</p> |

## MABS support on Azure Stack

You can deploy MABS on an Azure Stack VM so that you can manage backup of Azure Stack VMs and workloads from a single location.

| COMPONENT                                     | DETAILS                                                                                                                                                                                                                                                                             |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>MABS on Azure Stack VM</b>                 | <p>At least size A2. We recommend you start with a Windows Server 2012 R2 or Windows Server 2016 image from the Azure Marketplace.</p> <p>Don't install anything else on the MABS VM.</p>                                                                                           |
| <b>MABS storage</b>                           | Use a separate storage account for the MABS VM. The MARS agent running on MABS needs temporary storage for a cache location and to hold data restored from the cloud.                                                                                                               |
| <b>MABS storage pool</b>                      | The size of the MABS storage pool is determined by the number and size of disks that are attached to the MABS VM. Each Azure Stack VM size has a maximum number of disks. For example, A2 is four disks.                                                                            |
| <b>MABS retention</b>                         | Don't retain backed up data on the local MABS disks for more than five days.                                                                                                                                                                                                        |
| <b>MABS scale up</b>                          | <p>To scale up your deployment, you can increase the size of the MABS VM. For example, you can change from A to D series.</p> <p>You can also ensure that you're offloading data with backup to Azure regularly. If necessary, you can deploy additional MABS servers.</p>          |
| <b>.NET Framework on MABS</b>                 | The MABS VM needs .NET Framework 3.3 SP1 or later installed on it.                                                                                                                                                                                                                  |
| <b>MABS domain</b>                            | The MABS VM must be joined to a domain. A domain user with admin privileges must install MABS on the VM.                                                                                                                                                                            |
| <b>Azure Stack VM data backup</b>             | You can back up files, folders, and apps.                                                                                                                                                                                                                                           |
| <b>Supported backup</b>                       | <p>These operating systems are supported for VMs that you want to back up:</p> <ul style="list-style-type: none"> <li>Windows Server Semi-Annual Channel (Datacenter, Enterprise, Standard)</li> <li>Windows Server 2016, Windows Server 2012 R2, Windows Server 2008 R2</li> </ul> |
| <b>SQL Server support for Azure Stack VMs</b> | <p>Back up SQL Server 2016, SQL Server 2014, SQL Server 2012 SP1.</p> <p>Back up and recover a database.</p>                                                                                                                                                                        |
| <b>SharePoint support for Azure Stack VMs</b> | <p>SharePoint 2016, SharePoint 2013, SharePoint 2010.</p> <p>Back up and recover a farm, database, front end, and web server.</p>                                                                                                                                                   |
| <b>Network requirements for backed up VMs</b> | All VMs in Azure Stack workload must belong to the same virtual network and belong to the same subscription.                                                                                                                                                                        |

# DPM/MABS networking support

## URL access

The DPM server/MABS needs access to these URLs:

- `http://www.msftncsi.com/ncsi.txt`
- \*.Microsoft.com
- \*.WindowsAzure.com
- \*.microsoftonline.com
- \*.windows.net

## Azure ExpressRoute support

You can back up your data over Azure ExpressRoute with public peering (available for old circuits) and Microsoft peering. Backup over private peering is not supported.

With public peering: Ensure access to the following domains/addresses:

- `http://www.msftncsi.com/ncsi.txt`
- `microsoft.com`
- `.WindowsAzure.com`
- `.microsoftonline.com`
- `.windows.net`

With Microsoft peering, please select the following services/regions and relevant community values:

- Azure Active Directory (12076:5060)
- Microsoft Azure Region (according to the location of your Recovery Services vault)
- Azure Storage (according to the location of your Recovery Services vault)

For more details, see the [ExpressRoute routing requirements](#).

### NOTE

Public Peering is deprecated for new circuits.

## DPM/MABS connectivity to Azure Backup

Connectivity to the Azure Backup service is required for backups to function properly, and the Azure subscription should be active. The following table shows the behavior if these two things don't occur.

| MABS TO AZURE | SUBSCRIPTION | BACKUP/RESTORE                                                                              |
|---------------|--------------|---------------------------------------------------------------------------------------------|
| Connected     | Active       | Back up to DPM/MABS disk.<br>Back up to Azure.<br>Restore from disk.<br>Restore from Azure. |
| Not Connected | Active       | Back up to Azure.<br>Restore from disk.<br>Restore from Azure.                              |
| Connected     | Not Active   | Back up to DPM/MABS disk.<br>Back up to Azure.<br>Restore from disk.<br>Restore from Azure. |
| Not Connected | Not Active   | Back up to Azure.<br>Restore from disk.<br>Restore from Azure.                              |

| MABS TO AZURE                         | SUBSCRIPTION          | BACKUP/RESTORE                                                                                                                                                                                                                           |
|---------------------------------------|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Connected                             | Expired/deprovisioned | <p>No backup to disk or Azure.</p> <p>If the subscription is expired, you can restore from disk or Azure.</p> <p>If the subscription is decommissioned, you can't restore from disk or Azure. The Azure recovery points are deleted.</p> |
| No connectivity for more than 15 days | Active                | <p>No backup to disk or Azure.</p> <p>You can restore from disk or Azure.</p>                                                                                                                                                            |
| No connectivity for more than 15 days | Expired/deprovisioned | <p>No backup to disk or Azure.</p> <p>If the subscription is expired, you can restore from disk or Azure.</p> <p>If the subscription is decommissioned, you can't restore from disk or Azure. The Azure recovery points are deleted.</p> |

## DPM/MABS storage support

Data that is backed up to DPM/MABS is stored on local disk storage.

| STORAGE                                | DETAILS                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>MBS</b>                             | Modern backup storage (MBS) is supported from DPM 2016/MABS v2 and later. It isn't available for MABS v1.                                                                                                                                                                                                                                                                                                                                                                         |
| <b>MABS storage on Azure VM</b>        | <p>Data is stored on Azure disks that are attached to the DPM/MABS VM, and that are managed in DPM/MABS. The number of disks that can be used for DPM/MABS storage pool is limited by the size of the VM.</p> <p>A2 VM: 4 disks; A3 VM: 8 disks; A4 VM: 16 disks, with a maximum size of 1 TB for each disk. This determines the total backup storage pool that is available.</p> <p>The amount of data you can back up depends on the number and size of the attached disks.</p> |
| <b>MABS data retention on Azure VM</b> | We recommend that you retain data for one day on the DPM/MABS Azure disk, and back up from DPM/MABS to the vault for longer retention. You can thus protect a larger amount of data by offloading it to Azure Backup.                                                                                                                                                                                                                                                             |

### Modern backup storage (MBS)

From DPM 2016/MABS v2 (running on Windows Server 2016) and later, you can take advantage of modern backup storage (MBS).

- MBS backups are stored on a Resilient File System (ReFS) disk.
- MBS uses ReFS block cloning for faster backup and more efficient use of storage space.
- When you add volumes to the local DPM/MABS storage pool, you configure them with drive letters. You can then configure workload storage on different volumes.

- When you create protection groups to back up data to DPM/MABS, you select the drive you want to use. For example, you might store backups for SQL or other high IOPS workloads on a high-performance drive, and store workloads that are backed up less frequently on a lower performance drive.

## Supported backups to MABS

For information on the various servers and workloads that you can protect with Azure Backup Server, refer to the [Azure Backup Server Protection Matrix](#).

## Supported backups to DPM

For information on the various servers and workloads that you can protect with Data Protection Manager, refer to the article [What can DPM back up?](#).

- Clustered workloads backed up by DPM/MABS should be in the same domain as DPM/MABS or in a child/trusted domain.
- You can use NTLM/certificate authentication to back up data in untrusted domains or workgroups.

## Next steps

- [Learn more](#) about MABS architecture.
- [Review](#) what's supported for the MARS agent.
- [Set up](#) a MABS server.
- [Set up DPM](#).

# Support matrix for backup with the Microsoft Azure Recovery Services (MARS) agent

2/24/2020 • 7 minutes to read • [Edit Online](#)

You can use the [Azure Backup service](#) to back up on-premises machines and apps and to back up Azure virtual machines (VMs). This article summarizes support settings and limitations when you use the Microsoft Azure Recovery Services (MARS) agent to back up machines.

## The MARS agent

Azure Backup uses the MARS agent to back up data from on-premises machines and Azure VMs to a backup Recovery Services vault in Azure. The MARS agent can:

- Run on on-premises Windows machines so that they can back up directly to a backup Recovery Services vault in Azure.
- Run on Windows VMs so that they can back up directly to a vault.
- Run on Microsoft Azure Backup Server (MABS) or a System Center Data Protection Manager (DPM) server. In this scenario, machines and workloads back up to MABS or to the DPM server. The MARS agent then backs up this server to a vault in Azure.

### NOTE

Azure Backup doesn't support automatic adjustment of clock for daylight savings time (DST). Modify the policy to ensure daylight savings is taken into account to prevent discrepancy between the actual time and scheduled backup time.

Your backup options depend on where the agent is installed. For more information, see [Azure Backup architecture using the MARS agent](#). For information about MABS and DPM backup architecture, see [Back up to DPM or MABS](#). Also see [requirements](#) for the backup architecture.

| INSTALLATION                   | DETAILS                                                                                                                                                                                                               |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Download the latest MARS agent | You can download the latest version of the agent from the vault, or <a href="#">download it directly</a> .                                                                                                            |
| Install directly on a machine  | You can install the MARS agent directly on an on-premises Windows server or on a Windows VM that's running any of the <a href="#">supported operating systems</a> .                                                   |
| Install on a backup server     | When you set up DPM or MABS to back up to Azure, you download and install the MARS agent on the server. You can install the agent on <a href="#">supported operating systems</a> in the backup server support matrix. |

#### **NOTE**

By default, Azure VMs that are enabled for backup have an Azure Backup extension installation. This extension backs up the entire VM. You can install and run the MARS agent on an Azure VM alongside the extension if you want to back up specific folders and files, rather than the complete VM. When you run the MARS agent on an Azure VM, it backs up files or folders that are in temporary storage on the VM. Backups fail if the files or folders are removed from the temporary storage or if the temporary storage is removed.

## Cache folder support

When you use the MARS agent to back up data, the agent takes a snapshot of the data and stores it in a local cache folder before it sends the data to Azure. The cache (scratch) folder has several requirements:

| CACHE            | DETAILS                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Size             | Free space in the cache folder should be at least 5 to 10 percent of the overall size of your backup data.                                                                                                                                                                                                                                                                                                 |
| Location         | The cache folder must be locally stored on the machine that's being backed up, and it must be online. The cache folder shouldn't be on a network share, on removable media, or on an offline volume.                                                                                                                                                                                                       |
| Folder           | The cache folder should not be encrypted on a deduplicated volume or in a folder that's compressed, that's sparse, or that has a reparse point.                                                                                                                                                                                                                                                            |
| Location changes | You can change the cache location by stopping the backup engine ( <code>net stop bengine</code> ) and copying the cache folder to a new drive. (Ensure the new drive has sufficient space.) Then update two registry entries under <b>HKLM\SOFTWARE\Microsoft\Windows Azure Backup (Config/ScratchLocation and Config/CloudBackupProvider/ScratchLocation)</b> to the new location and restart the engine. |

## Networking and access support

### **URL and IP access**

The MARS agent needs access to these URLs:

- <http://www.msftncsi.com/ncsi.txt>
- \*.Microsoft.com
- \*.WindowsAzure.com
- \*.MicrosoftOnline.com
- \*.Windows.net

And to these IP addresses:

- 20.190.128.0/18
- 40.126.0.0/18

Access to all of the URLs and IP addresses listed above uses the HTTPS protocol on port 443.

### **Azure ExpressRoute support**

You can back up your data over Azure ExpressRoute with public peering (available for old circuits) and Microsoft peering. Backup over private peering is not supported.

With public peering: Ensure access to the following domains/addresses:

- `http://www.msftncsi.com/ncsi.txt`
- `microsoft.com`
- `.WindowsAzure.com`
- `.microsoftonline.com`
- `.windows.net`

With Microsoft peering, please select the following services/regions and relevant community values:

- Azure Active Directory (12076:5060)
- Microsoft Azure Region (according to the location of your Recovery Services vault)
- Azure Storage (according to the location of your Recovery Services vault)

For more details, see the [ExpressRoute routing requirements](#).

**NOTE**

Public Peering is deprecated for new circuits.

## Throttling support

| FEATURE            | DETAILS                                                                                                      |
|--------------------|--------------------------------------------------------------------------------------------------------------|
| Bandwidth control  | Supported. In the MARS agent, use <b>Change Properties</b> to adjust bandwidth.                              |
| Network throttling | Not available for backed-up machines that run Windows Server 2008 R2, Windows Server 2008 SP2, or Windows 7. |

## Support for direct backups

**NOTE**

The MARS agent does not support Windows Server Core SKUs.

You can use the MARS agent to back up directly to Azure on the operating systems listed below that run on:

1. On-premises Windows Servers
2. Azure VMs running Windows

The operating systems must be 64 bit and should be running the latest service packs and updates. The following table summarizes these operating systems:

| OPERATING SYSTEM                   | FILES/FOLDERS | SYSTEM STATE | SOFTWARE/MODULE REQUIREMENTS                                            |
|------------------------------------|---------------|--------------|-------------------------------------------------------------------------|
| Windows 10 (Enterprise, Pro, Home) | Yes           | No           | Check the corresponding server version for software/module requirements |

| OPERATING SYSTEM                                                      | FILES/FOLDERS | SYSTEM STATE | SOFTWARE/MODULE REQUIREMENTS                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------|---------------|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Windows 8.1 (Enterprise, Pro)                                         | Yes           | No           | Check the corresponding server version for software/module requirements                                                                                                                                                                                                  |
| Windows 8 (Enterprise, Pro)                                           | Yes           | No           | Check the corresponding server version for software/module requirements                                                                                                                                                                                                  |
| Windows 7 (Ultimate, Enterprise, Pro, Home Premium/Basic, Starter)    | Yes           | No           | Check the corresponding server version for software/module requirements                                                                                                                                                                                                  |
| Windows Server 2016 (Standard, Datacenter, Essentials)                | Yes           | Yes          | <ul style="list-style-type: none"> <li>- .NET 4.5</li> <li>- Windows PowerShell</li> <li>- Latest Compatible Microsoft VC++ Redistributable</li> <li>- Microsoft Management Console (MMC) 3.0</li> </ul>                                                                 |
| Windows Server 2012 R2 (Standard, Datacenter, Foundation, Essentials) | Yes           | Yes          | <ul style="list-style-type: none"> <li>- .NET 4.5</li> <li>- Windows PowerShell</li> <li>- Latest Compatible Microsoft VC++ Redistributable</li> <li>- Microsoft Management Console (MMC) 3.0</li> </ul>                                                                 |
| Windows Server 2012 (Standard, Datacenter, Foundation)                | Yes           | Yes          | <ul style="list-style-type: none"> <li>- .NET 4.5</li> <li>- Windows PowerShell</li> <li>- Latest Compatible Microsoft VC++ Redistributable</li> <li>- Microsoft Management Console (MMC) 3.0</li> <li>- Deployment Image Servicing and Management (DISM.exe)</li> </ul> |
| Windows Storage Server 2016/2012 R2/2012 (Standard, Workgroup)        | Yes           | No           | <ul style="list-style-type: none"> <li>- .NET 4.5</li> <li>- Windows PowerShell</li> <li>- Latest Compatible Microsoft VC++ Redistributable</li> <li>- Microsoft Management Console (MMC) 3.0</li> </ul>                                                                 |
| Windows Server 2019 (Standard, Datacenter, Essentials)                | Yes           | Yes          | <ul style="list-style-type: none"> <li>- .NET 4.5</li> <li>- Windows PowerShell</li> <li>- Latest Compatible Microsoft VC++ Redistributable</li> <li>- Microsoft Management Console (MMC) 3.0</li> </ul>                                                                 |

For more information, see [Supported MABS and DPM operating systems](#).

## Backup limits

### Size limits

Azure Backup limits the size of a file or folder data source that can be backed up. The items that you back up from a single volume can't exceed the sizes summarized in this table:

| OPERATING SYSTEM             | SIZE LIMIT |
|------------------------------|------------|
| Windows Server 2012 or later | 54,400 GB  |
| Windows Server 2008 R2 SP1   | 1,700 GB   |
| Windows Server 2008 SP2      | 1,700 GB   |
| Windows 8 or later           | 54,400 GB  |
| Windows 7                    | 1,700 GB   |

### Other limitations

- MARS does not support protection of multiple machines with the same name to a single vault.

## Supported file types for backup

| TYPE                                       | SUPPORT                 |
|--------------------------------------------|-------------------------|
| Encrypted                                  | Supported.              |
| Compressed                                 | Supported.              |
| Sparse                                     | Supported.              |
| Compressed and sparse                      | Supported.              |
| Hard links                                 | Not supported. Skipped. |
| Reparse point                              | Not supported. Skipped. |
| Encrypted and sparse                       | Not supported. Skipped. |
| Compressed stream                          | Not supported. Skipped. |
| Sparse stream                              | Not supported. Skipped. |
| OneDrive (synced files are sparse streams) | Not supported.          |
| Folders with DFS Replication enabled       | Not supported.          |

## Supported drives or volumes for backup

| Drive/volume               | Support       | Details                                                                                                                  |
|----------------------------|---------------|--------------------------------------------------------------------------------------------------------------------------|
| Read-only volumes          | Not supported | Volume Copy Shadow Service (VSS) works only if the volume is writable.                                                   |
| Offline volumes            | Not supported | VSS works only if the volume is online.                                                                                  |
| Network share              | Not supported | The volume must be local on the server.                                                                                  |
| BitLocker-locked volumes   | Not supported | The volume must be unlocked before the backup starts.                                                                    |
| File system identification | Not supported | Only NTFS is supported.                                                                                                  |
| Removable media            | Not supported | All backup item sources must have a <i>fixed</i> status.                                                                 |
| Deduplicated drives        | Supported     | Azure Backup converts deduplicated data to normal data. It optimizes, encrypts, stores, and sends the data to the vault. |

## Support for initial offline backup

Azure Backup supports *offline seeding* to transfer initial backup data to Azure by using disks. This support is helpful if your initial backup is likely to be in the size range of terabytes (TBs). Offline backup is supported for:

- Direct backup of files and folders on on-premises machines that are running the MARS agent.
- Backup of workloads and files from a DPM server or MABS.

Offline backup can't be used for system state files.

## Support for data restoration

By using the [Instant Restore](#) feature of Azure Backup, you can restore data before it's copied to the vault. The machine you're backing up must be running .NET Framework 4.5.2 or higher.

Backups can't be restored to a target machine that's running an earlier version of the operating system. For example, a backup taken from a computer that's running Windows 7 can be restored on Windows 8 or later. But a backup taken from a computer that's running Windows 8 can't be restored on a computer that's running Windows 7.

## Next steps

- Learn more about [backup architecture that uses the MARS agent](#).
- Learn what's supported when you [run the MARS agent on MABS or a DPM server](#).

# Support matrix for backup of SAP HANA databases on Azure VMs

2/27/2020 • 2 minutes to read • [Edit Online](#)

Azure Backup supports the backup of SAP HANA databases to Azure. This article summarizes the scenarios supported and limitations present when you use Azure Backup to back up SAP HANA databases on Azure VMs.

## NOTE

The frequency of log backup can now be set to a minimum of 15 minutes. Log backups only begin to flow after a successful full backup for the database has completed.

## Scenario support

| SCENARIO                | SUPPORTED CONFIGURATIONS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | UNSUPPORTED CONFIGURATIONS                                    |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| <b>Topology</b>         | SAP HANA running in Azure Linux VMs only                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | HANA Large Instances (HLI)                                    |
| <b>Geos</b>             | <b>GA:</b><br><b>Americas</b> – Central US, East US 2, East US, North Central US, South Central US, West US 2, West Central US, West US, Canada Central, Canada East, Brazil South<br><b>Asia Pacific</b> – Australia Central, Australia Central 2, Australia East, Australia Southeast, Japan East, Japan West, Korea Central, Korea South, East Asia, Southeast Asia, Central India, South India, West India, China East, China North, China East2, China North 2<br><b>Europe</b> – West Europe, North Europe, France Central, UK South, UK West, Germany North, Germany West Central, Switzerland North, Switzerland West, Central Switzerland North<br><b>Africa / ME</b> - South Africa North, South Africa West, UAE North, UAE Central<br><b>Azure Government regions</b> | France South, Germany Central, Germany Northeast, US Gov IOWA |
| <b>OS versions</b>      | SLES 12 with SP2, SP3, or SP4; SLES 15                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | RHEL                                                          |
| <b>HANA versions</b>    | SDC on HANA 1.x, MDC on HANA 2.x <= SPS04 Rev 45                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | -                                                             |
| <b>HANA deployments</b> | SAP HANA on a single Azure VM - Scale up only                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Scale-out                                                     |
| <b>HANA Instances</b>   | A single SAP HANA instance on a single Azure VM – scale up only                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Multiple SAP HANA instances on a single VM                    |

| SCENARIO                      | SUPPORTED CONFIGURATIONS                                                                      | UNSUPPORTED CONFIGURATIONS                         |
|-------------------------------|-----------------------------------------------------------------------------------------------|----------------------------------------------------|
| <b>HANA database types</b>    | Single Database Container (SDC) ON 1.x, Multi-Database Container (MDC) on 2.x                 | MDC in HANA 1.x                                    |
| <b>HANA database size</b>     | 2-TB full backup size as reported by HANA)                                                    |                                                    |
| <b>Backup types</b>           | Full, Differential, and Log backups                                                           | Incremental, Snapshots                             |
| <b>Restore types</b>          | Refer to the SAP HANA Note <a href="#">1642148</a> to learn about the supported restore types |                                                    |
| <b>Backup limits</b>          | Up to 2 TB of full backup size per SAP HANA instance                                          |                                                    |
| <b>Special configurations</b> |                                                                                               | SAP HANA + Dynamic Tiering<br>Cloning through LaMa |

#### NOTE

Backup and restore operations from SAP HANA native clients (SAP HANA Studio/ Cockpit/ DBA Cockpit) aren't currently supported.

## Next steps

- Learn how to [Backup SAP HANA databases running on Azure VMs](#)
- Learn how to [Restore SAP HANA databases running on Azure VMs](#)
- Learn how to [manage SAP HANA databases that are backed up using Azure Backup](#)
- Learn how to [troubleshoot common issues when backing up SAP HANA databases](#)

# Supported VM SKUs for Azure Policy

12/10/2019 • 2 minutes to read • [Edit Online](#)

Azure Backup provides a built-in policy (using Azure Policy) that can be assigned to **all Azure VMs in a specified location within a subscription or resource group**. When this policy is assigned to a given scope, all new VMs created in that scope are automatically configured for backup to an **existing vault in the same location and subscription**. The table below lists all the VM SKUs supported by this policy.

## Supported VMs

**Policy Name:** Configure backup on VMs of a location to an existing central vault in the same location

| IMAGE PUBLISHER        | IMAGE OFFER   | IMAGE SKU                                                                                        |
|------------------------|---------------|--------------------------------------------------------------------------------------------------|
| MicrosoftWindowsServer | WindowsServer | Windows Server 2008 R2 SP1 (2008-R2-SP1)                                                         |
| MicrosoftWindowsServer | WindowsServer | [smalldisk] Windows Server 2008 R2 SP (2008-R2-SP1-smalldisk)                                    |
| MicrosoftWindowsServer | WindowsServer | Windows Server 2012 Datacenter (2012-Datacenter)                                                 |
| MicrosoftWindowsServer | WindowsServer | [smalldisk] Windows Server 2012 Datacenter (2012-Datacenter-smalldisk)                           |
| MicrosoftWindowsServer | WindowsServer | Windows Server 2012 R2 Datacenter (2012-R2-Datacenter)                                           |
| MicrosoftWindowsServer | WindowsServer | [smalldisk] Windows Server 2012 R2 Datacenter (2012-R2-Datacenter-smalldisk)                     |
| MicrosoftWindowsServer | WindowsServer | Windows Server 2016 Datacenter (2016-Datacenter)                                                 |
| MicrosoftWindowsServer | WindowsServer | Windows Server 2016 Datacenter - Server Core (2016-Datacenter-Server-Core)                       |
| MicrosoftWindowsServer | WindowsServer | [smalldisk] Windows Server 2016 Datacenter - Server Core (2016-Datacenter-Server-Core-smalldisk) |
| MicrosoftWindowsServer | WindowsServer | [smalldisk] Windows Server 2016 Datacenter (2016-Datacenter-smalldisk)                           |
| MicrosoftWindowsServer | WindowsServer | Windows Server 2019 Datacenter Server Core with Containers (2016-Datacenter-with-Containers)     |

| IMAGE PUBLISHER               | IMAGE OFFER             | IMAGE SKU                                                                                                               |
|-------------------------------|-------------------------|-------------------------------------------------------------------------------------------------------------------------|
| MicrosoftWindowsServer        | WindowsServer           | Windows Server 2016 Remote Desktop Session Host 2016 (2016-Datacenter-with-RDSH)                                        |
| MicrosoftWindowsServer        | WindowsServer           | Windows Server 2019 Datacenter (2019-Datacenter)                                                                        |
| MicrosoftWindowsServer        | WindowsServer           | Windows Server 2019 Datacenter Server Core (2019-Datacenter-Core)                                                       |
| MicrosoftWindowsServer        | WindowsServer           | [smalldisk] Windows Server 2019 Datacenter Server Core (2019-Datacenter-Core-smalldisk)                                 |
| MicrosoftWindowsServer        | WindowsServer           | Windows Server 2019 Datacenter Server Core with Containers (2019-Datacenter-Core-with-Containers)                       |
| MicrosoftWindowsServer        | WindowsServer           | [smalldisk] Windows Server 2019 Datacenter Server Core with Containers (2019-Datacenter-Core-with-Containers-smalldisk) |
| MicrosoftWindowsServer        | WindowsServer           | [smalldisk] Windows Server 2019 Datacenter (2019-Datacenter-smalldisk)                                                  |
| MicrosoftWindowsServer        | WindowsServer           | Windows Server 2019 Datacenter with Containers (2019-Datacenter-with-Containers)                                        |
| MicrosoftWindowsServer        | WindowsServer           | [smalldisk] Windows Server 2019 Datacenter with Containers (2019-Datacenter-with-Containers-smalldisk)                  |
| MicrosoftWindowsServer        | WindowsServer           | Windows Server 2019 Datacenter (zh-cn) (2019-Datacenter-zhcn)                                                           |
| MicrosoftWindowsServer        | WindowsServerSemiAnnual | Datacenter-Core-1709-smalldisk                                                                                          |
| MicrosoftWindowsServer        | WindowsServerSemiAnnual | Datacenter-Core-1709-with-Containers-smalldisk                                                                          |
| MicrosoftWindowsServer        | WindowsServerSemiAnnual | Datacenter-Core-1803-with-Containers-smalldisk                                                                          |
| MicrosoftWindowsServerHPCPack | WindowsServerHPCPack    | All Image SKUs                                                                                                          |
| MicrosoftSQLServer            | SQL2016SP1-WS2016       | All Image SKUs                                                                                                          |
| MicrosoftSQLServer            | SQL2016-WS2016          | All Image SKUs                                                                                                          |
| MicrosoftSQLServer            | SQL2016SP1-WS2016-BYOL  | All Image SKUs                                                                                                          |
| MicrosoftSQLServer            | SQL2012SP3-WS2012R2     | All Image SKUs                                                                                                          |

| IMAGE PUBLISHER         | IMAGE OFFER              | IMAGE SKU                                         |
|-------------------------|--------------------------|---------------------------------------------------|
| MicrosoftSQLServer      | SQL2016-WS2012R2         | All Image SKUs                                    |
| MicrosoftSQLServer      | SQL2014SP2-WS2012R2      | All Image SKUs                                    |
| MicrosoftSQLServer      | SQL2012SP3-WS2012R2-BYOL | All Image SKUs                                    |
| MicrosoftSQLServer      | SQL2014SP1-WS2012R2-BYOL | All Image SKUs                                    |
| MicrosoftSQLServer      | SQL2014SP2-WS2012R2-BYOL | All Image SKUs                                    |
| MicrosoftSQLServer      | SQL2016-WS2012R2-BYOL    | All Image SKUs                                    |
| MicrosoftRServer        | MLServer-WS2016          | All Image SKUs                                    |
| MicrosoftVisualStudio   | VisualStudio             | All Image SKUs                                    |
| MicrosoftVisualStudio   | Windows                  | All Image SKUs                                    |
| MicrosoftDynamicsAX     | Dynamics                 | Pre-Req-AX7-Onebox-U8                             |
| microsoft-ads           | windows-data-science-vm  | All Image SKUs                                    |
| MicrosoftWindowsDesktop | Windows-10               | All Image SKUs                                    |
| RedHat                  | RHEL                     | 6.7, 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7 |
| RedHat                  | RHEL-SAP-HANA            | 6.7, 7.2, 7.3                                     |
| SUSE                    | SLES                     | 12.X                                              |
| SUSE                    | SLES-HPC                 | 12.X                                              |
| SUSE                    | SLES-HPC-Priority        | 12.X                                              |
| SUSE                    | SLES-SAP                 | 12.X                                              |
| SUSE                    | SLES-SAP-BYOS            | 12.X                                              |
| SUSE                    | SLES-Priority            | 12.X                                              |
| SUSE                    | SLES-BYOS                | 12.X                                              |
| SUSE                    | SLES-SAPCAL              | 12.X                                              |
| SUSE                    | SLES-Standard            | 12.X                                              |
| Canonical               | UbuntuServer             | 14.04.0-LTS                                       |
| Canonical               | UbuntuServer             | 14.04.1-LTS                                       |

| IMAGE PUBLISHER | IMAGE OFFER        | IMAGE SKU                          |
|-----------------|--------------------|------------------------------------|
| Canonical       | UbuntuServer       | 14.04.2-LTS                        |
| Canonical       | UbuntuServer       | 14.04.3-LTS                        |
| Canonical       | UbuntuServer       | 14.04.4-LTS                        |
| Canonical       | UbuntuServer       | 14.04.5-DAILY-LTS                  |
| Canonical       | UbuntuServer       | 14.04.5-LTS                        |
| Canonical       | UbuntuServer       | 16.04-DAILY-LTS                    |
| Canonical       | UbuntuServer       | 16.04-LTS                          |
| Canonical       | UbuntuServer       | 16.04.0-LTS                        |
| Canonical       | UbuntuServer       | 18.04-DAILY-LTS                    |
| Canonical       | UbuntuServer       | 18.04-LTS                          |
| Oracle          | Oracle-Linux       | 6.8, 6.9, 6.10, 7.3, 7.4, 7.5, 7.6 |
| OpenLogic       | CentOS             | 6.X, 7.X                           |
| OpenLogic       | CentOS-LVM         | 6.X, 7.X                           |
| OpenLogic       | CentOS-SRIOV       | 6.X, 7.X                           |
| cloudera        | cloudera-centos-os | 7.X                                |

# Azure Backup - Frequently asked questions

12/18/2019 • 9 minutes to read • [Edit Online](#)

This article answers common questions about the Azure Backup service.

## Recovery services vault

### **Is there any limit on the number of vaults that can be created in each Azure subscription?**

Yes. You can create up to 500 Recovery Services vaults, per supported region of Azure Backup, per subscription. If you need additional vaults, create an additional subscription.

### **Are there limits on the number of servers/machines that can be registered against each vault?**

You can register up to 1000 Azure Virtual machines per vault. If you are using the Microsoft Azure Backup Agent, you can register up to 50 MAB agents per vault. And you can register 50 MAB servers/DPM servers to a vault.

### **How many datasources/items can be protected in a vault?**

You can protect up to 2000 datasources/items across all workloads (IaaS VM, SQL, AFS, etc.) in a vault. For example, if you have already protected 500 VMs and 400 Azure Files shares in the vault, you can only protect up to 1100 SQL databases in it.

### **How many policies can I create per vault?**

You can only have up to 200 policies per vault.

### **If my organization has one vault, how can I isolate data from different servers in the vault when restoring data?**

Server data that you want to recover together should use the same passphrase when you set up backup. If you want to isolate recovery to a specific server or servers, use a passphrase for that server or servers only. For example, human resources servers could use one encryption passphrase, accounting servers another, and storage servers a third.

### **Can I move my vault between subscriptions?**

Yes. To move a Recovery Services vault, refer this [article](#)

### **Can I move backup data to another vault?**

No. Backup data stored in a vault can't be moved to a different vault.

### **Can I change from GRS to LRS after a backup?**

No. A Recovery Services vault can only change storage options before any backups have been stored.

### **Can I do an Item Level Restore (ILR) for VMs backed up to a Recovery Services vault?**

- ILR is supported for Azure VMs backed up by Azure VM backup. For more information, see [article](#)
- ILR is not supported for online recovery points of on-premises VMs backed up by Azure backup Server or System Center DPM.

## Azure Backup agent

### **Where can I find common questions about the Azure Backup agent for Azure VM backup?**

- For the agent running on Azure VMs, read this [FAQ](#).
- For the agent used to back up Azure file folders, read this [FAQ](#).

# General backup

## Are there limits on backup scheduling?

Yes.

- You can back up Windows Server or Windows machines up to three times a day. You can set the scheduling policy to daily or weekly schedules.
- You can back up DPM up to twice a day. You can set the scheduling policy to daily, weekly, monthly, and yearly.
- You back up Azure VMs once a day.

## What operating systems are supported for backup?

Azure Backup supports these operating systems for backing up files and folders, and apps protected by Azure Backup Server and DPM.

| OS                                    | SKU                                                                   | Details                                                           |
|---------------------------------------|-----------------------------------------------------------------------|-------------------------------------------------------------------|
| Workstation                           |                                                                       |                                                                   |
| Windows 10 64 bit                     | Enterprise, Pro, Home                                                 | Machines should be running the latest services packs and updates. |
| Windows 8.1 64 bit                    | Enterprise, Pro                                                       | Machines should be running the latest services packs and updates. |
| Windows 8 64 bit                      | Enterprise, Pro                                                       | Machines should be running the latest services packs and updates. |
| Windows 7 64 bit                      | Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter | Machines should be running the latest services packs and updates. |
| Server                                |                                                                       |                                                                   |
| Windows Server 2019 64 bit            | Standard, Datacenter, Essentials                                      | With the latest service packs/updates.                            |
| Windows Server 2016 64 bit            | Standard, Datacenter, Essentials                                      | With the latest service packs/updates.                            |
| Windows Server 2012 R2 64 bit         | Standard, Datacenter, Foundation                                      | With the latest service packs/updates.                            |
| Windows Server 2012 64 bit            | Datacenter, Foundation, Standard                                      | With the latest service packs/updates.                            |
| Windows Storage Server 2016 64 bit    | Standard, Workgroup                                                   | With the latest service packs/updates.                            |
| Windows Storage Server 2012 R2 64 bit | Standard, Workgroup, Essential                                        | With the latest service packs/updates.                            |
| Windows Storage Server 2012 64 bit    | Standard, Workgroup                                                   | With the latest service packs/updates.                            |
| Windows Server 2008 R2 SP1 64 bit     | Standard, Enterprise, Datacenter, Foundation                          | With the latest updates.                                          |
| Windows Server 2008 64 bit            | Standard, Enterprise, Datacenter                                      | With latest updates.                                              |

Azure Backup doesn't support 32-bit operating systems.

For Azure VM Linux backups, Azure Backup supports [the list of distributions endorsed by Azure](#), except Core OS

Linux and 32-bit operating system. Other bring-your-own Linux distributions might work as long as the VM agent is available on the VM, and support for Python exists.

### Are there size limits for data backup?

Sizes limits are as follows:

| OS/MACHINE                                  | SIZE LIMIT OF DATA SOURCE                                                                                                                                                                                                              |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Windows 8 or later                          | 54,400 GB                                                                                                                                                                                                                              |
| Windows 7                                   | 1700 GB                                                                                                                                                                                                                                |
| Windows Server 2012 or later                | 54,400 GB                                                                                                                                                                                                                              |
| Windows Server 2008, Windows Server 2008 R2 | 1700 GB                                                                                                                                                                                                                                |
| Azure VM                                    | <p>16 data disks<br/>To sign up for the private preview of VMs with 16+ disks (up to 32 disks), write to us at <a href="mailto:AskAzureBackupTeam@microsoft.com">AskAzureBackupTeam@microsoft.com</a></p> <p>Data disk up to 32 TB</p> |

### How is the data source size determined?

The following table explains how each data source size is determined.

| DATA SOURCE         | DETAILS                                                                                  |
|---------------------|------------------------------------------------------------------------------------------|
| Volume              | The amount of data being backed up from single volume VM being backed up.                |
| SQL Server database | Size of single SQL database size being backed up.                                        |
| SharePoint          | Sum of the content and configuration databases within a SharePoint farm being backed up. |
| Exchange            | Sum of all Exchange databases in an Exchange server being backed up.                     |
| BMR/System state    | Each individual copy of BMR or system state of the machine being backed up.              |

### Is there a limit on the amount of data backed up using a Recovery Services vault?

There is no limit on the amount of data you can back up using a Recovery Services vault.

### Why is the size of the data transferred to the Recovery Services vault smaller than the data selected for backup?

Data backed up from Azure Backup Agent, DPM, and Azure Backup Server is compressed and encrypted before being transferred. With compression and encryption is applied, the data in the vault is 30-40% smaller.

### Can I delete individual files from a recovery point in the vault?

No, Azure Backup doesn't support deleting or purging individual items from stored backups.

### If I cancel a backup job after it starts, is the transferred backup data deleted?

No. All data that was transferred into the vault before the backup job was canceled remains in the vault.

- Azure Backup uses a checkpoint mechanism to occasionally add checkpoints to the backup data during the backup.
- Because there are checkpoints in the backup data, the next backup process can validate the integrity of the files.
- The next backup job will be incremental to the data previously backed up. Incremental backups only transfer new or changed data, which equates to better utilization of bandwidth.

If you cancel a backup job for an Azure VM, any transferred data is ignored. The next backup job transfers incremental data from the last successful backup job.

## Retention and recovery

### Are the retention policies for DPM and Windows machines without DPM the same?

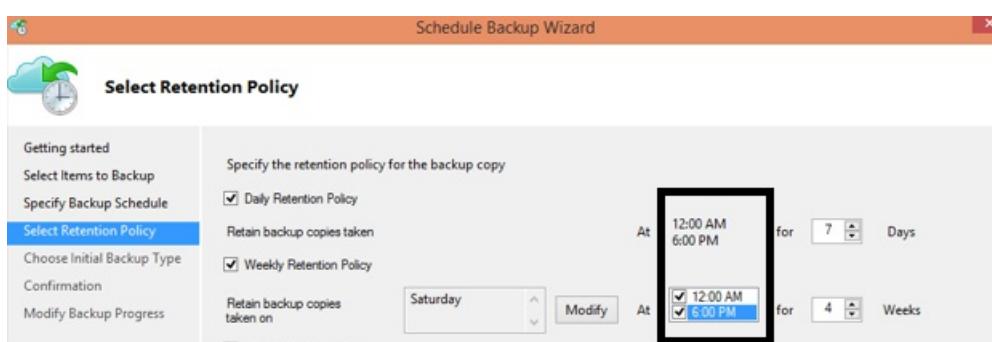
Yes, they both have daily, weekly, monthly, and yearly retention policies.

### Can I customize retention policies?

Yes, you have customize policies. For example, you can configure weekly and daily retention requirements, but not yearly and monthly.

### Can I use different times for backup scheduling and retention policies?

No. Retention policies can only be applied on backup points. For example, this image shows a retention policy for backups taken at 12am and 6pm.



### If a backup is kept for a long time, does it take more time to recover an older data point?

No. The time to recover the oldest or the newest point is the same. Each recovery point behaves like a full point.

### If each recovery point is like a full point, does it impact the total billable backup storage?

Typical long-term retention point products store backup data as full points.

- The full points are storage *inefficient* but are easier and faster to restore.
- Incremental copies are storage *efficient* but require you to restore a chain of data, which impacts your recovery time

Azure Backup storage architecture gives you the best of both worlds by optimally storing data for fast restores and incurring low storage costs. This ensures that your ingress and egress bandwidth is used efficiently. The amount of data storage, and the time needed to recover the data, is kept to a minimum. Learn more about [incremental backups](#).

### Is there a limit on the number of recovery points that can be created?

You can create up to 9999 recovery points per protected instance. A protected instance is a computer, server (physical or virtual), or workload that backs up to Azure.

- Learn more about [backup and retention](#).

### How many times can I recover data that's backed up to Azure?

There is no limit on the number of recoveries from Azure Backup.

## **When restoring data, do I pay for the egress traffic from Azure?**

No. Recovery is free and you aren't charged for the egress traffic.

## **What happens when I change my backup policy?**

When a new policy is applied, schedule and retention of the new policy is followed.

- If retention is extended, existing recovery points are marked to keep them as per new policy.
- If retention is reduced, they are marked for pruning in the next cleanup job and subsequently deleted.

## **Encryption**

### **Is the data sent to Azure encrypted?**

Yes. Data is encrypted on the on-premises machine using AES256. The data is sent over a secure HTTPS link. The data transmitted in cloud is protected by HTTPS link only between storage and recovery service. iSCSI protocol secures the data transmitted between recovery service and user machine. Secure tunneling is used to protect the iSCSI channel.

### **Is the backup data on Azure encrypted as well?**

Yes. The data in Azure is encrypted-at-rest.

- For on-premises backup, encryption-at-rest is provided using the passphrase you provide when backing up to Azure.
- For Azure VMs, data is encrypted-at-rest using Storage Service Encryption (SSE).

Microsoft does not decrypt the backup data at any point.

### **What is the minimum length of encryption the key used to encrypt backup data?**

The encryption key should be at least 16 characters when you are using Azure backup agent. For Azure VMs, there is no limit to length of keys used by Azure KeyVault.

### **What happens if I misplace the encryption key? Can I recover the data? Can Microsoft recover the data?**

The key used to encrypt the backup data is present only on your site. Microsoft does not maintain a copy in Azure and does not have any access to the key. If you misplace the key, Microsoft can't recover the backup data.

## **Next steps**

Read the other FAQs:

- [Common questions](#) about Azure VM backups.
- [Common questions](#) about the Azure Backup agent

# Frequently asked questions-Back up Azure VMs

1/23/2020 • 7 minutes to read • [Edit Online](#)

This article answers common questions about backing up Azure VMs with the [Azure Backup](#) service.

## Backup

### Which VM images can be enabled for backup when I create them?

When you create a VM, you can enable backup for VMs running [supported operating systems](#)

### Is the backup cost included in the VM cost?

No. Backup costs are separate from a VM's costs. Learn more about [Azure Backup pricing](#).

### Which permissions are required to enable backup for a VM?

If you're a VM contributor, you can enable backup on the VM. If you're using a custom role, you need the following permissions to enable backup on the VM:

- Microsoft.RecoveryServices/Vaults/write
- Microsoft.RecoveryServices/Vaults/read
- Microsoft.RecoveryServices/locations/\*
- Microsoft.RecoveryServices/Vaults/backupFabrics/protectionContainers/protectedItems/\*/read
- Microsoft.RecoveryServices/Vaults/backupFabrics/protectionContainers/protectedItems/read
- Microsoft.RecoveryServices/Vaults/backupFabrics/protectionContainers/protectedItems/write
- Microsoft.RecoveryServices/Vaults/backupFabrics/backupProtectionIntent/write
- Microsoft.RecoveryServices/Vaults/backupPolicies/read
- Microsoft.RecoveryServices/Vaults/backupPolicies/write

If your Recovery Services vault and VM have different resource groups, make sure you have write permissions in the resource group for the Recovery Services vault.

### Does an on-demand backup job use the same retention schedule as scheduled backups?

No. Specify the retention range for an on-demand backup job. By default, it's retained for 30 days when triggered from the portal.

### I recently enabled Azure Disk Encryption on some VMs. Will my backups continue to work?

Provide permissions for Azure Backup to access Key Vault. Specify the permissions in PowerShell as described in the **Enable backup** section in the [Azure Backup PowerShell](#) documentation.

### I migrated VM disks to managed disks. Will my backups continue to work?

Yes, backups work seamlessly. There's no need to reconfigure anything.

### Why can't I see my VM in the Configure Backup wizard?

The wizard only lists VMs in the same region as the vault, and that aren't already being backed up.

### My VM is shut down. Will an on-demand or a scheduled backup work?

Yes. Backups run when a machine is shut down. The recovery point is marked as crash consistent.

### Can I cancel an in-progress backup job?

Yes. You can cancel backup job in a **Taking snapshot** state. You can't cancel a job if data transfer from the snapshot is in progress.

**I enabled lock on resource group created by Azure Backup Service (i.e. `AzureBackupRG_<geo>_<number>`), will my backups continue to work?**

If you lock the resource group created by Azure Backup Service, backups will start to fail as there's a maximum limit of 18 restore points.

User needs to remove the lock and clear the restore point collection from that resource group in order to make the future backups successful, [follow these steps](#) to remove the restore point collection.

**Does Azure backup support standard SSD-managed disks?**

Yes, Azure Backup supports [standard SSD managed disks](#).

**Can we back up a VM with a Write Accelerator (WA)-enabled disk?**

Snapshots can't be taken on the WA-enabled disk. However, the Azure Backup service can exclude the WA-enabled disk from backup.

**I have a VM with Write Accelerator (WA) disks and SAP HANA installed. How do I back up?**

Azure Backup can't back up the WA-enabled disk but can exclude it from backup. However, the backup won't provide database consistency because information on the WA-enabled disk isn't backed up. You can back up disks with this configuration if you want operating system disk backup, and backup of disks that aren't WA-enabled.

We're running private preview for an SAP HANA backup with an RPO of 15 minutes. It's built in a similar way to SQL DB backup, and uses the `backInt` interface for third-party solutions certified by SAP HANA. If you're interested, email us at [AskAzureBackupTeam@microsoft.com](mailto:AskAzureBackupTeam@microsoft.com) with the subject **Sign up for private preview for backup of SAP HANA in Azure VMs**.

**What is the maximum delay I can expect in backup start time from the scheduled backup time I have set in my VM backup policy?**

The scheduled backup will be triggered within 2 hours of the scheduled backup time. For example, If 100 VMs have their backup start time scheduled at 2:00 AM, then by maximum 4:00 AM all the 100 VMs will have backup job in progress. If scheduled backups have been paused due to outage and resumed/retried, then backup can start outside of this scheduled two-hour window.

**What is the minimum allowed retention range for daily backup point?**

Azure Virtual Machine backup policy supports a minimum retention range of seven days up to 9999 days. Any modification to an existing VM backup policy with less than seven days will require an update to meet the minimum retention range of seven days.

**Can I backup or restore selective disks attached to a VM?**

Azure Backup now supports selective disk backup and restore using the Azure Virtual Machine backup solution.

Today, Azure Backup supports backing up all the disks (Operating System and data) in a VM together using the Virtual Machine backup solution. With exclude-disk functionality, you get an option to backup one or a few from the many data disks in a VM. This provides an efficient and cost-effective solution for your backup and restore needs. Each recovery point contains data of the disks included in the backup operation, which further allows you to have a subset of disks restored from the given recovery point during the restore operation. This applies to restore both from the snapshot and the vault.

To sign up for the preview, write to us at [AskAzureBackupTeam@microsoft.com](mailto:AskAzureBackupTeam@microsoft.com)

## Restore

**How do I decide whether to restore disks only or a full VM?**

Think of a VM restore as a quick create option for an Azure VM. This option changes disk names, containers used by the disks, public IP addresses, and network interface names. The change maintains unique resources when a VM is created. The VM isn't added to an availability set.

You can use the restore disk option if you want to:

- Customize the VM that gets created. For example, change the size.
- Add configuration settings that weren't there at the time of backup.
- Control the naming convention for resources that are created.
- Add the VM to an availability set.
- Add any other setting that must be configured using PowerShell or a template.

### **Can I restore backups of unmanaged VM disks after I upgrade to managed disks?**

Yes, you can use backups taken before disks were migrated from unmanaged to managed.

### **How do I restore a VM to a restore point before the VM was migrated to managed disks?**

The restore process remains the same. If the recovery point is of a point-in-time when VM had unmanaged disks, you can [restore disks as unmanaged](#). If the VM had managed disks then, you can [restore disks as managed disks](#). Then you can [create a VM from those disks](#).

[Learn more](#) about doing this in PowerShell.

### **Can I restore the VM that's been deleted?**

Yes. Even if you delete the VM, you can go to corresponding backup item in the vault and restore from a recovery point.

### **How to restore a VM to the same availability sets?**

For Managed Disk Azure VM, restoring to the availability sets is enabled by providing an option in template while restoring as managed Disks. This template has the input parameter called **Availability sets**.

### **How do we get faster restore performances?**

[Instant Restore](#) capability helps in faster backups and instant restores from the snapshots.

### **What happens when we change the key vault settings for the encrypted VM?**

After you change the KeyVault settings for the encrypted VM, backups will continue to work with the new set of details. However, after the restore from a recovery point prior to the change, you will have to restore the secrets in a KeyVault before you can create the VM from it. For more information, refer this [article](#)

Operations like secret/key roll-over do not require this step and the same KeyVault can be used after restore.

### **Can I access the VM once restored due to a VM having broken relationship with domain controller?**

Yes, you access the VM once restored due to a VM having broken relationship with domain controller. For more information, refer this [article](#)

## Manage VM backups

### **What happens if I modify a backup policy?**

The VM is backed up using the schedule and retention settings in the modified or new policy.

- If retention is extended, existing recovery points are marked and kept in accordance with the new policy.
- If retention is reduced, recovery points are marked for pruning in the next cleanup job, and subsequently deleted.

### **How do I move a VM backed up by Azure Backup to a different resource group?**

1. Temporarily stop the backup, and retain backup data.
2. Move the VM to the target resource group.
3. Re-enabled backup in the same or new vault.

You can restore the VM from available restore points that were created before the move operation.

**Is there a limit on number of VMs that can be associated with a same backup policy?**

Yes, there is a limit of 100 VMs that can be associated to the same backup policy from portal. We recommend that for more than 100 VMs, create multiple backup policies with same schedule or different schedule.

# Common questions about backing up files and folders

2/17/2020 • 7 minutes to read • [Edit Online](#)

This article answers common questions about backing up files and folders with the Microsoft Azure Recovery Services (MARS) Agent in the [Azure Backup](#) service.

## Configure backups

### Where can I download the latest version of the MARS agent?

The latest MARS agent used when backing up Windows Server machines, System Center DPM, and Microsoft Azure Backup server is available for [download](#).

### How long are vault credentials valid?

Vault credentials expire after 48 hours. If the credentials file expires, download the file again from the Azure portal.

### From what drives can I back up files and folders?

You can't back up the following types of drives and volumes:

- Removable media: All backup item sources must report as fixed.
- Read-only volumes: The volume must be writable for the volume shadow copy service (VSS) to function.
- Offline volumes: The volume must be online for VSS to function.
- Network shares: The volume must be local to the server to be backed up using online backup.
- BitLocker-protected volumes: The volume must be unlocked before the backup can occur.
- File System Identification: NTFS is the only file system supported.

### What file and folder types are supported?

[Learn more](#) about the types of files and folders supported for backup.

### Can I use the MARS agent to back up files and folders on an Azure VM?

Yes. Azure Backup provides VM-level backup for Azure VMs using the VM extension for the Azure VM agent. If you want to back up files and folders on the guest Windows operating system on the VM, you can install the MARS agent to do that.

### Can I use the MARS agent to back up files and folders on temporary storage for the Azure VM?

Yes. Install the MARS agent, and back up files and folders on the guest Windows operating system to temporary storage.

- Backup jobs fail when temporary storage data is wiped out.
- If the temporary storage data is deleted, you can only restore to non-volatile storage.

### How do I register a server to another region?

Backup data is sent to the datacenter of the vault in which the server is registered. The easiest way to change the datacenter is to uninstall and reinstall the agent, and then register the machine to a new vault in the region you need.

### Does the MARS agent support Windows Server 2012 deduplication?

Yes. The MARS agent converts the deduplicated data to normal data when it prepares the backup operation. It

then optimizes the data for backup, encrypts the data, and then sends the encrypted data to the vault.

## Manage backups

### What happens if I rename a Windows machine configured for backup?

When you rename a Windows machine, all currently configured backups are stopped.

- You need to register the new machine name with the Backup vault.
- When you register the new name with the vault, the first operation is a *full* backup.
- If you need to recover data backed up to the vault with the old server name, use the option to restore to an alternate location in the Recover Data Wizard. [Learn more](#).

### What is the maximum file path length for backup?

The MARS agent relies on NTFS, and uses the filepath length specification limited by the [Windows API](#). If the files you want to protect are longer than the allowed value, back up the parent folder or the disk drive.

### What characters are allowed in file paths?

The MARS agent relies on NTFS, and allows [supported characters](#) in file names/paths.

### The warning "Azure Backups have not been configured for this server" appears

This warning can appear even though you've configured a backup policy, when the backup schedule settings stored on the local server aren't the same as the settings stored in the backup vault.

- When the server or the settings have been recovered to a known good state, backup schedules can become unsynchronized.
- If you receive this warning, [configure](#) the backup policy again, and then run an on-demand backup to resynchronize the local server with Azure.

## Manage the backup cache folder

### What's the minimum size requirement for the cache folder?

The size of the cache folder determines the amount of data that you are backing up.

- The cache folder volumes should have free space that equals at least 5-10% of the total size of backup data.
- If the volume has less than 5% free space, either increase the volume size, or move the cache folder to a volume with enough space by following [these steps](#).
- If you backup Windows System State, you'll need an additional 30-35 GB of free space in the volume containing the cache folder.

### How to check if scratch folder is valid and accessible?

1. By default scratch folder is located at `\Program Files\Microsoft Azure Recovery Services Agent\Scratch`

2. Make sure the path of your scratch folder location matches with the values of the registry key entries shown below:

| REGISTRY PATH                                                                                    | REGISTRY KEY | VALUE                     |
|--------------------------------------------------------------------------------------------------|--------------|---------------------------|
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ScratchLocation<br>Azure Backup\Config                     |              | New cache folder location |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ScratchLocation<br>Azure Backup\Config\CloudBackupProvider |              | New cache folder location |

### How do I change the cache location for the MARS agent?

1. Run this command in an elevated command prompt to stop the Backup engine:

```
Net stop obengine
```

2. If you have configured System State backup, open Disk Management and unmount the disk(s) with names in the format "CBSBVol\_<ID>" .
3. By default, the scratch folder is located at \Program Files\Microsoft Azure Recovery Services Agent\Scratch
4. Copy the entire \Scratch folder to a different drive that has sufficient space. Ensure the contents are copied, not moved.
5. Update the following registry entries with the path of the newly moved scratch folder.

| REGISTRY PATH                                                                                    | REGISTRY KEY    | VALUE                              |
|--------------------------------------------------------------------------------------------------|-----------------|------------------------------------|
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ScratchLocation<br>Azure Backup\Config                     | ScratchLocation | <i>New scratch folder location</i> |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ScratchLocation<br>Azure Backup\Config\CloudBackupProvider | ScratchLocation | <i>New scratch folder location</i> |

6. Restart the Backup engine at an elevated command prompt:

```
Net stop obengine

Net start obengine
```

7. Run an on-demand backup. After the backup finishes successfully using the new location, you can remove the original cache folder.

### Where should the cache folder be located?

The following locations for the cache folder aren't recommended:

- Network share/removable media: The cache folder must be local to the server that needs backing up using online backup. Network locations or removable media like USB drives aren't supported.
- Offline volumes: The cache folder must be online for expected backup using Azure Backup Agent

### Are there any attributes of the cache folder that aren't supported?

The following attributes or their combinations are not supported for the cache folder:

- Encrypted
- De-duplicated
- Compressed
- Sparse
- Reparse-Point

The cache folder and the metadata VHD don't have the necessary attributes for the Azure Backup agent.

### Is there a way to adjust the amount of bandwidth used for backup?

Yes, you can use the **Change Properties** option in the MARS agent to adjust the bandwidth and timing. [Learn more](#).

## Restore

### Manage

**Can I recover if I forgot my passphrase?** The Azure Backup agent requires a passphrase (that you provided

during registration) to decrypt the backed-up data during restore. Review the scenarios below to understand your options for handling a lost passphrase:

| ORIGINAL MACHINE<br><i>(SOURCE MACHINE WHERE BACKUPS<br/>WERE TAKEN)</i> | PASSPHRASE | AVAILABLE OPTIONS                                                                                                                                                                                              |
|--------------------------------------------------------------------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Available                                                                | Lost       | If your original machine (where backups were taken) is available and still registered with the same Recovery Services vault, then you can regenerate the passphrase by following these <a href="#">steps</a> . |
| Lost                                                                     | Lost       | Not possible to recover the data or data is not available                                                                                                                                                      |

Consider the following conditions:

- If you uninstall and re-register the agent on the same original machine with
  - *Same passphrase*, then you will be able to restore your backed-up data.
  - *Different passphrase*, then you will not be able to restore your backed-up data.
- If you install the agent on a *different machine* with
  - *Same passphrase* (used in the original machine), then you will be able to restore your backed-up data.
  - *Different passphrase*, you will not be able to restore your backed-up data.
- If your original machine is corrupted (preventing you from regenerating the passphrase through the MARS console), but you can restore or access the original scratch folder used by the MARS agent, then you might be able to restore (if you forgot the password). For more assistance, contact Customer Support.

### How do I recover if I lost my original machine (where backups were taken)?

If you have the same passphrase (that you provided during registration) of the original machine, then you can restore the backed-up data to an alternate machine. Review the scenarios below to understand your restore options.

| ORIGINAL MACHINE | PASSPHRASE | AVAILABLE OPTIONS                                                                                                                                                                                                                                                                            |
|------------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Lost             | Available  | You can install and register the MARS agent on another machine with the same passphrase that you provided during registration of the original machine. Choose <b>Recovery Option &gt; Another location</b> to perform your restore. For more information, see this <a href="#">article</a> . |
| Lost             | Lost       | Not possible to recover the data or data is not available                                                                                                                                                                                                                                    |

### What happens if I cancel an ongoing restore job?

If an ongoing restore job is canceled, the restore process stops. All files restored before the cancellation stay in configured destination (original or alternate location), without any rollbacks.

### Does the MARS agent back up and restore ACLs set on files, folders, and volumes?

- The MARS agent backs up ACLs set on files, folders, and volumes
- For Volume Restore recovery option, the MARS agent provides an option to skip restoring ACL permissions

to the file or folder being recovered

- For the individual file and folders recovery option, the MARS agent will restore with ACL permissions (there is no option to skip ACL restore).

## Next steps

[Learn](#) how to back up a Windows machine.

# Questions about backing up Azure Files

1/20/2020 • 4 minutes to read • [Edit Online](#)

This article answers common questions about backing up Azure Files. In some of the answers, there are links to the articles that have comprehensive information. You can also post questions about the Azure Backup service in the [discussion forum](#).

To quickly scan the sections in this article, use the links to the right, under **In this article**.

## Configuring the backup job for Azure Files

### **Why can't I see some of my Storage Accounts I want to protect, that contain valid Azure file shares?**

During preview, Backup for Azure file Shares does not support all types of Storage Accounts. Refer to the list [here](#) to see the list of supported Storage Accounts. It is also possible that the Storage Account you are looking for is already protected or registered with another Vault. [Unregister](#) from the vault to discover the Storage Account in other Vaults for protection.

### **Why can't I see some of my Azure file shares in the Storage Account when I'm trying to configure backup?**

Check if the Azure file share is already protected in the same Recovery Services vault or if it has been deleted recently.

### **Can I protect File Shares connected to a Sync Group in Azure Files Sync?**

Yes. Protection of Azure File Shares connected to Sync Groups is enabled and part of Public preview.

### **When trying to back up file shares, I clicked on a Storage Account for discovering the file shares in it. However, I did not protect them. How do I protect these file shares with any other Vault?**

When trying to back up, selecting a Storage Account to discover file shares within it registers the Storage Account with the Vault from which this is done. If you choose to protect the file shares with a different Vault, [Unregister](#) the chosen Storage Account from this Vault.

### **Can I change the Vault to which I back up my file shares?**

Yes. However, you'll need to [Stop protection on a file share](#) from the connected Vault, [Unregister](#) this Storage Account, and then protect it from a different Vault.

### **In which geos can I back up Azure File shares?**

Backup for Azure File shares is currently in Preview and is available only in the following geos:

- Australia East (AE)
- Australia South East (ASE)
- Brazil South (BRS)
- Canada Central (CNC)
- Canada East (CE)
- Central US (CUS)
- East Asia (EA)
- East US (EUS)
- East US 2 (EUS2)
- Japan East (JPE)
- Japan West (JPW)
- India Central (INC)

- India South (INS)
- Korea Central (KRC)
- Korea South (KRS)
- North Central US (NCUS)
- North Europe (NE)
- South Central US (SCUS)
- South East Asia (SEA)
- UK South (UKS)
- UK West (UKW)
- West Europe (WE)
- West US (WUS)
- West Central US (WCUS)
- West US 2 (WUS 2)
- US Gov Arizona (UGA)
- US Gov Texas (UGT)
- US Gov Virginia (UGV)
- Australia Central (ACL)
- India West(INW)
- South Africa North(SAN)
- UAE North(UAN)
- France Central (FRC)
- Germany North (GN)
- Germany West Central (GWC)
- South Africa West (SAW)
- UAE Central (UAC)
- NWE (Norway East)
- NWW (Norway West)
- SZN (Switzerland North)

Write to [AskAzureBackupTeam@microsoft.com](mailto:AskAzureBackupTeam@microsoft.com) if you need to use it in a specific geo that is not listed above.

#### **How many Azure file shares can I protect in a Vault?**

During the preview, you can protect Azure file shares from up to 50 Storage Accounts per Vault. You can also protect up to 200 Azure file shares in a single vault.

#### **Can I protect two different file shares from the same Storage Account to different Vaults?**

No. All file shares in a Storage Account can be protected only by the same Vault.

## Backup

#### **How many scheduled backups can I configure per file share?**

Azure Backup currently supports configuring scheduled once-daily backups of Azure File Shares.

#### **How many On-Demand backups can I take per file share?**

You can have up to 200 Snapshots for a file share at any point in time. The limit includes snapshots taken by Azure Backup as defined by your policy. If your backups start failing after reaching the limit, delete On-Demand restore points for successful future backups.

## Restore

## **Can I recover from a deleted Azure file share?**

When an Azure file share is deleted, you're shown the list of backups that will be deleted and a confirmation is sought. A deleted Azure file share can't be restored.

## **Can I restore from backups if I stopped protection on an Azure file share?**

Yes. If you chose **Retain Backup Data** when you stopped protection, then you can restore from all existing restore points.

## **What happens if I cancel an ongoing restore job?**

If an ongoing restore job is canceled, the restore process stops and all files restored before the cancellation, stay in configured destination (original or alternate location) without any rollbacks.

# Manage backup

## **Can I use PowerShell to configure/manage/restore backups of Azure File shares?**

Yes. Please refer to the detailed documentation [here](#)

## **Can I access the snapshots taken by Azure Backups and mount it?**

All Snapshots taken by Azure Backup can be accessed by Viewing Snapshots in the portal, PowerShell, or CLI. To learn more about Azure Files share snapshots, see [Overview of share snapshots for Azure Files \(preview\)](#).

## **What is the maximum retention I can configure for backups?**

Backup for Azure file shares offers the ability to configure policies with retention up to 180 days. However, using the "On-demand backup" option in [PowerShell](#), you can retain a recovery point even for 10 years.

## **What happens when I change the Backup policy for an Azure file share?**

When a new policy is applied on file share(s), schedule and retention of the new policy is followed. If retention is extended, existing recovery points are marked to keep them as per new policy. If retention is reduced, they're marked for pruning in the next cleanup job and deleted.

# Next steps

To learn more about other areas of Azure Backup, see some of these other Backup FAQs:

- [Recovery Services vault FAQ](#)
- [Azure VM backup FAQ](#)
- [Azure Backup agent FAQ](#)

# FAQ about SQL Server databases that are running on an Azure VM backup

2/25/2020 • 5 minutes to read • [Edit Online](#)

This article answers common questions about backing up SQL Server databases that run on Azure virtual machines (VMs) and use the [Azure Backup](#) service.

## Can I use Azure backup for IaaS VM as well as SQL Server on the same machine?

Yes, you can have both VM backup and SQL backup on the same VM. In this case, we internally trigger copy-only full backup on the VM to not truncate the logs.

## Does the solution retry or auto-heal the backups?

Under some circumstances, the Azure Backup service triggers remedial backups. Auto-heal can happen for any of the six conditions mentioned below:

- If log or differential backup fails due to LSN Validation Error, next log or differential backup is instead converted to a full backup.
- If no full backup has happened before a log or differential backup, that log or differential backup is instead converted to a full backup.
- If the latest full backup's point-in-time is older than 15 days, the next log or differential backup is instead converted to a full backup.
- All the backup jobs that get canceled due to an extension upgrade are re-triggered after the upgrade is completed and the extension is started.
- If you choose to overwrite the database during Restore, the next log/differential backup fails and a full backup is triggered instead.
- In cases where a full backup is required to reset the log chains due to change in database recovery model, a full gets triggered automatically on the next schedule.

Auto-heal as a capability is enabled for all user by default; However in case you choose to opt-out of it, then perform the below:

- On the SQL Server instance, in the *C:\Program Files\Azure Workload Backup\bin* folder, create or edit the **ExtensionSettingsOverrides.json** file.
- In the **ExtensionSettingsOverrides.json**, set `{"EnableAutoHealer":false}`.
- Save your changes and close the file.
- On the SQL Server instance, open **Task Manager** and then restart the **AzureWLBackupCoordinatorSvc** service.

## Can I control how many concurrent backups run on the SQL server?

Yes. You can throttle the rate at which the backup policy runs to minimize the impact on a SQL Server instance. To change the setting:

1. On the SQL Server instance, in the *C:\Program Files\Azure Workload Backup\bin* folder, create the **ExtensionSettingsOverrides.json** file.

2. In the `ExtensionSettingsOverrides.json` file, change the **DefaultBackupTasksThreshold** setting to a lower value (for example, 5).

```
{"DefaultBackupTasksThreshold": 5}
```

The default value of `DefaultBackupTasksThreshold` is **20**.

3. Save your changes and close the file.

4. On the SQL Server instance, open **Task Manager**. Restart the **AzureWLBackupCoordinatorSvc** service.

While this method helps if the backup application is consuming a large quantity of resources, SQL Server [Resource Governor](#) is a more generic way to specify limits on the amount of CPU, physical IO, and memory that incoming application requests can use.

**NOTE**

In the UX you can still go ahead and schedule as many backups at any given time, however they will be processed in a sliding window of say, 5, as per the above example.

## Can I run a full backup from a secondary replica?

According to SQL limitations, you can run Copy Only Full backup on Secondary Replica; however Full backup is not allowed.

## Can I protect availability groups on-premises?

No. Azure Backup protects SQL Server databases running in Azure. If an availability group (AG) is spread between Azure and on-premises machines, the AG can be protected only if the primary replica is running in Azure. Also, Azure Backup protects only the nodes that run in the same Azure region as the Recovery Services vault.

## Can I protect availability groups across regions?

The Azure Backup Recovery Services vault can detect and protect all nodes that are in the same region as the vault. If your SQL Server Always On availability group spans multiple Azure regions, set up the backup from the region that has the primary node. Azure Backup can detect and protect all databases in the availability group according to your backup preference. When your backup preference isn't met, backups fail and you get the failure alert.

## Do successful backup jobs create alerts?

No. Successful backup jobs don't generate alerts. Alerts are sent only for backup jobs that fail. Detailed behavior for portal alerts is documented [here](#). However, in case you are interested do have alerts even for successful jobs, you can use [Monitoring using Azure Monitor](#).

## Can I see scheduled backup jobs in the Backup Jobs menu?

The **Backup Job** menu will only show on-demand backup jobs. For scheduled job use [Monitoring using Azure Monitor](#).

## Are future databases automatically added for backup?

Yes, you can achieve this capability with [auto-protection](#).

## If I delete a database from an autoprotected instance, what will happen to the backups?

If a database is dropped from an autoprotected instance, the database backups are still attempted. This implies that the deleted database begins to show up as unhealthy under **Backup Items** and is still protected.

The correct way to stop protecting this database is to do **Stop Backup** with **delete data** on this database.

## If I do stop backup operation of an autoprotected database what will be its behavior?

If you do **stop backup with retain data**, no future backups will take place and the existing recovery points will remain intact. The database will still be considered as protected and be shown under the **Backup items**.

If you do **stop backup with delete data**, no future backups will take place and the existing recovery points will also be deleted. The database will be considered un-protected and be shown under the instance in the Configure Backup. However, unlike other up-protected databases that can be selected manually or that can get autoprotected, this database appears greyed out and can't be selected. The only way to re-protect this database is to disable auto-protection on the instance. You can now select this database and configure protection on it or re-enable auto-protection on the instance again.

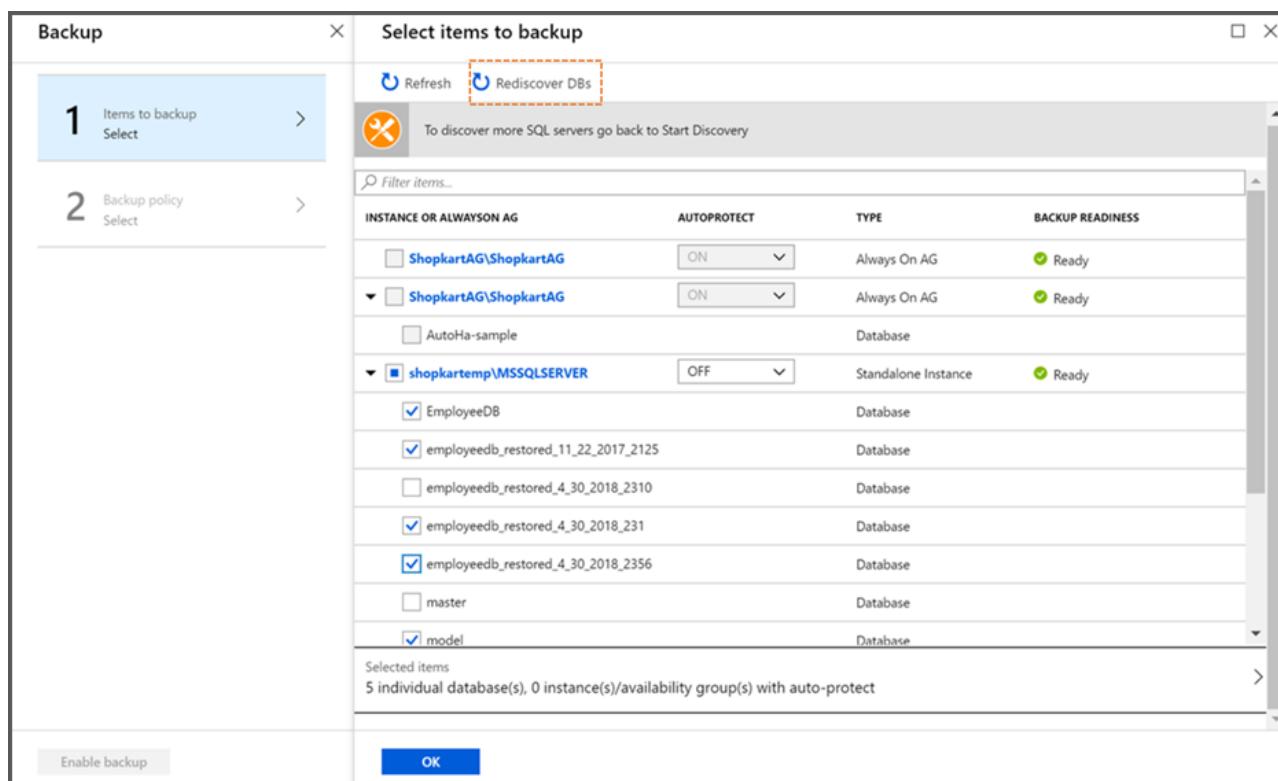
## If I change the name of the database after it has been protected, what will be the behavior?

A renamed database is treated as a new database. Hence, the service will treat this situation as if the database were not found and will fail the backups.

You can select the database, which is now renamed and configure protection on it. In case the auto-protection is enabled on the instance, the renamed database will be automatically detected and protected.

## Why can't I see an added database for an autoprotected instance?

A database that you [add to an autoprotected instance](#) might not immediately appear under protected items. This is because the discovery typically runs every 8 hours. However, you can discover and protect new databases immediately if you manually run a discovery by selecting **Rediscover DBs**, as shown in the following image:



## Next steps

Learn how to [back up a SQL Server database](#) that's running on an Azure VM.

# Frequently asked questions – Back up SAP HANA databases on Azure VMs

2/27/2020 • 2 minutes to read • [Edit Online](#)

This article answers common questions about backing up SAP HANA databases using the Azure Backup service.

## Backup

### **How many full backups are supported per day?**

We support only one full backup per day. You cannot have differential backup and full backup triggered on the same day.

### **Do successful backup jobs create alerts?**

No. Successful backup jobs don't generate alerts. Alerts are sent only for backup jobs that fail. Detailed behavior for portal alerts is documented [here](#). However, if you are interested having alerts even for successful jobs, you can use [Azure Monitor](#).

### **Can I see scheduled backup jobs in the Backup Jobs menu?**

The Backup Job menu will only show ad-hoc backup jobs. For scheduled jobs, use [Azure Monitor](#).

### **Are future databases automatically added for backup?**

No, this is not currently supported.

### **If I delete a database from an instance, what will happen to the backups?**

If a database is dropped from an SAP HANA instance, the database backups are still attempted. This implies that the deleted database begins to show up as unhealthy under **Backup Items** and is still protected. The correct way to stop protecting this database is to perform **Stop Backup with delete data** on this database.

### **If I change the name of the database after it has been protected, what will the behavior be?**

A renamed database is treated as a new database. Therefore, the service will treat this situation as if the database were not found and with fail the backups. The renamed database will appear as a new database and must be configured for protection.

### **What are the prerequisites to back up SAP HANA databases on an Azure VM?**

Refer to the [prerequisites](#) and [What the pre-registration script does](#) sections.

### **What permissions should be set for Azure to be able to back up SAP HANA databases?**

Running the pre-registration script sets the required permissions to allow Azure to back up SAP HANA databases. You can find more what the pre-registration script does [here](#).

### **Will backups work after migrating SAP HANA from 1.0 to 2.0?**

Refer to [this section](#) of the troubleshooting guide.

## Restore

### **Why can't I see the HANA system I want my database to be restored to?**

Check if all the prerequisites for the restore to target SAP HANA instance are met. For more information, see [Prerequisites - Restore SAP HANA databases in Azure VM](#).

### **Why is the Overwrite DB restore failing for my database?**

Ensure that the **Force Overwrite** option is selected while restoring.

### Why do I see the “Source and target systems for restore are incompatible” error?

Refer to the SAP HANA Note [1642148](#) to see what restore types are currently supported.

## Next steps

Learn how to [back up SAP HANA databases](#) running on Azure VMs.

# Azure Backup Server and DPM - FAQ

11/18/2019 • 2 minutes to read • [Edit Online](#)

## General questions

This article answers frequently asked questions about the Azure Backup Server and DPM.

### **Can I use Azure Backup Server to create a Bare Metal Recovery (BMR) backup for a physical server?**

Yes.

### **Can I register the server to multiple vaults?**

No. A DPM or Azure Backup server can be registered to only one vault.

### **Can I use DPM to back up apps in Azure Stack?**

No. You can use Azure Backup to protect Azure Stack, Azure Backup doesn't support using DPM to back up apps in Azure Stack.

### **If I've installed Azure Backup agent to protect my files and folders, can I install System Center DPM to back up on-premises workloads to Azure?**

Yes. But you should set up DPM first, and then install the Azure Backup agent. Installing components in this order ensures that the Azure Backup agent works with DPM. Installing the agent before installing DPM isn't advised or supported.

### **Why can't I add an external DPM server after installing UR7 and latest Azure Backup agent?**

For the DPM servers with data sources that are protected to the cloud (by using an update rollup earlier than Update Rollup 7), you must wait at least one day after installing the UR7 and latest Azure Backup agent, to start

**Add External DPM server.** The one-day time period is needed to upload the metadata of the DPM protection groups to Azure. Protection group metadata is uploaded the first time through a nightly job.

## VMware and Hyper-V backup

### **Can I back up VMware vCenter servers to Azure?**

Yes. You can use Azure Backup Server to back up VMware vCenter Server and ESXi hosts to Azure.

- [Learn more](#) about supported versions.
- [Follow these steps](#) to back up a VMware server.

### **Do I need a separate license to recover a full on-premises VMware/Hyper-V cluster?**

You don't need separate licensing for VMware/Hyper-V protection.

- If you're a System Center customer, use System Center Data Protection Manager (DPM) to protect VMware VMs.
- If you aren't a System Center customer, you can use Azure Backup Server (pay-as-you-go) to protect VMware VMs.

## SharePoint

### **Can I recover a SharePoint item to the original location if SharePoint is configured by using SQL AlwaysOn (with protection on disk)?**

Yes, the item can be recovered to the original SharePoint site.

## **Can I recover a SharePoint database to the original location if SharePoint is configured by using SQL AlwaysOn?**

Because SharePoint databases are configured in SQL AlwaysOn, they cannot be modified unless the availability group is removed. As a result, DPM cannot restore a database to the original location. You can recover a SQL Server database to another SQL Server instance.

## **Next steps**

Read the other FAQs:

- [Learn more](#) about Azure Backup Server and DPM support matrix.
- [Learn more](#) about the Azure Backup Server and DPM troubleshooting guidelines.

# Azure Backup Monitoring Alert - FAQ

2/4/2020 • 3 minutes to read • [Edit Online](#)

This article answers common questions about Azure Backup monitoring and reporting.

## Configure Azure Backup reports

### How do I check if reporting data has started flowing into a Log Analytics (LA) Workspace?

Navigate to the LA Workspace you have configured, navigate to the **Logs** menu item, and run the query `CoreAzureBackup | take 1`. If you see a record being returned, it means data has started flowing into the workspace. The initial data push may take up to 24 hours.

### What is the frequency of data push to an LA Workspace?

The diagnostic data from the vault is pumped to the Log Analytics workspace with some lag. Every event arrives at the Log Analytics workspace 20 to 30 minutes after it's pushed from the Recovery Services vault. Here are further details about the lag:

- Across all solutions, the backup service's built-in alerts are pushed as soon as they're created. So they usually appear in the Log Analytics workspace after 20 to 30 minutes.
- Across all solutions, on-demand backup jobs and restore jobs are pushed as soon as they finish.
- For all solutions except SQL backup, scheduled backup jobs are pushed as soon as they finish.
- For SQL backup, because log backups can occur every 15 minutes, information for all the completed scheduled backup jobs, including logs, is batched and pushed every 6 hours.
- Across all solutions, other information such as the backup item, policy, recovery points, storage, and so on, is pushed at least once per day.
- A change in the backup configuration (such as changing policy or editing policy) triggers a push of all related backup information.

### How long can I retain reporting data?

After you create an LA Workspace, you can choose to retain data for a maximum of 2 years. By default, an LA Workspace retains data for 31 days.

### Will I see all my data in reports after I configure the LA Workspace?

All the data generated after you configure diagnostics settings is pushed to the LA Workspace and is available in reports. In-progress jobs aren't pushed for reporting. After the job finishes or fails, it is sent to reports.

### Can I view reports across vaults and subscriptions?

Yes, you can view reports across vaults and subscriptions as well as regions. Your data may reside in a single LA Workspace or a group of LA Workspaces.

### Can I view reports across tenants?

If you are an [Azure Lighthouse](#) user with delegated access to your customers' subscriptions or LA Workspaces, you can use Backup Reports to view data across all your tenants.

### How long does it take for the Azure backup agent job status to reflect in the portal?

The Azure portal can take up to 15 mins to reflect the Azure backup agent job status.

### When a backup job fails, how long does it take to raise an alert?

An alert is raised within 20 mins of the Azure backup failure.

### **Is there a case where an email won't be sent if notifications are configured?**

Yes. In the following situations, notifications are not sent.

- If notifications are configured hourly, and an alert is raised and resolved within the hour
- When a job is canceled
- If a second backup job fails because the original backup job is in progress

## Recovery Services Vault

### **How long does it take for the Azure backup agent job status to reflect in the portal?**

The Azure portal can take up to 15 mins to reflect the Azure backup agent job status.

### **When a backup job fails, how long does it take to raise an alert?**

An alert is raised within 20 mins of the Azure backup failure.

### **Is there a case where an email won't be sent if notifications are configured?**

Yes. In the following situations, notifications are not sent:

- If notifications are configured hourly, and an alert is raised and resolved within the hour
- When a job is canceled
- If a second backup job fails because the original backup job is in progress

## Next steps

Read the other FAQs:

- [Common questions](#) about Azure VM backups.
- [Common questions](#) about the Azure Backup agent

# Azure Backup architecture and components

2/24/2020 • 12 minutes to read • [Edit Online](#)

You can use the [Azure Backup service](#) to back up data to the Microsoft Azure cloud platform. This article summarizes Azure Backup architecture, components, and processes.

## What does Azure Backup do?

Azure Backup backs up the data, machine state, and workloads running on on-premises machines and Azure virtual machine (VM) instances. There are a number of Azure Backup scenarios.

## How does Azure Backup work?

You can back up machines and data by using a number of methods:

- **Back up on-premises machines:**

- You can back up on-premises Windows machines directly to Azure by using the Azure Backup Microsoft Azure Recovery Services (MARS) agent. Linux machines aren't supported.
- You can back up on-premises machines to a backup server - either System Center Data Protection Manager (DPM) or Microsoft Azure Backup Server (MABS). You can then back up the backup server to a Recovery Services vault in Azure.

- **Back up Azure VMs:**

- You can back up Azure VMs directly. Azure Backup installs a backup extension to the Azure VM agent that's running on the VM. This extension backs up the entire VM.
- You can back up specific files and folders on the Azure VM by running the MARS agent.
- You can back up Azure VMs to the MABS that's running in Azure, and you can then back up the MABS to a Recovery Services vault.

Learn more about [what you can back up](#) and about [supported backup scenarios](#).

## Where is data backed up?

Azure Backup stores backed-up data in a Recovery Services vault. A vault is an online-storage entity in Azure that's used to hold data, such as backup copies, recovery points, and backup policies.

Recovery Services vaults have the following features:

- Vaults make it easy to organize your backup data, while minimizing management overhead.
- In each Azure subscription, you can create up to 500 vaults.
- You can monitor backed-up items in a vault, including Azure VMs and on-premises machines.
- You can manage vault access with Azure [role-based access control \(RBAC\)](#).
- You specify how data in the vault is replicated for redundancy:
  - **Locally redundant storage (LRS):** To protect against failure in a datacenter, you can use LRS. LRS replicates data to a storage scale unit. [Learn more](#).
  - **Geo-redundant storage (GRS):** To protect against region-wide outages, you can use GRS. GRS replicates your data to a secondary region. [Learn more](#).
  - By default, Recovery Services vaults use GRS.

# Backup agents

Azure Backup provides different backup agents, depending on what type of machine is being backed up:

| AGENT                     | DETAILS                                                                                                                                                                                                                                                                                                                  |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>MARS agent</b>         | <ul style="list-style-type: none"><li>Runs on individual on-premises Windows Server machines to back up files, folders, and the system state.</li><li>Runs on Azure VMs to back up files, folders, and the system state.</li><li>Runs on DPM/MABS servers to back up the DPM/MABS local storage disk to Azure.</li></ul> |
| <b>Azure VM extension</b> | Runs on Azure VMs to back them up to a vault.                                                                                                                                                                                                                                                                            |

## Backup types

The following table explains the different types of backups and when they're used:

| BACKUP TYPE         | DETAILS                                                                                                                                                                                                                                                                                            | USAGE                                                                                                |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| <b>Full</b>         | A full backup contains the entire data source. Takes more network bandwidth than differential or incremental backups.                                                                                                                                                                              | Used for initial backup.                                                                             |
| <b>Differential</b> | A differential backup stores the blocks that changed since the initial full backup. Uses a smaller amount of network and storage, and doesn't keep redundant copies of unchanged data.<br><br>Inefficient because data blocks that are unchanged between later backups are transferred and stored. | Not used by Azure Backup.                                                                            |
| <b>Incremental</b>  | An incremental backup stores only the blocks of data that changed since the previous backup. High storage and network efficiency.<br><br>With incremental backup, there's no need to supplement with full backups.                                                                                 | Used by DPM/MABS for disk backups, and used in all backups to Azure. Not used for SQL Server backup. |

## SQL Server backup types

The following table explains the different types of backups used for SQL Server databases and how often they're used:

| BACKUP TYPE | DETAILS | USAGE |
|-------------|---------|-------|
|-------------|---------|-------|

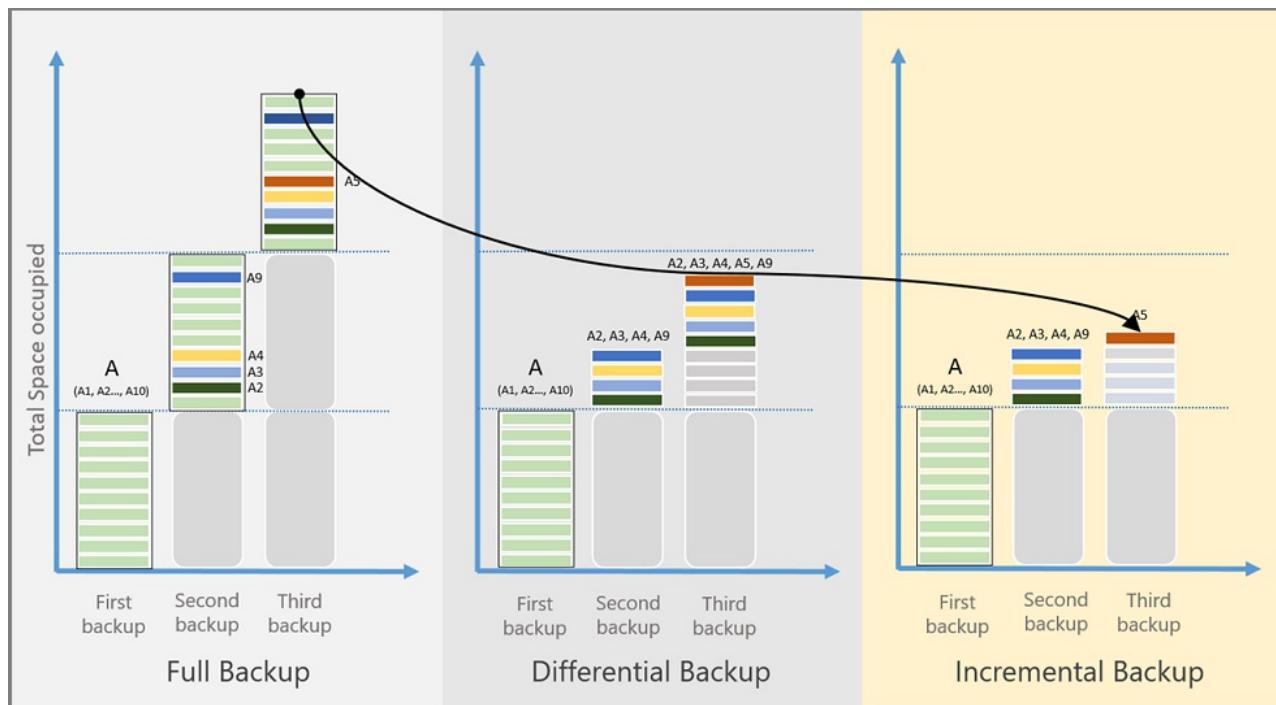
| Backup type                   | Details                                                                                                                                                                                                | Usage                                                                                                                                         |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Full backup</b>            | A full database backup backs up the entire database. It contains all the data in a specific database or in a set of filegroups or files. A full backup also contains enough logs to recover that data. | At most, you can trigger one full backup per day.<br><br>You can choose to make a full backup on a daily or weekly interval.                  |
| <b>Differential backup</b>    | A differential backup is based on the most recent, previous full-data backup.<br><br>It captures only the data that's changed since the full backup.                                                   | At most, you can trigger one differential backup per day.<br><br>You can't configure a full backup and a differential backup on the same day. |
| <b>Transaction log backup</b> | A log backup enables point-in-time restoration up to a specific second.                                                                                                                                | At most, you can configure transactional log backups every 15 minutes.                                                                        |

### Comparison of backup types

Storage consumption, recovery time objective (RTO), and network consumption varies for each type of backup.

The following image shows a comparison of the backup types:

- 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.
- For differential backups, 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.
- For incremental backups, in the second month, blocks A2, A3, A4, and A9 are marked as changed and transferred. In the third month, only changed block A5 is marked and transferred.



## Backup features

The following table summarizes the supported features for the different types of backup:

| FEATURE                                 | DIRECT BACKUP OF FILES AND FOLDERS (USING MARS AGENT) | AZURE VM BACKUP                                                                                         | MACHINES OR APPS WITH DPM/MABS                      |
|-----------------------------------------|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| Back up to vault                        |                                                       |                                                                                                         |                                                     |
| Back up to DPM/MABS disk, then to Azure |                                                       |                                                                                                         |                                                     |
| Compress data sent for backup           |                                                       | No compression is used when transferring data. Storage is inflated slightly, but restoration is faster. |                                                     |
| Run incremental backup                  |                                                       |                                                                                                         |                                                     |
| Back up deduplicated disks              |                                                       |                                                                                                         | <br>For DPM/MABS servers deployed on-premises only. |

Key = Supported = Partially Supported <blank> = Not Supported

## Backup policy essentials

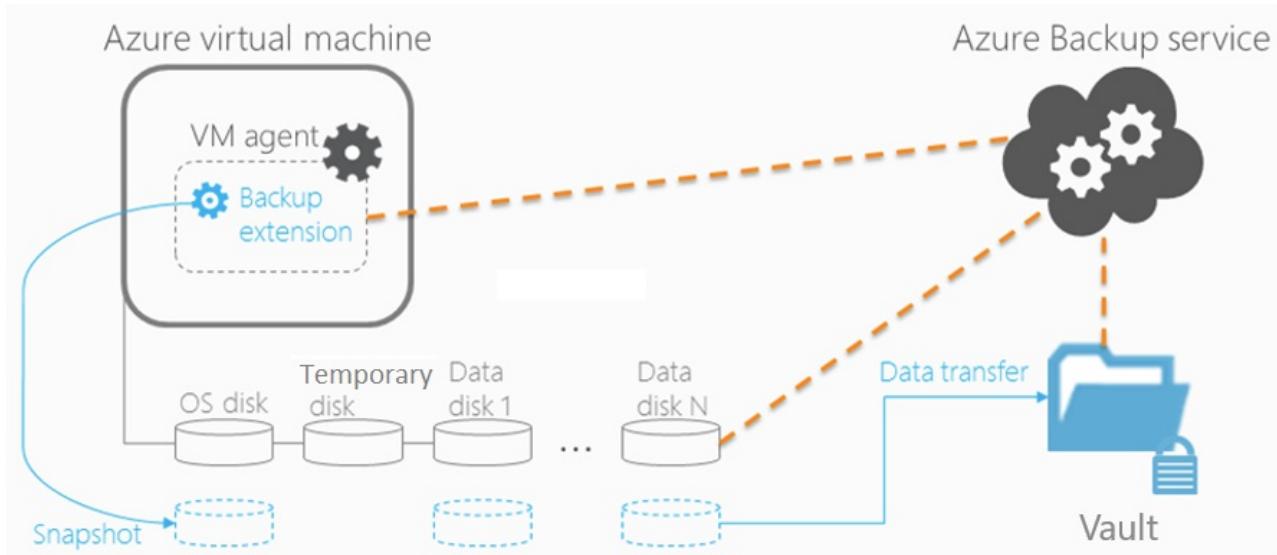
- A backup policy is created per vault.
- A backup policy can be created for the backup of following workloads
  - Azure VM
  - SQL in Azure VM
  - Azure File Share
- A policy can be assigned to many resources. An Azure VM backup policy can be used to protect many Azure VMs.
- A policy consists of two components
  - Schedule: When to take the backup
  - Retention: For how long each backup should be retained.
- Schedule can be defined as "daily" or "weekly" with a specific point of time.
- Retention can be defined for "daily", "weekly", "monthly", "yearly" backup points.
- "weekly" refers to a backup on a certain day of the week, "monthly" means a backup on a certain day of the month and "yearly" refers to a backup on a certain day of the year.
- Retention for "monthly", "yearly" backup points is referred to as "LongTermRetention".
- When a vault is created, a policy for Azure VM backups called "DefaultPolicy" is also created and can be used to back up Azure VMs.

## Architecture: Built-in Azure VM Backup

1. When you enable backup for an Azure VM, a backup runs according to the schedule you specify.
2. During the first backup, a backup extension is installed on the VM if the VM is running.
  - For Windows VMs, the VMSnapshot extension is installed.
  - For Linux VMs, the VMSnapshot Linux extension is installed.
3. The extension takes a storage-level snapshot.

- For Windows VMs that are running, Backup coordinates with the Windows Volume Shadow Copy Service (VSS) to take an app-consistent snapshot of the VM. By default, Backup takes full VSS backups. If Backup is unable to take an app-consistent snapshot, then it takes a file-consistent snapshot.
  - For Linux VMs, Backup takes a file-consistent snapshot. For app-consistent snapshots, you need to manually customize pre/post scripts.
  - Backup is optimized by backing up each VM disk in parallel. For each disk being backed up, Azure Backup reads the blocks on disk and stores only the changed data.
4. After the snapshot is taken, the data is transferred to the vault.
- Only blocks of data that changed since the last backup are copied.
  - Data isn't encrypted. Azure Backup can back up Azure VMs that were encrypted by using Azure Disk Encryption.
  - Snapshot data might not be immediately copied to the vault. At peak times, the backup might take some hours. Total backup time for a VM will be less than 24 hours for daily backup policies.
5. After the data is sent to the vault, a recovery point is created. By default, snapshots are retained for two days before they are deleted. This feature allows restore operation from these snapshots, thereby cutting down the restore times. It reduces the time that's required to transform and copy data back from the vault. See [Azure Backup Instant Restore Capability](#).

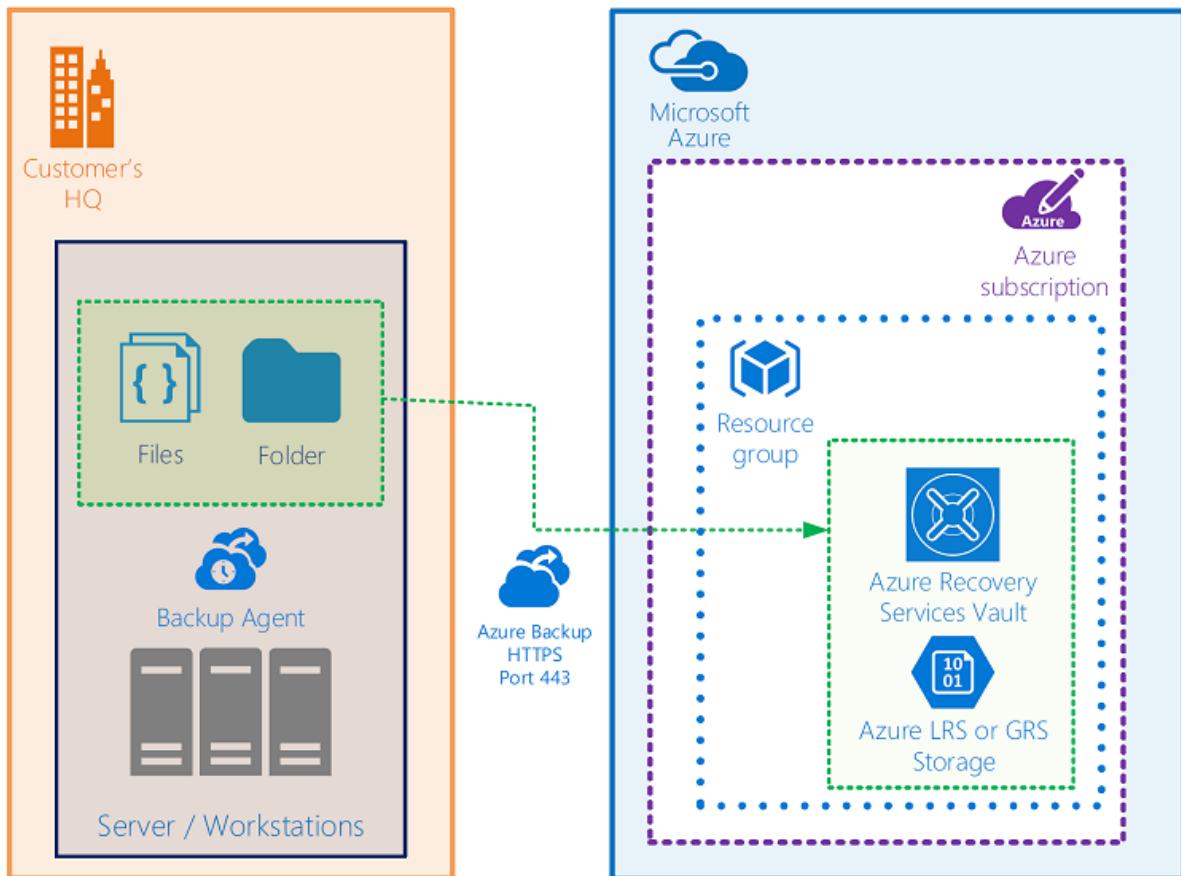
You do not need to explicitly allow internet connectivity to back up your Azure VMs.



## Architecture: Direct backup of on-premises Windows Server machines or Azure VM files or folders

1. To set up the scenario, you download and install the MARS agent on the machine. You then select what to back up, when backups will run, and how long they'll be kept in Azure.
2. The initial backup runs according to your backup settings.
3. The MARS agent uses VSS to take a point-in-time snapshot of the volumes selected for backup.
  - The MARS agent uses only the Windows system write operation to capture the snapshot.
  - Because the agent doesn't use any application VSS writers, it doesn't capture app-consistent snapshots.
4. After taking the snapshot with VSS, the MARS agent creates a virtual hard disk (VHD) in the cache folder you specified when you configured the backup. The agent also stores checksums for each data block.
5. Incremental backups run according to the schedule you specify, unless you run an on-demand backup.
6. In incremental backups, changed files are identified and a new VHD is created. The VHD is compressed and encrypted, and then it's sent to the vault.
7. After the incremental backup finishes, the new VHD is merged with the VHD created after the initial replication. This merged VHD provides the latest state to be used for comparison for ongoing backup.

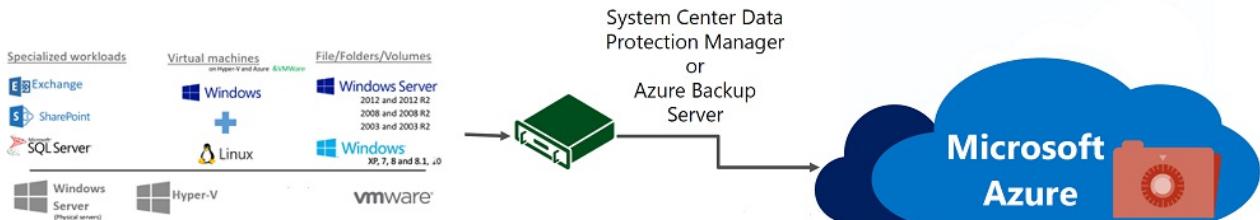
#### Azure Backup: Back up on-premises Windows files/folders to Azure



## Architecture: Back up to DPM/MABS

1. You install the DPM or MABS protection agent on machines you want to protect. You then add the machines to a DPM protection group.
  - To protect on-premises machines, the DPM or MABS server must be located on-premises.
  - To protect Azure VMs, the MABS server must be located in Azure, running as an Azure VM.
  - With DPM/MABS, you can protect backup volumes, shares, files, and folders. You can also protect a machine's system state (bare metal), and you can protect specific apps with app-aware backup settings.
2. When you set up protection for a machine or app in DPM/MABS, you select to back up to the MABS/DPM local disk for short-term storage and to Azure for online protection. You also specify when the backup to local DPM/MABS storage should run and when the online backup to Azure should run.
3. The disk of the protected workload is backed up to the local MABS/DPM disks, according to the schedule you specified.
4. The DPM/MABS disks are backed up to the vault by the MARS agent that's running on the DPM/MABS server.

#### Azure Backup: Back up workloads (on-premises and on Azure VMs) protected by DPM or Microsoft Azure Backup Server (MABS)



## Azure VM storage

Azure VMs use disks to store their operating system, apps, and data. Each Azure VM has at least two disks: a disk for the operating system and a temporary disk. Azure VMs can also have data disks for app data. Disks are stored

as VHDS.

- VHDS are stored as page blobs in standard or premium storage accounts in Azure:
  - **Standard storage:** Reliable, low-cost disk support for VMs running workloads that aren't sensitive to latency. Standard storage can use standard solid-state drive (SSD) disks or standard hard disk drive (HDD) disks.
  - **Premium storage:** High-performance disk support. Uses premium SSD disks.
- There are different performance tiers for disks:
  - **Standard HDD disk:** Backed by HDDs, and used for cost-effective storage.
  - **Standard SSD disk:** Combines elements of premium SSD disks and standard HDD disks. Offers more consistent performance and reliability than HDD, but still cost-effective.
  - **Premium SSD disk:** Backed by SSDs, and provides high-performance and low-latency for VMs that are running I/O-intensive workloads.
- Disks can be managed or unmanaged:
  - **Unmanaged disks:** Traditional type of disks used by VMs. For these disks, you create your own storage account and specify it when you create the disk. You then need to figure out how to maximize storage resources for your VMs.
  - **Managed disks:** Azure creates and manages the storage accounts for you. You specify the disk size and performance tier, and Azure creates managed disks for you. As you add disks and scale VMs, Azure handles the storage accounts.

For more information about disk storage and the available disk types for VMs, see these articles:

- [Azure managed disks for Windows VMs](#)
- [Azure managed disks for Linux VMs](#)
- [Available disk types for VMs](#)

## Back up and restore Azure VMs with premium storage

You can back up Azure VMs by using premium storage with Azure Backup:

- During the process of backing up VMs with premium storage, the Backup service creates a temporary staging location, named *AzureBackup-*, in the storage account. The size of the staging location equals the size of the recovery point snapshot.
- Make sure that the premium storage account has adequate free space to accommodate the temporary staging location. For more information, see [Scalability targets for premium page blob storage accounts](#). Don't modify the staging location.
- After the backup job finishes, the staging location is deleted.
- The price of storage used for the staging location is consistent with [premium storage pricing](#).

When you restore Azure VMs by using premium storage, you can restore them to premium or standard storage. Typically, you would restore them to premium storage. But if you need only a subset of files from the VM, it might be cost effective to restore them to standard storage.

## Back up and restore managed disks

You can back up Azure VMs with managed disks:

- You back up VMs with managed disks in the same way that you do any other Azure VM. You can back up the VM directly from the virtual machine settings, or you can enable backup for VMs in the Recovery Services vault.
- You can back up VMs on managed disks through RestorePoint collections built on top of managed disks.
- Azure Backup also supports backing up VMs with managed disks that were encrypted by using Azure Disk Encryption.

When you restore VMs with managed disks, you can restore to a complete VM with managed disks or to a storage account:

- During the restore process, Azure handles the managed disks. If you're using the storage account option, you manage the storage account that's created during the restore process.
- If you restore a managed VM that's encrypted, make sure the VM's keys and secrets exist in the key vault before you start the restore process.

## Next steps

- Review the support matrix to [learn about supported features and limitations for backup scenarios](#).
- Set up backup for one of these scenarios:
  - [Back up Azure VMs](#).
  - [Back up Windows machines directly](#), without a backup server.
  - [Set up MABS](#) for backup to Azure, and then back up workloads to MABS.
  - [Set up DPM](#) for backup to Azure, and then back up workloads to DPM.

# Recovery Services vaults overview

11/18/2019 • 3 minutes to read • [Edit Online](#)

This article describes the features of a Recovery Services vault. A 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 (VMs), workloads, servers, or workstations. You can use Recovery Services vaults to hold backup data for various Azure services such as IaaS VMs (Linux or Windows) 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.

Within an Azure subscription, you can create up to 500 Recovery Services vaults per subscription per region.

## Comparing Recovery Services vaults and Backup vaults

If you still have Backup vaults, they are being auto-upgraded to Recovery Services vaults. By November 2017, all Backup vaults have been upgraded to Recovery Services vaults.

Recovery Services vaults are based on the Azure Resource Manager model of Azure, whereas Backup vaults were based on the Azure Service Manager model. When you upgrade a Backup vault to a Recovery Services vault, the backup data remains intact during and after the upgrade process. Recovery Services vaults provide features not available for Backup vaults, such as:

- **Enhanced capabilities to help secure backup data:** With Recovery Services vaults, Azure Backup provides security capabilities to protect cloud backups. The security features ensure you can secure your backups, and safely recover data, even if production and backup servers are compromised. [Learn more](#)
- **Central monitoring for your hybrid IT environment:** With Recovery Services vaults, you can monitor not only your [Azure IaaS VMs](#) but also your [on-premises assets](#) from a central portal. [Learn more](#)
- **Role-Based Access Control (RBAC):** RBAC provides fine-grained access management control in Azure. [Azure provides various built-in roles](#), and Azure Backup has three [built-in roles to manage recovery points](#). Recovery Services vaults are compatible with RBAC, which restricts backup and restore access to the defined set of user roles. [Learn more](#)
- **Protect all configurations of Azure Virtual Machines:** Recovery Services vaults protect Resource Manager-based VMs including Premium Disks, Managed Disks, and Encrypted VMs. Upgrading a Backup vault to a Recovery Services vault gives you the opportunity to upgrade your Service Manager-based VMs to Resource Manager-based VMs. While upgrading the vault, you can retain your Service Manager-based VM recovery points and configure protection for the upgraded (Resource Manager-enabled) VMs. [Learn more](#)
- **Instant restore for IaaS VMs:** Using Recovery Services vaults, you can restore files and folders from an IaaS VM without restoring the entire VM, which enables faster restore times. Instant restore for IaaS VMs is available for both Windows and Linux VMs. [Learn more](#)

## Managing your Recovery Services vaults in the portal

Creation and management of Recovery Services vaults in the Azure portal is easy because the Backup service integrates into other Azure services. This integration means you can create or manage a Recovery Services vault *in the context of the target service*. For example, to view the recovery points for a VM, select your VM, and click **Backup** in the Operations menu.

The screenshot shows the Azure portal interface for managing a virtual machine named ContosoVM. On the left, a sidebar lists various management options like Size, Security, Extensions, and Backup. The 'Backup' option is selected and highlighted with a red box. The main content area displays two charts: 'CPU (average)' and 'Network (total)'. The CPU chart shows usage from 0% to 100% over a 30-day period, with a value of 0.18% highlighted. The Network chart shows traffic in kB from 0B to 400B over the same period, with values for Network In (1.29 kB) and Network Out (360 kB) highlighted.

If the VM doesn't have backup configured, then it will prompt you to configure backup. If backup has been configured, you'll see backup information about the VM, including a list of restore points.

The screenshot shows the 'File Recovery' section for the ContosoVM virtual machine. It displays the following information:

- Alerts and Jobs**: Shows 'View all Alerts' (last 24 hours) and 'View all Jobs' (last 24 hours).
- Backup status**: Shows 'Backup Pre-Check' Passed, 'Last backup status' Success 8/10/2018, 8:38:54 AM, and 'Oldest restore point' 7/10/2018, 2:33:34 AM (1 month(s) ago).
- Summary**: Shows 'Recovery services vault' ContosoVM-demovault and 'Backup policy' DailyPolicy.
- Restore points (31)**: A table showing 31 restore points, categorized by consistency:
  - CRASH CONSISTENT**: 0
  - APPLICATION CONSISTENT**: 31
  - FILE-SYSTEM CONSISTENT**: 0
 The table lists the restore points with their creation times and consistency levels.

In the previous example, **ContosoVM** is the name of the virtual machine. **ContosoVM-demovault** is the name of the Recovery Services vault. You don't need to remember the name of the Recovery Services vault that stores the recovery points, you can access this information from the virtual machine.

If one Recovery Services vault protects multiple servers, it may be more logical to look at the Recovery Services vault. You can search for all Recovery Services vaults in the subscription, and choose one from the list.

The following sections contain links to articles that explain how to use a Recovery Services vault in each type of activity.

**NOTE**

Recovery Services vault cannot be created with the same name if it has been deleted within 24 hours. Use a different resource name or choose a different resource group or retry again after 24 hours.

**Back up data**

- [Back up an Azure VM](#)
- [Back up Windows Server or Windows workstation](#)
- [Back up DPM workloads to Azure](#)
- [Prepare to back up workloads using Azure Backup Server](#)

**Manage recovery points**

- [Manage Azure VM backups](#)
- [Managing files and folders](#)

**Restore data from the vault**

- [Recover individual files from an Azure VM](#)
- [Restore an Azure VM](#)

**Secure the vault**

- [Securing cloud backup data in Recovery Services vaults](#)

## Next steps

Use the following articles to:

- [Back up an IaaS VM](#)
- [Back up an Azure Backup Server](#)
- [Back up a Windows Server](#)

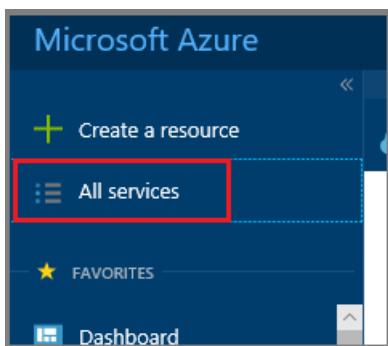
# Create a Recovery Services vault

2/28/2020 • 5 minutes to read • [Edit Online](#)

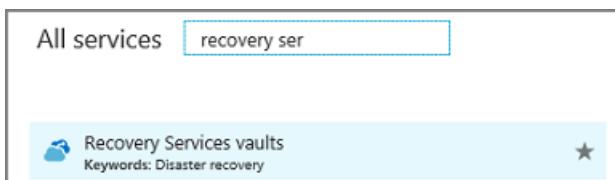
A Recovery Services vault is an entity that stores the backups and recovery points created over time. The Recovery Services vault also contains the backup policies that are associated with the protected virtual machines.

To create a Recovery Services vault:

1. Sign in to your subscription in the [Azure portal](#).
2. On the left menu, select **All services**.

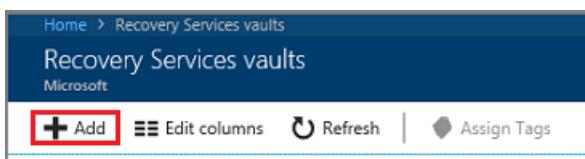


3. In the **All services** dialog box, enter **Recovery Services**. The list of resources filters according to your input. In the list of resources, select **Recovery Services vaults**.

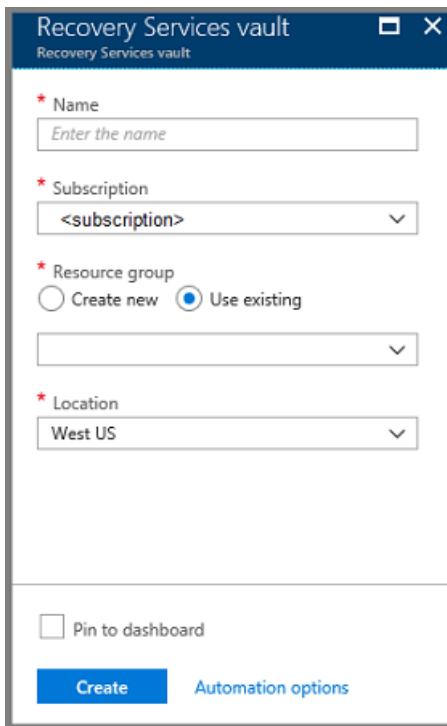


The list of Recovery Services vaults in the subscription appears.

4. On the **Recovery Services vaults** dashboard, select **Add**.



The **Recovery Services vault** dialog box opens. Provide values for the **Name**, **Subscription**, **Resource group**, and **Location**.

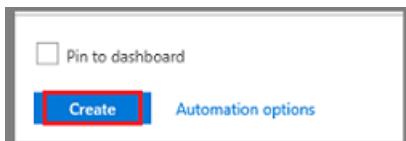


- **Name:** Enter a friendly name to identify the vault. The name must be unique to the Azure subscription. Specify a name that has at least two, but not more than 50 characters. The name must start with a letter and consist only of letters, numbers, and hyphens.
- **Subscription:** Choose the subscription to use. If you're a member of only one subscription, you'll see that name. If you're not sure which subscription to use, use the default (suggested) subscription. There are multiple choices only if your work or school account is associated with more than one Azure subscription.
- **Resource group:** Use an existing resource group or create a new one. To see the list of available resource groups in your subscription, select **Use existing**, and then select a resource from the drop-down list box. To create a new resource group, select **Create new** and enter the name. For complete information about resource groups, see [Azure Resource Manager overview](#).
- **Location:** Select the geographic region for the vault. To create a vault to protect virtual machines, the vault **must** be in the same region as the virtual machines.

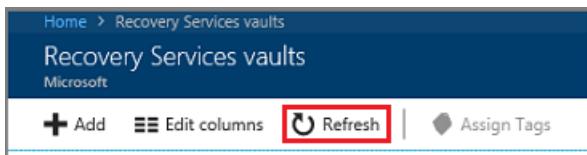
#### IMPORTANT

If you're not sure of the location of your VM, close the dialog box. Go to the list of virtual machines in the portal. If you have virtual machines in several regions, create a Recovery Services vault in each region. Create the vault in the first location, before you create the vault for another location. There's no need to specify storage accounts to store the backup data. The Recovery Services vault and the Azure Backup service handle that automatically.

5. When you're ready to create the Recovery Services vault, select **Create**.



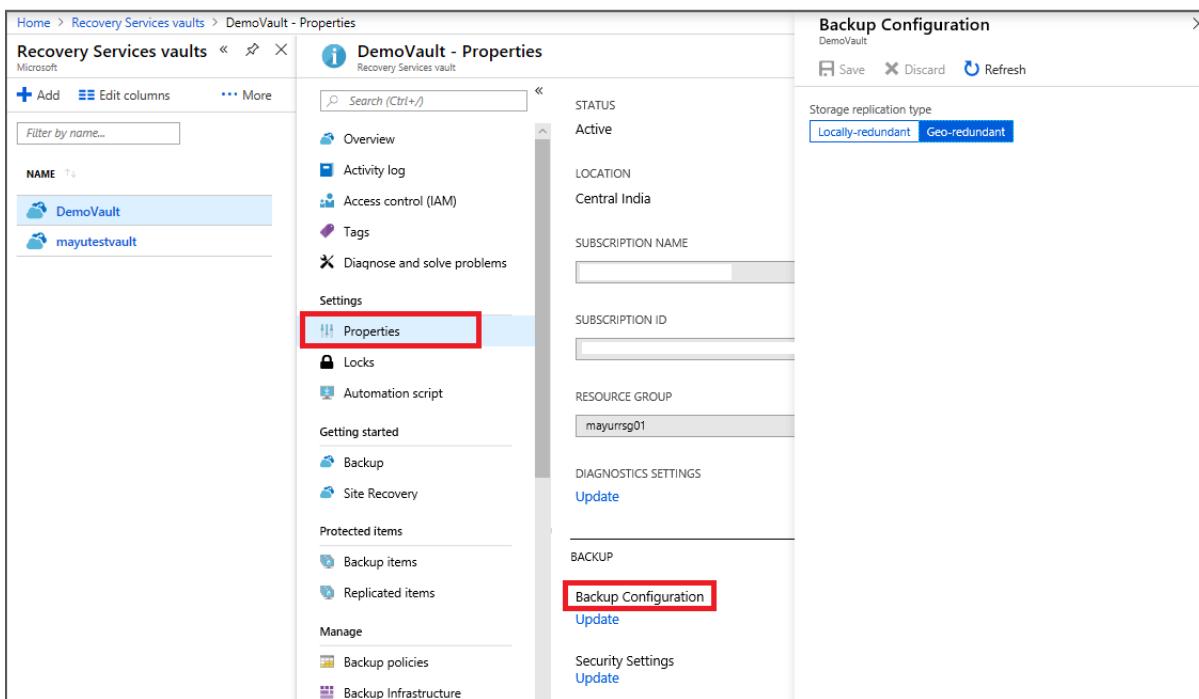
It can take a while to create the Recovery Services vault. Monitor the status notifications in the **Notifications** area at the upper-right corner of the portal. After your vault is created, it's visible in the list of Recovery Services vaults. If you don't see your vault, select **Refresh**.



## Set storage redundancy

Azure Backup automatically handles storage for the vault. You need to specify how that storage is replicated.

1. From the **Recovery Services vaults** blade, click the new vault. Under the **Settings** section, click **Properties**.
2. In **Properties**, under **Backup Configuration**, click **Update**.
3. Select the storage replication type, and click **Save**.



- We recommend that if you're using Azure as a primary backup storage endpoint, continue to use the default **Geo-redundant** setting.
- If you don't use Azure as a primary backup storage endpoint, then choose **Locally-redundant**, which reduces the Azure storage costs.
- Learn more about [geo](#) and [local](#) redundancy.

### NOTE

Changing **Storage Replication type** (Locally-redundant/ Geo-redundant) for a Recovery services vault has to be done before configuring backups in the vault. Once you configure backup, the option to modify is disabled and you cannot change the **Storage Replication type**.

## Set Cross Region Restore

As one of the restore options, Cross Region Restore (CRR) allows you to restore Azure VMs in a secondary region, which is an [Azure paired region](#). This option allows you to:

- conduct drills when there's an audit or compliance requirement
- restore the VM or its disk if there's a disaster in the primary region.

To choose this feature, select **Enable Cross Region Restore** from the **Backup Configuration** blade.

For this process, there are pricing implications as it is at the storage level.

#### NOTE

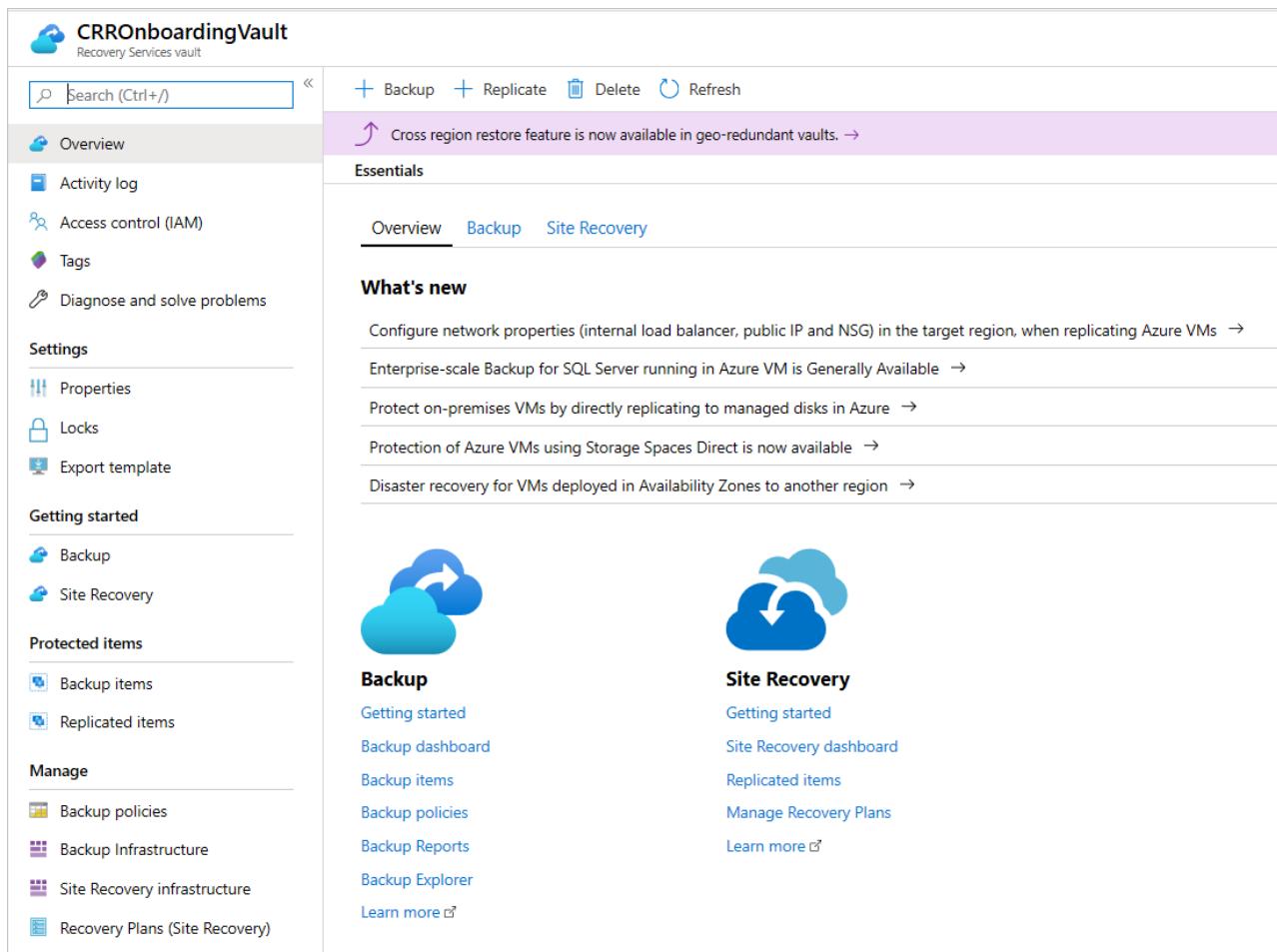
Before you begin:

- Review the [support matrix](#) for a list of supported managed types and regions.
- The Cross Region Restore (CRR) feature is currently only available in the following regions: West Central US, West US 2, Australia East, and Australia Southeast.
- CRR is a vault level opt-in feature for any GRS vault (turned off by default).
- Please use the following command to onboard your subscription for this feature:  

```
Register-AzProviderFeature -FeatureName CrossRegionRestore -ProviderNamespace Microsoft.RecoveryServices
```
- If you are onboarded to this feature during public limited preview, the review approval email will include pricing policy details.
- After opting-in, it might take up to 48 hours for the backup items to be available in secondary regions.
- Currently CRR is supported only for Backup Management Type - ARM Azure VM (classic Azure VM will not be supported). When additional management types support CRR, then they will be **automatically** enrolled.

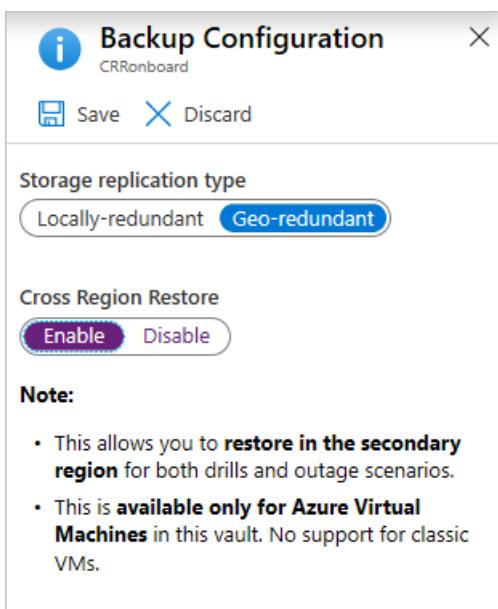
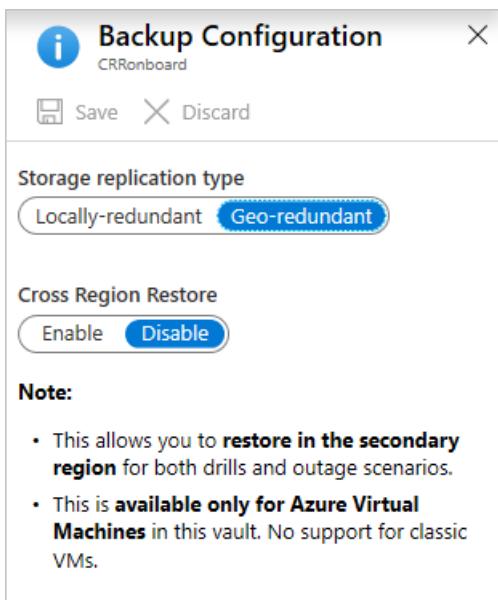
## Configure Cross Region Restore

A vault created with GRS redundancy includes the option to configure the Cross Region Restore feature. Every GRS vault will have a banner, which will link to the documentation. To configure CRR for the vault, go to the Backup Configuration blade, which contains the option to enable this feature.



The screenshot shows the Azure Recovery Services vault configuration blade for a vault named 'CRROnboardingVault'. The left sidebar lists various vault management options like Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. Under Settings, there are links for Properties, Locks, and Export template. The Getting started section includes links for Backup and Site Recovery. The Protected items section lists Backup items and Replicated items. The Manage section includes links for Backup policies, Backup Infrastructure, Site Recovery infrastructure, and Recovery Plans (Site Recovery). The main content area features a purple banner stating 'Cross region restore feature is now available in geo-redundant vaults.' Below the banner, the Essentials tab is selected, showing tabs for Overview, Backup, and Site Recovery. The Overview tab is active. The What's new section lists several recent updates related to network properties, enterprise-scale backup for SQL Server, protecting on-premises VMs, protection using Storage Spaces Direct, and disaster recovery for VMs in Availability Zones. At the bottom, there are two large icons: 'Backup' (blue cloud with a circular arrow) and 'Site Recovery' (blue cloud with a downward arrow). Each icon has a 'Getting started' link and a detailed list of sub-options under 'Backup' and 'Site Recovery' respectively.

1. From the portal, go to Recovery Services vault > Settings > Properties.
2. Click **Enable Cross Region Restore in this vault** to enable the functionality.



Learn how to [view backup items in the secondary region](#).

Learn how to [restore in the secondary region](#).

Learn how to [monitor secondary region restore jobs](#).

## Modifying default settings

We highly recommend you review the default settings for **Storage Replication type** and **Security settings** before configuring backups in the vault.

- **Storage Replication type** by default is set to **Geo-redundant**. Once you configure the backup, the option to modify is disabled. Follow these [steps](#) to review and modify the settings.
- **Soft delete** by default is **Enabled** on newly created vaults to protect backup data from accidental or malicious deletes. Follow these [steps](#) to review and modify the settings.

## Next steps

Learn about Recovery Services vaults. Learn about Delete Recovery Services vaults.

# Delete an Azure Backup Recovery Services vault

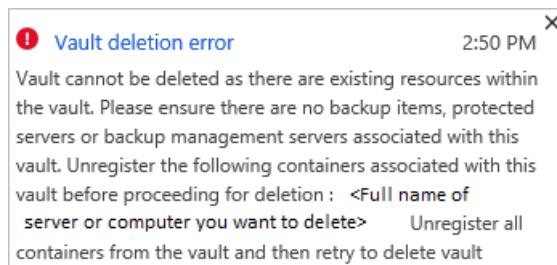
2/24/2020 • 10 minutes to read • [Edit Online](#)

This article describes how to delete a Microsoft [Azure Backup](#) Recovery Services (MARS) vault. It contains instructions for removing dependencies and then deleting a vault.

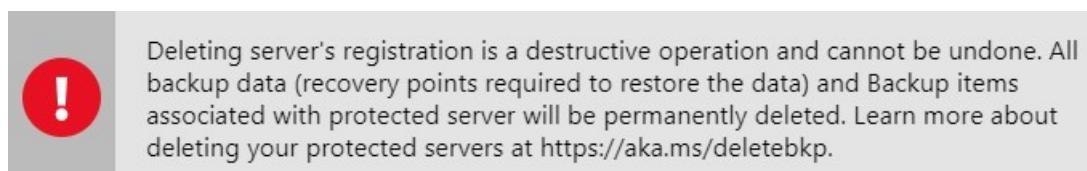
## Before you start

You can't delete a Recovery Services vault that has dependencies, such as protected servers or backup management servers, associated with it.

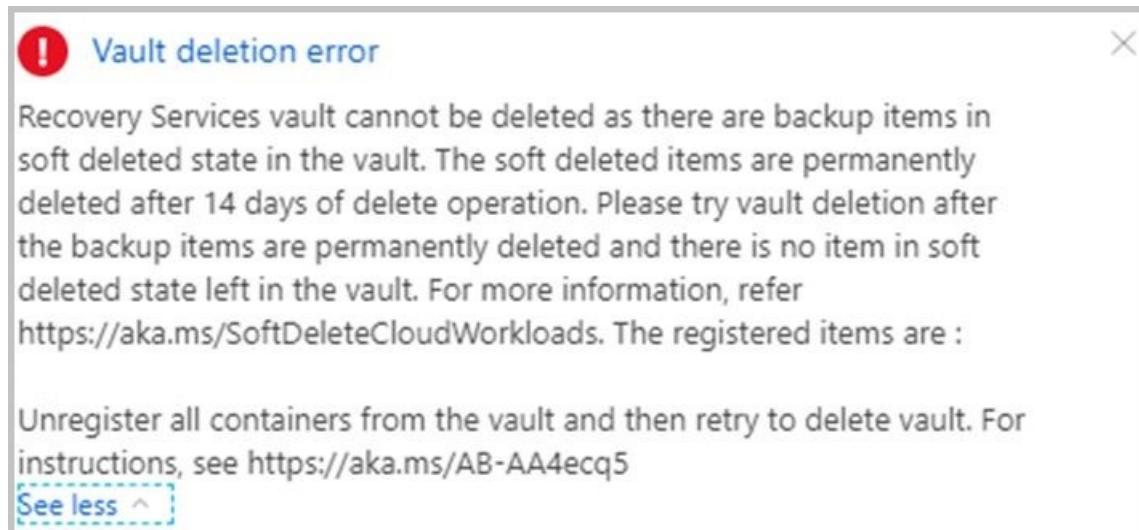
- Vaults that contain backup data can't be deleted (even if you've stopped protection but retained the backup data).
- If you delete a vault that contains dependencies, the following message appears:



- If you delete an on-premises protected item from a portal that contains dependencies, a warning message appears:



- If backup items are in soft deleted state below warning message appears and you will have to wait until they are permanently deleted. For more information, see this [article](#).



To delete the vault, choose the scenario that matches your setup and follow the recommended steps:

| SCENARIO                                                                                                                                             | STEPS TO REMOVE DEPENDENCIES TO DELETE VAULT                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| I have on-premises files and folders protected by using the Azure Backup agent, backing up to Azure                                                  | Perform the steps in <a href="#">Delete backup items from the MARS management console</a>                                                                                                                                                                                                   |
| I have on-premises machines that are protected by using MABS (Microsoft Azure Backup Server) or DPM (System Center Data Protection Manager) to Azure | Perform the steps in <a href="#">Delete backup items from the MABS management console</a>                                                                                                                                                                                                   |
| I have protected items in the cloud (for example, an IaaS virtual machine or an Azure Files share)                                                   | Perform the steps in <a href="#">Delete protected items in the cloud</a>                                                                                                                                                                                                                    |
| I have protected items both on premises and in the cloud                                                                                             | Perform the steps in all of the following sections, in the following order:<br>1. <a href="#">Delete protected items in the cloud</a><br>2. <a href="#">Delete backup items from the MARS management console</a><br>3. <a href="#">Delete backup items from the MABS Management console</a> |
| I don't have any protected items on-premises or cloud; however, I am still getting the Vault deletion error                                          | Perform the steps in <a href="#">Delete the Recovery Services vault by using Azure Resource Manager</a>                                                                                                                                                                                     |

## Delete protected items in the cloud

First, read the [Before you start](#) section to understand the dependencies and vault deletion process.

To stop protection and delete the backup data, perform the following steps:

- From the portal, go to **Recovery Services vault**, and then go to **Backup items**. Then, choose the protected items in the cloud (for example, Azure Virtual Machines, Azure Storage [the Azure Files service], or SQL Server on Azure Virtual Machines).

| BACKUP MANAGEMENT TYPE      | BACKUP ITEM COUNT |
|-----------------------------|-------------------|
| Azure Storage (Azure Files) | 7                 |
| SQL in Azure VM             | 4                 |
| Azure Backup Server         | 3                 |
| Azure Virtual Machine       | 2                 |
| Azure Backup Agent          | 1                 |
| SAP HANA in Azure VM        | 0                 |
| DPM                         | 0                 |

- Right-click to select the backup item. Depending on whether the backup item is protected or not, the menu displays either the **Stop Backup** pane or the **Delete Backup Data** pane.
  - If the **Stop Backup** pane appears, select **Delete Backup Data** from the drop-down menu. Enter the name of the backup item (this field is case-sensitive), and then select a reason from the drop-down

menu. Enter your comments, if you have any. Then, select **Stop backup**.

The screenshot shows the 'Backup Items (Azure Virtual Machine)' page. On the left, there's a list of backup items: 'ZonePinnedVM' and 'WonderSQLVM'. A context menu is open over 'ZonePinnedVM' with options: 'Pin to dashboard', 'Backup now', 'Restore VM', 'File Recovery', 'Stop backup' (which is highlighted with a red box), and 'Delete backup data'. On the right, a 'Stop Backup' dialog is displayed. It includes a note about stopping scheduled backup jobs and deleting backup data, a field to type the backup item name ('ZonePinnedVM'), a dropdown for reason ('0 selected'), a comments field, and an error message at the bottom: 'Please fix the errors on this page before continuing.' A 'Stop backup' button is at the bottom.

- If the **Delete Backup Data** pane appears, enter the name of the backup item (this field is case-sensitive), and then select a reason from the drop-down menu. Enter your comments, if you have any. Then, select **Delete**.

The screenshot shows the 'Backup Items (SQL in Azure VM)' page. On the left, there's a list of databases: 'msdb', 'master', 'laptoplist', and 'model'. A context menu is open over 'msdb' with options: 'Pin to dashboard', 'Backup now', 'Restore DB', 'Stop backup', and 'Delete backup data' (which is highlighted with a red box). On the right, a 'Delete Backup Data' dialog is displayed. It includes a note about stopping scheduled backup jobs and deleting backup data, a field to type the backup item name ('msdb'), a dropdown for reason ('0 selected'), a comments field, and an error message at the bottom: 'Please fix the errors on this page before continuing.' A 'Delete' button is at the bottom.

- Check the **Notification** icon: After the process finishes, the service displays the following message: *Stopping backup and deleting backup data for "Backup Item". Successfully completed the operation.*
- Select **Refresh** on the **Backup Items** menu, to make sure the backup item was deleted.

## Delete protected items on premises

First, read the **Before you start** section to understand the dependencies and vault deletion process.

1. From the vault dashboard menu, select **Backup Infrastructure**.
2. Depending on your on-premises scenario, choose the one of the following options:
  - For MARS, select **Protected Servers** and then **Azure Backup Agent**. Then, select the server that you want to delete.

- For MABS or DPM, select **Backup Management Servers**. Then, select the server that you want to delete.

3. The **Delete** pane appears with a warning message.

... > DPMV2ACCESSD3.DPMDOM02.SELFHOST.CORP.MICROSOFT.COM > Delete

## Delete

DPMV2ACCESSD3.DPMDOM02.SELFHOST.CORP.MICROSOFT.COM

**!** Deleting server's registration is a destructive operation and cannot be undone. All backup data (recovery points required to restore the data) and Backup items associated with protected server will be permanently deleted. Learn more about deleting your protected servers at <https://aka.ms/deletebckp>.

\* TYPE THE SERVER NAME

\* Reason  
0 selected

\* Comments

\* There is backup data of 3 backup items associated with this server. I understand that clicking "Confirm" will permanently delete all the cloud backup data. This action cannot be undone. An alert may be sent to the administrators of this subscription notifying them of this deletion.

View the list of backup items whose cloud backup data will be permanently deleted : [Click here](#)

**Delete** **Cancel**

Review the warning message and the instructions in the consent check box.

#### NOTE

- If the protected server is synced with Azure services and backup items exist, the consent check box will display the number of dependent backup items and the link to view the backup items.
- If the protected server is not synced with Azure services and backup items exist, the consent check box will display only the number of backup items.
- If there are no backup items, the consent check box will ask for deletion.

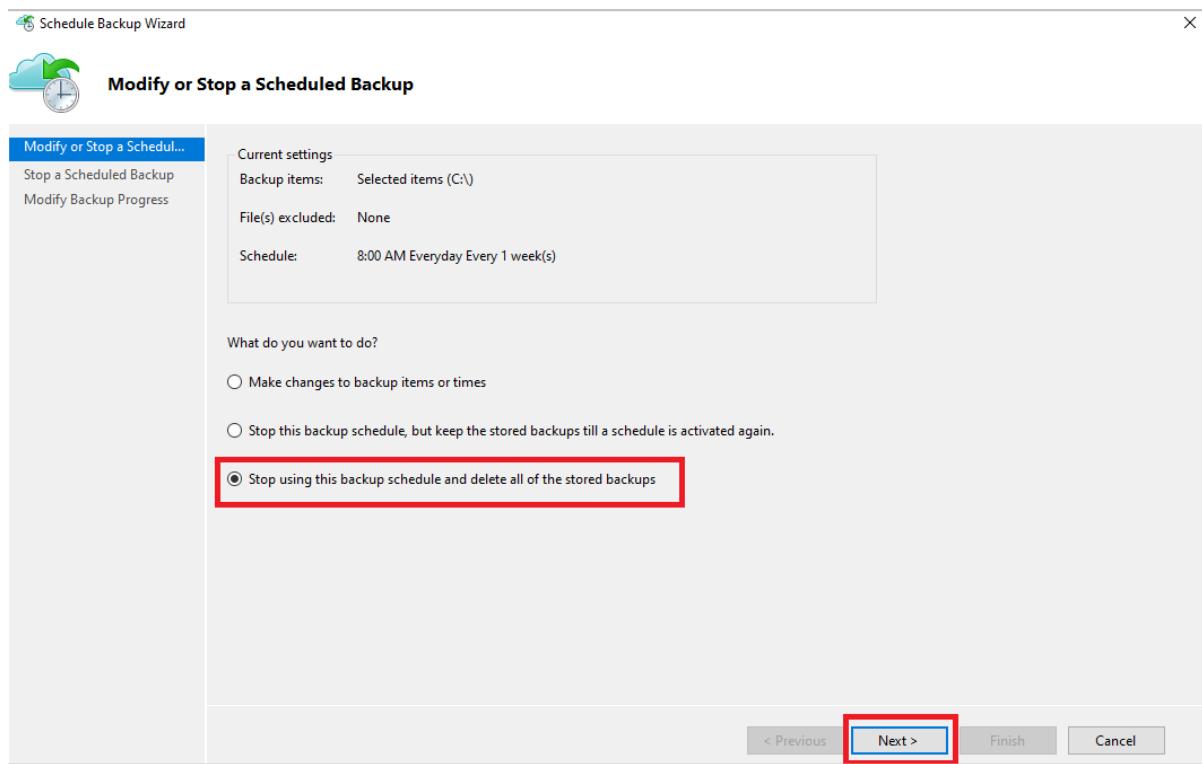
4. Select the consent check box, and then select **Delete**.
5. Check the **Notification** icon . After the operation finishes, the service displays the message: *Stopping backup and deleting backup data for "Backup Item." Successfully completed the operation.*
6. Select **Refresh** on the **Backup Items** menu, to make sure the backup item is deleted.

After this process finishes, you can delete the backup items from management console:

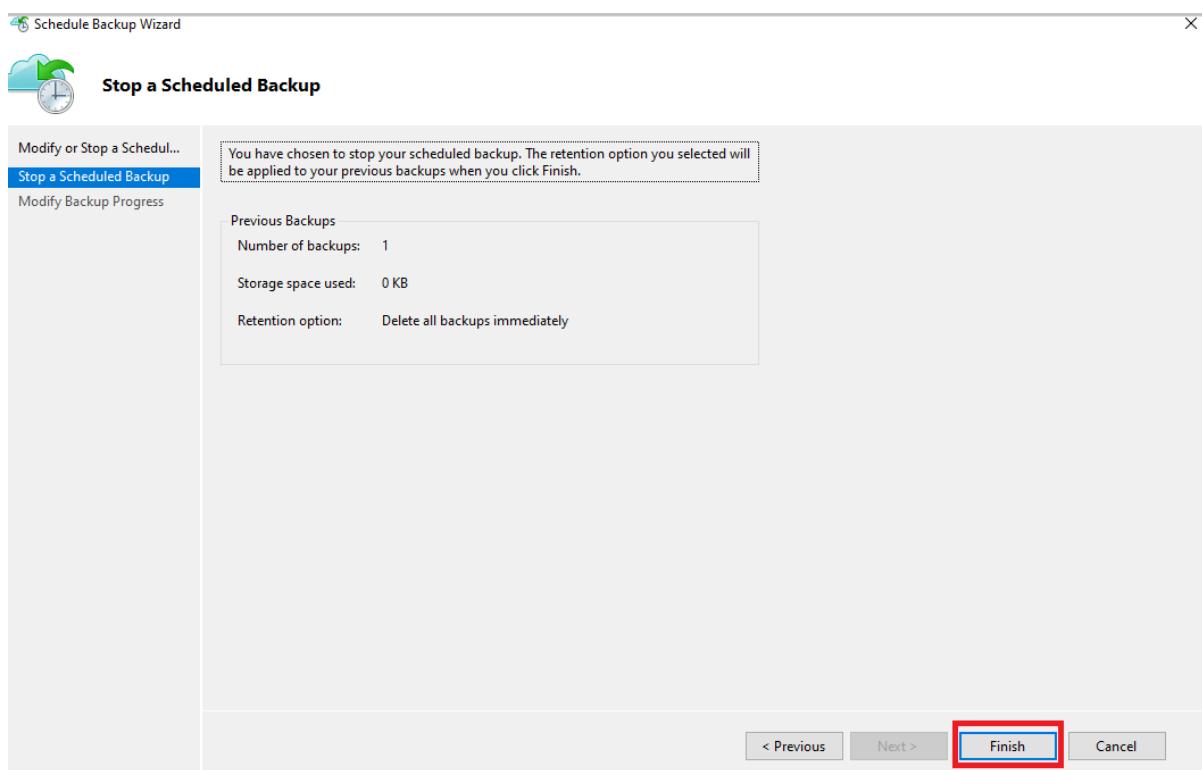
- [Delete backup items from the MARS management console](#)
- [Delete backup items from the MABS management console](#)

#### Delete backup items from the MARS management console

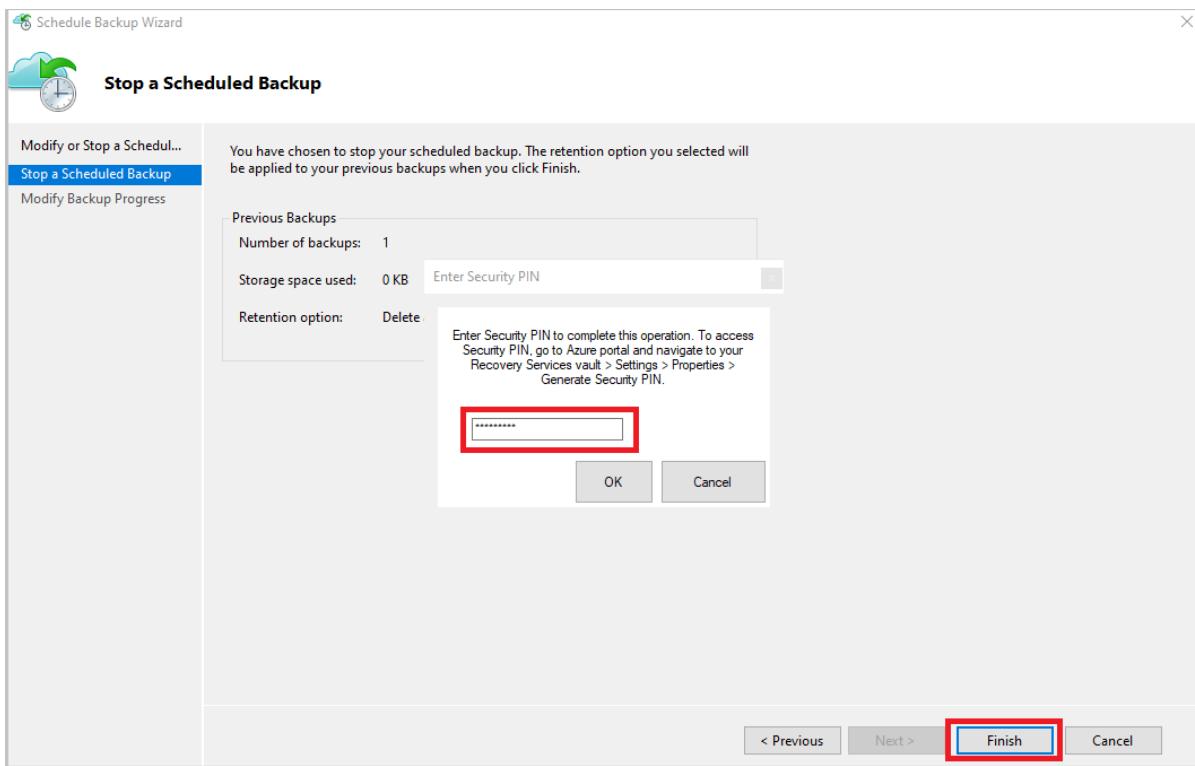
1. Open the MARS management console, go to the **Actions** pane, and select **Schedule Backup**.
2. From the **Modify or Stop a Scheduled Backup** page, select **Stop using this backup schedule and delete all the stored backups**. Then, select **Next**.



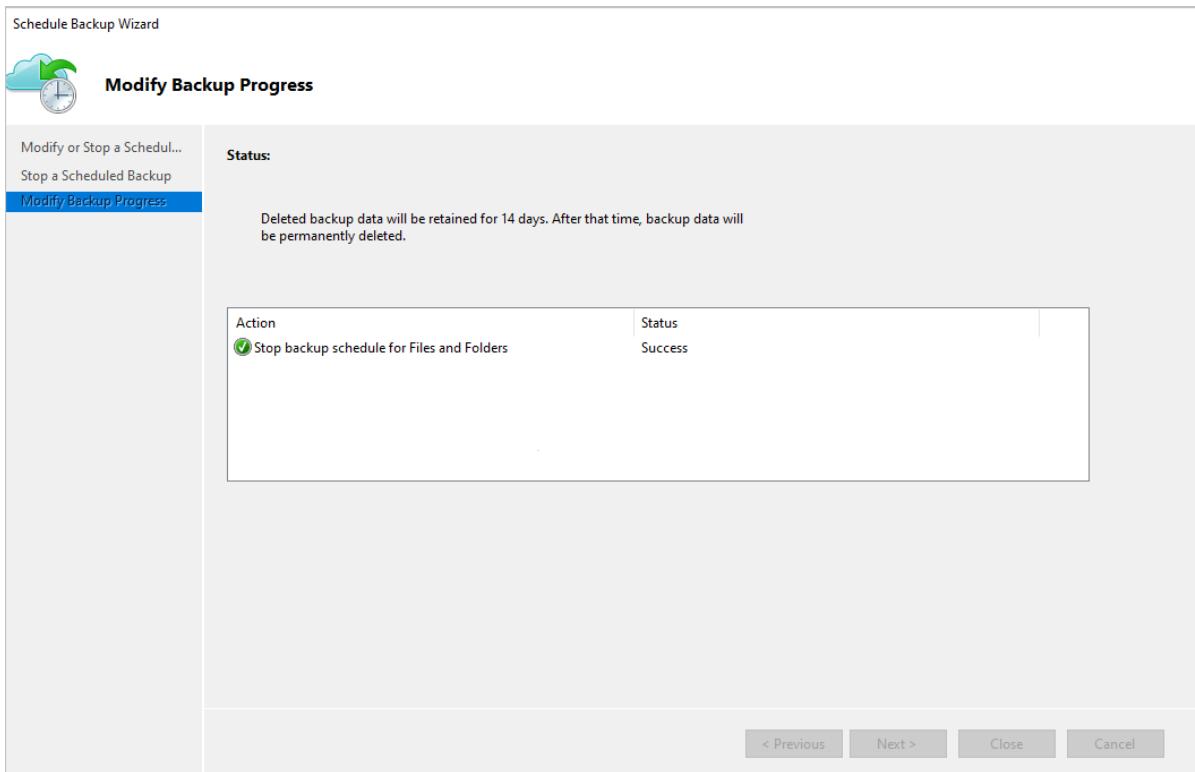
3. From the **Stop a Scheduled Backup** page, select **Finish**.



4. You are prompted to enter a security PIN (personal identification number), which you must generate manually. To do this, first sign in to the Azure portal.
5. Go to **Recovery Services vault** > **Settings** > **Properties**.
6. Under **Security PIN**, select **Generate**. Copy this PIN. The PIN is valid for only five minutes.
7. In the management console, paste the PIN, and then select **OK**.



8. In the **Modify Backup Progress** page, the following message appears: *Deleted backup data will be retained for 14 days. After that time, backup data will be permanently deleted.*



After you delete the on-premises backup items, follow the next steps from the portal.

### Delete backup items from the MABS management console

There are two methods you can use to delete backup items from the MABS management console.

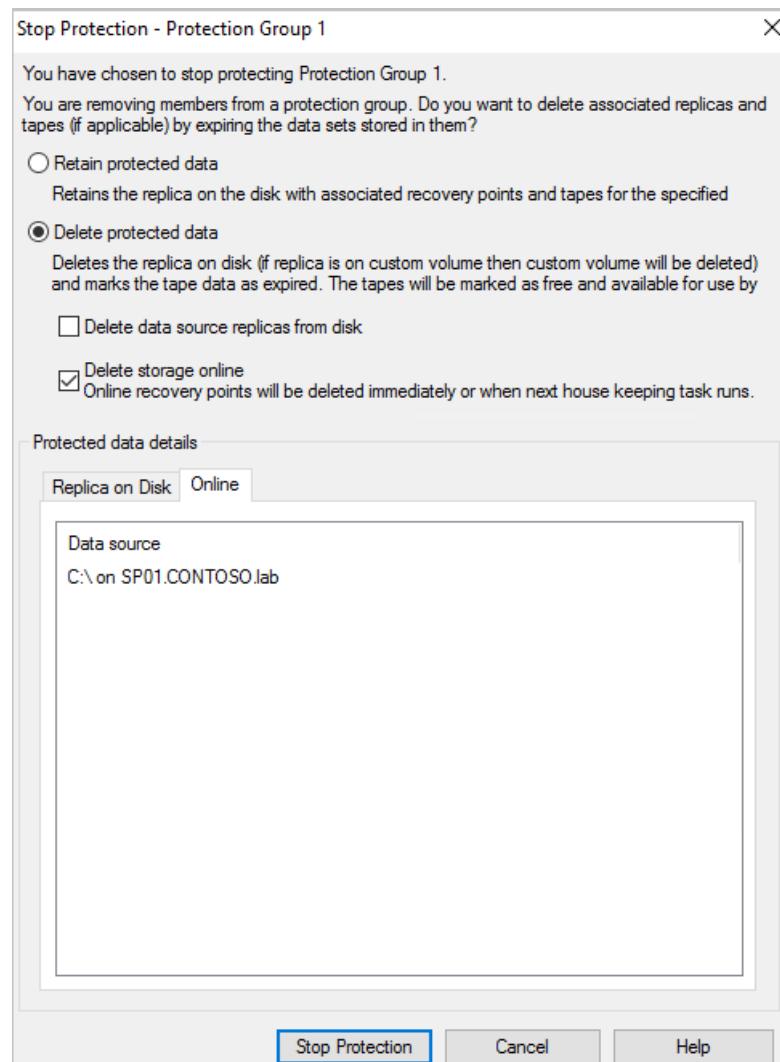
#### Method 1

To stop protection and delete backup data, do the following steps:

1. Open the DPM Administrator Console, and then select **Protection** on the navigation bar.
2. In the display pane, select the protection group member that you want to remove. Right-click to select the

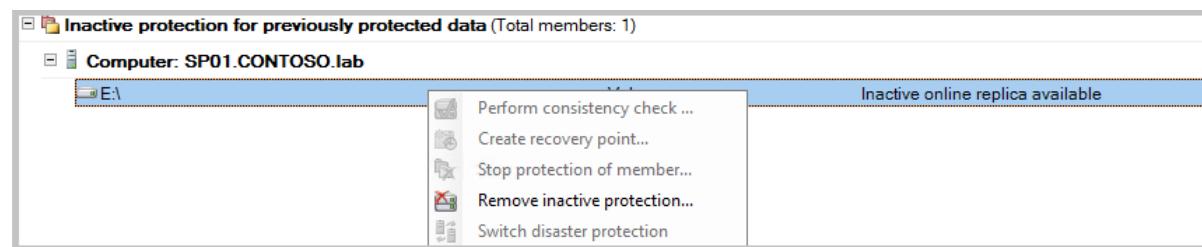
**Stop Protection of Group Members** option.

- From the **Stop Protection** dialog box, select **Delete protected data**, and then select the **Delete storage online** check box. Then, select **Stop Protection**.

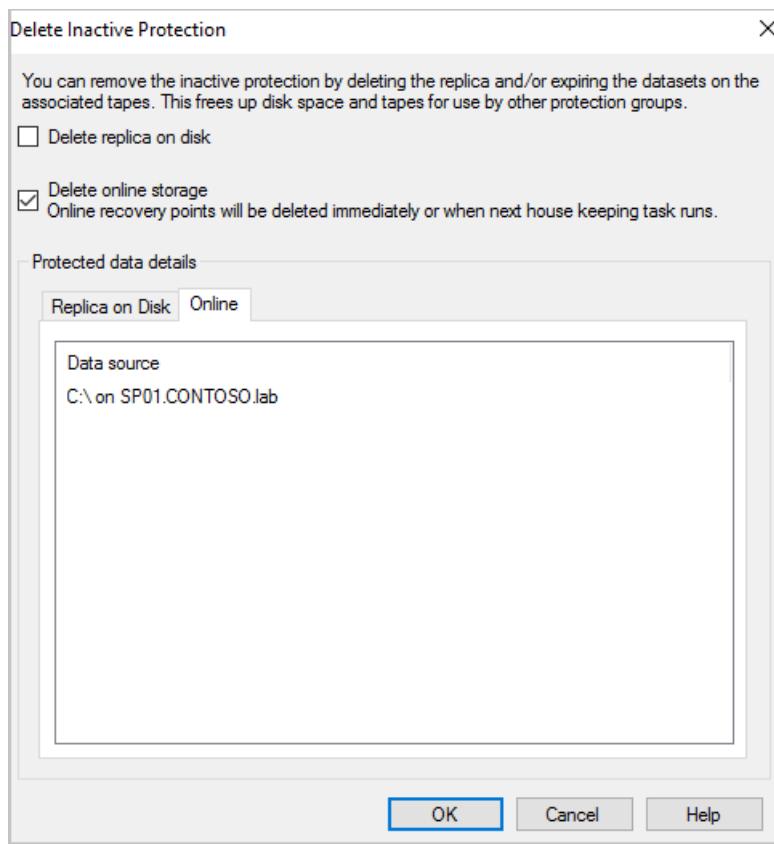


The protected member status changes to *Inactive replica available*.

- Right-click the inactive protection group and select **Remove inactive protection**.

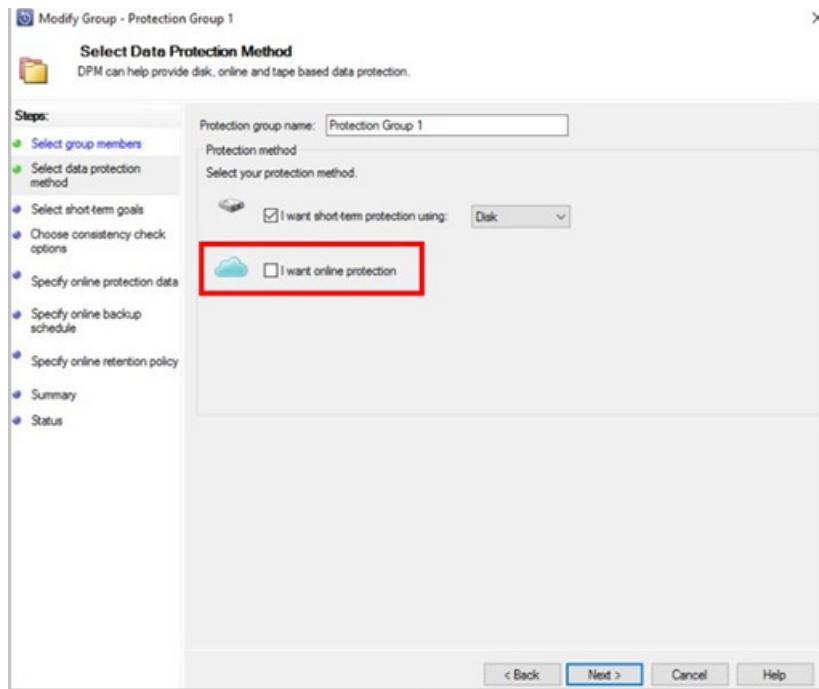


- From the **Delete Inactive Protection** window, select the **Delete online storage** check box, and then select **OK**.



#### Method 2

Open the **MABS management** console. Under **Select data protection method**, clear the **I want online protection** check box.



After you delete the on-premises backup items, follow the next steps from the portal.

## Delete the Recovery Services vault

1. When all dependencies have been removed, scroll to the **Essentials** pane in the vault menu.
2. Verify that there aren't any backup items, backup management servers, or replicated items listed. If items still appear in the vault, refer to the [Before you start](#) section.
3. When there are no more items in the vault, select **Delete** on the vault dashboard.

- Select **Yes** to verify that you want to delete the vault. The vault is deleted. The portal returns to the **New** service menu.

## Delete the Recovery Services vault by using PowerShell

First, read the **Before you start** section to understand the dependencies and vault deletion process.

To stop protection and delete the backup data:

- If you are using SQL in Azure VMs backup and enabled auto-protection for SQL instances, first disable the auto-protection.

```
Disable-AzRecoveryServicesBackupAutoProtection
 [-InputItem] <ProtectableItemBase>
 [-BackupManagementType] <BackupManagementType>
 [-WorkloadType] <WorkloadType>
 [-PassThru]
 [-VaultId <String>]
 [-DefaultProfile <IAzureContextContainer>]
 [-WhatIf]
 [-Confirm]
 [<CommonParameters>]
```

[Learn more](#) on how to disable protection for an Azure Backup-protected item.

- Stop protection and delete data for all backup-protected items in cloud (ex. IaaS VM, Azure File Share etc.):

```
Disable-AzRecoveryServicesBackupProtection
 [-Item] <ItemBase>
 [-RemoveRecoveryPoints]
 [-Force]
 [-VaultId <String>]
 [-DefaultProfile <IAzureContextContainer>]
 [-WhatIf]
 [-Confirm]
 [<CommonParameters>]
```

[Learn more](#) about disables protection for a Backup-protected item.

- For on-premises Files and Folders protected using Azure Backup Agent (MARS) backing up to Azure, use the following PowerShell command to delete the backed-up data from each MARS PowerShell module:

```
Get-OBPolicy | Remove-OBPolicy -DeleteBackup -SecurityPIN <Security Pin>
```

Post where the following prompt would appear:

*Microsoft Azure Backup Are you sure you want to remove this backup policy? Deleted backup data will be retained for 14 days. After that time, backup data will be permanently deleted.*

[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"):

- For on-premises machines protected using MABS (Microsoft Azure Backup Server) or DPM to Azure (System Center Data Protection Manager), use the following command to delete the backed-up data in Azure.

```
Get-OBPolicy | Remove-OBPolicy -DeleteBackup -SecurityPIN <Security Pin>
```

Post where the following prompt would appear:

*Microsoft Azure Backup Are you sure you want to remove this backup policy? Deleted backup data will be retained for 14 days. After that time, backup data will be permanently deleted.*

[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"):

After deleting the backed-up data, un-register any on-premises containers and management servers.

- For on-premises Files and Folders protected using Azure Backup Agent (MARS) backing up to Azure:

```
Unregister-AzRecoveryServicesBackupContainer
 [-Container] <ContainerBase>
 [-PassThru]
 [-VaultId <String>]
 [-DefaultProfile <IAzureContextContainer>]
 [-WhatIf]
 [-Confirm]
 [<CommonParameters>]
```

[Learn more](#) about un-registering a Windows Server or other container from the vault.

- For on-premises machines protected using MABS (Microsoft Azure Backup Server) or DPM to Azure (System Center Data Protection Manager):

```
Unregister-AzRecoveryServicesBackupManagementServer
 [-AzureRmBackupManagementServer] <BackupEngineBase>
 [-PassThru]
 [-VaultId <String>]
 [-DefaultProfile <IAzureContextContainer>]
 [-WhatIf]
 [-Confirm]
 [<CommonParameters>]
```

[Learn more](#) about un-registering a Backup management container from the vault.

After permanently deleting backed up data and un-registering all containers, proceed to delete the vault.

To delete a Recovery Services vault:

```
Remove-AzRecoveryServicesVault
-Vault <ARSVault>
[-DefaultProfile <IAzureContextContainer>]
[-WhatIf]
[-Confirm]
[<CommonParameters>]
```

[Learn more](#) about deleting a recovery services vault.

## Delete the Recovery Services vault by using CLI

First, read the [Before you start](#) section to understand the dependencies and vault deletion process.

### NOTE

Currently, Azure Backup CLI supports managing only Azure VM backups, so the following command to delete the vault works only if the vault contains Azure VM backups. You cannot delete a vault using Azure Backup CLI, if the vault contains any backup item of type other than Azure VMs.

To delete existing Recovery services vault, perform the below:

- To stop protection and delete the backup data

```
az backup protection disable --container-name
 --item-name
 [--delete-backup-data {false, true}]
 [--ids]
 [--resource-group]
 [--subscription]
 [--vault-name]
 [--yes]
```

For more information, see this[article](#).

- Delete an existing Recovery services vault:

```
az backup vault delete [--force]
 [--ids]
 [--name]
 [--resource-group]
 [--subscription]
 [--yes]
```

For more information, see this[article](#)

## Delete the Recovery Services vault by using Azure Resource Manager

This option to delete the Recovery Services vault is recommended only if all of the dependencies are removed and you're still getting the *Vault deletion error*. Try any or all of the following tips:

- From the **Essentials** pane in the vault menu, verify that there aren't any backup items, backup management servers, or replicated items listed. If there are backup items, refer the [Before you start](#) section.
- Try [deleting the vault from the portal](#) again.
- If all of the dependencies are removed and you're still getting the *Vault deletion error*, use the ARMClient tool to perform the following steps (after the note).

1. Go to [chocolatey.org](https://chocolatey.org) to download and install Chocolatey. Then, install ARMClient by running the following command:

```
choco install armclient --source=https://chocolatey.org/api/v2/
```

2. Sign in to your Azure account, and then run the following command:

```
ARMClient.exe login [environment name]
```

3. In the Azure portal, gather the subscription ID and resource group name for the vault you want to delete.

For more information on the ARMClient command, see [ARMClient README](#).

### Use the Azure Resource Manager client to delete a Recovery Services vault

1. Run the following command by using your subscription ID, resource group name, and vault name. If you don't have any dependencies, the vault is deleted when you run the following command:

```
ARMClient.exe delete
/subscriptions/<subscriptionID>/resourceGroups/<resourcegroupname>/providers/Microsoft.RecoveryServices/
vaults/<recovery services vault name>?api-version=2015-03-15
```

2. If the vault is not empty, you'll receive the following error message: *Vault cannot be deleted as there are existing resources within this vault*. To remove a protected item or container within a vault, run the following command:

```
ARMClient.exe delete
/subscriptions/<subscriptionID>/resourceGroups/<resourcegroupname>/providers/Microsoft.RecoveryServices/
vaults/<recovery services vault name>/registeredIdentities/<container name>?api-version=2016-06-01
```

3. In the Azure portal, make sure that the vault is deleted.

## Next steps

[Learn about Recovery Services vaults](#)

[Learn about monitoring and managing Recovery Services vaults](#)

# Move a Recovery Services vault across Azure Subscriptions and Resource Groups

2/10/2020 • 5 minutes to read • [Edit Online](#)

This article explains how to move a Recovery Services vault configured for Azure Backup across Azure subscriptions, or to another resource group in the same subscription. You can use the Azure portal or PowerShell to move a Recovery Services vault.

## Supported regions

Resource move for Recovery Services vault is supported in Australia East, Australia South East, Canada Central, Canada East, South East Asia, East Asia, Central US, North Central US, East US, East US2, South central US, West Central US, West Central US2, West US, Central India, South India, Japan East, Japan West, Korea Central, Korea South, North Europe, West Europe, South Africa North, South Africa West, UK South, and UK West.

## Unsupported regions

France Central, France South, Germany Northeast, Germany Central, US Gov Iowa, China North, China North2, China East, China East2

## Prerequisites for moving Recovery Services vault

- During vault move across resource groups, both the source and target resource groups are locked preventing the write and delete operations. For more information, see this [article](#).
- Only admin subscription has the permissions to move a vault.
- For moving vault across subscriptions, the target subscription must reside in the same tenant as the source subscription and its state should be enabled.
- You must have permission to perform write operations on the target resource group.
- Moving the vault only changes the resource group. The Recovery Services vault will reside on the same location and it cannot be changed.
- You can move only one Recovery Services vault, per region, at a time.
- If a VM doesn't move with the Recovery Services vault across subscriptions, or to a new resource group, the current VM recovery points will remain intact in the vault until they expire.
- Whether the VM is moved with the vault or not, you can always restore the VM from the retained backup history in the vault.
- The Azure Disk Encryption requires that the key vault and VMs reside in the same Azure region and subscription.
- To move a virtual machine with managed disks, see this [article](#).
- The options for moving resources deployed through the Classic model differ depending on whether you are moving the resources within a subscription, or to a new subscription. For more information, see this [article](#).
- Backup policies defined for the vault are retained after the vault moves across subscriptions or to a new resource group.
- Moving vault with the Azure Files, Azure File Sync, or SQL in IaaS VMs across subscriptions and resource groups is not supported.
- If you move a vault containing VM backup data, across subscriptions, you must move your VMs to the same subscription, and use the same target VM resource group name (as it was in old subscription) to continue backups.

## NOTE

Recovery Services vaults configured to use with **Azure Site Recovery** can't move, yet. If you have configured any VMs (Azure IaaS, Hyper-V, VMware) or physical machines for disaster recovery using the **Azure Site Recovery**, the move operation will be blocked. The resource move feature for Site Recovery service is not yet available.

## Use Azure portal to move Recovery Services vault to different resource group

To move a recovery services vault and its associated resources to different resource group

1. Sign in to the [Azure portal](#).
2. Open the list of **Recovery Services vaults** and select the vault you want to move. When the vault dashboard opens, it appears as shown in the following image.

The screenshot shows the 'Overview' tab of a Recovery Services vault named 'sogupcreatevmvault'. The left sidebar includes sections for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Properties, Locks, Automation script, Getting started (Backup, Site Recovery), Protected items (Backup items, Replicated items), and Manage. The main content area displays 'What's new' with links to Accelerated Networking, Azure Site Recovery, Azure Backup for SQL Server, Disaster recovery for Azure IaaS, and Instant Recovery. Below this are two large cloud icons: 'Backup' and 'Site Recovery', each with their own 'Getting started' and 'Site Recovery dashboard' links.

If you do not see the **Essentials** information for your vault, click the drop-down icon. You should now see the Essentials information for your vault.

This screenshot is identical to the previous one, but the 'Resource group' dropdown in the top right has been opened, showing the current value 'anurag-sql' and a 'change' link. A red box highlights the 'change' link. The rest of the interface is identical to the first screenshot.

3. In the vault overview menu, click **change** next to the **Resource group**, to open the **Move resources** blade.

The screenshot shows the Azure portal interface for a Recovery Services vault named 'sogupcreatevmvault'. The left sidebar has a search bar and navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and Settings. The main content area shows the vault's details: Resource group (anurag-sql), Location (Southeast Asia), Subscription (Backup PM Demo Subscription1), and Subscription ID. A red box highlights the 'Resource group' dropdown menu item.

- In the **Move resources** blade, for the selected vault it is recommended to move the optional related resources by selecting the checkbox as shown in the following image.

The screenshot shows the 'Move resources' blade. It lists resources to move under 'Resources to move' and related resources to move under 'Related resources to move (optional)'. A red box highlights the 'SELECT ALL' checkbox at the top left of the list.

| Resource Type                                | Resource Name                                           |
|----------------------------------------------|---------------------------------------------------------|
| Disk                                         | EUStest_disk2_3bc45b057306407d97e51c98b8a5c2bc          |
| Disk                                         | EUStest_OsDisk_1_7269cdca59e6c42eea46c483b4e9963b3      |
| Disk                                         | FileServer55_OsDisk_1_9d7b5c2279734ad99a07e91774018287e |
| Disk                                         | SQLtestEU2_disk2_2e96d18014cc4599be63d5e396600e8b5      |
| Disk                                         | SQLtestEU2_OsDisk_1_2f1a3237e9b41c0ba3b8aa50d812c48     |
| Virtual machine                              | EUStest                                                 |
| microsoft.compute/virtualmachines/extensions | eustest/AzureBackupWindowsWorkload                      |
| microsoft.compute/virtualmachines/extensions | EUStest/MicrosoftMonitoringAgent                        |
| microsoft.compute/virtualmachines/extensions | EUStest/SqlliaasExtension                               |
| Virtual machine                              | FileServer55                                            |

- To add the target resource group, in the **Resource group** drop-down list select an existing resource group or click **create a new group** option.

The screenshot shows the 'Move these resources' dialog box. It includes fields for 'Resource group' and a checkbox for understanding moved resources. A red box highlights the 'Create a new group' button.

- After adding the resource group, confirm **I understand that tools and scripts associated with moved resources will not work until I update them to use new resource IDs** option and then click **OK** to complete moving the vault.

The screenshot shows the 'Move these resources' dialog box again, but this time the 'Create a new group' checkbox is checked. The 'OK' button is highlighted.

## Use Azure portal to move Recovery Services vault to a different subscription

You can move a Recovery Services vault and its associated resources to a different subscription

- Sign in to the [Azure portal](#).
- Open the list of Recovery Services vaults and select the vault you want to move. When the vault dashboard opens, it appears as shown the following image.

The screenshot shows the Azure Recovery Services vault overview page for 'sogupcreatevmvault'. The left sidebar contains a navigation menu with various options such as Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Properties, Locks, Automation script, Getting started (Backup, Site Recovery), Protected items (Backup items, Replicated items), and Manage. The main content area features two large blue cloud icons labeled 'Backup' and 'Site Recovery'. Below each icon are links for 'Getting started', 'Backup dashboard', 'Backup items', 'Backup policies' (under Backup), 'Site Recovery dashboard', 'Replicated items', and 'Manage Recovery Plans' (under Site Recovery). A 'What's new' section at the bottom lists several recent updates.

If you do not see the **Essentials** information for your vault, click the drop-down icon. You should now see the Essentials information for your vault.

The screenshot shows the same Azure Recovery Services vault overview page for 'sogupcreatevmvault'. The left sidebar and main content area are identical to the previous screenshot. However, the 'Subscription' field in the center pane is highlighted with a red box, indicating it is the target for modification.

3. In the vault overview menu, click **change** next to **Subscription**, to open the **Move resources** blade.

The screenshot shows the same Azure Recovery Services vault overview page for 'sogupcreatevmvault'. The left sidebar and main content area are identical to the previous screenshots. The 'Subscription' field in the center pane is highlighted with a red box. Additionally, the 'change' button next to the 'Subscription' field is also highlighted with a red box, indicating the user is about to open the 'Move resources' blade.

4. Select the resources to be moved, here we recommend you to use the **Select All** option to select all the listed optional resources.

The screenshot shows the 'Move resources' dialog in the Azure portal. It lists resources to move from a source subscription to a target Recovery Services vault. The resources include:

- EUtest\_disk2\_3bc45b85730640797e51c98b8a5c2bc (Disk)
- EUtest\_OsDisk\_1\_7269cd8a59e6c42eeaa45c485b4e996353 (Disk)
- FileServerSS\_OsDisk\_1\_9d7b5c2278734ad9ad7e39174018257e (Disk)
- SQLtestEU2\_disk2\_2e96d18014cc4599b63d5e396600e8b5 (Disk)
- SQLtestEU2\_OsDisk\_1\_23f1a3237e9b41c0b3b3aa350d812c48 (Disk)
- EUtest (Virtual machine)
- eustest/AzureBackupWindowsWorkload (microsoft.compute/virtualmachines/extensions)
- EUtest/MicrosoftMonitoringAgent (microsoft.compute/virtualmachines/extensions)
- EUtest/SqlIaasExtension (microsoft.compute/virtualmachines/extensions)

- Select the target subscription from the **Subscription** drop-down list, where you want the vault to be moved.
- To add the target resource group, in the **Resource group** drop-down list select an existing resource group or click **create a new group** option.

The screenshot shows the 'Move these resources' dialog. It includes a 'Subscription' dropdown set to 'ASR A2A PM Canary subscription 2', a 'Resource group' input field, a checkbox for understanding resource ID changes, and a 'Create a new group' button highlighted with a red box.

- Click **I understand that tools and scripts associated with moved resources will not work until I update them to use new resource IDs** option to confirm, and then click **OK**.

#### NOTE

Cross subscription backup (RS vault and protected VMs are in different subscriptions) is not a supported scenario. Also, storage redundancy option from local redundant storage (LRS) to global redundant storage (GRS) and vice versa cannot be modified during the vault move operation.

## Use PowerShell to move Recovery Services vault

To move a Recovery Services vault to another resource group, use the `Move-AzureRMResource` cmdlet.

`Move-AzureRMResource` requires the resource name and type of resource. You can get both from the `Get-AzureRmRecoveryServicesVault` cmdlet.

```
$destinationRG = "<destinationResourceGroupName>"
$vault = Get-AzureRmRecoveryServicesVault -Name <vaultname> -ResourceGroupName <vaultRGname>
Move-AzureRmResource -DestinationResourceGroupName $destinationRG -ResourceId $vault.ID
```

To move the resources to different subscription, include the `-DestinationSubscriptionId` parameter.

```
Move-AzureRmResource -DestinationSubscriptionId "<destinationSubscriptionID>" -DestinationResourceGroupName
$destinationRG -ResourceId $vault.ID
```

After executing the above cmdlets, you will be asked to confirm that you want to move the specified resources. Type **Y** to confirm. After a successful validation, the resource moves.

## Use CLI to move Recovery Services vault

To move a Recovery Services vault to another resource group, use the following cmdlet:

```
az resource move --destination-group <destinationResourceGroupName> --ids <VaultResourceID>
```

To move to a new subscription, provide the `--destination-subscription-id` parameter.

## Post migration

1. Set/verify the access controls for the resource groups.
2. The Backup reporting and monitoring feature needs to be configured again for the vault post the move completes. The previous configuration will be lost during the move operation.

## Next steps

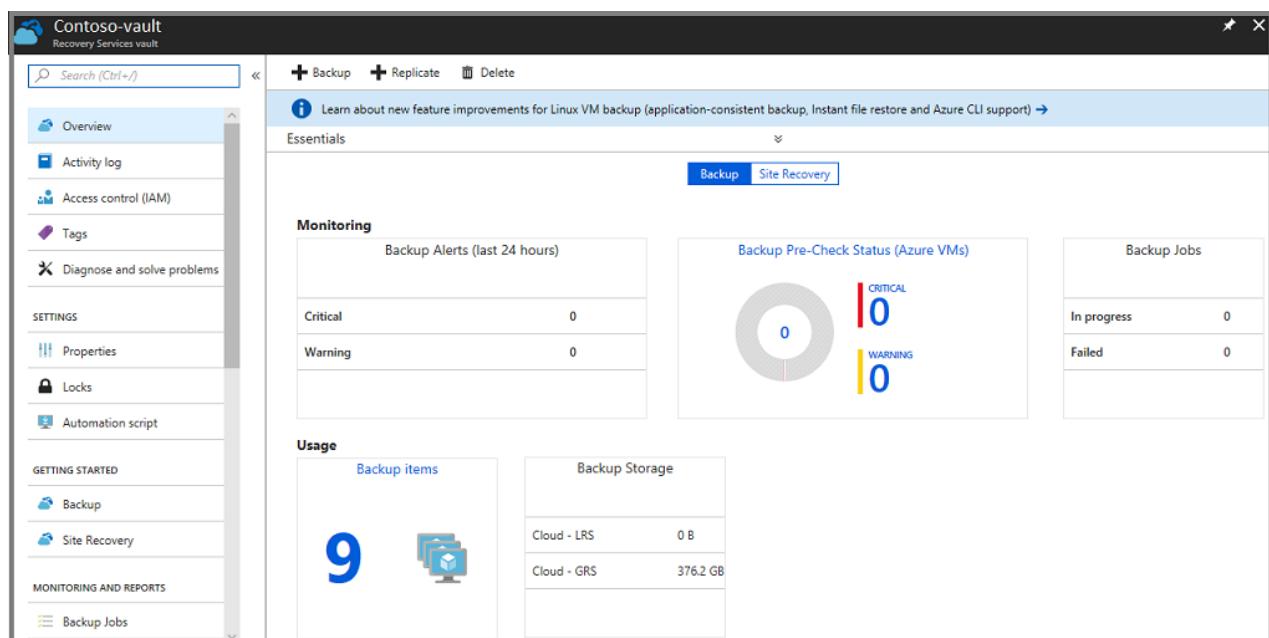
You can move many different types of resources between resource groups and subscriptions.

For more information, see [Move resources to new resource group or subscription](#).

# Monitor and manage Recovery Services vaults

2/24/2020 • 8 minutes to read • [Edit Online](#)

This article explains how to use the Recovery Services vault **Overview** dashboard to monitor and manage your Recovery Services vaults. When you open a Recovery Services vault from the list, the **Overview** dashboard for the selected vault, opens. The dashboard provides various details about the vault. There are *tiles* that show: the status of critical and warning alerts, in-progress and failed backup jobs, and the amount of locally redundant storage (LRS) and geo redundant storage (GRS) used. If you back up Azure VMs to the vault, the **Backup Pre-Check Status** tile displays any critical or warning items. The following image is the **Overview** dashboard for **Contoso-vault**. The **Backup Items** tile shows there are nine items registered to the vault.



The prerequisites for this article are: an Azure subscription, a Recovery Services vault, and that there is at least one backup item configured for the vault.

## NOTE

Azure has two different deployment models you can use to create and work with resources: [Azure Resource Manager](#) and [classic](#). This article covers the use of the Resource Manager deployment model. We recommend the Resource Manager deployment model for new deployments instead of the classic deployment model.

## Open a Recovery Services vault

To monitor alerts, or view management data about a Recovery Services vault, open the vault.

1. Sign in to the [Azure portal](#) using your Azure subscription.
2. In the portal, click **All services**.

The screenshot shows the Microsoft Azure portal's search interface. The search bar at the top contains the text "recovery". Below it, the "All services" button is highlighted with a red box. The search results list two items: "Recovery Services vaults" and "Site recovery vaults (classic)".

3. In the **All services** dialog box, type **Recovery Services**. As you begin typing, the list filters based on your input. When the **Recovery Services vaults** option appears, click it to open the list of Recovery Services vaults in your subscription.

The screenshot shows the "Recovery Services vaults" list page. It displays four vaults: Contoso-MAB-server, Contoso-testvault, Contoso-vault, and DPM-demo-vault. All four vaults are located in the "Contoso-Resources" resource group and "Southeast Asia" location. The "Subscription" column shows "<subscription>" for all entries.

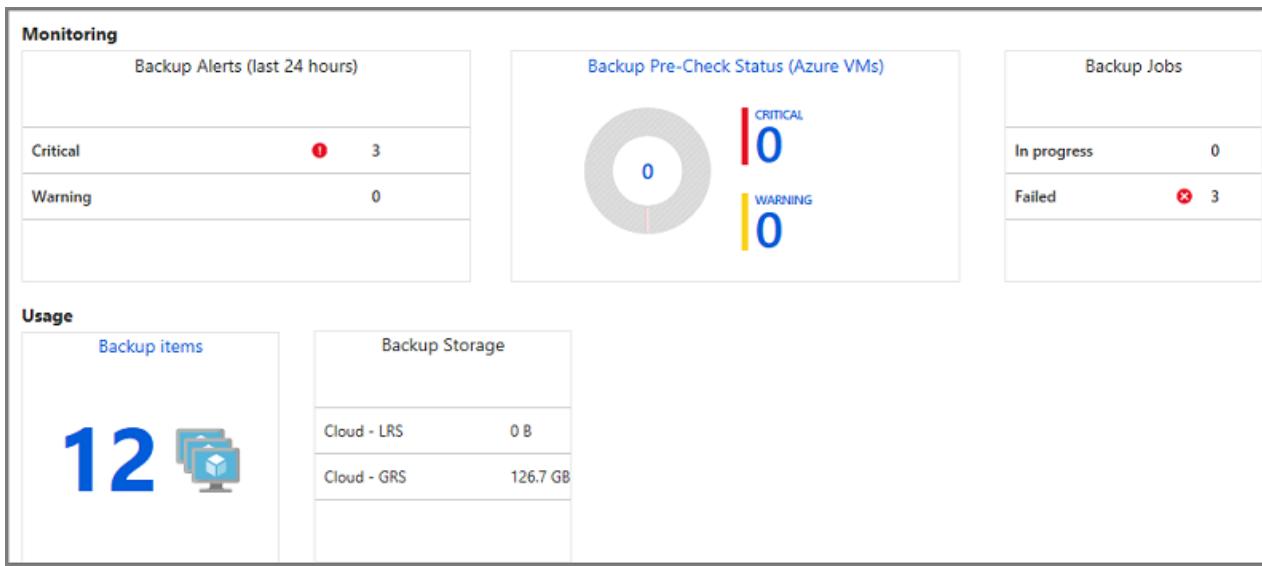
4. From the list of vaults, click a vault to open its **Overview** dashboard.

The screenshot shows the "Contoso-vault" Overview dashboard. The left sidebar lists navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Properties, Locks, Automation script, Backup, Site Recovery, and Backup Jobs. The main area features a "Monitoring" section with a grid for Backup Alerts (last 24 hours) and a "Backup Pre-Check Status (Azure VMs)" circular progress bar. The "Usage" section shows 9 backup items and storage details for Cloud - LRS and Cloud - GRS. A "Backup Jobs" section shows 0 In progress and 0 Failed jobs.

The Overview dashboard uses tiles to provide alerts and backup job data.

## Monitor backup jobs and alerts

The Recovery Services vault **Overview** dashboard provides tiles for Monitoring and Usage information. The tiles in the Monitoring section display Critical and Warning alerts, and In progress and Failed jobs. Click a particular alert or job to open the Backup Alerts or Backup Jobs menu, filtered for that job or alert.



The Monitoring section shows the results of predefined **Backup Alerts** and **Backup Jobs** queries. The Monitoring tiles provide up-to-date information about:

- Critical and Warning alerts for Backup jobs (in the last 24 hours)
- Pre-check status for Azure VMs - For complete information on the pre-check status, see the [Backup blog on Backup Pre-check status](#).
- The Backup jobs in progress, and jobs that have failed (in the last 24 hours).

The Usage tiles provide:

- The number of Backup items configured for the vault.
- The Azure storage (separated by LRS and GRS) consumed by the vault.

Click the tiles (except Backup Storage) to open the associated menu. In the image above, the Backup Alerts tile shows three Critical alerts. Clicking the Critical alerts row in the Backup Alerts tile, opens the Backup Alerts filtered for Critical alerts.

| ALERT          | BACKUP ITEM  | PROTECTED SERVER           | SEVERITY | DURATION | CREATION TIME        | STATUS |
|----------------|--------------|----------------------------|----------|----------|----------------------|--------|
| Backup failure | C:\          | Contoso.server.contoso.com | Critical | 16:44:39 | 8/12/2018 7:52:54 PM | Active |
| Backup failure | C:\          | Contoso.server.contoso.com | Critical | 16:46:43 | 8/12/2018 7:50:50 PM | Active |
| Backup failure | contososhare | contosodemostorage         | Critical | 19:04:16 | 8/12/2018 5:33:17 PM | Active |

The Backup Alerts menu, in the image above, is filtered by: Status is Active, Severity is Critical, and time is the previous 24 hours.

## Manage Backup alerts

To access the Backup Alerts menu, in the Recovery Services vault menu, click **Backup Alerts**.

The screenshot shows the Azure Recovery Services vault 'WonderDemoVault'. The left sidebar has sections for SETTINGS (Properties, Locks, Automation script), GETTING STARTED (Backup, Site Recovery), and MONITORING AND REPORTS (Backup Jobs, Site Recovery Jobs, Backup Alerts, Site Recovery Events, Backup Reports). The 'Backup Alerts' item is selected and highlighted with a red border. The main content area shows monitoring statistics: Backup Alerts (last 24 hours) with 2 Critical and 0 Warning; Usage showing 12 Backup items; and Backup Storage with Cloud - LRS at 0.8 GB and Cloud - GRS at 127.2 GB.

The Backup Alerts report lists the alerts for the vault.

| ALERT          | BACKUP ITEM  | PROTECTED SERVER           | SEVERITY | DURATION | CREATION TIME        | LATEST OCCURRENCE TIME | STATUS |
|----------------|--------------|----------------------------|----------|----------|----------------------|------------------------|--------|
| Backup failure | CA           | contoso.server.contoso.com | Critical | 07:47:05 | 8/14/2018 7:02:10 AM | 8/14/2018 7:02:10 AM   | Active |
| Backup failure | contososhare | contoso.server.com         | Critical | 21:15:07 | 8/13/2018 5:34:08 PM | 8/13/2018 5:34:08 PM   | Active |

## Alerts

The Backup Alerts list displays the selected information for the filtered alerts. In the Backup Alerts menu, you can filter for Critical or Warning alerts.

| ALERT LEVEL   | EVENTS THAT GENERATE ALERTS                                                                                                                                                                                             |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Critical      | You receive critical alerts when: Backup jobs fail, recovery jobs fail, and when you stop protection on a server, but retain the data.                                                                                  |
| Warning       | You receive warning alerts when: Backup jobs complete with warnings, for example when fewer than 100 files are not backed up due to corruption issues, or when greater than 1,000,000 files are successfully backed up. |
| Informational | currently, no informational alerts are in use.                                                                                                                                                                          |

## Viewing alert details

The Backup Alerts report tracks eight details about each alert. Use the **Choose columns** button to edit the details in the report.

| ALERT          | BACKUP ITEM  | PROTECTED SERVER           | SEVERITY | DURATION | CREATION TIME        | LATEST OCCURRENCE TIME | STATUS |
|----------------|--------------|----------------------------|----------|----------|----------------------|------------------------|--------|
| Backup failure | C:\          | contoso.server.contoso.com | Critical | 07:47:05 | 8/14/2018 7:02:10 AM | 8/14/2018 7:02:10 AM   | Active |
| Backup failure | contososhare | contoso.server.com         | Critical | 21:15:07 | 8/13/2018 5:34:08 PM | 8/13/2018 5:34:08 PM   | Active |

By default, all details, except **Latest Occurrence Time**, appear in the report.

- Alert
- Backup Item
- Protected Server
- Severity
- Duration
- Creation Time
- Status
- Latest Occurrence Time

### Change the details in alerts report

1. To change the report information, in the **Backup Alerts** menu, click **Choose columns**.

The **Choose columns** menu opens.

2. In the **Choose columns** menu, choose the details you want to appear in the report.

3. Click **Done** to save your changes and close the Choose columns menu.

If you make changes, but don't want to keep the changes, click **Reset** to return the selected to the last saved configuration.

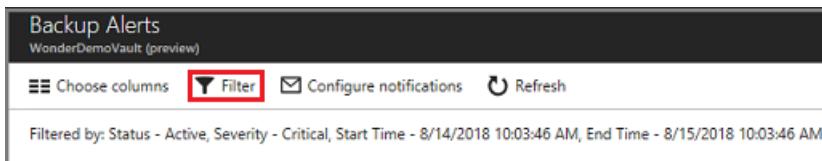
## Change the filter in alerts report

Use the **Filter** menu to change the Severity, Status, Start time and End time for the alerts.

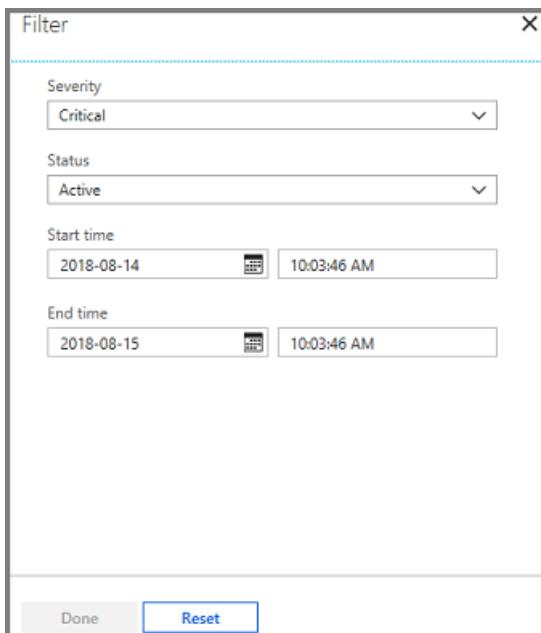
### NOTE

Editing the Backup Alerts filter doesn't change the Critical or Warning alerts in the vault Overview dashboard.

1. To change the Backup Alerts filter, in the Backup Alerts menu, click **Filter**.



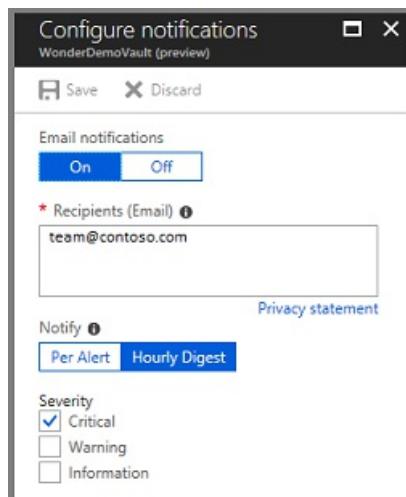
The Filter menu appears.



2. Edit the Severity, Status, Start time, or End time, and click **Done** to save your changes.

## Configuring notifications for alerts

Configure notifications to generate emails when a Warning or Critical alert occurs. You can send email alerts each hour, or when a particular alert occurs.



By default, Email notifications are **On**. Click **Off** to stop the email notifications.

On the **Notify** control, choose **Per Alert** if don't want grouping or don't have many items that could generate alerts. Every alert results in one notification (the default setting), and a resolution email is sent immediately.

If you select **Hourly Digest**, an email is sent to the recipients explaining the unresolved alerts generated in the last hour. A resolution email is sent out at the end of the hour.

Choose the alert severity (Critical or Warning) used to generate email. Currently there are no Information alerts.

## Manage Backup items

A Recovery Services vault holds many types of backup data. [Learn more](#) about what you can back up. To manage the various servers, computers, databases, and workloads, click the **Backup Items** tile to view the contents of the vault.

The screenshot shows the Azure Recovery Services vault management interface. At the top, there are buttons for '+ Backup', '+ Replicate', and 'Delete'. A blue banner at the top right provides information about new feature improvements for Linux VM backup. Below the banner, the 'Essentials' section has tabs for 'Backup' (selected) and 'Site Recovery'. The 'Monitoring' section includes a 'Backup Alerts (last 24 hours)' table with 1 Critical alert and 0 Warning alerts, and a 'Backup Pre-Check Status (Azure VMs)' chart showing 0 Critical and 0 Warning errors. The 'Backup Jobs' section shows 0 In progress and 1 Failed job. The 'Usage' section features a large red-bordered box containing the number '12' and icons representing backup items, and a 'Backup Storage' table showing Cloud - LRS (0 B) and Cloud - GRS (133.4 GB).

The list of Backup Items, organized by Backup Management Type, opens.

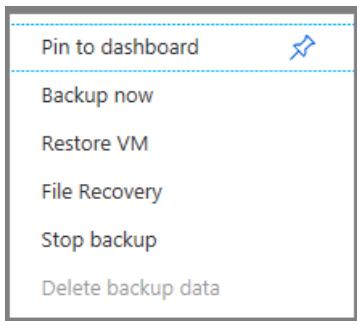
| BACKUP MANAGEMENT TYPE      | BACKUP ITEM COUNT |
|-----------------------------|-------------------|
| Azure Storage (Azure Files) | 4                 |
| Azure Backup Server         | 3                 |
| Azure Backup Agent          | 2                 |
| Azure Virtual Machine       | 2                 |
| SQL in Azure VM             | 1                 |
| DPM                         | 0                 |

To explore a specific type of protected instance, click the item in the Backup Management Type column. For example, in the above image, there are two Azure virtual machines protected in this vault. Clicking **Azure Virtual Machine**, opens the list of protected virtual machines in this vault.

The screenshot shows a list of backup items for an Azure Virtual Machine. At the top, there's a header bar with a refresh button, an 'Add' button, and a 'Filter' button. Below the header, a message says 'Fetching data from service completed.' There's a search bar labeled 'Filter items ...'. The main table has columns: NAME, RESOURCE GROUP, BACKUP PRE-CHECK, LAST BACKUP STATUS, and LATEST RESTORE POINT. Two rows are listed:

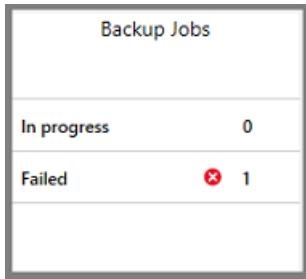
| NAME        | RESOURCE GROUP | BACKUP PRE-CHECK | LAST BACKUP STATUS | LATEST RESTORE POINT  |
|-------------|----------------|------------------|--------------------|-----------------------|
| Contoso-VM1 | ContosoRG      | Passed           | Success            | 8/19/2018 10:03:05 PM |
| WonderSQLVM | WonderDemoRG   | Passed           | Success            | 8/19/2018 10:06:45 PM |

The list of virtual machines has helpful data: the associated Resource Group, previous [Backup Pre-Check](#), Last Backup Status, and date of the most recent Restore Point. The ellipsis, in the last column, opens the menu to trigger common tasks. The helpful data provided in columns, is different for each backup type.



## Manage Backup jobs

The **Backup Jobs** tile in the vault dashboard shows the number of jobs that are In Progress, or Failed in the last 24 hours. The tile provides a glimpse into the Backup Jobs menu.

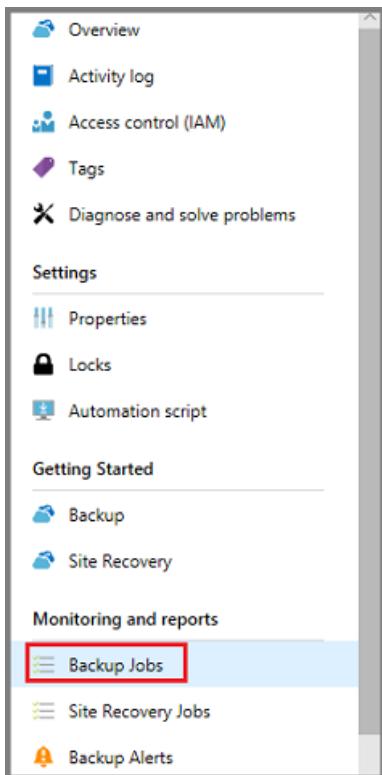


To see additional details about the jobs, click **In Progress** or **Failed** to open the Backup Jobs menu filtered for that state.

### Backup jobs menu

The **Backup Jobs** menu displays information about the Item type, Operation, Status, Start Time, and Duration.

To open the Backup Jobs menu, in the vault's main menu, click **Backup Jobs**.



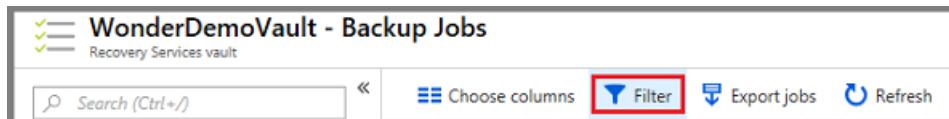
The list of Backup jobs opens.

| Choose columns                                                                                                                                               |           |           |                       |                       |          |     |     | Filter | Export jobs | Refresh |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-----------|-----------------------|-----------------------|----------|-----|-----|--------|-------------|---------|
| Filtered by: Item Type - All item types, Operation - All Operations, Status - All Status, Start Time - 8/20/2018 3:28:56 PM, End Time - 8/21/2018 3:28:56 PM |           |           |                       |                       |          |     |     |        |             |         |
| Completed fetching data from the service.                                                                                                                    |           |           |                       |                       |          |     |     |        |             |         |
| Filter items...                                                                                                                                              |           |           |                       |                       |          |     |     |        |             |         |
| WORKLOAD NAME                                                                                                                                                | OPERATION | STATUS    | TYPE                  | START TIME            | DURATION |     |     |        |             |         |
| contosotest                                                                                                                                                  | Backup    | Completed | Azure virtual machine | 8/20/2018 10:04:26 PM | 00:30:30 | ... | ... | ...    | ...         | ...     |
| ContosoSQLVM                                                                                                                                                 | Backup    | Completed | Azure virtual machine | 8/20/2018 10:03:52 PM | 01:35:41 | ... | ... | ...    | ...         | ...     |
| ContosoFilefolder                                                                                                                                            | Backup    | Completed | Files and folders     | 8/20/2018 10:03:05 PM | 00:00:49 | ... | ... | ...    | ...         | ...     |
| contosoHRsh(contosostorage)                                                                                                                                  | Backup    | Failed    | AzureStorage          | 8/20/2018 5:34:22 PM  | 00:00:01 | ... | ... | ...    | ...         | ...     |
| contososhare(contosostorage)                                                                                                                                 | Backup    | Completed | AzureStorage          | 8/20/2018 5:34:22 PM  | 00:00:03 | ... | ... | ...    | ...         | ...     |
| contoso100(contosostorage)                                                                                                                                   | Backup    | Completed | AzureStorage          | 8/20/2018 5:34:22 PM  | 00:00:03 | ... | ... | ...    | ...         | ...     |

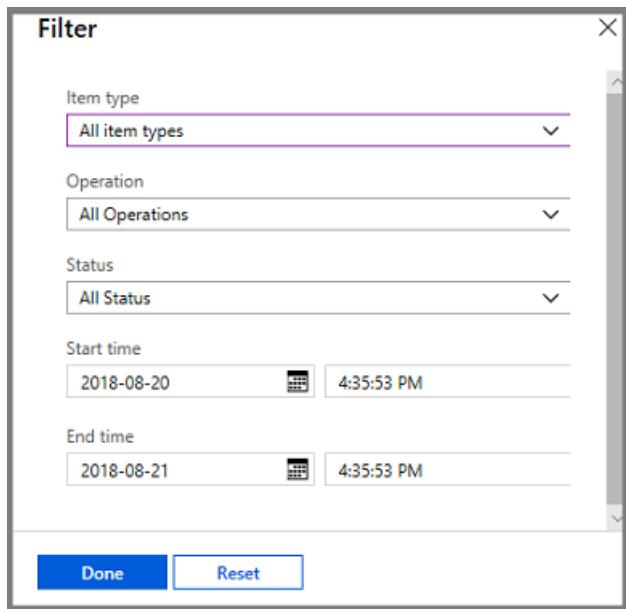
The Backup Jobs menu shows the status for all operations, on all backup types, for the last 24 hours. Use **Filter** to change the filters. The filters are explained in the following sections.

To change the filters:

1. In the vault Backup Jobs menu, click **Filter**.



The Filter menu opens.



2. Choose the filter settings and click **Done**. The filtered list refreshes based on the new settings.

#### Item type

The Item type is the backup management type of the protected instance. There are four types; see the following list. You can view all item types, or one item type. You can't select two or three item types. The available Item types are:

- All item types
- Azure virtual machine
- Files and folders
- Azure Storage
- Azure workload

#### Operation

You can view one operation, or all operations. You can't select two or three operations. The available Operations are:

- All Operations
- Register
- Configure backup
- Backup
- Restore
- Disable backup
- Delete backup data

#### Status

You can view All Status or one. You can't select two or three statuses. The available statuses are:

- All Status
- Completed
- In progress
- Failed
- Canceled
- Completed with warnings

#### Start time

The day and time that the query begins. The default is a 24-hour period.

#### **End time**

The day and time when the query ends.

#### **Export jobs**

Use **Export jobs** to create a spreadsheet containing all Jobs menu information. The spreadsheet has one sheet that holds a summary of all jobs, and individual sheets for each job.

To export the jobs information to a spreadsheet, click **Export jobs**. The service creates a spreadsheet using the name of the vault and date, but you can change the name.

## Monitor Backup usage

The Backup Storage tile in the dashboard shows the storage consumed in Azure. Storage usage is provided for:

- Cloud LRS storage usage associated with the vault
- Cloud GRS storage usage associated with the vault

## Troubleshooting monitoring issues

**Issue:** Jobs and/or alerts from the Azure Backup agent do not appear in the portal.

**Troubleshooting steps:** The process, `OBRecoveryServicesManagementAgent`, sends the job and alert data to the Azure Backup service. Occasionally this process can become stuck or shutdown.

1. To verify the process isn't running, open **Task Manager**, and check `OBRecoveryServicesManagementAgent` is running.
2. If the process isn't running, open **Control Panel**, and browse the list of services. Start or restart **Microsoft Azure Recovery Services Management Agent**.

For further information, browse the logs at:

`<AzureBackup_agent_install_folder>\Microsoft Azure Recovery Services Agent\Temp\GatewayProvider*` For example:

`C:\Program Files\Microsoft Azure Recovery Services Agent\Temp\GatewayProvider0.errlog`

## Next steps

- [Restore Windows Server or Windows Client from Azure](#)
- To learn more about Azure Backup, see [Azure Backup Overview](#)

# An overview of Azure VM backup

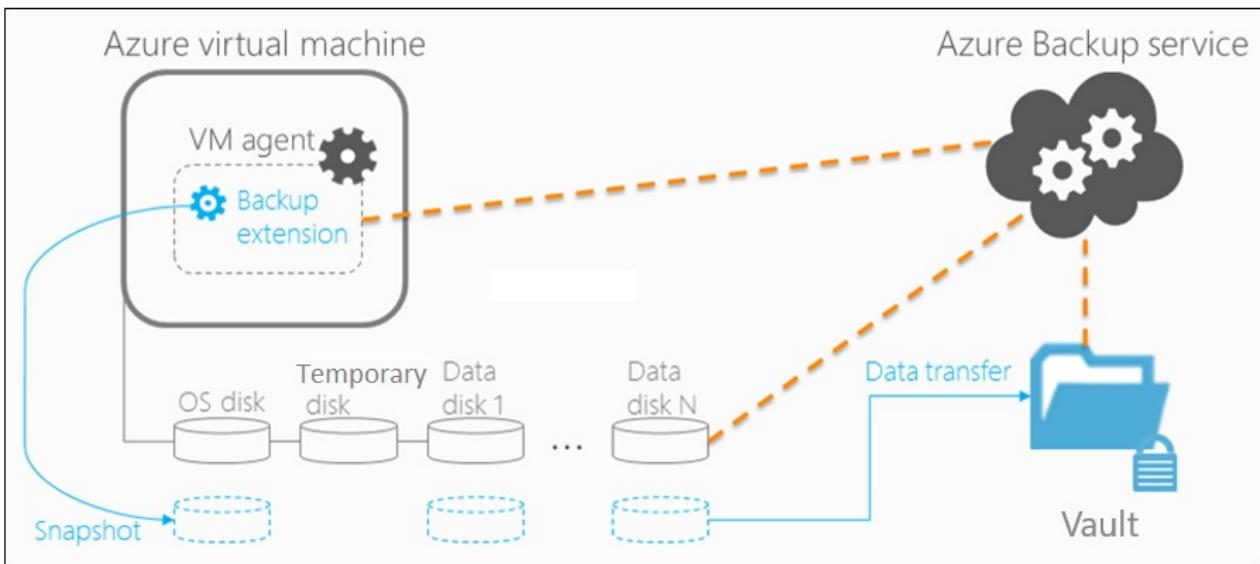
2/25/2020 • 10 minutes to read • [Edit Online](#)

This article describes how the [Azure Backup service](#) backs up Azure virtual machines (VMs).

## Backup process

Here's how Azure Backup completes a backup for Azure VMs:

1. For Azure VMs that are selected for backup, Azure Backup starts a backup job according to the backup schedule you specify.
2. During the first backup, a backup extension is installed on the VM if the VM is running.
  - For Windows VMs, the *VMSnapshot* extension is installed.
  - For Linux VMs, the *VMSnapshotLinux* extension 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).
4. For Linux VMs, Backup takes a file-consistent backup. For app-consistent snapshots, you need to manually customize pre/post scripts.
5. 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.
6. Changes made to a Windows VM after Azure Backup is enabled on it are:
  - Microsoft Visual C++ 2013 Redistributable(x64) - 12.0.40660 is installed in the VM
  - Startup type of Volume Shadow Copy service (VSS) changed to automatic from manual
  - IaaSVmProvider Windows service is added
7. When the data transfer is complete, the snapshot is removed, and a recovery point is created.



## Encryption of Azure VM backups

When you back up Azure VMs with Azure Backup, VMs are encrypted at rest with Storage Service Encryption (SSE). Azure Backup can also back up Azure VMs that are encrypted by using Azure Disk Encryption.

| ENCRYPTION                   | DETAILS                                                                                                                                                                                                                                                                                            | SUPPORT                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Azure Disk Encryption</b> | <p>Azure Disk Encryption encrypts both OS and data disks for Azure VMs.</p> <p>Azure Disk Encryption integrates with BitLocker encryption keys (BEKs), which are safeguarded in a key vault as secrets. Azure Disk Encryption also integrates with Azure Key Vault key encryption keys (KEKs).</p> | <p>Azure Backup supports backup of managed and unmanaged Azure VMs encrypted with BEKs only, or with BEKs together with KEKs.</p> <p>Both BEKs and KEKs are backed up and encrypted.</p> <p>Because KEKs and BEKs are backed up, users with the necessary permissions can restore keys and secrets back to the key vault if needed. These users can also recover the encrypted VM.</p> <p>Encrypted keys and secrets can't be read by unauthorized users or by Azure.</p> |
| <b>SSE</b>                   | <p>With SSE, Azure Storage provides encryption at rest by automatically encrypting data before storing it. Azure Storage also decrypts data before retrieving it.</p>                                                                                                                              | <p>Azure Backup uses SSE for at-rest encryption of Azure VMs.</p>                                                                                                                                                                                                                                                                                                                                                                                                         |

For managed and unmanaged Azure VMs, Backup supports both VMs encrypted with BEKs only or VMs encrypted with BEKs together with KEKs.

The backed-up BEKs (secrets) and KEKs (keys) are encrypted. They can be read and used only when they're restored back to the key vault by authorized users. Neither unauthorized users, or Azure, can read or use backed-up keys or secrets.

BEKs are also backed up. So, if the BEKs are lost, authorized users can restore the BEKs to the key vault and recover the encrypted VMs. Only users with the necessary level of permissions can back up and restore encrypted VMs or keys and secrets.

# Snapshot creation

Azure Backup takes snapshots according to the backup schedule.

- **Windows VMs:** For Windows VMs, the Backup service coordinates with VSS to take an app-consistent snapshot of the VM disks. By default, Azure Backup takes a full VSS backup (it truncates the logs of application such as SQL Server at the time of backup to get application level consistent backup). If you are using a SQL Server database on Azure VM backup, then you can modify the setting to take a VSS Copy backup (to preserve logs). For more information, see [this article](#).
- **Linux VMs:** To take app-consistent snapshots of Linux VMs, use the Linux pre-script and post-script framework to write your own custom scripts to ensure consistency.
  - Azure Backup invokes only the pre/post scripts written by you.
  - If the pre-scripts and post-scripts execute successfully, Azure Backup marks the recovery point as application-consistent. However, when you're using custom scripts, you're ultimately responsible for the application consistency.
  - [Learn more](#) about how to configure scripts.

## Snapshot consistency

The following table explains the different types of snapshot consistency:

| SNAPSHOT                      | DETAILS                                                                                                                                                                                                               | RECOVERY                                                                                                                                                                                                                    | CONSIDERATION                                                                                            |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| <b>Application-consistent</b> | App-consistent backups capture memory content and pending I/O operations. App-consistent snapshots use a VSS writer (or pre/post scripts for Linux) to ensure the consistency of the app data before a backup occurs. | When you're recovering a VM with an app-consistent snapshot, the VM boots up. There's no data corruption or loss. The apps start in a consistent state.                                                                     | Windows: All VSS writers succeeded<br><br>Linux: Pre/post scripts are configured and succeeded           |
| <b>File-system consistent</b> | File-system consistent backups provide consistency by taking a snapshot of all files at the same time.                                                                                                                | When you're recovering a VM with a file-system consistent snapshot, the VM boots up. There's no data corruption or loss. Apps need to implement their own "fix-up" mechanism to make sure that restored data is consistent. | Windows: Some VSS writers failed<br><br>Linux: Default (if pre/post scripts aren't configured or failed) |

| Snapshot                | Details                                                                                                                                                                                    | Recovery                                                                                                                                                                                                                                                                                                                                                                                                                                                | Consideration                                   |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| <b>Crash-consistent</b> | Crash-consistent snapshots typically occur if an Azure VM shuts down at the time of backup. Only the data that already exists on the disk at the time of backup is captured and backed up. | Starts with the VM boot process followed by a disk check to fix corruption errors. Any in-memory data or write operations that weren't transferred to disk before the crash are lost. Apps implement their own data verification. For example, a database app can use its transaction log for verification. If the transaction log has entries that aren't in the database, the database software rolls transactions back until the data is consistent. | VM is in shutdown (stopped/ deallocated) state. |

## Backup and restore considerations

| Consideration            | Details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Disk</b>              | Backup of VM disks is parallel. For example, if a VM has four disks, the Backup service attempts to back up all four disks in parallel. Backup is incremental (only changed data).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Scheduling</b>        | To reduce backup traffic, back up different VMs at different times of the day and make sure the times don't overlap. Backing up VMs at the same time causes traffic jams.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Preparing backups</b> | Keep in mind the time needed to prepare the backup. The preparation time includes installing or updating the backup extension and triggering a snapshot according to the backup schedule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Data transfer</b>     | <p>Consider the time needed for Azure Backup to identify the incremental changes from the previous backup.</p> <p>In an incremental backup, Azure Backup determines the changes by calculating the checksum of the block. If a block is changed, it's marked for transfer to the vault. The service analyzes the identified blocks to attempt to further minimize the amount of data to transfer. After evaluating all the changed blocks, Azure Backup transfers the changes to the vault.</p> <p>There might be a lag between taking the snapshot and copying it to vault.</p> <p>At peak times, it can take up to eight hours for backups to be processed. The backup time for a VM will be less than 24 hours for the daily backup.</p> |
| <b>Initial backup</b>    | Although the total backup time for incremental backups is less than 24 hours, that might not be the case for the first backup. The time needed for the initial backup will depend on the size of the data and when the backup is processed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| CONSIDERATION        | DETAILS                                                                                                                                                                                                                                                                                                                               |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Restore queue</b> | Azure Backup processes restore jobs from multiple storage accounts at the same time, and it puts restore requests in a queue.                                                                                                                                                                                                         |
| <b>Restore copy</b>  | <p>During the restore process, data is copied from the vault to the storage account.</p> <p>The total restore time depends on the I/O operations per second (IOPS) and the throughput of the storage account.</p> <p>To reduce the copy time, select a storage account that isn't loaded with other application writes and reads.</p> |

## Backup performance

These common scenarios can affect the total backup time:

- **Adding a new disk to a protected Azure VM:** If a VM is undergoing incremental backup and a new disk is added, the backup time will increase. The total backup time might last more than 24 hours because of initial replication of the new disk, along with delta replication of existing disks.
- **Fragmented disks:** Backup operations are faster when disk changes are contiguous. If changes are spread out and fragmented across a disk, backup will be slower.
- **Disk churn:** If protected disks that are undergoing incremental backup have a daily churn of more than 200 GB, backup can take a long time (more than eight hours) to complete.
- **Backup versions:** The latest version of Backup (known as the Instant Restore version) uses a more optimized process than checksum comparison for identifying changes. But if you're using Instant Restore and have deleted a backup snapshot, the backup switches to checksum comparison. In this case, the backup operation will exceed 24 hours (or fail).

## Best practices

When you're configuring VM backups, we suggest following these practices:

- Modify the default schedule times that are set in a policy. For example, if the default time in the policy is 12:00 AM, increment the timing by several minutes so that resources are optimally used.
- If you're restoring VMs from a single vault, we highly recommend that you use different [general-purpose v2 storage accounts](#) to ensure that the target storage account doesn't get throttled. For example, each VM must have a different storage account. For example, if 10 VMs are restored, use 10 different storage accounts.
- For backup of VMs that are using premium storage, with Instant Restore, we recommend allocating 50% free space of the total allocated storage space, which is required **only** for the first backup. The 50% free space is not a requirement for backups after the first backup is complete
- The limit on the number of disks per storage account is relative to how heavily the disks are being accessed by applications that are running on an infrastructure as a service (IaaS) VM. As a general practice, if 5 to 10 disks or more are present on a single storage account, balance the load by moving some disks to separate storage accounts.

## Backup costs

Azure VMs backed up with Azure Backup are subject to [Azure Backup pricing](#).

Billing doesn't start until the first successful backup finishes. At this point, the billing for both storage and protected VMs begins. Billing continues as long as any backup data for the VM is stored in a vault. If you stop protection for a VM, but backup data for the VM exists in a vault, billing continues.

Billing for a specified VM stops only if the protection is stopped and all backup data is deleted. When protection stops and there are no active backup jobs, the size of the last successful VM backup becomes the protected instance size used for the monthly bill.

The protected-instance size calculation is based on the *actual* size of the VM. The VM's size is the sum of all the data in the VM, excluding the temporary storage. Pricing is based on the actual data that's stored on the data disks, not on the maximum supported size for each data disk that's attached to the VM.

Similarly, the backup storage bill is based on the amount of data that's stored in Azure Backup, which is the sum of the actual data in each recovery point.

For example, take an A2-Standard-sized VM that has two additional data disks with a maximum size of 32 TB each. The following table shows the actual data stored on each of these disks:

| DISK                 | MAX SIZE | ACTUAL DATA PRESENT            |
|----------------------|----------|--------------------------------|
| OS disk              | 32 TB    | 17 GB                          |
| Local/temporary disk | 135 GB   | 5 GB (not included for backup) |
| Data disk 1          | 32 TB    | 30 GB                          |
| Data disk 2          | 32 TB    | 0 GB                           |

The actual size of the VM in this case is  $17 \text{ GB} + 30 \text{ GB} + 0 \text{ GB} = 47 \text{ GB}$ . This protected-instance size (47 GB) becomes the basis for the monthly bill. As the amount of data in the VM grows, the protected-instance size used for billing changes to match.

## Next steps

Now, [prepare for Azure VM backup](#).

# Get improved backup and restore performance with Azure Backup Instant Restore capability

1/23/2020 • 7 minutes to read • [Edit Online](#)

## NOTE

Based on feedback from users we are renaming **VM backup stack V2** to **Instant Restore** to reduce confusion with Azure Stack functionality. All the Azure backup users have now been upgraded to **Instant Restore**.

The new model for Instant Restore provides the following feature enhancements:

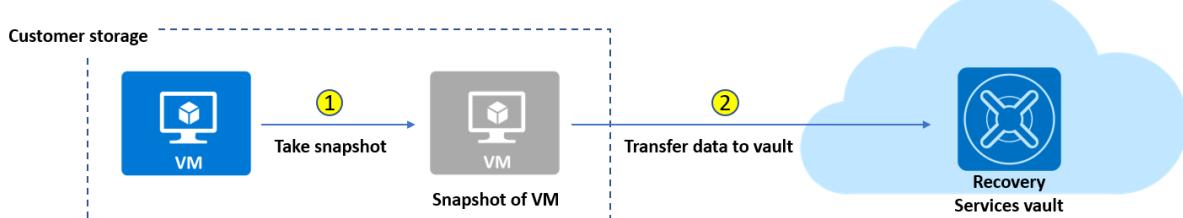
- Ability to use snapshots taken as part of a backup job that is available for recovery without waiting for data transfer to the vault to finish. It reduces the wait time for snapshots to copy to the vault before triggering restore.
- Reduces backup and restore times by retaining snapshots locally, for two days by default. This default snapshot retention value is configurable to any value between 1 to 5 days.
- Supports disk sizes up to 32 TB. Resizing of disks is not recommended by Azure Backup.
- Supports Standard SSD disks along with Standard HDD disks and Premium SSD disks.
- Ability to use an unmanaged VMs original storage accounts (per disk), when restoring. This ability exists even when the VM has disks that are distributed across storage accounts. It speeds up restore operations for a wide variety of VM configurations.
- For backup of VMs that are using premium storage, with Instant Restore, we recommend allocating 50% free space of the total allocated storage space, which is required **only** for the first backup. The 50% free space is not a requirement for backups after the first backup is complete.

## What's new in this feature

Currently, the backup job consists of two phases:

1. Taking a VM snapshot.
2. Transferring a VM snapshot to the Azure Recovery Services vault.

A recovery point is considered created only after phases 1 and 2 are completed. As a part of this upgrade, a recovery point is created as soon as the snapshot is finished and this recovery point of snapshot type can be used to perform a restore using the same restore flow. You can identify this recovery point in the Azure portal by using "snapshot" as the recovery point type, and after the snapshot is transferred to the vault, the recovery point type changes to "snapshot and vault".



By default, snapshots are retained for two days. This feature allows restore operation from these snapshots there

by cutting down the restore times. It reduces the time that is required to transform and copy data back from the vault.

## Feature considerations

- Snapshots are stored along with the disks to boost recovery point creation and to speed up restore operations. As a result, you'll see storage costs that correspond to snapshots taken during this period.
- Incremental snapshots are stored as page blobs. All the users using unmanaged disks are charged for the snapshots stored in their local storage account. Since the restore point collections used by Managed VM backups use blob snapshots at the underlying storage level, for managed disks you will see costs corresponding to blob snapshot pricing and they are incremental.
- For premium storage accounts, the snapshots taken for instant recovery points count towards the 10-TB limit of allocated space.
- You get an ability to configure the snapshot retention based on the restore needs. Depending on the requirement, you can set the snapshot retention to a minimum of one day in the backup policy blade as explained below. This will help you save cost for snapshot retention if you don't perform restores frequently.
- It is a one directional upgrade, once upgraded to Instant restore, you cannot go back.

### NOTE

With this instant restore upgrade, the snapshot retention duration of all the customers (**new and existing both included**) will be set to a default value of two days. However, you can set the duration as per your requirement to any value between 1 to 5 days.

## Cost impact

The incremental snapshots are stored in the VM's storage account, which is used for instant recovery. Incremental snapshot means the space occupied by a snapshot is equal to the space occupied by pages that are written after the snapshot was created. Billing is still for the per GB used space occupied by the snapshot, and the price per GB is same as mentioned on the [pricing page](#). For VMs that use unmanaged disks, the snapshots can be seen in the menu for the VHD file of each disk. For managed disks, snapshots are stored in a restore point collection resource in a designated resource group, and the snapshots themselves are not directly visible.

### NOTE

Snapshot retention is fixed to 5 days for weekly policies.

## Configure snapshot retention

### Using Azure portal

In the Azure portal, you can see a field added in the **VM Backup Policy** blade under the **Instant Restore** section. You can change the snapshot retention duration from the **VM Backup Policy** blade for all the VMs associated with the specific backup policy.

Home > Recovery Services vaults > sogupcreatevmvault - Backup policies > DefaultPolicy

## DefaultPolicy

Associated items Delete Save Discard

Backup schedule

\* Frequency \* Time \* Timezone  
Daily 1:30 AM (UTC-11:00) Coordinated Universal ...

**Instant Restore**

Retain instant recovery snapshot(s) for  
2 Day(s)

**Retention range**

Retention of daily backup point.

\* At For  
1:30 AM 30 Day(s)

Retention of weekly backup point.

Not Configured

Retention of monthly backup point.

Not Configured

## Using PowerShell

### NOTE

From Az PowerShell version 1.6.0 onwards, you can update the instant restore snapshot retention period in policy using PowerShell

```
$bkpPol = Get-AzureRmRecoveryServicesBackupProtectionPolicy -WorkloadType "AzureVM"
$bkpPol.SnapshotRetentionInDays=5
Set-AzureRmRecoveryServicesBackupProtectionPolicy -policy $bkpPol
```

The default snapshot retention for each policy is set to two days. User can change the value to a minimum of 1 and a maximum of five days. For weekly policies, the snapshot retention is fixed to five days.

## Frequently asked questions

### What are the cost implications of Instant restore?

Snapshots are stored along with the disks to speed up recovery point creation and restore operations. As a result, you'll see storage costs that correspond to the snapshot retention selected as a part of VM backup policy.

### In Premium Storage accounts, do the snapshots taken for instant recovery point occupy the 10-TB snapshot limit?

Yes, for premium storage accounts the snapshots taken for instant recovery point occupy 10 TB of allocated snapshot space.

### How does the snapshot retention work during the five-day period?

Each day a new snapshot is taken, then there are five individual incremental snapshots. The size of the snapshot depends on the data churn, which are in most cases around 2%-7%.

### Is an instant restore snapshot an incremental snapshot or full snapshot?

Snapshots taken as a part of instant restore capability are incremental snapshots.

### **How can I calculate the approximate cost increase due to instant restore feature?**

It depends on the churn of the VM. In a steady state, you can assume the increase in cost is = Snapshot retention period daily churn per VM storage cost per GB.

### **If the recovery type for a restore point is "Snapshot and vault" and I perform a restore operation, which recovery type will be used?**

If the recovery type is "snapshot and vault", restore will be automatically done from the local snapshot, which will be much faster compared to the restore done from the vault.

### **What happens if I select retention period of restore point (Tier 2) less than the snapshot (Tier1) retention period?**

The new model does not allow deleting the restore point (Tier2) unless the snapshot (Tier1) is deleted. We recommend scheduling restore point (Tier2) retention period greater than the snapshot retention period.

### **Why is my snapshot existing even after the set retention period in backup policy?**

If the recovery point has snapshot and that is the latest RP available, it is retained until the time there is a next successful backup. This is as per the designed "garbage collection" (GC) policy today that mandates at least one latest RP to be always present in case all backups further on fail due to an issue in the VM. In normal scenarios, RPs are cleaned up in maximum of 24 hours after their expiry.

### **I don't need Instant Restore functionality. Can it be disabled?**

Instant restore feature is enabled for everyone and cannot be disabled. You can reduce the snapshot retention to a minimum of one day.

#### **NOTE**

#### **Azure Backup now supports selective disk backup and restore using the Azure Virtual Machine backup solution.**

Today, Azure Backup supports backing up all the disks (Operating System and data) in a VM together using the Virtual Machine backup solution. With exclude-disk functionality, you get an option to backup one or a few from the many data disks in a VM. This provides an efficient and cost-effective solution for your backup and restore needs. Each recovery point contains data of the disks included in the backup operation, which further allows you to have a subset of disks restored from the given recovery point during the restore operation. This applies to restore both from the snapshot and the vault.

\*\*To sign up for the preview, write to us at [AskAzureBackupTeam@microsoft.com](mailto:AskAzureBackupTeam@microsoft.com)\*\*

# Enable backup when you create an Azure VM

12/18/2019 • 3 minutes to read • [Edit Online](#)

Use the Azure Backup service to back up Azure virtual machines (VMs). VMs are backed up according to a schedule specified in a backup policy, and recovery points are created from backups. Recovery points are stored in Recovery Services vaults.

This article details how to enable backup when you create a virtual machine (VM) in the Azure portal.

## Before you start

- [Check](#) which operating systems are supported if you enable backup when you create a VM.

## Sign in to Azure

If you aren't already signed in to your account, sign in to the [Azure portal](#).

## Create a VM with Backup configured

1. In Azure portal, click **Create a resource**.
2. In the Azure Marketplace, click **Compute**, and then select a VM image.
3. Set up the VM in accordance with the [Windows](#) or [Linux](#) instructions.
4. On the **Management** tab, in **Enable backup**, click **On**.
5. Azure Backup backups to a Recovery Services vault. Click **Create New** if you don't have an existing vault.
6. Accept the suggested vault name or specify your own.
7. Specify or create a resource group in which the vault will be located. The resource group vault can be different from the VM resource group.

## Create a virtual machine

### BACKUP

Enable backup [i](#)

On  Off

\* Recovery Services vault [i](#)

Create new  Use existing

vault508

\* Resource group

(New) 123

[Create new](#)

\* Backup policy

(new) DailyPolicy

[Create new](#)

[Review + create](#)

[Previous](#)

[Next : Advanced >](#)

8. Accept the default backup policy, or modify the settings.

- A backup policy specifies how frequently to take backup snapshots of the VM, and how long to keep those backup copies.
- The default policy backs up the VM once a day.
- You can customize your own backup policy for an Azure VM to take backups daily or weekly.
- [Learn more](#) about backup considerations for Azure VMs.
- [Learn more](#) about the instant restore functionality.

## Backup policy

\* Policy name i

### Backup schedule

\* Frequency

\* Time

\* Timezone

### Instant Restore i

Retain instant recovery snapshot(s) for

 Day(s)

### Retention range

Retention of daily backup point.

\* At

For

 Day(s)

Retention of weekly backup point.

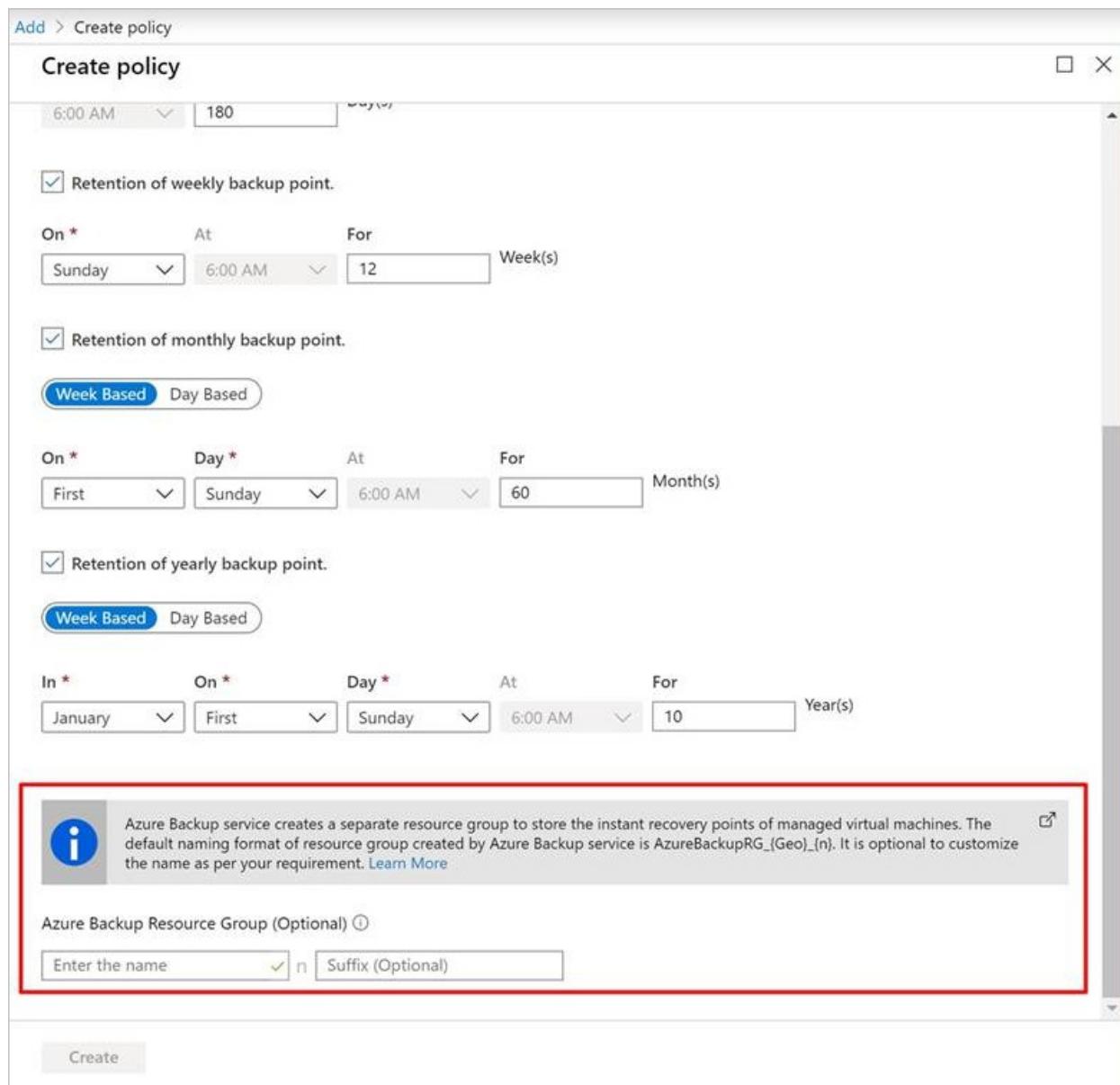
Not Configured

## Azure Backup resource group for Virtual Machines

The Backup service creates a separate resource group (RG), different than the resource group of the VM to store the restore point collection (RPC). The RPC houses the instant recovery points of managed VMs. The default naming format of the resource group created by the Backup service is: `AzureBackupRG_<Geo>_<number>`. For example: `AzureBackupRG_northeurope_1`. You now can customize the Resource group name created by Azure Backup.

Points to note:

1. You can either use the default name of the RG, or edit it according to your company requirements.
2. You provide the RG name pattern as input during VM backup policy creation. The RG name should be of the following format: `<alpha-numeric string>* n <alpha-numeric string>`. 'n' is replaced with an integer (starting from 1) and is used for scaling out if the first RG is full. One RG can have a max of 600 RPCs today.



3. The pattern should follow the RG naming rules below and the total length should not exceed the maximum allowed RG name length.
  - a. Resource group names only allow alphanumeric characters, periods, underscores, hyphens, and parenthesis. They cannot end in a period.
  - b. Resource group names can contain up to 74 characters, including the name of the RG and the suffix.
4. The first <alpha-numeric-string> is mandatory while the second one after 'n' is optional. This applies only if you give a customized name. If you don't enter anything in either of the textboxes, the default name is used.
5. You can edit the name of the RG by modifying the policy if and when required. If the name pattern is changed, new RPs will be created in the new RG. However, the old RPs will still reside in the old RG and won't be moved, as RP Collection does not support resource move. Eventually the RPs will get garbage collected as the points expire.

**DefaultPolicy**

Associated items Delete Save Discard

Frequency \* Time \* Timezone \*

Daily 1:30 AM (UTC-11:00) Coordinated Universal Time-11

Instant Restore ⓘ

Retain instant recovery snapshot(s) for 4 Day(s)

Retention range

Retention of daily backup point.

At For 1:30 AM 30 Day(s)

Retention of weekly backup point.

Not Configured

Retention of monthly backup point.

Not Configured

Retention of yearly backup point.

Not Configured

Azure Backup service creates a separate resource group to store the instant recovery points of managed virtual machines. The default naming format of resource group created by Azure Backup service is AzureBackupRG\_{Geo}\_{In}. It is optional to customize the name as per your requirement. [Learn More](#)

Azure Backup Resource Group (Optional)

Enter the name Suffix (Optional)

6. It is advised to not lock the resource group created for use by the Backup service.

## Start a backup after creating the VM

Your VM backup will run in accordance with your backup policy. However, we recommend that you run an initial backup.

After the VM is created, do the following:

1. In the VM properties, click **Backup**. The VM status is Initial Backup Pending until the initial backup runs
2. Click **Back up now** to run an on-demand backup.

| Alerts and Jobs                                                                                                                          |                          | Backup status                                                  | Summary                                                           |
|------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|----------------------------------------------------------------|-------------------------------------------------------------------|
| <a href="#">View all Alerts (last 24 hours)</a>                                                                                          |                          | Backup Pre-Check <span style="color: green;">Passed</span>     | Recovery service: <span style="color: blue;">Backup policy</span> |
| <a href="#">View all Jobs (last 24 hours)</a>                                                                                            |                          | Last backup status <span style="color: orange;">Warning</span> | Oldest restore po                                                 |
| <hr/>                                                                                                                                    |                          |                                                                |                                                                   |
| Restore points                                                                                                                           |                          |                                                                |                                                                   |
| This list is filtered for last 30 days of restore points. To recover from restore point older than 30 days, <a href="#">click here</a> . |                          |                                                                |                                                                   |
| CRASH CONSISTENT 0                                                                                                                       | APPLICATION CONSISTENT 0 | FILE-SYSTEM CONSISTENT 0                                       |                                                                   |
| TIME ↑                                                                                                                                   | CONSISTENCY ↑            | RECOVERY TYPE ↑                                                |                                                                   |
| No restore points available.                                                                                                             |                          |                                                                |                                                                   |

## Use a Resource Manager template to deploy a protected VM

The previous steps explain how to use the Azure portal to create a virtual machine and protect it in a Recovery Services vault. To quickly deploy one or more VMs and protect them in a Recovery Services vault, see the template [Deploy a Windows VM and enable backup](#).

## Next steps

Now that you've protected your VM, learn how to manage and restore them.

- [Manage and monitor VMs](#)
- [Restore VM](#)

If you encounter any issues, [review](#) the troubleshooting guide.

# Back up an Azure VM from the VM settings

1/23/2020 • 3 minutes to read • [Edit Online](#)

This article explains how to back up Azure VMs with the [Azure Backup](#) service. You can back up Azure VMs using a couple of methods:

- Single Azure VM: The instructions in this article describe how to back up an Azure VM directly from the VM settings.
- Multiple Azure VMs: You can set up a Recovery Services vault and configure backup for multiple Azure VMs. Follow the instructions in [this article](#) for this scenario.

## Before you start

1. [Learn](#) how backup works, and [verify](#) support requirements.
2. [Get an overview](#) of Azure VM backup.

### Azure VM agent installation

In order to back up Azure VMs, Azure Backup installs an extension on the VM agent running on the machine. If your VM was created from an Azure marketplace image, the agent will be running. In some cases, for example if you create a custom VM, or you migrate a machine from on-premises, you might need to install the agent manually.

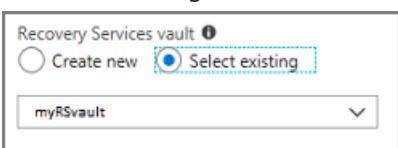
- If you do need to install the VM agent manually, follow the instructions for [Windows](#) or [Linux](#) VMs.
- After the agent is installed, when you enable backup, Azure Backup installs the backup extension to the agent. It updates and patches the extension without user intervention.

## Back up from Azure VM settings

1. Sign in to the [Azure portal](#).
2. Click **All services** and in the Filter, type **Virtual machines**, and then click **Virtual machines**.
3. From the list of VMs select the VM you want to back up.
4. On the VM menu, click **Backup**.

### 5. In **Recovery Services vault**, do the following:

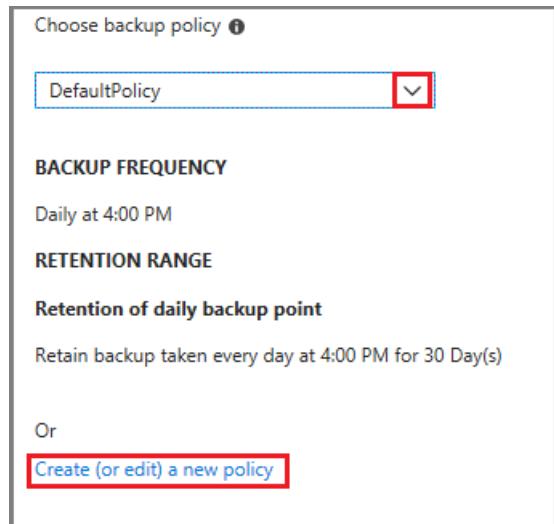
- If you already have a vault, click **Select existing**, and select a vault.
- If you don't have a vault, click **Create new**. Specify a name for the vault. It's created in the same region and resource group as the VM. You can't modify these settings when you enable backup directly from the VM settings.



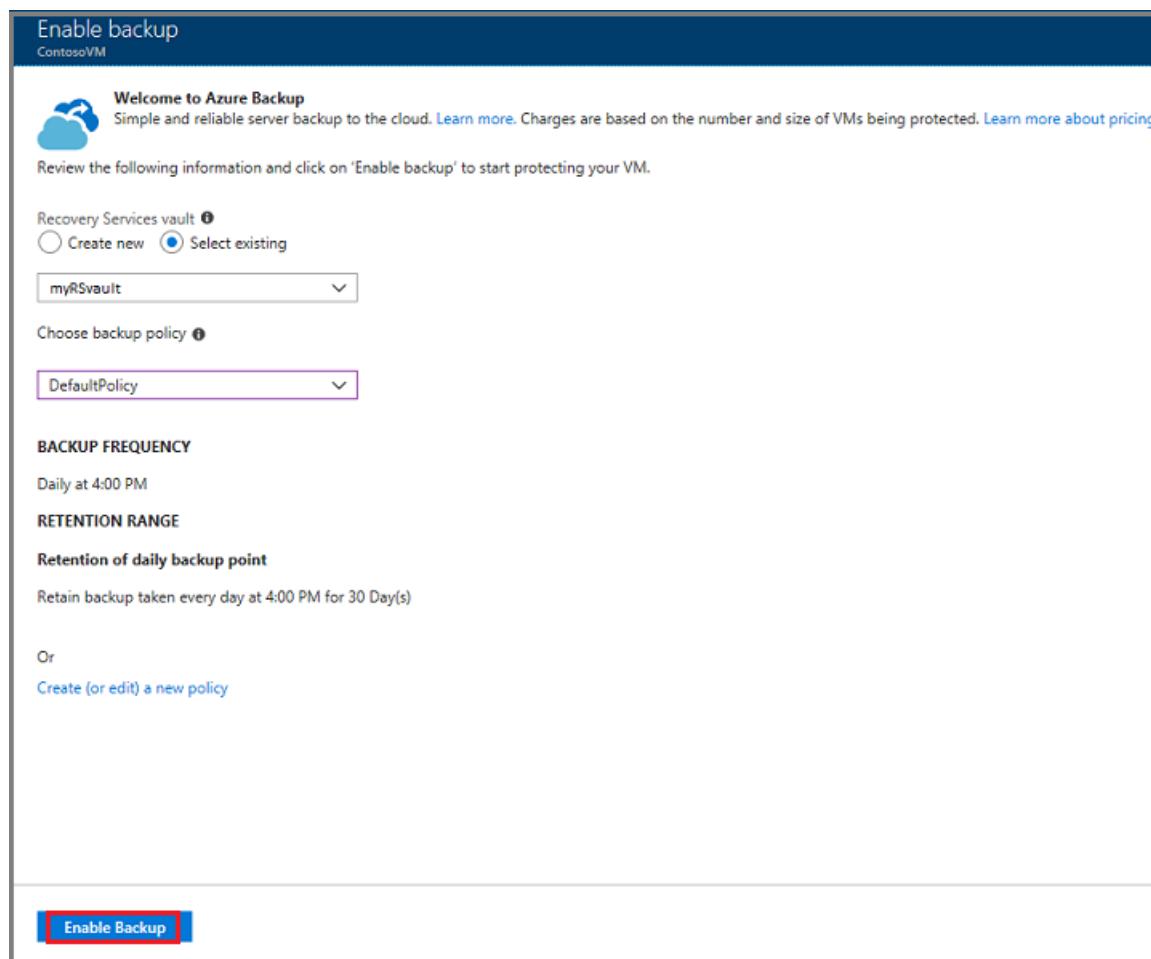
### 6. In **Choose backup policy**, do the following:

- Leave the default policy. This backs up the VM once a day at the time specified, and retains backups in the vault for 30 days.
- Select an existing backup policy if you have one.

- Create a new policy, and define the policy settings.



7. Click **Enable Backup**. This associates the backup policy with the VM.



8. You can track the configuration progress in the portal notifications.

9. After the job completes, in the VM menu, click **Backup**. The page shows backup status for the VM, information about recovery points, jobs running, and alerts issued.

ContosoVM - Backup

Virtual machine

Search (Ctrl+ /)

Backup now | Restore VM | File Recovery | Stop backup | Resume backup | Delete backup data

Properties | Locks | Automation script

Operations

- Auto-shutdown
- Backup**
- Disaster recovery (Preview)
- Update management
- Inventory
- Change tracking

Monitoring

- Metrics
- Alerts (classic)
- Diagnostics settings
- Advisor recommendations
- Diagram

Alerts and Jobs

Backup status

Backup Pre-Check: Passed

Last backup status: Warning(Initial backup pending)

Summary

Recovery services vault: myRSVault

Backup policy: DailyPolicy

Oldest restore point: -

Restore points

This list is filtered for last 30 days of restore points. To recover from restore point older than 30 days, click here.

CRASH CONSISTENT: 0 | APPLICATION CONSISTENT: 0 | FILE-SYSTEM CONSISTENT: 0

TIME | CONSISTENCY | RECOVERY TYPE

No restore points available.

- After enabling backup, an initial backup runs. You can start the initial backup immediately, or wait until it starts in accordance with the backup schedule.
  - Until the initial backup completes, the **Last backup status** shows as **Warning (Initial backup pending)**.
  - To see when the next scheduled backup will run, click the backup policy name.

## Run a backup immediately

- To run a backup immediately, in the VM menu, click **Backup > Backup now**.

ContosoVM - Backup

Virtual machine

Search (Ctrl+ /)

**Backup now** | Restore VM | File Recovery | Stop backup | Resume backup | Delete backup data

Properties | Locks | Automation script

Alerts and Jobs

Backup status

Backup Pre-Check: Passed

Last backup status: Warning(Initial backup pending)

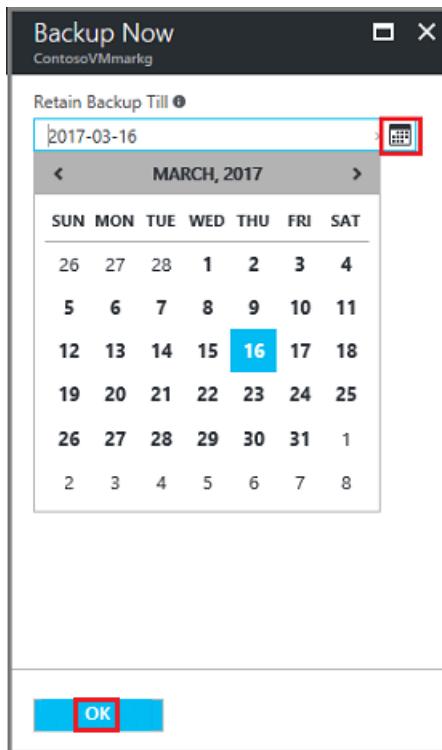
Summary

Recovery service

Backup policy

Oldest restore p

- In **Backup Now** use the calendar control to select until when the recovery point will be retained > and **OK**.



3. Portal notifications let you know the backup job has been triggered. To monitor backup progress, click **View all jobs**.

## Back up from the Recovery Services vault

Follow the instructions in this article to enable backup for Azure VMs by setting up an Azure Backup Recovery Services vault, and enabling backup in the vault.

### NOTE

**Azure Backup now supports selective disk backup and restore using the Azure Virtual Machine backup solution.**

Today, Azure Backup supports backing up all the disks (Operating System and data) in a VM together using the Virtual Machine backup solution. With exclude-disk functionality, you get an option to backup one or a few from the many data disks in a VM. This provides an efficient and cost-effective solution for your backup and restore needs. Each recovery point contains data of the disks included in the backup operation, which further allows you to have a subset of disks restored from the given recovery point during the restore operation. This applies to restore both from the snapshot and the vault.

\*\*To sign up for the preview, write to us at [AskAzureBackupTeam@microsoft.com](mailto:AskAzureBackupTeam@microsoft.com)\*\*

## Next steps

- If you have difficulties with any of the procedures in this article, consult the [troubleshooting guide](#).
- [Learn about](#) managing your backups.

# Back up Azure VMs in a Recovery Services vault

1/23/2020 • 8 minutes to read • [Edit Online](#)

This article describes how to back up Azure VMs in a Recovery Services vault, using the [Azure Backup](#) service.

In this article, you learn how to:

- Prepare Azure VMs.
- Create a vault.
- Discover VMs and configure a backup policy.
- Enable backup for Azure VMs.
- Run the initial backup.

## NOTE

This article describes how to set up a vault and select VMs to back up. It's useful if you want to back up multiple VMs.

Alternatively, you can [back up a single Azure VM](#) directly from the VM settings.

## Before you start

- [Review](#) the Azure VM backup architecture.
- [Learn about](#) Azure VM backup, and the backup extension.
- [Review the support matrix](#) before you configure backup.

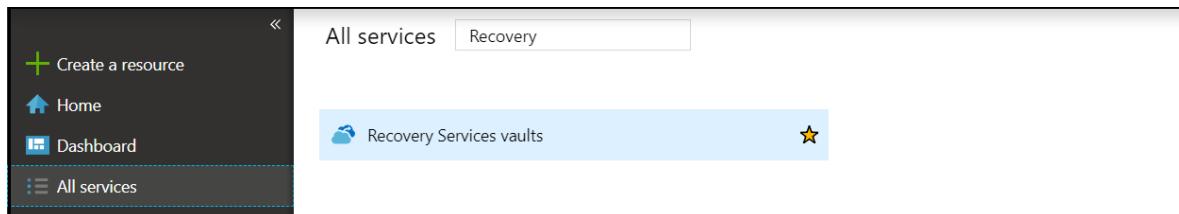
In addition, there are a couple of things that you might need to do in some circumstances:

- **Install the VM agent on the VM:** Azure Backup backs up Azure VMs by installing an extension to the Azure VM agent running on the machine. If your VM was created from an Azure marketplace image, the agent is installed and running. If you create a custom VM, or you migrate an on-premises machine, you might need to [install the agent manually](#).

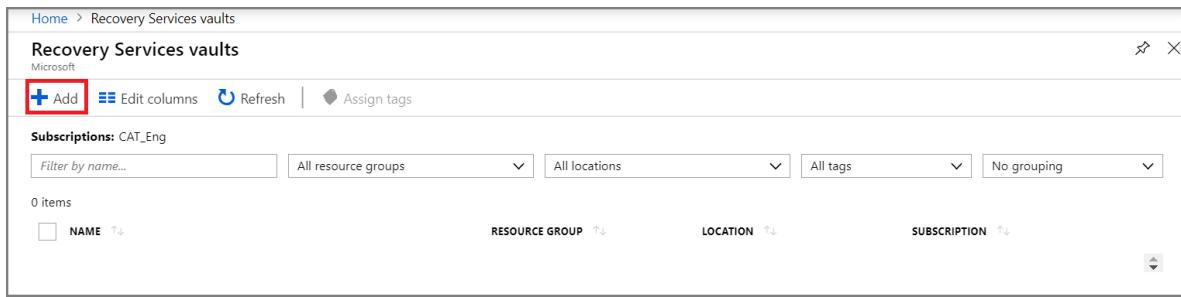
## Create a vault

A vault stores backups and recovery points created over time, and stores backup policies associated with backed up machines. Create a vault as follows:

1. Sign in to the [Azure portal](#).
2. In search, type **Recovery Services**. Under **Services**, click **Recovery Services vaults**.



3. In **Recovery Services vaults** menu, click **+Add**.



4. In **Recovery Services vault**, type in a friendly name to identify the vault.

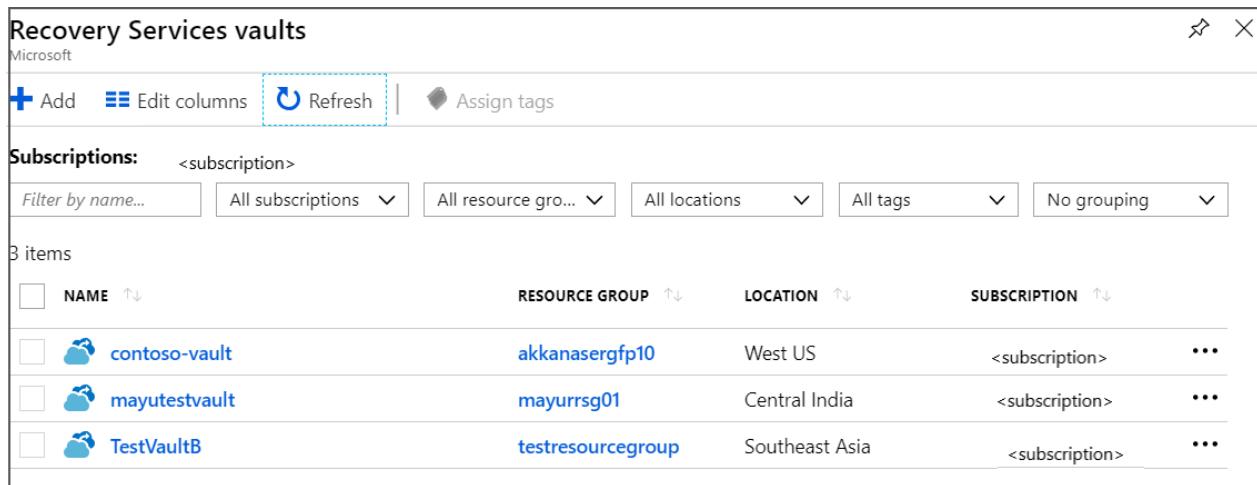
- The name needs to be unique for the Azure subscription.
- It can contain 2 to 50 characters.
- It must start with a letter, and it can contain only letters, numbers, and hyphens.

5. Select the Azure subscription, resource group, and geographic region in which the vault should be created.

Then click **Create**.

- It can take a while for the vault to be created.
- Monitor the status notifications in the upper-right area of the portal.

After the vault is created, it appears in the Recovery Services vaults list. If you don't see your vault, select **Refresh**.



| NAME          | RESOURCE GROUP    | LOCATION       | SUBSCRIPTION   | ... |
|---------------|-------------------|----------------|----------------|-----|
| contoso-vault | akkanasergfp10    | West US        | <subscription> | ... |
| mayutestvault | mayurrg01         | Central India  | <subscription> | ... |
| TestVaultB    | testresourcegroup | Southeast Asia | <subscription> | ... |

#### NOTE

Azure Backup now allows customization of the resource group name created by the Azure Backup service. For more information, see [Azure Backup resource group for Virtual Machines](#).

## Modify storage replication

By default, vaults use **geo-redundant storage (GRS)**.

- If the vault is your primary backup mechanism, we recommend you use GRS.
- You can use **locally-redundant storage (LRS)** for a cheaper option.

Modify storage replication type as follows:

1. In the new vault, click **Properties** in the **Settings** section.
2. In **Properties**, under **Backup Configuration**, click **Update**.
3. Select the storage replication type, and click **Save**.

**DemoVault - Properties**

**Backup Configuration**

Status: Active

Location: Central India

Subscription Name: [redacted]

Subscription ID: [redacted]

Resource Group: mayursg01

**DIAGNOSTICS SETTINGS**

[Update](#)

**BACkUP**

**Backup Configuration** (highlighted with a red box)

[Update](#)

Security Settings

[Update](#)

#### NOTE

You can't modify the storage replication type after the vault is set up and contains backup items. If you want to do this you need to recreate the vault.

## Apply a backup policy

Configure a backup policy for the vault.

1. In the vault, click **+Backup** in the **Overview** section.

**Test4FFinVM**

**Recovery Services vault**

**Backup** (highlighted with a red box)

**Replicate**

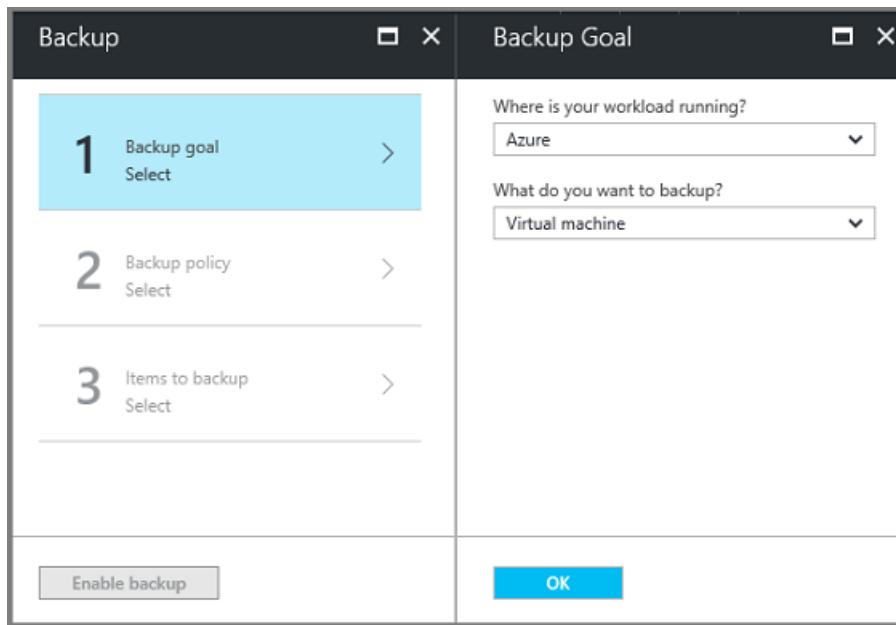
**Delete**

**Essentials**

Resource group (change) [NewDemoRG](#)

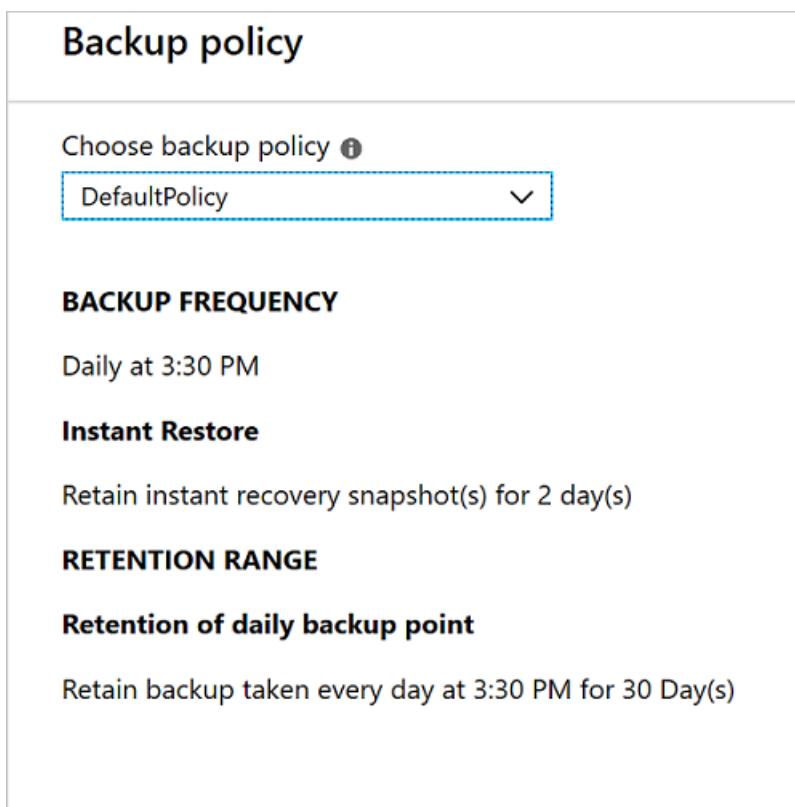
Backup items 0

2. In **Backup Goal > Where is your workload running?** select **Azure**. In **What do you want to back up?** select **Virtual machine** > **OK**. This registers the VM extension in the vault.



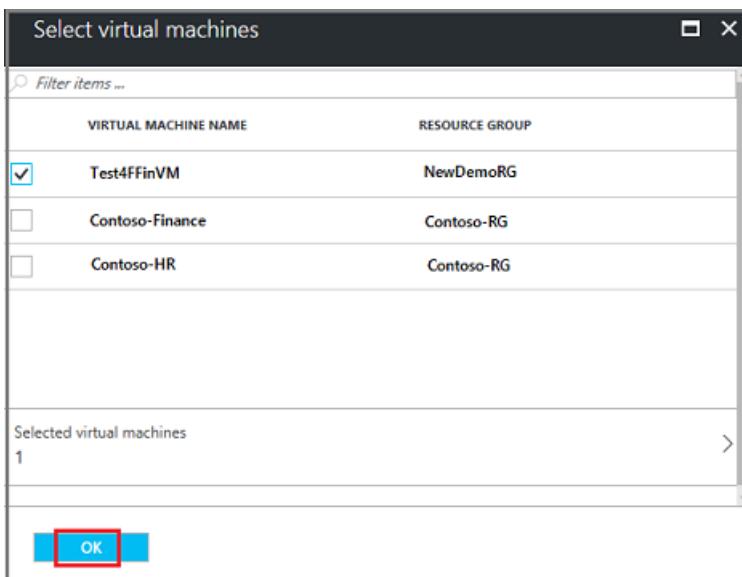
3. In **Backup policy**, select the policy that you want to associate with the vault.

- The default policy backs up the VM once a day. The daily backups are retained for 30 days. Instant recovery snapshots are retained for two days.
- If you don't want to use the default policy, select **Create New**, and create a custom policy as described in the next procedure.

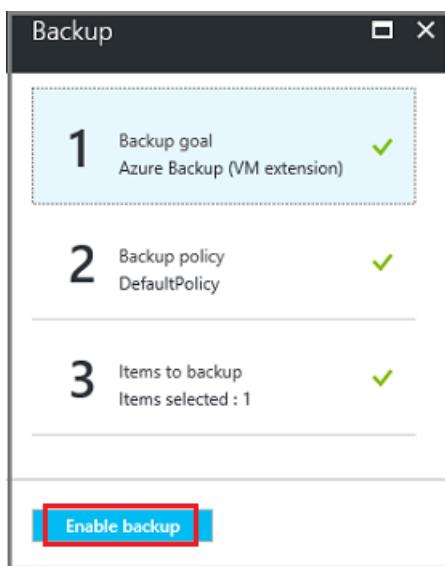


4. In **Select virtual machines**, select the VMs you want to back up using the policy. Then click **OK**.

- The selected VMs are validated.
- You can only select VMs in the same region as the vault.
- VMs can only be backed up in a single vault.



- In **Backup**, click **Enable backup**. This deploys the policy to the vault and to the VMs, and installs the backup extension on the VM agent running on the Azure VM.



After enabling backup:

- The Backup service installs the backup extension whether or not the VM is running.
- An initial backup will run in accordance with your backup schedule.
- When backups run, note that:
  - A VM that's running have the greatest chance for capturing an application-consistent recovery point.
  - However, even if the VM is turned off it's backed up. Such a VM is known as an offline VM. In this case, the recovery point will be crash-consistent.
- Explicit outbound connectivity is not required to allow backup of Azure VMs.

#### Create a custom policy

If you selected to create a new backup policy, fill in the policy settings.

- In **Policy name**, specify a meaningful name.
- In **Backup schedule**, specify when backups should be taken. You can take daily or weekly backups for Azure VMs.
- In **Instant Restore**, specify how long you want to retain snapshots locally for instant restore.
  - When you restore, backed up VM disks are copied from storage, across the network to the recovery

storage location. With instant restore, you can leverage locally-stored snapshots taken during a backup job, without waiting for backup data to be transferred to the vault.

- You can retain snapshots for instant restore for between one to five days. Two days is the default setting.

4. In **Retention range**, specify how long you want to keep your daily or weekly backup points.
5. In **Retention of monthly backup point**, specify whether you want to keep a monthly backup of your daily or weekly backups.
6. Click **OK** to save the policy.

## Backup policy

Choose backup policy i

Create New ▼

\* Policy name i

Backup schedule

\* Frequency

Daily

\* Time

10:30 PM

\* Timezone

(UTC) Coordinated Universal Time

▼

**Instant Restore** i

Retain instant recovery snapshot(s) for

2

Day(s)

**Retention range**

Retention of daily backup point.

\* At

For

10:30 PM

180

Day(s)

Retention of weekly backup point.

\* On

\* At

For

Sunday

10:30 PM

12

Week(s)

Retention of monthly backup point.

**OK**

### NOTE

Azure Backup doesn't support automatic clock adjustment for daylight-saving changes for Azure VM backups. As time changes occur, modify backup policies manually as required.

## Trigger the initial backup

The initial backup will run in accordance with the schedule, but you can run it immediately as follows:

1. In the vault menu, click **Backup items**.
2. In **Backup Items**, click **Azure Virtual Machine**.
3. In the **Backup Items** list, click the ellipses (...).
4. Click **Backup now**.
5. In **Backup Now**, use the calendar control to select the last day that the recovery point should be retained. Then click **OK**.
6. Monitor the portal notifications. You can monitor the job progress in the vault dashboard > **Backup Jobs** > **In progress**. Depending on the size of your VM, creating the initial backup may take a while.

## Verify Backup job status

The Backup job details for each VM backup consist of two phases, the **Snapshot** phase followed by the **Transfer data to vault** phase.

The snapshot phase guarantees the availability of a recovery point stored along with the disks for **Instant Restores** and are available for a maximum of five days depending on the snapshot retention configured by the user. Transfer data to vault creates a recovery point in the vault for long-term retention. Transfer data to vault only starts after the snapshot phase is completed.

| WORKLOAD NAME                  | OPERATION | STATUS    | TYPE                  | START TIME            | DURATION |
|--------------------------------|-----------|-----------|-----------------------|-----------------------|----------|
| minint-5on613p.fareast.corp... | Backup    | Completed | Files and folders     | 5/2/2019, 9:28:48 AM  | 00:02:01 |
| saphanardemo                   | Backup    | Completed | Azure virtual machine | 5/2/2019, 6:06:37 PM  | 01:26:19 |
| nopcommerceweb                 | Backup    | Completed | Azure virtual machine | 5/2/2019, 6:01:26 PM  | 01:11:25 |
| minint-5on613p.fareast.corp... | Backup    | Completed | Files and folders     | 5/2/2019, 10:15:44 AM | 00:01:44 |

There are two **Sub Tasks** running at the backend, one for front-end backup job that can be checked from the **Backup Job** details blade as given below:

**Backup**

nopcommerceweb

### Job Details

|                    |                                      |
|--------------------|--------------------------------------|
| <b>VM Name</b>     | nopcommerceweb                       |
| <b>Backup Size</b> | 607 MB                               |
| <b>Activity ID</b> | ed863617-d2f6-4069-bebf-15300fa86c65 |

### Sub Tasks

| NAME                   | STATUS      |
|------------------------|-------------|
| Take Snapshot          | ✓ Completed |
| Transfer data to vault | ✓ Completed |

The **Transfer data to vault** phase can take multiple days to complete depending on the size of the disks, churn per disk and several other factors.

Job status can vary depending on the following scenarios:

| SNAPSHOT  | TRANSFER DATA TO VAULT | JOB STATUS             |
|-----------|------------------------|------------------------|
| Completed | In progress            | In progress            |
| Completed | Skipped                | Completed              |
| Completed | Completed              | Completed              |
| Completed | Failed                 | Completed with warning |
| Failed    | Failed                 | Failed                 |

Now with this capability, for the same VM, two backups can run in parallel, but in either phase (snapshot, transfer data to vault) only one sub task can be running. So in scenarios where a backup job in progress resulted in the next day's backup to fail will be avoided with this decoupling functionality. Subsequent day's backups can have snapshot completed while **Transfer data to vault** skipped if an earlier day's backup job is in progress state. The incremental recovery point created in the vault will capture all the churn from the last recovery point created in the vault. There is no cost impact on the user.

## Optional steps

### Install the VM agent

Azure Backup backs up Azure VMs by installing an extension to the Azure VM agent running on the machine. If your VM was created from an Azure Marketplace image, the agent is installed and running. If you create a custom VM, or you migrate an on-premises machine, you might need to install the agent manually, as summarized in the table.

| VM             | DETAILS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Windows</b> | <ol style="list-style-type: none"><li>1. <a href="#">Download and install</a> the agent MSI file.</li><li>2. Install with admin permissions on the machine.</li><li>3. Verify the installation. In <code>C:\WindowsAzure\Packages</code> on the VM, right-click <b>WaAppAgent.exe</b> &gt; <b>Properties</b>. On the <b>Details</b> tab, <b>Product Version</b> should be 2.6.1198.718 or higher.<br/><br/>If you're updating the agent, make sure that no backup operations are running, and <a href="#">reinstall the agent</a>.</li></ol> |
| <b>Linux</b>   | <p>Install by using an RPM or a DEB package from your distribution's package repository. This is the preferred method for installing and upgrading the Azure Linux agent. All the <a href="#">endorsed distribution providers</a> integrate the Azure Linux agent package into their images and repositories. The agent is available on <a href="#">GitHub</a>, but we don't recommend installing from there.</p> <p>If you're updating the agent, make sure no backup operations are running, and update the binaries.</p>                  |

#### NOTE

**Azure Backup now supports selective disk backup and restore using the Azure Virtual Machine backup solution.**

Today, Azure Backup supports backing up all the disks (Operating System and data) in a VM together using the Virtual Machine backup solution. With exclude-disk functionality, you get an option to backup one or a few from the many data disks in a VM. This provides an efficient and cost-effective solution for your backup and restore needs. Each recovery point contains data of the disks included in the backup operation, which further allows you to have a subset of disks restored from the given recovery point during the restore operation. This applies to restore both from the snapshot and the vault.

\*\*To sign up for the preview, write to us at [AskAzureBackupTeam@microsoft.com](mailto:AskAzureBackupTeam@microsoft.com)\*\*

## Next steps

- Troubleshoot any issues with [Azure VM agents](#) or [Azure VM backup](#).
- [Restore](#) Azure VMs.

# Back up and restore encrypted Azure VM

2/24/2020 • 5 minutes to read • [Edit Online](#)

This article describes how to back up and restore Windows or Linux Azure virtual machines (VMs) with encrypted disks using the [Azure Backup](#) service.

If you want to learn more about how Azure Backup interacts with Azure VMs before you begin, review these resources:

- [Review](#) the Azure VM backup architecture.
- [Learn about](#) Azure VM backup, and the Azure Backup extension.

## Encryption support

Azure Backup supports backup of Azure VMs that have their OS/data disks encrypted with Azure Disk Encryption (ADE). ADE uses BitLocker for encryption of Windows VMs, and the dm-crypt feature for Linux VMs. ADE integrates with Azure Key Vault to manage disk-encryption keys and secrets. Key Vault Key Encryption Keys (KEKs) can be used to add an additional layer of security, encrypting encryption secrets before writing them to Key Vault.

Azure Backup can back up and restore Azure VMs using ADE with and without the Azure AD app, as summarized in the following table.

| VM DISK TYPE     | ADE (BEK/DM-CRYPT) | ADE AND KEK |
|------------------|--------------------|-------------|
| <b>Unmanaged</b> | Yes                | Yes         |
| <b>Managed</b>   | Yes                | Yes         |

- Learn more about [ADE](#), [Key Vault](#), and [KEKs](#).
- Read the [FAQ](#) for Azure VM disk encryption.

## Limitations

- You can back up and restore encrypted VMs within the same subscription and region.
- Azure Backup supports VMs encrypted using standalone keys. Any key that is a part of a certificate used to encrypt a VM isn't currently supported.
- You can back up and restore encrypted VMs within the same subscription and region as the Recovery Services Backup vault.
- Encrypted VMs can't be recovered at the file/folder level. You need to recover the entire VM to restore files and folders.
- When restoring a VM, you can't use the [replace existing VM](#) option for encrypted VMs. This option is only supported for unencrypted managed disks.

## Before you start

Before you start, do the following:

1. Make sure you have one or more [Windows](#) or [Linux](#) VMs with ADE enabled.
2. [Review the support matrix](#) for Azure VM backup
3. [Create](#) a Recovery Services Backup vault if you don't have one.
4. If you enable encryption for VMs that are already enabled for backup, you simply need to provide Backup with

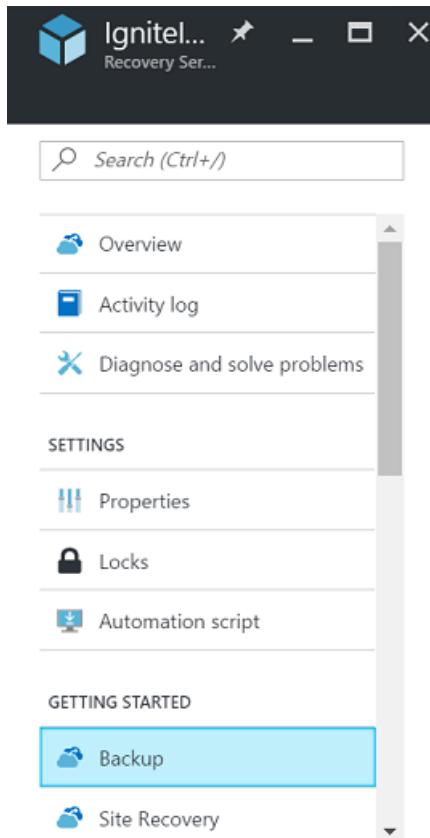
permissions to access the Key Vault so that backups can continue without disruption. [Learn more](#) about assigning these permissions.

In addition, there are a couple of things that you might need to do in some circumstances:

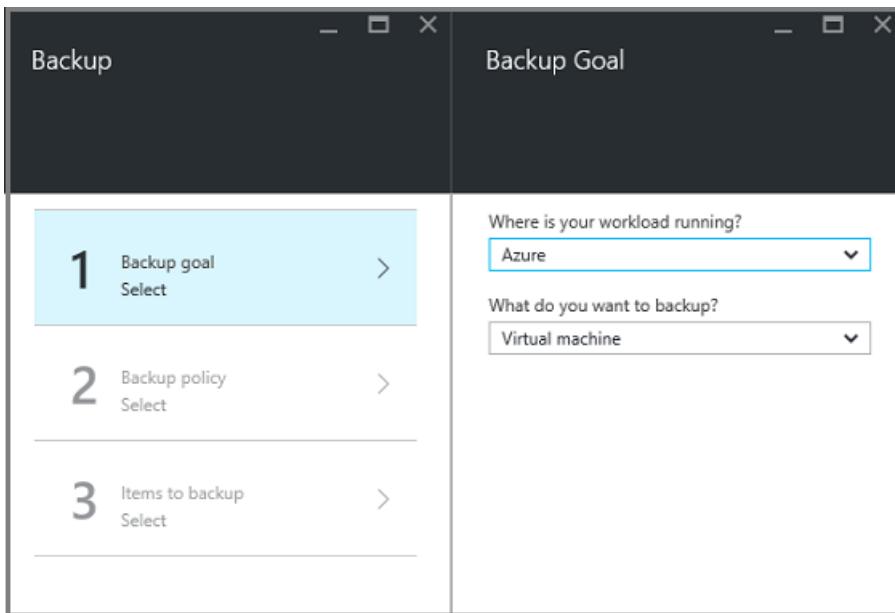
- **Install the VM agent on the VM:** Azure Backup backs up Azure VMs by installing an extension to the Azure VM agent running on the machine. If your VM was created from an Azure marketplace image, the agent is installed and running. If you create a custom VM, or you migrate an on-premises machine, you might need to [install the agent manually](#).

## Configure a backup policy

1. If you haven't yet created a Recovery Services backup vault, follow [these instructions](#)
2. Open the vault in the portal, and select **Backup** in the **Getting Started** section.

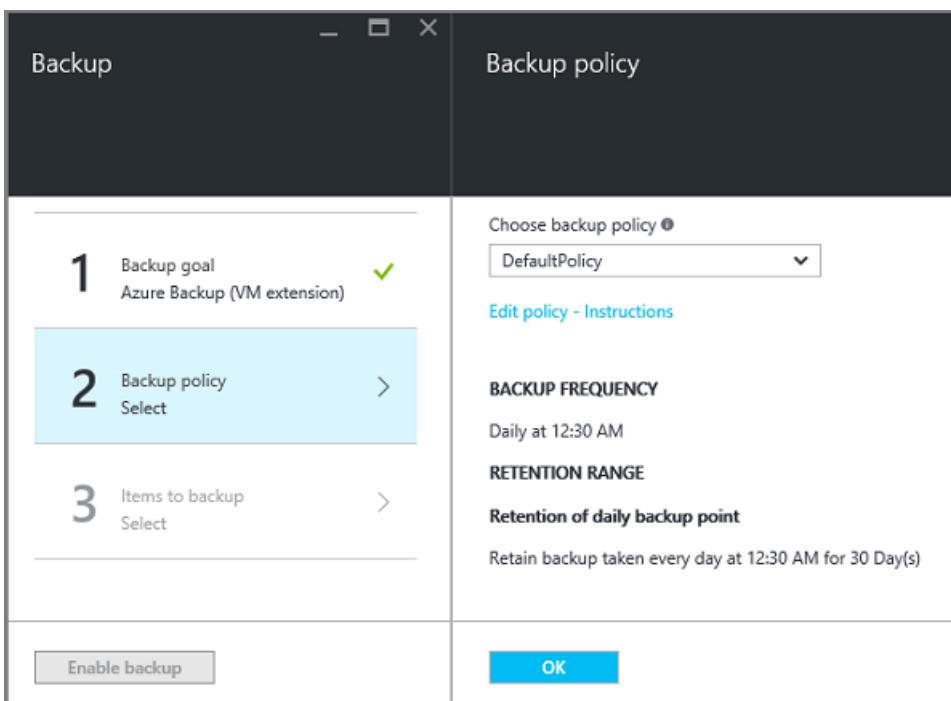


3. In **Backup goal > Where is your workload running?** select **Azure**.
4. In **What do you want to back up?** select **Virtual machine** > **OK**.

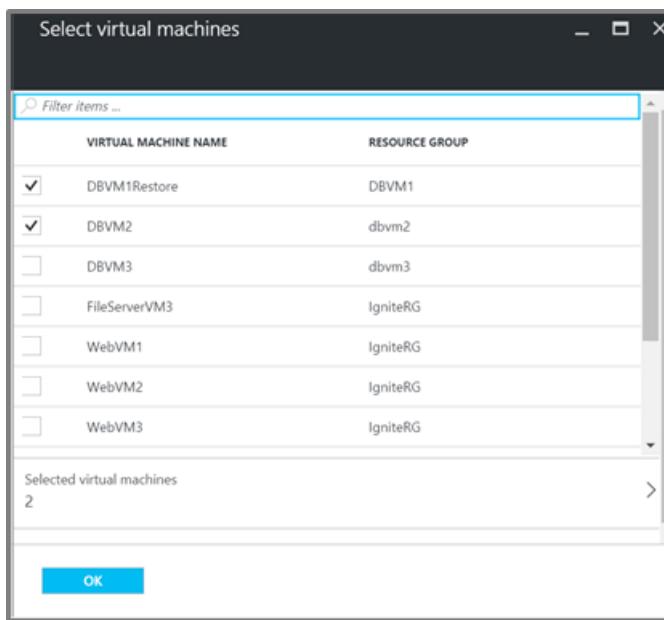


5. In **Backup policy > Choose backup policy**, select the policy that you want to associate with the vault. Then click **OK**.

- A backup policy specifies when backups are taken, and how long they are stored.
- The details of the default policy are listed under the drop-down menu.

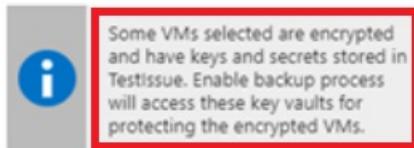


6. If you don't want to use the default policy, select **Create New**, and [create a custom policy](#).  
7. Choose the encrypted VMs you want to back up using the select policy, and select **OK**.

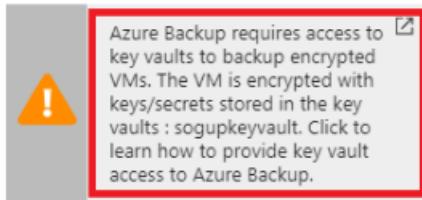


8. If you're using Azure Key Vault, on the vault page, you see a message that Azure Backup needs read-only access to the keys and secrets in the Key Vault.

- If you receive this message, no action is required.



- If you receive this message, you need to set permissions as described in the [procedure below](#).



9. Click **Enable Backup** to deploy the backup policy in the vault, and enable backup for the selected VMs.

## Trigger a backup job

The initial backup will run in accordance with the schedule, but you can run it immediately as follows:

1. In the vault menu, click **Backup items**.
2. In **Backup Items**, click **Azure Virtual Machine**.
3. In the **Backup Items** list, click the ellipses (...).
4. Click **Backup now**.
5. In **Backup Now**, use the calendar control to select the last day that the recovery point should be retained. Then click **OK**.
6. Monitor the portal notifications. You can monitor the job progress in the vault dashboard > **Backup Jobs** > **In progress**. Depending on the size of your VM, creating the initial backup may take a while.

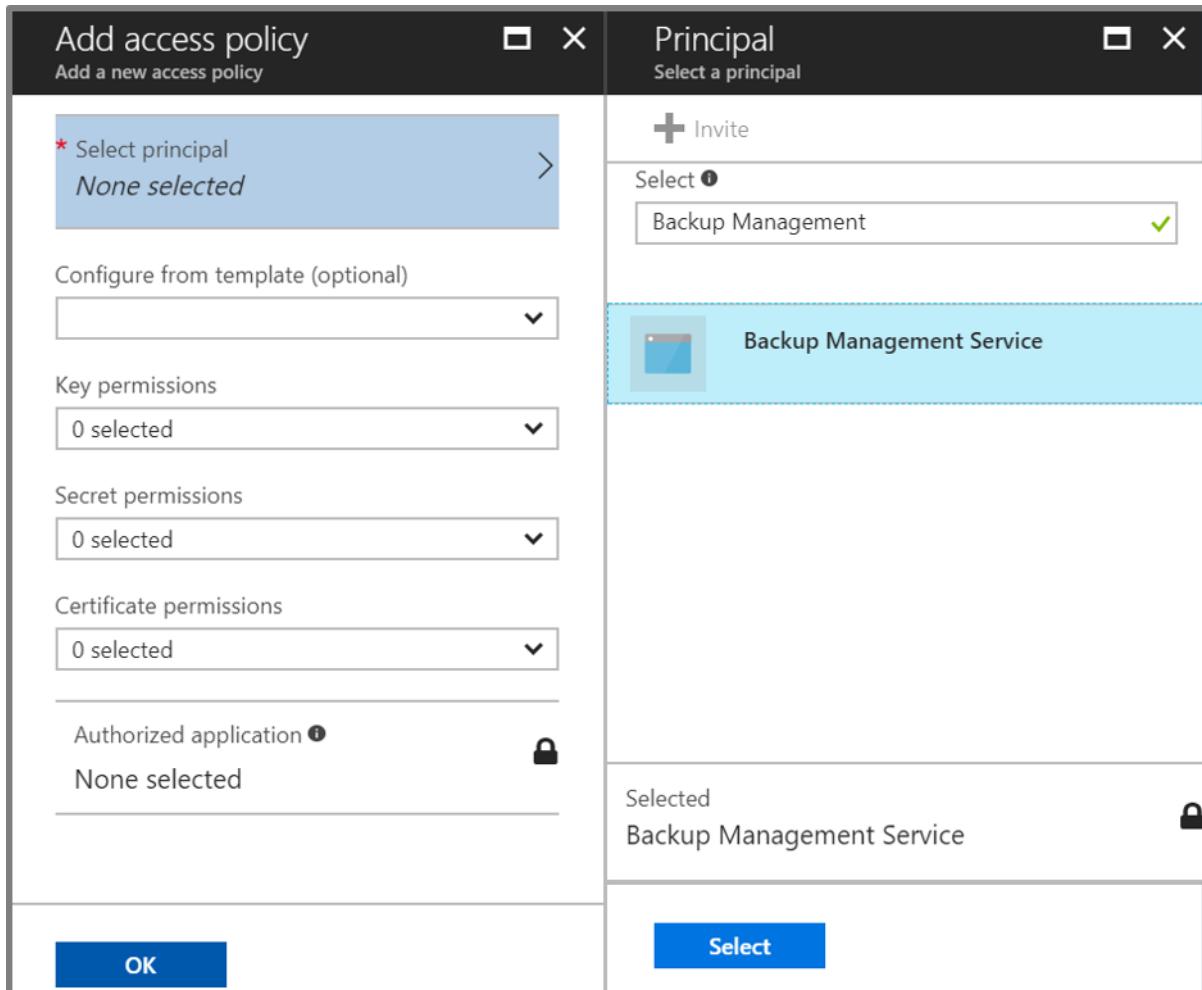
## Provide permissions

Azure VM needs read-only access to back up the keys and secrets, along with the associated VMs.

- Your Key Vault is associated with the Azure AD tenant of the Azure subscription. If you're a **Member user**, Azure Backup acquires access to the Key Vault without further action.
- If you're a **Guest user**, you must provide permissions for Azure Backup to access the key vault.

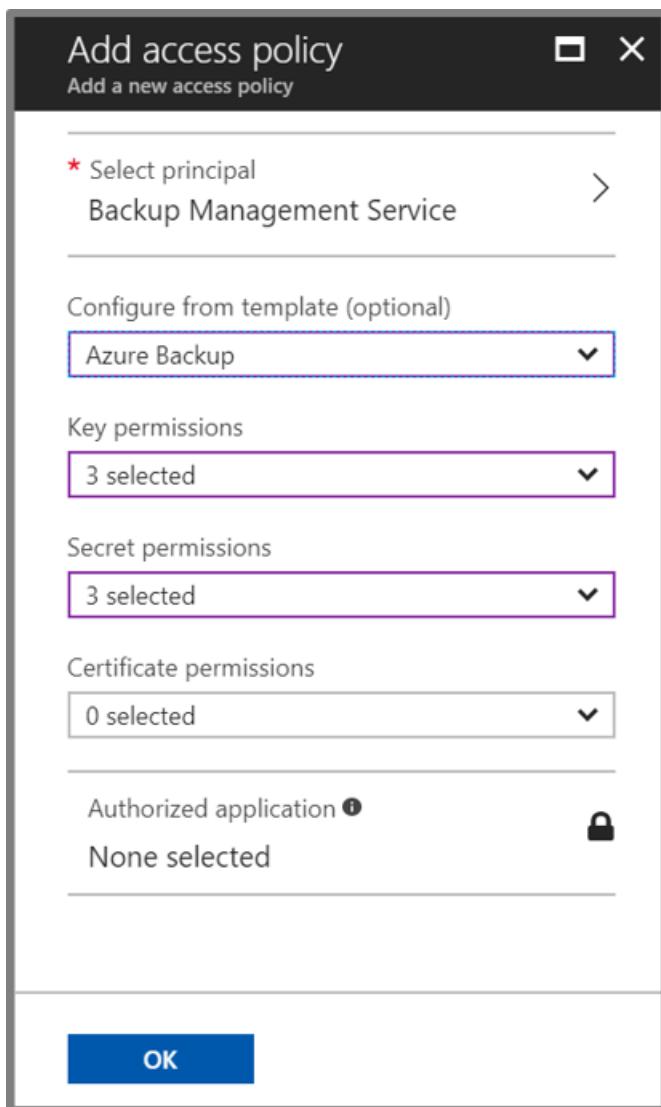
To set permissions:

1. In the Azure portal, select **All services**, and search for **Key vaults**.
2. Select the key vault associated with the encrypted VM you're backing up.
3. Select **Access policies** > **Add new**.
4. Select **Select principal**, and then type **Backup Management**.
5. Select **Backup Management Service** > **Select**.



6. In **Add access policy** > **Configure from template (optional)**, select **Azure Backup**.

- The required permissions are prefilled for **Key permissions** and **Secret permissions**.
- If your VM is encrypted using **BEK only**, remove the selection for **Key permissions** since you only need permissions for secrets.



7. Click **OK**. **Backup Management Service** is added to **Access policies**.

The screenshot shows the 'Access policies' section of the Azure Key Vault interface. On the left, a sidebar lists several options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Keys, Secrets, Access policies (which is highlighted in blue), Advanced access policies, and Properties. The main pane displays a list of access policies, showing one entry: 'Backup Management Service APPLICATION'. At the top of the main pane are buttons for Save, Discard, and Refresh.

8. Click **Save** to provide Azure Backup with the permissions.

## Restore an encrypted VM

You restore encrypted VMs as follows:

1. [Restore the VM disk](#).
2. Recreate the virtual machine instance by doing one of the following:
  - a. Use the template that's generated during the restore operation to customize VM settings, and trigger VM deployment. [Learn more](#).
  - b. Create a new VM from the restored disks using PowerShell. [Learn more](#).
3. For Linux VMs, reinstall the ADE extension so the data disks are open and mounted.

## Next steps

If you run into any issues, review these articles:

- [Common errors](#) when backing up and restoring encrypted Azure VMs.
- [Azure VM agent/backup extension issues](#).

# Application-consistent backup of Azure Linux VMs

11/18/2019 • 5 minutes to read • [Edit Online](#)

When taking backup snapshots of your VMs, application consistency means your applications start when the VMs boot after being restored. As you can imagine, application consistency is extremely important. To ensure your Linux VMs are application consistent, you can use the Linux pre-script and post-script framework to take application-consistent backups. The pre-script and post-script framework supports Azure Resource Manager-deployed Linux virtual machines. Scripts for application consistency do not support Service Manager-deployed virtual machines or Windows virtual machines.

## How the framework works

The framework provides an option to run custom pre-scripts and post-scripts while you're taking VM snapshots. Pre-scripts run just before you take the VM snapshot, and post-scripts run immediately after you take the VM snapshot. Pre-scripts and post-scripts provide the flexibility to control your application and environment, while you're taking VM snapshots.

Pre-scripts invoke native application APIs, which quiesce the IOs, and flush in-memory content to the disk. These actions ensure the snapshot is application consistent. Post-scripts use native application APIs to thaw the IOs, which enable the application to resume normal operations after the VM snapshot.

## Steps to configure pre-script and post-script

1. Sign in as the root user to the Linux VM that you want to back up.
2. From [GitHub](#), download **VMSnapshotScriptPluginConfig.json** and copy it to the **/etc/azure** folder for all VMs you want to back up. If the **/etc/azure** folder doesn't exist, create it.
3. Copy the pre-script and post-script for your application on all VMs you plan to back up. You can copy the scripts to any location on the VM. Be sure to update the full path of the script files in the **VMSnapshotScriptPluginConfig.json** file.
4. Ensure the following permissions for these files:
  - **VMSnapshotScriptPluginConfig.json**: Permission "600." For example, only "root" user should have "read" and "write" permissions to this file, and no user should have "execute" permissions.
  - **Pre-script file**: Permission "700." For example, only "root" user should have "read", "write", and "execute" permissions to this file.
  - **Post-script** Permission "700." For example, only "root" user should have "read", "write", and "execute" permissions to this file.

### IMPORTANT

The framework gives users a lot of power. Secure the framework, and ensure only "root" user has access to critical JSON and script files. If the requirements aren't met, the script won't run, which results in a file system crash and inconsistent backup.

5. Configure **VMSnapshotScriptPluginConfig.json** as described here:

- **pluginName**: Leave this field as is, or your scripts might not work as expected.

- **preScriptLocation:** Provide the full path of the pre-script on the VM that's going to be backed up.
- **postScriptLocation:** Provide the full path of the post-script on the VM that's going to be backed up.
- **preScriptParams:** Provide the optional parameters that need to be passed to the pre-script. All parameters should be in quotes. If you use multiple parameters, separate the parameters with a comma.
- **postScriptParams:** Provide the optional parameters that need to be passed to the post-script. All parameters should be in quotes. If you use multiple parameters, separate the parameters with a comma.
- **preScriptNoOfRetries:** Set the number of times the pre-script should be retried if there is any error before terminating. Zero means only one try and no retry if there is a failure.
- **postScriptNoOfRetries:** Set the number of times the post-script should be retried if there is any error before terminating. Zero means only one try and no retry if there is a failure.
- **timeoutInSeconds:** Specify individual timeouts for the pre-script and the post-script (maximum value can be 1800).
- **continueBackupOnFailure:** Set this value to **true** if you want Azure Backup to fall back to a file system consistent/crash consistent backup if pre-script or post-script fails. Setting this to **false** fails the backup in case of script failure (except when you have single-disk VM that falls back to crash-consistent backup regardless of this setting).
- **fsFreezeEnabled:** Specify whether Linux fsfreeze should be called while you're taking the VM snapshot to ensure file system consistency. We recommend keeping this setting set to **true** unless your application has a dependency on disabling fsfreeze.
- **ScriptsExecutionPollTimeSeconds:** Set the time the extension has to sleep between each poll to the script execution. For example, if the value is 2, the extension checks whether the pre/post script execution completed every 2 seconds. The minimum and maximum value it can take is 1 and 5 respectively. The value should be strictly an integer.

6. The script framework is now configured. If the VM backup is already configured, the next backup invokes the scripts and triggers application-consistent backup. If the VM backup is not configured, configure it by using [Back up Azure virtual machines to Recovery Services vaults](#).

## Troubleshooting

Make sure you add appropriate logging while writing your pre-script and post-script, and review your script logs to fix any script issues. If you still have problems running scripts, refer to the following table for more information.

| ERROR                      | ERROR MESSAGE                                                                                                              | RECOMMENDED ACTION                                                                                                            |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Pre-ScriptExecutionFailed  | The pre-script returned an error, so backup might not be application-consistent.                                           | Look at the failure logs for your script to fix the issue.                                                                    |
| Post-ScriptExecutionFailed | The post-script returned an error that might impact application state.                                                     | Look at the failure logs for your script to fix the issue and check the application state.                                    |
| Pre-ScriptNotFound         | The pre-script was not found at the location that's specified in the <b>VMSnapshotScriptPluginConfig.json</b> config file. | Make sure that pre-script is present at the path that's specified in the config file to ensure application-consistent backup. |

| ERROR                                | ERROR MESSAGE                                                                                                                                                                               | RECOMMENDED ACTION                                                                                                                            |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Post-ScriptNotFound                  | The post-script wasn't found at the location that's specified in the <b>VMSnapshotScriptPluginConfig.json</b> config file.                                                                  | Make sure that post-script is present at the path that's specified in the config file to ensure application-consistent backup.                |
| IncorrectPluginhostFile              | The <b>Pluginhost</b> file, which comes with the VmSnapshotLinux extension, is corrupted, so pre-script and post-script cannot run and the backup won't be application-consistent.          | Uninstall the <b>VmSnapshotLinux</b> extension, and it will automatically be reinstalled with the next backup to fix the problem.             |
| IncorrectJSONConfigFile              | The <b>VMSnapshotScriptPluginConfig.json</b> file is incorrect, so pre-script and post-script cannot run and the backup won't be application-consistent.                                    | Download the copy from <a href="#">GitHub</a> and configure it again.                                                                         |
| InsufficientPermissionforPre-Script  | For running scripts, "root" user should be the owner of the file and the file should have "700" permissions (that is, only "owner" should have "read", "write", and "execute" permissions). | Make sure "root" user is the "owner" of the script file and that only "owner" has "read", "write" and "execute" permissions.                  |
| InsufficientPermissionforPost-Script | For running scripts, root user should be the owner of the file and the file should have "700" permissions (that is, only "owner" should have "read", "write", and "execute" permissions).   | Make sure "root" user is the "owner" of the script file and that only "owner" has "read", "write" and "execute" permissions.                  |
| Pre-ScriptTimeout                    | The execution of the application-consistent backup pre-script timed-out.                                                                                                                    | Check the script and increase the timeout in the <b>VMSnapshotScriptPluginConfig.json</b> file that's located at <a href="#">/etc/azure</a> . |
| Post-ScriptTimeout                   | The execution of the application-consistent backup post-script timed out.                                                                                                                   | Check the script and increase the timeout in the <b>VMSnapshotScriptPluginConfig.json</b> file that's located at <a href="#">/etc/azure</a> . |

## Next steps

[Configure VM backup to a Recovery Services vault](#)

# How to restore Azure VM data in Azure portal

2/25/2020 • 13 minutes to read • [Edit Online](#)

This article describes how to restore Azure VM data from the recovery points stored in [Azure Backup Recovery Services vaults](#).

## Restore options

Azure Backup provides a number of ways to restore a VM.

| RESTORE OPTION         | DETAILS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Create a new VM</b> | <p>Quickly creates and gets a basic VM up and running from a restore point.</p> <p>You can specify a name for the VM, select the resource group and virtual network (VNet) in which it will be placed, and specify a storage account for the restored VM. The new VM must be created in the same region as the source VM.</p>                                                                                                                                                                                                                                                                                                                                    |
| <b>Restore disk</b>    | <p>Restores a VM disk, which can then be used to create a new VM.</p> <p>Azure Backup provides a template to help you customize and create a VM.</p> <p>The restore job generates a template that you can download and use to specify custom VM settings, and create a VM.</p> <p>The disks are copied to the Resource Group you specify.</p> <p>Alternatively, you can attach the disk to an existing VM, or create a new VM using PowerShell.</p> <p>This option is useful if you want to customize the VM, add configuration settings that weren't there at the time of backup, or add settings that must be configured using the template or PowerShell.</p> |

| RESTORE OPTION                         | DETAILS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Replace existing</b>                | <p>You can restore a disk, and use it to replace a disk on the existing VM.</p> <p>The current VM must exist. If it's been deleted, this option can't be used.</p> <p>Azure Backup takes a snapshot of the existing VM before replacing the disk, and stores it in the staging location you specify. Existing disks connected to the VM are replaced with the selected restore point.</p> <p>The snapshot is copied to the vault, and retained in accordance with the retention policy.</p> <p>After the replace disk operation, the original disk is retained in the resource group. You can choose to manually delete the original disks if they are not needed.</p> <p>Replace existing is supported for unencrypted managed VMs. It's not supported for unmanaged disks, <a href="#">generalized VMs</a>, or for VMs <a href="#">created using custom images</a>.</p> <p>If the restore point has more or less disks than the current VM, then the number of disks in the restore point will only reflect the VM configuration.</p> <p>Replace existing isn't supported for VMs with linked resources (like <a href="#">user-assigned managed-identity</a> or <a href="#">Key Vault</a>) because the backup client-app doesn't have permissions on these resources while performing the restore.</p> |
| <b>Cross Region (secondary region)</b> | <p>Cross Region restore can be used to restore Azure VMs in the secondary region, which is an <a href="#">Azure paired region</a>.</p> <p>You can restore all the Azure VMs for the selected recovery point if the backup is done in the secondary region.</p> <p>This feature is available for the options below:</p> <ul style="list-style-type: none"> <li>* <a href="#">Create a VM</a></li> <li>* <a href="#">Restore Disks</a></li> </ul> <p>We don't currently support the <a href="#">Replace existing disks</a> option.</p> <p>Permissions</p> <p>The restore operation on secondary region can be performed by Backup Admins and App admins.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

#### NOTE

You can also recover specific files and folders on an Azure VM. [Learn more](#).

If you're running the [latest version](#) of Azure Backup for Azure VMs (known as Instant Restore), snapshots are kept for up to seven days, and you can restore a VM from snapshots before the backup data is sent to the vault. If you want to restore a VM from a backup from the last seven days, it's quicker to restore from the snapshot and not from the vault.

## Storage accounts

Some details about storage accounts:

- **Create VM:** When you create a new VM, the VM will be placed in the storage account you specify.
- **Restore disk:** When you restore a disk, the disk is copied to the storage account you specify. The restore job generates a template that you can download and use to specify custom VM settings. This template is placed in the specified storage account.
- **Replace disk:** When you replace a disk on an existing VM, Azure Backup takes a snapshot of the existing VM before replacing the disk. The snapshot is stored in the staging location (storage account) you specify. This storage account is used to temporarily store the snapshot during the restore process, and we recommend that you create a new account to do this, that can be easily removed afterwards.
- **Storage account location:** The storage account must be in the same region as the vault. Only these accounts are displayed. If there are no storage accounts in the location, you need to create one.
- **Storage type:** Blob storage isn't supported.
- **Storage redundancy:** Zone redundant storage (ZRS) isn't supported. The replication and redundancy information for the account is shown in parentheses after the account name.
- **Premium storage:**
  - When restoring non-premium VMs, premium storage accounts aren't supported.
  - When restoring managed VMs, premium storage accounts configured with network rules aren't supported.

## Before you start

To restore a VM (create a new VM), make sure you have the correct role-based access control (RBAC) [permissions](#) for the Restore VM operation.

If you don't have permissions, you can [restore a disk](#), and then after the disk is restored, you can [use the template](#) that was generated as part of the restore operation to create a new VM.

## Select a restore point

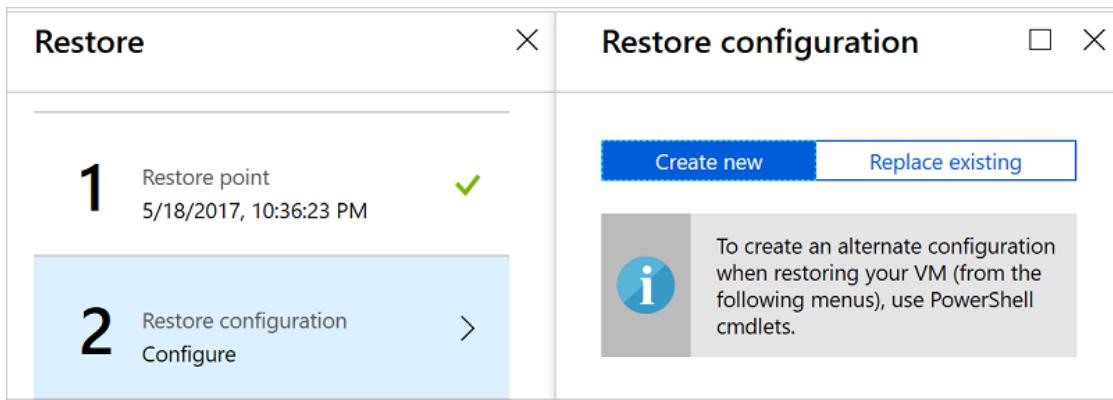
1. In the vault associated with the VM you want to restore, click **Backup items > Azure Virtual Machine**.
2. Click a VM. By default on the VM dashboard, recovery points from the last 30 days are displayed. You can display recovery points older than 30 days, or filter to find recovery points based on dates, time ranges, and different types of snapshot consistency.
3. To restore the VM, click **Restore VM**.

| Alerts and Jobs                                 |                                               | Backup status      |                                                                     | Summary                 |                                        |
|-------------------------------------------------|-----------------------------------------------|--------------------|---------------------------------------------------------------------|-------------------------|----------------------------------------|
| <a href="#">View all Alerts</a> (last 24 hours) | <a href="#">View all Jobs</a> (last 24 hours) | Backup Pre-Check   | <span style="color: green;">✔ Passed</span>                         | Recovery services vault | <a href="#">ExtensionTestBkpVault</a>  |
|                                                 |                                               | Last backup status | <span style="color: green;">✔ Success</span> 5/18/2017, 10:35:15 PM | Backup policy           | <a href="#">DailyPolicy</a>            |
|                                                 |                                               |                    |                                                                     | Oldest restore point    | 5/18/2017, 10:36:23 PM (1 year(s) ago) |

4. Select a restore point to use for the recovery.

## Choose a VM restore configuration

1. In **Restore configuration**, select a restore option:
  - **Create new:** Use this option if you want to create a new VM. You can create a VM with simple settings, or restore a disk and create a customized VM.
  - **Replace existing:** Use this option if you want to replace disks on an existing VM.

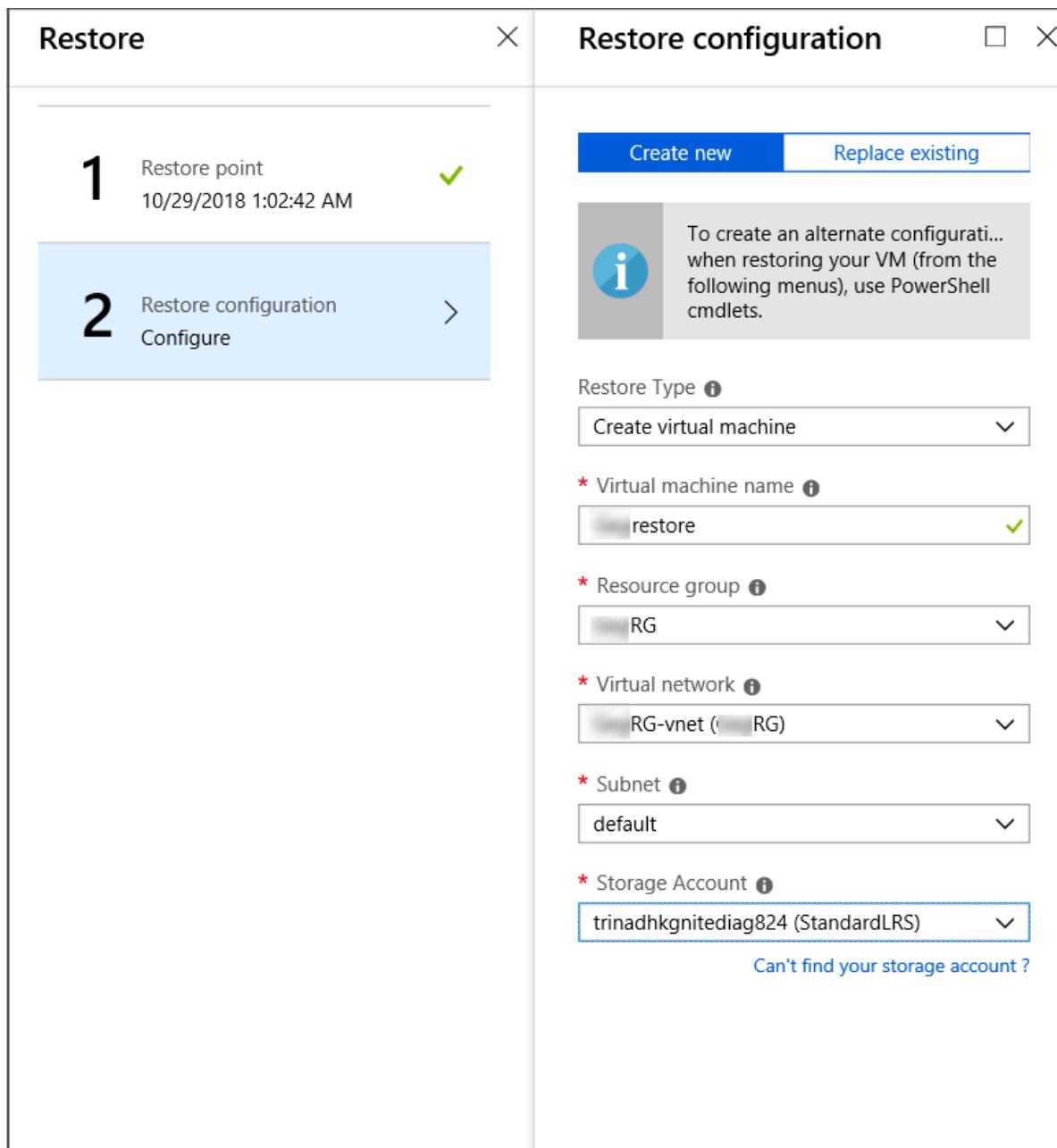


- Specify settings for your selected restore option.

## Create a VM

As one of the [restore options](#), you can create a VM quickly with basic settings from a restore point.

- In **Restore configuration** > **Create new** > **Restore Type**, select **Create a virtual machine**.
- In **Virtual machine name**, specify a VM that doesn't exist in the subscription.
- In **Resource group**, select an existing resource group for the new VM, or create a new one with a globally unique name. If you assign a name that already exists, Azure assigns the group the same name as the VM.
- In **Virtual network**, select the VNet in which the VM will be placed. All VNets associated with the subscription are displayed. Select the subnet. The first subnet is selected by default.
- In **Storage Location**, specify the storage account for the VM. [Learn more](#).



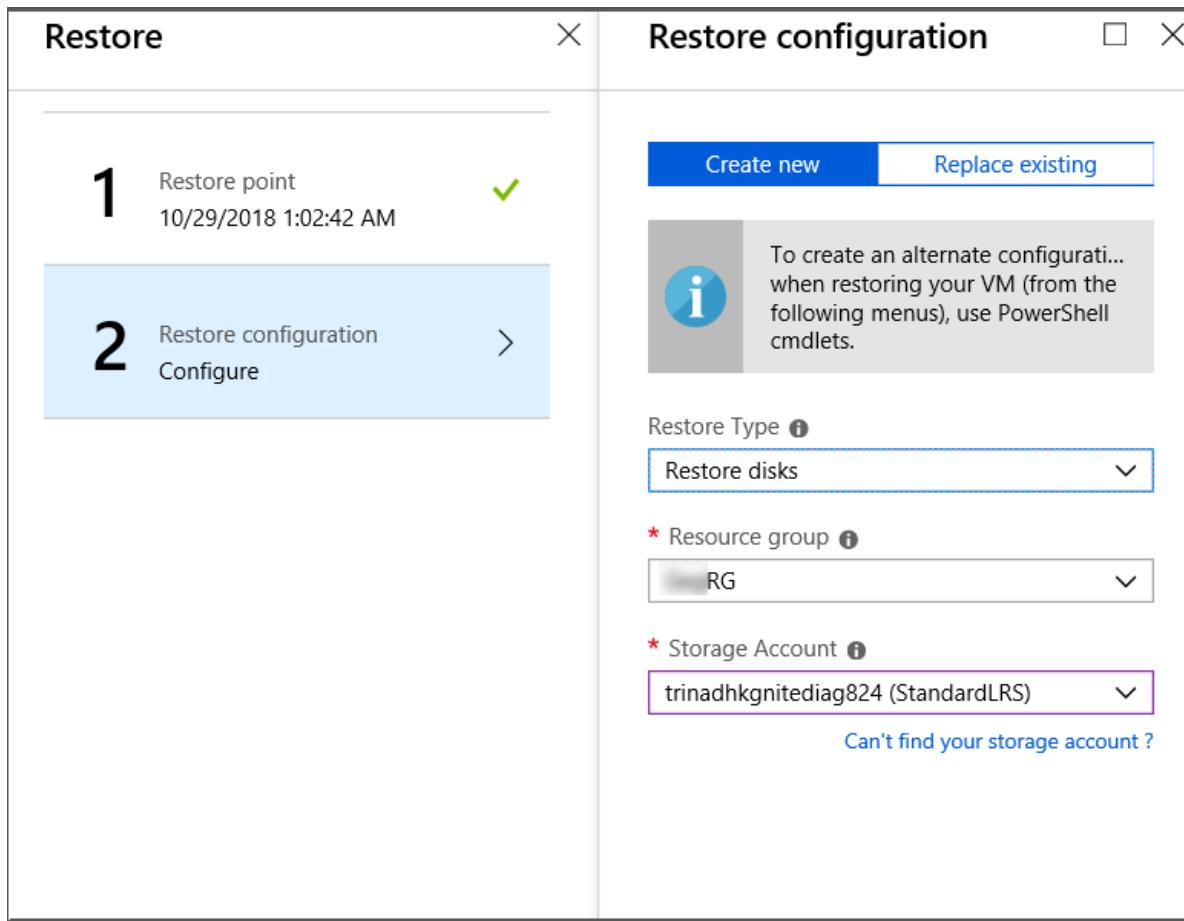
6. In **Restore configuration**, select **OK**. In **Restore**, click **Restore** to trigger the restore operation.

## Restore disks

As one of the [restore options](#), you can create a disk from a restore point. Then with the disk, you can do one of the following:

- Use the template that is generated during the restore operation to customize settings, and trigger VM deployment. You edit the default template settings, and submit the template for VM deployment.
- [Attach restored disks](#) to an existing VM.
- [Create a new VM](#) from the restored disks using PowerShell.

1. In **Restore configuration > Create new > Restore Type**, select **Restore disks**.
2. In **Resource group**, select an existing resource group for the restored disks, or create a new one with a globally unique name.
3. In **Storage account**, specify the account to which to copy the VHDs. [Learn more](#).



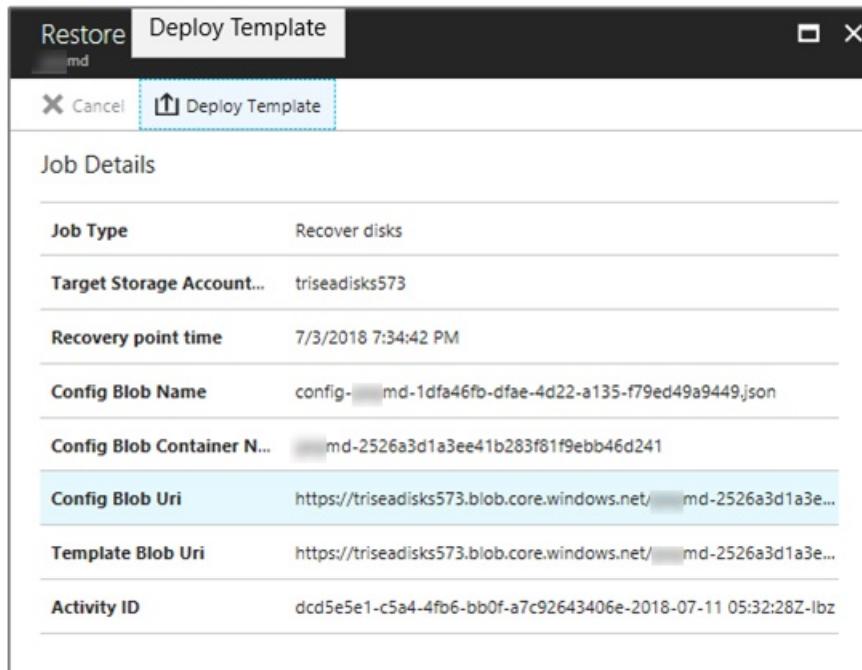
4. In **Restore configuration**, select **OK**. In **Restore**, click **Restore** to trigger the restore operation.

When your virtual machine uses managed disks and you select the **Create virtual machine** option, Azure Backup doesn't use the specified storage account. In the case of **Restore disks** and **Instant Restore**, the storage account is used only for storing the template. Managed disks are created in the specified resource group. When your virtual machine uses unmanaged disks, they are restored as blobs to the storage account.

#### Use templates to customize a restored VM

After the disk is restored, use the template that was generated as part of the restore operation to customize and create a new VM:

1. Open **Restore Job Details** for the relevant job.
2. In **Restore Job Details**, select **Deploy Template** to initiate template deployment.



3. To customize the VM setting provided in the template, click **Edit template**. If you want to add more customizations, click **Edit parameters**.
- [Learn more](#) about deploying resources from a custom template.
  - [Learn more](#) about authoring templates.



4. Enter the custom values for the VM, accept the **Terms and Conditions** and click **Purchase**.

## Custom deployment

Deploy from a custom template

|                                                 |               |  |
|-------------------------------------------------|---------------|--|
| * Virtual Machine Name <small>i</small>         | RestoredVM    |  |
| Virtual Network <small>i</small>                | RG-vnet       |  |
| Virtual Network Resource Group <small>i</small> | RG            |  |
| Subnet <small>i</small>                         | default       |  |
| Os Disk Name <small>i</small>                   | MDOSDisk      |  |
| Data Disk Prefix Name <small>i</small>          | MDDataDisk    |  |
| Network Interface Prefix Name <small>i</small>  | MDRestoredNIC |  |
| Public Ip Address Name <small>i</small>         | MDRestoredip  |  |

### TERMS AND CONDITIONS

[Azure Marketplace Terms](#) | [Azure Marketplace](#)

By clicking "Purchase," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.

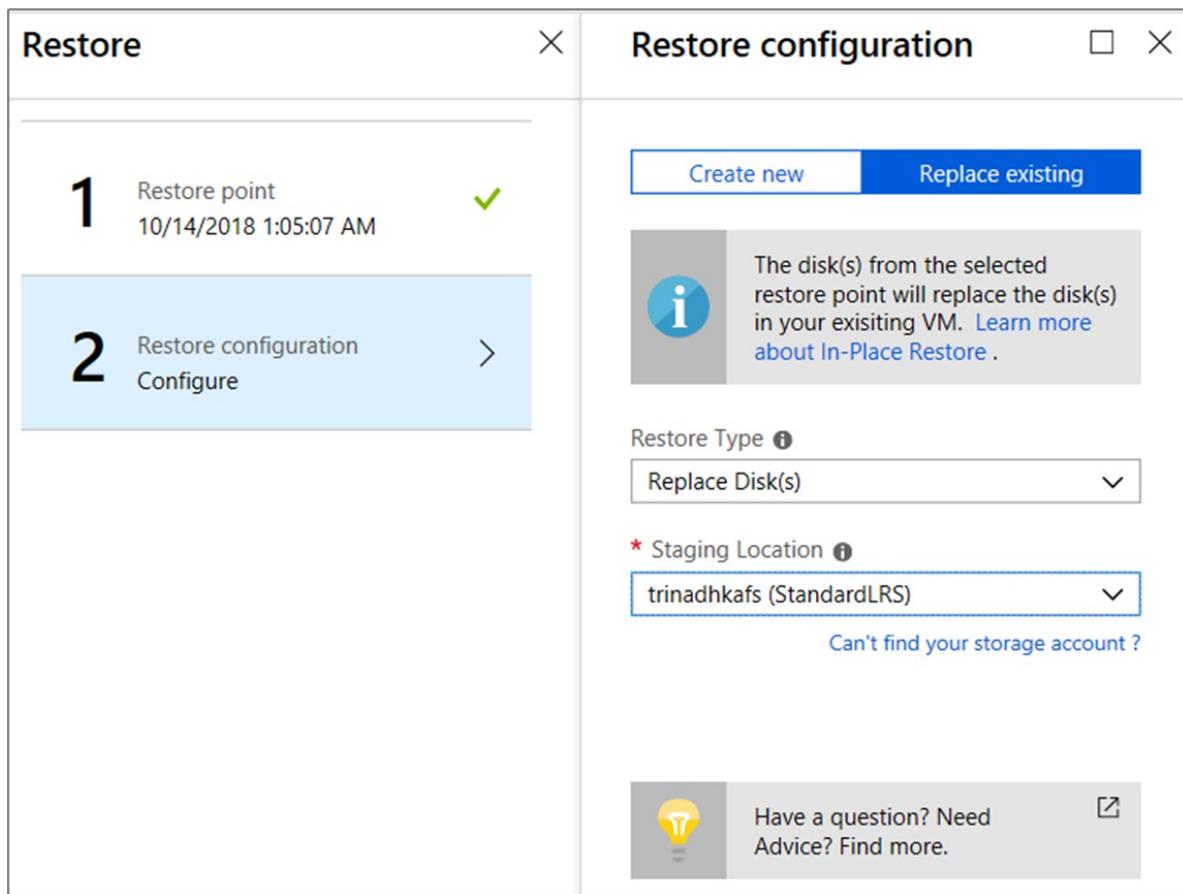
I agree to the terms and conditions stated above

[Purchase](#)

## Replace existing disks

As one of the [restore options](#), you can replace an existing VM disk with the selected restore point. [Review all](#) restore options.

1. In **Restore configuration**, click **Replace existing**.
2. In **Restore Type**, select **Replace disk/s**. This is the restore point that will be used replace existing VM disks.
3. In **Staging Location**, specify where snapshots of the current managed disks should be saved during the restore process. [Learn more](#).



## Cross Region Restore

As one of the [restore options](#), Cross Region Restore (CRR) allows you to restore Azure VMs in a secondary region, which is an Azure paired region.

To onboard to the feature during the preview, please read the [Before You Begin](#) section.

To see if CRR is enabled, follow the instructions in [Configure Cross Region Restore](#)

### **View backup items in secondary region**

If CRR is enabled, you can view the backup items in the secondary region.

1. From the portal, go to **Recovery Services vault > Backup items**
2. Click **Secondary Region** to view the items in the secondary region.

**CRRIgniteDemoVault - Backup items**  
Recovery Services vault

Search (Ctrl+ /) Refresh Primary Region Secondary Region

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings**
  - Properties
  - Locks
  - Export template
- Getting started**
  - Backup
  - Site Recovery

| BACKUP MANAGEMENT TYPE | BACKUP ITEM COUNT |
|------------------------|-------------------|
| Azure Virtual Machine  | 2                 |
| SAP HANA in Azure VM   | 0                 |
| SQL in Azure VM        | 0                 |
| DPM                    | 0                 |
| Azure Backup Server    | 0                 |
| Azure Backup Agent     | 0                 |

**CRRIgniteDemoVault - Backup items**  
Recovery Services vault

Search (Ctrl+ /) Refresh Primary Region Secondary Region

Showing data from "eastus2euap" (Secondary Region)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings**
  - Properties

| BACKUP MANAGEMENT TYPE | BACKUP ITEM COUNT |
|------------------------|-------------------|
| Azure Virtual Machine  | 2                 |

## Restore in secondary region

The secondary region restore user experience will be similar to the primary region restore user experience. When configuring details in the Restore Configuration blade to configure your restore, you'll be prompted to provide only secondary region parameters.

Backup Items (Azure Virtual Machine)

Refresh + Add Filter

Showing data from eastus2euap (secondary region)

Fetching data from service completed.

Filter items ...

| Name            | Resource Group | Backup Pre-Check | Last Backup Status | Latest restore point  |
|-----------------|----------------|------------------|--------------------|-----------------------|
| CRRIgniteDemoVM | BackEndDemo    | Passed           | Success            | 12/2/2019, 2:36:17 AM |

CRRIgniteDemoVM

- Pin to dashboard
- Backup now
- Restore VM
- File Recovery
- Stop backup
- Delete backup data

**Restore**

**1** Restore point Select >

**2** Restore configuration Configure >

### Select restore point

Filter

Filtered for last 30 days

Showing data from "eastus2euap" (Secondary Region)

CRASH CONSISTENT APPLICATION CONSISTENT FILE-SYSTEM CONSISTENT

| Time                   | Consistency            | Recovery Type |
|------------------------|------------------------|---------------|
| 12/2/2019, 2:34:17 AM  | File-system Consistent | Vault         |
| 12/1/2019, 2:35:12 AM  | File-system Consistent | Vault         |
| 11/30/2019, 2:31:56 AM | File-system Consistent | Vault         |
| 11/29/2019, 2:30:37 AM | File-system Consistent | Vault         |
| 11/28/2019, 2:32:57 AM | File-system Consistent | Vault         |
| 11/27/2019, 2:34:01 AM | File-system Consistent | Vault         |

**Restore**

**1** Restore point 12/2/2019, 2:34:17 AM ✓

**2** Restore configuration Configure >

### Restore configuration

Showing data from "eastus2euap" (Secondary Region)

Create new Replace existing

**i** To create an alternate configuration when restoring your VM (from the following menus), use PowerShell cmdlets.

**Restore Type** Create virtual machine

**Virtual machine name \*** CRRVMrestoredsec ✓

**Resource group \*** Backupdemo

**Virtual network \*** ignitereusvnet (igniterg)

**Subnet \*** default

**Storage Account \*** srikanthgrs1 (StandardRAGRS) ✓

[Can't find your storage account ?](#)

Triggering restore for crrgnitedemovm 3:56 PM  
Trigger restore in progress.

Showing data from eastus2euap (secondary region)

Latest restore point ↑↓  
12/2/2019, 2:34:17 AM ...

- To restore and create a VM, refer to [Create a VM](#).
- To restore as a disk, refer to [Restore disks](#).

#### NOTE

After the restore is triggered and in the data transfer phase, the restore job cannot be cancelled.

## Monitoring secondary region restore jobs

1. From the portal, go to **Recovery Services vault > Backup Jobs**
2. Click **Secondary Region** to view the items in the secondary region.

Backup jobs

Choose columns Filter Export jobs Refresh View jobs in secondary region

Filtered by: Item Type - All item types, Operation - All Operations, Status - All Status, Start Time - 12/30/2019, 12:24:51 PM, End Time - 12/31/2019, 12:24:51 PM

Showing data from eastus2euap (secondary region)

Completed fetching data from the service.

Filter items...

| Workload name  | Operation          | Status      | Type                  | Start time              | Duration | ... |
|----------------|--------------------|-------------|-----------------------|-------------------------|----------|-----|
| crrgnitedemovm | CrossRegionRestore | In progress | Azure virtual machine | 12/31/2019, 12:24:37 PM | 00:00:15 | ... |
| crrgnitedemovm | CrossRegionRestore | Completed   | Azure virtual machine | 12/30/2019, 3:57:29 PM  | 00:28:53 | ... |

## Restore VMs with special configurations

There are a number of common scenarios in which you might need to restore VMs.

| SCENARIO                                    | GUIDANCE                                                                                                                                                                                                                                                                      |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Restore VMs using Hybrid Use Benefit</b> | If a Windows VM uses <a href="#">Hybrid Use Benefit (HUB) licensing</a> , restore the disks, and create a new VM using the provided template (with <b>License Type</b> set to <b>Windows_Server</b> ), or PowerShell. This setting can also be applied after creating the VM. |

| SCENARIO                                                       | GUIDANCE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Restore VMs during an Azure datacenter disaster</b>         | If the vault uses GRS and the primary datacenter for the VM goes down, Azure Backup supports restoring backed-up VMs to the paired datacenter. You select a storage account in the paired datacenter, and restore as normal. Azure Backup uses the compute service in the paired region to create the restored VM. <a href="#">Learn more</a> about datacenter resiliency.                                                                                                                                                          |
| <b>Restore single domain controller VM in single domain</b>    | <p>Restore the VM like any other VM. Note that:</p> <p>From an Active Directory perspective, the Azure VM is like any other VM.</p> <p>Directory Services Restore Mode (DSRM) is also available, so all Active Directory recovery scenarios are viable. <a href="#">Learn more</a> about backup and restore considerations for virtualized domain controllers.</p>                                                                                                                                                                  |
| <b>Restore multiple domain controller VMs in single domain</b> | If other domain controllers in the same domain can be reached over the network, the domain controller can be restored like any VM. If it's the last remaining domain controller in the domain, or a recovery in an isolated network is performed, use a <a href="#">forest recovery</a> .                                                                                                                                                                                                                                           |
| <b>Restore multiple domains in one forest</b>                  | We recommend a <a href="#">forest recovery</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Bare-metal restore</b>                                      | The major difference between Azure VMs and on-premises hypervisors is that there's no VM console available in Azure. A console is required for certain scenarios, such as recovering by using a bare-metal recovery (BMR)-type backup. However, VM restore from the vault is a full replacement for BMR.                                                                                                                                                                                                                            |
| <b>Restore VMs with special network configurations</b>         | Special network configurations include VMs using internal or external load balancing, using multiple NICs, or multiple reserved IP addresses. You restore these VMs by using the <a href="#">restore disk option</a> . This option makes a copy of the VHDs into the specified storage account, and you can then create a VM with an <a href="#">internal</a> or <a href="#">external</a> load balancer, <a href="#">multiple NICs</a> , or <a href="#">multiple reserved IP addresses</a> , in accordance with your configuration. |
| <b>Network Security Group (NSG) on NIC/Subnet</b>              | Azure VM backup supports Backup and Restore of NSG information at vnet, subnet, and NIC level.                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Zone Pinned VMs</b>                                         | Azure Backup supports backup and restore of zoned pinned VMs. <a href="#">Learn more</a>                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## Track the restore operation

After you trigger the restore operation, the backup service creates a job for tracking. Azure Backup displays notifications about the job in the portal. If they aren't visible, select the **Notifications** symbol, and then select **View all Jobs** to see the Restore Process Status.

The screenshot shows the Azure Backup vault interface. At the top, there are navigation links: Backup now, Restore VM, File Recovery, Stop backup, Resume backup, and Delete backup data. Below this, the 'Alerts and Jobs' section displays 'View all Alerts (last 24 hours)' and 'View all Jobs (last 24 hours)'. The 'Backup status' section shows 'Backup Pre-Check' as Passed, 'Last backup status' as Success 7/10/2018, 1:10:06 AM, and 'Backup policy' as DefaultPolicy. The 'Summary' section shows a 'Restore vault' named 'restorevault' and an 'Oldest restore point' at 7/3/2018, 1:09:37 AM (7 day(s) ago). A notification on the right says 'Triggering restore for gemd' at 3:42 PM, with a message: 'Restore triggered successfully. Please monitor progress in backup jobs page.'

Track restore as follows:

1. To view operations for the job, click the notifications hyperlink. Alternatively, in the vault, click **Backup jobs**, and then click the relevant VM.

| WORKLOAD NAME | OPERATION | STATUS    | TYPE                  | START TIME           | DURATION |     |
|---------------|-----------|-----------|-----------------------|----------------------|----------|-----|
| gemd          | Restore   | Completed | Azure virtual machine | 9/10/2018 4:06:24 PM | 00:10:49 | ... |
| gemd          | Restore   | Completed | Azure virtual machine | 9/10/2018 3:23:03 PM | 00:18:42 | ... |

2. To monitor restore progress, click any restore job with a status of **In-progress**. This displays the progress bar, which displays information about the restore progress:

- **Estimated time of restore:** Initially provides the time taken to complete the restore operation. As the operation progresses, the time taken reduces and reaches zero when the restore operation finishes.
- **Percentage of restore:** Shows the percentage of restore operation that's done.
- **Number of bytes transferred:** If you're restoring by creating a new VM, it shows the bytes that were transferred against the total number of bytes to be transferred.

## Post-restore steps

There are a number of things to note after restoring a VM:

- Extensions present during the backup configuration are installed, but not enabled. If you see an issue, reinstall the extensions.
- If the backed-up VM had a static IP address, the restored VM will have a dynamic IP address to avoid conflict. You can [add a static IP address to the restored VM](#).
- A restored VM doesn't have an availability set. If you use the restore disk option, then you can [specify an availability set](#) when you create a VM from the disk using the provided template or PowerShell.
- If you use a cloud-init-based Linux distribution, such as Ubuntu, for security reasons the password is blocked after the restore. Use the VMAccess extension on the restored VM to [reset the password](#). We recommend using SSH keys on these distributions, so you don't need to reset the password after the restore.
- If you are unable to access VM once restored due to VM having broken relationship with domain controller, then follow the steps below to bring up the VM:
  - Attach OS disk as a data disk to a recovered VM.
  - Manually install VM agent if Azure Agent is found to be unresponsive by following this [link](#).
  - Enable Serial Console access on VM to allow command-line access to VM

```
bcdedit /store <drive letter>:\boot\bcd /enum
bcdedit /store <VOLUME LETTER WHERE THE BCD FOLDER IS>:\boot\bcd /set {bootmgr} displaybootmenu yes
bcdedit /store <VOLUME LETTER WHERE THE BCD FOLDER IS>:\boot\bcd /set {bootmgr} timeout 5
bcdedit /store <VOLUME LETTER WHERE THE BCD FOLDER IS>:\boot\bcd /set {bootmgr} bootevals yes
bcdedit /store <VOLUME LETTER WHERE THE BCD FOLDER IS>:\boot\bcd /ems {<<BOOT LOADER IDENTIFIER>>} ON
bcdedit /store <VOLUME LETTER WHERE THE BCD FOLDER IS>:\boot\bcd /emssettings EMSPORT:1
EMSBAUDRATE:115200
```

- When the VM is rebuilt use Azure portal to reset local administrator account and password
- Use Serial console access and CMD to disjoin VM from domain

```
cmd /c "netdom remove <<MachineName>> /domain:<<DomainName>> /userD:<<DomainAdminhere>>
/passwordD:<<PasswordHere>> /reboot:10 /Force"
```

- Once the VM is disjoined and restarted, you will be able to successfully RDP to VM with local admin credentials and rejoin VM back to domain successfully.

## Backing up restored VMs

- If you restored a VM to the same resource group with the same name as the originally backed-up VM, backup continues on the VM after restore.
- If you restored the VM to a different resource group or you specified a different name for the restored VM, you need to set up backup for the restored VM.

## Next steps

- If you experience difficulties during the restore process, [review](#) common issues and errors.
- After the VM is restored, learn about [managing virtual machines](#)

# Recover files from Azure virtual machine backup

2/27/2020 • 14 minutes to read • [Edit Online](#)

Azure Backup provides the capability to restore [Azure virtual machines \(VMs\) and disks](#) from Azure VM backups, also known as recovery points. This article explains how to recover files and folders from an Azure VM backup. Restoring files and folders is available only for Azure VMs deployed using the Resource Manager model and protected to a Recovery services vault.

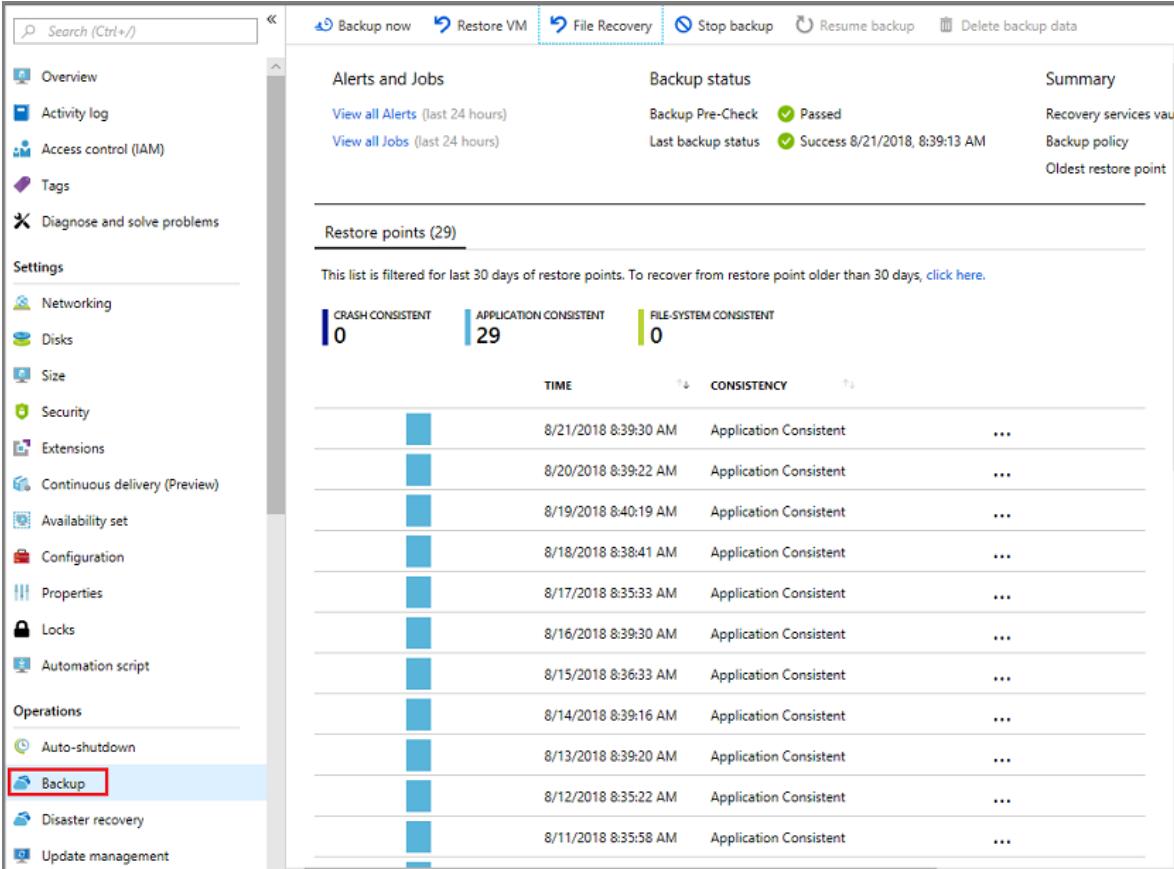
## NOTE

This feature is available for Azure VMs deployed using the Resource Manager model and protected to a Recovery Services vault. File recovery from an encrypted VM backup is not supported.

## Mount the volume and copy files

To restore files or folders from the recovery point, go to the virtual machine and choose the desired recovery point.

1. Sign in to the [Azure portal](#) and in the left pane, click **Virtual machines**. From the list of virtual machines, select the virtual machine to open that virtual machine's dashboard.
2. In the virtual machine's menu, click **Backup** to open the Backup dashboard.



The screenshot shows the Azure Backup dashboard for a specific virtual machine. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Networking, Disks, Size, Security, Extensions, Continuous delivery (Preview), Availability set, Configuration, Properties, Locks, Automation script), Operations (Auto-shutdown, Backup, Disaster recovery, Update management). The 'Backup' link is highlighted with a red box. The main content area has tabs for Backup now, Restore VM, File Recovery (which is selected and highlighted with a blue border), Stop backup, Resume backup, and Delete backup data. Under 'File Recovery', there are sections for Alerts and Jobs (View all Alerts, View all Jobs), Backup status (Backup Pre-Check Passed, Last backup status Success 8/21/2018, 8:39:13 AM), and Summary (Recovery services vault, Backup policy, Oldest restore point). Below these is a section for 'Restore points (29)'. A note says 'This list is filtered for last 30 days of restore points. To recover from restore point older than 30 days, click here.' The restore points table has columns for CRASH CONSISTENT (0), APPLICATION CONSISTENT (29), FILE-SYSTEM CONSISTENT (0), TIME (sorted by descending date), and CONSISTENCY. Each row shows a blue icon, the timestamp (e.g., 8/21/2018 8:39:30 AM), the consistency level (Application Consistent), and three dots for more options.

| CRASH CONSISTENT | APPLICATION CONSISTENT | FILE-SYSTEM CONSISTENT | TIME                 | CONSISTENCY            |
|------------------|------------------------|------------------------|----------------------|------------------------|
| 0                | 29                     | 0                      | 8/21/2018 8:39:30 AM | Application Consistent |
|                  |                        |                        | 8/20/2018 8:39:22 AM | Application Consistent |
|                  |                        |                        | 8/19/2018 8:40:19 AM | Application Consistent |
|                  |                        |                        | 8/18/2018 8:38:41 AM | Application Consistent |
|                  |                        |                        | 8/17/2018 8:35:33 AM | Application Consistent |
|                  |                        |                        | 8/16/2018 8:39:30 AM | Application Consistent |
|                  |                        |                        | 8/15/2018 8:36:33 AM | Application Consistent |
|                  |                        |                        | 8/14/2018 8:39:16 AM | Application Consistent |
|                  |                        |                        | 8/13/2018 8:39:20 AM | Application Consistent |
|                  |                        |                        | 8/12/2018 8:35:22 AM | Application Consistent |
|                  |                        |                        | 8/11/2018 8:35:58 AM | Application Consistent |

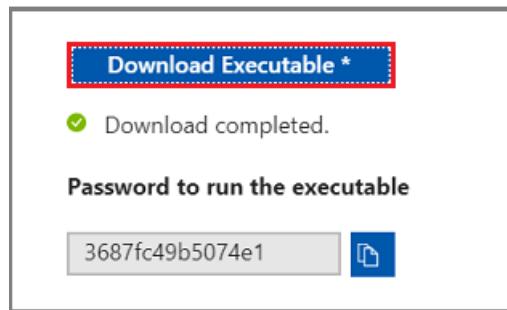
3. In the Backup dashboard menu, click **File Recovery**.

The screenshot shows the Azure portal interface with the 'File Recovery' menu highlighted by a red box. The menu includes options like 'Backup now', 'Restore VM', 'File Recovery' (which is selected), 'Stop backup', 'Resume backup', and 'Delete backup data'. On the left sidebar, there are sections for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Networking, and Disks. The main content area displays 'Alerts and Jobs' with links to 'View all Alerts (last 24 hours)' and 'View all Jobs (last 24 hours)'. It also shows 'Backup status' with 'Backup Pre-Check Passed' and 'Last backup status Success 8/21/2018, 8:39:13 AM'. A section for 'Restore points (29)' is shown, with a note that it's filtered for the last 30 days. Below this are three status indicators: 'CRASH CONSISTENT' (0), 'APPLICATION CONSISTENT' (29), and 'FILE-SYSTEM CONSISTENT' (0).

The **File Recovery** menu opens.

The screenshot shows the 'File Recovery' wizard. Step 1: Select recovery point. A dropdown menu is open, showing '7/20/2017, 1:36:40 PM [Latest] (AppCo...)' as the selected option. Step 2: Download script to browse and recover files. A note explains that the script will mount disks from the selected recovery point as local drives on the machine where it is run, remaining mounted for 12 hours. A blue button labeled 'Download Executable \*' is visible. Step 3: Unmount the disks after recovery. A note says to unmount disks and close the connection to the recovery point. A grey button labeled 'Unmount Disks' is visible. At the bottom, there are three bullet points: 'Run this script on the machine where you want to copy the files', 'To restore files larger than 10GB, restore entire VM to an alternate location or restore disks using PowerShell', and 'Data transfer rate: up to 1GB/Hr'. A note at the bottom says 'If you have trouble finding your files, click here'.

4. From the **Select recovery point** drop-down menu, select the recovery point that holds the files you want. By default, the latest recovery point is already selected.
5. To download the software used to copy files from the recovery point, click **Download Executable** (for Windows Azure VMs) or **Download Script** (for Linux Azure VMs, a python script is generated).

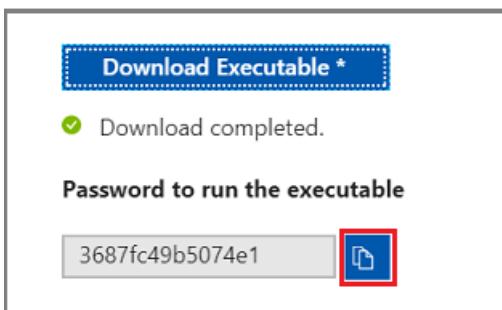


Azure downloads the executable or script to the local computer.

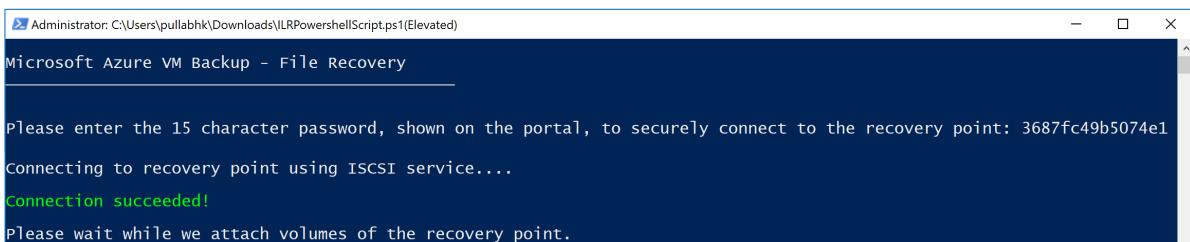


To run the executable or script as an administrator, it's suggested you save the downloaded file to your computer.

6. The executable or script is password protected and requires a password. In the **File Recovery** menu, click the copy button to load the password into memory.



7. From the download location (usually the Downloads folder), right-click the executable or script and run it with Administrator credentials. When prompted, type the password or paste the password from memory, and press **Enter**. Once the valid password is entered, the script connects to the recovery point.



8. For Linux machines, a python script is generated. One needs to download the script and copy it to the relevant/compatible Linux server. You may have to modify the permissions to execute it with `chmod +x <python file name>`. Then run the python file with `./<python file name>`.

Refer to the [Access requirements](#) section to make sure the script is run successfully.

## Identifying volumes

### For Windows

When you run the executable, the operating system mounts the new volumes and assigns drive letters. You can use Windows Explorer or File Explorer to browse those drives. The drive letters assigned to the volumes may not be the same letters as the original virtual machine. However, the volume name is preserved. For example, if the volume on the original virtual machine was "Data Disk (E: \ )", that volume can be attached on the local computer as "Data Disk ('Any letter': \ )". Browse through all volumes mentioned in the script output until you find your files or folder.

```
Connecting to recovery point using iSCSI service....
Connection succeeded!
Please wait while we attach volumes of the recovery point.
1 recovery volumes attached
D:\Local disk
***** Open Explorer to browse for files *****
After recovery, to remove the disks and close the connection to the recovery point, please click 'Unmount Disks' in step 3 of the portal.
Press 'Q/q' key to exit ...
```

#### For Linux

In Linux, the volumes of the recovery point are mounted to the folder where the script is run. The attached disks, volumes, and the corresponding mount paths are shown accordingly. These mount paths are visible to users having root level access. Browse through the volumes mentioned in the script output.

```
Microsoft Azure VM Backup - File Recovery

Connecting to recovery point using iSCSI service...
Connection succeeded!
Please wait while we attach volumes of the recovery point to this machine...
***** Volumes of the recovery point and their mount paths on this machine *****
Sr.No. | Disk | Volume | MountPath
1) | /dev/sdf | /dev/sdf1 | /home/arvindt/Documents/ILRCentOS73-20170309145505/Volume1
2) | /dev/sdg | /dev/sdg1 | /home/arvindt/Documents/ILRCentOS73-20170309145505/Volume2
3) | /dev/sdg | /dev/sdg2 | /home/arvindt/Documents/ILRCentOS73-20170309145505/Volume3
```

## Closing the connection

After identifying the files and copying them to a local storage location, remove (or unmount) the additional drives. To unmount the drives, on the **File Recovery** menu in the Azure portal, click **Unmount Disks**.

**File Recovery**  
v2win2012r2

✓ Step 1: Select recovery point  
7/20/2017, 1:36:40 PM [Latest] (AppCo... ▾)

✓ 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 Executable \***

✓ Download completed.

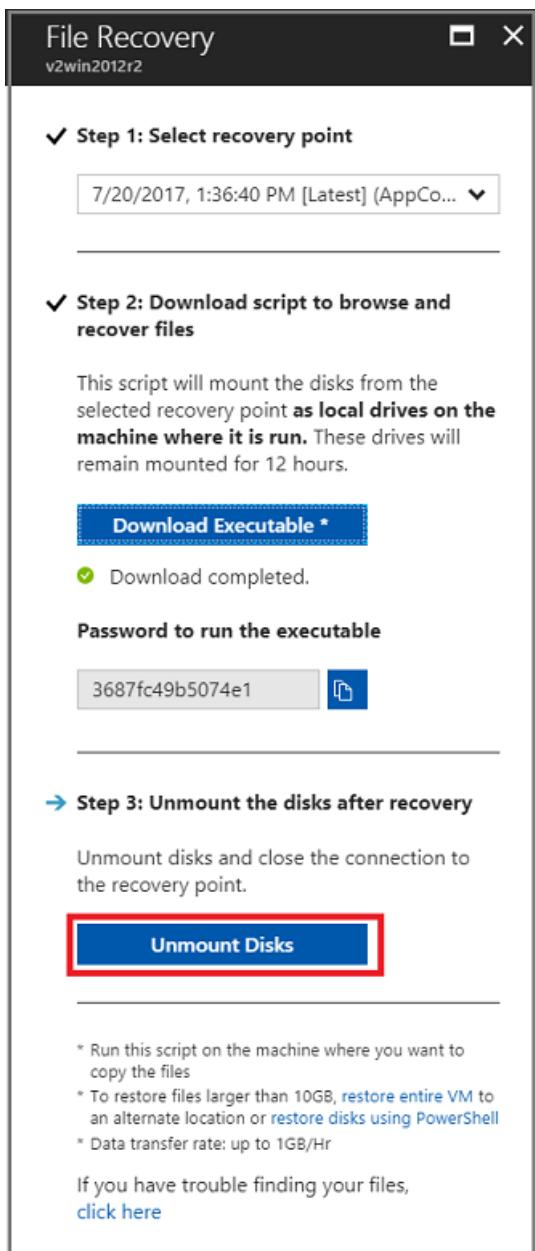
**Password to run the executable**  
3687fc49b5074e1 

→ Step 3: Unmount the disks after recovery  
Unmount disks and close the connection to the recovery point.

**Unmount Disks**

\* Run this script on the machine where you want to copy the files  
\* To restore files larger than 10GB, [restore entire VM](#) to an alternate location or [restore disks using PowerShell](#)  
\* Data transfer rate: up to 1GB/Hr

If you have trouble finding your files, [click here](#)



Once the disks have been unmounted, you receive a message. It may take a few minutes for the connection to refresh so that you can remove the disks.

In Linux, after the connection to the recovery point is severed, the OS doesn't remove the corresponding mount paths automatically. The mount paths exist as "orphan" volumes and are visible, but throw an error when you access/write the files. They can be manually removed. The script, when run, identifies any such volumes existing from any previous recovery points and cleans them up upon consent.

## Special configurations

### Dynamic disks

If the protected Azure VM has volumes with one or both of the following characteristics, you can't run the executable script on the same VM.

- Volumes that span multiple disks (spanned and striped volumes)
- Fault-tolerant volumes (mirrored and RAID-5 volumes) on dynamic disks

Instead, run the executable script on any other computer with a compatible operating system.

### Windows Storage Spaces

Windows Storage Spaces is a Windows technology that enables you to virtualize storage. With Windows Storage

Spaces you can group industry-standard disks into storage pools. Then you use the available space in those storage pools to create virtual disks, called storage spaces.

If the protected Azure VM uses Windows Storage Spaces, you can't run the executable script on the same VM. Instead, run the executable script on any other machine with a compatible operating system.

### LVM/RAID arrays

In Linux, Logical volume manager (LVM) and/or software RAID Arrays are used to manage logical volumes over multiple disks. If the protected Linux VM uses LVM and/or RAID Arrays, you can't run the script on the same VM. Instead run the script on any other machine with a compatible OS and which supports the file system of the protected VM.

The following script output displays the LVM and/or RAID Arrays disks and the volumes with the partition type.

```
***** Volumes from RAID Arrays/LVM partitions *****

Sr.No. | Disk | Volume | Partition Type

1) | /dev/sdc | /dev/sdc1 | Linux raid autodetect partition
2) | /dev/sdd | /dev/sdd1 | Linux raid autodetect partition
3) | /dev/sde | /dev/sde1 | Linux LVM Physical Volume partition
4) | /dev/sdh | /dev/sdh1 | Linux LVM Physical Volume partition

Run the following commands to mount and bring the partitions online.
```

To bring these partitions online, run the commands in the following sections.

#### For LVM partitions

To list the volume group names under a physical volume:

```
#!/bin/bash
pvs <volume name as shown above in the script output>
```

To list all logical volumes, names, and their paths in a volume group:

```
#!/bin/bash
lvdisplay <volume-group-name from the pvs command's results>
```

To mount the logical volumes to the path of your choice:

```
#!/bin/bash
mount <LV path> </mountpath>
```

#### For RAID arrays

The following command displays details about all raid disks:

```
#!/bin/bash
mdadm -detail -scan
```

The relevant RAID disk is displayed as `/dev/mdm/<RAID array name in the protected VM>`

Use the mount command if the RAID disk has physical volumes:

```

#!/bin/bash
mount [RAID Disk Path] [/mountpath]

```

If the RAID disk has another LVM configured in it, then use the preceding procedure for LVM partitions but use the volume name in place of the RAID Disk name.

## System requirements

### For Windows OS

The following table shows the compatibility between server and computer operating systems. When recovering files, you can't restore files to a previous or future operating system version. For example, you can't restore a file from a Windows Server 2016 VM to Windows Server 2012 or a Windows 8 computer. You can restore files from a VM to the same server operating system, or to the compatible client operating system.

| SERVER OS              | COMPATIBLE CLIENT OS |
|------------------------|----------------------|
| Windows Server 2019    | Windows 10           |
| Windows Server 2016    | Windows 10           |
| Windows Server 2012 R2 | Windows 8.1          |
| Windows Server 2012    | Windows 8            |
| Windows Server 2008 R2 | Windows 7            |

### For Linux OS

In Linux, the OS of the computer used to restore files must support the file system of the protected virtual machine. When selecting a computer to run the script, ensure the computer has a compatible OS, and uses one of the versions identified in the following table:

| LINUX OS     | VERSIONS        |
|--------------|-----------------|
| Ubuntu       | 12.04 and above |
| CentOS       | 6.5 and above   |
| RHEL         | 6.7 and above   |
| Debian       | 7 and above     |
| Oracle Linux | 6.4 and above   |
| SLES         | 12 and above    |
| openSUSE     | 42.2 and above  |

#### NOTE

We have found some issues in running the file recovery script on machines with SLES 12 SP4 OS and we are investigating with the SLES team. Currently, running the file recovery script is working on machines with SLES 12 SP2 and SP3 OS versions.

The script also requires Python and bash components to execute and connect securely to the recovery point.

| COMPONENT | VERSION                 |
|-----------|-------------------------|
| bash      | 4 and above             |
| python    | 2.6.6 and above         |
| TLS       | 1.2 should be supported |

## Access requirements

If you run the script on a computer with restricted access, ensure there is access to:

- [download.microsoft.com](https://download.microsoft.com)
- Recovery Service URLs (geo-name refers to the region where the recovery service vault resides)
  - <https://pod01-rec2.geo-name.backup.windowsazure.com> (For Azure public geos)
  - <https://pod01-rec2.geo-name.backup.windowsazure.cn> (For Azure China 21Vianet)
  - <https://pod01-rec2.geo-name.backup.windowsazure.us> (For Azure US Government)
  - <https://pod01-rec2.geo-name.backup.windowsazure.de> (For Azure Germany)
- Outbound ports 53 (DNS), 443, 3260

#### NOTE

- The downloaded script file name will have the **geo-name** to be filled in the URL. For example: The downloaded script name begins with 'VMname' '\_geoname' '\_GUID', like *ContosoVM\_wcus\_12345678*
- The URL would be <https://pod01-rec2.wcus.backup.windowsazure.com>"

For Linux, the script requires 'open-iscsi' and 'lshw' components to connect to the recovery point. If the components don't exist on the computer where the script is run, the script asks for permission to install the components. Provide consent to install the necessary components.

The access to [download.microsoft.com](https://download.microsoft.com) is required to download components used to build a secure channel between the machine where the script is run and the data in the recovery point.

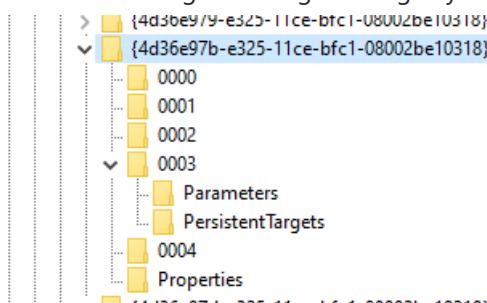
You can run the script on any machine that has the same (or compatible) operating system as the backed-up VM. See the [Compatible OS table](#) for compatible operating systems. If the protected Azure virtual machine uses Windows Storage Spaces (for Windows Azure VMs) or LVM/RAID Arrays (for Linux VMs), you can't run the executable or script on the same virtual machine. Instead, run the executable or script on any other machine with a compatible operating system.

## File recovery from Virtual machine backups having large disks

This section explains how to perform file recovery from backups of Azure Virtual machines with more than 16 disks and each disk size is greater than 32 TB.

Since file recovery process attaches all disks from the backup, when large number of disks (>16) or large disks (> 32 TB each) are used, the following action points are recommended:

- Keep a separate restore server (Azure VM D2v3 VMs) for file recovery. You can use that only for file recovery and then shut it down when not required. Restoring on the original machine isn't recommended since it will have significant impact on the VM itself.
- Then run the script once to check if the file recovery operation succeeds.
- If the file recovery process hangs (the disks are never mounted or they're mounted but volumes don't appear), perform the following steps.
  - If the restore server is a Windows VM:
    - Ensure that the OS is WS 2012 or higher.
    - Ensure the registry keys are set as suggested below in the restore server and make sure to reboot the server. The number beside the GUID can range from 0001-0005. In the following example, it's 0004. Navigate through the registry key path until the parameters section.



```
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Disk\TimeOutValue - change this from 60 to 1200
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4d36e97b-e325-11ce-bfc1-08002be10318}\0003\Parameters\SrbTimeoutDelta - change this from 15 to 1200
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4d36e97b-e325-11ce-bfc1-08002be10318}\0003\Parameters\EnableNPOut - change this from 0 to 1
- HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4d36e97b-e325-11ce-bfc1-08002be10318}\0003\Parameters\MaxRequestHoldTime - change this from 60 to 1200
```

- If the restore server is a Linux VM:
  - In the file /etc/iscsi/iscsid.conf, change the setting from:
    - node.conn[0].timeo.nop\_out\_timeout = 5 to node.conn[0].timeo.nop\_out\_timeout = 30
- After making the change above, run the script again. With these changes, it's highly probable that the file recovery will succeed.
- Each time user downloads a script, Azure Backup initiates the process of preparing the recovery point for download. With large disks, this process will take considerable time. If there are successive bursts of requests, the target preparation will go into a download spiral. Therefore, it's recommended to download a script from Portal/Powershell/CLI, wait for 20-30 minutes (a heuristic) and then run it. By this time, the target is expected to be ready for connection from script.
- After file recovery, make sure you go back to the portal and click **Unmount disks** for recovery points where you weren't able to mount volumes. Essentially, this step will clean any existing processes/sessions and increase the chance of recovery.

## Troubleshooting

If you have problems while recovering files from the virtual machines, check the following table for additional information.

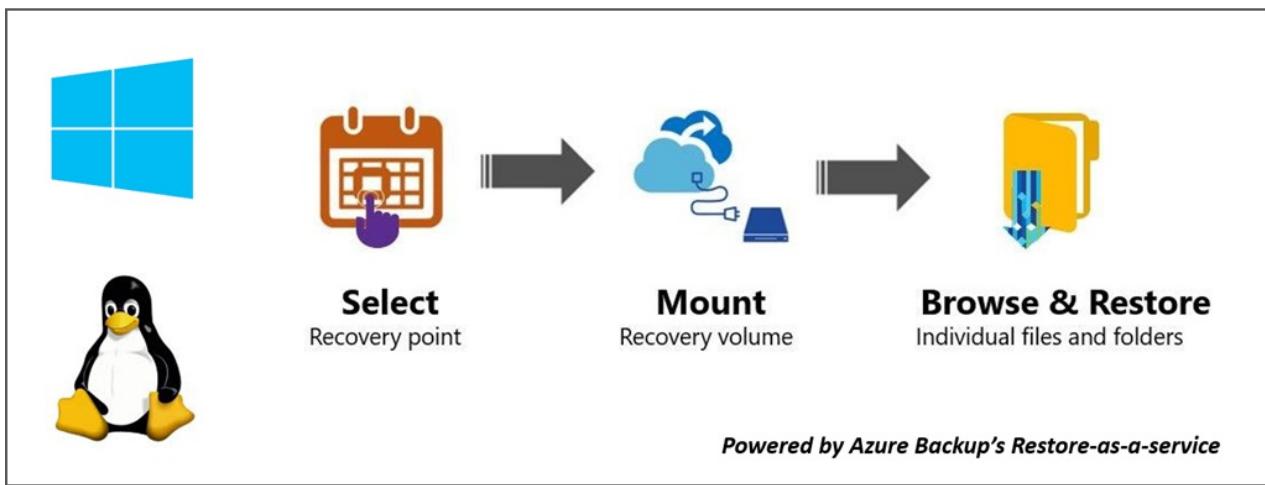
| ERROR MESSAGE / SCENARIO                                                                                                                                     | PROBABLE CAUSE                                                                                                         | RECOMMENDED ACTION                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Exe output: <i>Exception caught while connecting to target</i>                                                                                               | The script isn't able to access the recovery point                                                                     | Check whether the machine fulfills the <a href="#">previous access requirements</a> .                                                                                                                                                                                         |
| Exe output: <i>The target has already been logged in via an iSCSI session.</i>                                                                               | The script was already executed on the same machine and the drives have been attached                                  | The volumes of the recovery point have already been attached. They may NOT be mounted with the same drive letters of the original VM. Browse through all the available volumes in the file explorer for your file.                                                            |
| Exe output: <i>This script is invalid because the disks have been dismounted via portal/exceeded the 12-hr limit. Download a new script from the portal.</i> | The disks have been dismounted from the portal or the 12-hour limit was exceeded                                       | This particular exe is now invalid and can't be run. If you want to access the files of that recovery point-in-time, visit the portal for a new exe.                                                                                                                          |
| On the machine where the exe is run: The new volumes aren't dismounted after the dismount button is clicked                                                  | The iSCSI initiator on the machine isn't responding/refreshing its connection to the target and maintaining the cache. | After clicking <b>Dismount</b> , wait a few minutes. If the new volumes aren't dismounted, browse through all volumes. Browsing all volumes forces the initiator to refresh the connection, and the volume is dismounted with an error message that the disk isn't available. |
| Exe output: The script is run successfully but "New volumes attached" is not displayed on the script output                                                  | This is a transient error                                                                                              | The volumes will have been already attached. Open Explorer to browse. If you're using the same machine for running scripts every time, consider restarting the machine and the list should be displayed in the subsequent exe runs.                                           |
| Linux specific: Not able to view the desired volumes                                                                                                         | The OS of the machine where the script is run may not recognize the underlying filesystem of the protected VM          | Check whether the recovery point is crash-consistent or file-consistent. If file-consistent, run the script on another machine whose OS recognizes the protected VM's filesystem.                                                                                             |
| Windows specific: Not able to view the desired volumes                                                                                                       | The disks may have been attached but the volumes weren't configured                                                    | From the disk management screen, identify the additional disks related to the recovery point. If any of these disks are in an offline state, try bringing them online by right-clicking on the disk and click <b>Online</b> .                                                 |

## Security

This section discusses the various security measures taken for the implementation of file recovery from Azure VM backups.

### Feature flow

This feature was built to access the VM data without the need to restore the entire VM or VM disks and with the minimum number of steps. Access to VM data is provided by a script (which mounts the recovery volume when run as shown below) and it forms the cornerstone of all security implementations:



## Security implementations

### Select Recovery point (who can generate script)

The script provides access to VM data, so it's important to regulate who can generate it in the first place. You need to sign in into the Azure portal and be [RBAC authorized](#) to generate the script.

File recovery needs the same level of authorization as required for VM restore and disks restore. In other words, only authorized users can view the VM data can generate the script.

The generated script is signed with the official Microsoft certificate for the Azure Backup service. Any tampering with the script means the signature is broken, and any attempt to run the script is highlighted as a potential risk by the OS.

### Mount Recovery volume (who can run script)

Only an Admin can run the script and it should run in elevated mode. The script only runs a pre-generated set of steps and doesn't accept input from any external source.

To run the script, a password is required that is only shown to the authorized user at the time of generation of script in the Azure portal or PowerShell/CLI. This is to ensure that the authorized user who downloads the script is also responsible for running the script.

### Browse files and folders

To browse files and folders, the script uses the iSCSI initiator in the machine and connects to the recovery point that is configured as an iSCSI target. Here you can imagine scenarios where one is trying to imitate/spoof either/all components.

We use a mutual CHAP authentication mechanism so that each component authenticates the other. This means it's extremely difficult for a fake initiator to connect to the iSCSI target and for a fake target to be connected to the machine where the script is run.

The data flow between the recovery service and the machine is protected by building a secure SSL tunnel over TCP ([TLS 1.2 should be supported](#) in the machine where script is run).

Any file Access Control List (ACL) present in the parent/backed up VM are preserved in the mounted file system as well.

The script gives read-only access to a recovery point and is valid for only 12 hours. If you wish to remove the access earlier, then sign into Azure Portal/PowerShell/CLI and perform **unmount disks** for that particular recovery point. The script will be invalidated immediately.

## Next steps

- For any problems while restoring files, refer to the [Troubleshooting](#) section
- Learn how to [restore files via Powershell](#)

- Learn how to restore files via Azure CLI
- After VM is restored, learn how to [manage backups](#)

# Back up and restore encrypted Azure VM

2/24/2020 • 5 minutes to read • [Edit Online](#)

This article describes how to back up and restore Windows or Linux Azure virtual machines (VMs) with encrypted disks using the [Azure Backup](#) service.

If you want to learn more about how Azure Backup interacts with Azure VMs before you begin, review these resources:

- [Review](#) the Azure VM backup architecture.
- [Learn about](#) Azure VM backup, and the Azure Backup extension.

## Encryption support

Azure Backup supports backup of Azure VMs that have their OS/data disks encrypted with Azure Disk Encryption (ADE). ADE uses BitLocker for encryption of Windows VMs, and the dm-crypt feature for Linux VMs. ADE integrates with Azure Key Vault to manage disk-encryption keys and secrets. Key Vault Key Encryption Keys (KEKs) can be used to add an additional layer of security, encrypting encryption secrets before writing them to Key Vault.

Azure Backup can back up and restore Azure VMs using ADE with and without the Azure AD app, as summarized in the following table.

| VM DISK TYPE     | ADE (BEK/DM-CRYPT) | ADE AND KEK |
|------------------|--------------------|-------------|
| <b>Unmanaged</b> | Yes                | Yes         |
| <b>Managed</b>   | Yes                | Yes         |

- Learn more about [ADE](#), [Key Vault](#), and [KEKs](#).
- Read the [FAQ](#) for Azure VM disk encryption.

## Limitations

- You can back up and restore encrypted VMs within the same subscription and region.
- Azure Backup supports VMs encrypted using standalone keys. Any key that is a part of a certificate used to encrypt a VM isn't currently supported.
- You can back up and restore encrypted VMs within the same subscription and region as the Recovery Services Backup vault.
- Encrypted VMs can't be recovered at the file/folder level. You need to recover the entire VM to restore files and folders.
- When restoring a VM, you can't use the [replace existing VM](#) option for encrypted VMs. This option is only supported for unencrypted managed disks.

## Before you start

Before you start, do the following:

1. Make sure you have one or more [Windows](#) or [Linux](#) VMs with ADE enabled.
2. [Review the support matrix](#) for Azure VM backup
3. [Create](#) a Recovery Services Backup vault if you don't have one.
4. If you enable encryption for VMs that are already enabled for backup, you simply need to provide Backup with

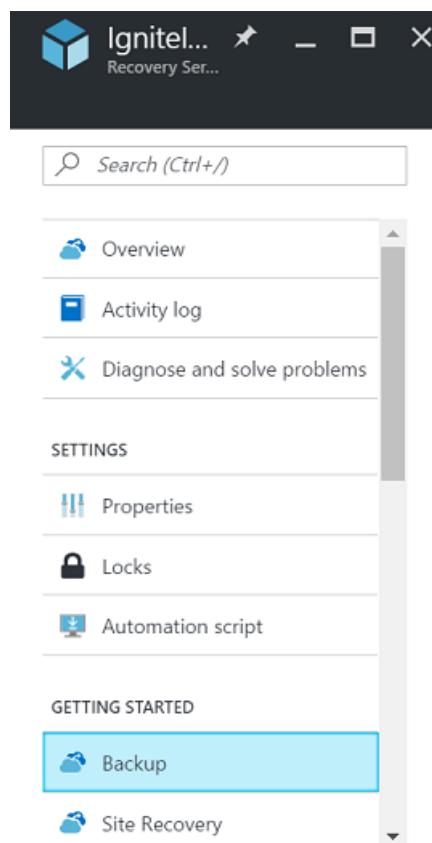
permissions to access the Key Vault so that backups can continue without disruption. [Learn more](#) about assigning these permissions.

In addition, there are a couple of things that you might need to do in some circumstances:

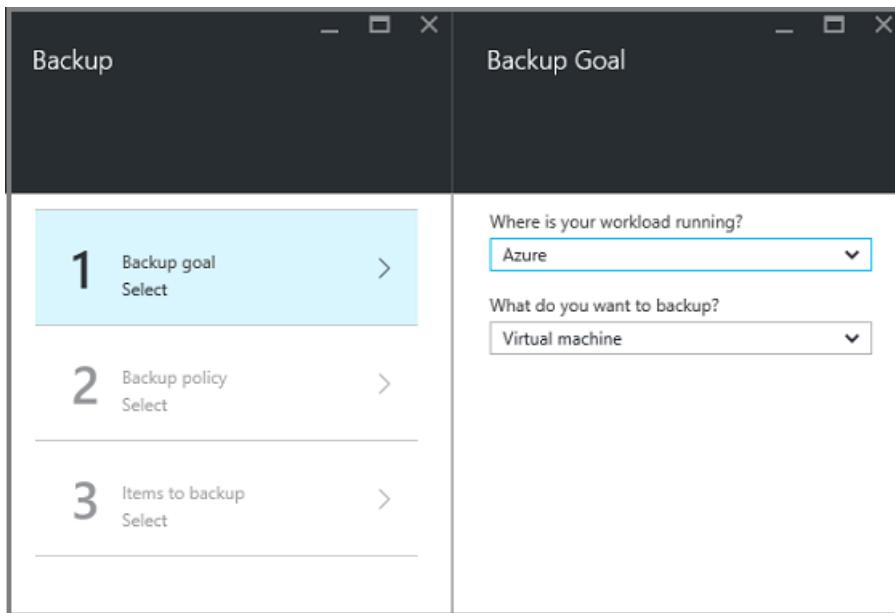
- **Install the VM agent on the VM:** Azure Backup backs up Azure VMs by installing an extension to the Azure VM agent running on the machine. If your VM was created from an Azure marketplace image, the agent is installed and running. If you create a custom VM, or you migrate an on-premises machine, you might need to [install the agent manually](#).

## Configure a backup policy

1. If you haven't yet created a Recovery Services backup vault, follow [these instructions](#)
2. Open the vault in the portal, and select **Backup** in the **Getting Started** section.

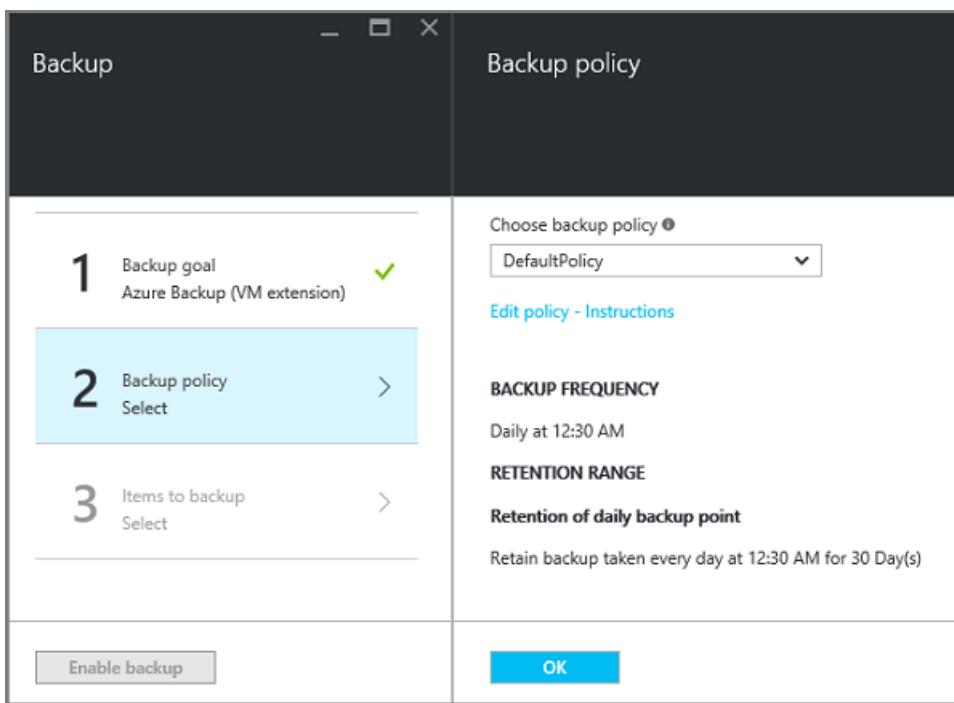


3. In **Backup goal > Where is your workload running?** select **Azure**.
4. In **What do you want to back up?** select **Virtual machine** > **OK**.

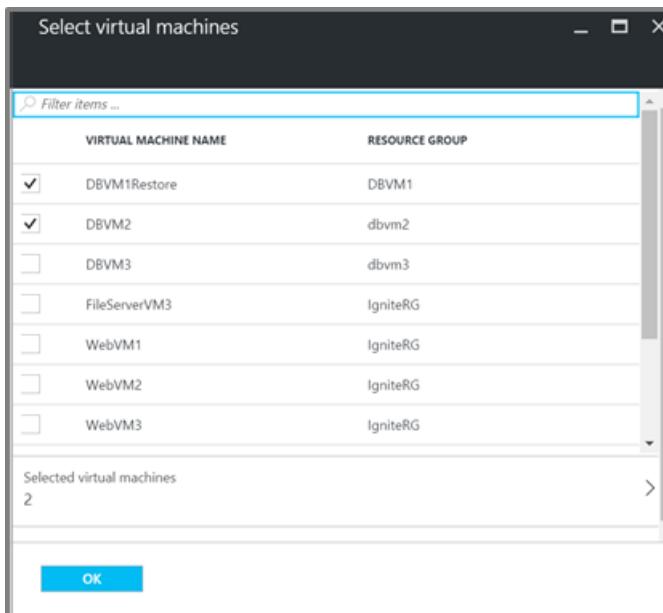


5. In **Backup policy > Choose backup policy**, select the policy that you want to associate with the vault. Then click **OK**.

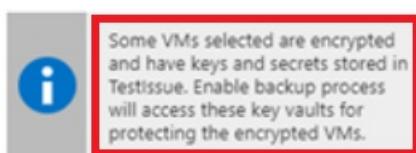
- A backup policy specifies when backups are taken, and how long they are stored.
- The details of the default policy are listed under the drop-down menu.



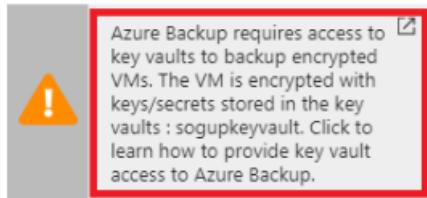
6. If you don't want to use the default policy, select **Create New**, and [create a custom policy](#).  
7. Choose the encrypted VMs you want to back up using the select policy, and select **OK**.



8. If you're using Azure Key Vault, on the vault page, you see a message that Azure Backup needs read-only access to the keys and secrets in the Key Vault.
  - If you receive this message, no action is required.



- If you receive this message, you need to set permissions as described in the [procedure below](#).



9. Click **Enable Backup** to deploy the backup policy in the vault, and enable backup for the selected VMs.

## Trigger a backup job

The initial backup will run in accordance with the schedule, but you can run it immediately as follows:

1. In the vault menu, click **Backup items**.
2. In **Backup Items**, click **Azure Virtual Machine**.
3. In the **Backup Items** list, click the ellipses (...).
4. Click **Backup now**.
5. In **Backup Now**, use the calendar control to select the last day that the recovery point should be retained. Then click **OK**.
6. Monitor the portal notifications. You can monitor the job progress in the vault dashboard > **Backup Jobs** > **In progress**. Depending on the size of your VM, creating the initial backup may take a while.

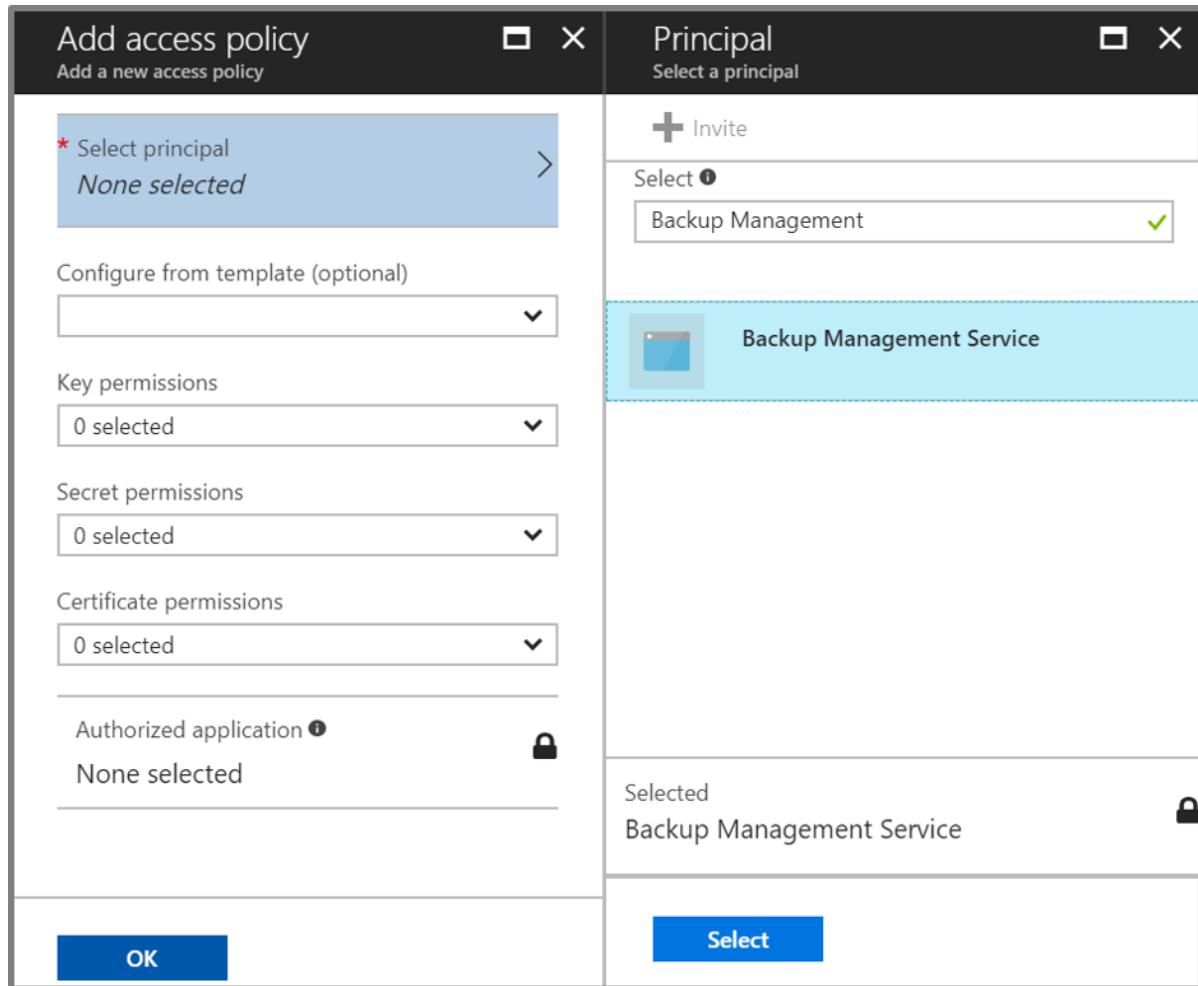
## Provide permissions

Azure VM needs read-only access to back up the keys and secrets, along with the associated VMs.

- Your Key Vault is associated with the Azure AD tenant of the Azure subscription. If you're a **Member user**, Azure Backup acquires access to the Key Vault without further action.
- If you're a **Guest user**, you must provide permissions for Azure Backup to access the key vault.

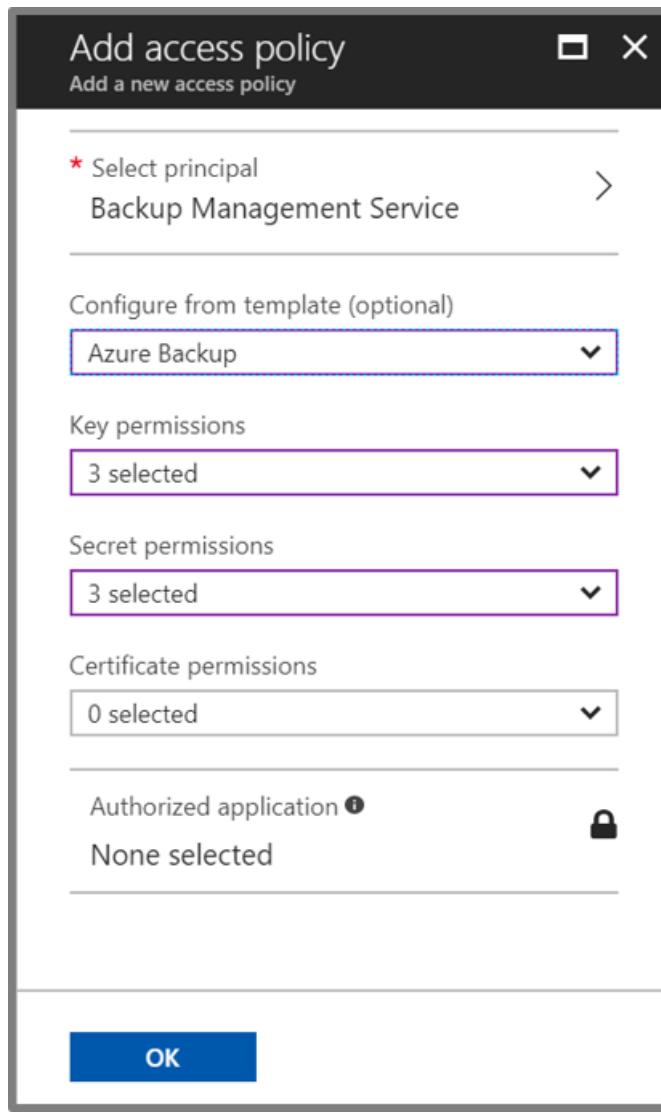
To set permissions:

1. In the Azure portal, select **All services**, and search for **Key vaults**.
2. Select the key vault associated with the encrypted VM you're backing up.
3. Select **Access policies** > **Add new**.
4. Select **Select principal**, and then type **Backup Management**.
5. Select **Backup Management Service** > **Select**.



6. In **Add access policy** > **Configure from template (optional)**, select **Azure Backup**.

- The required permissions are prefilled for **Key permissions** and **Secret permissions**.
- If your VM is encrypted using **BEK only**, remove the selection for **Key permissions** since you only need permissions for secrets.



7. Click **OK**. **Backup Management Service** is added to **Access policies**.

The screenshot shows the 'Access policies' page in the Azure portal. The left sidebar has 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', and 'Diagnose and solve problems'. Under 'SETTINGS', 'Access policies' is highlighted with a blue background, while 'Keys', 'Secrets', 'Advanced access policies', and 'Properties' are not. The main area shows a search bar, save, discard, and refresh buttons. A 'Add new' button with a plus sign is visible. Below it, a row shows a user icon and a blurred name. Another row shows a blue folder icon and 'Backup Management Service APPLICATION'. The title of the page is '- Access policies'.

8. Click **Save** to provide Azure Backup with the permissions.

## Restore an encrypted VM

You restore encrypted VMs as follows:

1. [Restore the VM disk](#).
2. Recreate the virtual machine instance by doing one of the following:
  - a. Use the template that's generated during the restore operation to customize VM settings, and trigger VM deployment. [Learn more](#).
  - b. Create a new VM from the restored disks using PowerShell. [Learn more](#).
3. For Linux VMs, reinstall the ADE extension so the data disks are open and mounted.

## Next steps

If you run into any issues, review these articles:

- [Common errors](#) when backing up and restoring encrypted Azure VMs.
- [Azure VM agent/backup extension issues](#).

# Restore Key Vault key and secret for encrypted VMs using Azure Backup

12/16/2019 • 4 minutes to read • [Edit Online](#)

This article talks about using Azure VM Backup to perform restore of encrypted Azure VMs, if your key and secret do not exist in the key vault. These steps can also be used if you want to maintain a separate copy of key (Key Encryption Key) and secret (BitLocker Encryption Key) for the restored VM.

## NOTE

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

## Prerequisites

- **Backup encrypted VMs** - Encrypted Azure VMs have been backed up using Azure Backup. Refer the article [Manage backup and restore of Azure VMs using PowerShell](#) for details about how to back up encrypted Azure VMs.
- **Configure Azure Key Vault** – Ensure that key vault to which keys and secrets need to be restored is already present. Refer the article [Get Started with Azure Key Vault](#) for details about key vault management.
- **Restore disk** - Ensure that you have triggered restore job for restoring disks for encrypted VM using [PowerShell steps](#). This is because this job generates a JSON file in your storage account containing keys and secrets for the encrypted VM to be restored.

## Get key and secret from Azure Backup

## NOTE

Once disk has been restored for the encrypted VM, ensure that:

- \$details is populated with restore disk job details, as mentioned in [PowerShell steps in Restore the Disks section](#)
- VM should be created from restored disks only **after key and secret is restored to key vault**.

Query the restored disk properties for the job details.

```
$properties = $details.properties
$storageAccountName = $properties["Target Storage Account Name"]
$containerName = $properties["Config Blob Container Name"]
$encryptedBlobName = $properties["Encryption Info Blob Name"]
```

Set the Azure storage context and restore JSON configuration file containing key and secret details for encrypted VM.

```

Set-AzCurrentStorageAccount -Name $storageaccountname -ResourceGroupName '<rg-name>'
$destination_path = 'C:\vmencryption_config.json'
Get-AzStorageBlobContent -Blob $encryptedBlobName -Container $containerName -Destination $destination_path
$encryptionObject = Get-Content -Path $destination_path | ConvertFrom-Json

```

## Restore key

Once the JSON file is generated in the destination path mentioned above, generate key blob file from the JSON and feed it to restore key cmdlet to put the key (KEK) back in the key vault.

```

$keyDestination = 'C:\keyDetails.blob'
[io.file]::WriteAllBytes($keyDestination,
[System.Convert]::FromBase64String($encryptionObject.OsDiskKeyAndSecretDetails.KeyBackupData))
Restore-AzureKeyVaultKey -VaultName '<target_key_vault_name>' -InputFile $keyDestination

```

## Restore secret

Use the JSON file generated above to get secret name and value and feed it to set secret cmdlet to put the secret (BEK) back in the key vault. Use these cmdlets if your **VM is encrypted using BEK and KEK**.

### Use these cmdlets if your Windows VM is encrypted using BEK and KEK.

```

$secretdata = $encryptionObject.OsDiskKeyAndSecretDetails.SecretData
$Secret = ConvertTo-SecureString -String $secretdata -AsPlainText -Force
$secretname = 'B3284AAA-DAAA-4AAA-B393-60CAA848AAAA'
$Tags = @{'DiskEncryptionKeyEncryptionAlgorithm' = 'RSA-OAEP'; 'DiskEncryptionKeyFileName' = 'B3284AAA-DAAA-4AAA-B393-60CAA848AAAA.BEK'; 'DiskEncryptionKeyEncryptionKeyURL' =
$encryptionObject.OsDiskKeyAndSecretDetails.KeyUrl; 'MachineName' = 'vm-name'}
Set-AzureKeyVaultSecret -VaultName '<target_key_vault_name>' -Name $secretname -SecretValue $Secret -
ContentType 'Wrapped BEK' -Tags $Tags

```

### Use these cmdlets if your Linux VM is encrypted using BEK and KEK.

```

$secretdata = $encryptionObject.OsDiskKeyAndSecretDetails.SecretData
$Secret = ConvertTo-SecureString -String $secretdata -AsPlainText -Force
$secretname = 'B3284AAA-DAAA-4AAA-B393-60CAA848AAAA'
$Tags = @{'DiskEncryptionKeyEncryptionAlgorithm' = 'RSA-OAEP'; 'DiskEncryptionKeyFileName' =
'LinuxPassPhraseFileName'; 'DiskEncryptionKeyEncryptionKeyURL' = <Key_url_of_newly_restored_key>; 'MachineName' =
'vm-name'}
Set-AzureKeyVaultSecret -VaultName '<target_key_vault_name>' -Name $secretname -SecretValue $Secret -
ContentType 'Wrapped BEK' -Tags $Tags

```

Use the JSON file generated above to get secret name and value and feed it to set secret cmdlet to put the secret (BEK) back in the key vault. Use these cmdlets if your **VM is encrypted using BEK only**.

```

$secretDestination = 'C:\secret.blob'
[io.file]::WriteAllBytes($secretDestination,
[System.Convert]::FromBase64String($encryptionObject.OsDiskKeyAndSecretDetails.KeyVaultSecretBackupData))
Restore-AzureKeyVaultSecret -VaultName '<target_key_vault_name>' -InputFile $secretDestination -Verbose

```

#### **NOTE**

- The value for \$secretname can be obtained by referring to the output of \$encryptionObject.OsDiskKeyAndSecretDetails.SecretUrl and using text after secrets/ e.g. output secret URL is <https://keyvaultname.vault.azure.net/secrets/B3284AAA-DAAA-4AAA-B393-60CAA848AAAA/xx00000xx0849999f3xx30000003163> and secret name is B3284AAA-DAAA-4AAA-B393-60CAA848AAAA
- The value of the tag DiskEncryptionKeyFileName is the same as the secret name.

## Create virtual machine from restored disk

If you have backed up encrypted VM using Azure VM Backup, the PowerShell cmdlets mentioned above help you restore key and secret back to the key vault. After restoring them, refer the article [Manage backup and restore of Azure VMs using PowerShell](#) to create encrypted VMs from restored disk, key, and secret.

## Legacy approach

The approach mentioned above would work for all the recovery points. However, the older approach of getting key and secret information from recovery point, would be valid for recovery points older than July 11, 2017 for VMs encrypted using BEK and KEK. Once restore disk job is complete for encrypted VM using [PowerShell steps](#), ensure that \$rp is populated with a valid value.

### **Restore key**

Use the following cmdlets to get key (KEK) information from recovery point and feed it to restore key cmdlet to put it back in the key vault.

```
$rp1 = Get-AzRecoveryServicesBackupRecoveryPoint -RecoveryPointId $rp[0].RecoveryPointId -Item $backupItem -KeyFileDownloadLocation 'C:\Users\downloads'
Restore-AzureKeyVaultKey -VaultName '<target_key_vault_name>' -InputFile 'C:\Users\downloads'
```

### **Restore secret**

Use the following cmdlets to get secret (BEK) information from recovery point and feed it to set secret cmdlet to put it back in the key vault.

```
$secretname = 'B3284AAA-DAAA-4AAA-B393-60CAA848AAAA'
$secretdata = $rp1.KeyAndSecretDetails.SecretData
$Secret = ConvertTo-SecureString -String $secretdata -AsPlainText -Force
$Tags = @{'DiskEncryptionKeyEncryptionAlgorithm' = 'RSA-OAEP'; 'DiskEncryptionKeyFileName' = 'B3284AAA-DAAA-4AAA-B393-60CAA848AAAA.BEK'; 'DiskEncryptionKeyEncryptionKeyURL' = 'https://mykeyvault.vault.azure.net:443/keys/KeyName/84daaac999949999030bf99aaa5a9f9'; 'MachineName' = 'vm-name'}
Set-AzureKeyVaultSecret -VaultName '<target_key_vault_name>' -Name $secretname -SecretValue $secret -Tags $Tags -SecretValue $Secret -ContentType 'Wrapped BEK'
```

**NOTE**

- Value for \$secretname can be obtained by referring to the output of \$rp1.KeyAndSecretDetails.SecretUrl and using text after secrets/ e.g. output secret URL is <https://keyvaultname.vault.azure.net/secrets/B3284AAA-DAAA-4AAA-B393-60CAA848AAAA/xx000000xx0849999f3xx30000003163> and secret name is B3284AAA-DAAA-4AAA-B393-60CAA848AAAA
- Value of the tag DiskEncryptionKeyFileName is same as secret name.
- Value for DiskEncryptionKeyEncryptionKeyURL can be obtained from key vault after restoring the keys back and using [Get-AzureKeyVaultKey](#) cmdlet

## Next steps

After restoring key and secret back to key vault, refer the article [Manage backup and restore of Azure VMs using PowerShell](#) to create encrypted VMs from restored disk, key, and secret.

# Manage Azure VM backups with Azure Backup service

2/4/2020 • 6 minutes to read • [Edit Online](#)

This article describes how to manage Azure virtual machines (VMs) that are backed up by using the [Azure Backup service](#). The article also summarizes the backup information you can find on the vault dashboard.

In the Azure portal, the Recovery Services vault dashboard provides access to vault information, including:

- The latest backup, which is also the latest restore point.
- The backup policy.
- The total size of all backup snapshots.
- The number of VMs that are enabled for backups.

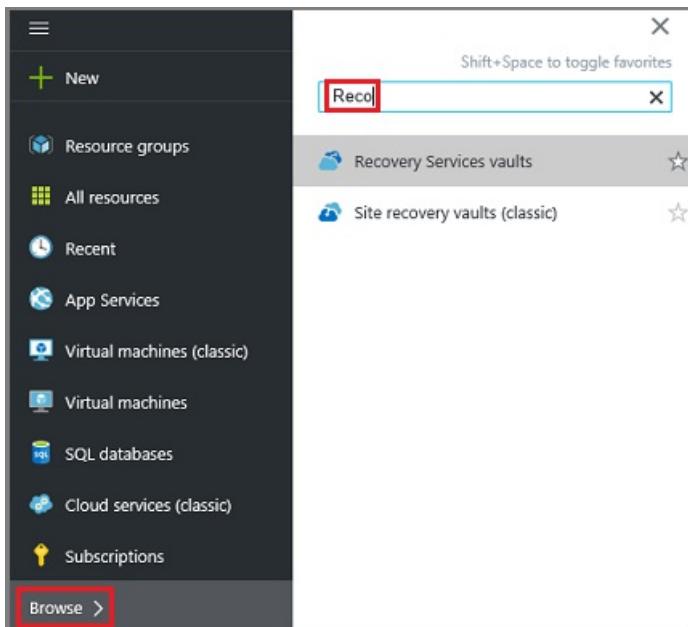
You can manage backups by using the dashboard and by drilling down to individual VMs. To begin machine backups, open the vault on the dashboard.

| BACKUP MANAGEMENT TYPE      | BACKUP ITEM COUNT |
|-----------------------------|-------------------|
| Azure Virtual Machine       | 1                 |
| SQL in Azure VM             | 0                 |
| Azure Storage (Azure Files) | 0                 |
| DPM                         | 0                 |
| Azure Backup Server         | 0                 |
| Azure Backup Agent          | 0                 |

## View VMs on the dashboard

To view VMs on the vault dashboard:

1. Sign in to the [Azure portal](#).
2. On the Hub menu, select **Browse**. In the list of resources, type **Recovery Services**. As you type, the list is filtered based on your input. Select **Recovery Services vaults**.



3. For ease of use, right-click the vault and select **Pin to dashboard**.

4. Open the vault dashboard.

5. On the **Backup Items** tile, select **Azure Virtual Machines**.

| BACKUP MANAGEMENT TYPE      | BACKUP ITEM COUNT |
|-----------------------------|-------------------|
| Azure Virtual Machine       | 1                 |
| SQL in Azure VM             | 0                 |
| Azure Storage (Azure Files) | 0                 |
| DPM                         | 0                 |
| Azure Backup Server         | 0                 |
| Azure Backup Agent          | 0                 |

6. On the **Backup Items** pane, you can view the list of protected VMs. In this example, the vault protects one virtual machine: demobackup.

Backup Items (Azure Virtual Machine)

| NAME       | RESOURCE GROUP | BACKUP PRE-CHECK | LAST BACKUP STATUS | LATEST RESTORE POINT  |
|------------|----------------|------------------|--------------------|-----------------------|
| demobackup | akkanasergfp10 | Passed           | Success            | 3/10/2019, 8:31:50 PM |

7. From the vault item's dashboard, modify backup policies, run an on-demand backup, stop or resume protection of VMs, delete backup data, view restore points, and run a restore.

demobackup

Backup now | Restore VM | File Recovery | Stop backup | Resume backup | Delete backup data

| CRASH CONSISTENT | APPLICATION CONSISTENT | FILE-SYSTEM CONSISTENT |
|------------------|------------------------|------------------------|
| 0                | 5                      | 0                      |

TIME | CONSISTENCY | RECOVERY TYPE

|                       |                        |       |
|-----------------------|------------------------|-------|
| 3/10/2019, 8:31:50 PM | Application Consistent | Vault |
| 3/9/2019, 8:36:16 PM  | Application Consistent | Vault |
| 3/8/2019, 8:40:49 PM  | Application Consistent | Vault |
| 3/7/2019, 8:33:29 PM  | Application Consistent | Vault |
| 3/6/2019, 8:37:45 PM  | Application Consistent | Vault |

## Manage backup policy for a VM

To manage a backup policy:

1. Sign in to the [Azure portal](#). Open the vault dashboard.
2. On the **Backup Items** tile, select **Azure Virtual Machines**.

| BACkUP MANAGEMENT TYPE      | BACkUP ITEM COUNT |
|-----------------------------|-------------------|
| Azure Virtual Machine       | 1                 |
| SQL in Azure VM             | 0                 |
| Azure Storage (Azure Files) | 0                 |
| DPM                         | 0                 |
| Azure Backup Server         | 0                 |
| Azure Backup Agent          | 0                 |

3. On the **Backup Items** pane, you can view the list of protected VMs and last backup status with latest restore points time.

The screenshot shows the 'Backup Items (Azure Virtual Machine)' page. At the top, there's a message: 'Fetching data from service completed.' Below is a search bar with the placeholder 'Filter items ...'. A table lists one item:

| NAME       | RESOURCE GROUP | BACKUP PRE-CHECK    | LAST BACKUP STATUS   | LATEST RESTORE POINT  | ... |
|------------|----------------|---------------------|----------------------|-----------------------|-----|
| demobackup | akkanasergfp10 | <span>Passed</span> | <span>Success</span> | 3/10/2019, 8:31:50 PM | ... |

4. From the vault item's dashboard, you can select a backup policy.

- To switch policies, select a different policy and then select **Save**. The new policy is immediately applied to the vault.

The screenshot shows the 'demobackup' vault item dashboard. On the right, the 'Backup Policy' pane is open, showing a dropdown menu with 'DefaultPolicy' selected. On the left, there's a summary table and a table of restore points:

| TIME                  | CONSISTENCY            | RECOVERY TYPE |
|-----------------------|------------------------|---------------|
| 3/10/2019, 8:31:50 PM | Application Consistent | Vault         |
| 3/9/2019, 8:36:16 PM  | Application Consistent | Vault         |
| 3/8/2019, 8:40:49 PM  | Application Consistent | Vault         |
| 3/7/2019, 8:33:29 PM  | Application Consistent | Vault         |
| 3/6/2019, 8:37:45 PM  | Application Consistent | Vault         |

## Run an on-demand backup

You can run an on-demand backup of a VM after you set up its protection. Keep these details in mind:

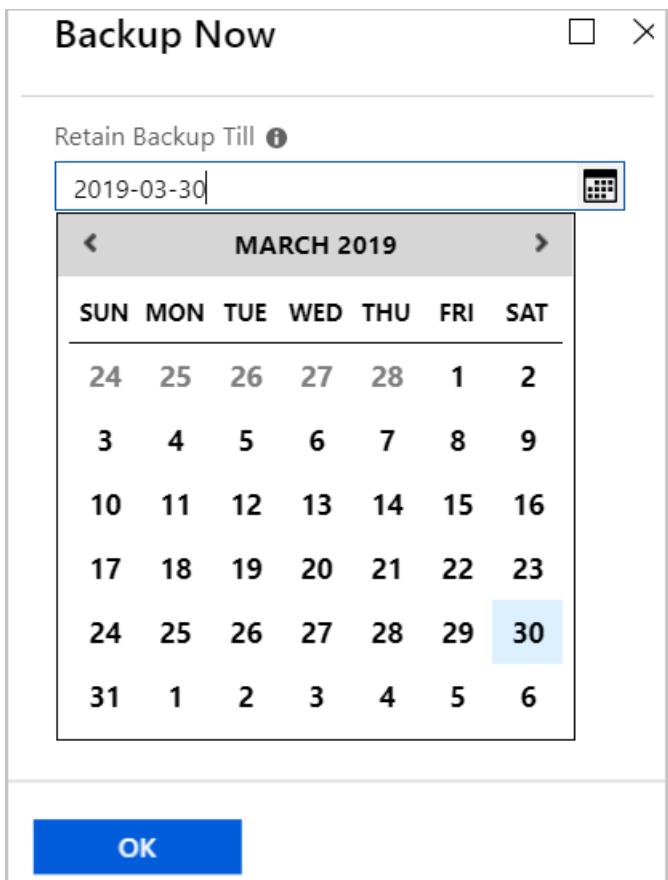
- If the initial backup is pending, on-demand backup creates a full copy of the VM in the Recovery Services vault.
- If the initial backup is complete, an on-demand backup will only send changes from the previous snapshot to the Recovery Services vault. That is, later backups are always incremental.
- The retention range for an on-demand backup is the retention value that you specify when you trigger the backup.

To trigger an on-demand backup:

- On the **vault item dashboard**, under **Protected Item**, select **Backup Item**.

The screenshot shows the 'Protected Item' ribbon with several buttons: 'Backup now' (highlighted with a red box), 'Restore VM', 'File Recovery', 'Stop backup', 'Resume backup', and 'Delete backup data'.

- From **Backup Management Type**, select **Azure Virtual Machine**. The **Backup Item (Azure Virtual Machine)** pane appears.
- Select a VM and select **Backup Now** to create an on-demand backup. The **Backup Now** pane appears.
- In the **Retain Backup Till** field, specify a date for the backup to be retained.



5. Select **OK** to run the backup job.

To track the job's progress, on the vault dashboard, select the **Backup Jobs** tile.

## Stop protecting a VM

There are two ways to stop protecting a VM:

- **Stop protection and retain backup data.** This option will stop all future backup jobs from protecting your VM; however, Azure Backup service will retain the recovery points that have been backed up. You'll need to pay to keep the recovery points in the vault (see [Azure Backup pricing](#) for details). You'll be able to restore the VM if needed. If you decide to resume VM protection, then you can use *Resume backup* option.
- **Stop protection and delete backup data.** This option will stop all future backup jobs from protecting your VM and delete all the recovery points. You won't be able to restore the VM nor use *Resume backup* option.

### NOTE

If you delete a data source without stopping backups, new backups will fail. Old recovery points will expire according to the policy, but one last recovery point will always be kept until you stop the backups and delete the data.

### Stop protection and retain backup data

To stop protection and retain data of a VM:

1. On the [vault item's dashboard](#), select **Stop backup**.
2. Choose **Retain Backup Data**, and confirm your selection as needed. Add a comment if you want. If you aren't sure of the item's name, hover over the exclamation mark to view the name.

## Stop Backup

SkipTransMac1

Retain Backup Data 



This option will stop all scheduled backup jobs but retains backup data. It will continue the pricing as is until data is removed.

Reason (optional)

0 selected 

Comments

**Stop backup**

A notification lets you know that the backup jobs have been stopped.

### Stop protection and delete backup data

To stop protection and delete data of a VM:

1. On the [vault item's dashboard](#), select **Stop backup**.
2. Choose **Delete Backup Data**, and confirm your selection as needed. Enter the name of the backup item and add a comment if you want.

**Stop Backup**

SkipTransMac1

Delete Backup Data

This option will stop all scheduled backup jobs, deletes backup data and can't be undone.

\* Type the name of Backup Item  
SkipTransMac1

Reason (optional)  
0 selected

Comments

**Stop backup**

## Resume protection of a VM

If you chose [Stop protection and retain backup data](#) option during stop VM protection, then you can use **Resume backup**. This option is not available if you choose [Stop protection and delete backup data](#) option or [Delete backup data](#).

To resume protection for a VM:

1. On the [vault item's dashboard](#), select **Resume backup**.
2. Follow the steps in [Manage backup policies](#) to assign the policy for the VM. You don't need to choose the VM's initial protection policy.
3. After you apply the backup policy to the VM, you see the following message:



## Delete backup data

There are two ways to delete a VM's backup data:

- From the vault item dashboard, select Stop backup and follow the instructions for [Stop protection and delete backup data](#) option.

- From the vault item dashboard, select Delete backup data. This option is enabled if you had chosen to [Stop protection and retain backup data](#) option during stop VM protection



- On the [vault item dashboard](#), select **Delete backup data**.
- Type the name of the backup item to confirm that you want to delete the recovery points.

**Stop Backup**  
SkipTransMac1

**Delete Backup Data**

**i** This option will stop all scheduled backup jobs, deletes backup data and can't be undone.

\* Type the name of Backup Item  
SkipTransMac1

Reason (optional)  
0 selected

Comments

**Stop backup**

The 'Delete Backup Data' button is highlighted with a purple border. A callout bubble from this button contains the text: 'This option will stop all scheduled backup jobs, deletes backup data and can't be undone.'

- To delete the backup data for the item, select **Delete**. A notification message lets you know that the backup data has been deleted.

To protect your data, Azure Backup includes the soft delete feature. With soft delete, even after the backup (all the recovery points) of a VM is deleted, the backup data is retained for 14 additional days. For more information, see [the soft delete documentation](#).

#### NOTE

When you delete backup data you delete all associated recovery points. You can't choose specific recovery points to delete.

#### Backup item where primary data source no longer exists

- If Azure VMs configured for Azure backup are either deleted or moved without stopping protection, then both scheduled backup jobs and on demand (ad-hoc) backup jobs will fail with the error UserErrorVmNotFoundV2. The backup pre-check will appear as critical only for failed on-demand backup jobs (failed scheduled jobs are not displayed).
- These backup items remain active in the system adhering to the backup and retention policy set by the user.

The backed-up data for these Azure VMs will be retained according to the retention policy. The expired recovery points (except the last recovery point) are cleaned according to the retention range set in the backup policy.

- Users are recommended to delete the backup items where the primary data source no longer exists to avoid any additional cost, if the backup item/data for the delete resources is no longer required as the last recovery point is retained forever and the user is charged as per the backup pricing applicable.

## Next steps

- Learn how to [back up Azure VMs from the VM's settings](#).
- Learn how to [restore VMs](#).
- Learn how to [monitor Azure VM backups](#).

# About SQL Server Backup in Azure VMs

11/25/2019 • 8 minutes to read • [Edit Online](#)

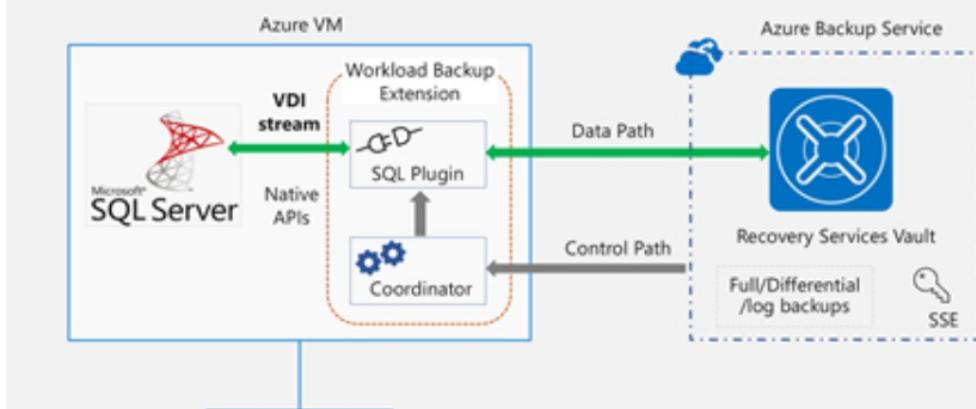
SQL Server databases are critical workloads that require a low recovery point objective (RPO) and long-term retention. You can back up SQL Server databases running on Azure VMs using [Azure Backup](#).

## Backup process

This solution leverages the SQL native APIs to take backups of your SQL databases.

- Once you specify the SQL Server VM that you want to protect and query for the databases in it, Azure Backup service will install a workload backup extension on the VM by the name `AzureBackupWindowsWorkload` extension.
- This extension consists of a coordinator and a SQL plugin. While the coordinator is responsible for triggering workflows for various operations like configure backup, backup and restore, the plugin is responsible for actual data flow.
- To be able to discover databases on this VM, Azure Backup creates the account `NT SERVICE\AzureWLBackupPluginSvc`. This account is used for backup and restore and requires SQL sysadmin permissions. The `NT SERVICE\AzureWLBackupPluginSvc` account is a [Virtual Service Account](#), and therefore does not require any password management. Azure Backup leverages the `NT AUTHORITY\SYSTEM` account for database discovery/inquiry, so this account needs to be a public login on SQL. If you didn't create the SQL Server VM from the Azure Marketplace, you might receive an error **UserErrorSQLNoSysadminMembership**. If this occurs [follow these instructions](#).
- Once you trigger configure protection on the selected databases, the backup service sets up the coordinator with the backup schedules and other policy details, which the extension caches locally on the VM.
- At the scheduled time, the coordinator communicates with the plugin and it starts streaming the backup data from the SQL server using VDI.
- The plugin sends the data directly to the recovery services vault, thus eliminating the need for a staging location. The data is encrypted and stored by the Azure Backup service in storage accounts.
- When the data transfer is complete, coordinator confirms the commit with the backup service.

## Architecture: Azure Backup for SQL Server running in Azure VM



# Before you start

Before you start, verify the below:

1. Make sure you have a SQL Server instance running in Azure. You can [quickly create a SQL Server instance](#) in the marketplace.
2. Review the [feature consideration](#) and [scenario support](#).
3. [Review common questions](#) about this scenario.

## Scenario support

| SUPPORT                              | DETAILS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Supported deployments</b>         | SQL Marketplace Azure VMs and non-Marketplace (SQL Server manually installed) VMs are supported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Supported geos</b>                | Australia South East (ASE), East Australia (AE), Australia Central (AC), Australia Central 2 (AC)<br>Brazil South (BRS)<br>Canada Central (CNC), Canada East (CE)<br>South East Asia (SEA), East Asia (EA)<br>East US (EUS), East US 2 (EUS2), West Central US (WCUS),<br>West US (WUS); West US 2 (WUS 2) North Central US (NCUS)<br>Central US (CUS) South Central US (SCUS)<br>India Central (INC), India South (INS), India West<br>Japan East (JPE), Japan West (JPW)<br>Korea Central (KRC), Korea South (KRS)<br>North Europe (NE), West Europe<br>UK South (UKS), UK West (UKW)<br>US Gov Arizona, US Gov Virginia, US Gov Texas, US DoD<br>Central, US DoD East<br>Germany North, Germany West Central<br>Switzerland North, Switzerland West<br>France Central<br>China East, China East 2, China North, China North 2 |
| <b>Supported operating systems</b>   | Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows Server 2008 R2 SP1<br><br>Linux isn't currently supported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Supported SQL Server versions</b> | SQL Server 2019, SQL Server 2017 as detailed on the <a href="#">Search product lifecycle page</a> , SQL Server 2016 and SPs as detailed on the <a href="#">Search product lifecycle page</a> , SQL Server 2014, SQL Server 2012, SQL Server 2008 R2, SQL Server 2008<br><br>Enterprise, Standard, Web, Developer, Express.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Supported .NET versions</b>       | .NET Framework 4.5.2 or later installed on the VM                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Feature consideration and limitations

- SQL Server backup can be configured in the Azure portal or **PowerShell**. We do not support CLI.
- The solution is supported on both kinds of [deployments](#) - Azure Resource Manager VMs and classic VMs.
- VM running SQL Server requires internet connectivity to access Azure public IP addresses.
- SQL Server **Failover Cluster Instance (FCI)** is not supported.
- Back up and restore operations for mirror databases and database snapshots aren't supported.

- Using more than one backup solutions to back up your standalone SQL Server instance or SQL Always on availability group may lead to backup failure; refrain from doing so.
- Backing up two nodes of an availability group individually with same or different solutions, may also lead to backup failure.
- Azure Backup supports only Full and Copy-only Full backup types for **Read-only** databases
- Databases with large number of files can't be protected. The maximum number of files that is supported is **~1000**.
- You can back up to **~2000** SQL Server databases in a vault. You can create multiple vaults in case you have a greater number of databases.
- You can configure backup for up to **50** databases in one go; this restriction helps optimize backup loads.
- We support databases up to **2 TB** in size; for sizes greater than that performance issues may come up.
- To have a sense of as to how many databases can be protected per server, we need to consider factors such as bandwidth, VM size, backup frequency, database size, etc. [Download](#) the resource planner that gives the approximate number of databases you can have per server based on the VM resources and the backup policy.
- In case of availability groups, backups are taken from the different nodes based on a few factors. The backup behavior for an availability group is summarized below.

### **Back up behavior in case of Always on availability groups**

It is recommended that the backup is configured on only one node of an AG. Backup should always be configured in the same region as the primary node. In other words, you always need the primary node to be present in the region in which you are configuring backup. If all the nodes of the AG are in the same region in which the backup is configured, there isn't any concern.

#### **For cross-region AG**

- Regardless of the backup preference, backups won't happen from the nodes that are not in the same region where the backup is configured. This is because the cross-region backups are not supported. If you have only two nodes and the secondary node is in the other region; in this case, the backups will continue to happen from primary node (unless your backup preference is 'secondary only').
- If a fail-over happens to a region different than the one in which the backup is configured, backups would fail on the nodes in the failed-over region.

Depending on the backup preference and backups types (full/differential/log/copy-only full), backups are taken from a particular node (primary/secondary).

- Backup preference: Primary**

| BACKUP TYPE    | NODE    |
|----------------|---------|
| Full           | Primary |
| Differential   | Primary |
| Log            | Primary |
| Copy-Only Full | Primary |

- Backup preference: Secondary Only**

| BACKUP TYPE | NODE    |
|-------------|---------|
| Full        | Primary |

| BACKUP TYPE    | NODE      |
|----------------|-----------|
| Differential   | Primary   |
| Log            | Secondary |
| Copy-Only Full | Secondary |

- **Backup preference: Secondary**

| BACKUP TYPE    | NODE      |
|----------------|-----------|
| Full           | Primary   |
| Differential   | Primary   |
| Log            | Secondary |
| Copy-Only Full | Secondary |

- **No Backup preference**

| BACKUP TYPE    | NODE      |
|----------------|-----------|
| Full           | Primary   |
| Differential   | Primary   |
| Log            | Secondary |
| Copy-Only Full | Secondary |

## Set VM permissions

When you run discovery on a SQL Server, Azure Backup does the following:

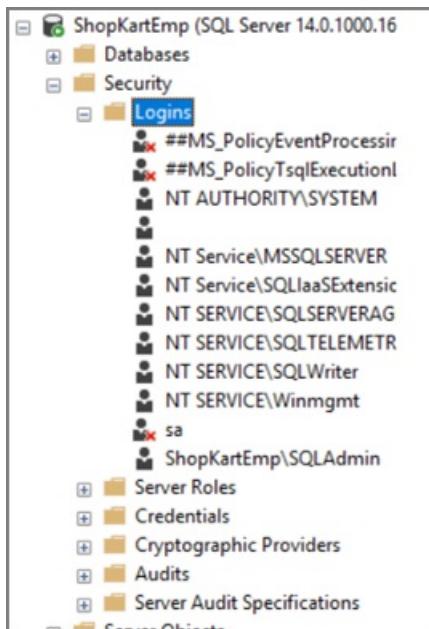
- Adds the AzureBackupWindowsWorkload extension.
- Creates an NT SERVICE\AzureWLBackupPluginSvc account to discover databases on the virtual machine. This account is used for a backup and restore and requires SQL sysadmin permissions.
- Discovers databases that are running on a VM, Azure Backup uses the NT AUTHORITY\SYSTEM account. This account must be a public sign-in on SQL.

If you didn't create the SQL Server VM in the Azure Marketplace or if you are on SQL 2008 and 2008 R2, you might receive a **UserErrorSQLNoSysadminMembership** error.

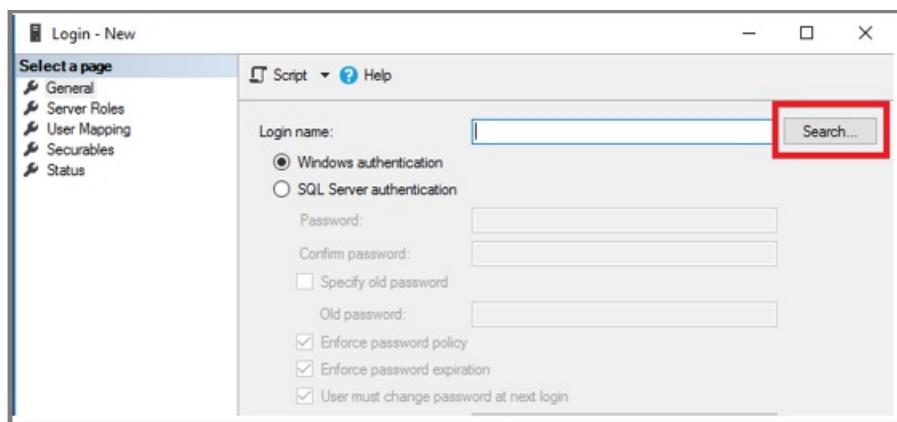
For giving permissions in case of **SQL 2008** and **2008 R2** running on Windows 2008 R2, refer [here](#).

For all other versions, fix permissions with the following steps:

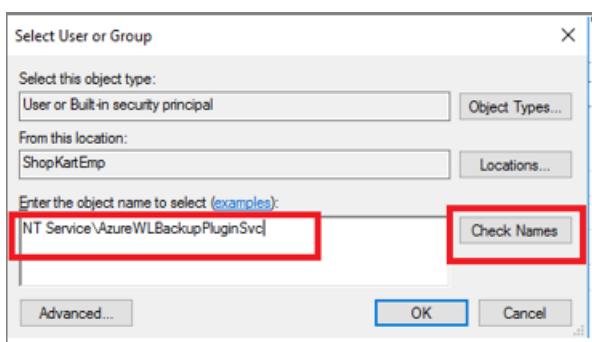
1. Use an account with SQL Server sysadmin permissions to sign in to SQL Server Management Studio (SSMS). Unless you need special permissions, Windows authentication should work.
2. On the SQL Server, open the **Security/Logins** folder.



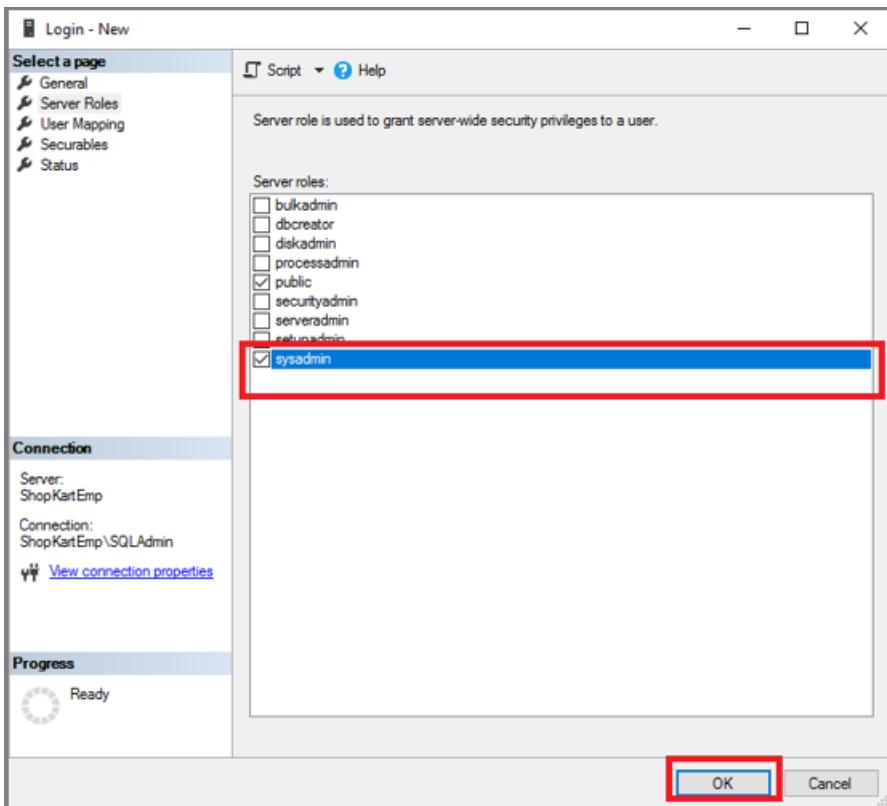
3. Right-click the **Logins** folder and select **New Login**. In **Login - New**, select **Search...**.



4. The Windows virtual service account **NT SERVICE\AzureWLBackupPluginSvc** was created during the virtual machine registration and SQL discovery phase. Enter the account name as shown in **Enter the object name to select**. Select **Check Names** to resolve the name. Click **OK**.



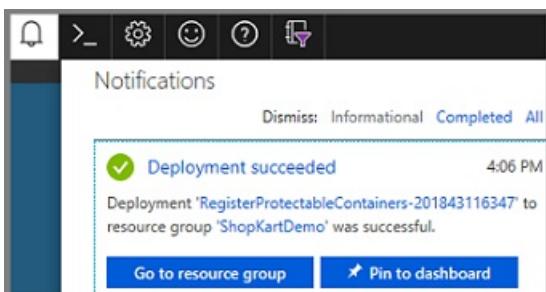
5. In **Server Roles**, make sure the **sysadmin** role is selected. Click **OK**. The required permissions should now exist.



6. Now associate the database with the Recovery Services vault. In the Azure portal, in the **Protected Servers** list, right-click the server that's in an error state > **Rediscover DBs**.

| VM NAME     | VM RG         | SERVER              | BUTTON | DETAILS       |
|-------------|---------------|---------------------|--------|---------------|
| sqlserver-0 | MercuryPMD... | sqlserver-0.shop... | Ready  | 3 DB(s) Found |
| sqlserver-1 | MercuryPMD... | sqlserver-1.shop... | Ready  | 3 DB(s) Found |
| ShopKartEmp | ShopKartDe... | shopkartemp         | Error  |               |
| ShopKarthR  | ShopKartDe... | shopkarthr          | Ready  | 3 DB(s) Found |
| sqlserver-0 | ShopKartDe... | sqlserver-0.shop... | Ready  | 3 DB(s) Found |
| sqlserver-1 | ShopKartDe... | sqlserver-1.shop... | Ready  | 3 DB(s) Found |
| SQLTest     | SQLUsability  | sqltest             | Ready  | 3 DB(s) Found |

7. Check progress in the **Notifications** area. When the selected databases are found, a success message appears.



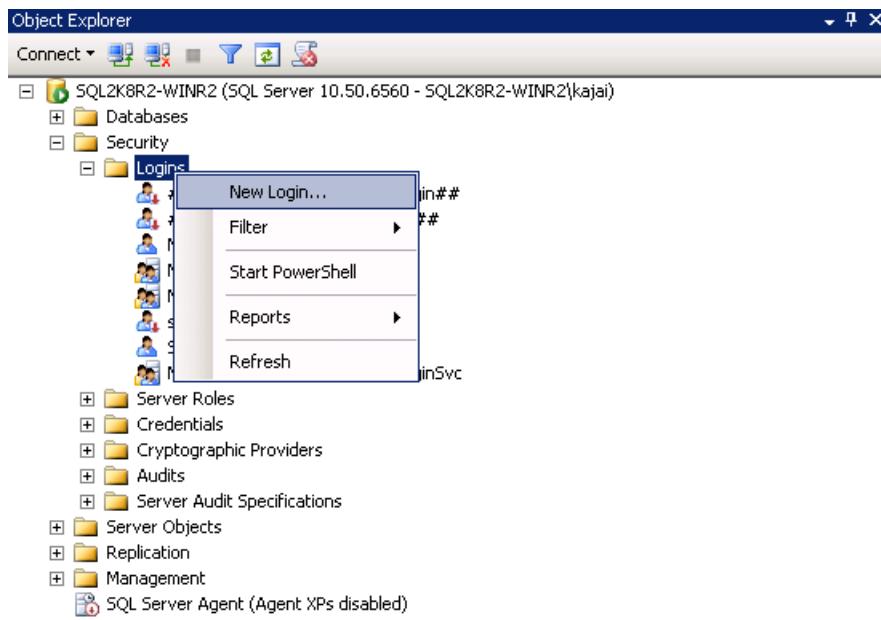
**NOTE**

If your SQL Server has multiple instances of SQL Server installed, then you must add sysadmin permission for **NT Service\AzureWLBackupPluginSvc** account to all SQL instances.

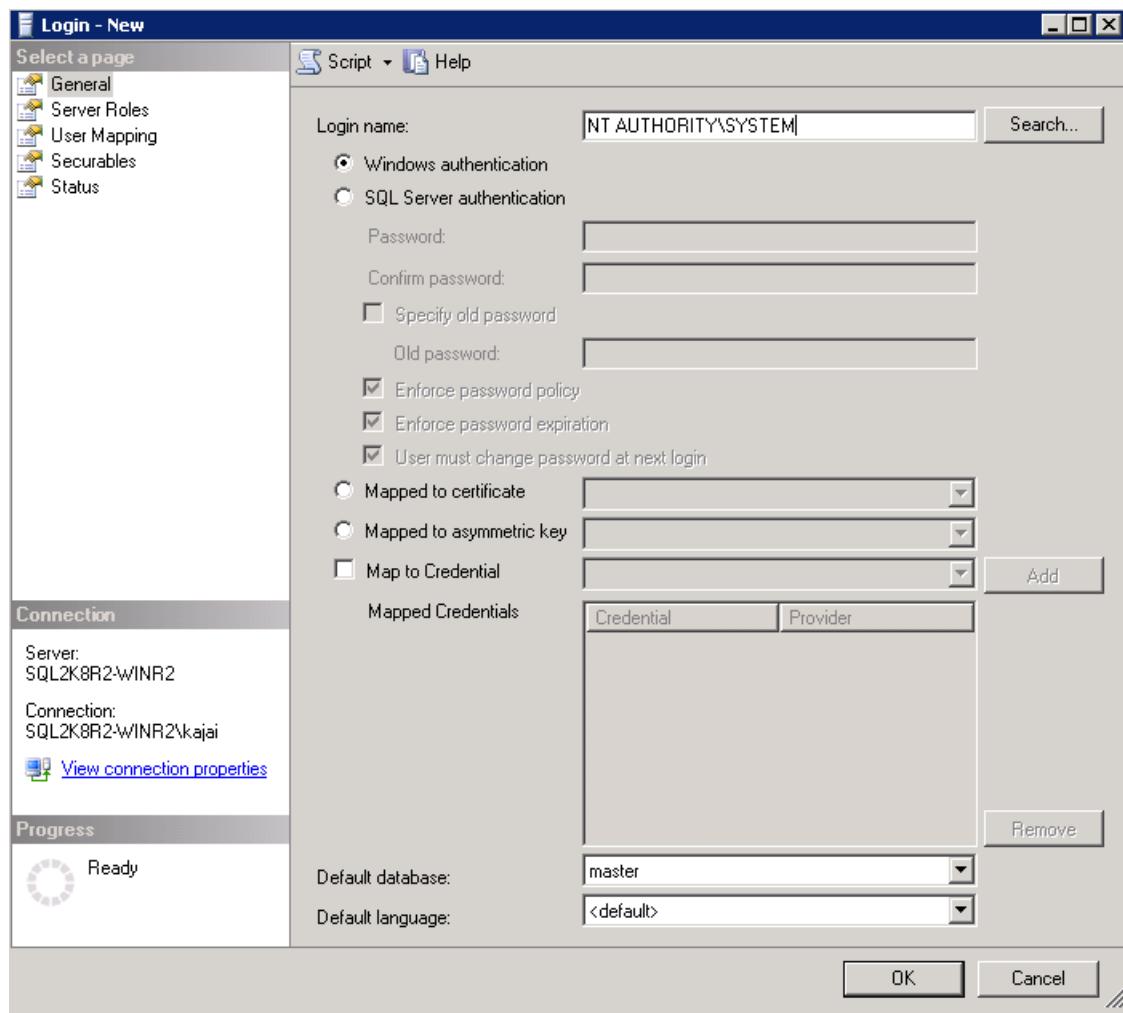
**Give SQL sysadmin permissions for SQL 2008 and SQL 2008 R2**

Add **NT AUTHORITY\SYSTEM** and **NT Service\AzureWLBackupPluginSvc** logins to the SQL Server Instance:

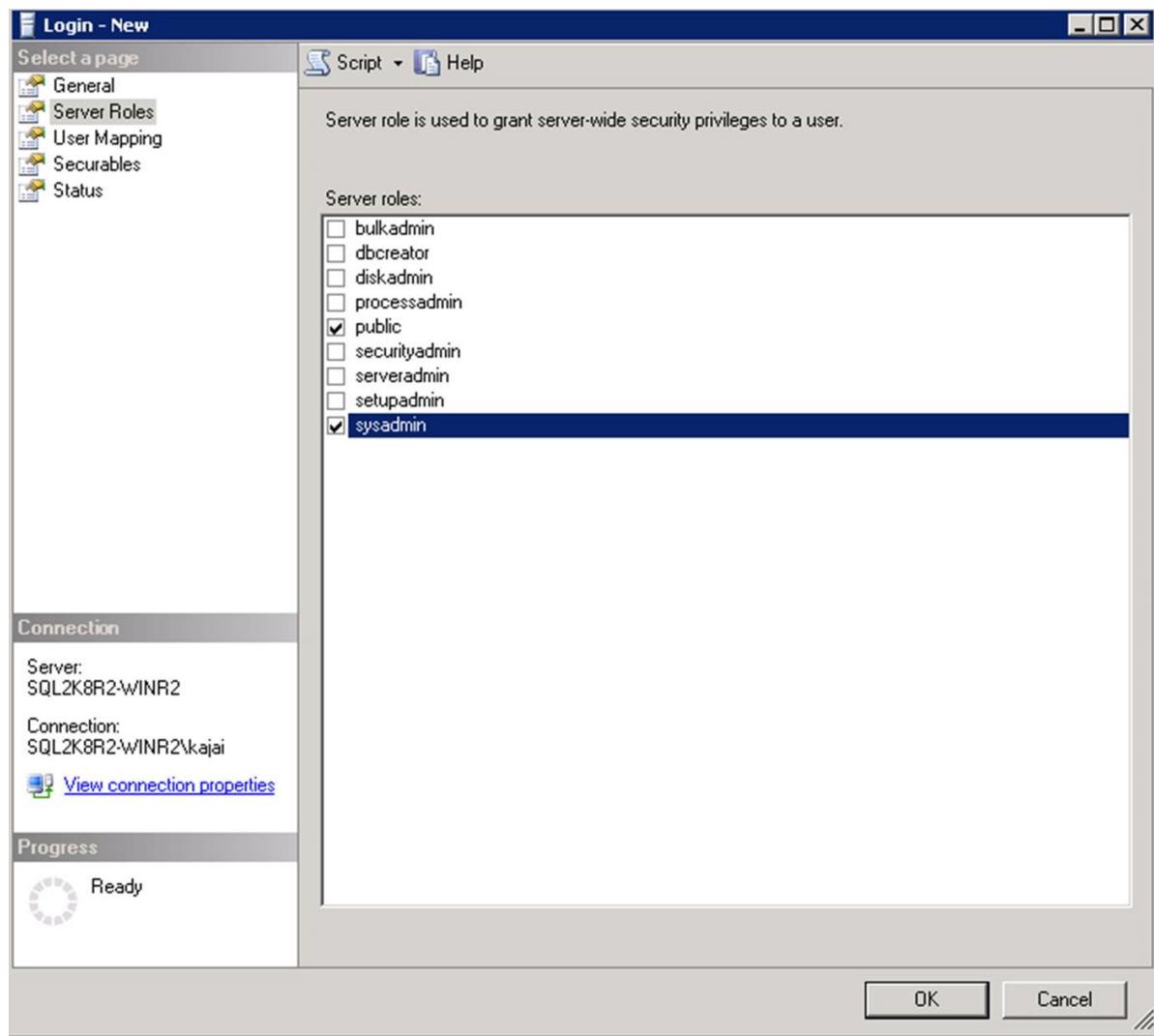
1. Go the SQL Server Instance in the Object explorer.
2. Navigate to Security -> Logins
3. Right click on the Logins and click *New Login...*



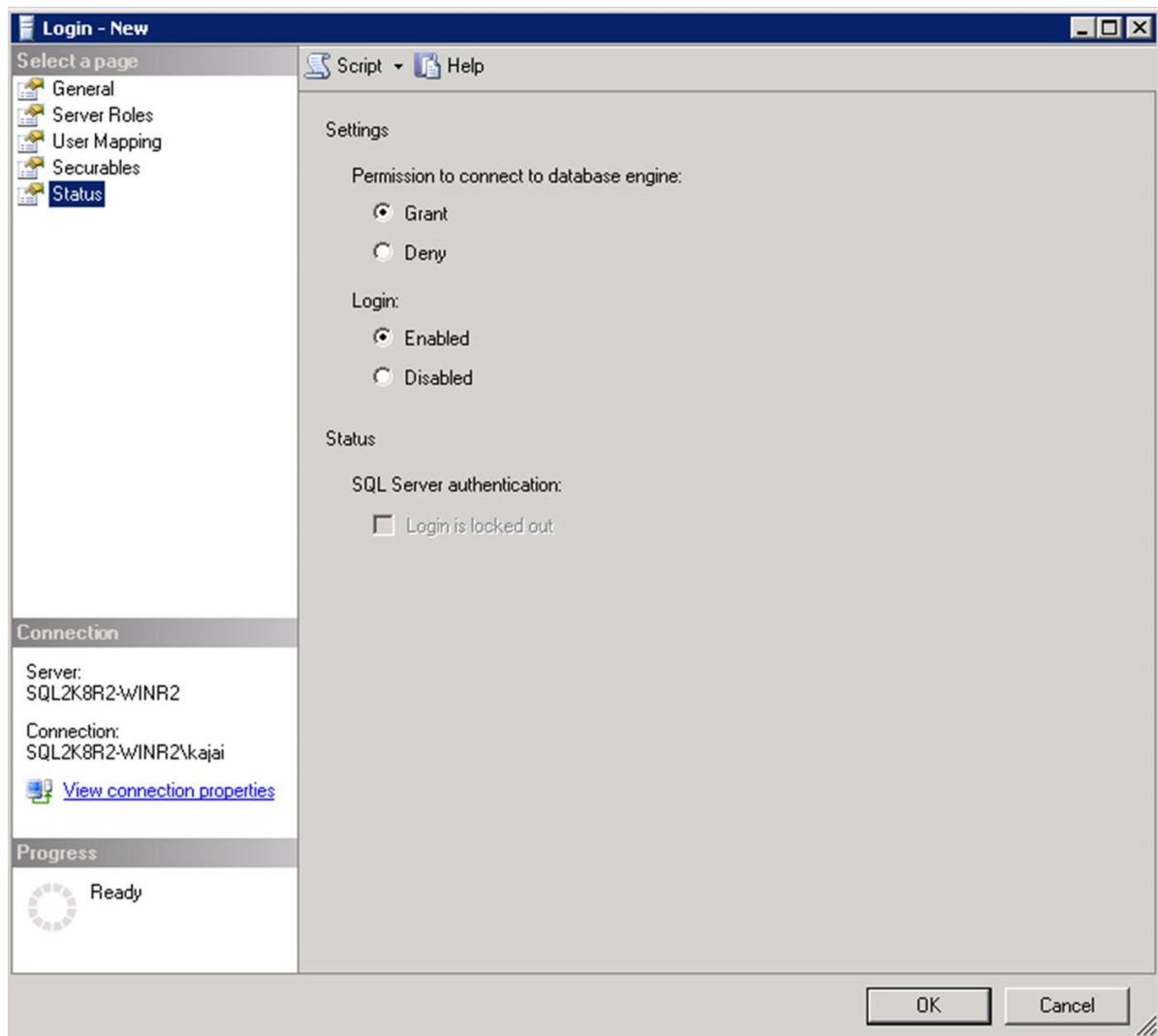
4. Go to the General tab and enter **NT AUTHORITY\SYSTEM** as the Login Name.



5. Go to *Server Roles* and choose *public* and *sysadmin* roles.



6. Go to *Status*. Grant the Permission to connect to database engine and Login as *Enabled*.



7. Click OK.
8. Repeat the same sequence of steps (1-7 above) to add NT Service\AzureWLBackupPluginSvc login to the SQL Server instance. If the login already exists, make sure it has the sysadmin server role and under Status it has Grant the Permission to connect to database engine and Login as Enabled.
9. After granting permission, **Rediscover DBs** in the portal: Vault -> Backup Infrastructure -> Workload in Azure VM:

Home > ShopKartDemoVault > Backup Infrastructure > Protected Servers (Workload in Azure VM)

**Protected Servers (Workload in Azure VM)**

ShopKartDemoVault

Refresh Filter

Fetching data from service completed.

| VM NAME         | VM RG        | SERVER | ...                                                                 |
|-----------------|--------------|--------|---------------------------------------------------------------------|
| ad-secondary-dc | ShopKartDemo | -      | ...                                                                 |
| ShopKartEmp     | ShopKartDemo | s      | <a href="#">Pin to dashboard</a> <a href="#">Rediscover DBs</a> ... |
| ShopKartHR      | ShopKartDemo | s      | ...                                                                 |
| sqlserver-0     | ShopKartDemo | s      | Unregister ...                                                      |

Alternatively, you can automate giving the permissions by running the following PowerShell commands in admin mode. The instance name is set to MSSQLSERVER by default. Change the instance name argument in script if need be:

```

param(
 [Parameter(Mandatory=$false)]
 [string] $InstanceName = "MSSQLSERVER"
)
if ($InstanceName -eq "MSSQLSERVER")
{
 $fullInstance = $env:COMPUTERNAME # In case it is the default SQL Server Instance
}
else
{
 $fullInstance = $env:COMPUTERNAME + "\\" + $InstanceName # In case of named instance
}
try
{
 sqlcmd.exe -S $fullInstance -Q "sp_addsrvrolemember 'NT Service\AzureWLBackupPluginSvc', 'sysadmin'" #
 Adds login with sysadmin permission if already not available
}
catch
{
 Write-Host "An error occurred:"
 Write-Host $_.Exception|format-list -force
}
try
{
 sqlcmd.exe -S $fullInstance -Q "sp_addsrvrolemember 'NT AUTHORITY\SYSTEM', 'sysadmin'" # Adds login with
 sysadmin permission if already not available
}
catch
{
 Write-Host "An error occurred:"
 Write-Host $_.Exception|format-list -force
}

```

## Next steps

- [Learn about](#) backing up SQL Server databases.
- [Learn about](#) restoring backed up SQL Server databases.
- [Learn about](#) managing backed up SQL Server databases.

# Back up SQL Server databases in Azure VMs

2/10/2020 • 14 minutes to read • [Edit Online](#)

SQL Server databases are critical workloads that require a low recovery-point objective (RPO) and long-term retention. You can back up SQL Server databases running on Azure virtual machines (VMs) by using [Azure Backup](#).

This article shows how to back up a SQL Server database that's running on an Azure VM to an Azure Backup Recovery Services vault.

In this article, you'll learn how to:

- Create and configure a vault.
- Discover databases and set up backups.
- Set up auto-protection for databases.

## NOTE

**Soft delete for SQL server in Azure VM and soft delete for SAP HANA in Azure VM workloads** is now available in preview.

To sign up for the preview, write to us at [AskAzureBackupTeam@microsoft.com](mailto:AskAzureBackupTeam@microsoft.com)

## Prerequisites

Before you back up a SQL Server database, check the following criteria:

1. Identify or create a [Recovery Services vault](#) in the same region and subscription as the VM hosting the SQL Server instance.
2. Verify that the VM has [network connectivity](#).
3. Make sure that the SQL Server databases follow the [database naming guidelines for Azure Backup](#).
4. Check that you don't have any other backup solutions enabled for the database. Disable all other SQL Server backups before you back up the database.

## NOTE

You can enable Azure Backup for an Azure VM and also for a SQL Server database running on the VM without conflict.

## Establish network connectivity

For all operations, a SQL Server VM requires connectivity to Azure public IP addresses. VM operations (database discovery, configure backups, schedule backups, restore recovery points, and so on) fail without connectivity to Azure public IP addresses.

Establish connectivity by using one of the following options:

### Allow the Azure datacenter IP ranges

This option allows the [IP ranges](#) in the downloaded file. To access a network security group (NSG), use the `Set-AzureNetworkSecurityRule` cmdlet. If your safe recipients list only includes region-specific IPs, you'll also need to update the safe recipients list the Azure Active Directory (Azure AD) service tag to enable authentication.

### Allow access using NSG tags

If you use NSG to restrict connectivity, then you should use AzureBackup service tag to allow outbound access to

Azure Backup. In addition, you should also allow connectivity for authentication and data transfer by using [rules](#) for Azure AD and Azure Storage. This can be done from the Azure portal or via PowerShell.

To create a rule using the portal:

1. In **All Services**, go to **Network security groups** and select the network security group.
2. Select **Outbound security rules** under **Settings**.
3. Select **Add**. Enter all the required details for creating a new rule as described in [security rule settings](#). Ensure the option **Destination** is set to **Service Tag** and **Destination service tag** is set to **AzureBackup**.
4. Click **Add**, to save the newly created outbound security rule.

To create a rule using PowerShell:

1. Add Azure account credentials and update the national clouds

```
Add-AzureRmAccount
```

2. Select the NSG subscription

```
Select-AzureRmSubscription "<Subscription Id>"
```

3. Select the NSG

```
$nsg = Get-AzureRmNetworkSecurityGroup -Name "<NSG name>" -ResourceGroupName "<NSG resource group name>"
```

4. Add allow outbound rule for Azure Backup service tag

```
Add-AzureRmNetworkSecurityRuleConfig -NetworkSecurityGroup $nsg -Name "AzureBackupAllowOutbound" -Access Allow -Protocol * -Direction Outbound -Priority <priority> -SourceAddressPrefix * -SourcePortRange * -DestinationAddressPrefix "AzureBackup" -DestinationPortRange 443 -Description "Allow outbound traffic to Azure Backup service"
```

5. Add allow outbound rule for Storage service tag

```
Add-AzureRmNetworkSecurityRuleConfig -NetworkSecurityGroup $nsg -Name "StorageAllowOutbound" -Access Allow -Protocol * -Direction Outbound -Priority <priority> -SourceAddressPrefix * -SourcePortRange * -DestinationAddressPrefix "Storage" -DestinationPortRange 443 -Description "Allow outbound traffic to Azure Backup service"
```

6. Add allow outbound rule for AzureActiveDirectory service tag

```
Add-AzureRmNetworkSecurityRuleConfig -NetworkSecurityGroup $nsg -Name "AzureActiveDirectoryAllowOutbound" -Access Allow -Protocol * -Direction Outbound -Priority <priority> -SourceAddressPrefix * -SourcePortRange * -DestinationAddressPrefix "AzureActiveDirectory" -DestinationPortRange 443 -Description "Allow outbound traffic to AzureActiveDirectory service"
```

7. Save the NSG

```
Set-AzureRmNetworkSecurityGroup -NetworkSecurityGroup $nsg
```

**Allow access by using Azure Firewall tags.** If you're using Azure Firewall, create an application rule by using the AzureBackup [FQDN tag](#). This allows outbound access to Azure Backup.

**Deploy an HTTP proxy server to route traffic.** When you back up a SQL Server database on an Azure VM, the backup extension on the VM uses the HTTPS APIs to send management commands to Azure Backup and data to Azure Storage. The backup extension also uses Azure AD for authentication. Route the backup extension traffic for these three services through the HTTP proxy. There are no wildcard domains in use with Azure Backup to add to the allow list for your proxy rules. You will need to use the public IP ranges for these services provided by Azure. The extensions are the only component that's configured for access to the public internet.

Connectivity options include the following advantages and disadvantages:

| OPTION | ADVANTAGES | DISADVANTAGES |
|--------|------------|---------------|
|--------|------------|---------------|

| OPTION                       | ADVANTAGES                                                                            | DISADVANTAGES                                                                                                                                    |
|------------------------------|---------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Allow IP ranges              | No additional costs                                                                   | Complex to manage because the IP address ranges change over time<br><br>Provides access to the whole of Azure, not just Azure Storage            |
| Use NSG service tags         | Easier to manage as range changes are automatically merged<br><br>No additional costs | Can be used with NSGs only<br><br>Provides access to the entire service                                                                          |
| Use Azure Firewall FQDN tags | Easier to manage as the required FQDNs are automatically managed                      | Can be used with Azure Firewall only                                                                                                             |
| Use an HTTP proxy            | Single point of internet access to VMs                                                | Additional costs to run a VM with the proxy software<br><br>No published FQDN addresses, allow rules will be subject to Azure IP address changes |

## Database naming guidelines for Azure Backup

Avoid using the following elements in database names:

- Trailing and leading spaces
- Trailing exclamation marks (!)
- Closing square brackets ()
- Semicolon ;
- Forward slash /

Aliasing is available for unsupported characters, but we recommend avoiding them. For more information, see [Understanding the Table Service Data Model](#).

### NOTE

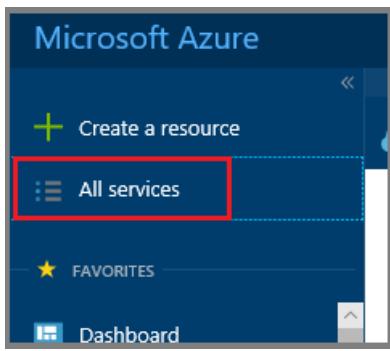
The **Configure Protection** operation for databases with special characters like "+" or "&" in their name is not supported. You can either change the database name or enable **Auto Protection**, which can successfully protect these databases.

## Create a Recovery Services vault

A Recovery Services vault is an entity that stores backups and recovery points created over time. The Recovery Services vault also contains the backup policies that are associated with the protected virtual machines.

To create a Recovery Services vault, follow these steps.

1. Sign in to your subscription in the [Azure portal](#).
2. On the left menu, select **All services**.



3. In the **All services** dialog box, enter *Recovery Services*. The list of resources filters according to your input. In the list of resources, select **Recovery Services vaults**.

A screenshot of the 'All services' search results. A search bar at the top contains the text 'recovery ser'. Below it, a list item for 'Recovery Services vaults' is shown, with a small star icon to its right. The list item has a blue background and white text.

The list of Recovery Services vaults in the subscription appears.

4. On the **Recovery Services vaults** dashboard, select **Add**.

A screenshot of the 'Recovery Services vaults' dashboard. At the top, there is a breadcrumb trail 'Home &gt; Recovery Services vaults'. Below it is a title 'Recovery Services vaults' and a Microsoft logo. At the bottom of the dashboard, there is a row of buttons: '+ Add' (which is highlighted with a red box), 'Edit columns', 'Refresh', and 'Assign Tags'.

The **Recovery Services vault** dialog box opens. Provide values for the **Name**, **Subscription**, **Resource group**, and **Location**.

A screenshot of the 'Recovery Services vault' creation dialog box. It has several input fields with validation stars: 'Name' (with placeholder 'Enter the name'), 'Subscription' (with placeholder '<subscription>'), 'Resource group' (with radio buttons for 'Create new' and 'Use existing', where 'Use existing' is selected), and 'Location' (with placeholder 'West US'). At the bottom, there is a checkbox for 'Pin to dashboard' and two buttons: 'Create' (highlighted with a blue box) and 'Automation options'.

- **Name:** Enter a friendly name to identify the vault. The name must be unique to the Azure subscription. Specify a name that has at least 2 but not more than 50 characters. The name must start with a letter and consist only of letters, numbers, and hyphens.
- **Subscription:** Choose the subscription to use. If you're a member of only one subscription, you'll see that name. If you're not sure which subscription to use, use the default (suggested) subscription.

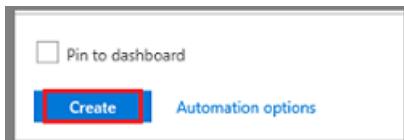
There are multiple choices only if your work or school account is associated with more than one Azure subscription.

- **Resource group:** Use an existing resource group or create a new one. To see the list of available resource groups in your subscription, select **Use existing**, and then select a resource from the drop-down list. To create a new resource group, select **Create new** and enter the name. For more information about resource groups, see [Azure Resource Manager overview](#).
- **Location:** Select the geographic region for the vault. To create a vault to protect virtual machines, the vault *must* be in the same region as the virtual machines.

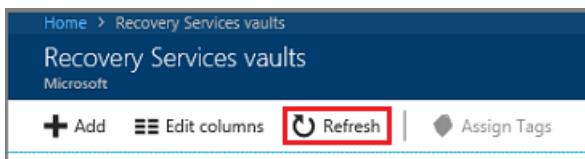
#### IMPORTANT

If you're not sure of the location of your VM, close the dialog box. Go to the list of virtual machines in the portal. If you have virtual machines in several regions, create a Recovery Services vault in each region. Create the vault in the first location, before you create the vault for another location. There's no need to specify storage accounts to store the backup data. The Recovery Services vault and Azure Backup handle that automatically.

5. When you're ready to create the Recovery Services vault, select **Create**.



It can take a while to create the Recovery Services vault. Monitor the status notifications in the **Notifications** area at the upper-right corner of the portal. After your vault is created, it's visible in the list of Recovery Services vaults. If you don't see your vault, select **Refresh**.



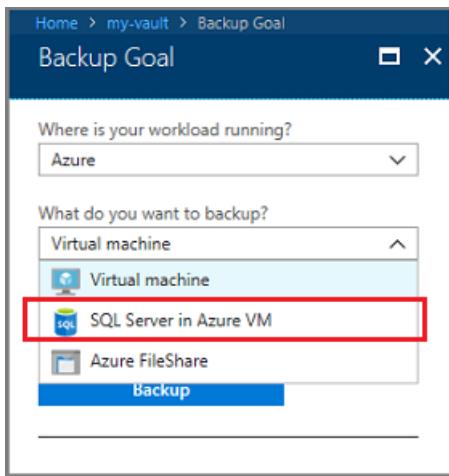
## Discover SQL Server databases

How to discover databases running on a VM:

1. In the [Azure portal](#), open the Recovery Services vault you use to back up the database.
2. In the **Recovery Services vault** dashboard, select **Backup**.



3. In **Backup Goal**, set **Where is your workload running?** to **Azure**.
4. In **What do you want to backup**, select **SQL Server in Azure VM**.



5. In **Backup Goal > Discover DBs in VMs**, select **Start Discovery** to search for unprotected VMs in the subscription. This search can take a while, depending on the number of unprotected VMs in the subscription.

- Unprotected VMs should appear in the list after discovery, listed by name and resource group.
- If a VM isn't listed as you expect, see whether it's already backed up in a vault.
- Multiple VMs can have the same name, but they'll belong to different resource groups.

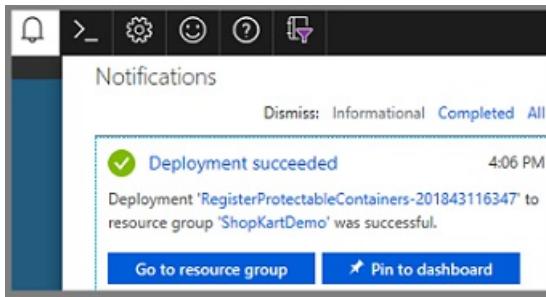
| VIRTUAL MACHINE NAME | RESOURCE GROUP |
|----------------------|----------------|
| MynewVM              | 00prjai3       |
| shivamrhel1          | abdemo-webapp  |
| cvttest              | abserver       |
| singaporehr          | AdiGanRG       |
| FileServerSS         | anurag-sql     |
| MGTSwinVM            | MGTSGRG_West   |
| MGLinuxVM            | MGTSGRGWestUS  |

**Selected Virtual Machines**

Azure Backup will need SQL sysadmin privilege for doing backups. It will create NT Service\AzureWLBackupPluginSvc account on the selected VMs which needs to be added to SQL login and given SQL sysadmin privilege. In case of a SQL Marketplace VM, Azure Backup will invoke SQL IaaS extension to automatically get required permissions. [Learn More](#)

**Discover DBs**

6. In the VM list, select the VM running the SQL Server database > **Discover DBs**.
7. Track database discovery in **Notifications**. The time required for this action depends on the number of VM databases. When the selected databases are discovered, a success message appears.



8. Azure Backup discovers all SQL Server databases on the VM. During discovery, the following elements occur in the background:

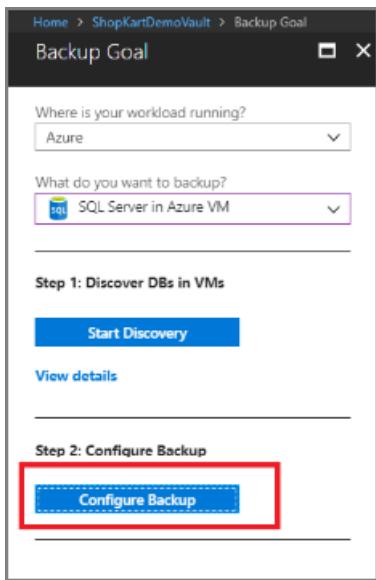
- Azure Backup registers the VM with the vault for workload backup. All databases on the registered VM can be backed up to this vault only.
- Azure Backup installs the AzureBackupWindowsWorkload extension on the VM. No agent is installed on a SQL database.
- Azure Backup creates the service account NT Service\AzureWLBackupPluginSvc on the VM.
  - All backup and restore operations use the service account.
  - NT Service\AzureWLBackupPluginSvc requires SQL sysadmin permissions. All SQL Server VMs created in the Marketplace come with the SqlIaaSExtension installed. The AzureBackupWindowsWorkload extension uses the SQLIaaSExtension to automatically get the required permissions.
- If you didn't create the VM from the Marketplace or if you are on SQL 2008 and 2008 R2, the VM may not have the SqlIaaSExtension installed, and the discovery operation fails with the error message UserErrorSQLNoSysAdminMembership. To fix this issue, follow the instructions under [Set VM permissions](#).

The screenshot shows the Azure portal's Protected Servers blade for the "ShopKartDemoVault" vault. On the left, a table lists protected servers. One row for "ShopKartHR" is highlighted with a red border and shows an "Error" status under the "DETAILS" column. On the right, a modal window titled "Error details" for "ShopKartHR" is open, also with a red border around its content area. It displays the following information:

|                    |                                                                                                                                                     |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Error Code         | UserErrorSQLNoSysadminMembership                                                                                                                    |
| Error Message      | Azure Backup service creates a service account "NTService\AzureWLBackupPluginSvc" for all operations and this account needs SQL sysadmin privilege. |
| Recommended Action | Please provide Sys Admin privileges to AzureWLBackupPluginSvc.                                                                                      |

## Configure backup

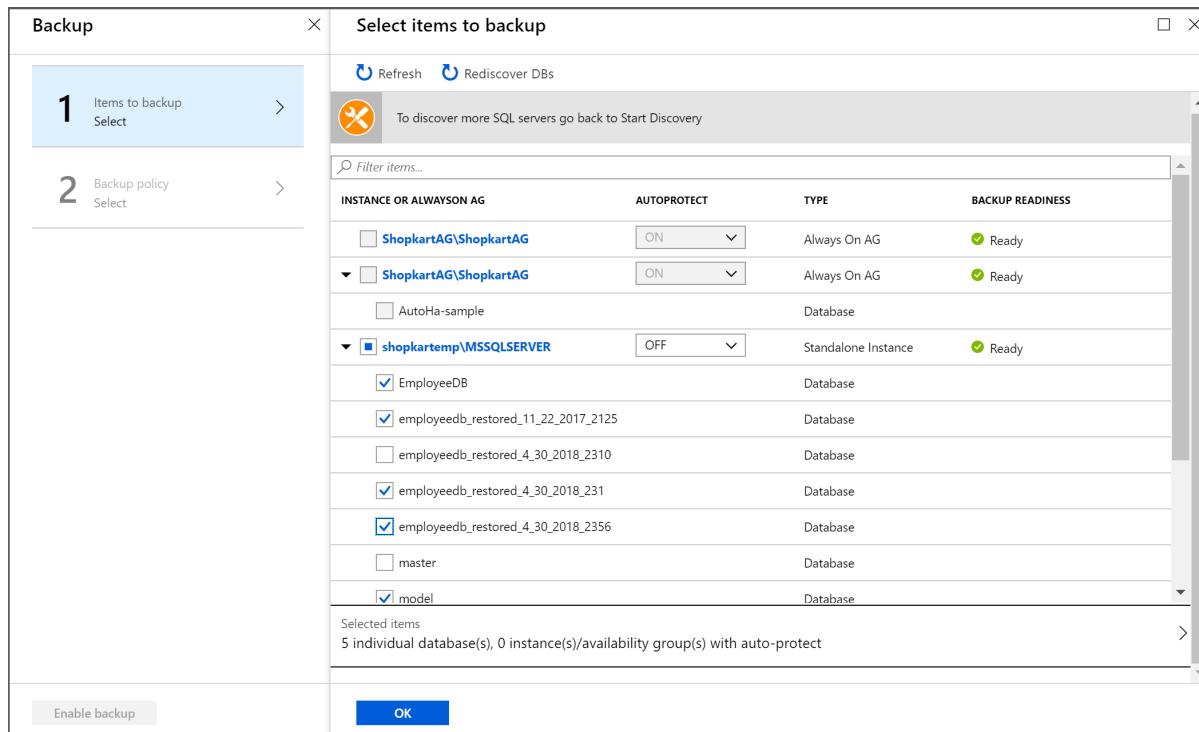
1. In **Backup Goal > Step 2: Configure Backup**, select **Configure Backup**.



2. In **Select items to backup**, you see all the registered availability groups and standalone SQL Server instances. Select the arrow to the left of a row to expand the list of all the unprotected databases in that instance or Always On availability group.

| INSTANCE OR ALWAYSON AG             | AUTOPROTECT | TYPE                | BACKUP READINESS |
|-------------------------------------|-------------|---------------------|------------------|
| ShopkartAG\ShopkartAG               | ON          | Always On AG        | Ready            |
| ShopkartAG\ShopkartAG               | ON          | Always On AG        | Ready            |
| AutoHa-sample                       |             | Database            |                  |
| shopkarttemp\MSSQLSERVER            | OFF         | Standalone Instance | Ready            |
| EmployeeDB                          |             | Database            |                  |
| employeedb_restored_11_22_2017_2125 |             | Database            |                  |
| employeedb_restored_4_30_2018_2310  |             | Database            |                  |
| employeedb_restored_4_30_2018_2311  |             | Database            |                  |
| employeedb_restored_4_30_2018_2356  |             | Database            |                  |
| master                              |             | Database            |                  |
| model                               |             | Database            |                  |

3. Choose all the databases you want to protect, and then select **OK**.



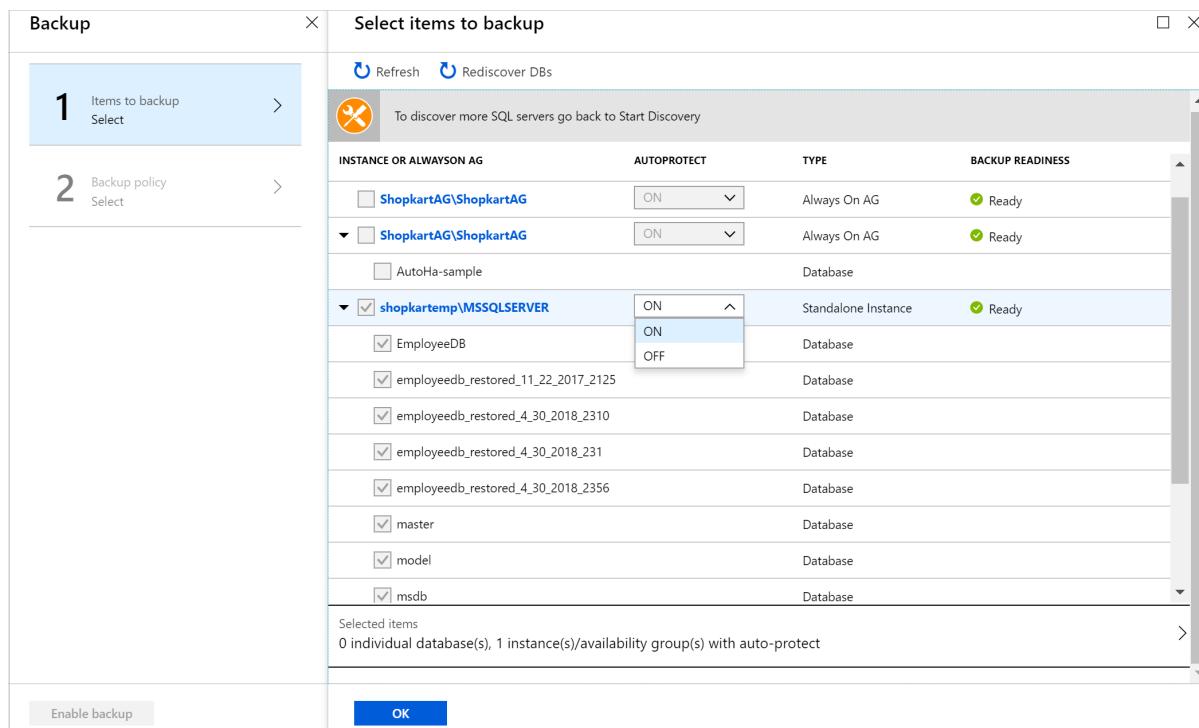
To optimize backup loads, Azure Backup sets a maximum number of databases in one backup job to 50.

- To protect more than 50 databases, configure multiple backups.
- To enable the entire instance or the Always On availability group, in the **AUTOPROTECT** drop-down list, select **ON**, and then select **OK**.

#### NOTE

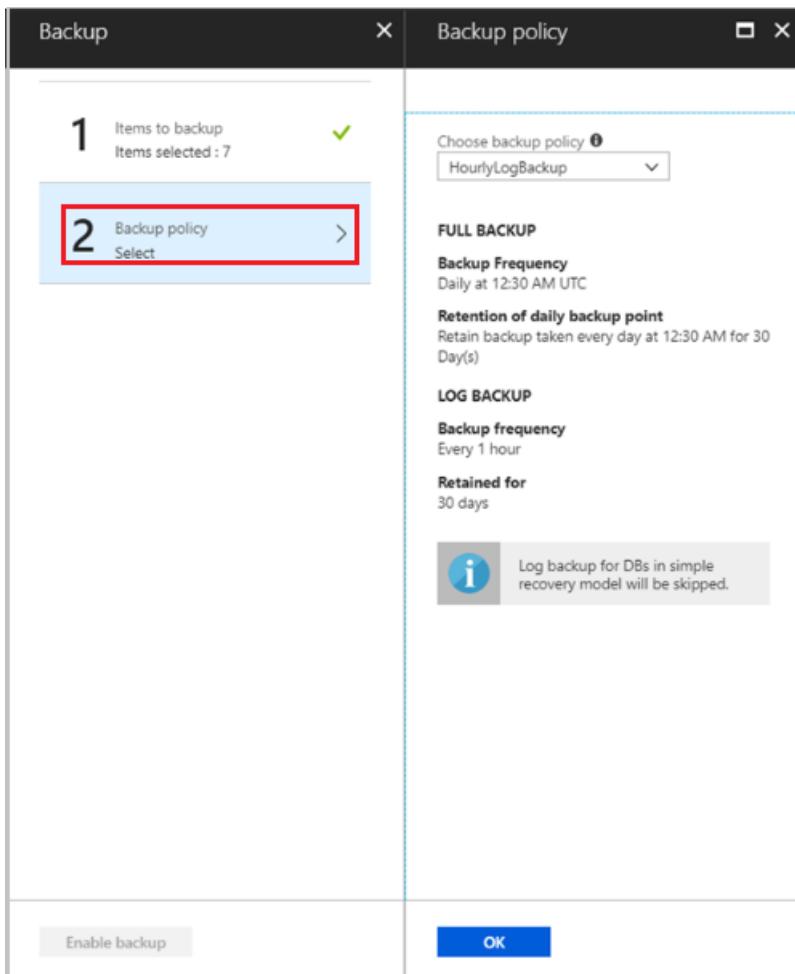
The [auto-protection](#) feature not only enables protection on all the existing databases at once, but also automatically protects any new databases added to that instance or the availability group.

#### 4. Select **OK** to open **Backup policy**.

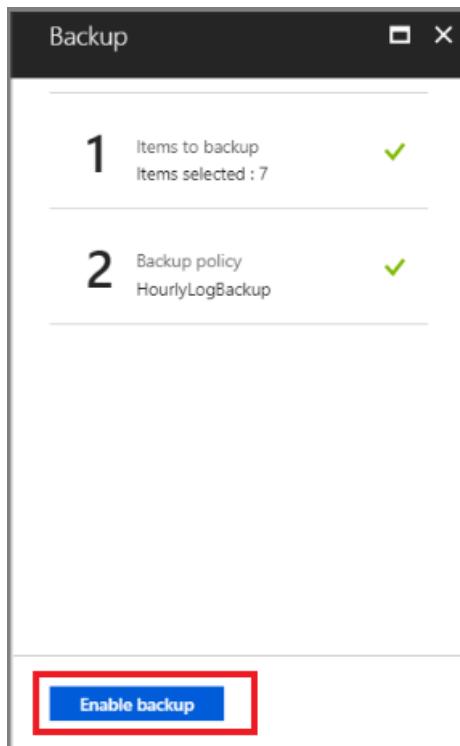


#### 5. In **Backup policy**, choose a policy and then select **OK**.

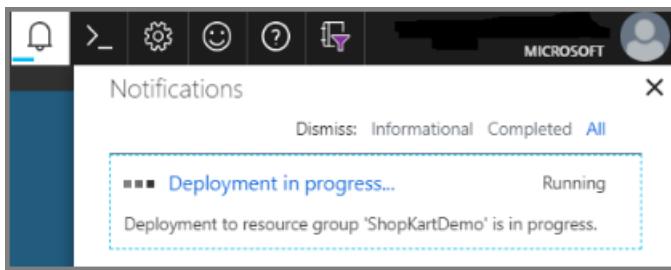
- Select the default policy as HourlyLogBackup.
- Choose an existing backup policy previously created for SQL.
- Define a new policy based on your RPO and retention range.



6. In **Backup**, select **Enable backup**.



7. Track the configuration progress in the **Notifications** area of the portal.



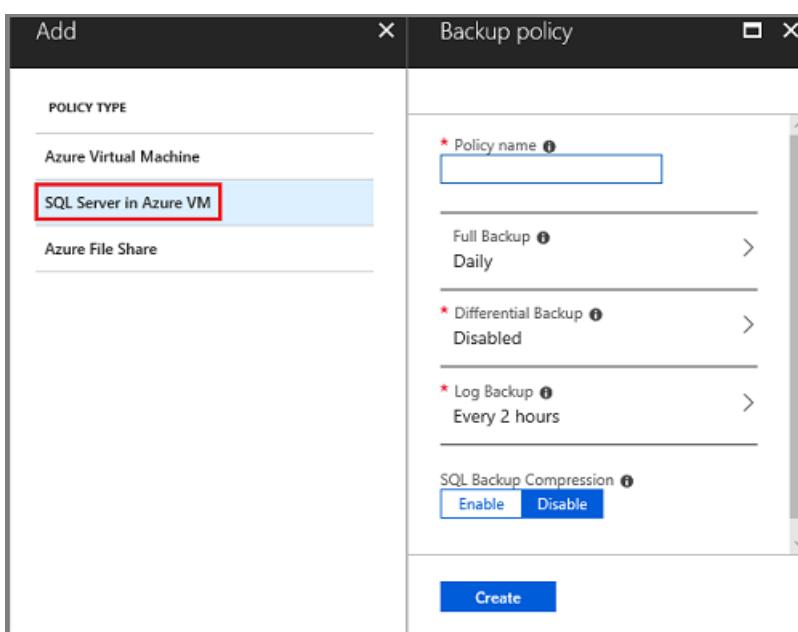
## Create a backup policy

A backup policy defines when backups are taken and how long they're retained.

- A policy is created at the vault level.
- Multiple vaults can use the same backup policy, but you must apply the backup policy to each vault.
- When you create a backup policy, a daily full backup is the default.
- You can add a differential backup, but only if you configure full backups to occur weekly.
- Learn about [different types of backup policies](#).

To create a backup policy:

1. In the vault, select **Backup policies > Add**.
2. In **Add**, select **SQL Server in Azure VM** to define the policy type.



3. In **Policy name**, enter a name for the new policy.
4. In **Full Backup policy**, select a **Backup Frequency**. Choose either **Daily** or **Weekly**.
  - For **Daily**, select the hour and time zone when the backup job begins.
  - For **Weekly**, select the day of the week, hour, and time zone when the backup job begins.
  - Run a full backup, because you can't turn off the **Full Backup** option.
  - Select **Full Backup** to view the policy.
  - You can't create differential backups for daily full backups.

**Backup Frequency**

|       |          |                                  |
|-------|----------|----------------------------------|
| Daily | 12:00 AM | (UTC) Coordinated Universal Time |
|-------|----------|----------------------------------|

**RETENTION RANGE**

Retention of daily backup point.

\* At 12:00 AM Retained for 180 Day(s)

Retention of weekly backup point.

\* On Sunday At 12:00 AM Retained for 104 Week(s)

Retention of monthly backup point.

**Week Based** **Day Based**

\* On First Day At 12:00 AM Retained for 60 Month(s)

Retention of yearly backup point.

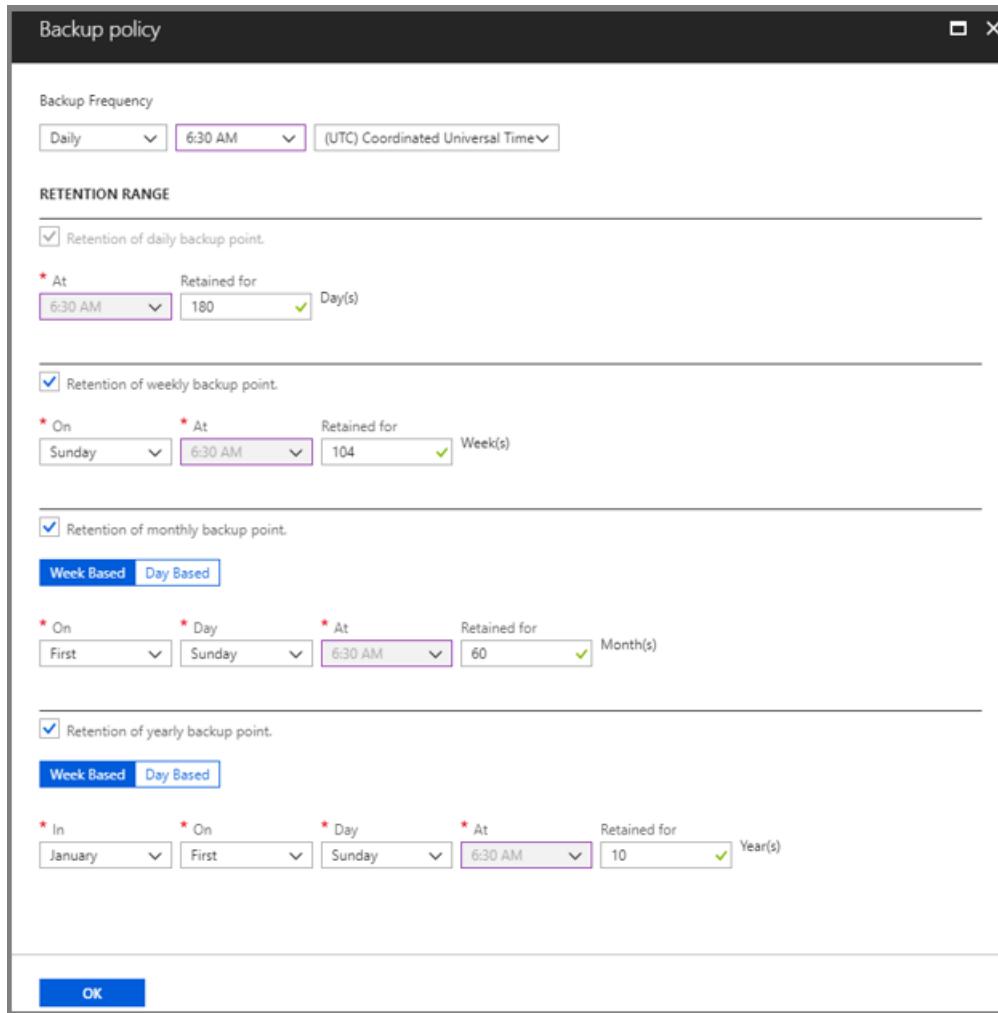
**Week Based** **Day Based**

\* In January On First Day At 12:00 AM Retained for 10 Year(s)

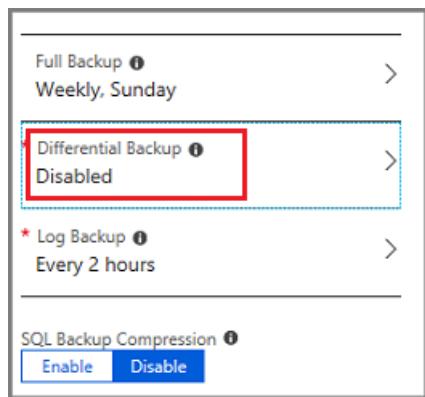
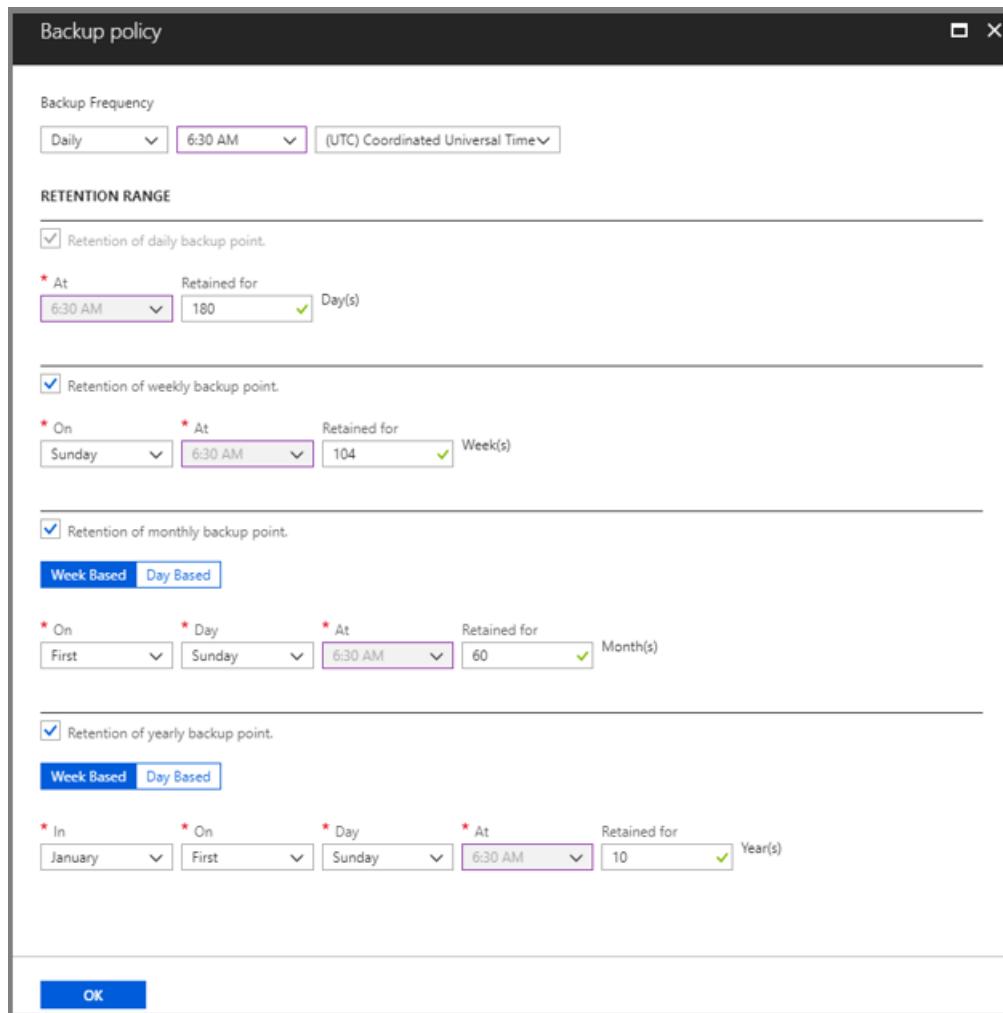
**OK**

5. In **RETENTION RANGE**, all options are selected by default. Clear any retention range limits that you don't want, and then set the intervals to use.

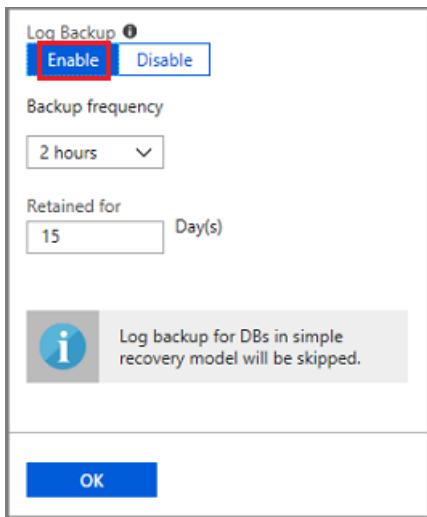
- Minimum retention period for any type of backup (full, differential, and log) is seven days.
- Recovery points are tagged for retention based on their retention range. For example, if you select a daily full backup, only one full backup is triggered each day.
- The backup for a specific day is tagged and retained based on the weekly retention range and the weekly retention setting.
- Monthly and yearly retention ranges behave in a similar way.



6. In the **Full Backup policy** menu, select **OK** to accept the settings.
7. To add a differential backup policy, select **Differential Backup**.



8. In **Differential Backup policy**, select **Enable** to open the frequency and retention controls.
  - You can trigger only one differential backup per day.
  - Differential backups can be retained for a maximum of 180 days. For longer retention, use full backups.
9. Select **OK** to save the policy and return to the main **Backup policy** menu.
10. To add a transactional log backup policy, select **Log Backup**.
11. In **Log Backup**, select **Enable**, and then set the frequency and retention controls. Log backups can occur as often as every 15 minutes and can be retained for up to 35 days.
12. Select **OK** to save the policy and return to the main **Backup policy** menu.



13. On the **Backup policy** menu, choose whether to enable **SQL Backup Compression** or not. This option is disabled by default. If enabled, SQL Server will send a compressed backup stream to the VDI. Please note that Azure Backup overrides instance level defaults with COMPRESSION / NO\_COMPRESSION clause depending on the value of this control.
14. After you complete the edits to the backup policy, select **OK**.

#### NOTE

Each log backup is chained to the previous full backup to form a recovery chain. This full backup will be retained until the retention of the last log backup has expired. This might mean that the full backup is retained for an extra period to make sure all the logs can be recovered. Let's assume user has a weekly full backup, daily differential and 2 hour logs. All of them are retained for 30 days. But, the weekly full can be really cleaned up/deleted only after the next full backup is available i.e., after  $30 + 7$  days. Say, a weekly full backup happens on Nov 16th. As per the retention policy, it should be retained until Dec 16th. The last log backup for this full happens before the next scheduled full, on Nov 22nd. Until this log is available until Dec 22nd, the Nov 16th full can't be deleted. So, the Nov 16th full is retained until Dec 22nd.

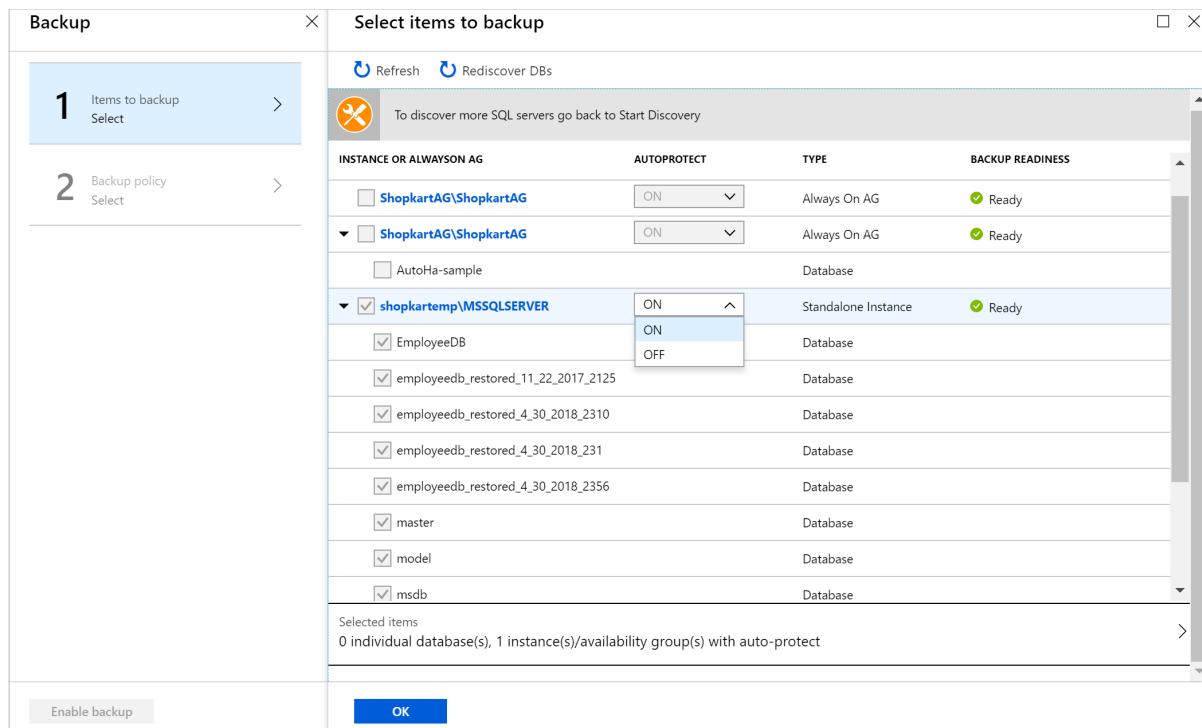
## Enable auto-protection

You can enable auto-protection to automatically back up all existing and future databases to a standalone SQL Server instance or to an Always On availability group.

- There's no limit on the number of databases you can select for auto-protection at one time.
- You can't selectively protect or exclude databases from protection in an instance at the time you enable auto-protection.
- If your instance already includes some protected databases, they'll remain protected under their respective policies even after you turn on auto-protection. All unprotected databases added later will have only a single policy that you define at the time of enabling auto-protection, listed under **Configure Backup**. However, you can change the policy associated with an auto-protected database later.

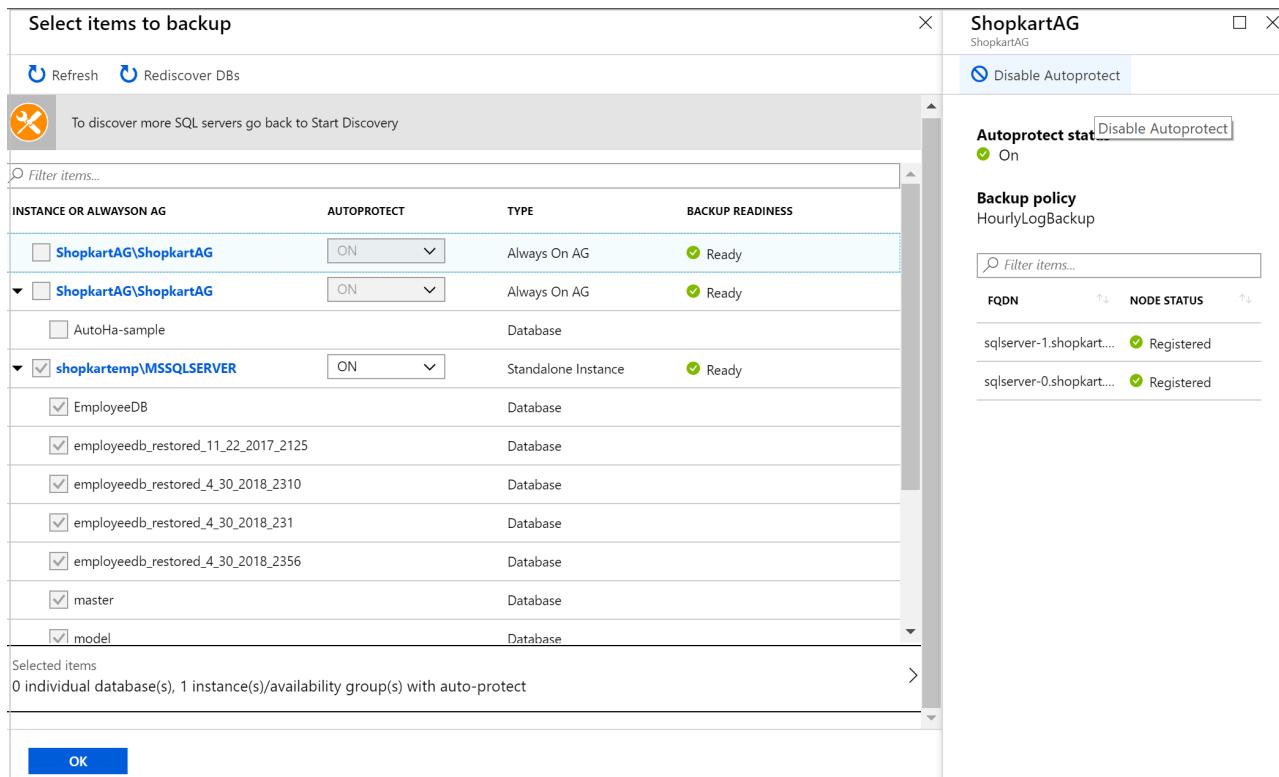
To enable auto-protection:

1. In **Items to backup**, select the instance for which you want to enable auto-protection.
2. Select the drop-down list under **AUTOPROTECT**, choose **ON**, and then select **OK**.



### 3. Backup is configured for all the databases together and can be tracked in **Backup Jobs**.

If you need to disable auto-protection, select the instance name under **Configure Backup**, and then select **Disable Autoprotect** for the instance. All databases will continue to be backed up, but future databases won't be automatically protected.



## Next steps

Learn how to:

- [Restore backed-up SQL Server databases](#)
- [Manage backed-up SQL Server databases](#)

# Restore SQL Server databases on Azure VMs

12/17/2019 • 6 minutes to read • [Edit Online](#)

This article describes how to restore a SQL Server database that's running on an Azure virtual machine (VM) that the [Azure Backup](#) service has backed up to an Azure Backup Recovery Services vault.

This article describes how to restore SQL Server databases. For more information, see [Back up SQL Server databases on Azure VMs](#).

## Restore to a time or a recovery point

Azure Backup can restore SQL Server databases that are running on Azure VMs as follows:

- Restore to a specific date or time (to the second) by using transaction log backups. Azure Backup automatically determines the appropriate full differential backup and the chain of log backups that are required to restore based on the selected time.
- Restore a specific full or differential backup to restore to a specific recovery point.

## Prerequisites

Before you restore a database, note the following:

- You can restore the database to an instance of a SQL Server in the same Azure region.
- The destination server must be registered to the same vault as the source.
- To restore a TDE-encrypted database to another SQL Server, you need to first [restore the certificate to the destination server](#).
- Before you restore the "master" database, start the SQL Server instance in single-user mode by using the startup option **-m AzureWorkloadBackup**.
  - The value for **-m** is the name of the client.
  - Only the specified client name can open the connection.
- For all system databases (model, master, msdb), stop the SQL Server Agent service before you trigger the restore.
- Close any applications that might try to take a connection to any of these databases.
- If you have multiple instances running on a server, all of the instances should be up and running otherwise the server would not appear in the list of destination servers for you to restore database to.

## Restore a database

To restore, you need the following permissions:

- **Backup Operator** permissions in the vault where you're doing the restore.
- **Contributor (write)** access to the source VM that's backed up.
- **Contributor (write)** access to the target VM:
  - If you're restoring to the same VM, this is the source VM.
  - If you're restoring to an alternate location, this is the new target VM.

Restore as follows:

1. Open the vault in which the SQL Server VM is registered.

2. On the vault dashboard, under **Usage**, select **Backup Items**.
3. In **Backup Items**, under **Backup Management Type**, select **SQL in Azure VM**.

| BACKUP MANAGEMENT TYPE      | BACKUP ITEM COUNT |
|-----------------------------|-------------------|
| SQL in Azure VM             | 5                 |
| Azure Virtual Machine       | 0                 |
| Azure Backup Agent          | 0                 |
| Azure Backup Server         | 0                 |
| DPM                         | 0                 |
| Azure Storage (Azure Files) | 0                 |

4. Select the database to restore.

| DATABASE       | INSTANCE OR ALWAYSON AG              | TYPE                | BACKUP STATUS                                | ... |
|----------------|--------------------------------------|---------------------|----------------------------------------------|-----|
| productcatalog | shopkart.com\ShopkartAG              | Always on AG        | <span>Healthy</span>                         | ... |
| master         | sqlserver-0.shopkart.com\MSSQLSERVER | Standalone Instance | <span>Healthy</span>                         | ... |
| employeeedb    | sqlserver-1.shopkart.com\MSSQLSERVER | Standalone Instance | <span>Healthy</span>                         | ... |
| msdb           | sqlserver-1.shopkart.com\MSSQLSERVER | Standalone Instance | <span>Warning(Initial backup pending)</span> | ... |
| model          | sqlserver-1.shopkart.com\MSSQLSERVER | Standalone Instance | <span>Healthy</span>                         | ... |

5. Review the database menu. It provides information about the database backup, including:
  - The oldest and latest restore points.
  - The log backup status for the last 24 hours for databases that are in full and bulk-logged recovery mode and that are configured for transactional log backups.
6. Select **Restore**.

The screenshot shows the Azure portal interface for managing a SQL database named 'testdb5'. At the top, there's a search bar and a user profile. Below it, the breadcrumb navigation shows: Dashboard > kajai-bvtd2-vault-1 - Backup items > Backup Items (SQL in Azure VM) > testdb5. On the left, a sidebar lists various services like Recovery services vault, Subscription name, and Server or Cluster. The main content area shows the 'Essentials' section with details: Backup Status (Healthy), Latest restore point (10/17/2019, 2:59:20 PM), Oldest restore point (7/30/2019, 7:41:31 AM), Backup policy (HourlyLogBackup), and Instance (MSSQLSERVER). Below this is the 'Restore points' section, which includes a 'Logs in last 24 hours' chart. The chart has two tabs: 'LOG (POINT IN TIME)' (selected) and 'NO LOGS AVAILABLE'. The timeline shows data from Wednesday 6:00 PM to Thursday 12:00 PM.

7. In **Restore Configuration**, specify where (or how) to restore the data:

- **Alternate Location:** Restore the database to an alternate location and keep the original source database.
- **Overwrite DB:** Restore the data to the same SQL Server instance as the original source. This option overwrites the original database.

**IMPORTANT**

If the selected database belongs to an Always On availability group, SQL Server doesn't allow the database to be overwritten. Only **Alternate Location** is available.

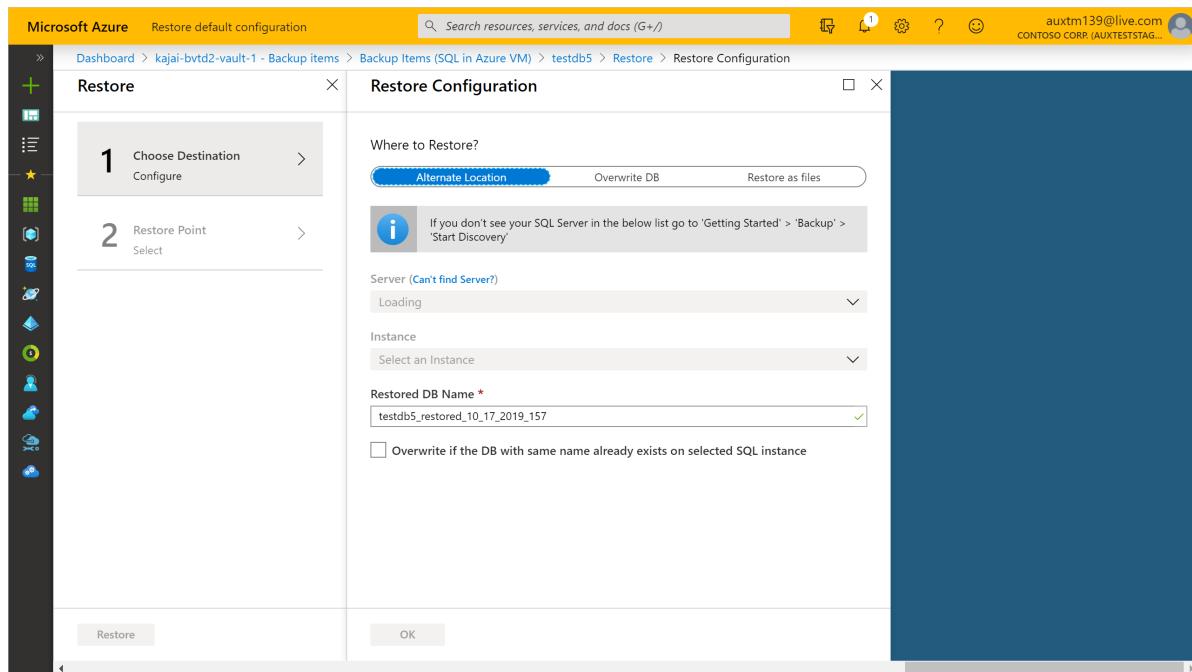
- **Restore as files:** Instead of restoring as a database, restore the backup files that can be recovered as a database later on any machine where the files are present using SQL Server Management Studio.

The screenshot shows the 'Restore Configuration' dialog box. It has two tabs: 'Choose Destination' (selected) and 'Restore Point'. Under 'Choose Destination', there are two steps: 'Configure' and 'Select'. Step 1 is currently active. The 'Where to Restore?' section shows 'Alternate Location' selected. Below it, there's an info message: 'If you don't see your SQL Server in the below list go to 'Getting Started' > 'Backup' > 'Start Discovery''. There are dropdown menus for 'Server' (loading) and 'Instance' (Select an instance). A checkbox 'Restored DB Name \*' is checked with the value 'testdb5\_restored\_10\_17\_2019\_157'. Another checkbox 'Overwrite if the DB with same name already exists on selected SQL instance' is unchecked. At the bottom are 'Restore' and 'OK' buttons.

**Restore to an alternate location**

1. In the **Restore Configuration** menu, under **Where to Restore**, select **Alternate Location**.
2. Select the SQL Server name and instance to which you want to restore the database.

3. In the **Restored DB Name** box, enter the name of the target database.
4. If applicable, select **Overwrite if the DB with the same name already exists on selected SQL instance**.
5. Select **OK**.



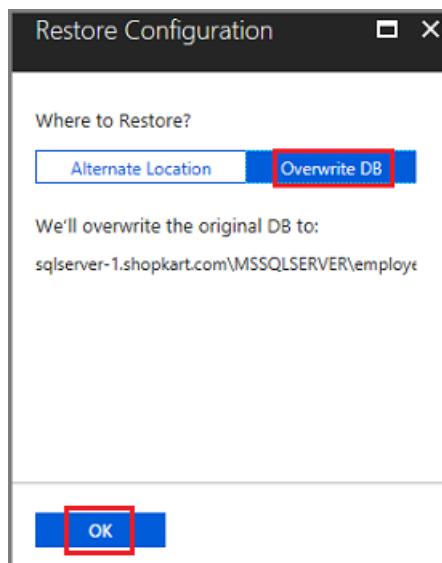
6. In **Select restore point**, select whether to [restore to a specific point in time](#) or to [restore to a specific recovery point](#).

**NOTE**

The point-in-time restore is available only for log backups for databases that are in full and bulk-logged recovery mode.

## Restore and overwrite

1. In the **Restore Configuration** menu, under **Where to Restore**, select **Overwrite DB > OK**.



2. In **Select restore point**, select **Logs (Point in Time)** to [restore to a specific point in time](#). Or select **Full & Differential** to restore to a [specific recovery point](#).

## NOTE

The point-in-time restore is available only for log backups for databases that are in full and bulk-logged recovery mode.

## Restore as files

To restore the backup data as .bak files instead of a database, choose **Restore as Files**. Once the files are dumped to a specified path, you can take these files to any machine where you want to restore them as a database. By the virtue of being able to move these files around to any machine, you can now restore the data across subscriptions and regions.

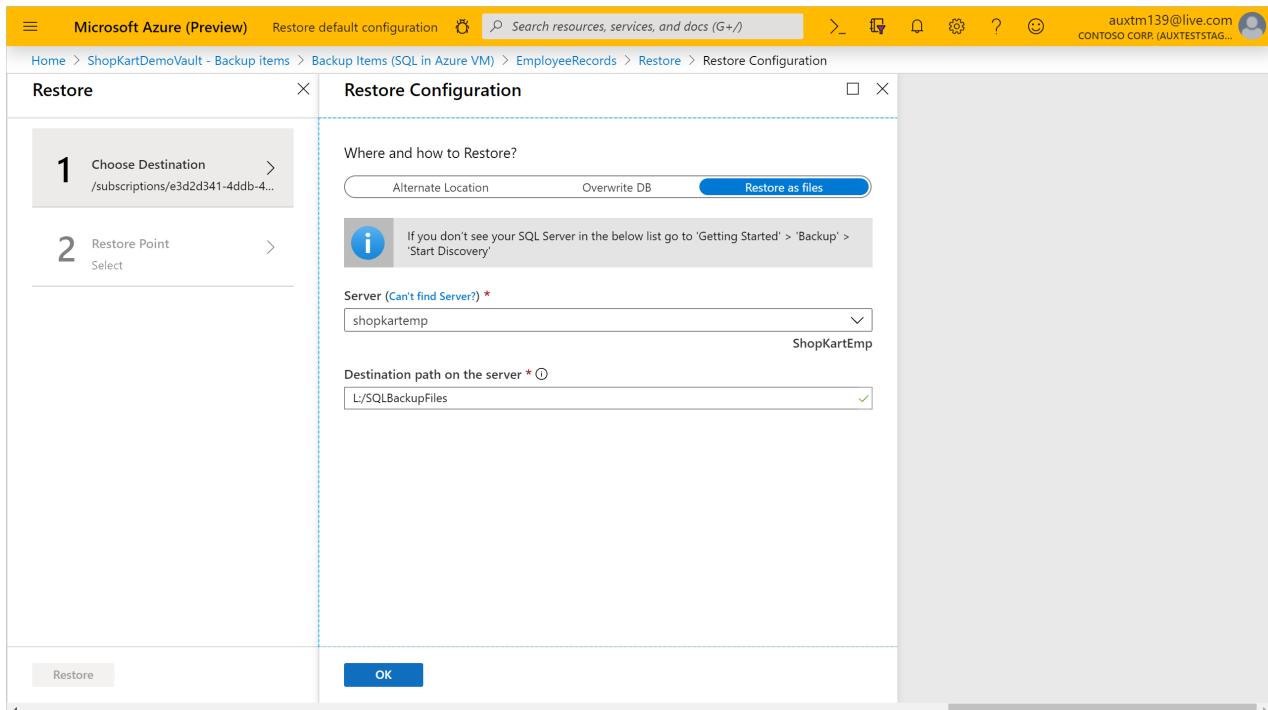
1. In the **Restore Configuration** menu, under **Where to Restore**, select **Restore as files**.
2. Select the SQL Server name to which you want to restore the backup files.
3. In the **Destination path on the server** input the folder path on the server selected in step 2. This is the location where the service will dump all the necessary backup files. Typically, a network share path, or path of a mounted Azure file share when specified as the destination path, enables easier access to these files by other machines in the same network or with the same Azure file share mounted on them.

To restore the database backup files on an Azure File Share mounted on the target registered VM, make sure that NT AUTHORITY\SYSTEM has access to the file share. You can perform the steps given below to grant the read/write permissions to the AFS mounted on the VM:

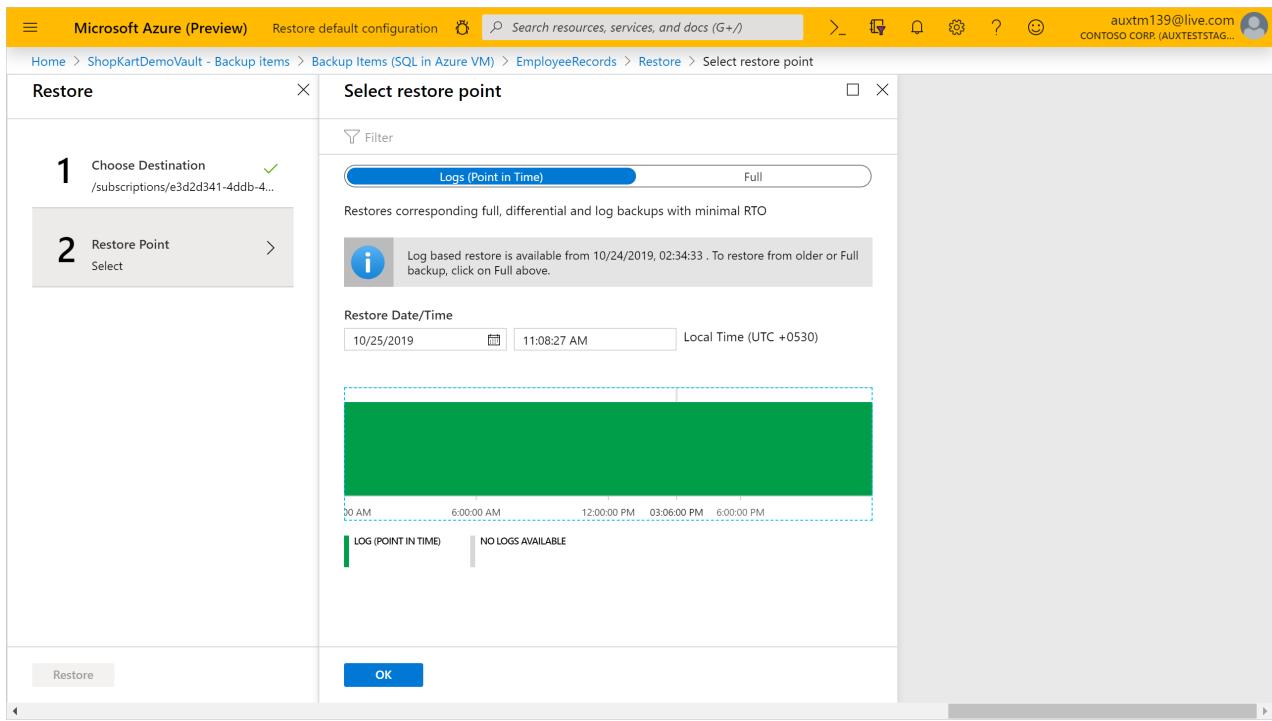
- Run `PsExec -s cmd` to enter into NT AUTHORITY\SYSTEM shell
  - Execute  
`cmdkey /add:<storageacct>.file.core.windows.net /user:AZURE\<storageacct> /pass:<storagekey>`
  - Verify access with `dir \\<storageacct>.file.core.windows.net\<filesharename>`
- Kick off a restore as files from the Backup Vault to `\\\<storageacct>.file.core.windows.net\<filesharename>` as the path

You can download PsExec via <https://docs.microsoft.com/sysinternals/downloads/psexec>

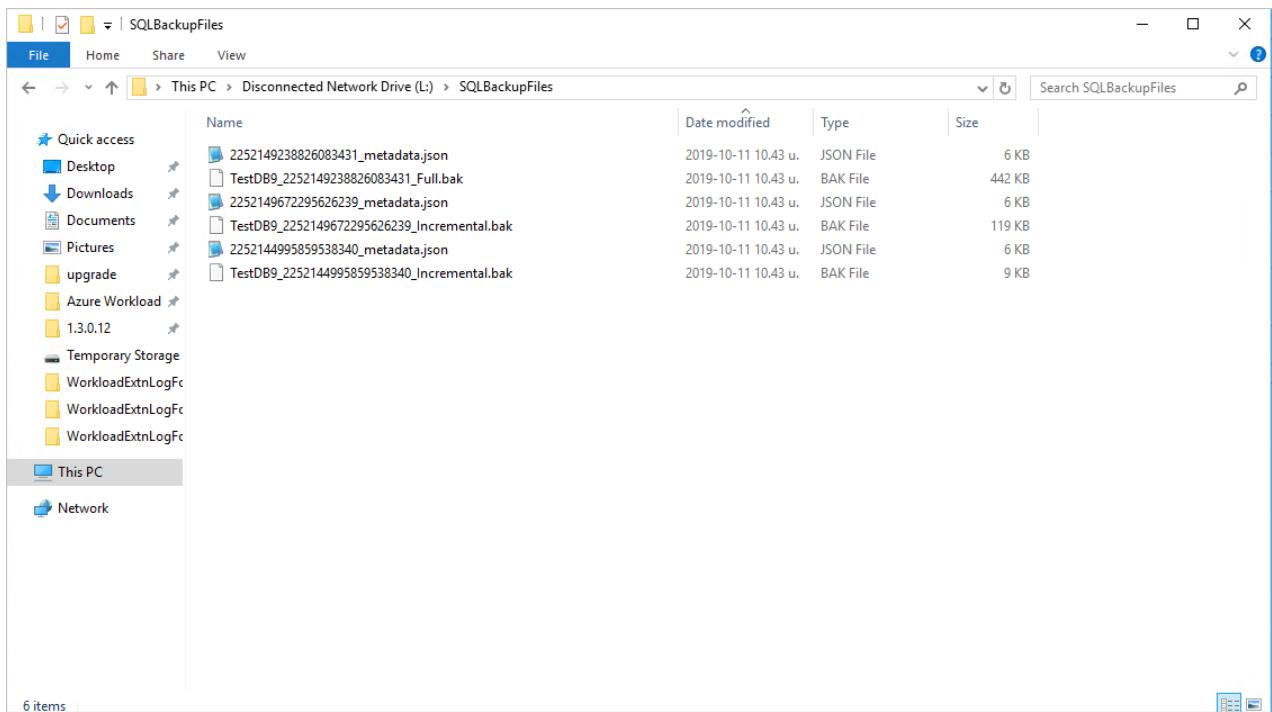
4. Select **OK**.



5. Select the **Restore Point** corresponding to which all the available .bak files will be restored.



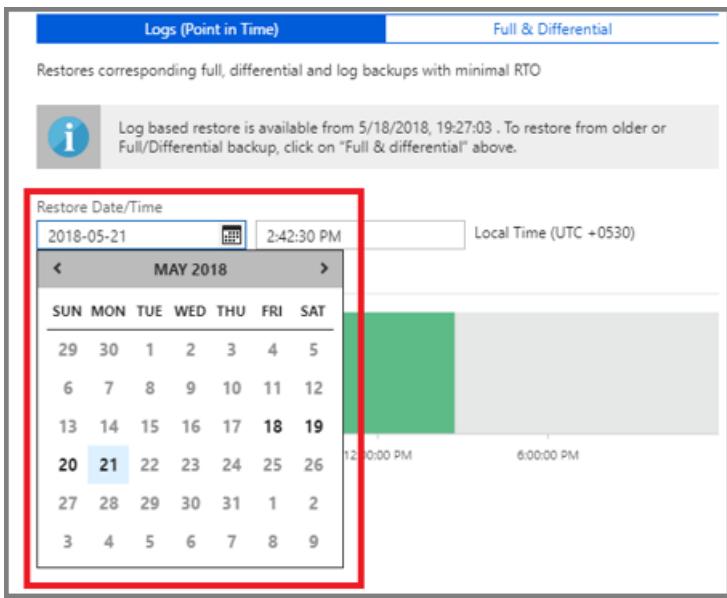
6. All the backup files associated with the selected recovery point are dumped into the destination path. You can restore the files as a database on any machine they are present on using SQL Server Management Studio.



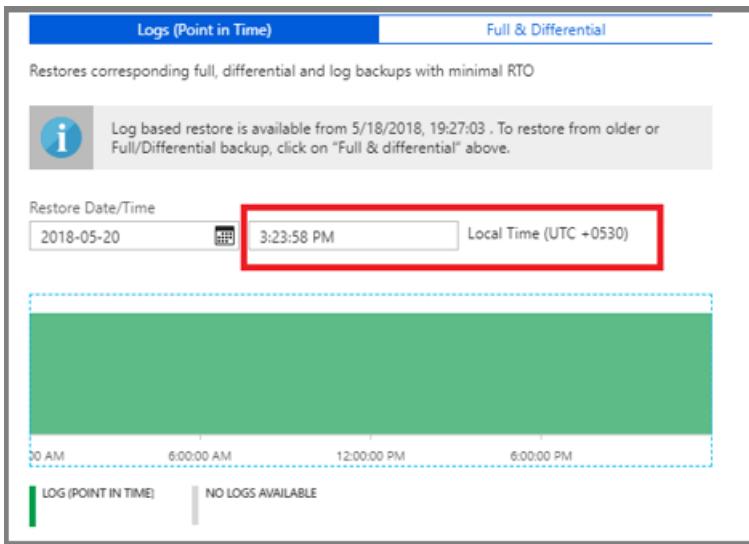
### Restore to a specific point in time

If you've selected **Logs (Point in Time)** as the restore type, do the following:

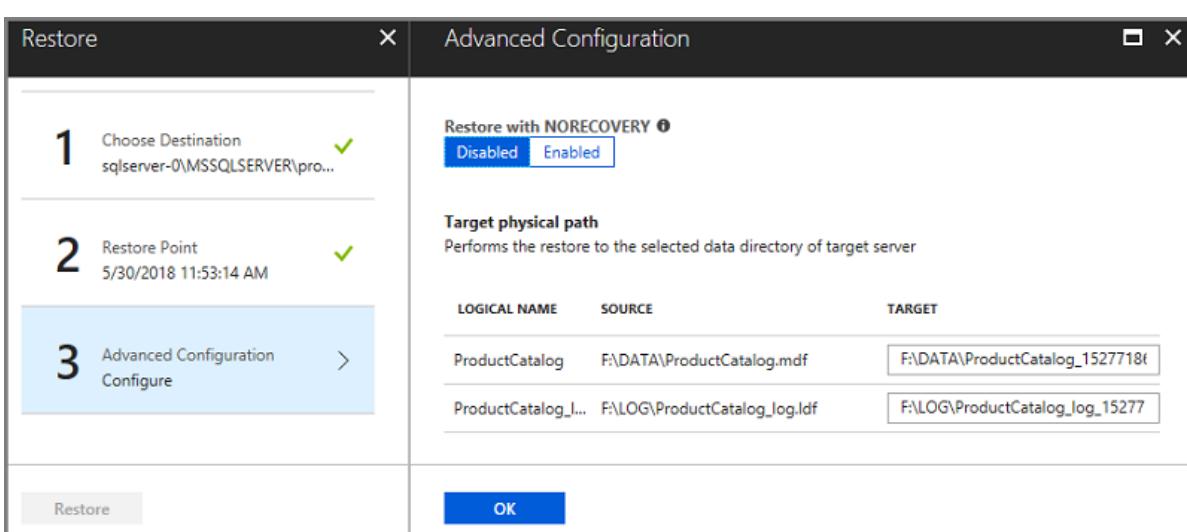
1. Under **Restore Date/Time**, open the calendar. On the calendar, the dates that have recovery points are displayed in bold type, and the current date is highlighted.
2. Select a date that has recovery points. You can't select dates that have no recovery points.



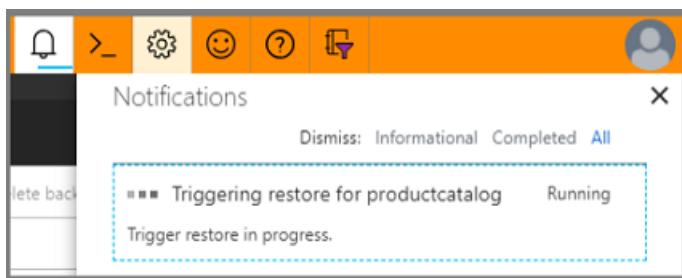
3. After you select a date, the timeline graph displays the available recovery points in a continuous range.
4. Specify a time for the recovery on the timeline graph, or select a time. Then select **OK**.



5. On the **Advanced Configuration** menu, if you want to keep the database nonoperational after the restore, enable **Restore with NORECOVERY**.
6. If you want to change the restore location on the destination server, enter a new target path.
7. Select **OK**.



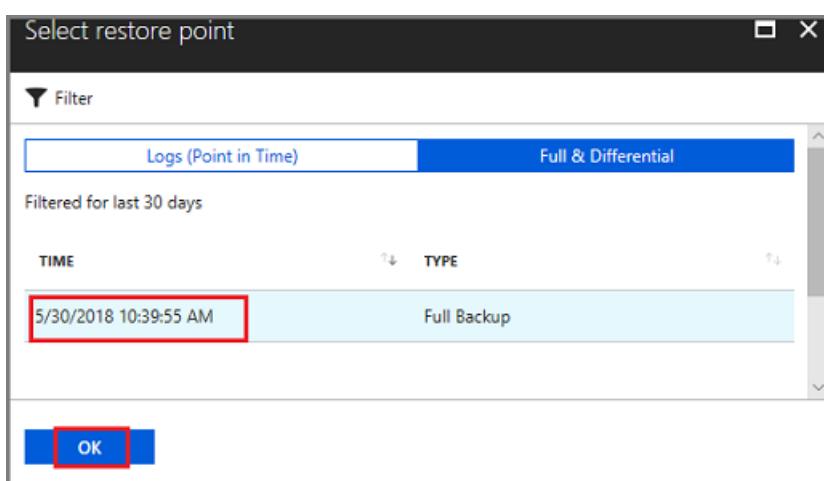
8. On the **Restore** menu, select **Restore** to start the restore job.
9. Track the restore progress in the **Notifications** area, or track it by selecting **Restore jobs** on the database menu.



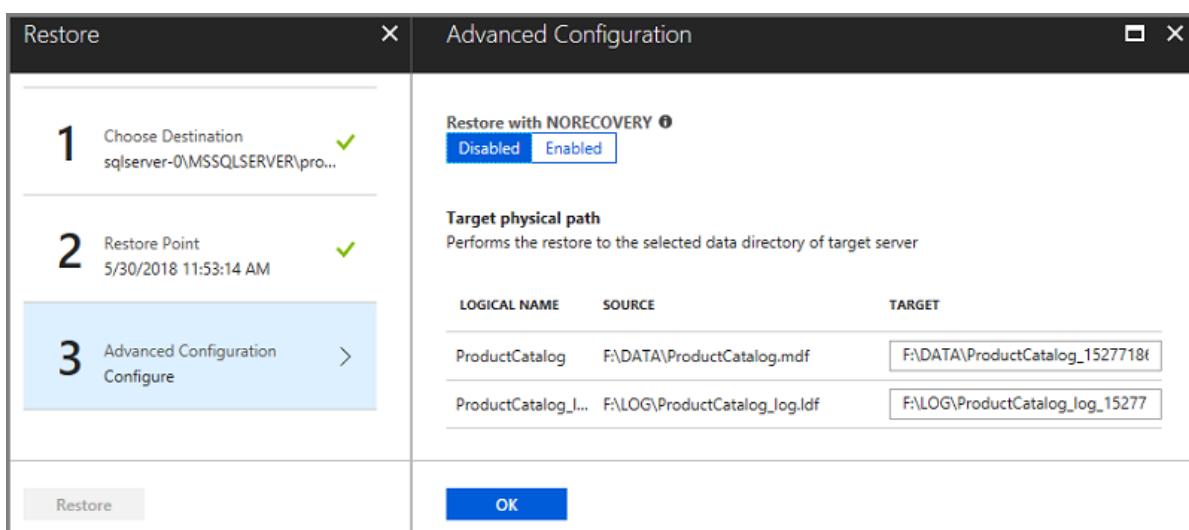
### Restore to a specific restore point

If you've selected **Full & Differential** as the restore type, do the following:

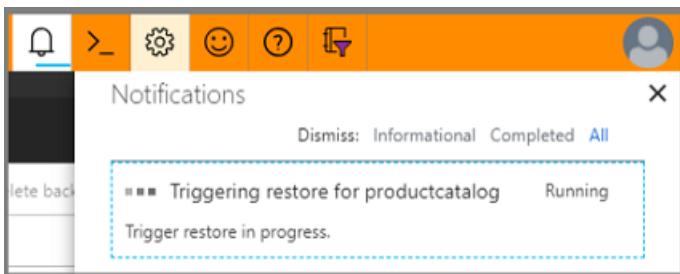
1. Select a recovery point from the list, and select **OK** to complete the restore point procedure.



2. On the **Advanced Configuration** menu, if you want to keep the database nonoperational after the restore, enable **Restore with NORECOVERY**.
3. If you want to change the restore location on the destination server, enter a new target path.
4. Select **OK**.



5. On the **Restore** menu, select **Restore** to start the restore job.
6. Track the restore progress in the **Notifications** area, or track it by selecting **Restore jobs** on the database menu.



## Restore databases with large number of files

If the total string size of files in a database is greater than a [particular limit](#), Azure Backup stores the list of database files in a different pit component such that you will not be able to set the target restore path during the restore operation. The files will be restored to the SQL default path instead.

A screenshot of the Azure portal's 'Restore' wizard. The left pane shows three steps: 1. Choose Destination (status: ✓), 2. Restore Point (status: ✓), and 3. Advanced Configuration (status: &gt;). Step 3 is highlighted with a blue background. The right pane is titled 'Advanced Configuration' and contains the following sections: 'Restore with NORECOVERY' (Enabled), 'Target physical path' (description: 'Performs the restore to the selected data directory of target server'), and a warning message: 'This database has too many files. You cannot restore this database the usual way. All the files will instead be restored to the default data and log paths of the destination SQL Server.' with an exclamation mark icon.

## Next steps

[Manage and monitor](#) SQL Server databases that are backed up by Azure Backup.

# Manage and monitor backed up SQL Server databases

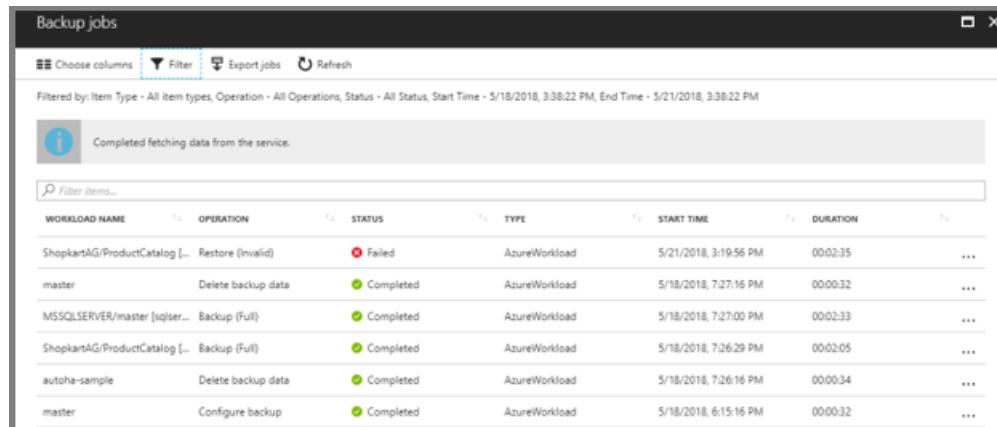
11/18/2019 • 4 minutes to read • [Edit Online](#)

This article describes common tasks for managing and monitoring SQL Server databases that are running on an Azure virtual machine (VM) and that are backed up to an Azure Backup Recovery Services vault by the [Azure Backup](#) service. You'll learn how to monitor jobs and alerts, stop and resume database protection, run backup jobs, and unregister a VM from backups.

If you haven't yet configured backups for your SQL Server databases, see [Back up SQL Server databases on Azure VMs](#)

## Monitor manual backup jobs in the portal

Azure Backup shows all manually triggered jobs in the **Backup jobs** portal. The jobs you see in this portal include database discovery and registering, and backup and restore operations.



The screenshot shows the 'Backup jobs' portal interface. At the top, there are buttons for 'Choose columns', 'Filter', 'Export jobs', and 'Refresh'. A message indicates 'Completed fetching data from the service.' Below this is a table with the following data:

| WORKLOAD NAME                   | OPERATION          | STATUS    | TYPE          | START TIME            | DURATION | ... |
|---------------------------------|--------------------|-----------|---------------|-----------------------|----------|-----|
| ShopkartAG/ProductCatalog [...] | Restore (Invalid)  | Failed    | AzureWorkload | 5/21/2018, 3:19:56 PM | 00:02:35 | ... |
| master                          | Delete backup data | Completed | AzureWorkload | 5/18/2018, 7:27:16 PM | 00:00:32 | ... |
| MSSQLSERVER/master [sqlservr]   | Backup (Full)      | Completed | AzureWorkload | 5/18/2018, 7:27:00 PM | 00:02:33 | ... |
| ShopkartAG/ProductCatalog [...] | Backup (Full)      | Completed | AzureWorkload | 5/18/2018, 7:26:29 PM | 00:02:05 | ... |
| autoha-sample                   | Delete backup data | Completed | AzureWorkload | 5/18/2018, 7:26:16 PM | 00:00:34 | ... |
| master                          | Configure backup   | Completed | AzureWorkload | 5/18/2018, 6:15:16 PM | 00:00:32 | ... |

### NOTE

The **Backup jobs** portal doesn't show scheduled backup jobs. Use SQL Server Management Studio to monitor scheduled backup jobs, as described in the next section.

For details on Monitoring scenarios, go to [Monitoring in the Azure portal](#) and [Monitoring using Azure Monitor](#).

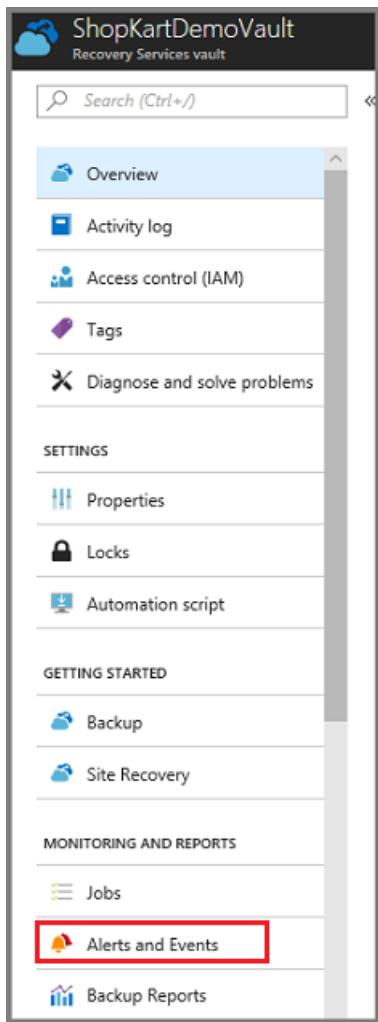
## View backup alerts

Because log backups occur every 15 minutes, monitoring backup jobs can be tedious. Azure Backup eases monitoring by sending email alerts. Email alerts are:

- Triggered for all backup failures.
- Consolidated at the database level by error code.
- Sent only for a database's first backup failure.

To monitor database backup alerts:

1. Sign in to the [Azure portal](#).
2. On the vault dashboard, select **Alerts and Events**.



3. In **Alerts and Events**, select **Backup Alerts**.

| ALERT                | BACKUP ITEM              | PROTECTED SERVER        | SEVERITY | DURATION | CREATION TIME         | STATUS |
|----------------------|--------------------------|-------------------------|----------|----------|-----------------------|--------|
| Backup failure (Log) | ShopkartAG/ProductCat... | ShopkartAG.shopkart.com | Critical | 08:08:02 | 5/30/2018 10:09:30 AM | Active |
| Backup failure (Log) | ShopkartAG/AutoHa-sa...  | ShopkartAG.shopkart.com | Critical | 08:23:02 | 5/30/2018 9:54:30 AM  | Active |

## Stop protection for a SQL Server database

You can stop backing up a SQL Server database in a couple of ways:

- Stop all future backup jobs, and delete all recovery points.
- Stop all future backup jobs, and leave the recovery points intact.

If you choose to leave recovery points, keep these details in mind:

- All recovery points will remain intact forever, all pruning shall stop at stop protection with retain data.
- You will be charged for the protected instance and the consumed storage. For more information, see [Azure Backup pricing](#).
- If you delete a data source without stopping backups, new backups will fail.

To stop protection for a database:

1. On the vault dashboard, select **Backup Items**.

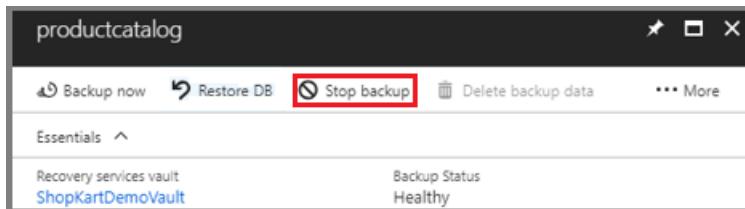
2. Under **Backup Management Type**, select **SQL in Azure VM**.

| BACKUP MANAGEMENT TYPE      | BACKUP ITEM COUNT |
|-----------------------------|-------------------|
| SQL in Azure VM             | 5                 |
| Azure Virtual Machine       | 0                 |
| Azure Backup Agent          | 0                 |
| Azure Backup Server         | 0                 |
| DPM                         | 0                 |
| Azure Storage (Azure Files) | 0                 |

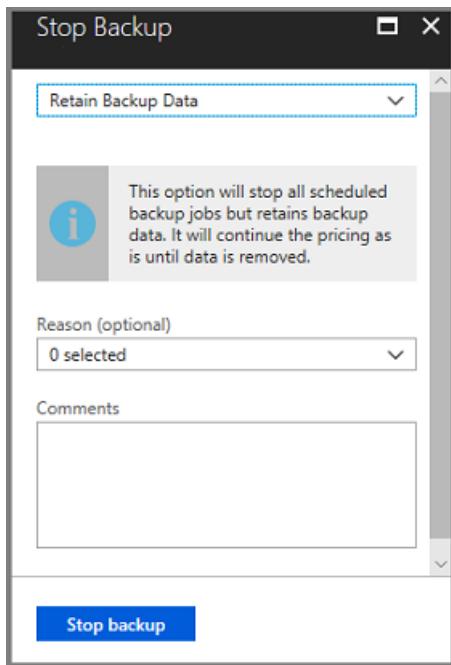
3. Select the database for which you want to stop protection.

| Backup Items (SQL in Azure VM) |                                      |                     |                                 |     |
|--------------------------------|--------------------------------------|---------------------|---------------------------------|-----|
| ShopCartDemoVault              |                                      |                     |                                 |     |
| DATABASE                       | INSTANCE OR ALWAYSON AG              | TYPE                | BACKUP STATUS                   |     |
| productcatalog                 | shopkart.com\ShopkartAG              | Always on AG        | Healthy                         | ... |
| master                         | sqlserver-0.shopkart.com\MSSQLSERVER | Standalone Instance | Healthy                         | ... |
| employeedb                     | sqlserver-1.shopkart.com\MSSQLSERVER | Standalone Instance | Healthy                         | ... |
| msdb                           | sqlserver-1.shopkart.com\MSSQLSERVER | Standalone Instance | Warning(Initial backup pending) | ... |
| model                          | sqlserver-1.shopkart.com\MSSQLSERVER | Standalone Instance | Healthy                         | ... |

4. On the database menu, select **Stop backup**.



5. On the **Stop Backup** menu, select whether to retain or delete data. If you want, provide a reason and comment.



6. Select **Stop backup**.

**NOTE**

For more information about the delete data option, see the FAQ below:

- [If I delete a database from an autoprotected instance, what will happen to the backups?](#)
- [If I do stop backup operation of an autoprotected database what will be its behavior?](#)

## Resume protection for a SQL database

When you stop protection for the SQL database, if you select the **Retain Backup Data** option, you can later resume protection. If you don't retain the backup data, you can't resume protection.

To resume protection for a SQL database:

1. Open the backup item and select **Resume backup**.



2. On the **Backup policy** menu, select a policy, and then select **Save**.

## Run an on-demand backup

You can run different types of on-demand backups:

- Full backup
- Copy-only full backup
- Differential backup
- Log backup

While you need to specify the retention duration for Copy-only full backup, the retention range for on-demand full backup will automatically be set to 45 days from current time.

For more information, see [SQL Server backup types](#).

# Unregister a SQL Server instance

Unregister a SQL Server instance after you disable protection but before you delete the vault.

1. On the vault dashboard, under **Manage**, select **Backup Infrastructure**.

The screenshot shows the 'ShopKartDemoVault - Backup Infrastructure' dashboard. The left sidebar has sections for Alerts and Events, Backup Reports, Policies (Backup policies), Protected Items (Backup items, Replicated items), Manage (Site Recovery Infrastructure, Backup Infrastructure, Recovery Plans (Site Recovery)), and Support + Troubleshooting (New support request). The 'Backup Infrastructure' link is highlighted with a red box.

2. Under **Management Servers**, select **Protected Servers**.

The screenshot shows the 'ShopKartDemoVault - Backup Infrastructure' dashboard. The left sidebar has sections for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Properties, Locks, and Automation script. The 'Protected Servers' link under Management Servers is highlighted with a red box. The right pane shows a table titled 'PROTECTED SERVERS' with columns for BACKUP MANAGEMENT TYPE and PROTECTED SERVER COUNT. It lists 'Workload in Azure VM' (3 servers), 'Azure Backup Server' (0), 'DPM' (0), and 'Azure Backup Agent' (0).

3. In **Protected Servers**, select the server to unregister. To delete the vault, you must unregister all servers.

4. Right-click the protected server, and select **Unregister**.

The screenshot shows the 'Protected Servers (Workload in Azure VM)' list view. The table has columns for VM NAME, VM RG, and SERVER. A context menu is open over the row for 'ShopKartHR', with options: Pin to dashboard, Rediscover DBs, Unregister (highlighted with a red box), and Re-register.

| VM NAME        | VM RG        | SERVER |
|----------------|--------------|--------|
| ad-secondry-dc | ShopKartDemo | ...    |
| ShopKartHR     | ShopKartDemo | ...    |
| sqlserver-0    | ShopKartDemo | ...    |
| sqlserver-1    | ShopKartDemo | ...    |

# Modify policy

Modify policy to change backup frequency or retention range.

## NOTE

Any change in the retention period will be applied retrospectively to all the older recovery points besides the new ones.

In the vault dashboard, go to **Manage > Backup Policies** and choose the policy you want to edit.

The screenshot shows the 'Backup policies' blade for the 'ShopKartDemoVault'. On the left, there's a navigation menu with 'Protected items' (Backup items, Replicated items), 'Manage' (Backup policies, Backup Infrastructure, Site Recovery infrastructure, Recovery Plans (Site Recovery), Backup Reports), and search/filter options. The 'Backup policies' item is selected. The main area displays a table of existing policies:

| NAME            | POLICY TYPE            | ... (More Options) |
|-----------------|------------------------|--------------------|
| HourlyLogBackup | SQL Server in Azure VM | ...                |
| UpdatedBP-8     | SQL Server in Azure VM | ...                |
| bhawnatestnew   | Azure Virtual Machine  | ...                |
| Bkp15mins       | SQL Server in Azure VM | ...                |
| test1           | Azure Virtual Machine  | ...                |
| TestSQL         | SQL Server in Azure VM | ...                |
| DefaultPolicy   | Azure Virtual Machine  | ...                |

Below this, a breadcrumb navigation shows 'Home > ShopKartDemoVault - Backup policies > Backup policy'. The 'Backup policy' blade itself has a title bar with 'Backup policy' and close/cancel buttons. It contains sections for 'Associated items' (with a 'Delete' button) and 'Full Backup' (set to 'Daily'). There are also sections for 'Differential Backup' (disabled) and 'Log Backup' (every 1 hour). At the bottom, there's a 'SQL Backup Compression' section with 'Enable' and 'Disable' buttons, and a large blue 'Modify' button.

Policy modification will impact all the associated Backup Items and trigger corresponding **configure protection** jobs.

## Inconsistent policy

Sometimes, a modify policy operation can lead to an **inconsistent** policy version for some backup items. This happens when the corresponding **configure protection** job fails for the backup item after a modify policy operation is triggered. It appears as follows in the backup item view:

Home > shracsql - Backup items > Backup Items (SQL in Azure VM) > prodshrac90

prodshrac90

Backup now | Restore DB | Stop backup | Delete backup data | Resume backup

The associated backup policy is inconsistent. Click here to fix the issues.

Essentials

Recovery services vault: shracsql  
Subscription name: <subscription\_name>  
<subscription\_ID>  
Server or Cluster: shrac3  
Item type: SQL Server in Azure VM

Backup Status: Not reachable  
Latest restore point: 5/14/2019, 5:39:31 PM (3 month(s) ago)  
Oldest restore point: 5/14/2019, 6:33:14 AM (4 month(s) ago)  
Backup policy: HourlyLogBackup  
Instance or AlwaysOn AG: MSSQLSERVER

Restore points

Logs in last 24 hours

24 hours | 72 hours

You can fix the policy version for all the impacted items in one click:

Home > shracsql - Backup items > Backup Items (SQL in Azure VM) > prodshrac90

prodshrac90

Backup now | Restore DB | Stop backup | Delete backup data | Resume backup

The associated backup policy is inconsistent. Click here to fix the issues.

Essentials

Recovery services vault: shracsql  
Subscription name: <subscription\_name>  
<subscription\_ID>  
Server or Cluster: shrac3  
Item type: SQL Server in Azure VM

Backup Status: Not reachable  
Latest restore point: 5/14/2019, 5:39:31 PM (3 n  
Oldest restore point: 5/14/2019, 6:33:14 AM (4 r  
Backup policy: HourlyLogBackup  
Instance or AlwaysOn AG: MSSQLSERVER

Restore points

Logs in last 24 hours

Fix Inconsistent Policy

This is a recommended action to fix the issue of 'inconsistent policy' for all the impacted backup items associated with the policy 'HourlyLogBackup'. Click 'OK' and track the progress under Backup jobs.

OK | Cancel

## Re-register extension on the SQL Server VM

Sometimes, the workload extension on the VM may get impacted for one reason or the other. In such cases, all the operations triggered on the VM will begin to fail. You may then need to re-register the extension on the VM. **Re-register** operation reinstalls the workload backup extension on the VM for operations to continue.

Use this option with caution; when triggered on a VM with an already healthy extension, this operation will cause the extension to get restarted. This may result in all the in-progress jobs to fail. Kindly check for one or more of the [symptoms](#) before triggering the re-register operation.

## Next steps

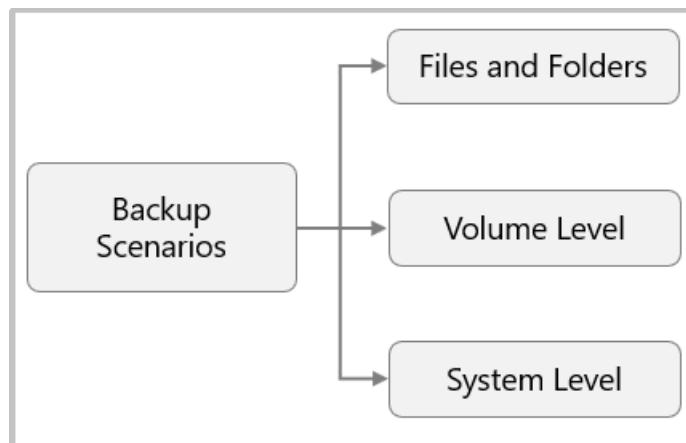
For more information, see [Troubleshoot backups on a SQL Server database](#).

# About the Microsoft Azure Recovery Services (MARS) agent

2/4/2020 • 2 minutes to read • [Edit Online](#)

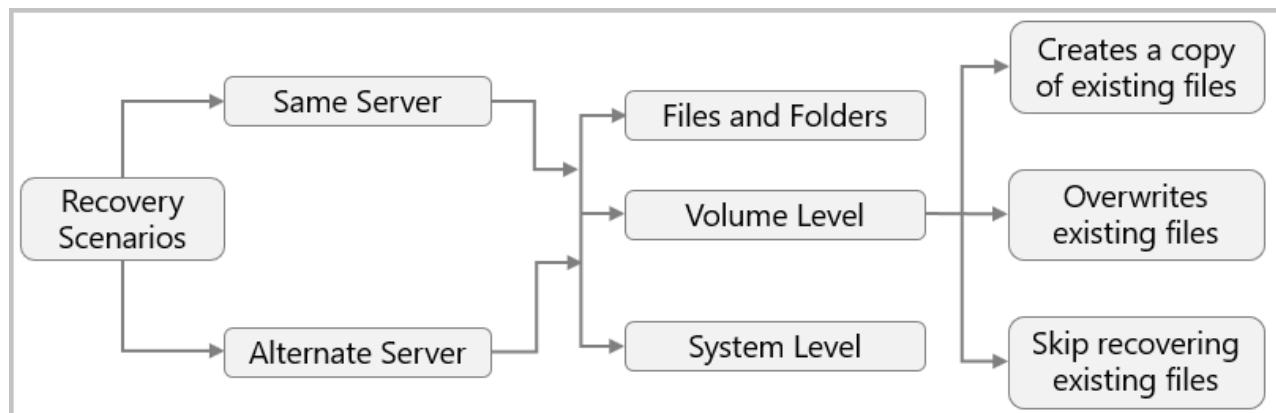
This article describes how the Azure Backup service uses the Microsoft Azure Recovery Services (MARS) agent to back up and restore files, folders, and the volume or system state from an on-premises computer to Azure.

The MARS agent supports the following backup scenarios:



- **Files and Folders:** Selectively protect Windows files and folders.
- **Volume Level:** Protect an entire Windows volume of your machine.
- **System Level:** Protect an entire Windows system state.

The MARS agent supports the following restore scenarios:



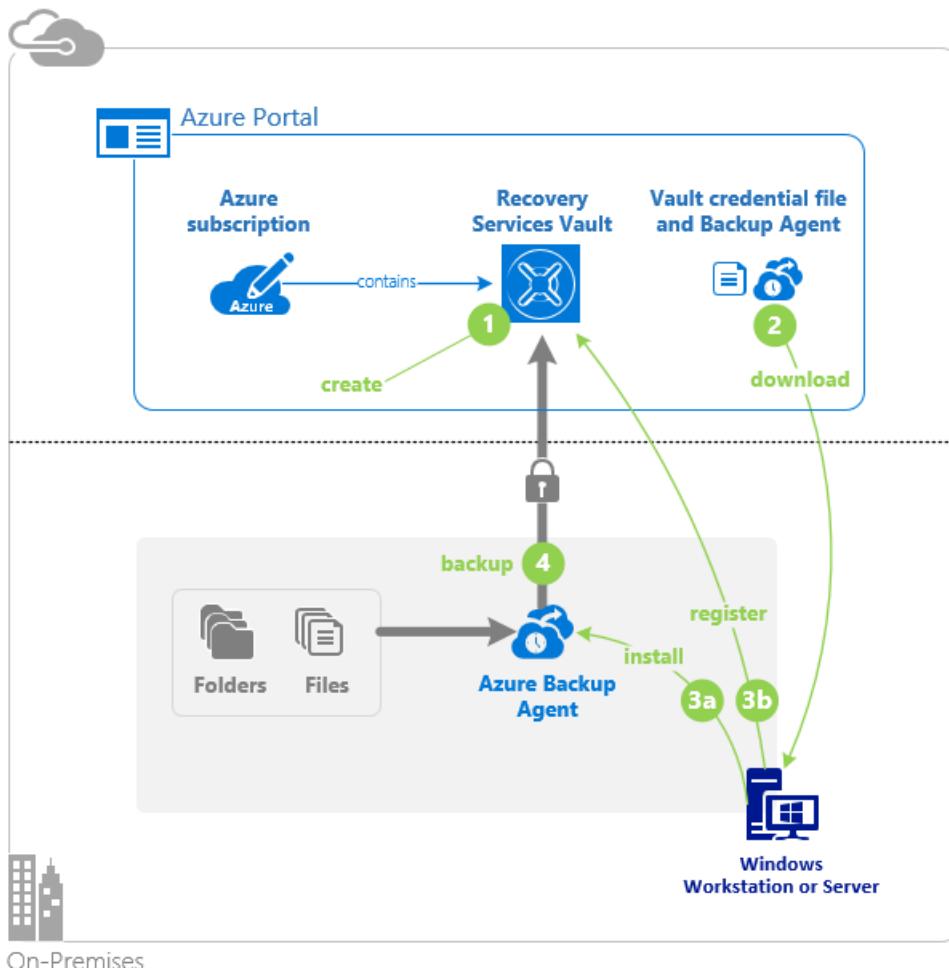
- **Same Server:** The server on which the backup was originally created.
  - **Files and Folders:** Choose the individual files and folders that you want to restore.
  - **Volume Level:** Choose the volume and recovery point that you want to restore and then restore it to the same location or an alternate location on the same machine. Create a copy of existing files, overwrite existing files, or skip recovering existing files.
  - **System Level:** Choose the system state and recovery point to restore to the same machine at a specified location.
- **Alternate Server:** A server other than the server where the backup was taken.
  - **Files and Folders:** Choose the individual files and folders whose recovery point you want to restore to a target machine.

- **Volume Level:** Choose the volume and recovery point that you want to restore to another location. Create a copy of existing files, overwrite existing files, or skip recovering existing files.
- **System Level:** Choose the system state and recovery point to restore as a System State file to an alternate machine.

## Backup process

1. From the Azure portal, create a [Recovery Services vault](#), and choose files, folders, and the system state from the Backup goals.
2. [Download the Recovery Services vault credentials and agent installer](#) to an on-premises machine. To protect the on-premises machine by selecting the Backup option, choose files, folders, and the system state, and then download the MARS agent.
3. Prepare the infrastructure:
  - a. Run the installer to [install the agent](#).
  - b. Use your downloaded vault credentials to register the machine to the Recovery Services vault.
4. From the agent console on the client, [configure the backup](#). Specify the retention policy of your backup data to start protecting it.

Azure



## Additional scenarios

- **Back up specific files and folders within Azure virtual machines:** The primary method for backing up Azure virtual machines (VMs) is to use an Azure Backup extension on the VM. The extension backs up the entire VM. If you want to back up specific files and folders within a VM, you can install the MARS agent in

the Azure VMs. For more information, see [Architecture: Built-in Azure VM Backup](#).

- **Offline seeding:** Initial full backups of data to Azure typically transfer large amounts of data and require more network bandwidth. Subsequent backups transfer only the delta, or incremental, amount of data. Azure Backup compresses the initial backups. Through the process of *offline seeding*, Azure Backup can use disks to upload the compressed initial backup data offline to Azure. For more information, see [Azure Backup offline-backup using Azure Data Box](#).

## Next steps

[MARS agent support matrix](#)

[MARS agent FAQ](#)

# Back up Windows machines by using the Azure Backup MARS agent

2/25/2020 • 11 minutes to read • [Edit Online](#)

This article explains how to back up Windows machines by using the [Azure Backup](#) service and the Microsoft Azure Recovery Services (MARS) agent. MARS is also known as the Azure Backup agent.

In this article, you learn how to:

- Verify the prerequisites and create a Recovery Services vault.
- Download and set up the MARS agent.
- Create a backup policy and schedule.
- Perform an on-demand backup.

## About the MARS agent

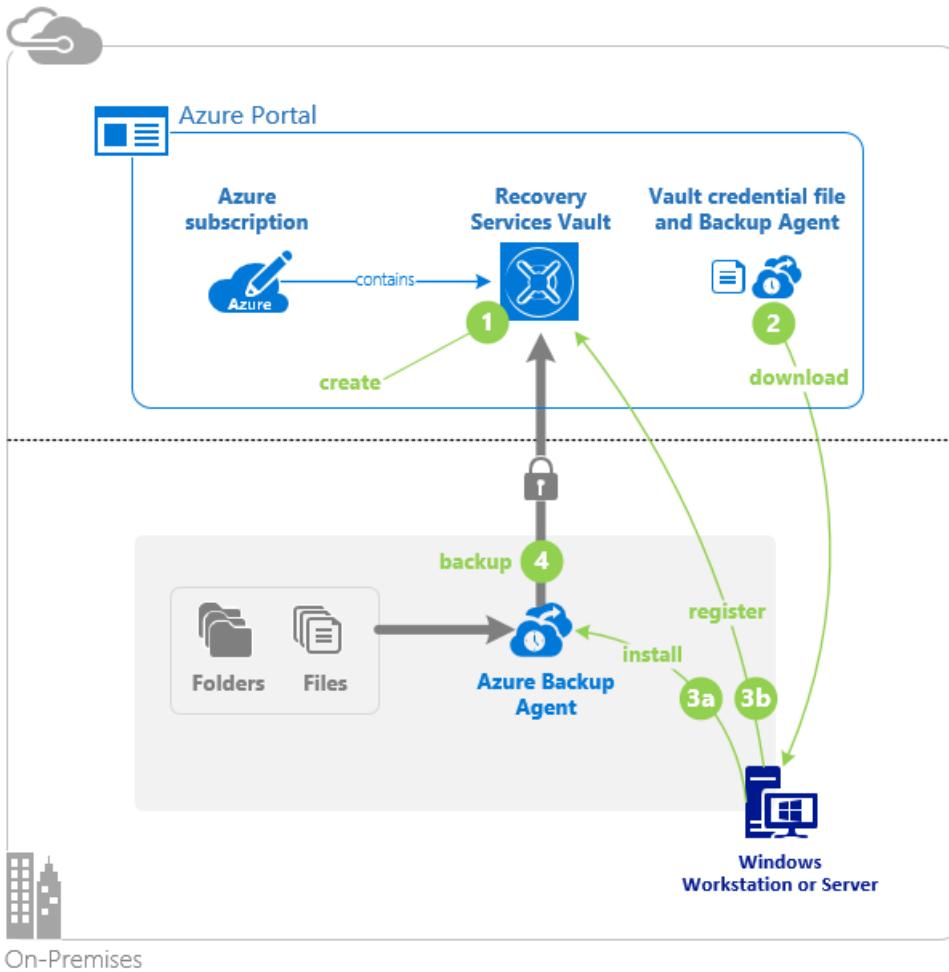
Azure Backup uses the MARS agent to back up files, folders, and system state from on-premises machines and Azure VMs. Those backups are stored in a Recovery Services vault in Azure. You can run the agent:

- 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.

### NOTE

Generally, you back up an Azure VM by using an Azure Backup extension on the VM. This method backs up the entire VM. If you want to back up specific files and folders on the VM, install and use the MARS agent alongside the extension. For more information, see [Architecture of a built-in Azure VM backup](#).



## Before you start

- Learn how [Azure Backup uses the MARS agent to back up Windows machines](#).
- Learn about the [backup architecture](#) that runs the MARS agent on a secondary MABS or Data Protection Manager server.
- Review [what's supported and what you can back up](#) by the MARS agent.
- Make sure that you have an Azure account if you need to back up a server or client to Azure. If you don't have an account, you can create a [free one](#) in just a few minutes.
- Verify internet access on the machines that you want to back up.

### Verify internet access

If your machine has limited internet access, ensure that firewall settings on the machine or proxy allow the following URLs and IP addresses:

- URLs
  - `www\.\msftncsi.com`
  - `*.Microsoft.com`
  - `*.WindowsAzure.com`
  - `*.microsoftonline.com`
  - `*.windows.net`
- IP addresses
  - `20.190.128.0/18`
  - `40.126.0.0/18`

## Use Azure ExpressRoute

You can back up your data over Azure ExpressRoute by using public peering (available for old circuits) and Microsoft peering. Backup over private peering isn't supported.

To use public peering, first ensure access to the following domains and addresses:

- <http://www.msftncsi.com/ncsi.txt>
- [microsoft.com](http://microsoft.com)
- [.WindowsAzure.com](http://.WindowsAzure.com)
- [.microsoftonline.com](http://.microsoftonline.com)
- [.windows.net](http://.windows.net)

To use Microsoft peering, select the following services, regions, and relevant community values:

- Azure Active Directory (12076:5060)
- Azure region, according to the location of your Recovery Services vault
- Azure Storage, according to the location of your Recovery Services vault

For more information, see [ExpressRoute routing requirements](#).

### NOTE

Public peering is deprecated for new circuits.

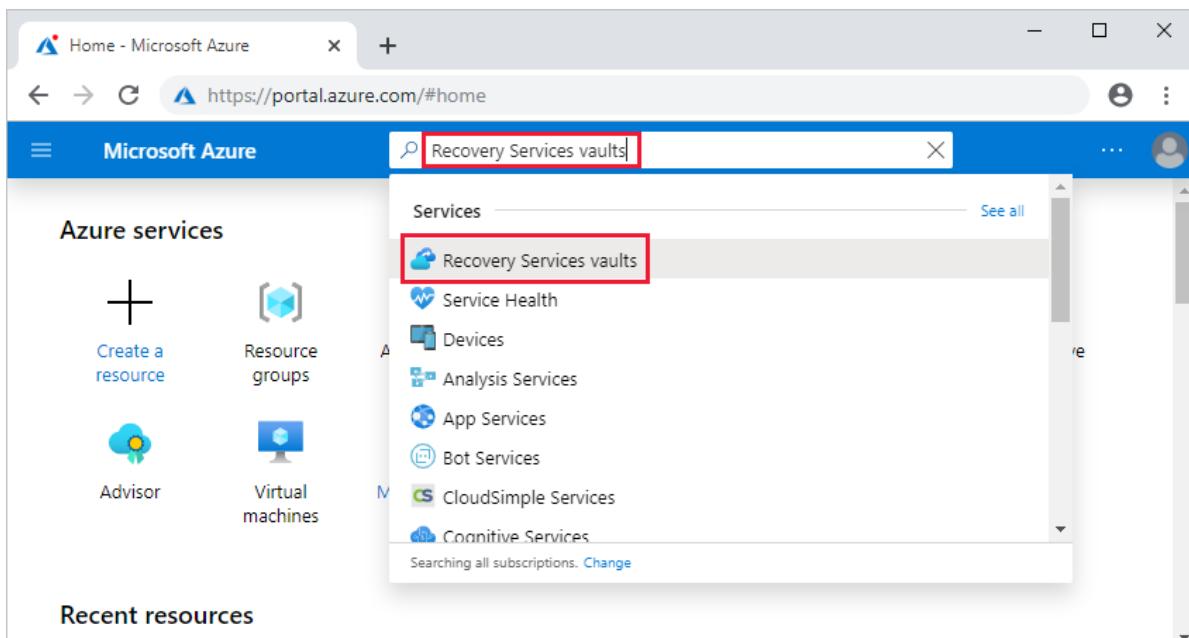
All of the preceding URLs and IP addresses use the HTTPS protocol on port 443.

## Create a Recovery Services vault

A Recovery Services vault stores all the backups and recovery points that you create over time. It also contains the backup policy for the backed-up machines.

To create a vault:

1. Sign in to the [Azure portal](#) by using your Azure subscription.
2. Search for and select **Recovery Services vaults**.



3. On the **Recovery Services vaults** menu, select **Add**.

The screenshot shows the 'Recovery Services vaults' page in the Azure portal. At the top left, there's a breadcrumb navigation: 'Home > Recovery Services vaults'. Below it, the title 'Recovery Services vaults' is followed by 'Microsoft'. A red box highlights the blue 'Add' button. To its right are 'Edit columns', 'Refresh', and 'Assign tags' buttons. The 'Subscriptions' dropdown is set to 'CAT\_Eng'. Below these are several filter and search boxes: 'Filter by name...', 'All resource groups', 'All locations', 'All tags', and 'No grouping'. A message '0 items' is displayed. The main table has columns: NAME (sorted by ascending), RESOURCE GROUP (sorted by ascending), LOCATION (sorted by ascending), and SUBSCRIPTION (sorted by ascending). The table is currently empty.

4. For **Name**, enter a friendly name to identify the vault.

- The name needs to be unique for the Azure subscription.
- It can contain 2 to 50 characters.
- It must start with a letter.
- It can contain only letters, numbers, and hyphens.

5. Select the Azure subscription, resource group, and geographic region in which the vault should be created.

Backup data is sent to the vault. Select **Create**.

The screenshot shows the 'Recovery Services vault' creation dialog. The title bar says 'Recovery Services vault'. The form contains four required fields: 'Name' (with placeholder 'Enter the name'), 'Subscription' (a dropdown menu), 'Resource group' (a dropdown menu with 'Create new' option), and 'Location' (a dropdown menu set to 'Central India'). At the bottom of the dialog are two buttons: a blue 'Create' button and a grey 'Automation options' button.

The system might take a while to create the vault. Monitor the status notifications in the upper-right area of the portal. If you don't see the vault after several minutes, select **Refresh**.

**Recovery Services vaults**

Microsoft

+ Add Edit columns Refresh Assign tags

## Set storage redundancy

Azure Backup automatically handles storage for the vault. You specify how to replicate that storage.

1. Under **Recovery Services vaults**, select the new vault. Under **Settings**, select **Properties**.
2. In **Properties**, under **Backup Configuration**, select **Update**.
3. Select the storage replication type, and select **Save**.

The screenshot shows the 'DemoVault - Properties' blade in the Azure portal. On the left, there's a sidebar with links like 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Properties' (which is highlighted with a red box), 'Locks', 'Automation script', 'Getting started', 'Backup', 'Site Recovery', 'Protected items', 'Backup items', 'Replicated items', 'Manage', 'Backup policies', and 'Backup Infrastructure'. The main area shows vault details: STATUS (Active), LOCATION (Central India), SUBSCRIPTION NAME, SUBSCRIPTION ID, RESOURCE GROUP (mayurssg01), and DIAGNOSTICS SETTINGS (Update). On the right, the 'Backup Configuration' tab is selected, showing options for 'Locally-redundant' and 'Geo-redundant' (which is highlighted with a red box). At the bottom, there are 'Save', 'Discard', and 'Refresh' buttons.

We recommend that if you use Azure as a primary backup storage endpoint, continue to use the default **Geo-redundant** setting. If you don't use Azure as a primary backup storage endpoint, select **Locally redundant** to reduce the Azure storage costs.

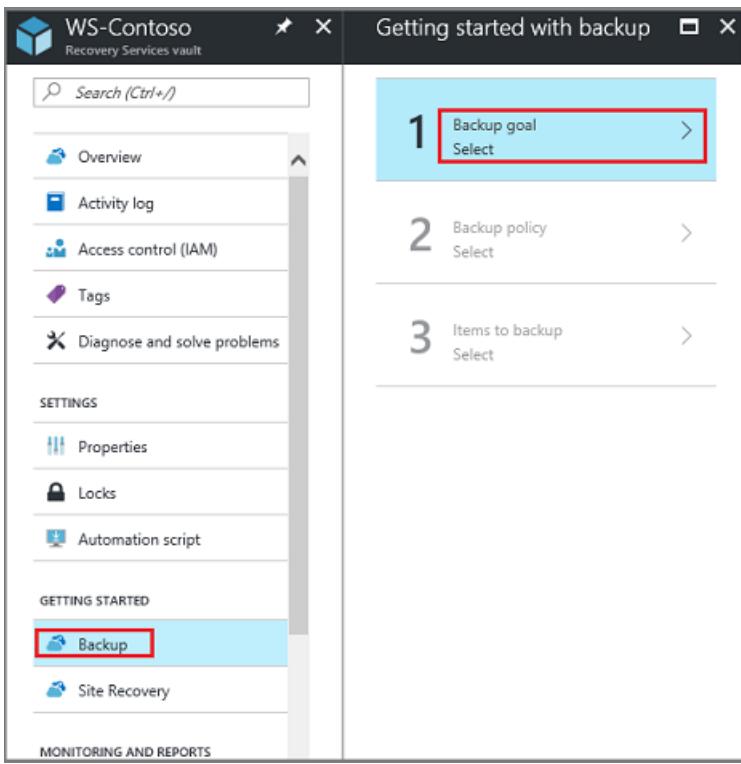
For more information, see [Geo-redundancy](#) and [Local redundancy](#).

## Download the MARS agent

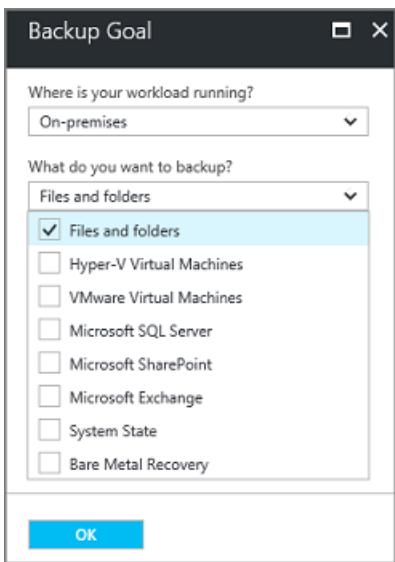
Download the MARS agent so that you can install it on the machines that you want to back up.

If you've already installed the agent on any machines, make sure that you're running the latest version of the agent. Find the latest version in the portal, or go directly to the [download](#).

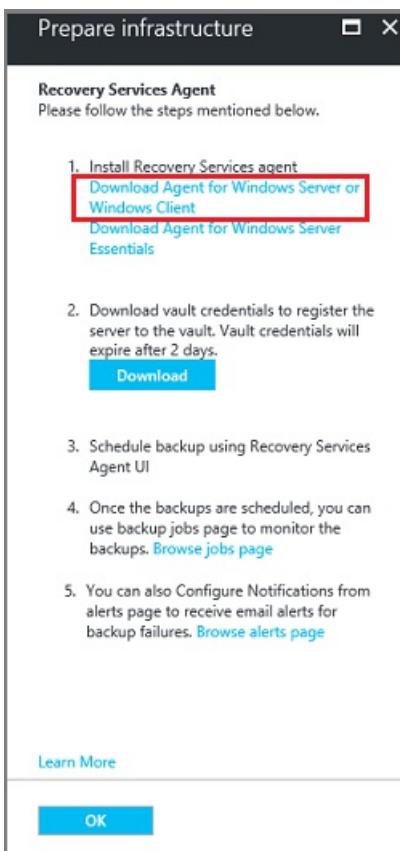
1. In the vault, under **Getting Started**, select **Backup**.



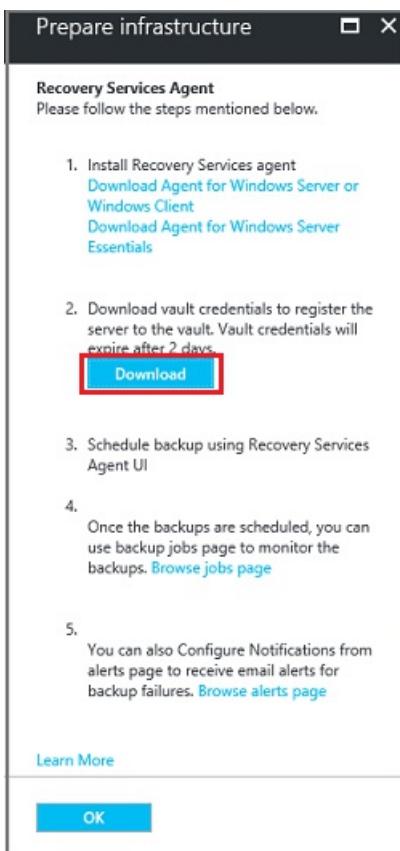
2. Under **Where is your workload running?**, select **On-premises**. Select this option even if you want to install the MARS agent on an Azure VM.
3. Under **What do you want to back up?**, select **Files and folders**. You can also select **System State**. Many other options are available, but these options are supported only if you're running a secondary backup server. Select **Prepare Infrastructure**.



4. For **Prepare infrastructure**, under **Install Recovery Services agent**, download the MARS agent.



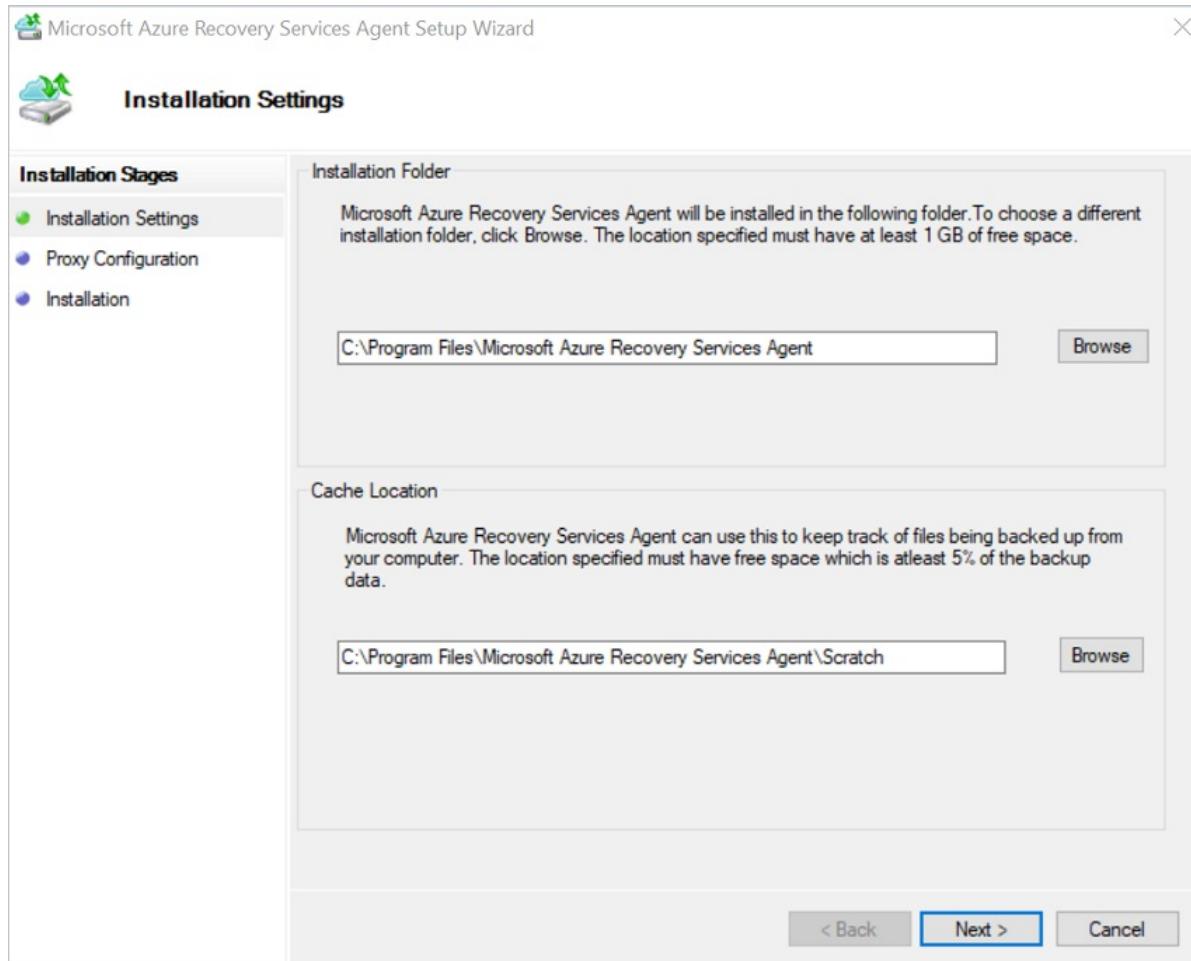
5. In the download menu, select **Save**. By default, the *MARSagentinstaller.exe* file is saved to your Downloads folder.
6. Select **Already download or using the latest Recovery Services Agent**, and then download the vault credentials.



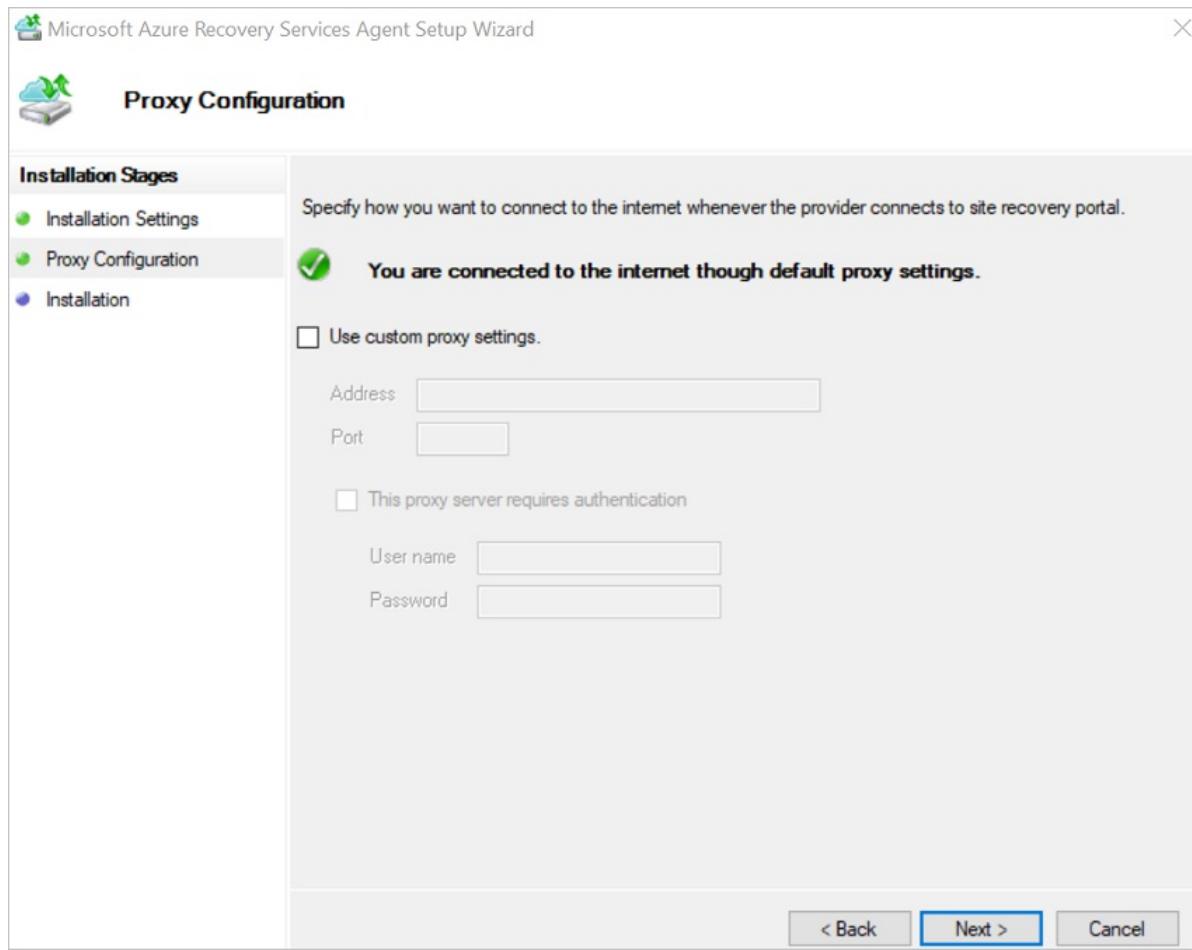
7. Select **Save**. The file is downloaded to your Downloads folder. You can't open the vault credentials file.

## Install and register the agent

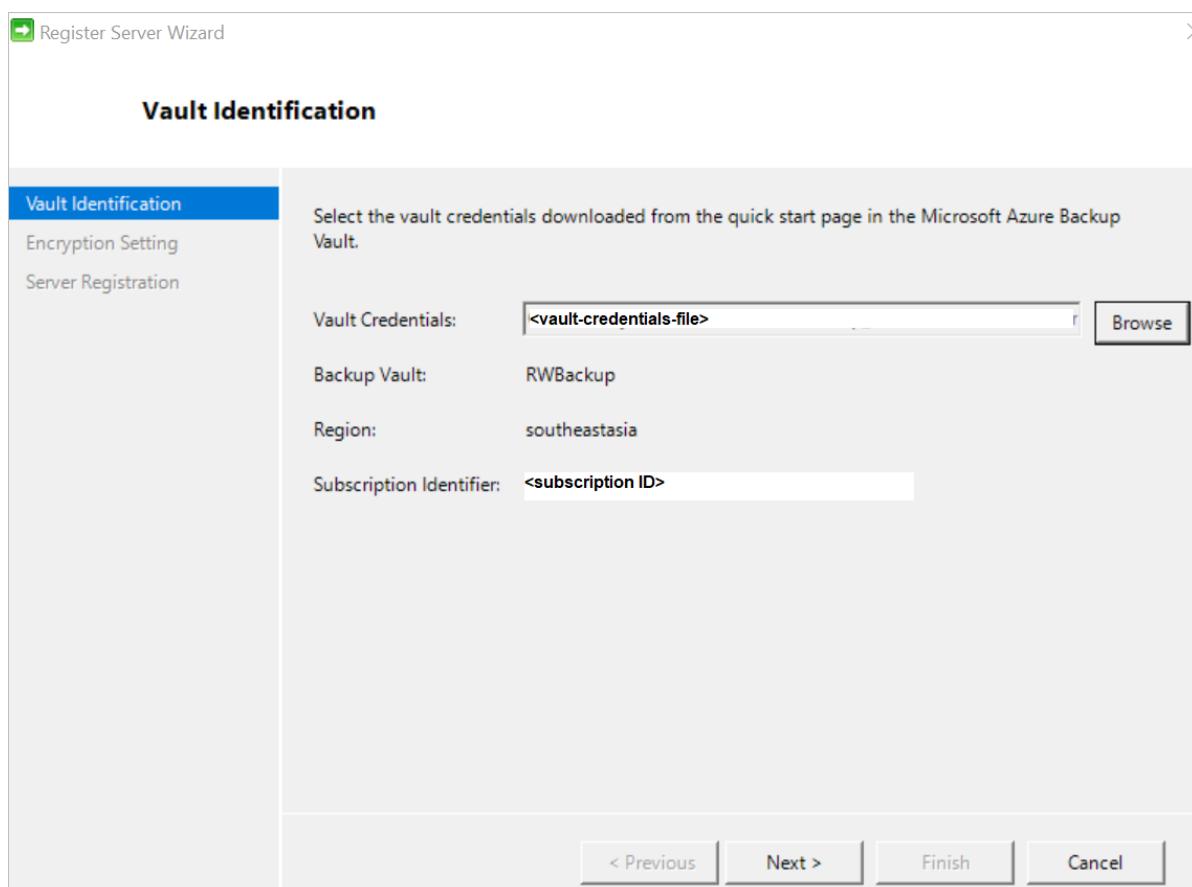
1. Run the *MARSagentinstaller.exe* file on the machines that you want to back up.
2. In the MARS Agent Setup Wizard, select **Installation Settings**. There, choose where to install the agent, and choose a location for the cache. Then select **Next**.
  - Azure Backup uses the cache to store data snapshots before sending them to Azure.
  - The cache location should have free space equal to at least 5 percent of the size of the data you'll back up.



3. For **Proxy Configuration**, specify how the agent that runs on the Windows machine will connect to the internet. Then select **Next**.
  - If you use a custom proxy, specify any necessary proxy settings and credentials.
  - Remember that the agent needs access to [specific URLs](#).



4. For **Installation**, review the prerequisites, and select **Install**.
5. After the agent is installed, select **Proceed to Registration**.
6. In **Register Server Wizard > Vault Identification**, browse to and select the credentials file that you downloaded. Then select **Next**.



7. On the **Encryption Setting** page, specify a passphrase that will be used to encrypt and decrypt backups for the machine.
  - Save the passphrase in a secure location. You need it to restore a backup.
  - If you lose or forget the passphrase, Microsoft can't help you recover the backup data.
8. Select **Finish**. The agent is now installed, and your machine is registered to the vault. You're ready to configure and schedule your backup.

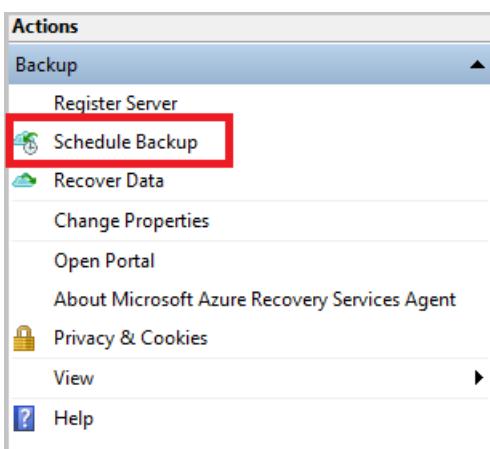
## Create a backup policy

The backup policy specifies when to take snapshots of the data to create recovery points. It also specifies how long to keep recovery points. You use the MARS agent to configure a backup policy.

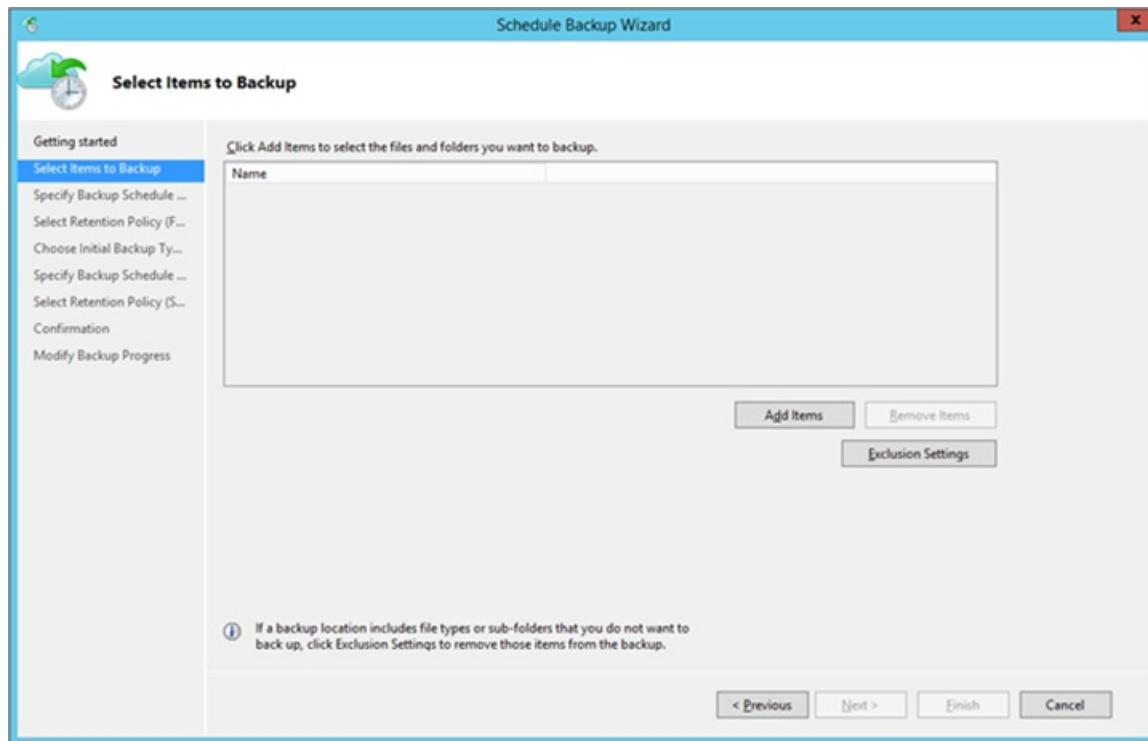
Azure Backup doesn't automatically take daylight saving time (DST) into account. This default could cause some discrepancy between the actual time and the scheduled backup time.

To create a backup policy:

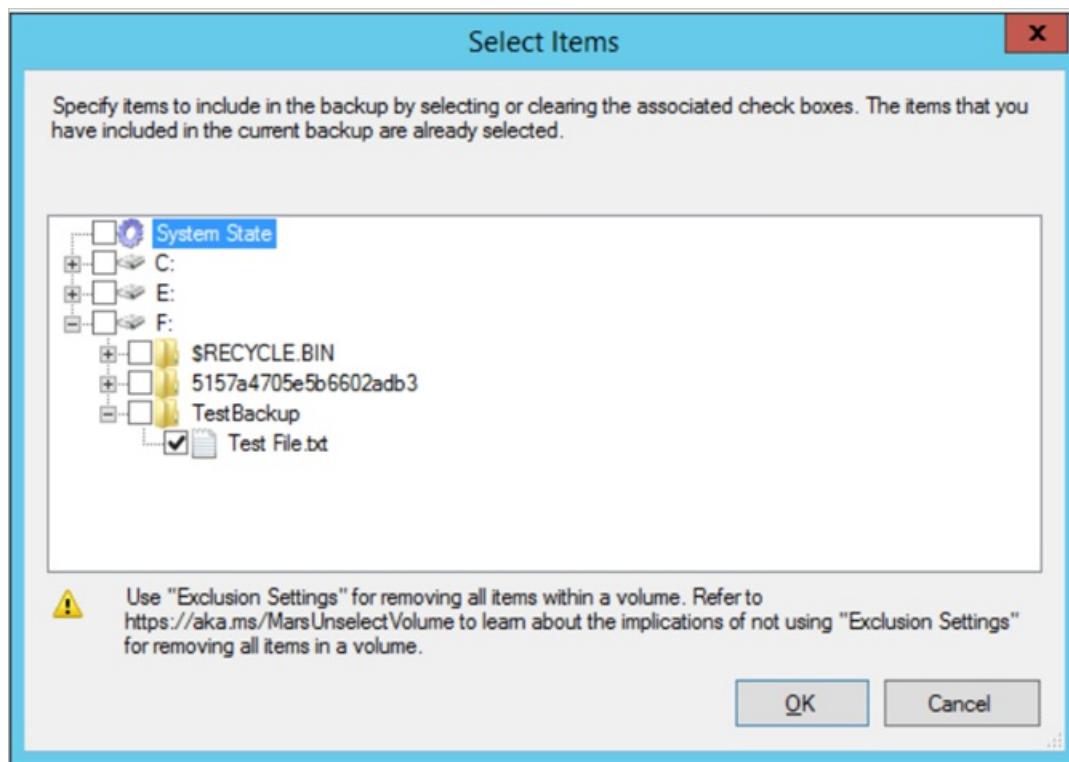
1. After you download and register the MARS agent, open the agent console. You can find it by searching your machine for **Microsoft Azure Backup**.
2. Under **Actions**, select **Schedule Backup**.



3. In the Schedule Backup Wizard, select **Getting started > Next**.
4. Under **Select Items to Back up**, select **Add Items**.



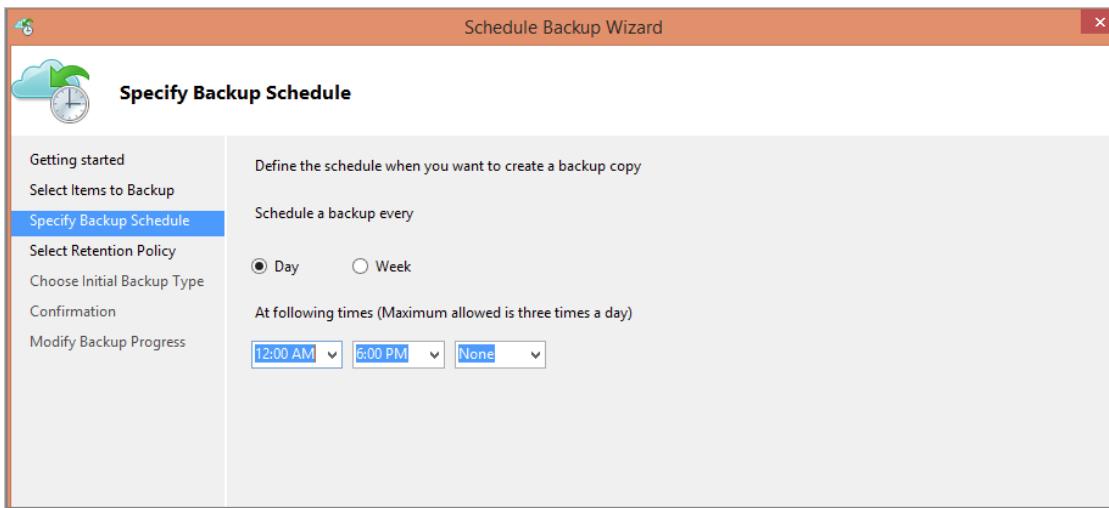
5. In the **Select Items** box, select items to back up, and then select **OK**.



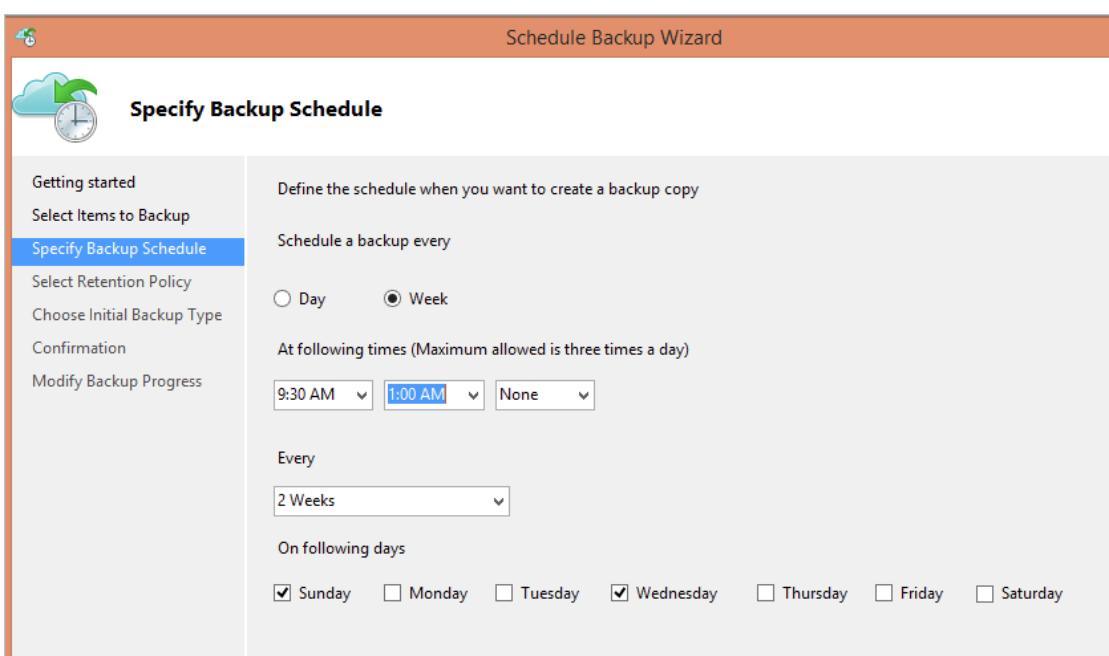
6. On the **Select Items to Back Up** page, select **Next**.

7. On the **Specify Backup Schedule** page, specify when to take daily or weekly backups. Then select **Next**.

- A recovery point is created when a backup is taken.
- The number of recovery points created in your environment depends on your backup schedule.
- You can schedule up to three daily backups per day. In the following example, two daily backups occur, one at midnight and one at 6:00 PM.

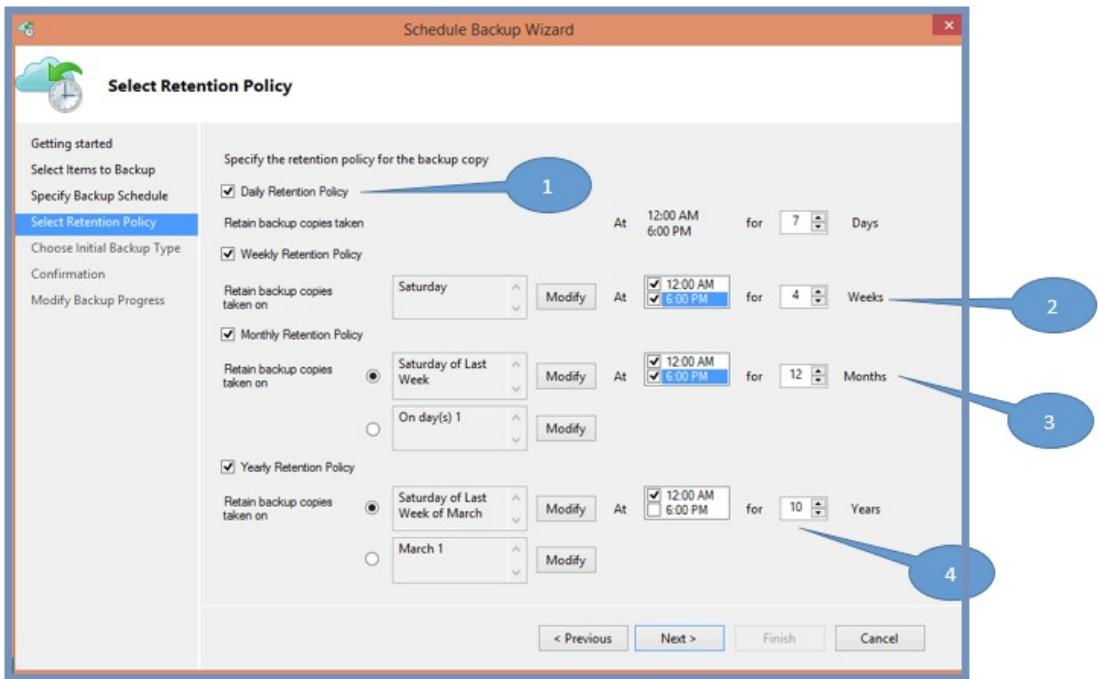


- You can run weekly backups too. In the following example, backups are taken every alternate Sunday and Wednesday at 9:30 AM and 1:00 AM.



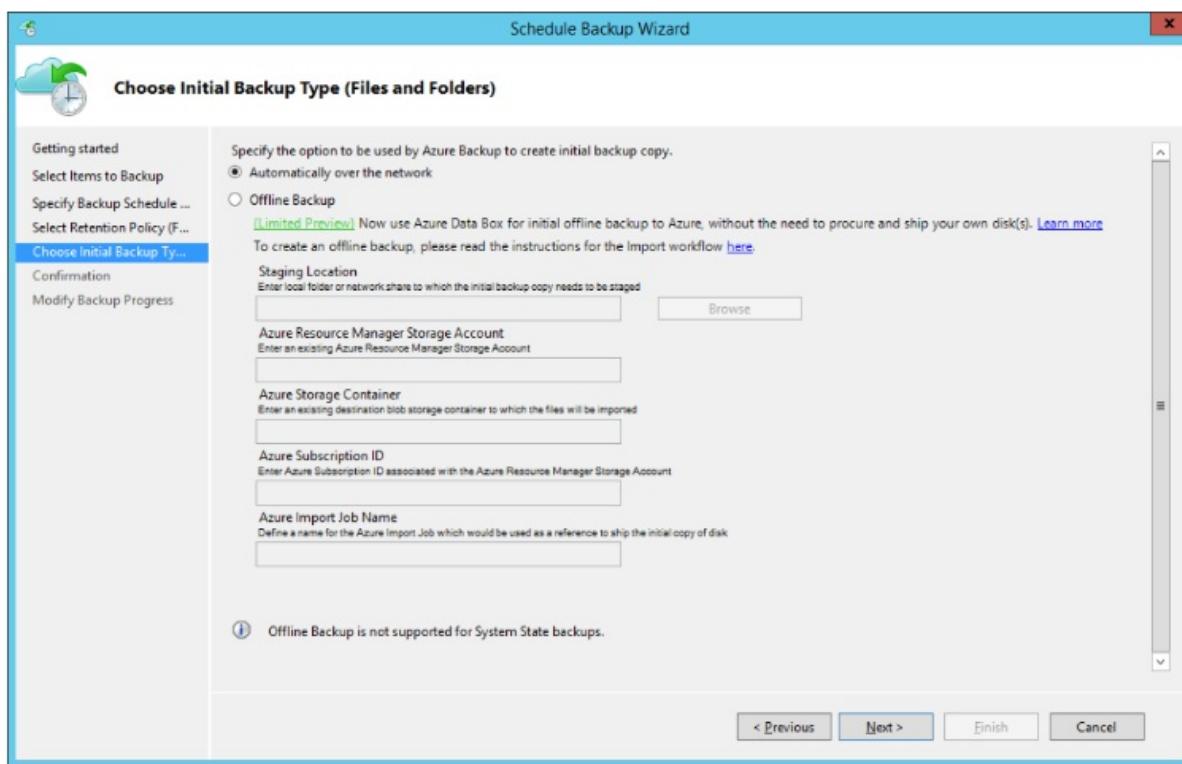
8. On the **Select Retention Policy** page, specify how to store historical copies of your data. Then select **Next**.

- Retention settings specify which recovery points to store and how long to store them.
- For a daily retention setting, you indicate that at the time specified for the daily retention, the latest recovery point will be retained for the specified number of days. Or you could specify a monthly retention policy to indicate that the recovery point created on the 30th of every month should be stored for 12 months.
- Retention for daily and weekly recovery points usually coincides with the backup schedule. So when the schedule triggers a backup, the recovery point that the backup creates is stored for the duration that the daily or weekly retention policy specifies.
- In the following example:
  - Daily backups at midnight and 6:00 PM are kept for seven days.
  - Backups taken on a Saturday at midnight and 6:00 PM are kept for four weeks.
  - Backups taken on the last Saturday of the month at midnight and 6:00 PM are kept for 12 months.
  - Backups taken on the last Saturday in March are kept for 10 years.

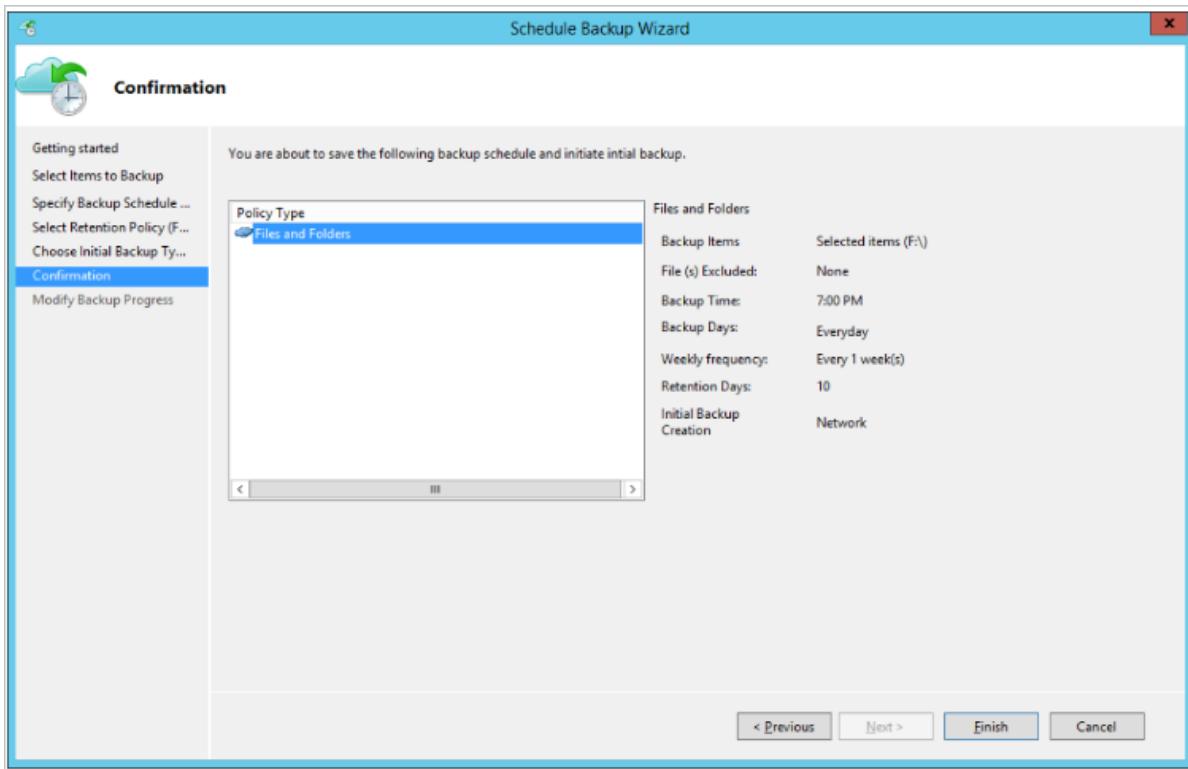


9. On the **Choose Initial Backup Type** page, decide if you want to take the initial backup over the network or use offline backup. To take the initial backup over the network, select **Automatically over the network** > **Next**.

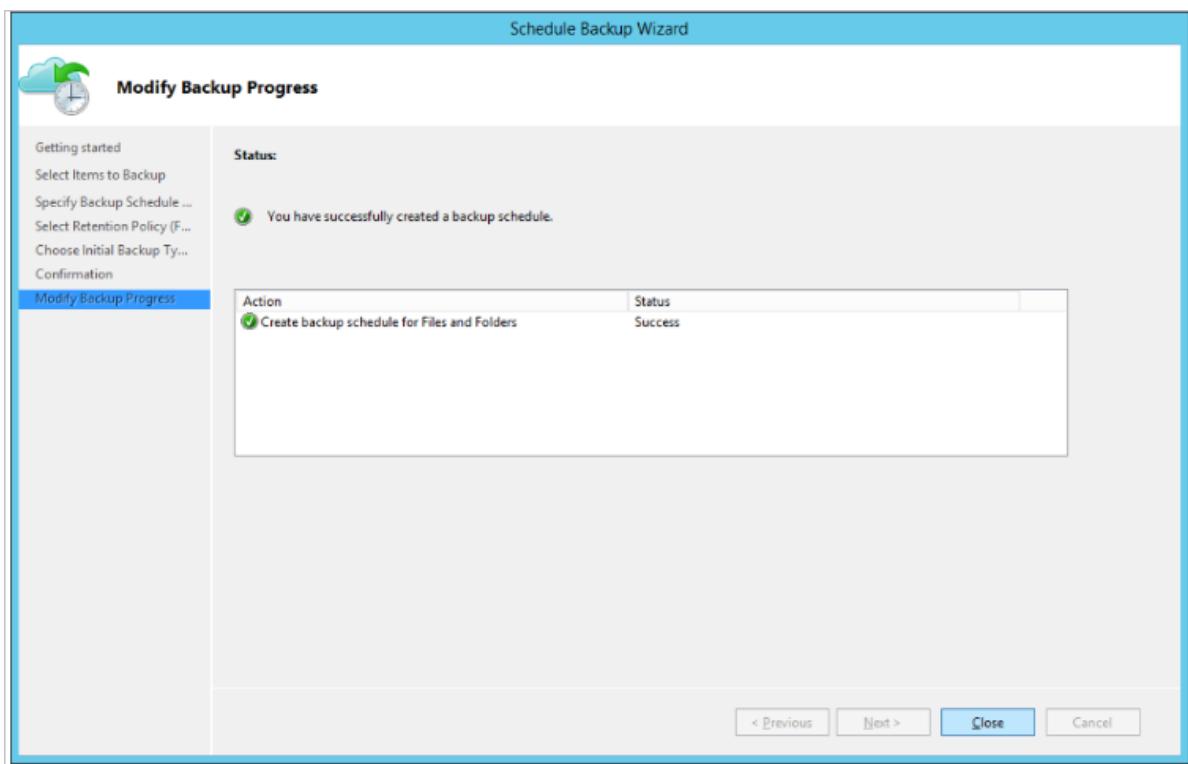
For more information about offline backup, see [Use Azure Data Box for offline backup](#).



10. On the **Confirmation** page, review the information, and then select **Finish**.



11. After the wizard finishes creating the backup schedule, select **Close**.



Create a policy on each machine where the agent is installed.

#### Do the initial backup offline

You can run an initial backup automatically over the network, or you can back up offline. Offline seeding for an initial backup is useful if you have large amounts of data that will require a lot of network bandwidth to transfer.

To do an offline transfer:

1. Write the backup data to a staging location.
2. Use the AzureOfflineBackupDiskPrep tool to copy the data from the staging location to one or more SATA disks.

The tool creates an Azure Import job. For more information, see [What is the Azure Import/Export service](#).

### 3. Send the SATA disks to an Azure datacenter.

At the datacenter, the disk data is copied to an Azure storage account. Azure Backup copies the data from the storage account to the vault, and incremental backups are scheduled.

For more information about offline seeding, see [Use Azure Data Box for offline backup](#).

### Enable network throttling

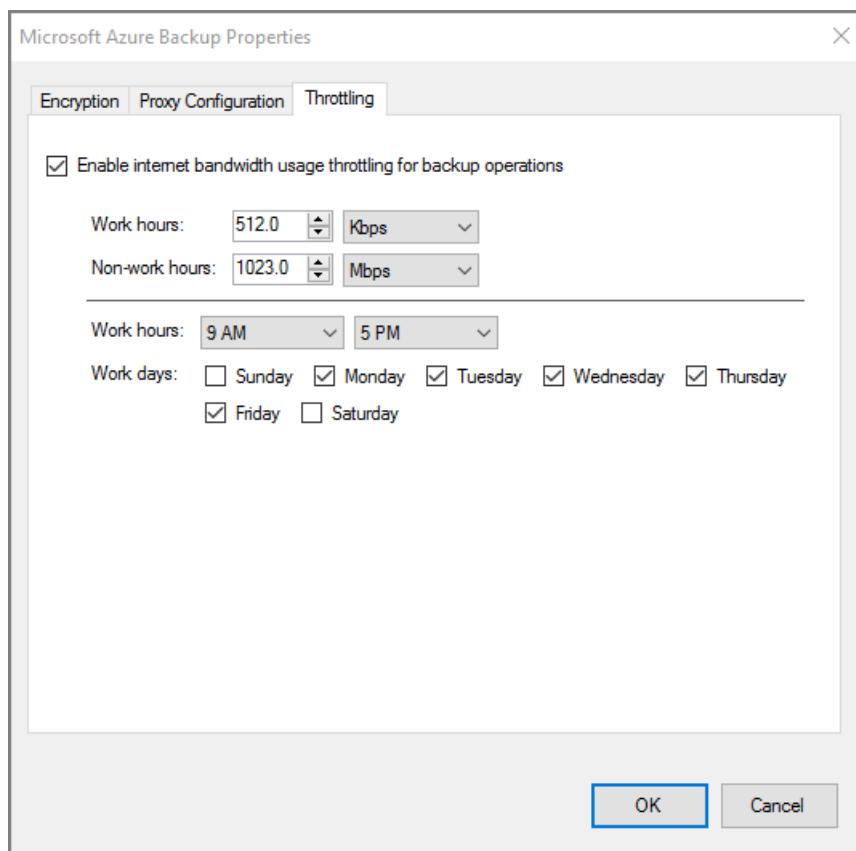
You can control how the MARS agent uses network bandwidth by enabling network throttling. Throttling is helpful if you need to back up data during work hours but you want to control how much bandwidth the backup and restore activity uses.

Network throttling in Azure Backup uses [Quality of Service \(QoS\)](#) on the local operating system.

Network throttling for backups is available on Windows Server 2012 and later, and on Windows 8 and later. Operating systems should be running the latest service packs.

To enable network throttling:

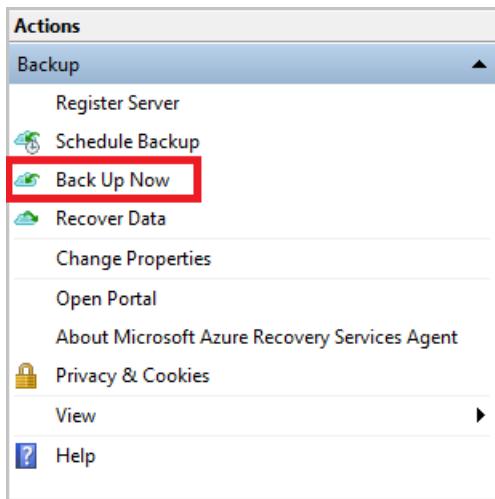
1. In the MARS agent, select **Change Properties**.
2. On the **Throttling** tab, select **Enable internet bandwidth usage throttling for backup operations**.



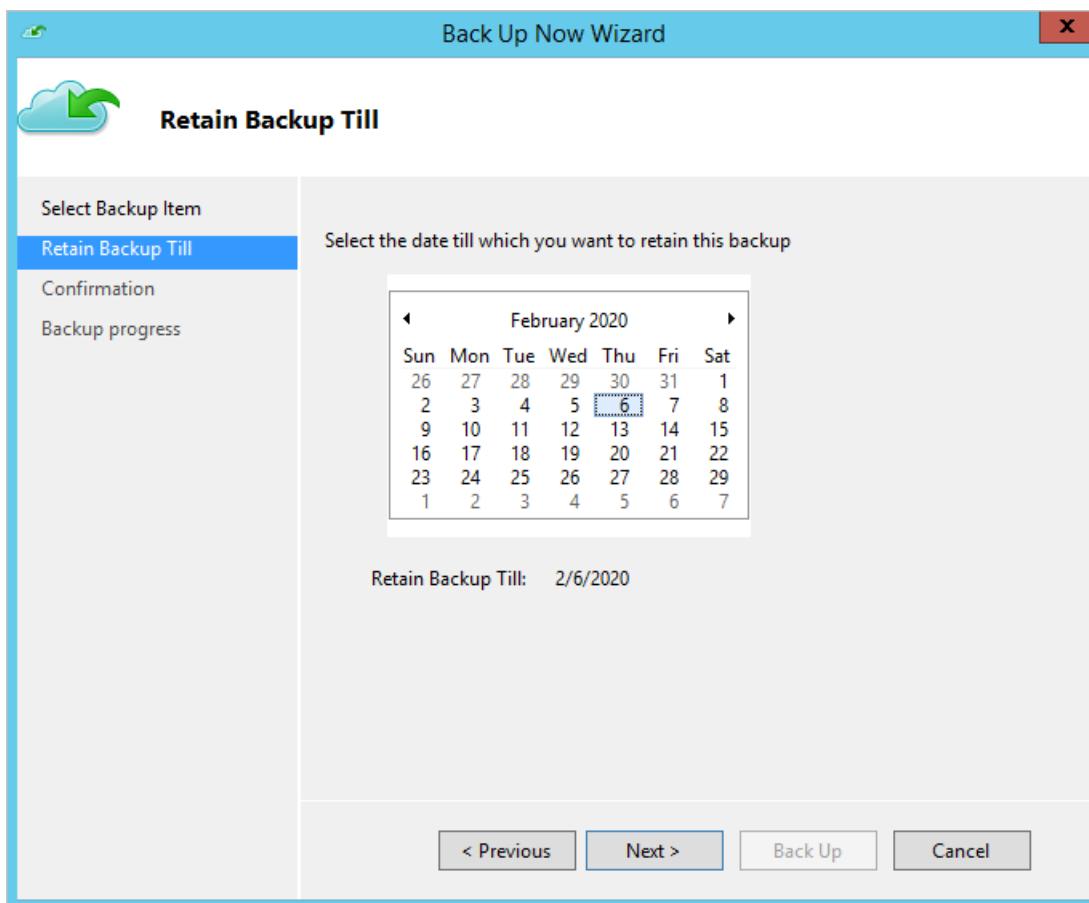
3. Specify the allowed bandwidth during work hours and nonwork hours. Bandwidth values begin at 512 Kbps and go up to 1,023 MBps. Then select **OK**.

## Run an on-demand backup

1. In the MARS agent, select **Back Up Now**.



2. If the MARS agent version is 2.0.9169.0 or newer, then you can set a custom retention date. In the **Retain Backup Till** section, choose a date from the calendar.



3. On the **Confirmation** page, review the settings, and select **Back Up**.
4. Select **Close** to close the wizard. If you close the wizard before the backup finishes, the wizard continues to run in the background.

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

## Set up on-demand backup policy retention behavior

### NOTE

This information applies only to MARS agent versions that are older than 2.0.9169.0.

| BACKUP-SCHEDULE OPTION | DURATION OF DATA RETENTION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Day                    | <p><b>Default retention:</b> Equivalent to the "retention in days for daily backups."</p> <p><b>Exception:</b> If a daily scheduled backup that's set for long-term retention (weeks, months, or years) fails, an on-demand backup that's triggered right after the failure is considered for long-term retention. Otherwise, the next scheduled backup is considered for long-term retention.</p> <p><b>Example scenario:</b> The scheduled backup on Thursday at 8:00 AM failed. This backup was to be considered for weekly, monthly, or yearly retention. So the first on-demand backup triggered before the next scheduled backup on Friday at 8:00 AM is automatically tagged for weekly, monthly, or yearly retention. This backup substitutes for the Thursday 8:00 AM backup.</p>                                                                                                                                   |
| Week                   | <p><b>Default retention:</b> One day. On-demand backups that are taken for a data source that has a weekly backup policy are deleted the next day. They're deleted even if they're the most recent backups for the data source.</p> <p><b>Exception:</b> If a weekly scheduled backup that's set for long-term retention (weeks, months, or years) fails, an on-demand backup that's triggered right after the failure is considered for long-term retention. Otherwise, the next scheduled backup is considered for long-term retention.</p> <p><b>Example scenario:</b> The scheduled backup on Thursday at 8:00 AM failed. This backup was to be considered for monthly or yearly retention. So the first on-demand backup that's triggered before the next scheduled backup on Thursday at 8:00 AM is automatically tagged for monthly or yearly retention. This backup substitutes for the Thursday 8:00 AM backup.</p> |

For more information, see [Create a backup policy](#).

## Next steps

Learn how to [Restore files in Azure](#).

# Back up Windows system state in Resource Manager deployment

2/24/2020 • 8 minutes to read • [Edit Online](#)

This article explains how to back up your Windows Server system state to Azure. It's intended to walk you through the basics.

If you want to know more about Azure Backup, read this [overview](#).

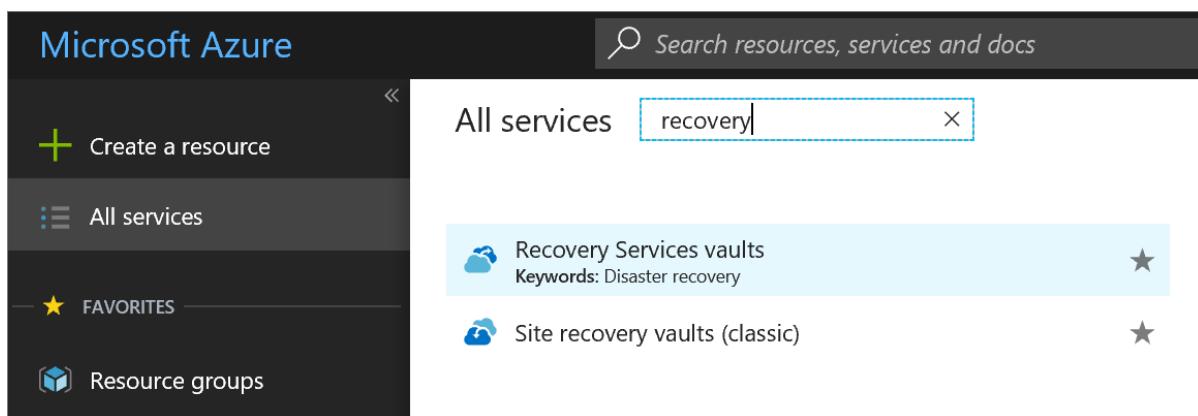
If you don't have an Azure subscription, create a [free account](#) that lets you access any Azure service.

## Create a recovery services vault

To back up your Windows Server System State, you need to create a Recovery Services vault in the region where you want to store the data. You also need to determine how you want your storage replicated.

### To create a Recovery Services vault

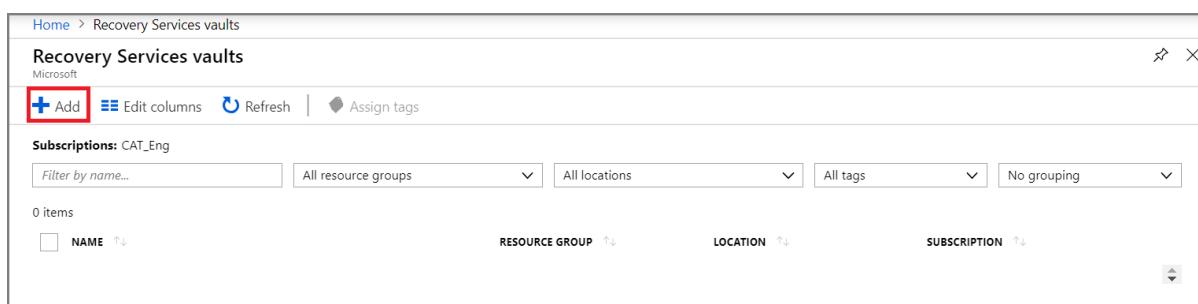
1. If you haven't already done so, sign in to the [Azure portal](#) using your Azure subscription.
2. On the Hub menu, click **All services** and in the list of resources, type **Recovery Services** and click **Recovery Services vaults**.



The screenshot shows the Microsoft Azure portal's search interface. The search bar at the top has the word "recovery" typed into it. Below the search bar, the results are displayed under the heading "All services". There are two entries: "Recovery Services vaults" and "Site recovery vaults (classic)". Each entry includes a small blue cloud icon, the name of the service, a brief description, and a star icon for favoriting.

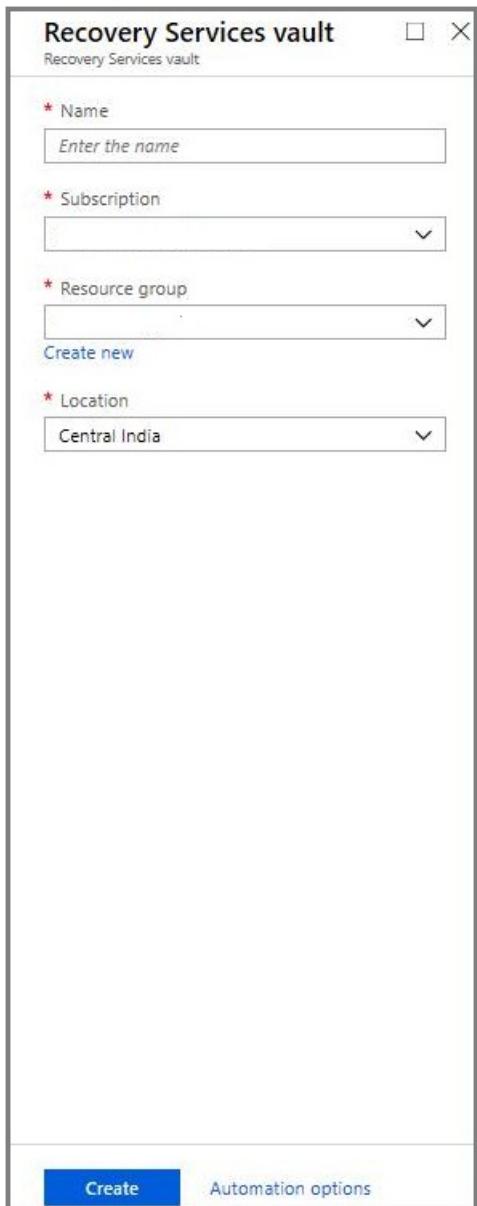
If there are recovery services vaults in the subscription, the vaults are listed.

3. On the **Recovery Services vaults** menu, click **Add**.



The screenshot shows the "Recovery Services vaults" blade in the Azure portal. At the top left, there is a breadcrumb navigation: "Home > Recovery Services vaults". Below the breadcrumb, the title "Recovery Services vaults" is followed by a "Microsoft" logo. A red box highlights the "Add" button, which is located in the top-left corner of the blade. The blade also features a "Edit columns" button, a "Refresh" button, and an "Assign tags" button. Below these buttons, there is a "Subscriptions" dropdown set to "CAT\_Eng". Underneath the subscriptions, there are filter fields for "Filter by name...", "All resource groups", "All locations", "All tags", and "No grouping". The main area of the blade displays a table with one row, indicating "0 items". The columns of the table are labeled "NAME", "RESOURCE GROUP", "LOCATION", and "SUBSCRIPTION".

The Recovery Services vault blade opens, prompting you to provide a **Name**, **Subscription**, **Resource group**, and **Location**.



4. For **Name**, enter a friendly name to identify the vault. The name needs to be unique for the Azure subscription. Type a name that contains between 2 and 50 characters. It must start with a letter, and can contain only letters, numbers, and hyphens.
5. In the **Subscription** section, use the drop-down menu to choose the Azure subscription. If you use only one subscription, that subscription appears and you can skip to the next step. If you are not sure which subscription to use, use the default (or suggested) subscription. There are multiple choices only if your organizational account is associated with multiple Azure subscriptions.
6. In the **Resource group** section:
  - select **Create new** if you want to create a Resource group. Or
  - select **Use existing** and click the drop-down menu to see the available list of Resource groups.For complete information on Resource groups, see the [Azure Resource Manager overview](#).
7. Click **Location** to select the geographic region for the vault. This choice determines the geographic region where your backup data is sent.
8. At the bottom of the Recovery Services vault blade, 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. If after several minutes you don't see your vault, click **Refresh**.

## Recovery Services vaults

Microsoft

+ Add

Edit columns

Refresh

Assign tags

Once you see your vault in the list of Recovery Services vaults, you are ready to set the storage redundancy.

### Set storage redundancy for the vault

When you create a Recovery Services vault, make sure storage redundancy is configured the way you want.

1. From the **Recovery Services vaults** blade, click the new vault.

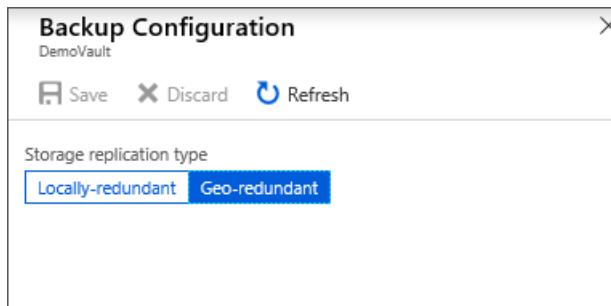
The screenshot shows the 'Recovery Services vaults' blade. On the left is a vertical toolbar with various icons. The main area has a header 'Recovery Services vaults' and 'Subscriptions: <subscription>'. Below is a table with four items:

| NAME               | RESOURCE GR...    | LOCATION       | SUBSCRIPTION   | ... |
|--------------------|-------------------|----------------|----------------|-----|
| Contoso-MAB-server | Contoso-Resources | Southeast Asia | <subscription> | ... |
| Contoso-testvault  | Contoso-Resources | Southeast Asia | <subscription> | ... |
| Contoso-vault      | Contoso-Resources | Southeast Asia | <subscription> | ... |
| WS-Contoso         | Contoso-Resources | Southeast Asia | <subscription> | ... |

When you select the vault, the **Recovery Services vault** blade narrows, and the Settings blade (*which has the name of the vault at the top*) and the vault details blade open.

2. In the new vault's Settings blade, use the vertical slide to scroll down to the Manage section, and click **Backup Infrastructure**. The Backup Infrastructure blade opens.
3. In the Backup Infrastructure blade, click **Backup Configuration** to open the **Backup Configuration** blade.

4. Choose the appropriate storage replication option for your vault.

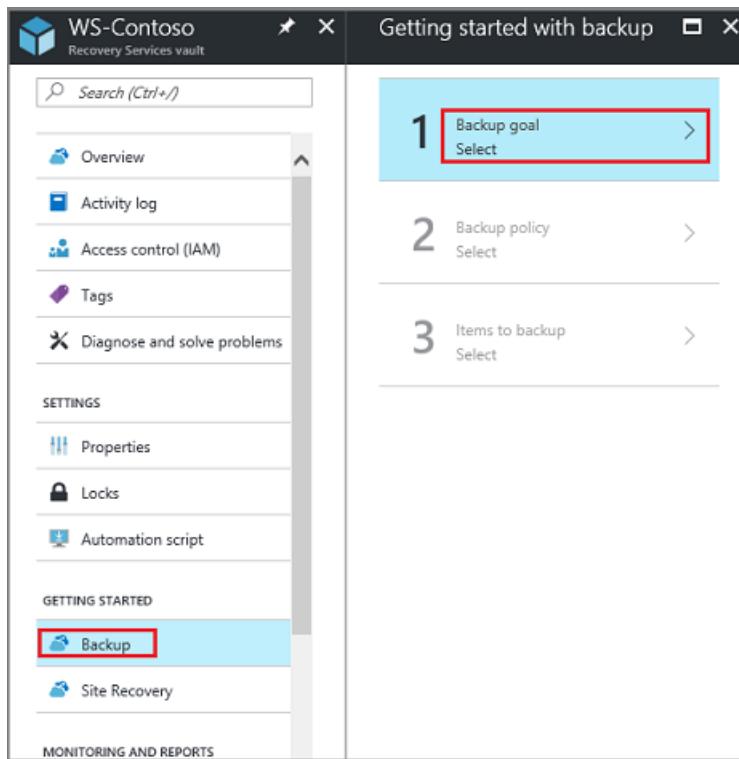


By default, your vault has geo-redundant storage. If you use Azure as a primary backup storage endpoint, continue to use **Geo-redundant**. If you don't use Azure as a primary backup storage endpoint, then choose **Locally-redundant**, which reduces the Azure storage costs. Read more about [geo-redundant](#) and [locally redundant](#) storage options in this [Storage redundancy overview](#).

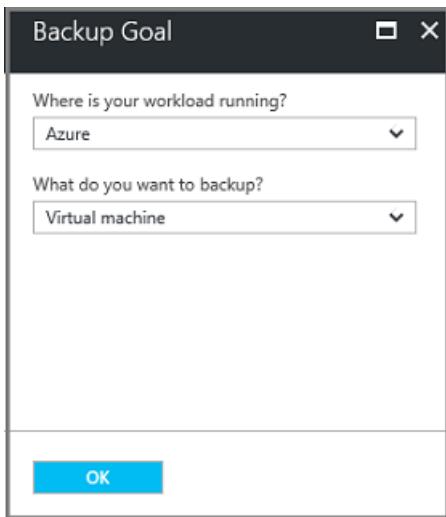
Now that you've created a vault, configure it for backing up Windows System State.

## Configure the vault

1. On the Recovery Services vault blade (for the vault you just created), in the Getting Started section, click **Backup**, then on the **Getting Started with Backup** blade, select **Backup goal**.



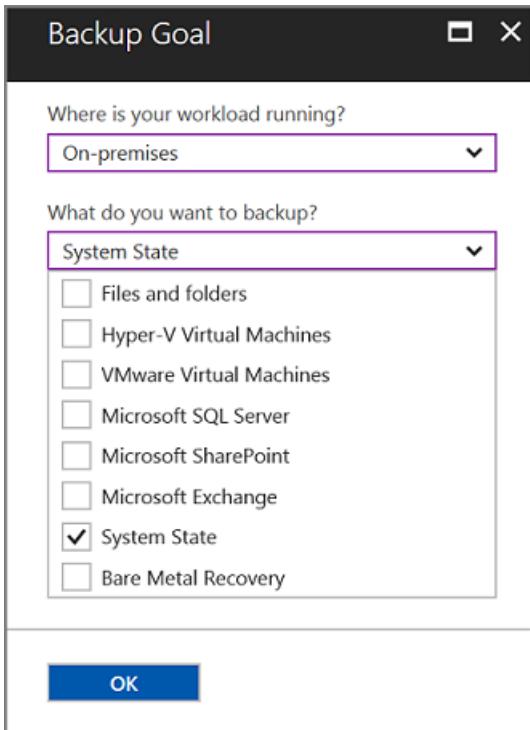
The **Backup Goal** blade opens.



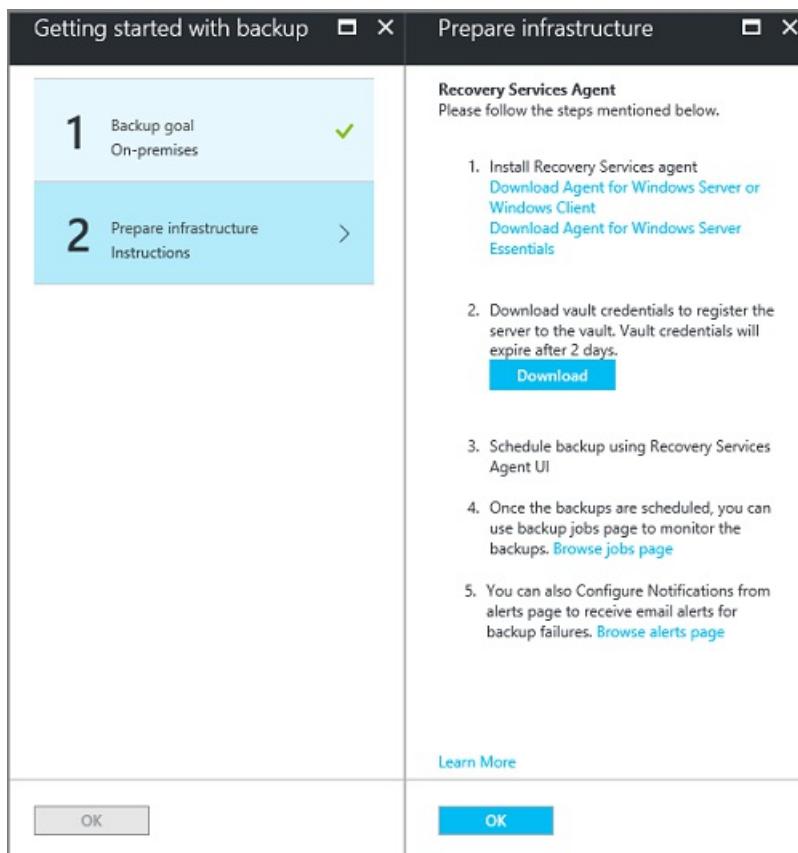
2. From the **Where is your workload running?** drop-down menu, select **On-premises**.

You choose **On-premises** because your Windows Server or Windows computer is a physical machine that is not in Azure.

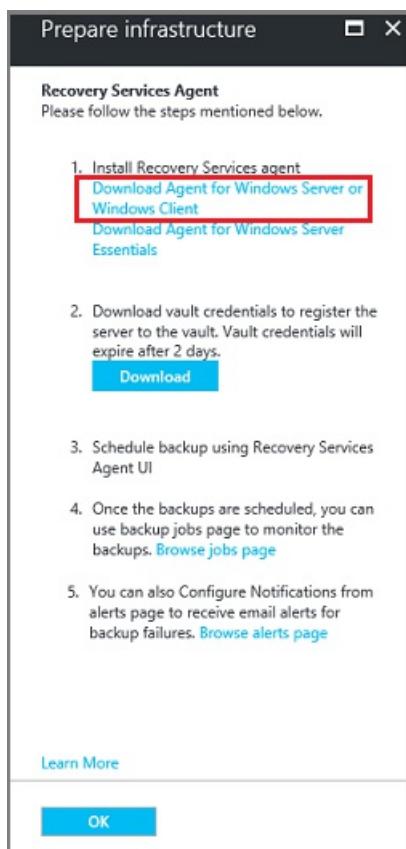
3. From the **What do you want to back up?** menu, select **System State**, and click **OK**.



After clicking OK, a checkmark appears next to **Backup goal**, and the **Prepare infrastructure** blade opens.



4. On the **Prepare infrastructure** blade, click **Download Agent for Windows Server or Windows Client**.



If you are using Windows Server Essential, then choose to download the agent for Windows Server Essential. A pop-up menu prompts you to run or save MARSAgentInstaller.exe.



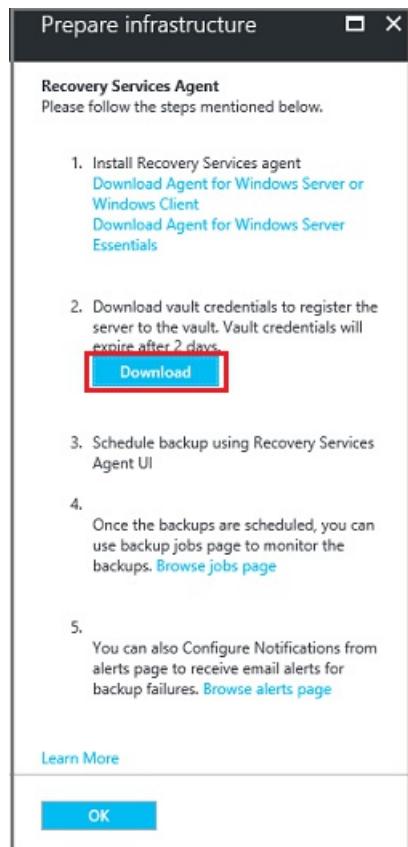
5. In the download pop-up menu, click **Save**.

By default, the **MARSagentinstaller.exe** file is saved to your Downloads folder. When the installer completes, you will see a pop-up asking if you want to run the installer, or open the folder.

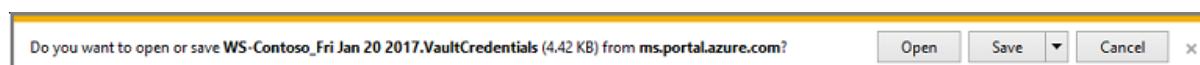


You don't need to install the agent yet. You can install the agent after you have downloaded the vault credentials.

6. On the **Prepare infrastructure** blade, click **Download**.



The vault credentials download to your Downloads folder. After the vault credentials finish downloading, you see 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.



**NOTE**

The vault credentials must be saved only to a location that is local to the Windows Server on which you intend to use the agent.

## Upgrade the MARS agent

Versions of the Microsoft Azure Recovery Service (MARS) agent below 2.0.9083.0 have a dependency on the Azure Access Control service (ACS). The MARS agent is also referred to as the Azure Backup agent. In 2018, Azure [deprecated the Azure Access Control service \(ACS\)](#). Beginning March 19, 2018, all versions of the MARS agent below 2.0.9083.0 will experience backup failures. To avoid or resolve backup failures, [upgrade your MARS agent to the latest version](#). To identify servers that require a MARS agent upgrade, follow the steps in the [Backup blog for upgrading MARS agents](#). The MARS agent is used to back up files and folders, and system state data to Azure.

System Center DPM and Azure Backup Server use the MARS agent to back up data to Azure.

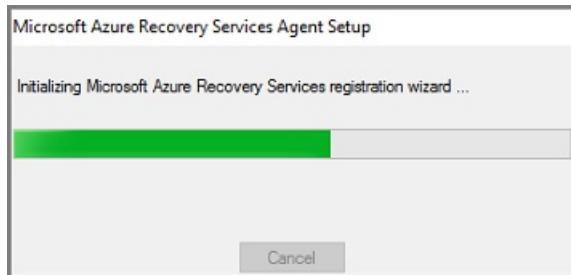
## Install and register the agent

### NOTE

Enabling backup through the Azure portal is not available, yet. Use the Microsoft Azure Recovery Services Agent to back up Windows Server System State.

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.



2. Complete the Microsoft Azure Recovery Services Agent Setup Wizard. To complete the wizard, you need to:

- 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.
- Provide the downloaded vault credentials
- Save the encryption passphrase in a secure location.

### NOTE

If you lose or forget the passphrase, Microsoft cannot help recover the backup data. Save the file in a secure location. It is required to restore a backup.

The agent is now installed and your machine is registered to the vault. You're ready to configure and schedule your backup.

## Back up Windows Server System State

The initial backup includes two tasks:

- Schedule the backup
- Back up System State for the first time

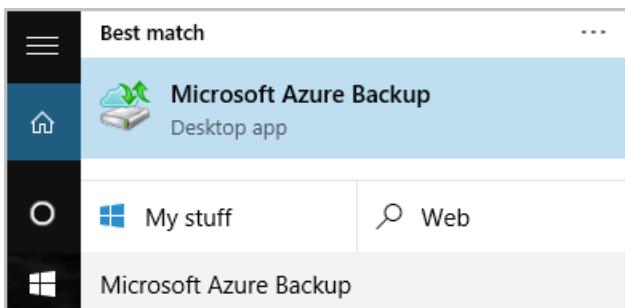
To complete the initial backup, use the Microsoft Azure Recovery Services agent.

### NOTE

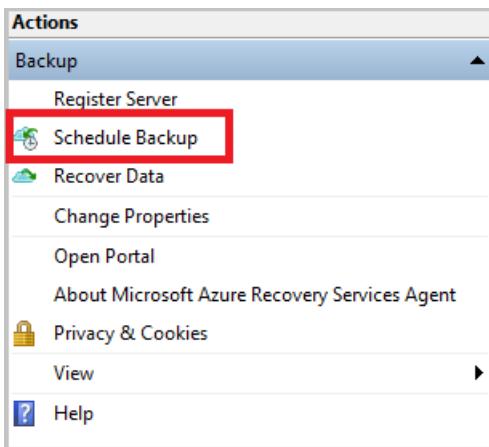
You can back up System State on Windows Server 2008 R2 through Windows Server 2016. System State back up is not supported on client SKUs. System State is not shown as an option for Windows clients, or Windows Server 2008 SP2 machines.

## To schedule the backup job

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



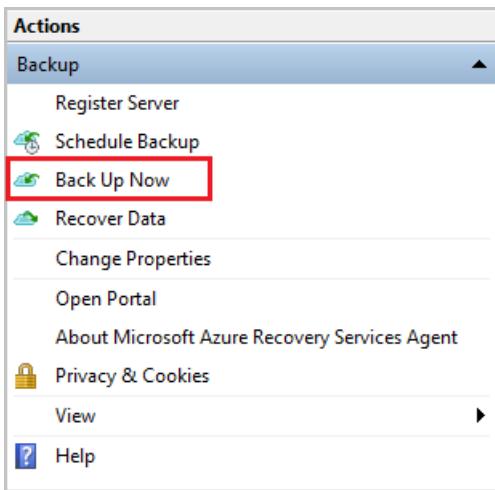
2. In the Recovery Services agent, click **Schedule Backup**.



3. On the Getting started page of the Schedule Backup Wizard, click **Next**.
4. On the Select Items to Backup page, click **Add Items**.
5. Select **System State** and then click **OK**.
6. Click **Next**.
7. Select the required Backup frequency and the retention policy for your System State backups in the subsequent pages.
8. On the Confirmation page, review the information, and then click **Finish**.
9. After the wizard finishes creating the backup schedule, click **Close**.

## To back up Windows Server System State for the first time

1. Make sure there are no pending updates for Windows Server that require a reboot.
2. In the Recovery Services agent, click **Back Up Now** to complete the initial seeding over the network.



3. Select **System State** on the **Select Backup Item** screen that appears and click **Next**.
4. On the Confirmation page, review the settings that the Back Up Now Wizard will use to back up the machine. Then click **Back Up**.
5. Click **Close** to close the wizard. If you close the wizard before the backup process finishes, the wizard continues to run in the background.

#### NOTE

The MARS Agent triggers SFC /verifyonly as part of the prechecks before every system state backup. This is to ensure that files backed up as part of System State have the correct versions corresponding to the Windows version. Learn more about System File Checker (SFC) in [this article](#).

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

The screenshot shows the Microsoft Azure Backup interface. The 'Jobs' tab is selected. A message states: 'Microsoft Azure Backup supports scheduled backups of files and folders to an online location'. Below this, a table lists a single job entry:

| Time              | Message | Description    |
|-------------------|---------|----------------|
| 3/25/2015 8:26 PM | Backup  | Job completed. |

## Questions?

If you have questions, or if there is any feature that you would like to see included, [send us feedback](#).

## Next steps

- Get more details about [backing up Windows machines](#).
- Now that you've backed up your Windows Server System State, you can [manage your vaults and servers](#).
- If you need to restore a backup, use this article to [restore files to a Windows machine](#).

# Restore files to Windows by using the Azure Resource Manager deployment model

12/16/2019 • 6 minutes to read • [Edit Online](#)

This article explains how to restore data from a backup vault. To restore data, you use the Recover Data wizard in the Microsoft Azure Recovery Services (MARS) Agent. You can:

- Restore data to the same machine from which the backups were taken.
- Restore data to an alternate machine.

Use the Instant Restore feature to mount a writeable recovery point snapshot as a recovery volume. You can then explore the recovery volume and copy files to a local computer, thereby selectively restoring files.

## NOTE

The [January 2017 Azure Backup update](#) is required if you want to use Instant Restore to restore data. Also, the backup data must be protected in vaults in locales listed in the support article. Consult the [January 2017 Azure Backup update](#) for the latest list of locales that support Instant Restore.

Use Instant Restore with Recovery Services vaults in the Azure portal. If you stored data in Backup vaults, they have been converted to Recovery Services vaults. If you want to use Instant Restore, download the MARS update, and follow the procedures that mention Instant Restore.

## NOTE

Azure has two different deployment models you can use to create and work with resources: [Azure Resource Manager](#) and [classic](#). This article covers the use of the Resource Manager deployment model. We recommend the Resource Manager deployment model for new deployments instead of the classic deployment model.

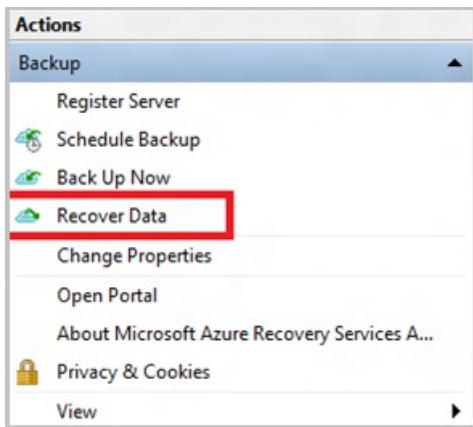
## Use Instant Restore to recover data to the same machine

If you accidentally deleted a file and want to restore it to the same machine (from which the backup is taken), the following steps will help you recover the data.

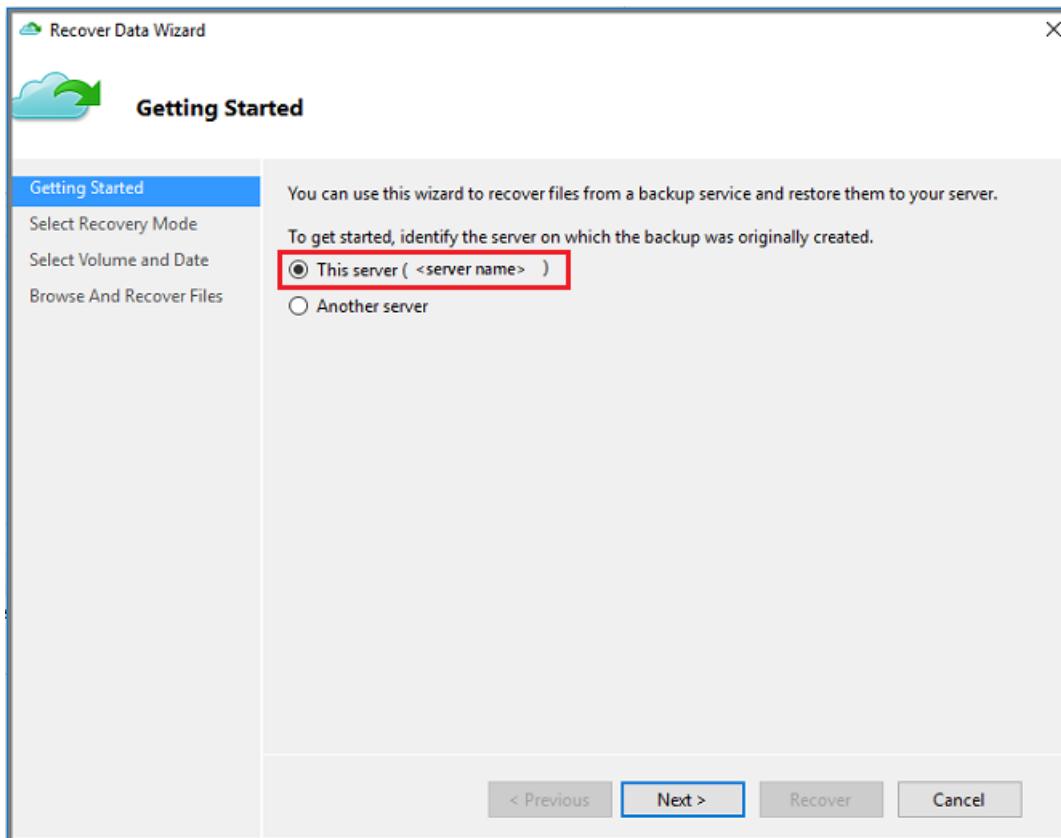
1. Open the **Microsoft Azure Backup** snap-in. If you don't know where the snap-in was installed, search the computer or server for **Microsoft Azure Backup**.

The desktop app should appear in the search results.

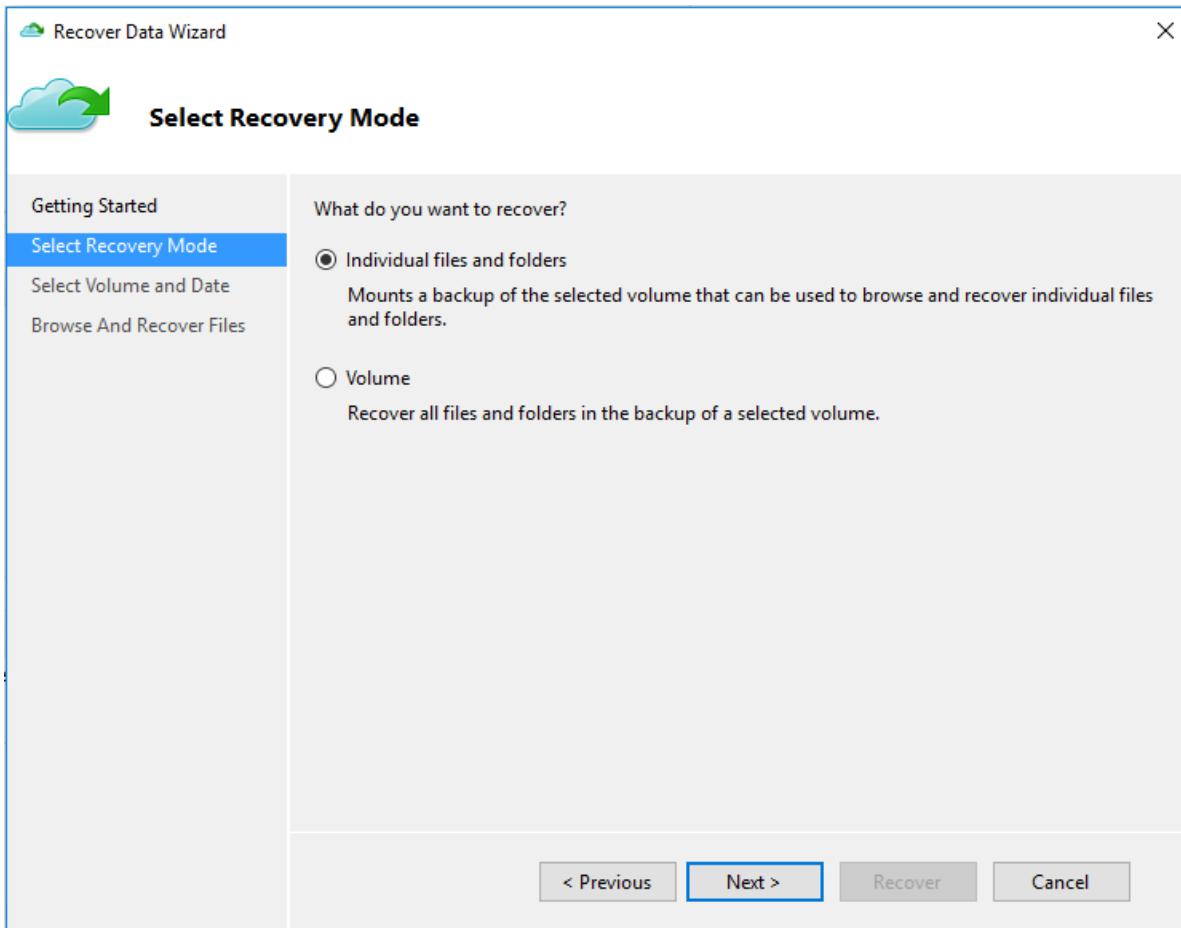
2. Select **Recover Data** to start the wizard.



3. On the **Getting Started** page, to restore the data to the same server or computer, select **This server ( <server name> )** > **Next**.



4. On the **Select Recovery Mode** page, choose **Individual files and folders** > **Next**.



#### IMPORTANT

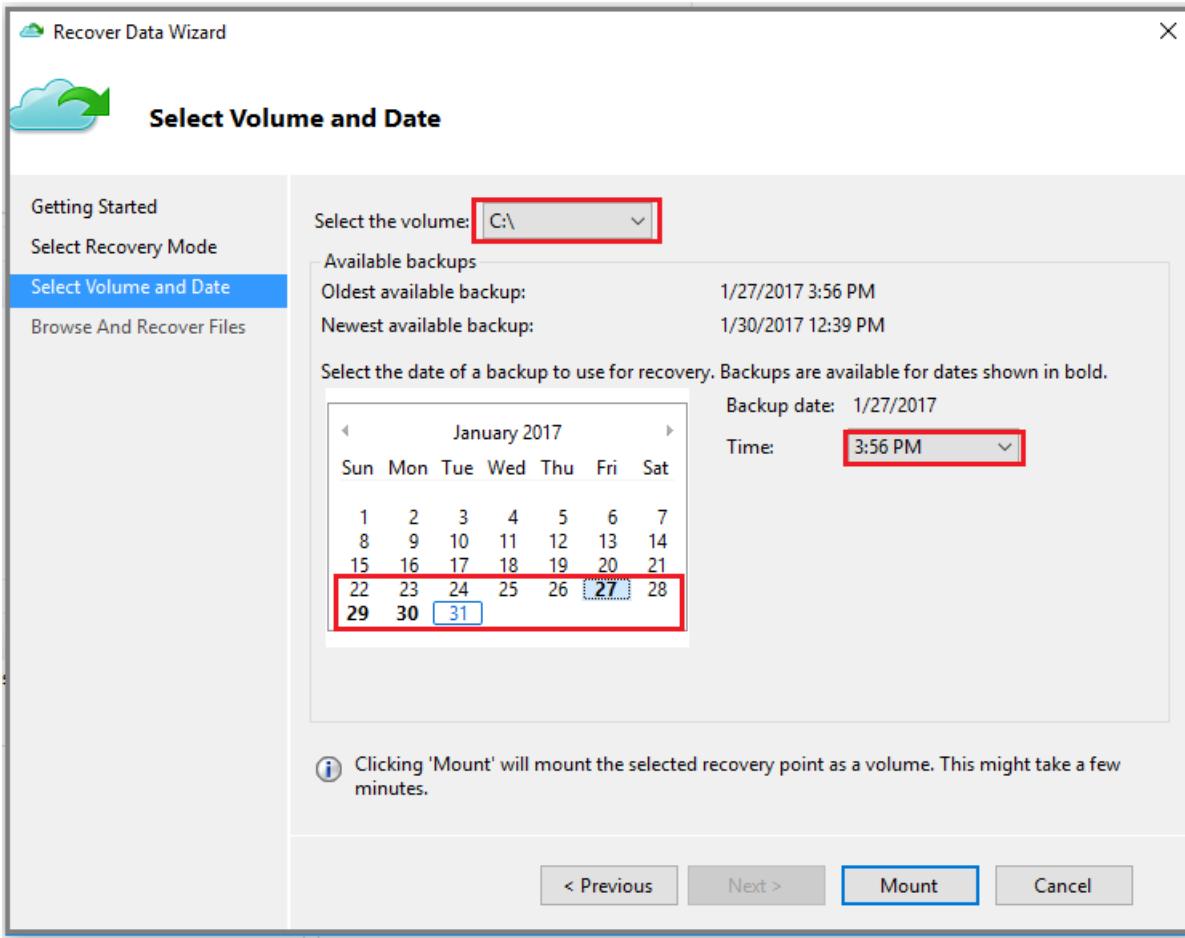
The option to restore individual files and folders requires .NET Framework 4.5.2 or later. If you do not see the **Individual files and folders** option, you must upgrade .NET Framework to version 4.5.2 or later, and try again.

#### TIP

The **Individual files and folders** option allows for quick access to the recovery point data. It is suitable for recovering individual files, with sizes totalling not more than 80 GB, and offers transfer or copy speeds up to 6 MBps during recovery. The **Volume** option recovers all backed up data in a specified volume. This option provides faster transfer speeds (up to 60 MBps), which is ideal for recovering large-sized data or entire volumes.

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

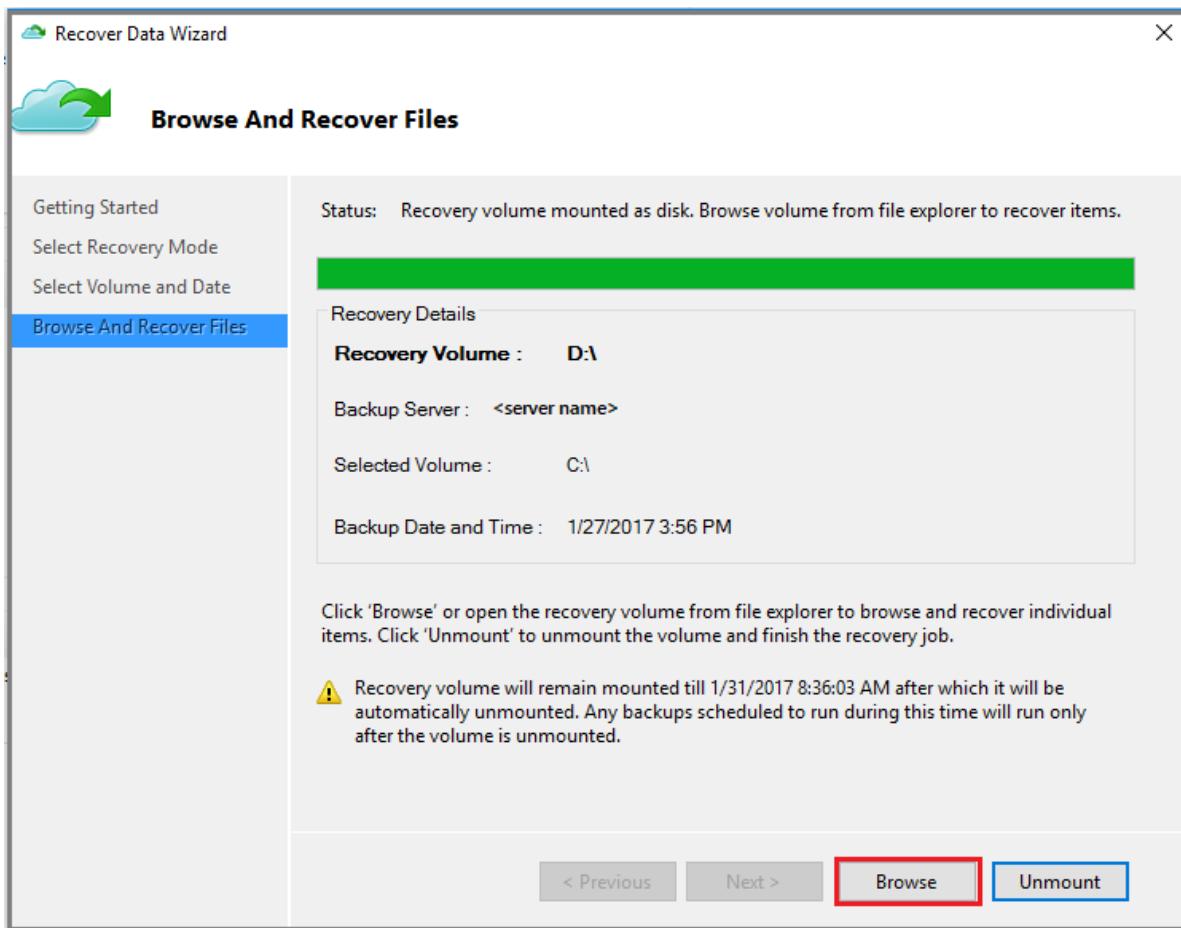
On the calendar, select a recovery point. Dates in **bold** indicate the availability of at least one recovery point. If multiple recovery points are available within a single date, choose the specific recovery point from the **Time** drop-down menu.



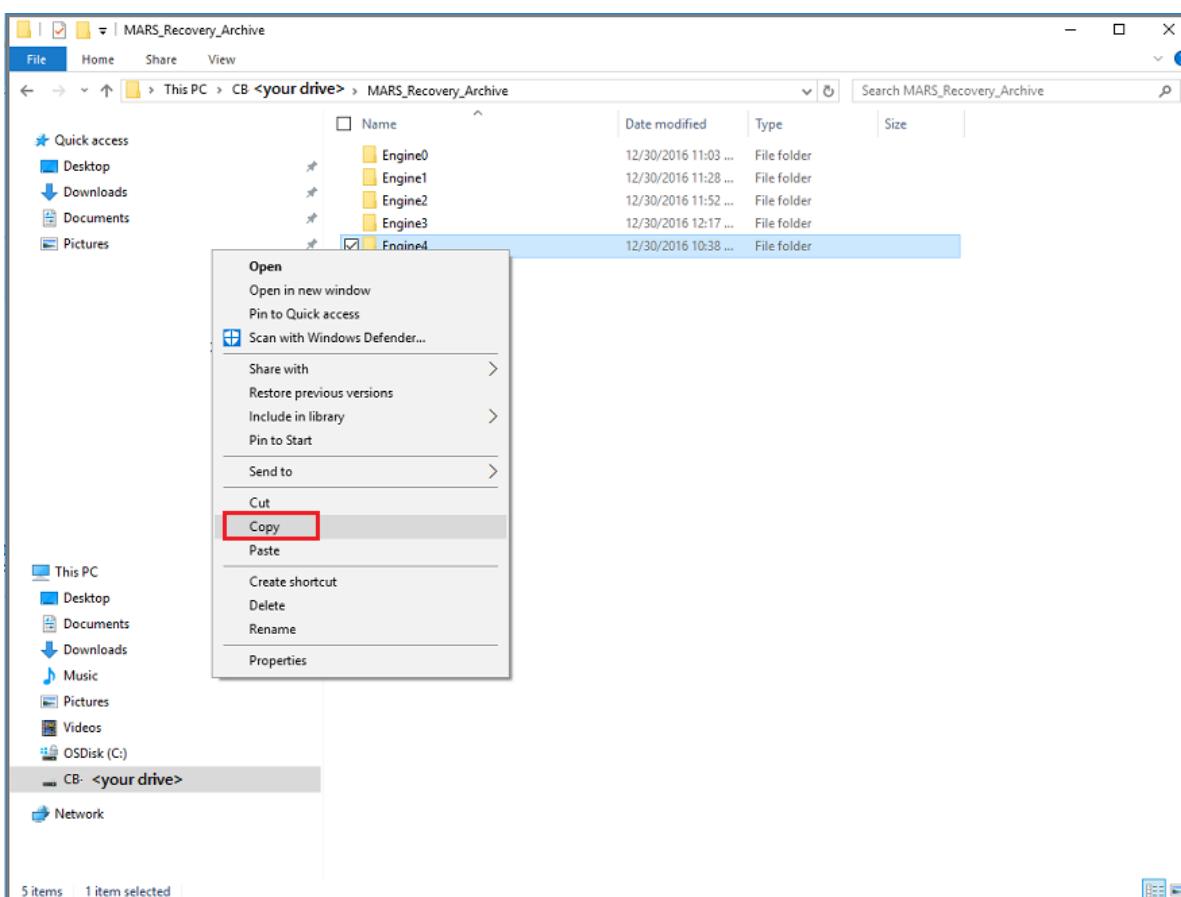
6. After choosing the recovery point to restore, select **Mount**.

Azure Backup mounts the local recovery point, and uses it as a recovery volume.

7. On the **Browse and Recover Files** page, select **Browse** to open Windows Explorer, and find the files and folders you want.

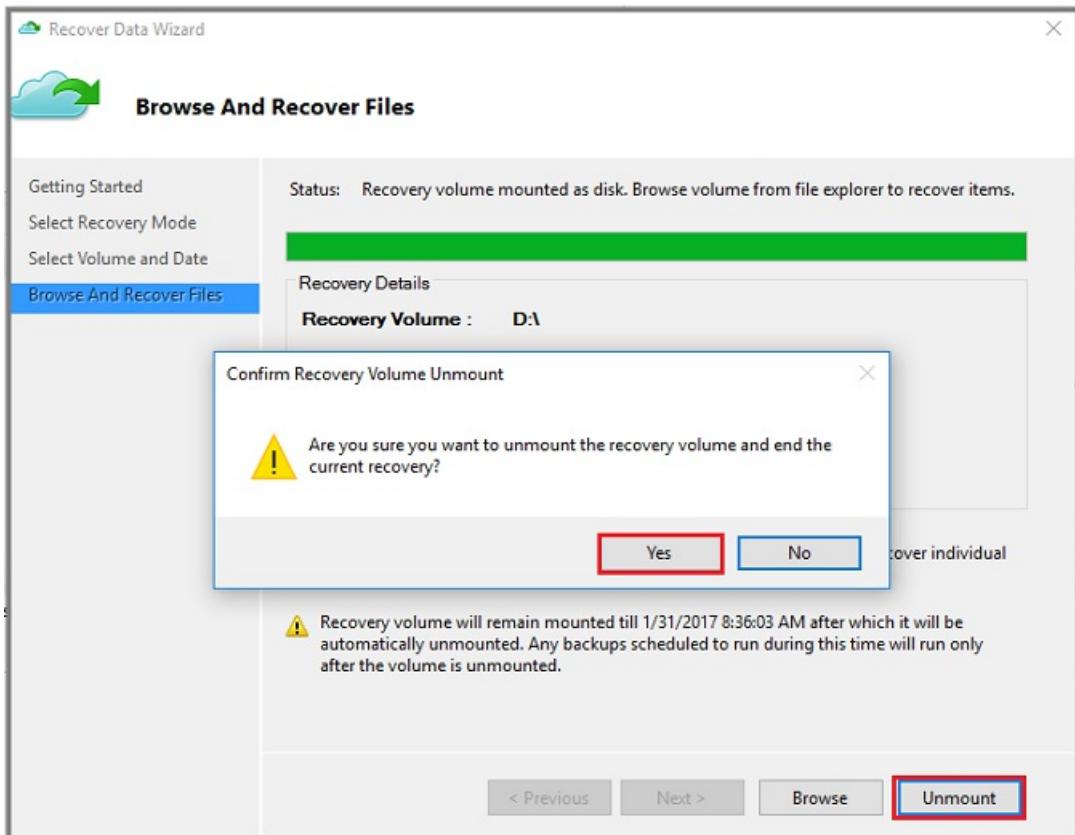


8. In Windows Explorer, copy the files and folders you want to restore, and paste them to any location local to the server or computer. You can open or stream the files directly from the recovery volume, and verify that you are recovering the correct versions.



9. When you are finished, on the **Browse and Recover Files** page, select **Unmount**. Then select **Yes** to

confirm that you want to unmount the volume.



#### IMPORTANT

If you do not select **Unmount**, the recovery volume will remain mounted for 6 hours from the time when it was mounted. However, the mount time is extended up to a maximum of 24 hours in case of an ongoing file-copy. No backup operations will run while the volume is mounted. Any backup operation scheduled to run during the time when the volume is mounted will run after the recovery volume is unmounted.

## Use Instant Restore to restore data to an alternate machine

If your entire server is lost, you can still recover data from Azure Backup to a different machine. The following steps illustrate the workflow.

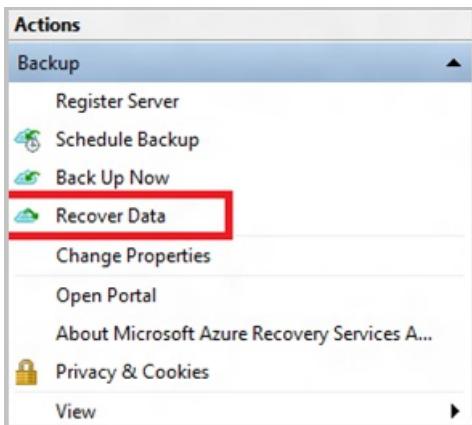
These steps include the following terminology:

- *Source machine* – The original machine from which the backup was taken, and which is currently unavailable.
- *Target machine* – The machine to which the data is being recovered.
- *Sample vault* – The Recovery Services vault to which the source machine and target machine are registered.

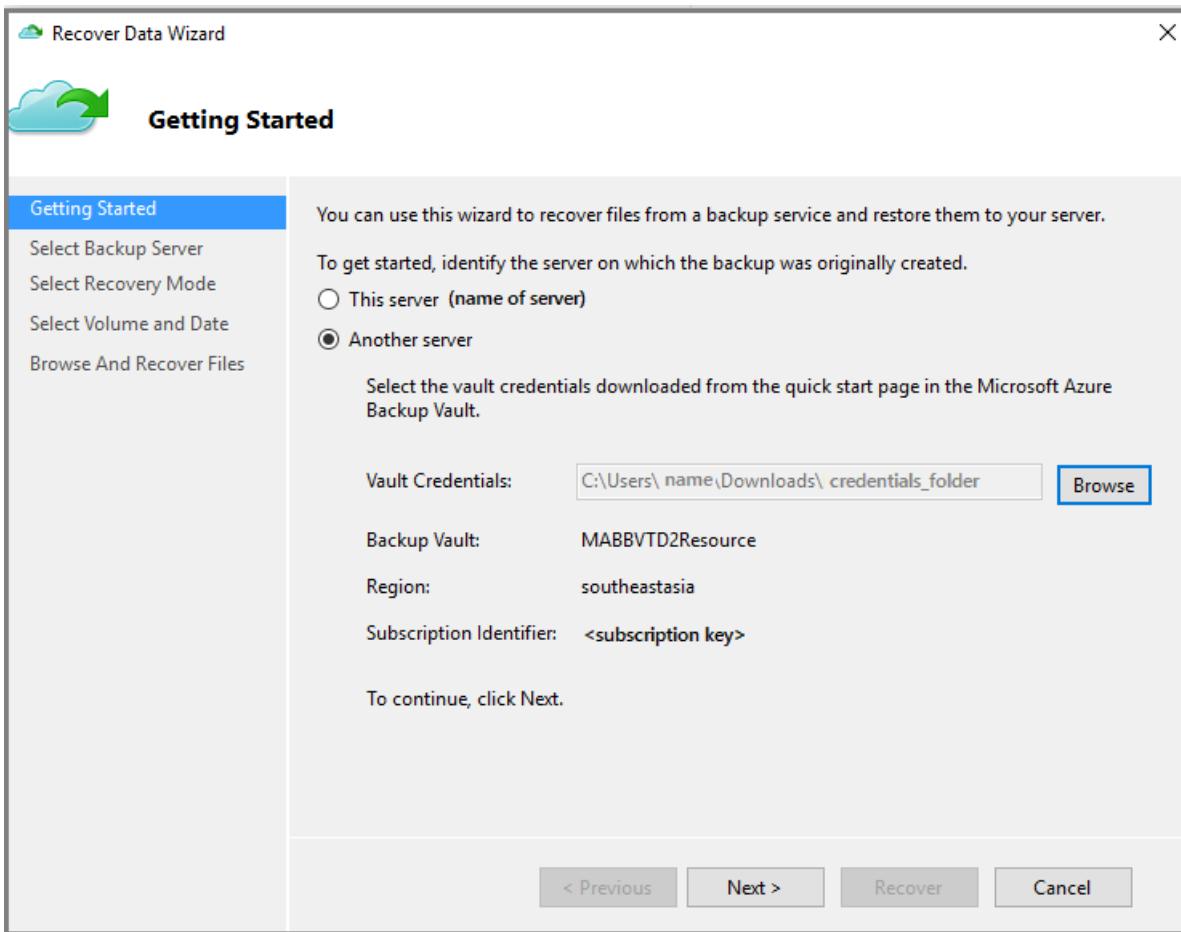
#### NOTE

Backups can't be restored to a target machine that is running an earlier version of the operating system. For example, a backup taken from a Windows 7 computer can be restored on a Windows 7 (or later) computer. A backup taken from a Windows 8 computer can't be restored to a Windows 7 computer.

1. Open the **Microsoft Azure Backup** snap-in on the target machine.
2. Ensure that the target machine and the source machine are registered to the same Recovery Services vault.
3. Select **Recover Data** to open the **Recover Data Wizard**.



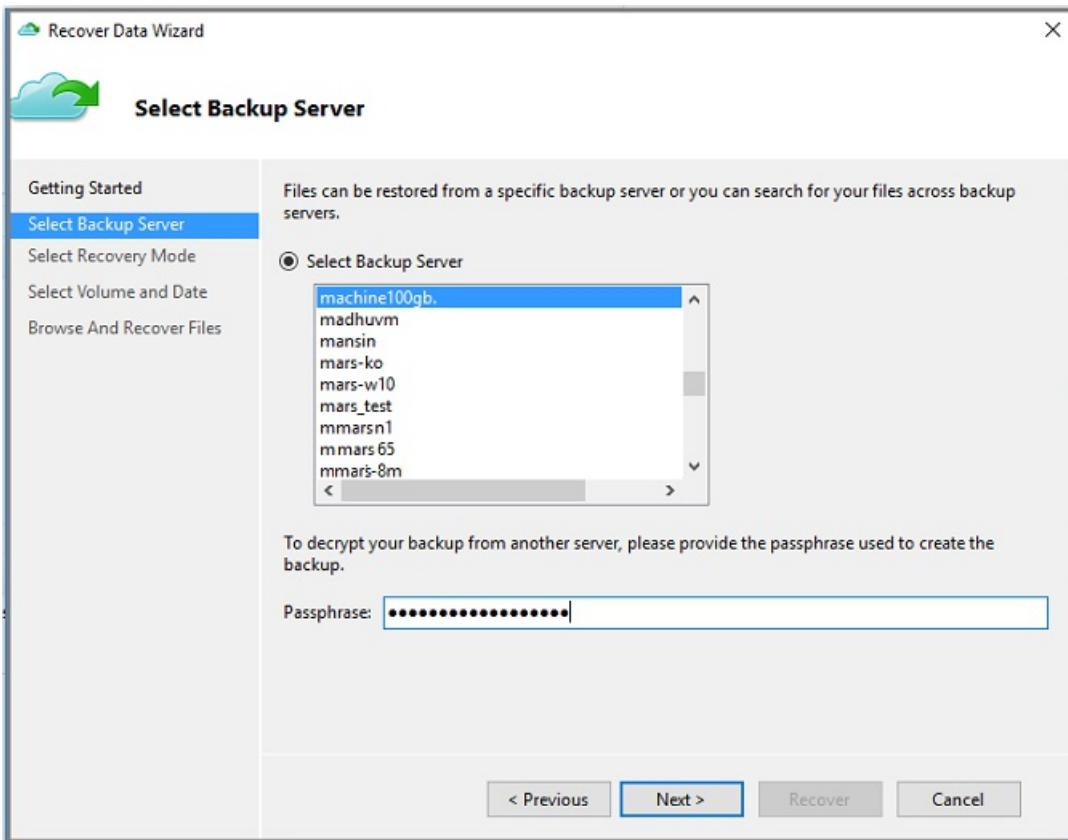
4. On the **Getting Started** page, select **Another server**.



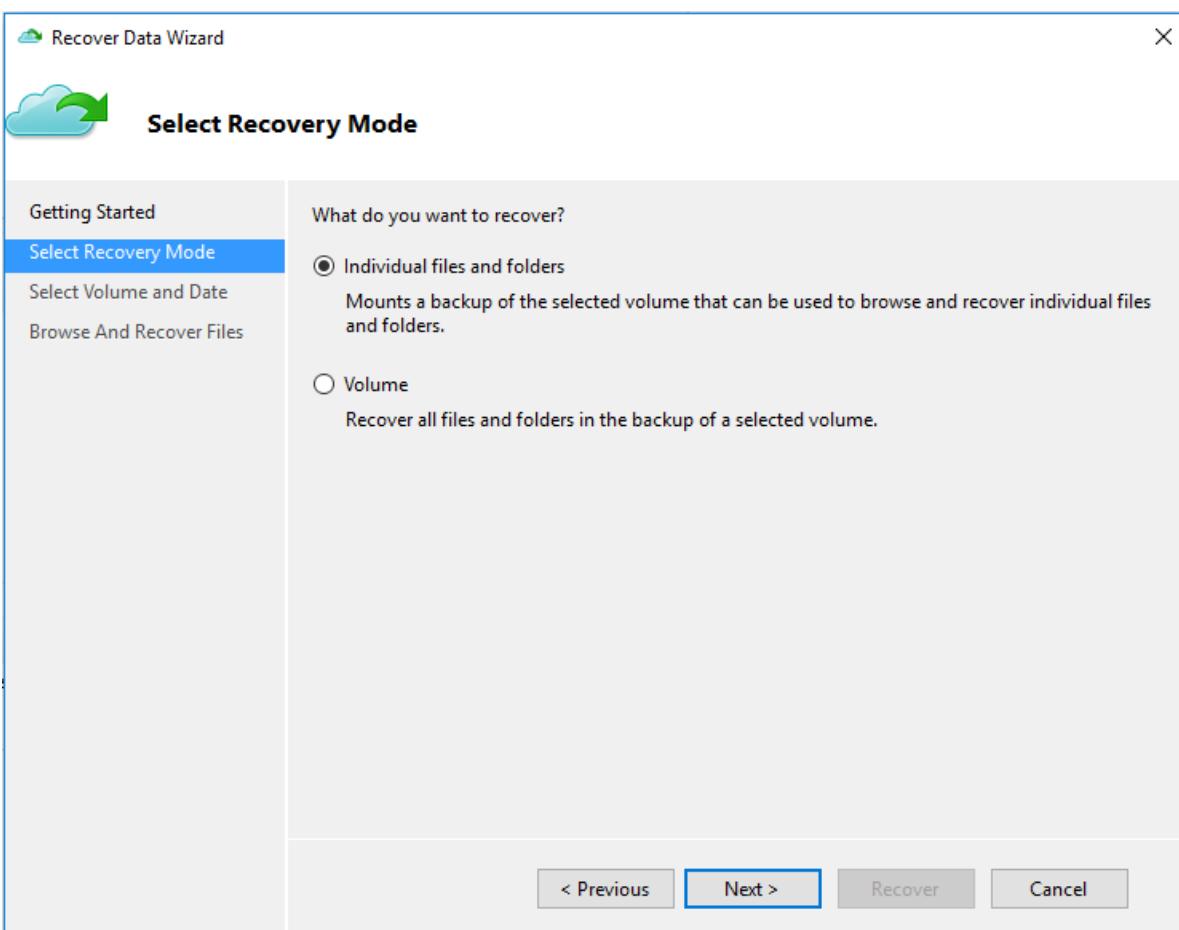
5. Provide the vault credential file that corresponds to the sample vault, and select **Next**.

If the vault credential file is invalid (or expired), download a new vault credential file from the sample vault in the Azure portal. After you provide a valid vault credential, the name of the corresponding backup vault appears.

6. On the **Select Backup Server** page, select the source machine from the list of displayed machines, and provide the passphrase. Then select **Next**.



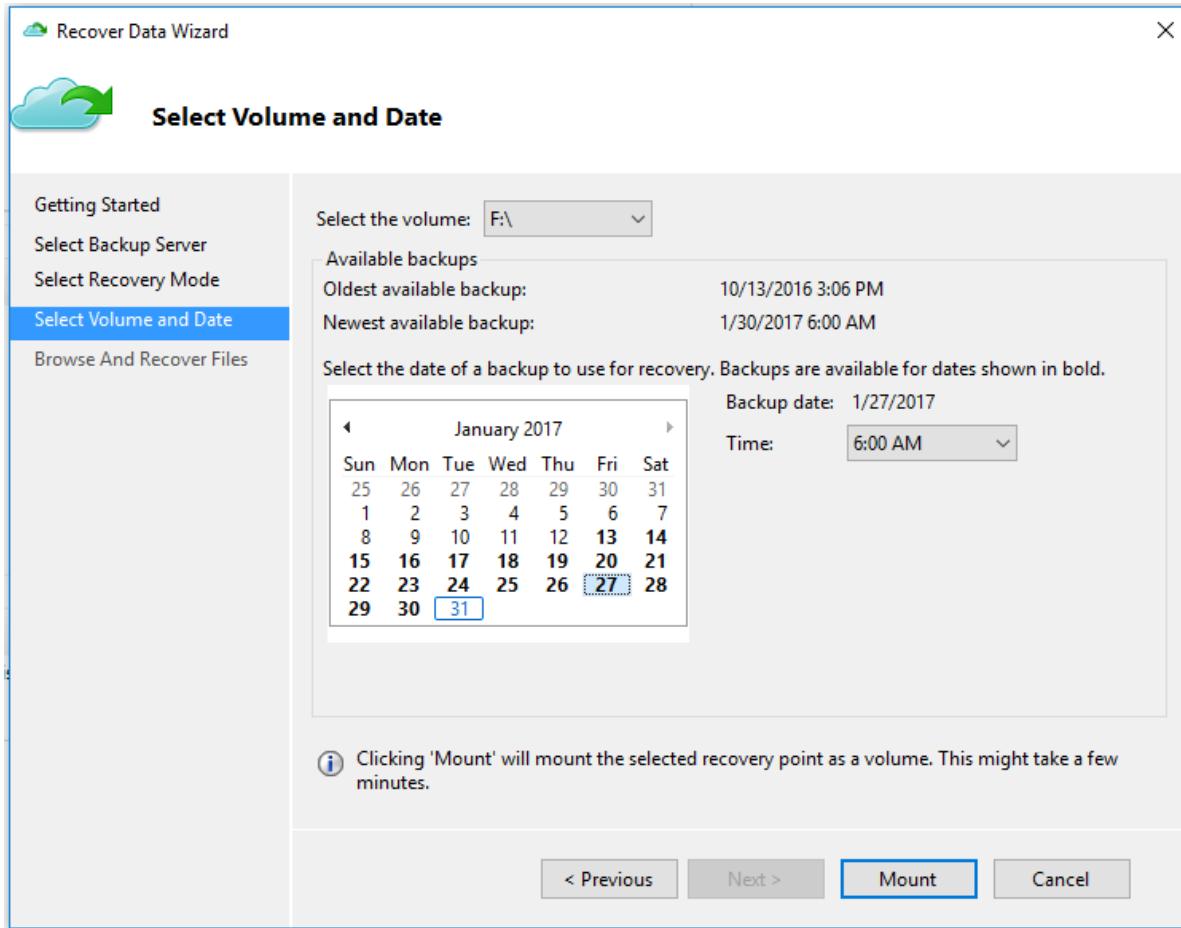
7. On the **Select Recovery Mode** page, select **Individual files and folders** > **Next**.



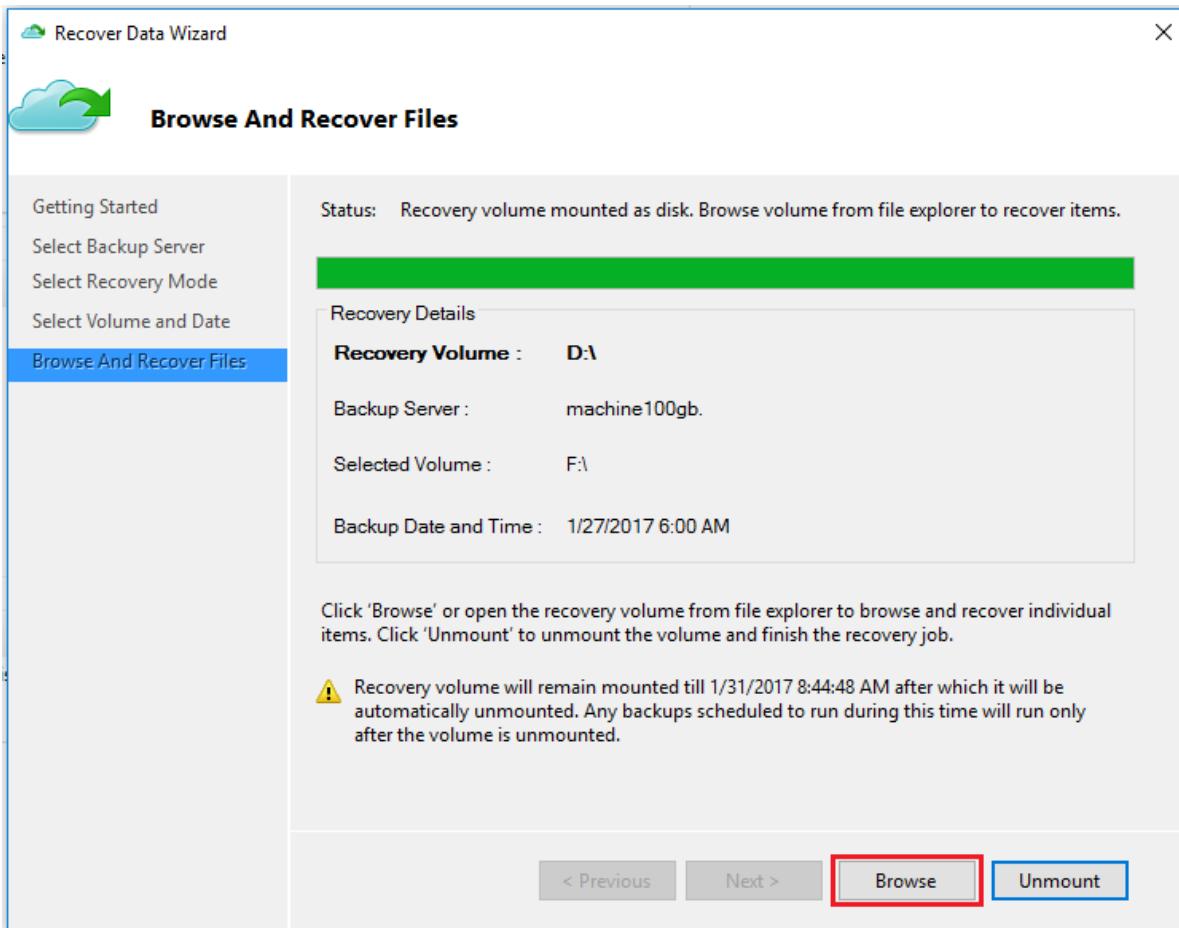
8. On the **Select Volume and Date** page, select the volume that contains the files and folders you want to restore.

On the calendar, select a recovery point. Dates in **bold** indicate the availability of at least one recovery point. If multiple recovery points are available within a single date, choose the specific recovery point from

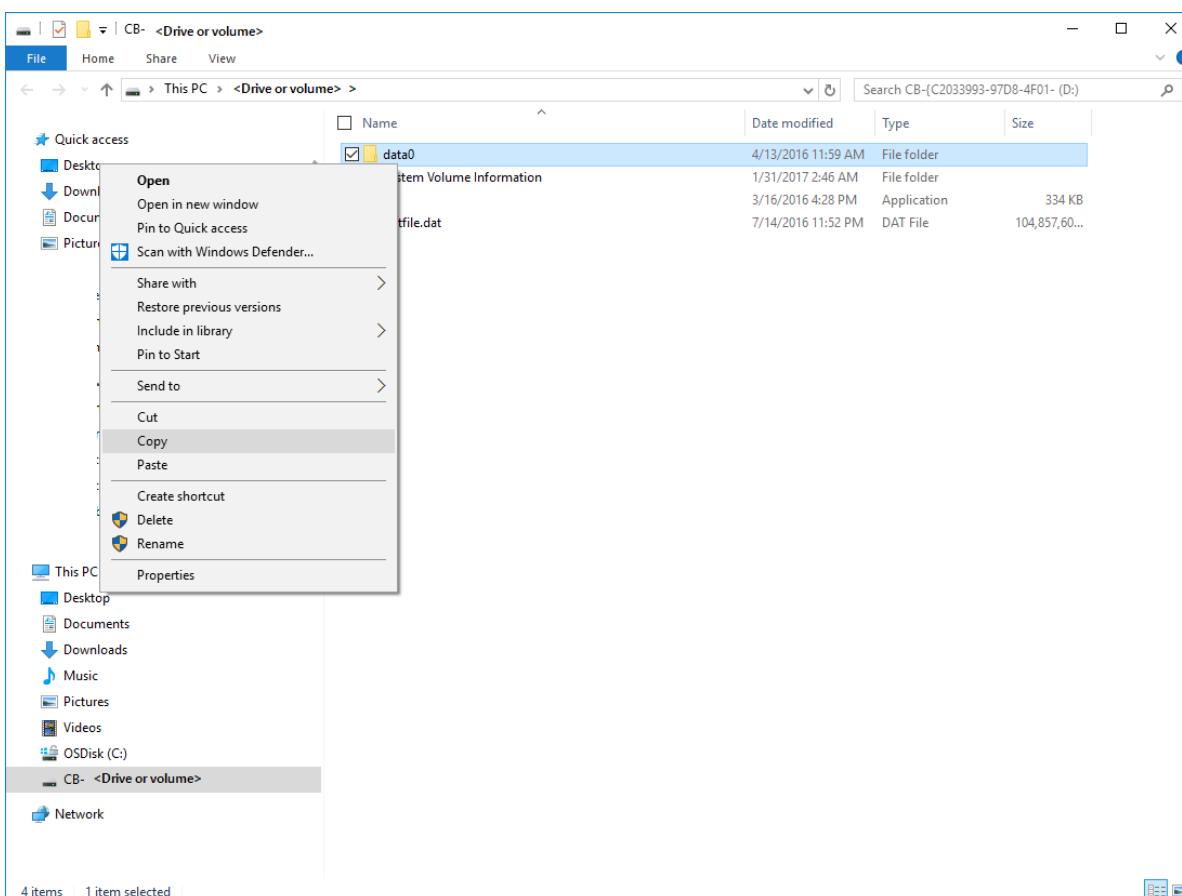
the **Time** drop-down menu.



9. Select **Mount** to locally mount the recovery point as a recovery volume on your target machine.
10. On the **Browse And Recover Files** page, select **Browse** to open Windows Explorer, and find the files and folders you want.

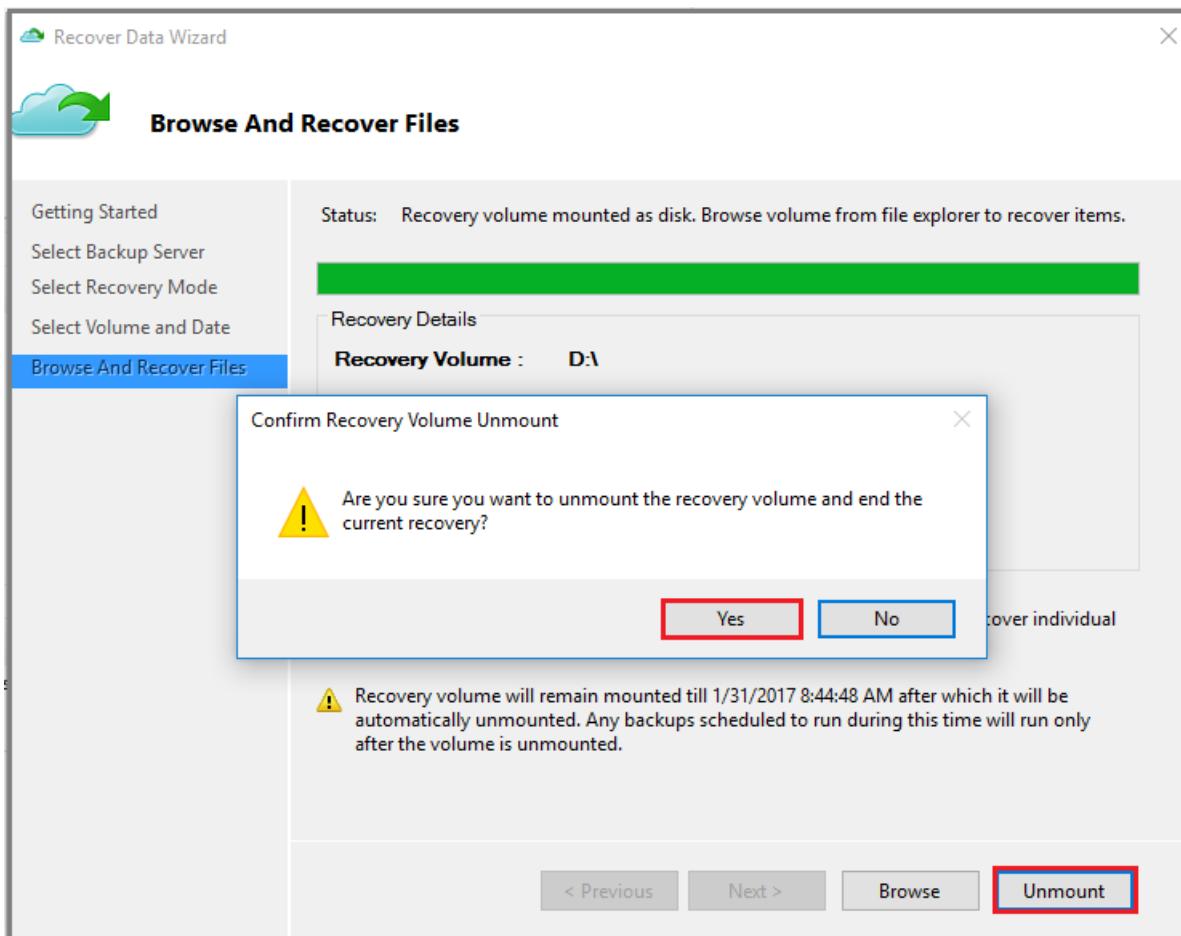


11. In Windows Explorer, copy the files and folders from the recovery volume, and paste them to your target machine location. You can open or stream the files directly from the recovery volume, and verify that the correct versions are recovered.



12. When you are finished, on the **Browse and Recover Files** page, select **Unmount**. Then select **Yes** to

confirm that you want to unmount the volume.



#### IMPORTANT

If you do not select **Unmount**, the recovery volume will remain mounted for 6 hours from the time when it was mounted. However, the mount time is extended up to a maximum of 24 hours in case of an ongoing file-copy. No backup operations will run while the volume is mounted. Any backup operation scheduled to run during the time when the volume is mounted will run after the recovery volume is unmounted.

## Next steps

Now that you've recovered your files and folders, you can [manage your backups](#).

# Restore System State to Windows Server

2/25/2020 • 7 minutes to read • [Edit Online](#)

This article explains how to restore Windows Server System State backups from an Azure Recovery Services vault.

To restore System State, you must have a System State backup (created using the instructions in [Back up System State](#), and make sure you have installed the [latest version of the Microsoft Azure Recovery Services \(MARS\) agent](#). Recovering Windows Server System State data from an Azure Recovery Services vault is a two-step process:

1. Restore System State as files from Azure Backup. When restoring System State as files from Azure Backup, you can either:
  - Restore System State to the same server where the backups were taken, or
  - Restore System State file to an alternate server.
2. Apply the restored System State files to a Windows Server.

## Recover System State files to the same server

The following steps explain how to roll back your Windows Server configuration to a previous state. Rolling your server configuration back to a known, stable state, can be extremely valuable. The following steps restore the server's System State from a Recovery Services vault.

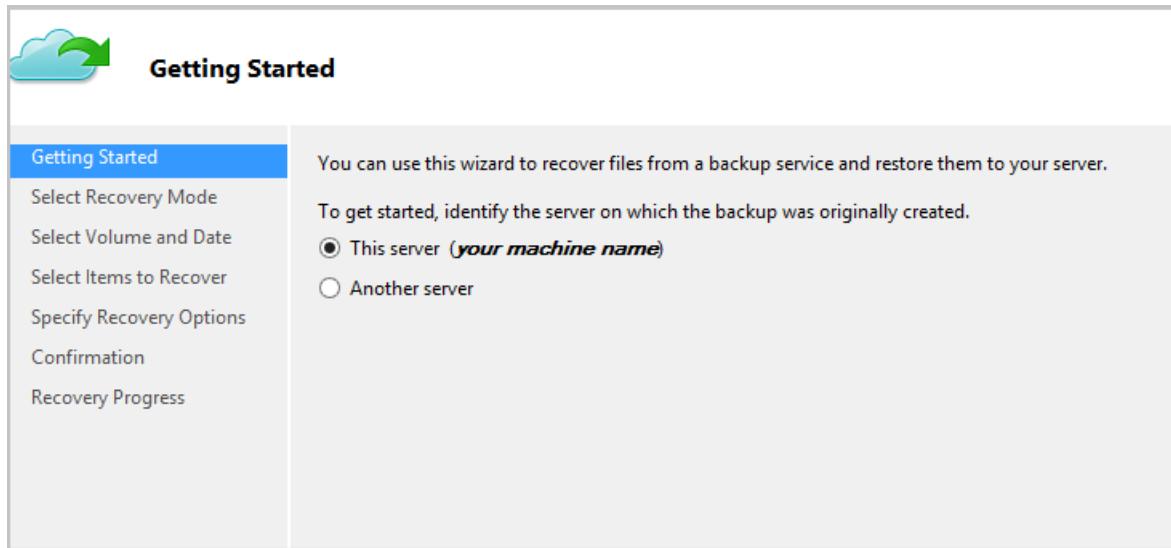
1. Open the **Microsoft Azure Backup** snap-in. If you don't know where the snap-in was installed, search the computer or server for **Microsoft Azure Backup**.

The desktop app should appear in the search results.

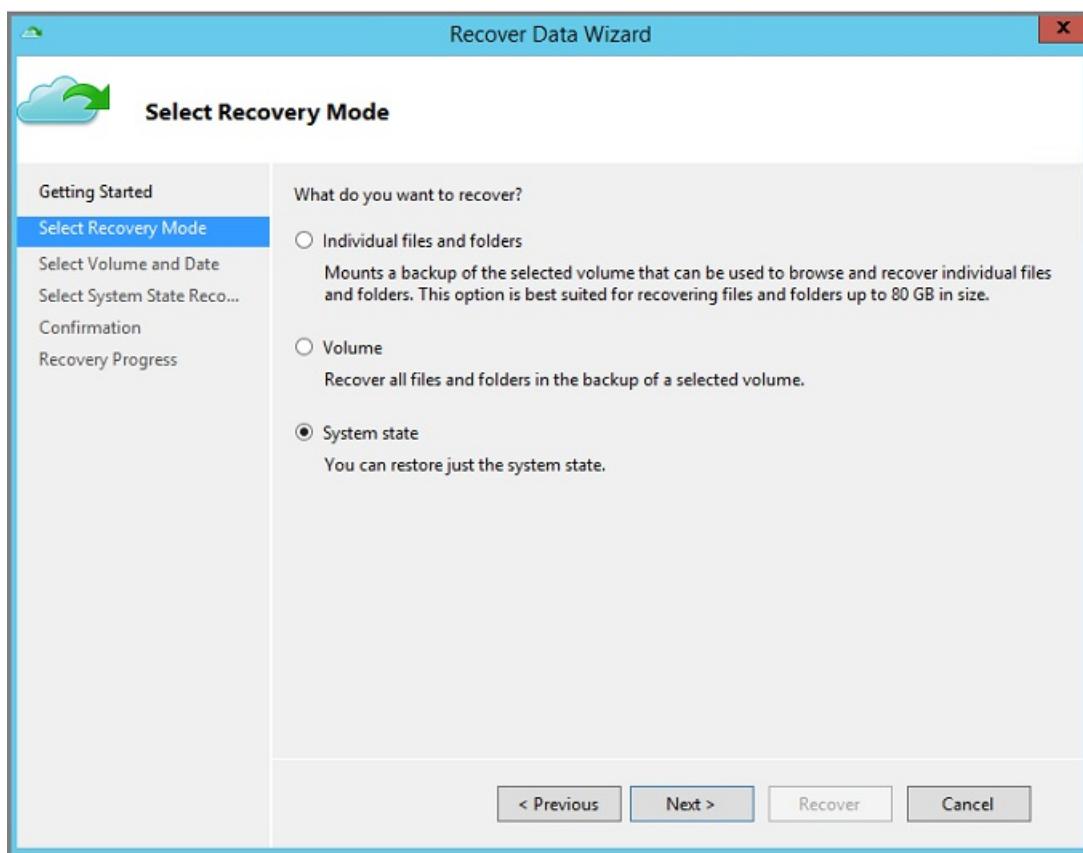
2. Click **Recover Data** to start the wizard.



3. On the **Getting Started** pane, to restore the data to the same server or computer, select **This server (<server name>)** and click **Next**.

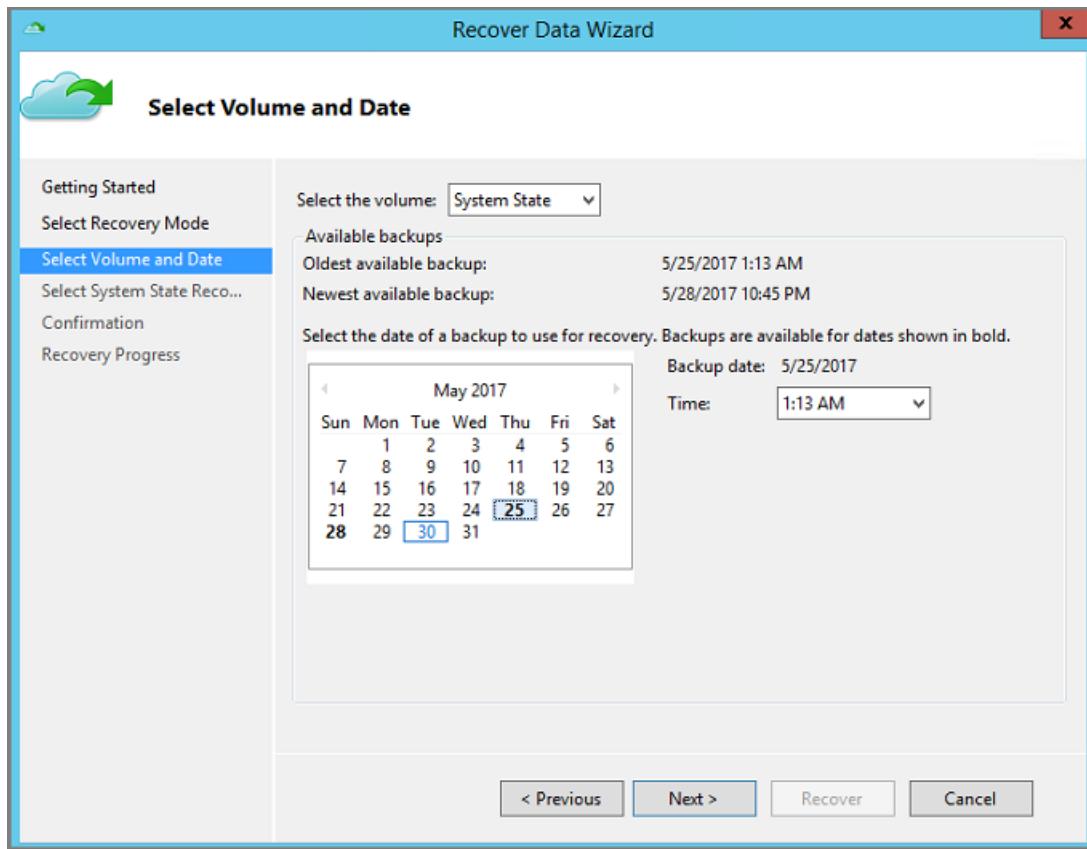


4. On the **Select Recovery Mode** pane, choose **System State** and then click **Next**.



5. On the calendar in **Select Volume and Date** pane, select a recovery point.

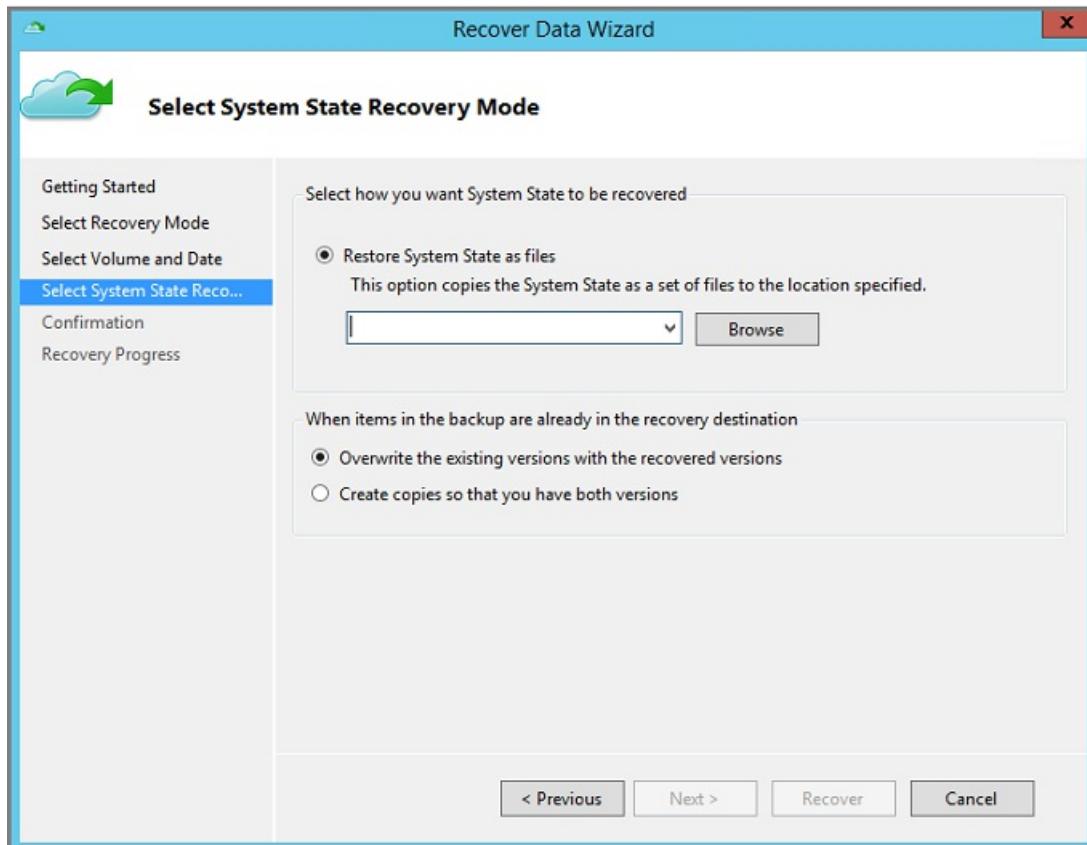
You can restore from any recovery point in time. Dates in **bold** indicate the availability of at least one recovery point. Once you select a date, if multiple recovery points are available, choose the specific recovery point from the **Time** drop-down menu.



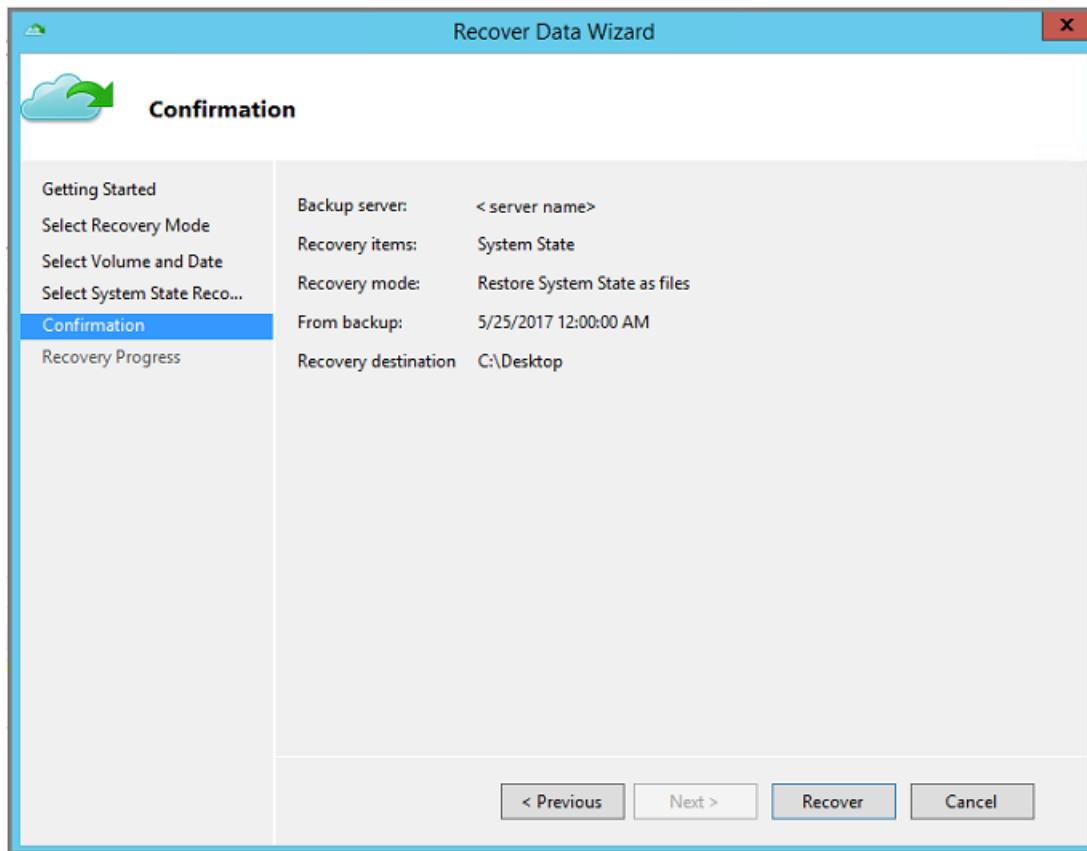
6. Once you have chosen the recovery point to restore, click **Next**.

Azure Backup mounts the local recovery point, and uses it as a recovery volume.

7. On the next pane, specify the destination for the recovered System State files and click **Browse** to open Windows Explorer and find the files and folders you want. The option, **Create copies so that you have both versions**, creates copies of individual files in an existing System State file archive instead of creating the copy of the entire System State archive.



8. Verify the details of recovery on the **Confirmation** pane and click **Recover**.



9. Copy the *WindowsImageBackup* directory in the Recovery destination to a non-critical volume of the server.  
Usually, the Windows OS volume is the critical volume.
10. Once the recovery is successful, follow the steps in the section, [Apply restored System State files to the Windows Server](#), to complete the System State recovery process.

## Recover System State files to an alternate server

If your Windows Server is corrupted or inaccessible, and you want to restore it to a stable state by recovering the Windows Server System State, you can restore the corrupted server's System State from another server. Use the following steps to the restore System State on a separate server.

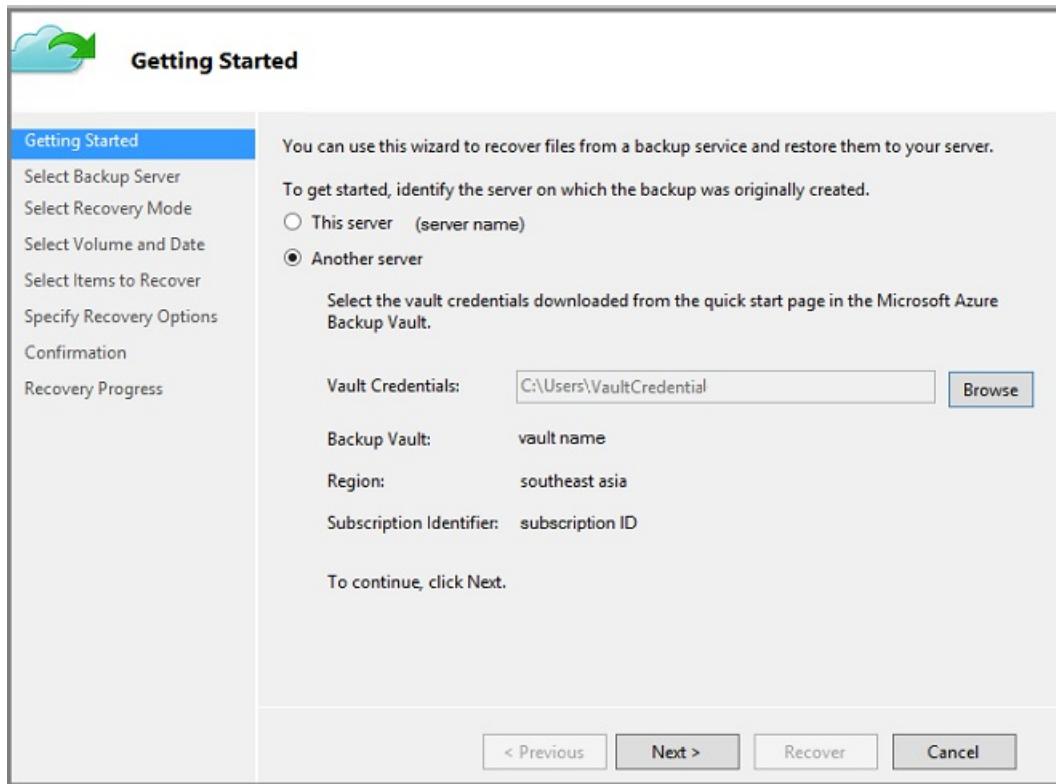
The terminology used in these steps includes:

- *Source machine* – The original machine from which the backup was taken and which is currently unavailable.
- *Target machine* – The machine to which the data is being recovered.
- *Sample vault* – The Recovery Services vault to which the *Source machine* and *Target machine* are registered.

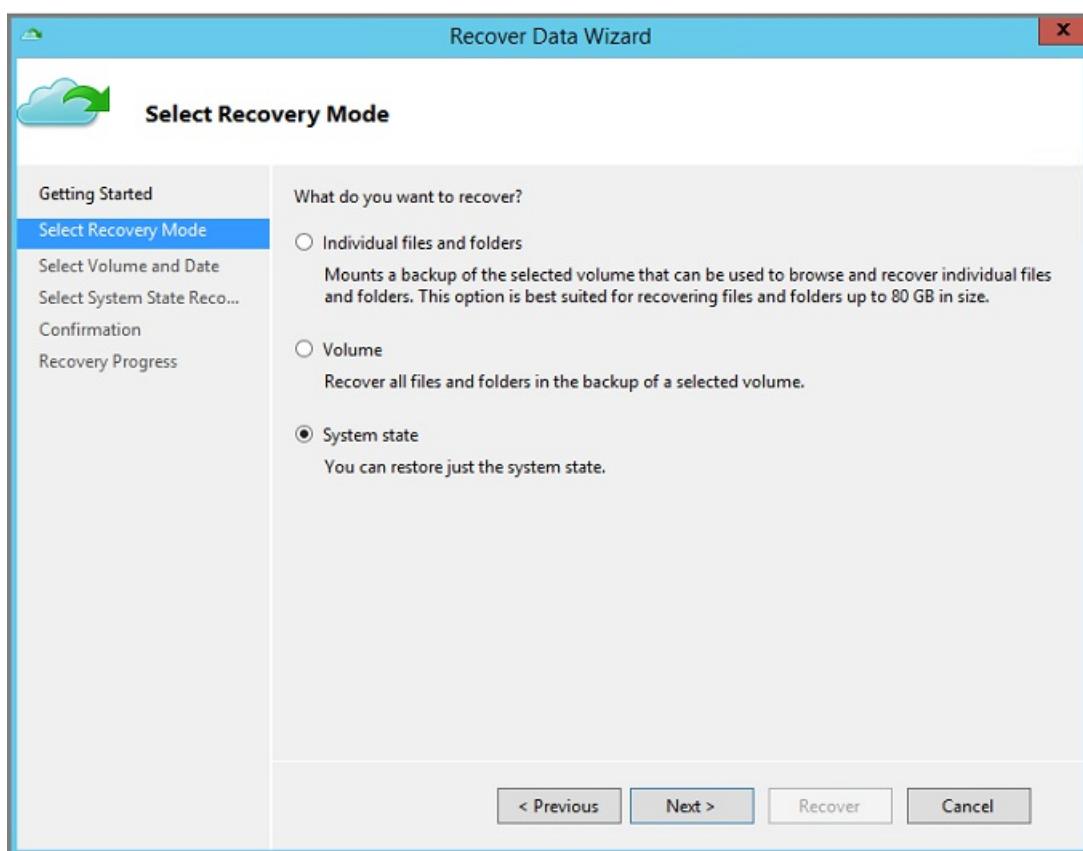
### NOTE

Backups taken from one machine cannot be restored to a machine running an earlier version of the operating system. For example, backups taken from a Windows Server 2016 machine can't be restored to Windows Server 2012 R2. However, the inverse is possible. You can use backups from Windows Server 2012 R2 to restore Windows Server 2016.

1. Open the **Microsoft Azure Backup** snap-in on the *Target machine*.
2. Ensure that the *Target machine* and the *Source machine* are registered to the same Recovery Services vault.
3. Click **Recover Data** to initiate the workflow.
4. Select **Another server**

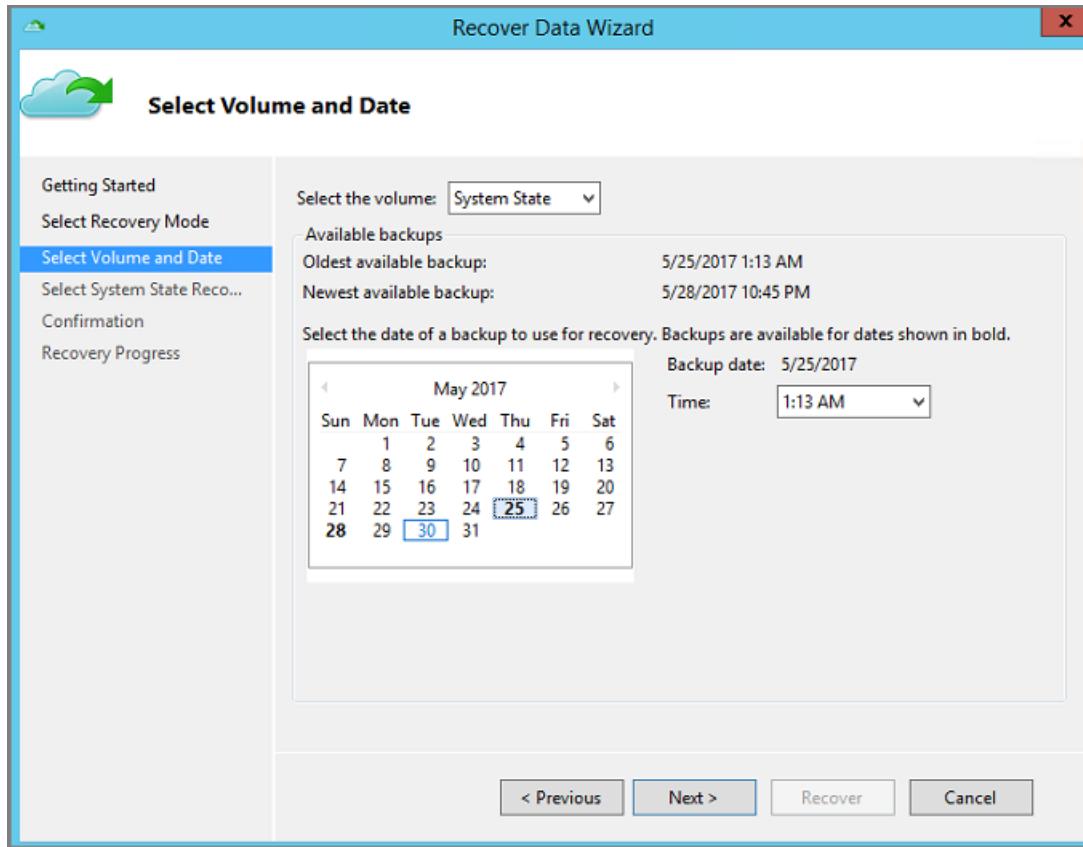


5. Provide the vault credential file that corresponds to the *Sample vault*. If the vault credential file is invalid (or expired), download a new vault credential file from the *Sample vault* in the Azure portal. Once the vault credential file is provided, the Recovery Services vault associated with the vault credential file appears.
6. On the Select Backup Server pane, select the *Source machine* from the list of displayed machines.
7. On the Select Recovery Mode pane, choose **System State** and click **Next**.

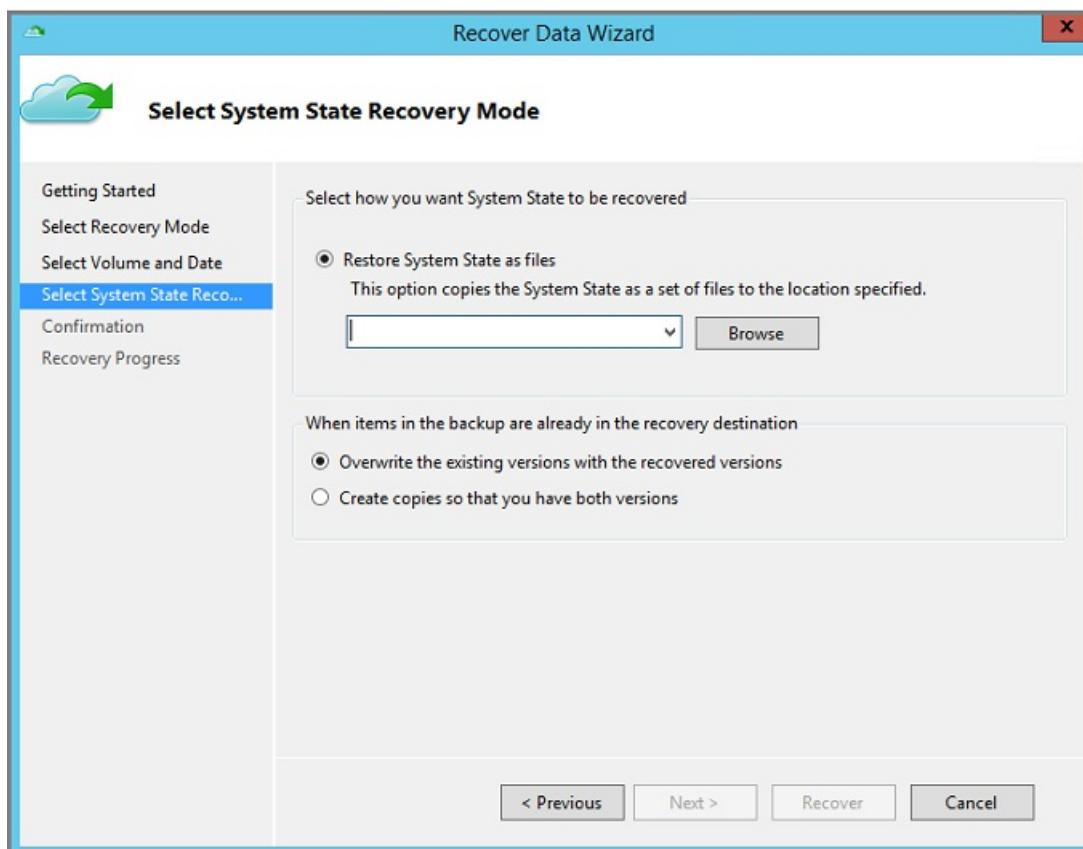


8. On the Calendar in the **Select Volume and Date** pane, select a recovery point. You can restore from any recovery point in time. Dates in **bold** indicate the availability of at least one recovery point. Once you select a date, if multiple recovery points are available, choose the specific recovery point from the **Time** drop-

down menu.

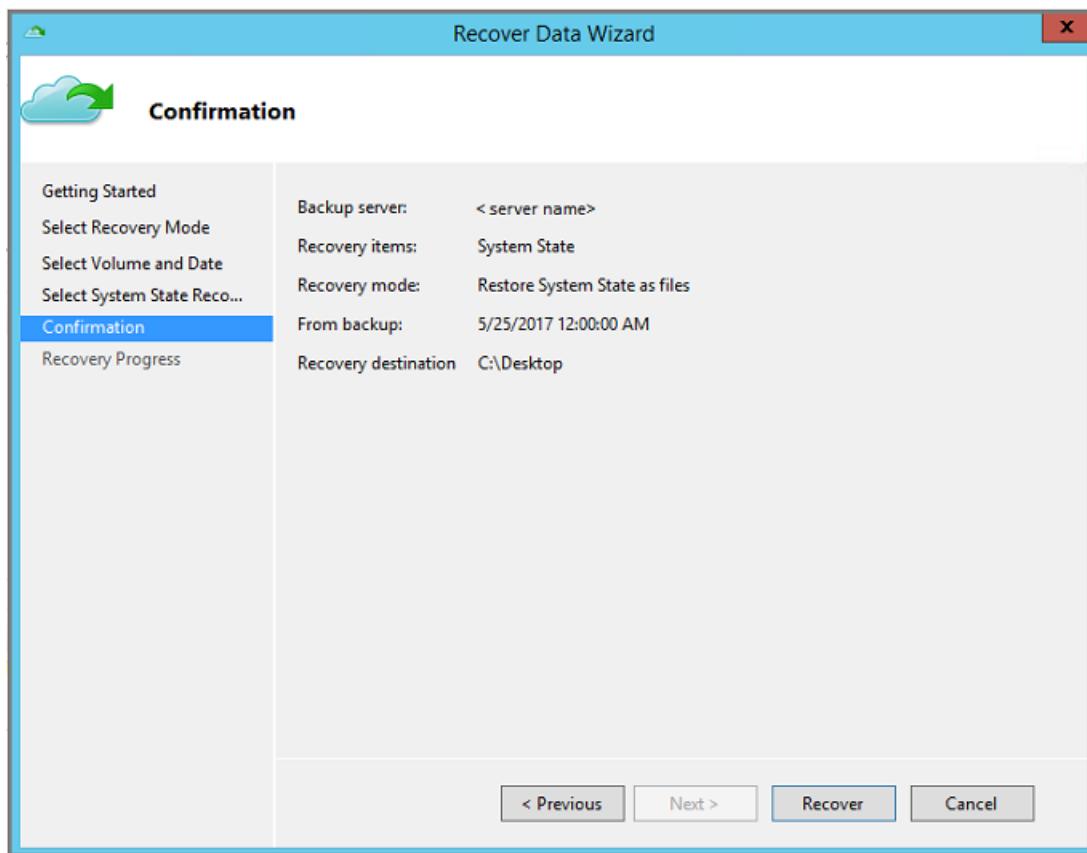


9. Once you have chosen the recovery point to restore, click **Next**.
10. On the **Select System State Recovery Mode** pane, specify the destination where you want System State files to be recovered, then click **Next**.



The option, **Create copies so that you have both versions**, creates copies of individual files in an existing System State file archive instead of creating the copy of the entire System State archive.

11. Verify the details of recovery on the Confirmation pane, and click **Recover**.



12. Copy the *WindowsImageBackup* directory to a non-critical volume of the server (for example D:). Usually the Windows OS volume is the critical volume.
13. To complete the recovery process, use the following section to [apply the restored System State files on a Windows Server](#).

## Apply restored System State on a Windows Server

Once you have recovered System State as files using Azure Recovery Services Agent, use the Windows Server Backup utility to apply the recovered System State to Windows Server. The Windows Server Backup utility is already available on the server. The following steps explain how to apply the recovered System State.

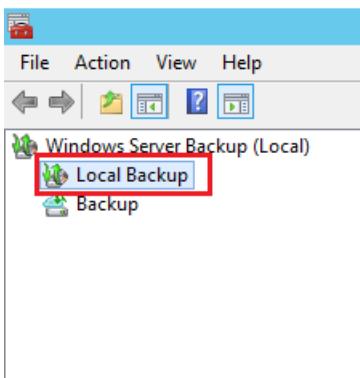
1. Use the following commands to reboot your server in *Directory Services Repair Mode*. In an elevated command prompt:

```
Bcdedit /set safeboot dsrepair
Shutdown /r /t 0
```

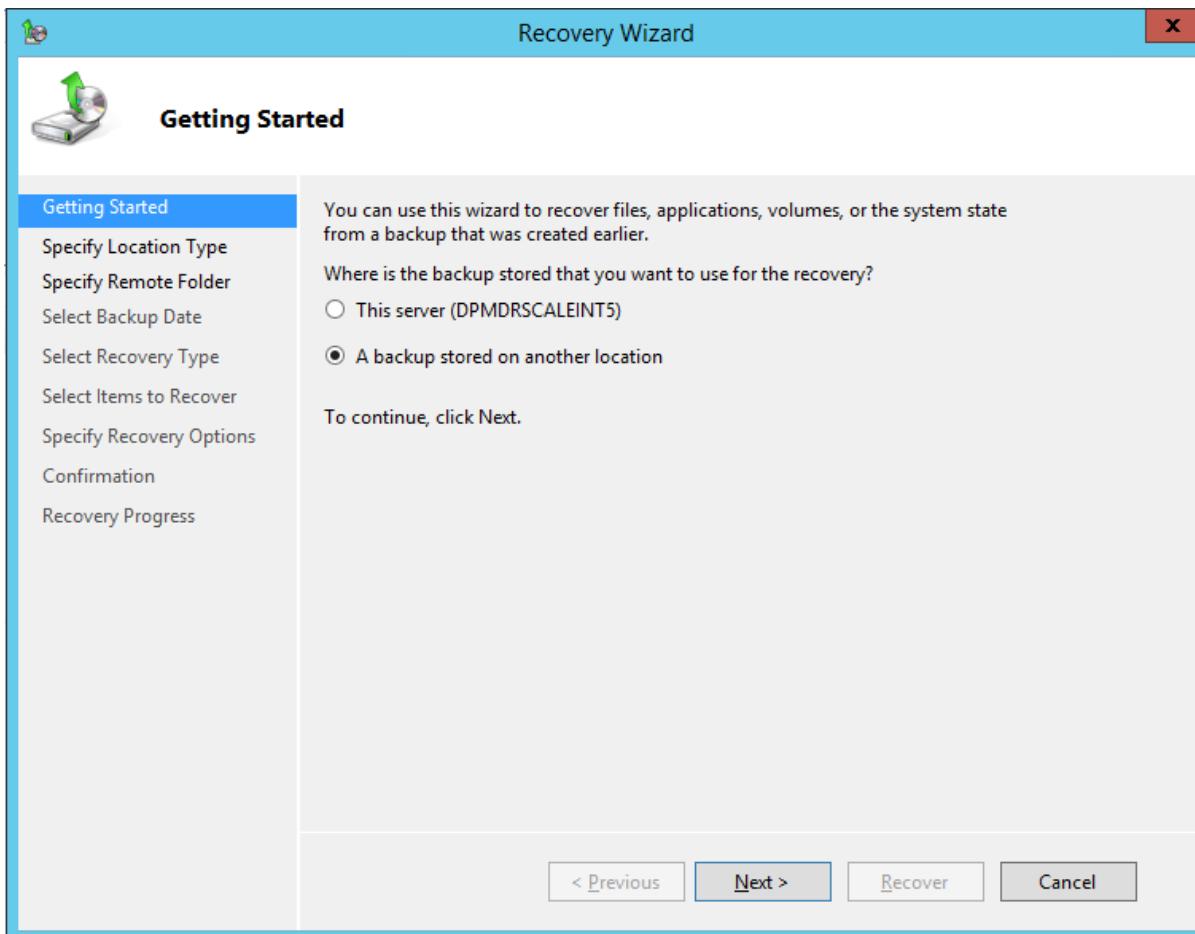
2. After the reboot, open the Windows Server Backup snap-in. If you don't know where the snap-in was installed, search the computer or server for **Windows Server Backup**.

The desktop app appears in the search results.

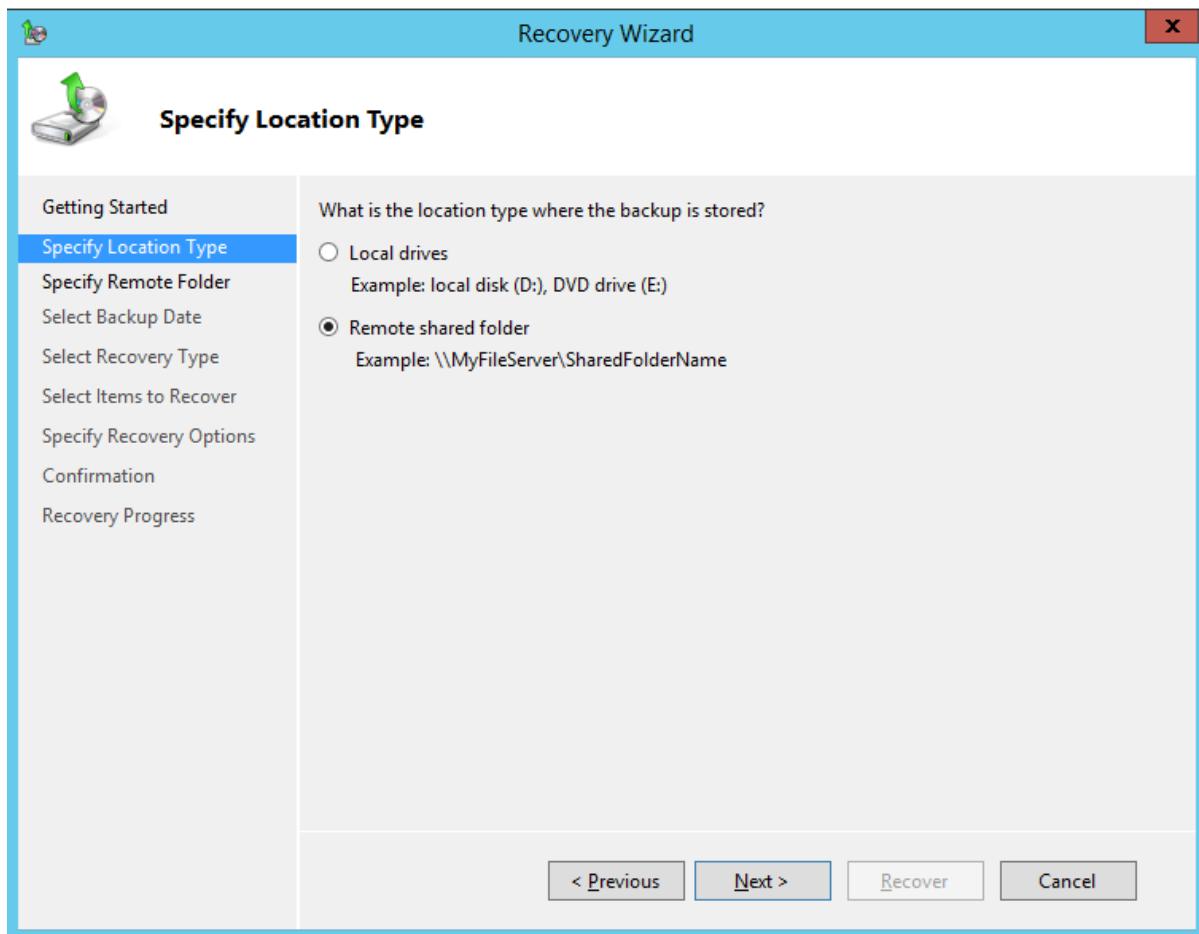
3. In the snap-in, select **Local Backup**.



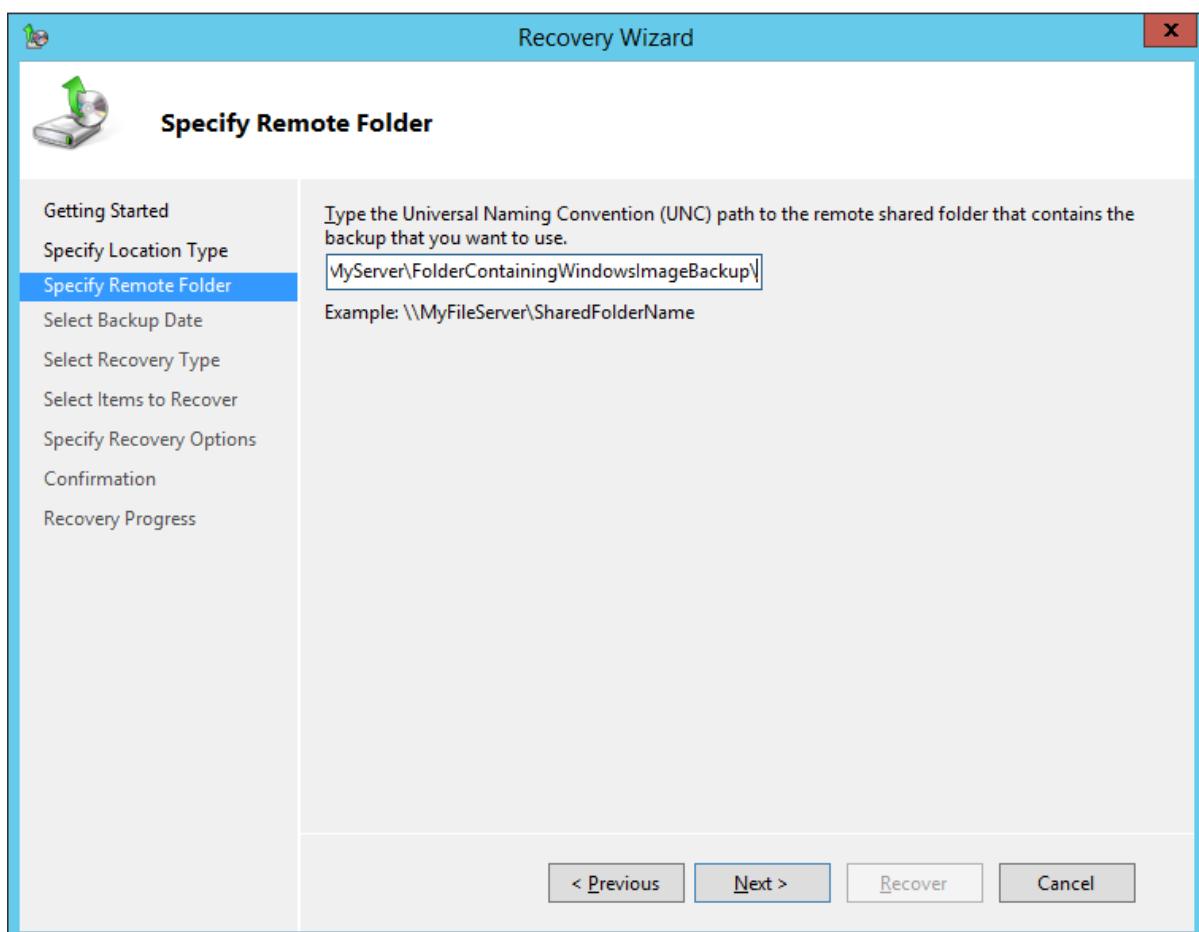
4. On the Local Backup console, in the **Actions Pane**, click **Recover** to open the Recovery Wizard.
5. Select the option, **A backup stored in another location**, and click **Next**.



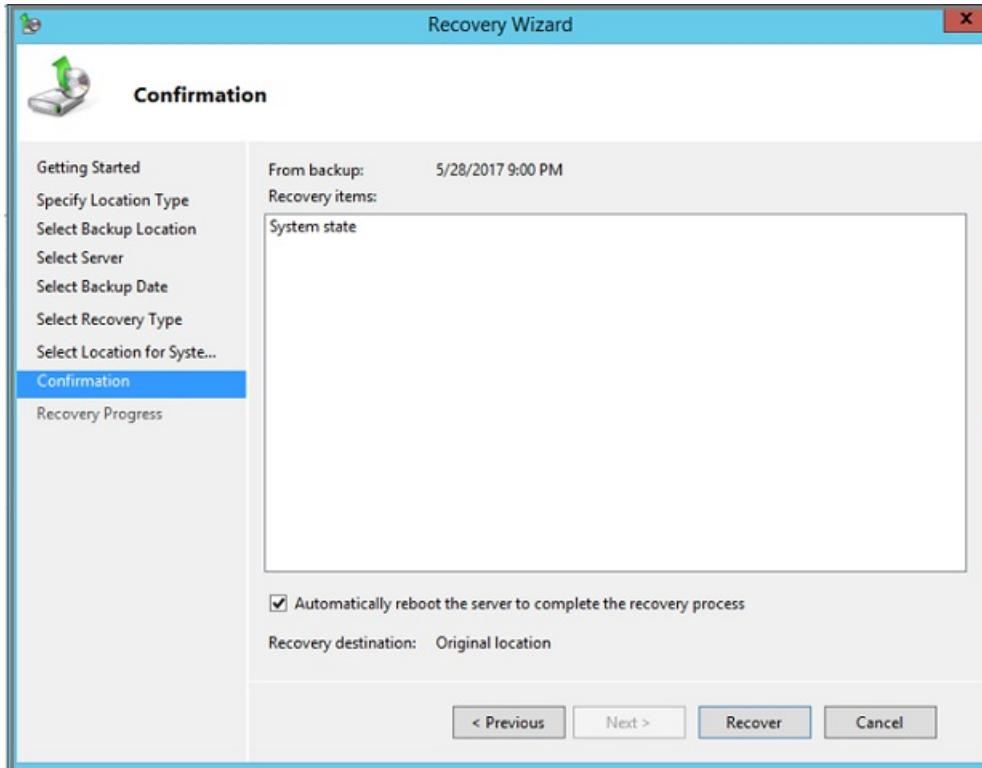
6. When specifying the location type, select **Remote shared folder** if your System State backup was recovered to another server. If your System State was recovered locally, then select **Local drives**.



7. Enter the path to the *WindowsImageBackup* directory, or choose the local drive containing this directory (for example, D:\\WindowsImageBackup), recovered as part of the System State files recovery using Azure Recovery Services Agent and click **Next**.



8. Select the System State version that you want to restore, and click **Next**.
9. In the Select Recovery Type pane, select **System State** and click **Next**.
10. For the location of the System State Recovery, select **Original Location**, and click **Next**.
11. Review the confirmation details, verify the reboot settings, and click **Recover** to apply the restored System State files.



## Special considerations for System State recovery on Active Directory server

System State backup includes Active Directory data. Use the following steps to restore Active Directory Domain Service (AD DS) from its current state to a previous state.

1. Restart the domain controller in Directory Services Restore Mode (DSRM).
2. Follow the steps [here](#) to use Windows Server Backup cmdlets to recover AD DS.

## Troubleshoot failed System State restore

If the previous process of applying System State does not complete successfully, use the Windows Recovery Environment (Win RE) to recover your Windows Server. The following steps explain how to recover using Win RE. Use this option only if Windows Server does not boot normally after a System State restore. The following process erases non-system data, use caution.

1. Boot your Windows Server into the Windows Recovery Environment (Win RE).
2. Select Troubleshoot from the three available options.

# Choose an option



**Continue**  
Exit and continue to Windows Server 2016



**Troubleshoot**  
Reset your PC or see advanced options



**Turn off your PC**

- From the **Advanced Options** screen, select **Command Prompt** and provide the server administrator username and password.

## ⟲ Advanced options



**System Image Recovery**  
Recover Windows using a specific system image file



**Command Prompt**  
Use the Command Prompt for advanced troubleshooting



**Startup Settings**  
Change Windows startup behavior

- Provide the server administrator username and password.

## ④ Command Prompt

Hi, Administrator

Enter the password for this account. (Keyboard Layout: US)

|

Change keyboard layout

Continue

- When you open the command prompt in administrator mode, run following command to get the System State backup versions.

```
Wbadmin get versions -backuptarget:<Volume where WindowsImageBackup folder is copied>:
```

```
Administrator:X:\windows\system32\cmd.exe
X:\windows\system32>wbadmin get versions -backuptarget:E:
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2013 Microsoft Corporation. All rights reserved.

Troubleshooting information for BMR: http://go.microsoft.com/fwlink/p/?LinkId=225039

The times of the backups displayed are based on the time zone of the current
operating system that you are using.
The time zone being used is (GMT -08:00) Pacific Standard Time.
Backup time: 5/25/2017 4:03 AM
Backup target: 1394/USB Disk labeled C:\Program Files\Microsoft Azure Recovery Services Agent\Scratch\SSBV
Version identifier: 05/25/2017-12:03
Can recover: Volume(s), File(s), Application(s)
Snapshot ID: {e03fdf60-769b-4fa1-b4c9-1613e54ea0ec}

X:\windows\system32>
```

- Run the following command to get all volumes available in the backup.

```
Wbadmin get items -version:<copy version from above step> -backuptarget:<Backup volume>
```

```
X:\windows\system32>wbadm in get items -version:05/25/2017-12:03 -backuptarget:E:
wbadm in 1.0 - Backup command-line tool
(C) Copyright 2013 Microsoft Corporation. All rights reserved.

Troubleshooting information for BMR: http://go.microsoft.com/fwlink/p/?LinkId=225039

Volume ID = {dea735eb-0000-0000-0000-501f00000000}
Volume '', mounted at D: ('', mounted at C: at the time
the backup was created)
Volume size = 97.21 GB
Can recover = Selected files

Application = Registry
Component = Registry (\Registry)
```

7. The following command recovers all volumes that are part of the System State Backup. Note that this step recovers only the critical volumes that are part of the System State. All non-System data is erased.

```
wbadm in start recovery -items:C: -itemtype:Volume -version:<Backupversion> -backuptarget:<backup target
volume>
```

```
X:\Administrator:X:\windows\system32\cmd.exe - wbadm in start recovery -items:C: -itemtype:Volume -version:05/25/2017-12:03 -backuptarget:E:
secrets, such as passwords, from read-only domain controller (RODC)
installation media. This makes transportation of the installation media
more secure.

X:\windows\system32>wbadm in start recovery -items:dea735eb-0000-0000-0000-501f00000000 -itemtype:Volume -version:05/25/2017-12:03 -backuptarget:E:
wbadm in 1.0 - Backup command-line tool
(C) Copyright 2013 Microsoft Corporation. All rights reserved.

Troubleshooting information for BMR: http://go.microsoft.com/fwlink/p/?LinkId=225039

Retrieving volume information...
The specified volume to recover is not in the backup.

X:\windows\system32>wbadm in start recovery -items:C: -itemtype:Volume -version:05/25/2017-12:03 -backuptarget:E:
wbadm in 1.0 - Backup command-line tool
(C) Copyright 2013 Microsoft Corporation. All rights reserved.

Troubleshooting information for BMR: http://go.microsoft.com/fwlink/p/?LinkId=225039

Retrieving volume information...
Warning: When this backup was created, only selected files or folders from
volumes 'C:' were included in the backup. If you continue, only those
specific files and folders will be recovered. Any other existing files or
folders on the recovery destination that were not part of the backup will be
deleted.

Do you want to continue?
[Y] Yes [N] No
```

## Next steps

- Now that you've recovered your files and folders, you can [manage your backups](#).

# Manage Microsoft Azure Recovery Services (MARS) Agent backups by using the Azure Backup service

2/25/2020 • 6 minutes to read • [Edit Online](#)

This article describes how to manage files and folders that are backed up with the Microsoft Azure Recovery Services Agent.

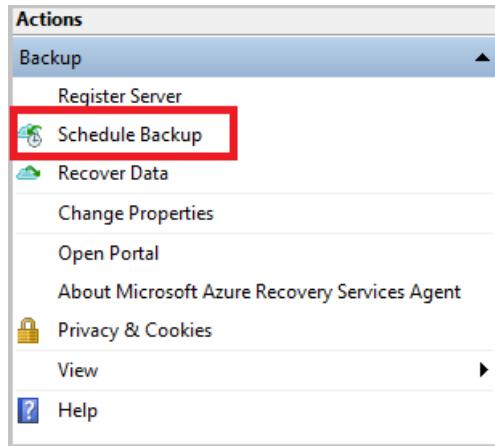
## Modify a backup policy

When you modify backup policy, you can add new items, remove existing items from backup, or exclude files from being backed up using Exclusion Settings.

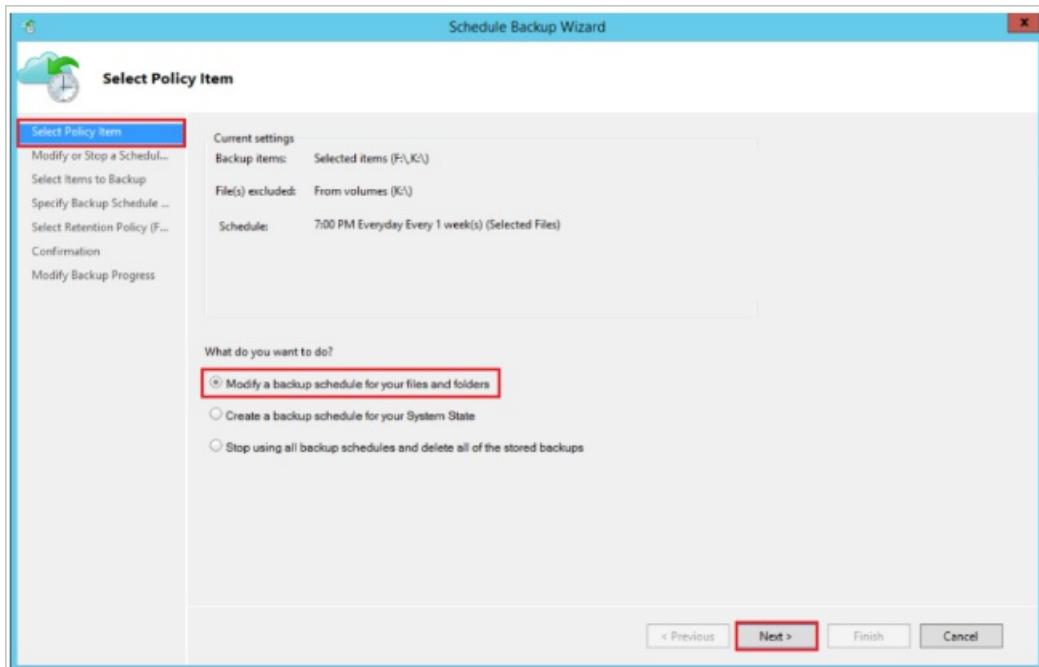
- **Add Items** use this option only for adding new items to back up. To remove existing items, use **Remove Items** or **Exclusion Settings** option.
- **Remove Items** use this option to remove items from being backed up.
  - Use **Exclusion Settings** for removing all items within a volume instead of **Remove Items**.
  - Clearing all selections in a volume causes old backups of the items, to be retained as per retention settings at the time of the last backup, without scope for modification.
  - Reselecting these items, leads to a first full-backup and new policy changes are not applied to old backups.
  - Unselecting entire volume retains past backup without any scope for modifying retention policy.
- **Exclusion Settings** use this option to exclude specific items from being backed up.

### Add new items to existing policy

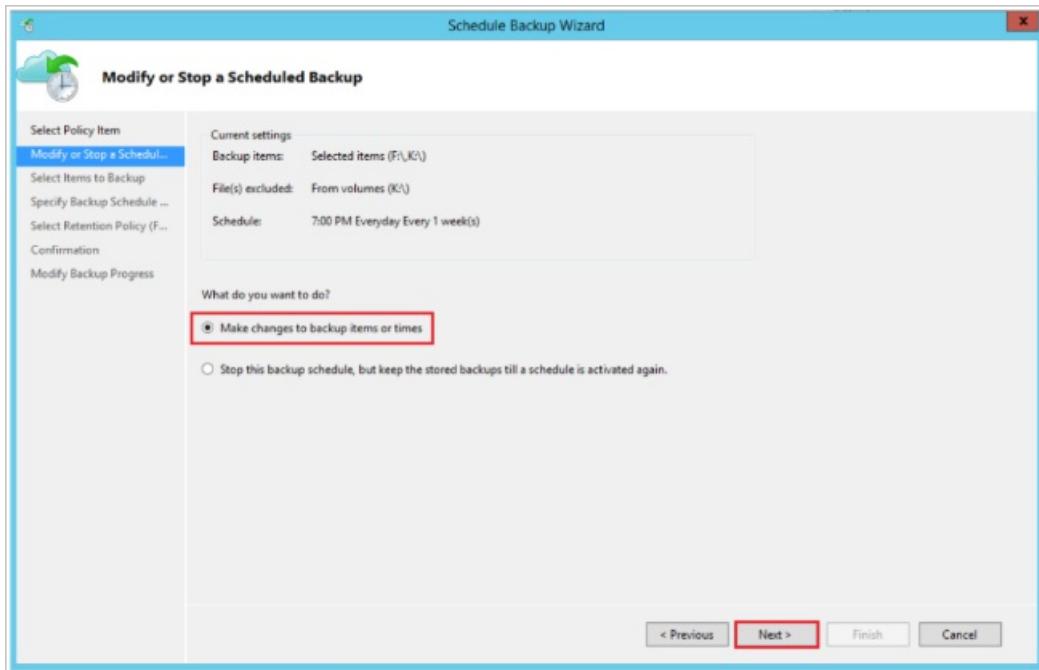
1. In **Actions**, click **Schedule Backup**.



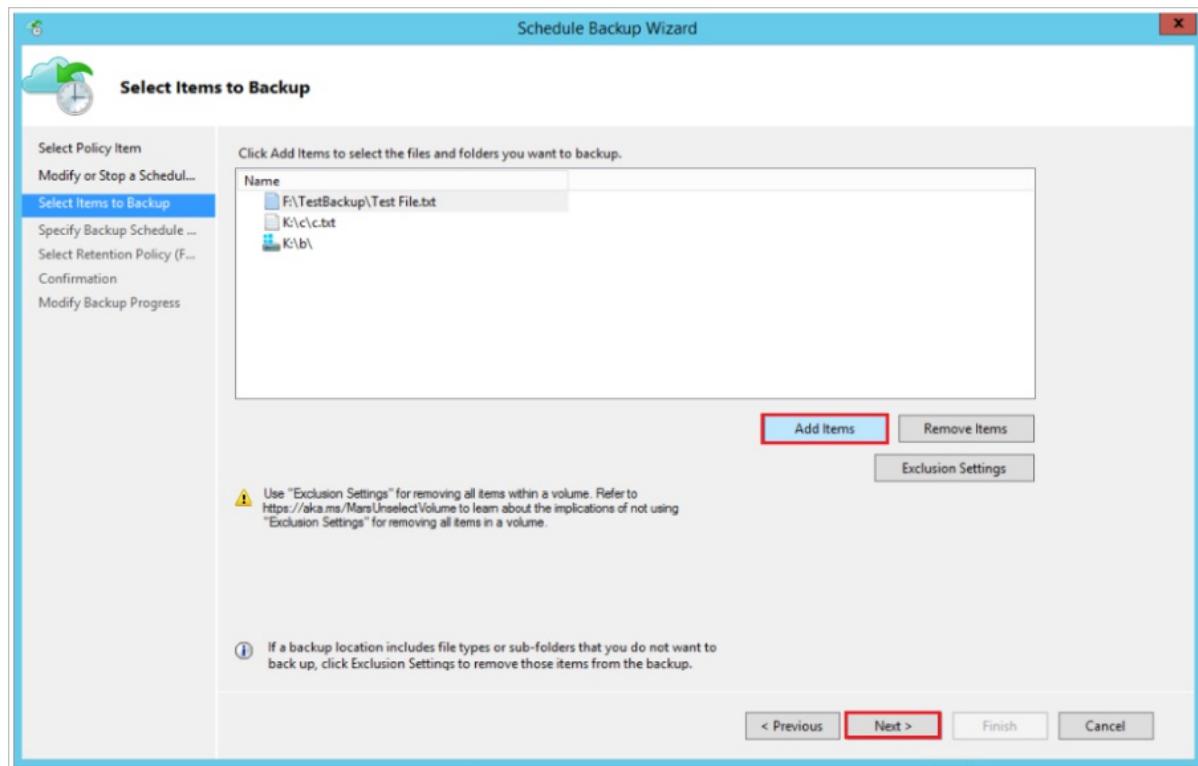
2. In **Select policy item** tab, and select **Modify backup schedule for your files and folders** and click **Next**.



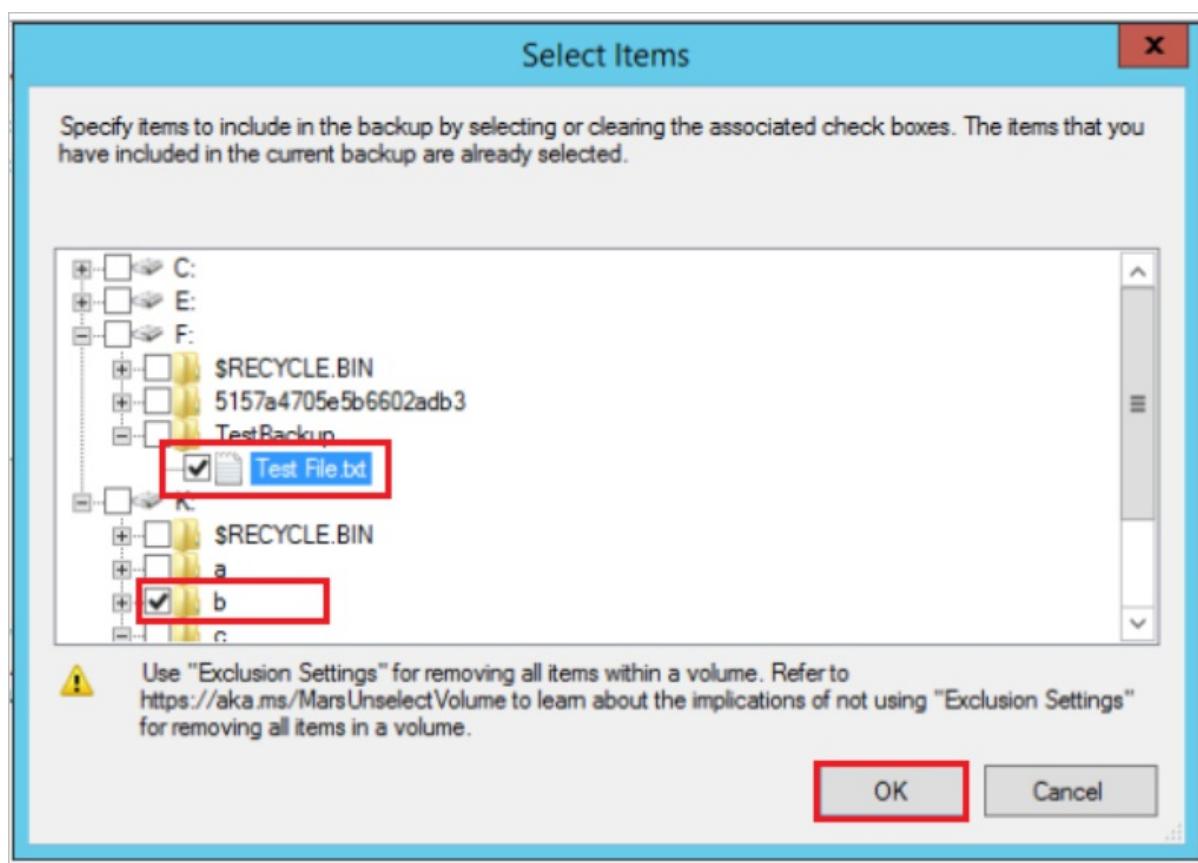
3. In **Modify or stop schedule backup** tab, select **Make changes to backup items or times** and click **Next**.



4. In **Select items to Backup** tab, click **Add items** to add the items that you want to back up.



5. In **Select Items** window, select files or folders that you want to add and click **OK**.

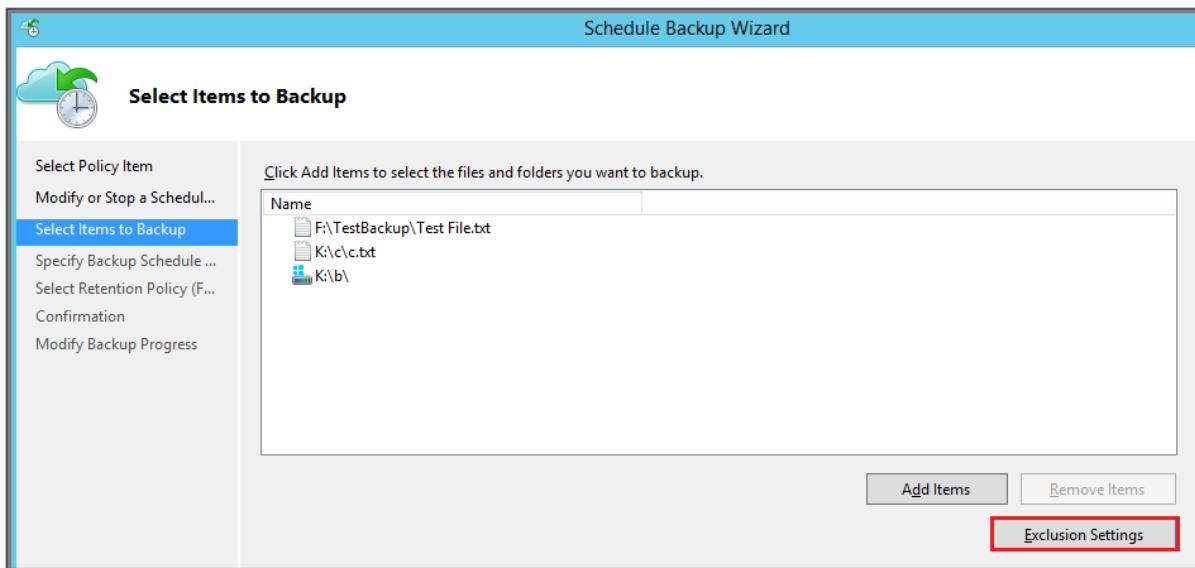


6. Complete the subsequent steps and click **Finish** to complete the operation.

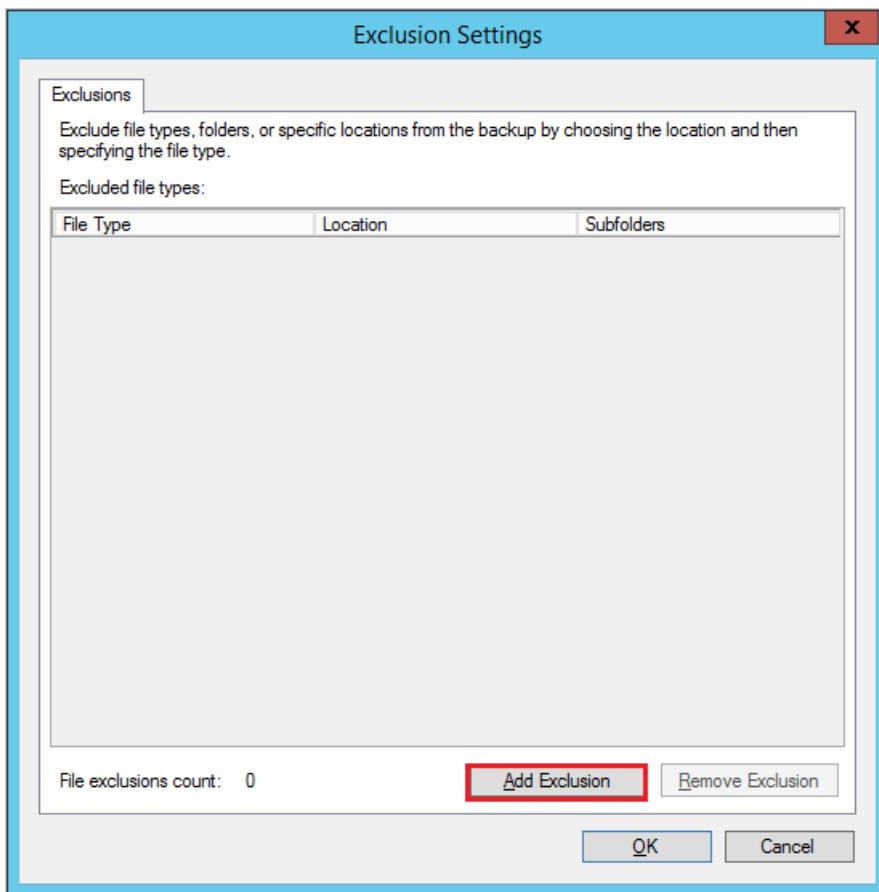
#### Add Exclusion rules to existing policy

You can add exclusion rules to skip files and folders that you don't want to be backed up. You can do this during when defining a new policy or modifying an existing policy.

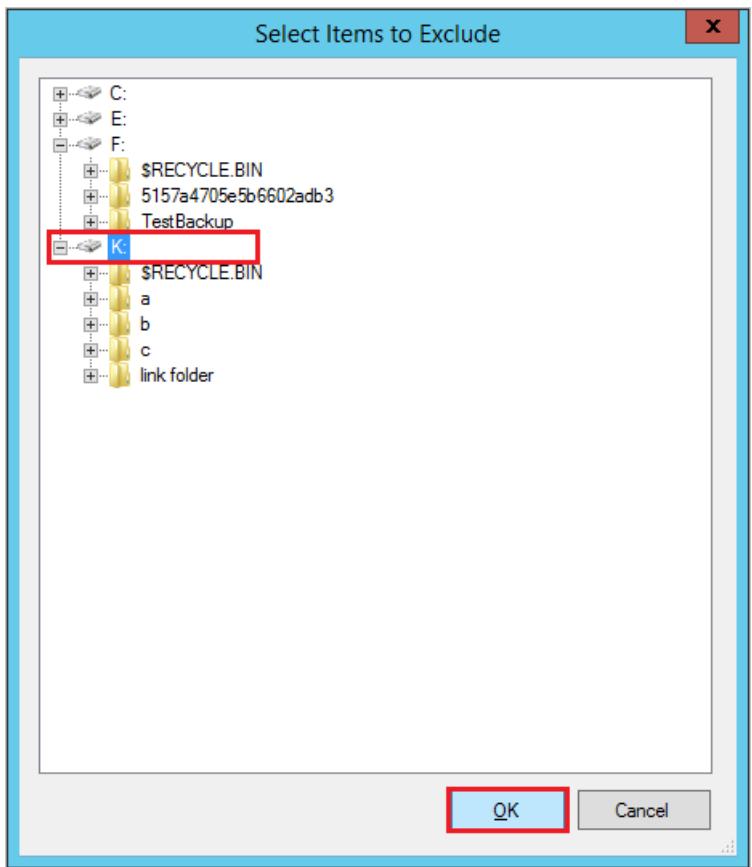
1. From the Actions pane, click **Schedule Backup**. Go to **Select items to Backup** and click **Exclusion Settings**.



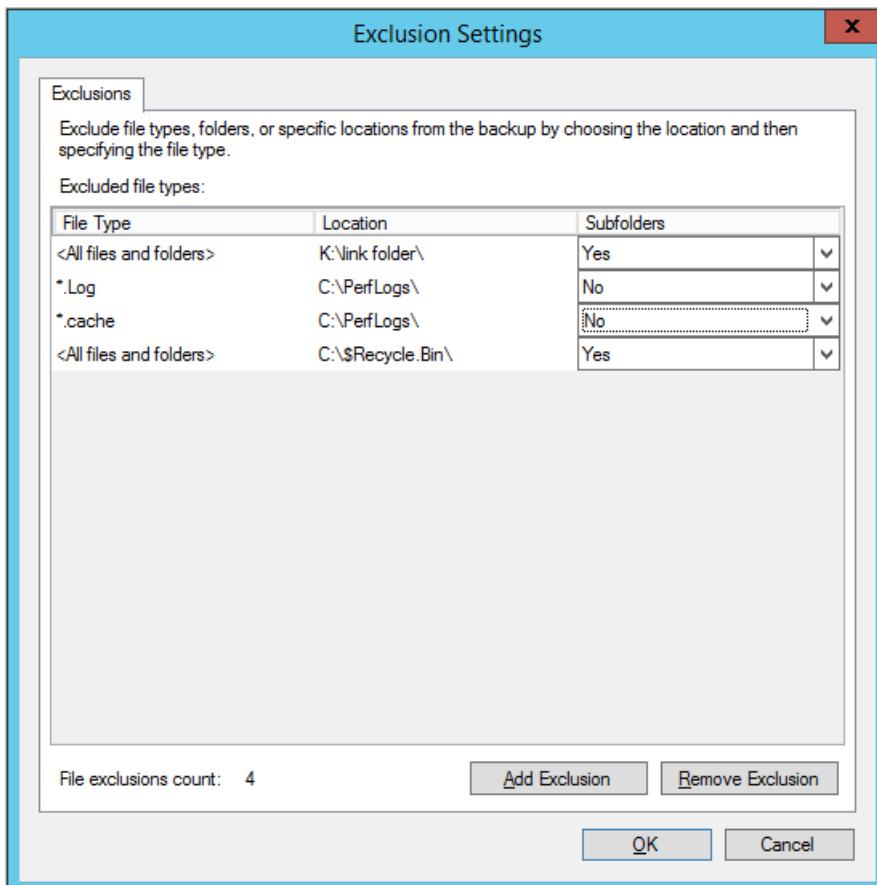
2. In **Exclusion Settings**, click **Add Exclusion**.



3. From **Select Items to Exclude**, browse the files and folders and select items that you want to exclude and click **OK**.



4. By default all **Subfolders** within the selected folders are excluded. You can change this by selecting **Yes** or **No**. You can edit and specify the file types to exclude as shown below:

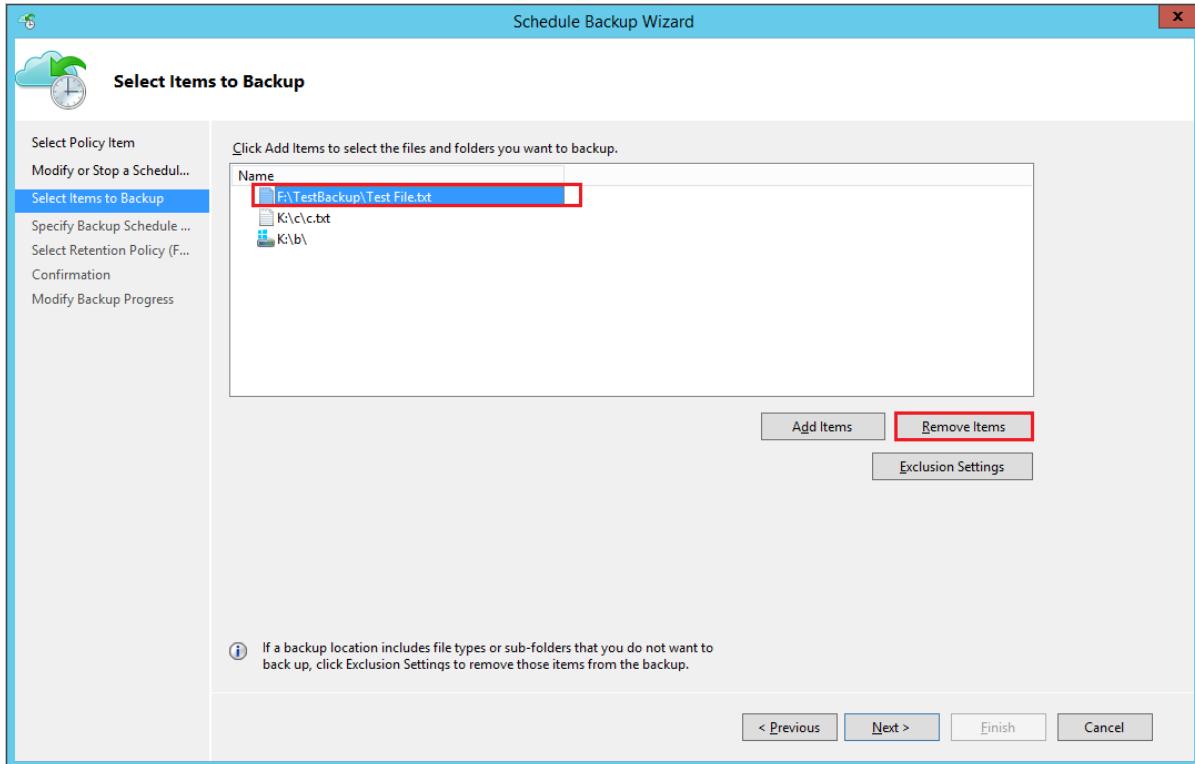


5. Complete the subsequent steps and click **Finish** to complete the operation.

#### Remove items from existing policy

- From the Actions pane, click **Schedule Backup**. Go to **Select items to Backup**. From the list, select the

files and folders that you want to remove from backup schedule and click **Remove items**.



#### NOTE

Proceed with caution when you completely remove a volume from the policy. If you need to add it again, then it will be treated as a new volume. The next scheduled backup will perform an Initial Backup (full backup) instead of Incremental Backup. If you need to temporarily remove and add items later, then it is recommended to use **Exclusions Settings** instead of **Remove Items** to ensure incremental backup instead of full backup.

2. Complete the subsequent steps and click **Finish** to complete the operation.

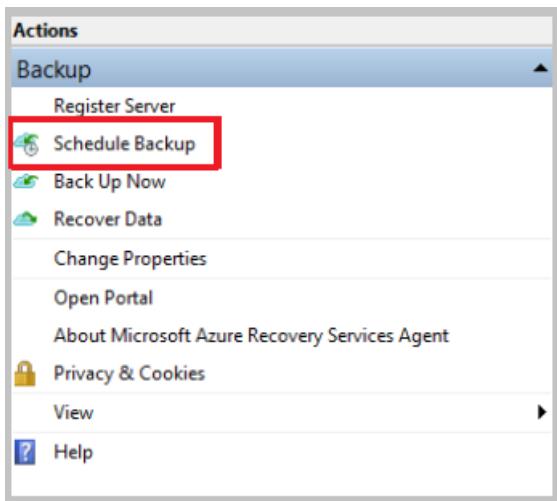
## Stop protecting Files and Folder backup

There are two ways to stop protecting Files and Folders backup:

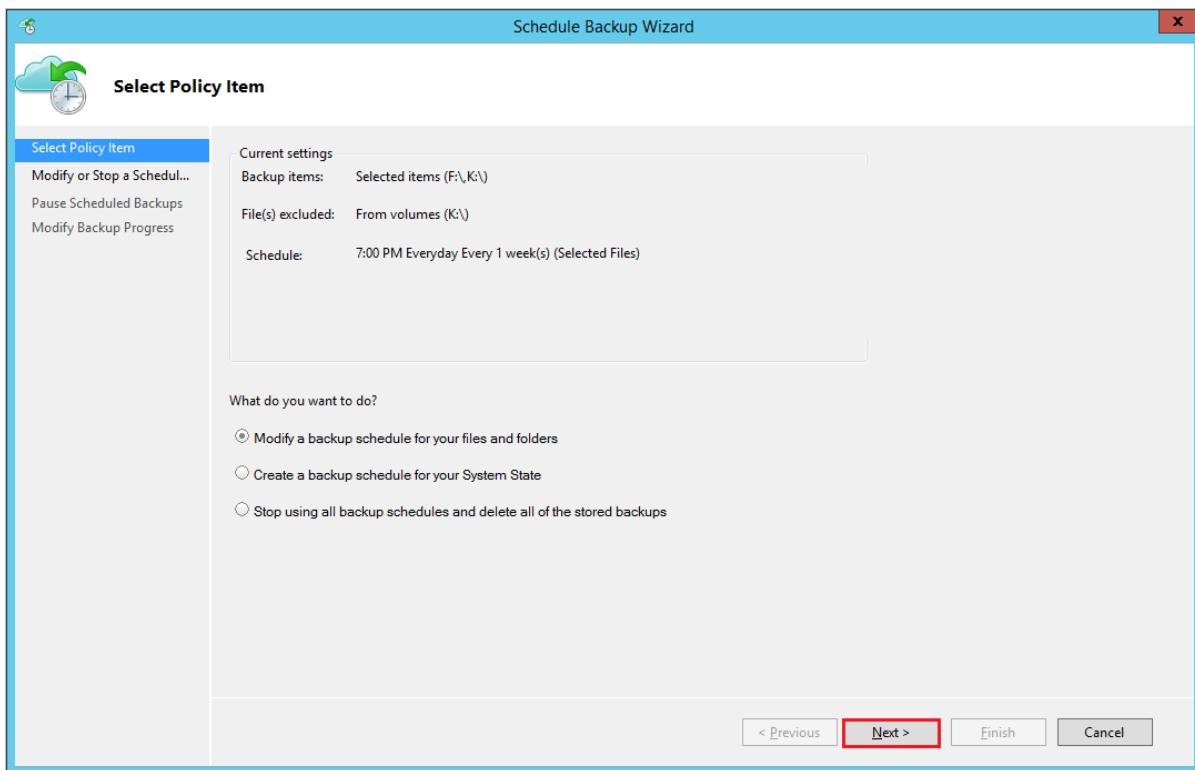
- **Stop protection and retain backup data.**
  - This option will stop all future backup jobs from protection.
  - Azure Backup service will retain the recovery points that have been backed up based on the retention policy.
  - You'll be able to restore the backed-up data for unexpired recovery points.
  - If you decide to resume protection, then you can use the *Re-enable backup schedule* option. After that, data would be retained based on the new retention policy.
- **Stop protection and delete backup data.**
  - This option will stop all future backup jobs from protecting your data and delete all the recovery points.
  - You will receive a delete Backup data alert email with a message *Your data for this Backup item has been deleted. This data will be temporarily available for 14 days, after which it will be permanently deleted* and recommended action *Reprotect the Backup item within 14 days to recover your data.*
  - To resume protection, reprotect within 14 days from delete operation.

### Stop protection and retain backup data

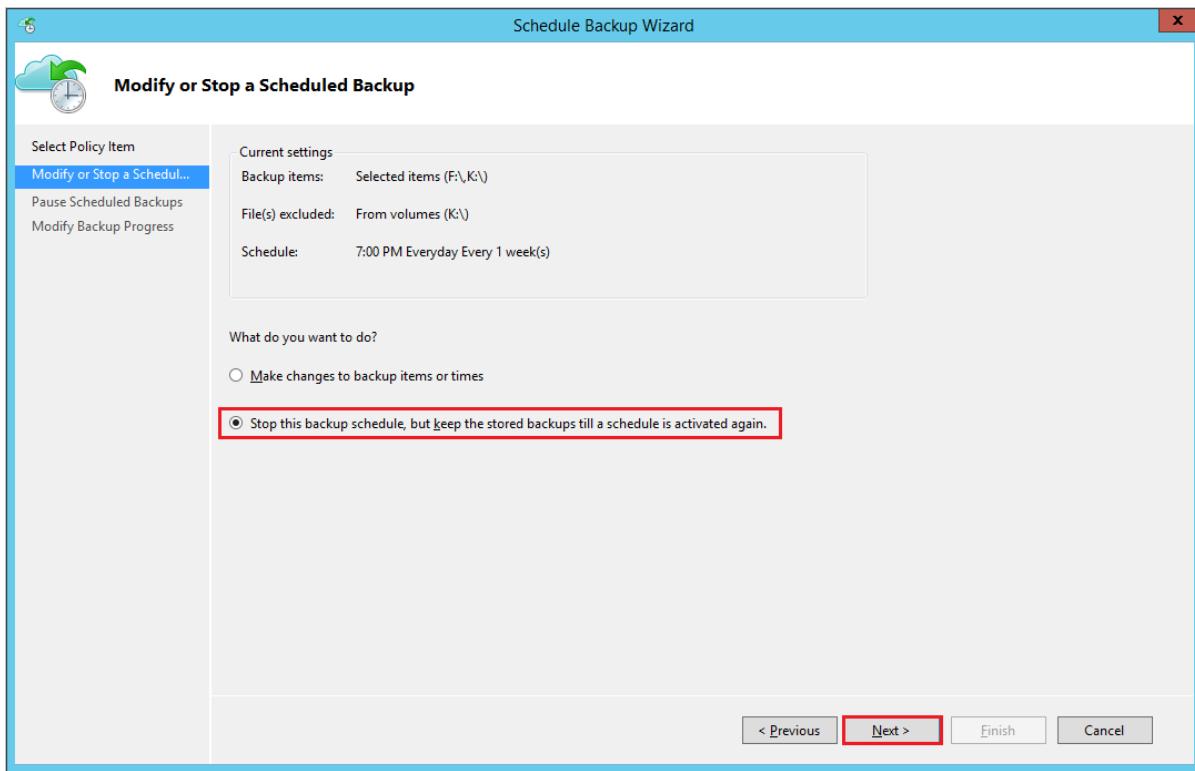
1. Open the MARS management console, go to the **Actions pane**, and **select Schedule Backup**.



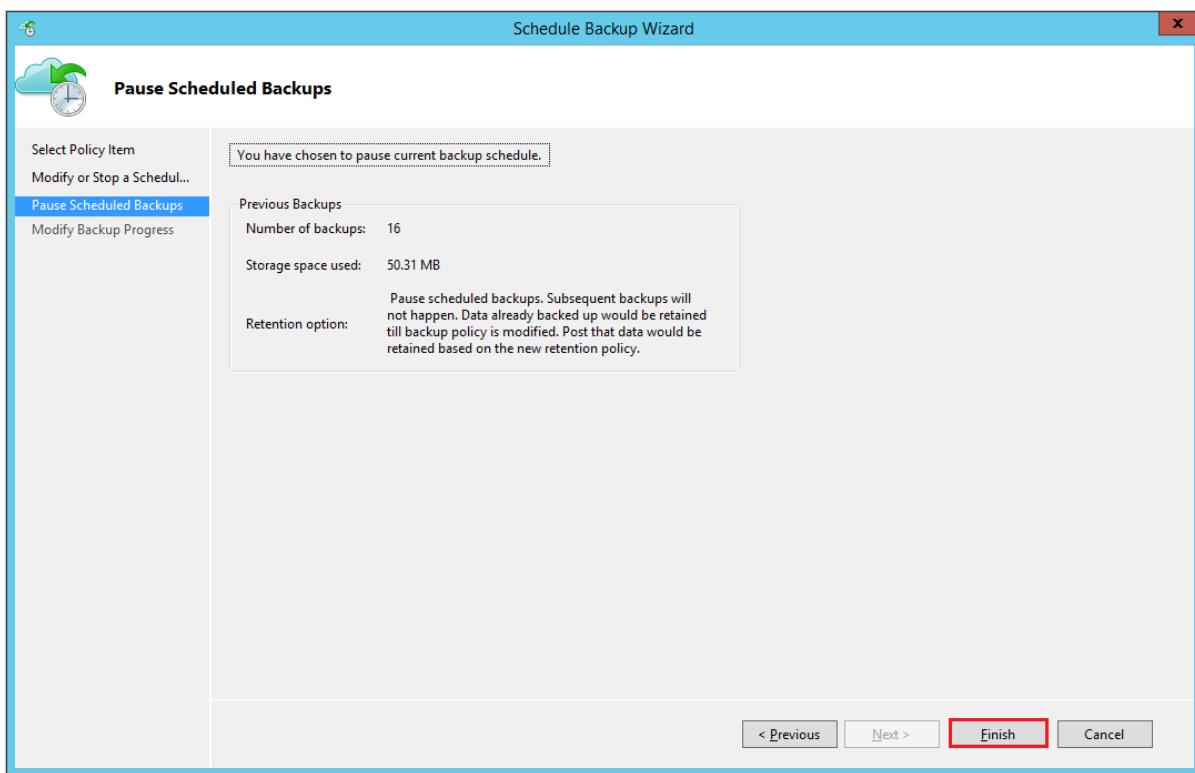
2. In **Select Policy Item** page, select **Modify a backup schedule for your files and folders** and click **Next**.



3. From the **Modify or Stop a Scheduled Backup** page, select **Stop using this backup schedule, but keep the stored backups until a schedule is activated again**. Then, select **Next**.



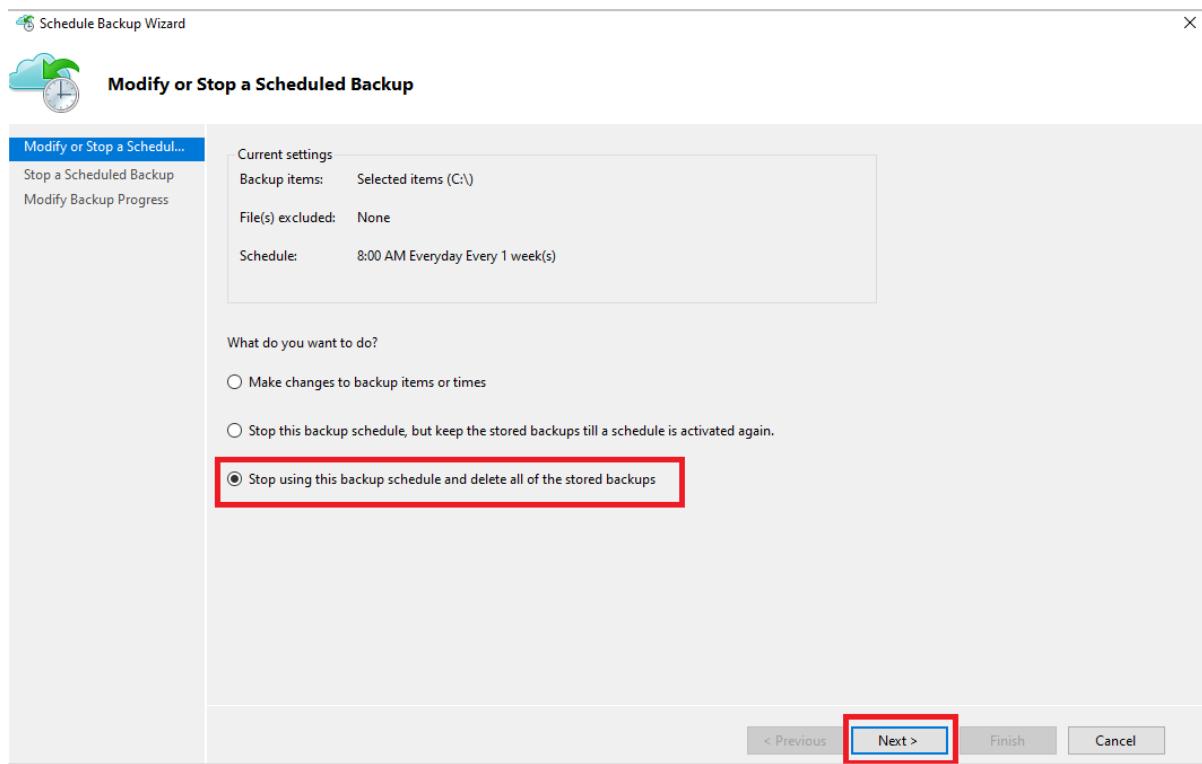
4. In **Pause Scheduled Backup** review the information and click **Finish**.



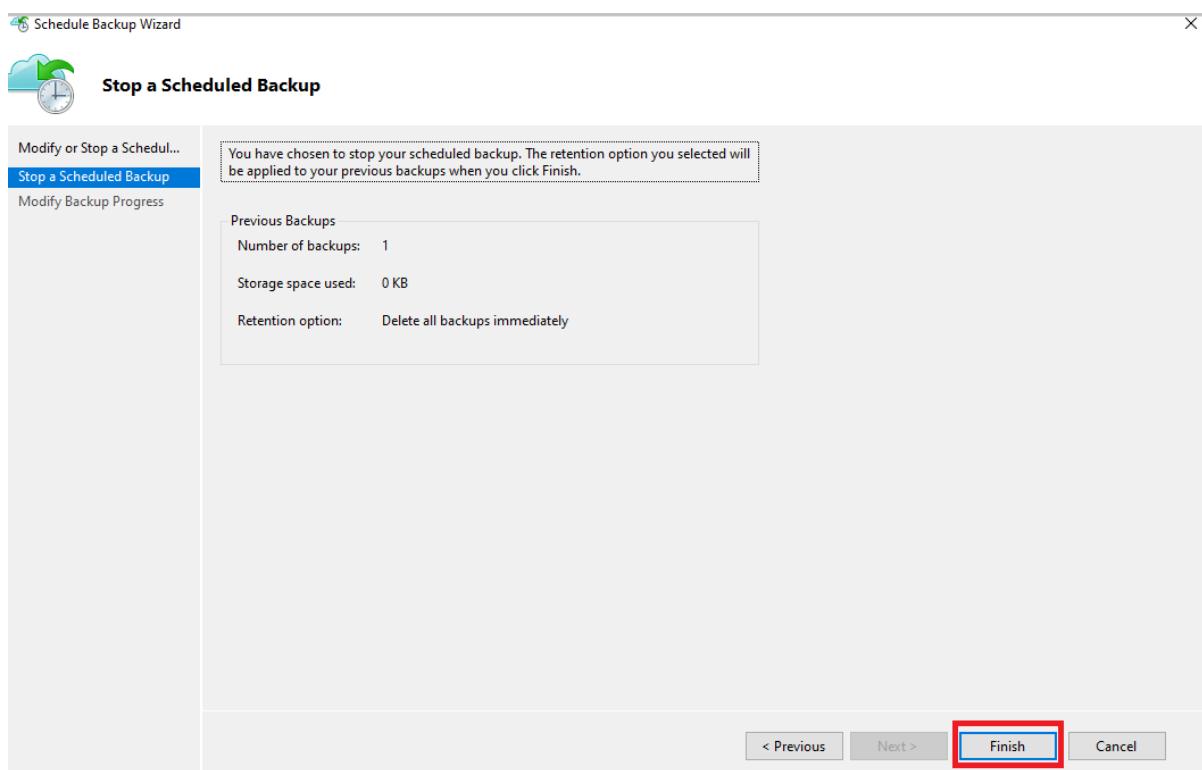
5. In **Modify backup process** check your schedule backup pause is in success status and click **close** to finish.

#### Stop protection and delete backup data

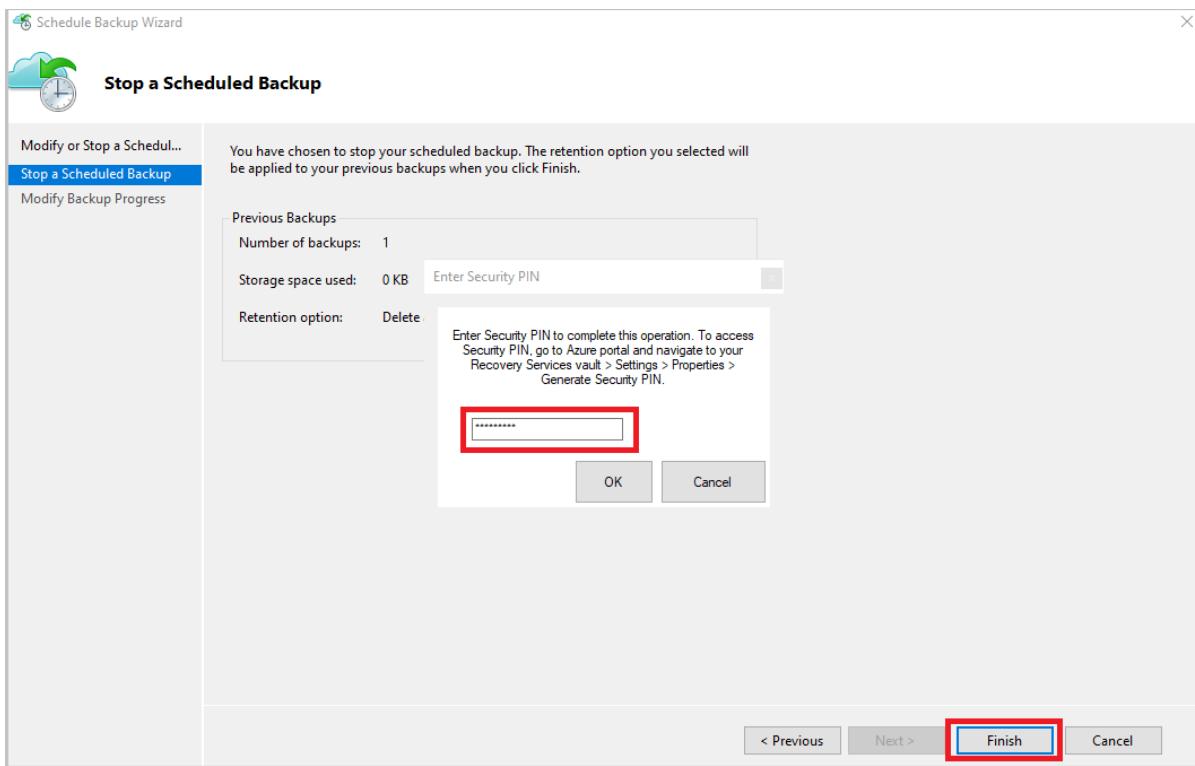
1. Open the MARS management console, go to the **Actions** pane, and select **Schedule Backup**.
2. From the **Modify or Stop a Scheduled Backup** page, select **Stop using this backup schedule and delete all the stored backups**. Then, select **Next**.



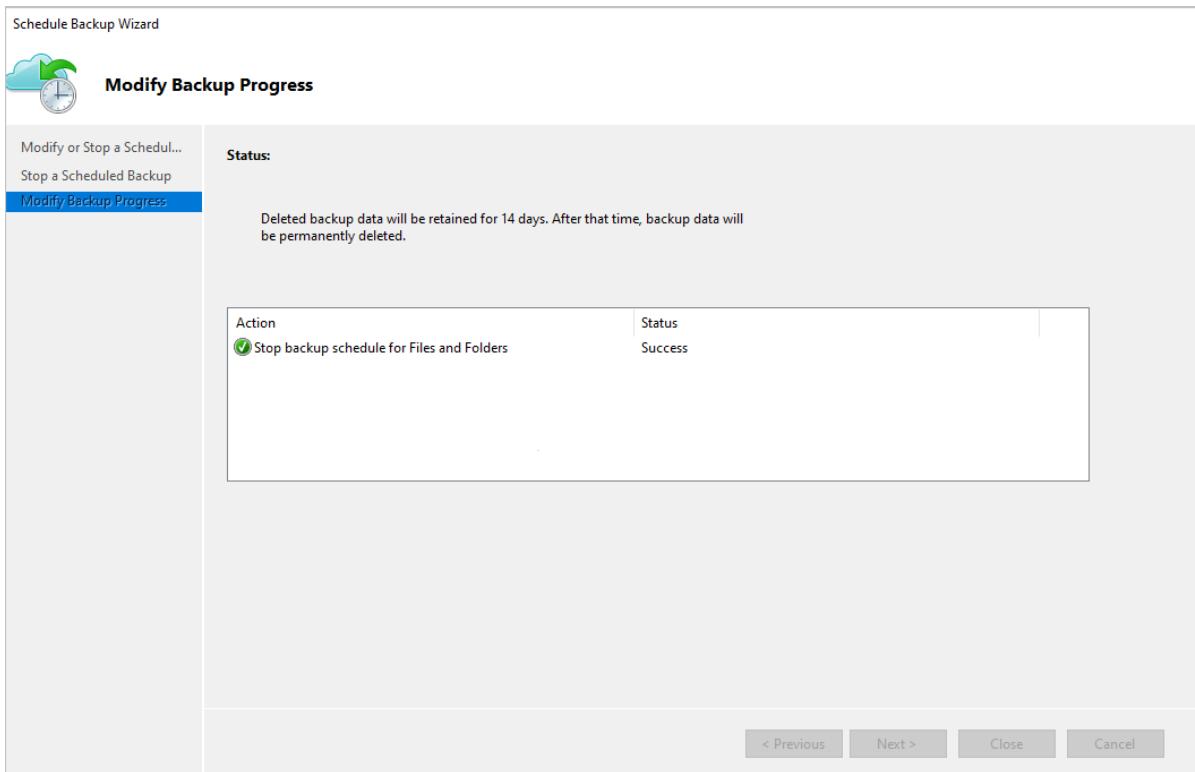
3. From the **Stop a Scheduled Backup** page, select **Finish**.



4. You are prompted to enter a security PIN (personal identification number), which you must generate manually. To do this, first sign in to the Azure portal.
5. Go to **Recovery Services vault** > **Settings** > **Properties**.
6. Under **Security PIN**, select **Generate**. Copy this PIN. The PIN is valid for only five minutes.
7. In the management console, paste the PIN, and then select **OK**.



8. In the **Modify Backup Progress** page, the following message appears: *Deleted backup data will be retained for 14 days. After that time, backup data will be permanently deleted.*

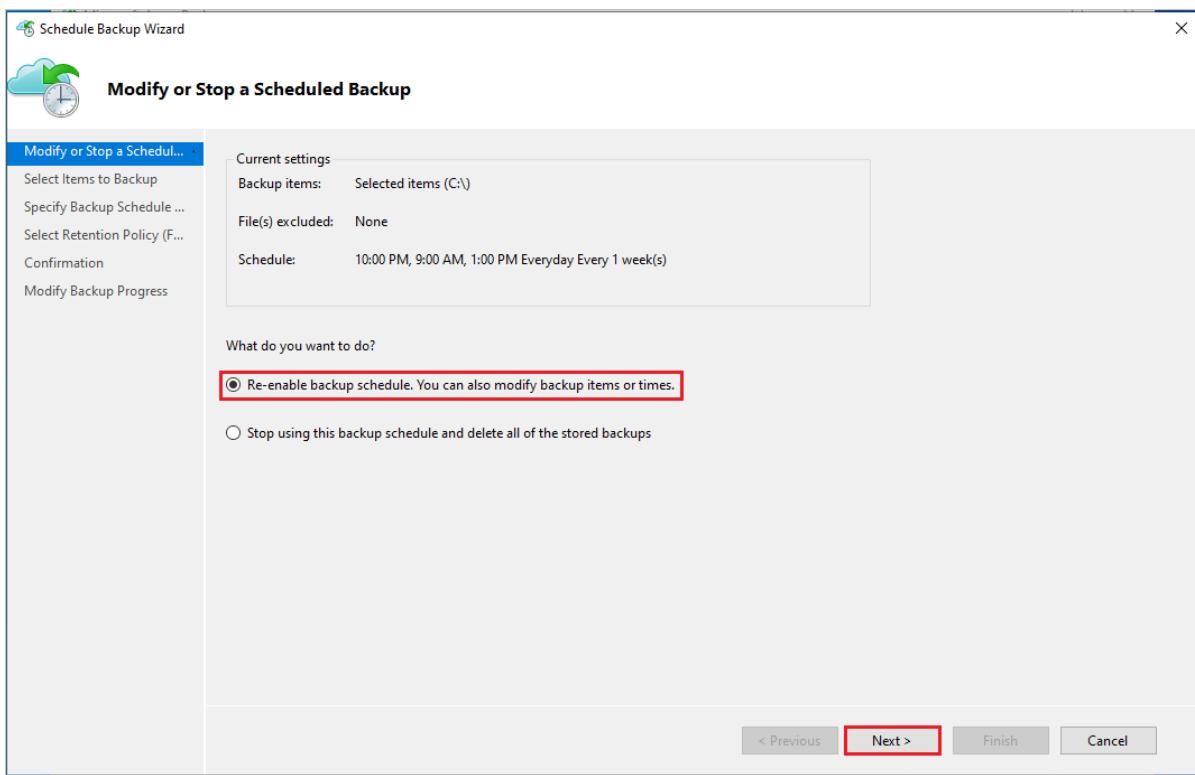


After you delete the on-premises backup items, follow the next steps from the portal.

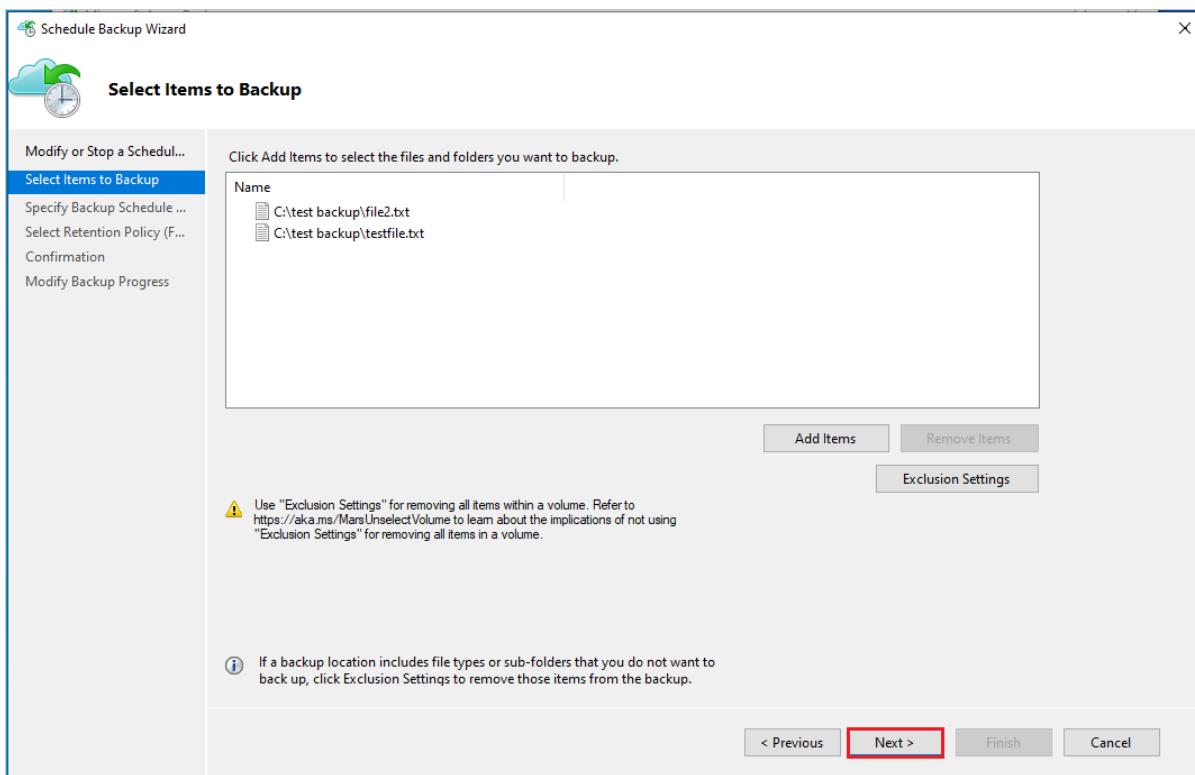
## Re-enable protection

If you stopped protection while retaining data and decided to resume protection, then you can re-enable the backup schedule using modify backup policy.

1. On **Actions** select **Schedule backup**.
2. Select **Re-enable backup schedule**. You can also modify backup items or times and click **Next**.



3. In **Select Items to Backup**, click **Next**.



4. In **Specify Backup Schedule**, specify the backup schedule and click **Next**.

5. In **Select Retention Policy**, specify retention duration and click **Next**.

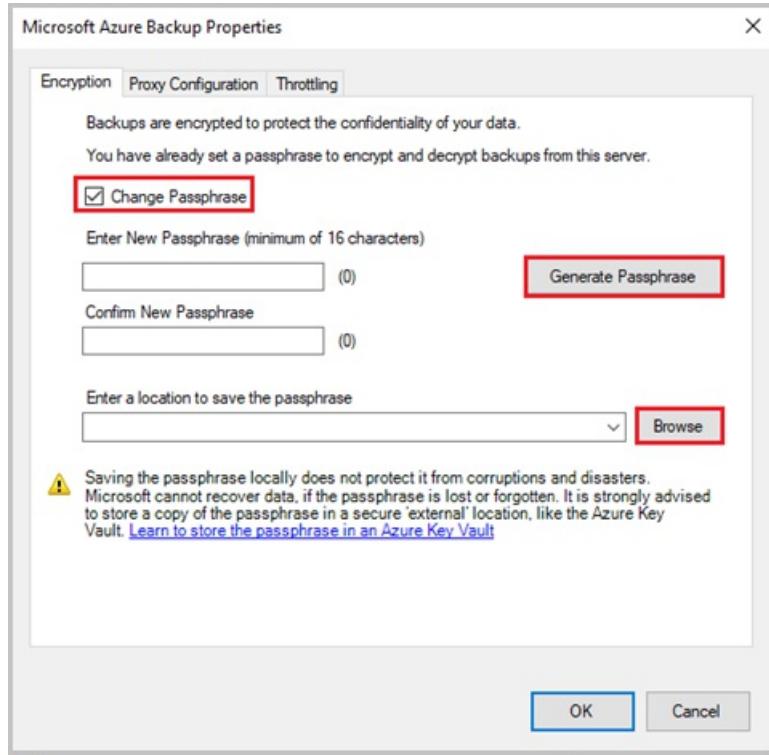
6. Finally in the **Confirmation** screen, review the policy details and click **Finish**.

## Re-generate passphrase

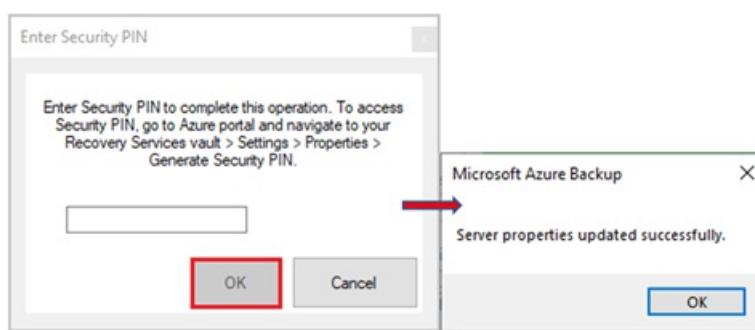
A passphrase is used to encrypt and decrypt data while backing up or restoring your on-premises or local machine using the MARS agent to or from Azure. If you lost or forgot the passphrase, then you can regenerate the passphrase (provided your machine is still registered with the Recovery Services Vault and the backup is

configured) by following these steps:

- From the MARS agent console, go to **Actions Pane** > **Change properties** >. Then go to **Encryption tab**.
- Select **Change Passphrase** checkbox.
- Enter a new passphrase or click **Generate Passphrase**.
- Click **Browse** to save the new passphrase.



- Click **OK** to apply changes. If the **Security Feature** is enabled on the Azure portal for the Recovery Services Vault, then you will be prompted to enter the Security PIN. To receive the PIN, follow the steps listed in this article.
- Paste the security PIN from the portal and click **OK** to apply the changes.



- Ensure that the passphrase is securely saved in an alternate location (other than the source machine), preferably in the Azure Key Vault. Keep track of all the passphrases if you have multiple machines being backed up with the MARS agents.

## Next steps

- For information about supported scenarios and limitations, refer to the [Support Matrix for the MARS Agent](#).
- Learn more about [On demand backup policy retention behavior](#).

# Back up Azure file shares in a Recovery Services vault

1/31/2020 • 6 minutes to read • [Edit Online](#)

This article explains how to use the Azure portal to back up [Azure file shares](#).

In this article, you'll learn how to:

- Create a Recovery Services vault.
- Discover file shares and configure backups.
- Run an on-demand backup job to create a restore point.

## Prerequisites

- Identify or create a [Recovery Services vault](#) in the same region as the storage account that hosts the file share.
- Ensure that the file share is present in one of the [supported storage account types](#).

## Limitations for Azure file share backup during preview

Backup for Azure file shares is in preview. Azure file shares in both general-purpose v1 and general-purpose v2 storage accounts are supported. Here are the limitations for backing up Azure file shares:

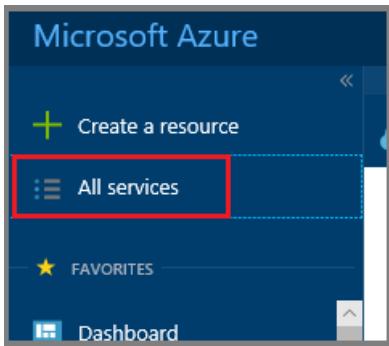
- Support for backup of Azure file shares in storage accounts with [zone-redundant storage](#) (ZRS) replication is currently limited to [these regions](#).
- Azure Backup currently supports configuring scheduled once-daily backups of Azure file shares.
- The maximum number of scheduled backups per day is one.
- The maximum number of on-demand backups per day is four.
- Use [resource locks](#) on the storage account to prevent accidental deletion of backups in your Recovery Services vault.
- Don't delete snapshots created by Azure Backup. Deleting snapshots can result in loss of recovery points or restore failures.
- Don't delete file shares that are protected by Azure Backup. The current solution deletes all snapshots taken by Azure Backup after the file share is deleted, so all restore points will be lost.

## Create a Recovery Services vault

A Recovery Services vault is an entity that stores backups and recovery points created over time. The Recovery Services vault also contains the backup policies that are associated with the protected virtual machines.

To create a Recovery Services vault, follow these steps.

1. Sign in to your subscription in the [Azure portal](#).
2. On the left menu, select **All services**.



3. In the **All services** dialog box, enter *Recovery Services*. The list of resources filters according to your input. In the list of resources, select **Recovery Services vaults**.

The list of Recovery Services vaults in the subscription appears.

4. On the **Recovery Services vaults** dashboard, select **Add**.

The **Recovery Services vault** dialog box opens. Provide values for the **Name**, **Subscription**, **Resource group**, and **Location**.

The dialog box contains the following fields:

- Name:** Enter the name of the vault. The name must be unique to the Azure subscription. Specify a name that has at least 2 but not more than 50 characters. The name must start with a letter and consist only of letters, numbers, and hyphens.
- Subscription:** Choose the subscription to use. If you're a member of only one subscription, you'll see that name. If you're not sure which subscription to use, use the default (suggested) subscription.
- Resource group:** You can either **Create new** or **Use existing**. If you choose to create a new one, you'll be prompted to enter a name for the new resource group.
- Location:** Select the location where the vault will be created. The options available will depend on the subscription selected.

At the bottom of the dialog box are two buttons: **Create** and **Automation options**.

- Name:** Enter a friendly name to identify the vault. The name must be unique to the Azure subscription. Specify a name that has at least 2 but not more than 50 characters. The name must start with a letter and consist only of letters, numbers, and hyphens.
- Subscription:** Choose the subscription to use. If you're a member of only one subscription, you'll see that name. If you're not sure which subscription to use, use the default (suggested) subscription.

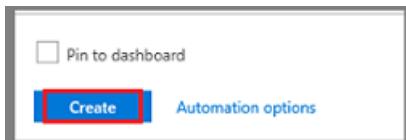
There are multiple choices only if your work or school account is associated with more than one Azure subscription.

- **Resource group:** Use an existing resource group or create a new one. To see the list of available resource groups in your subscription, select **Use existing**, and then select a resource from the drop-down list. To create a new resource group, select **Create new** and enter the name. For more information about resource groups, see [Azure Resource Manager overview](#).
- **Location:** Select the geographic region for the vault. To create a vault to protect virtual machines, the vault *must* be in the same region as the virtual machines.

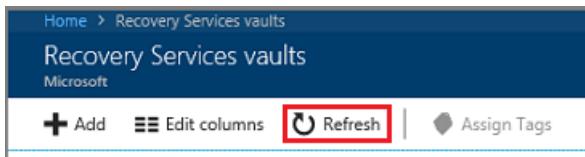
#### IMPORTANT

If you're not sure of the location of your VM, close the dialog box. Go to the list of virtual machines in the portal. If you have virtual machines in several regions, create a Recovery Services vault in each region. Create the vault in the first location, before you create the vault for another location. There's no need to specify storage accounts to store the backup data. The Recovery Services vault and Azure Backup handle that automatically.

5. When you're ready to create the Recovery Services vault, select **Create**.



It can take a while to create the Recovery Services vault. Monitor the status notifications in the **Notifications** area at the upper-right corner of the portal. After your vault is created, it's visible in the list of Recovery Services vaults. If you don't see your vault, select **Refresh**.



## Modify storage replication

By default, vaults use [geo-redundant storage \(GRS\)](#).

- If the vault is your primary backup mechanism, we recommend that you use GRS.
- You can use [locally redundant storage \(LRS\)](#) as a low-cost option.

To modify the storage replication type:

1. In the new vault, select **Properties** under the **Settings** section.
2. On the **Properties** page, under **Backup Configuration**, select **Update**.
3. Select the storage replication type, and select **Save**.

The screenshot shows the 'Demovault - Properties' page in the Azure portal. On the left, there's a sidebar with various options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (with Properties highlighted), Locks, Export template, Getting started (Backup and Site Recovery), Protected items (Backup items and Replicated items), Manage (Backup policies and Backup infrastructure), and Help & support. The main content area shows details for the vault, including Location (South Central US), Subscription Name (Backup PM Subscription), Subscription Id, Resource group (afstesting), and Diagnostic settings. Below these are sections for BACKUP (Backup Configuration and Update) and SECURITY SETTINGS (Update). At the top right, there's a 'Backup Configuration' dialog box with tabs for 'Locally-redundant' and 'Geo-redundant' (the latter is selected).

#### NOTE

You can't modify the storage replication type after the vault is set up and contains backup items. If you want to do this, you need to re-create the vault.

## Discover file shares and configure backup

1. In the [Azure portal](#), open the Recovery Services vault you want to use to back up the file share.
2. In the **Recovery Services vault** dashboard, select **+Backup**.

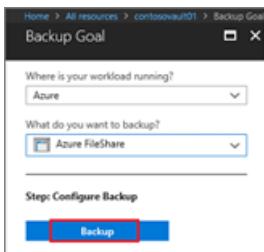
The screenshot shows the 'afstest' Recovery Services vault dashboard. It features a search bar, a top navigation bar with '+ Backup', '+ Replicate', 'Delete', and 'Refresh' buttons, and a 'Essentials' section. Below the navigation is an 'Overview' section.

- a. In **Backup Goal**, set **Where is your workload running?** to **Azure**.

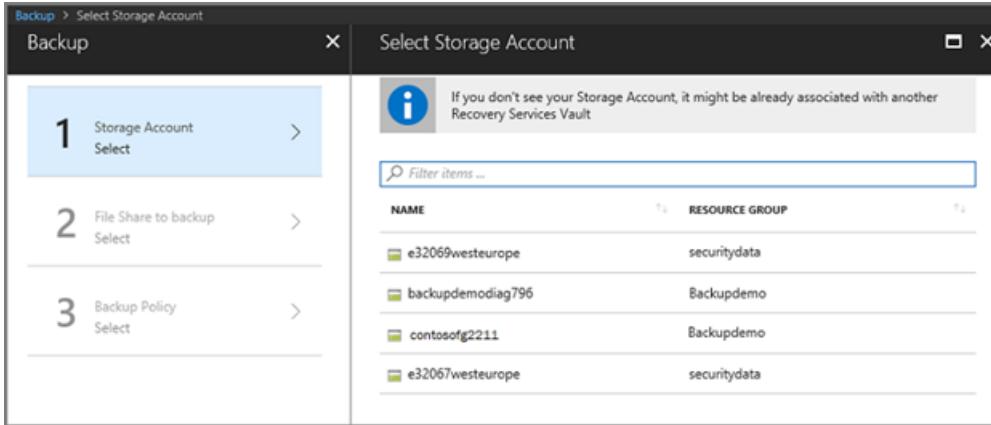
The screenshot shows the 'Backup Goal' dialog box. It asks 'Where is your workload running?' with a dropdown set to 'Azure'. It then asks 'What do you want to backup?' with a dropdown set to 'Virtual machine'. Below this, there's a list of options: 'Virtual machine' (selected), 'Azure FileShare' (highlighted with a red box), and 'SQL Server in Azure VM'. At the bottom is a 'Backup' button.

- b. In **What do you want to back up?**, select **Azure File Share** from the drop-down list.

- c. Select **Backup** to register the Azure file share extension in the vault.



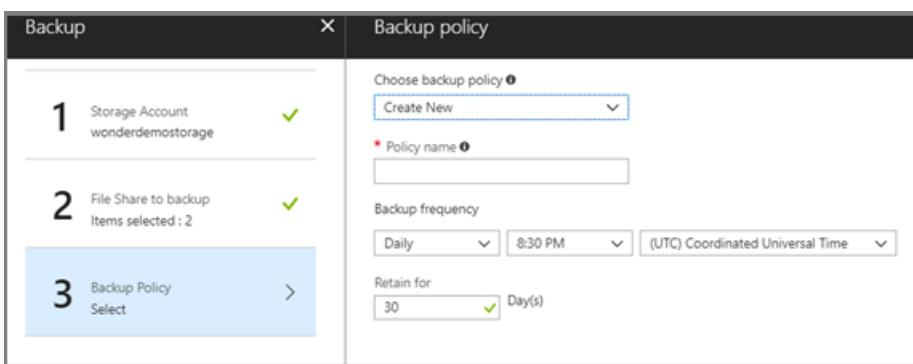
3. After you select **Backup**, the **Backup** pane opens and prompts you to select a storage account from a list of discovered supported storage accounts. They're either associated with this vault or present in the same region as the vault, but not yet associated to any Recovery Services vault.



4. From the list of discovered storage accounts, select an account, and select **OK**. Azure searches the storage account for file shares that can be backed up. If you recently added your file shares and don't see them in the list, allow some time for the file shares to appear.



5. From the **File Shares** list, select one or more of the file shares you want to back up. Select **OK**.
6. After you choose your file shares, the **Backup** menu switches to **Backup policy**. From this menu, either select an existing backup policy or create a new one. Then select **Enable Backup**.



After you set a backup policy, a snapshot of the file shares is taken at the scheduled time. The recovery point is also retained for the chosen period.

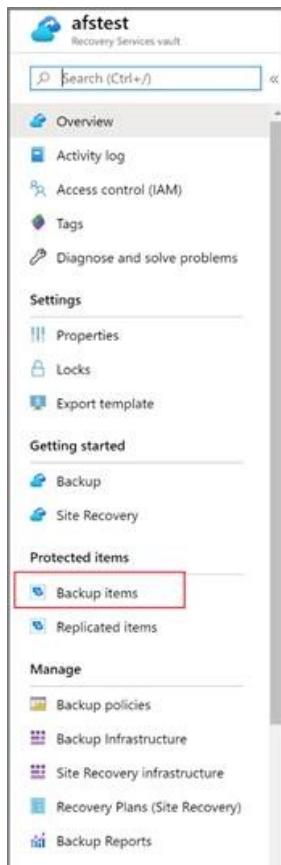
## Create an on-demand backup

Occasionally, you might want to generate a backup snapshot, or recovery point, outside of the times scheduled in the backup policy. A common reason to generate an on-demand backup is right after you've configured the backup policy. Based on the schedule in the backup policy, it might be hours or days until a snapshot is taken. To

protect your data until the backup policy engages, initiate an on-demand backup. Creating an on-demand backup is often required before you make planned changes to your file shares.

### Create a backup job on demand

1. Open the Recovery Services vault you used to back up your file share. On the **Overview** pane, select **Backup items** under the **Protected items** section.



2. After you select **Backup items**, a new pane that lists all **Backup Management Types** appears next to the **Overview** pane.

| Backup Items                |                   |
|-----------------------------|-------------------|
| Refresh                     |                   |
| BACKUP MANAGEMENT TYPE      | BACKUP ITEM COUNT |
| SQL in Azure VM             | 4                 |
| Azure Backup Server         | 3                 |
| Azure Storage (Azure Files) | 3                 |
| Azure Virtual Machine       | 1                 |
| Azure Backup Agent          | 1                 |

3. From the **Backup Management Type** list, select **Azure Storage (Azure Files)**. You'll see a list of all the file shares and the corresponding storage accounts backed up by using this vault.

| Backup Items (Azure Storage (Azure Files)) |                   |                |                    |                       |     |     |
|--------------------------------------------|-------------------|----------------|--------------------|-----------------------|-----|-----|
| WonderDemoVault                            |                   |                |                    |                       |     |     |
| Refresh                                    | Add               | Filter         |                    |                       |     |     |
| Fetching data from service completed.      |                   |                |                    |                       |     |     |
| NAME                                       | STORAGE ACCOUNT   | RESOURCE GROUP | LAST BACKUP STATUS | LAST BACKUP TIME      | ... | ... |
| batshare                                   | wonderdemostorage | wonderdemorg   | Success            | 15/2/2018, 6:02:58 AM | ... | ... |
| flashshare                                 | wonderdemostorage | wonderdemorg   | Success            | 15/2/2018, 6:02:55 AM | ... | ... |

4. From the list of Azure file shares, select the file share you want. The **Backup Item** details appear. On the **Backup Item** menu, select **Backup now**. Because this backup job is on demand, there's no retention policy associated with the recovery point.

The screenshot shows the Azure portal interface for managing backup items. The current path is: Dashboard > - Backup items > Backup Items (Azure Storage (Azure Files)) > dc-tileshare. The page title is 'Wonderdemo' and the sub-page title is 'Backup Item'. Below the title, there are several buttons: 'Backup now' (highlighted with a red box), 'Restore Share', 'File Recovery', 'Resume backup', 'Stop backup', and 'Delete backup data'. A 'Essentials' section displays the following information:

|                                     |                                         |
|-------------------------------------|-----------------------------------------|
| Recovery services vault test:       | Last backup status Success              |
| Subscription name Subscription Name | Last backup time 9/18/2019, 10:00:41 AM |
| Subscription ID                     | Backup policy                           |
| Subscription ID                     | FileSharePolicy                         |
| Item type                           |                                         |
| Azure File Share                    |                                         |
| Storage Account Wonderdemostorage   |                                         |

5. The **Backup Now** pane opens. Specify the last day you want to retain the recovery point. You can have a maximum retention of 10 years for an on-demand backup.



6. Select **OK** to confirm the on-demand backup job that runs.  
7. Monitor the portal notifications to keep a track of backup job run completion. You can monitor the job progress in the vault dashboard. Select **Backup Jobs > In progress**.

## Next steps

Learn how to:

- [Restore Azure file shares](#)
- [Manage Azure file share backups](#)

# Restore Azure file shares

2/24/2020 • 5 minutes to read • [Edit Online](#)

This article explains how to use the Azure portal to restore an entire file share or specific files from a restore point created by [Azure Backup](#).

In this article, you'll learn how to:

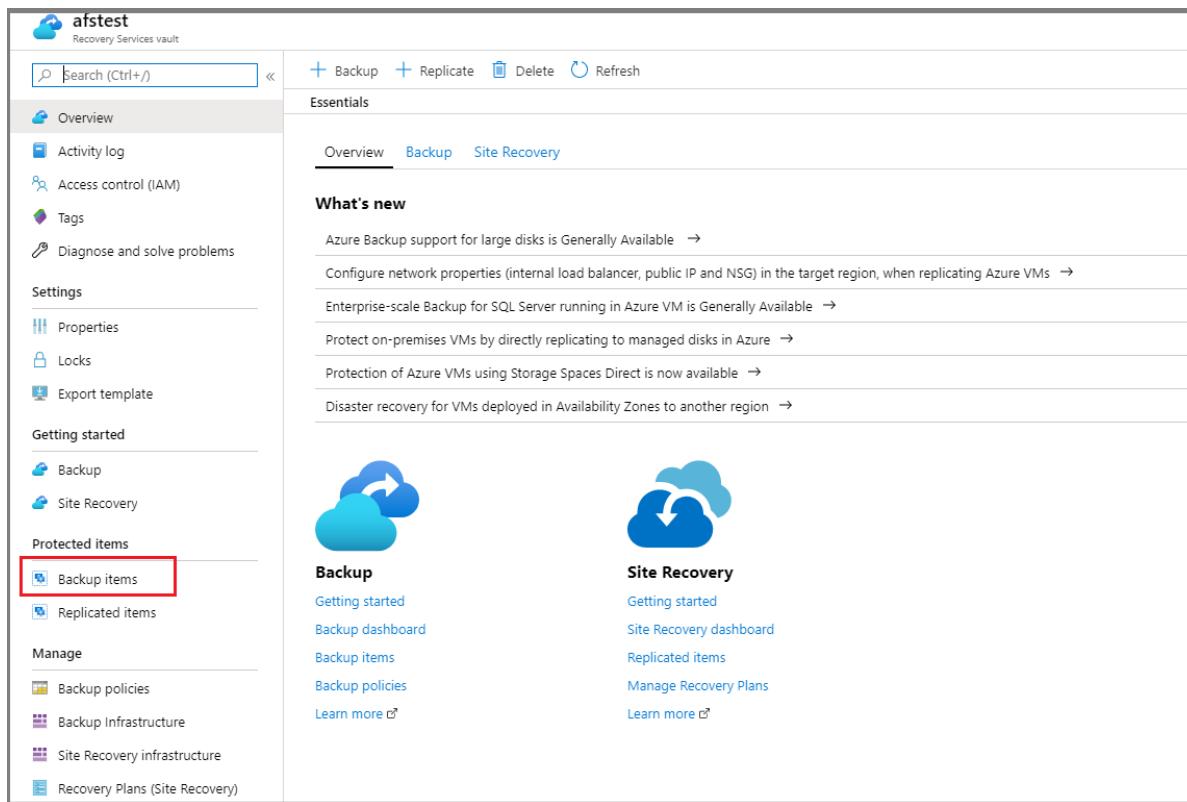
- Restore a full Azure file share.
- Restore individual files or folders.
- Track the restore operation status.

## Steps to perform a restore operation

To perform a restore operation, follow these steps.

### Select the file share to restore

1. In the [Azure portal](#), open the Recovery Services vault you used to configure backup for the file share.
2. In the overview pane, select **Backup items** under the **Protected items** section.



3. After you select **Backup items**, a new pane that lists all backup management types opens next to the overview pane.

4. In the **Backup Items** pane, under **Backup Management Type**, select **Azure Storage (Azure Files)**.

You'll see a list of all the file shares and their corresponding storage accounts backed up by using this vault.

5. From the list of Azure file shares, select the file share for which you want to perform the restore operation.

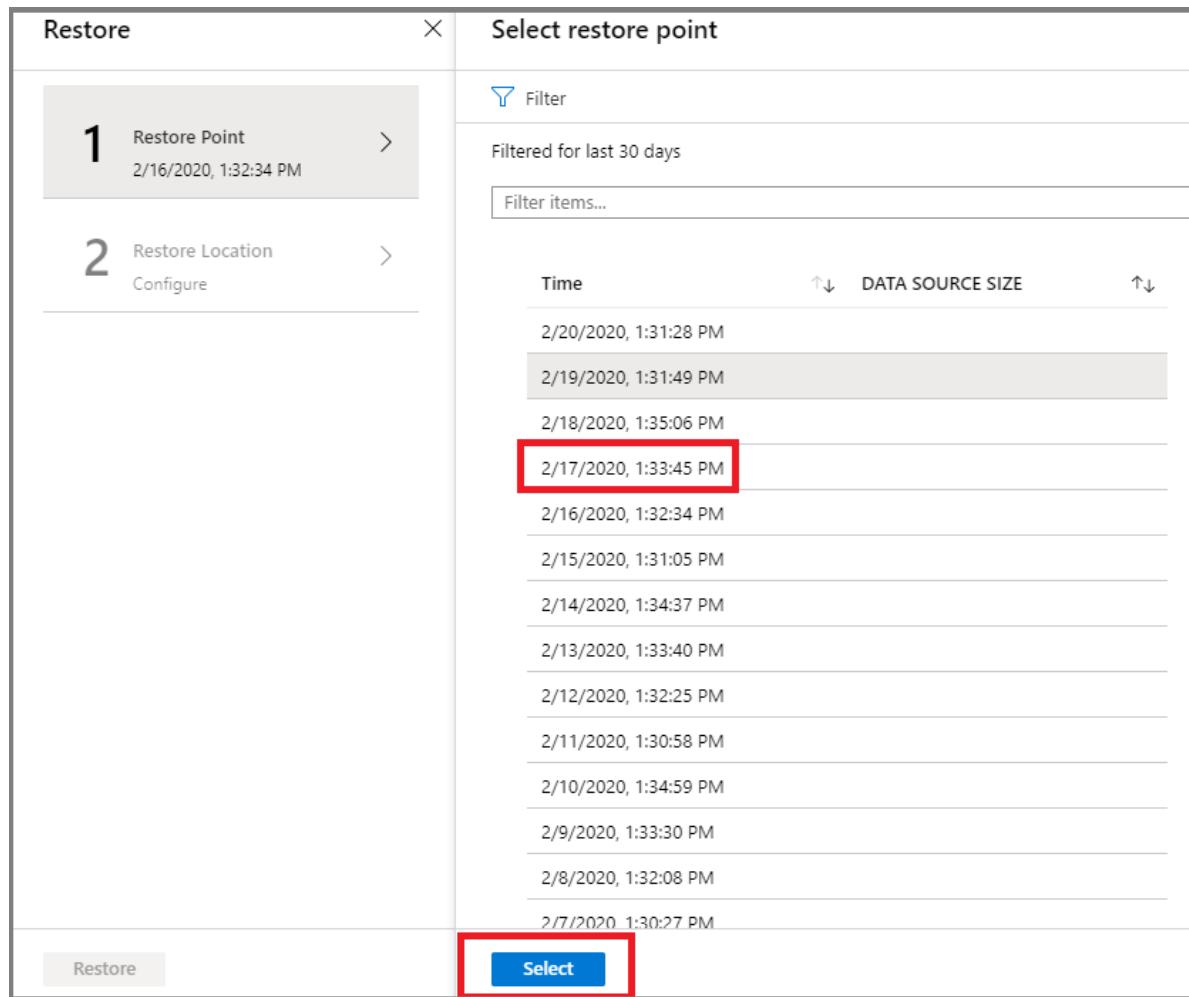
### Full share recovery

You can use this restore option to restore the complete file share in the original location or an alternate location.

1. Select the **Restore Share** option in the **Backup Item** pane that appears after you selected the file share to restore in step 5 of the [Select the file share to restore](#) section.

2. After you select **Restore Share**, the **Restore** pane opens with a **Restore Point** menu that displays a list of restore points available for the selected file share.

3. Select the restore point you want to use to perform the restore operation, and select **OK**.

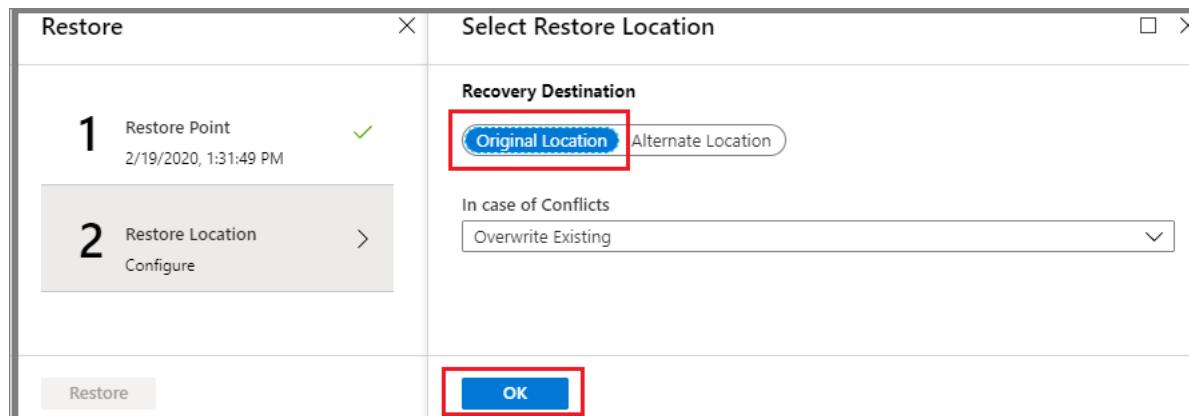


4. After you select **OK**, the **Restore** pane menu switches to **Restore Location**. In **Restore Location**, specify where or how to restore the data. Select one of the following two options:

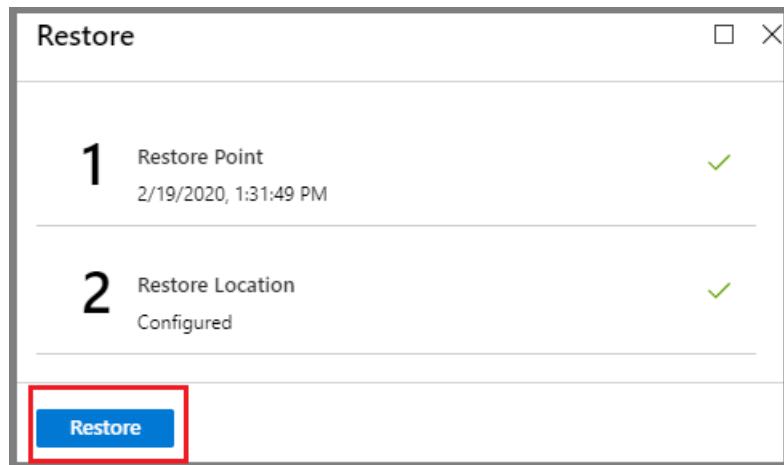
- **Original Location:** Restore the complete file share to the same location as the original source.
- **Alternate Location:** Restore the complete file share to an alternate location and keep the original file share as is.

#### Restore to the original location

1. Select **Original Location** as the **Recovery Destination**, and select whether to skip or overwrite if there are conflicts. After you make the appropriate selection, select **OK**.

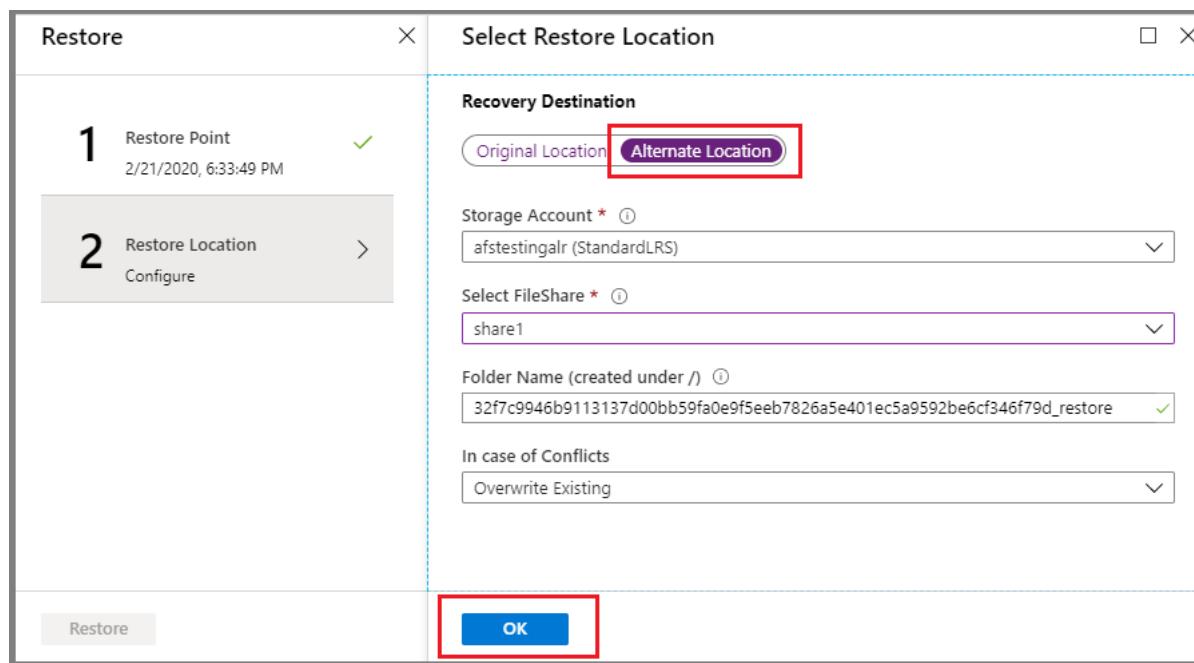


2. Select **Restore** to start the restore operation.

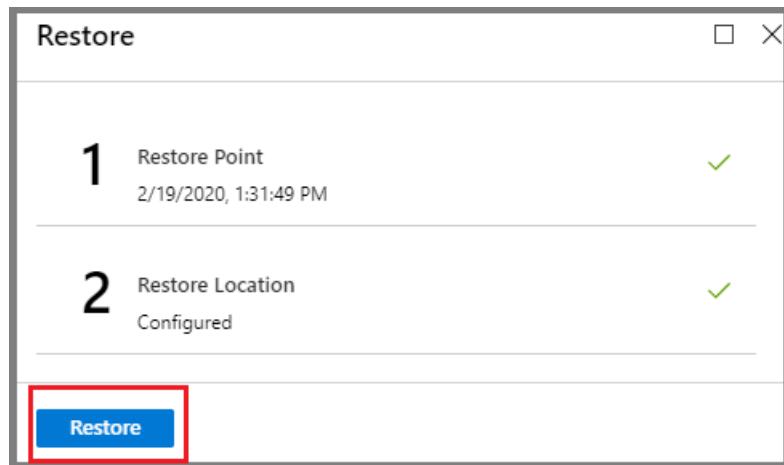


#### Restore to an alternate location

1. Select **Alternate Location** as the **Recovery Destination**.
2. Select the destination storage account where you want to restore the backed-up content from the **Storage Account** drop-down list.
3. The **Select File Share** drop-down list displays the file shares present in the storage account you selected in step 2. Select the file share where you want to restore the backed-up contents.
4. In the **Folder Name** box, specify a folder name you want to create in the destination file share with the restored contents.
5. Select whether to skip or overwrite if there are conflicts.
6. After you enter the appropriate values in all boxes, select **OK**.



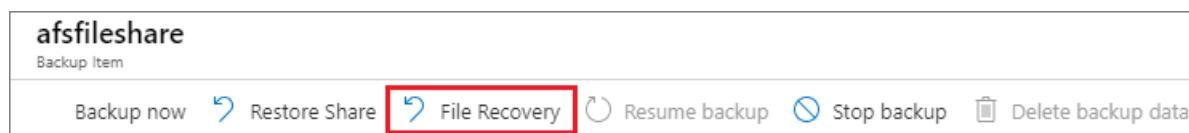
7. Select **Restore** to start the restore operation.



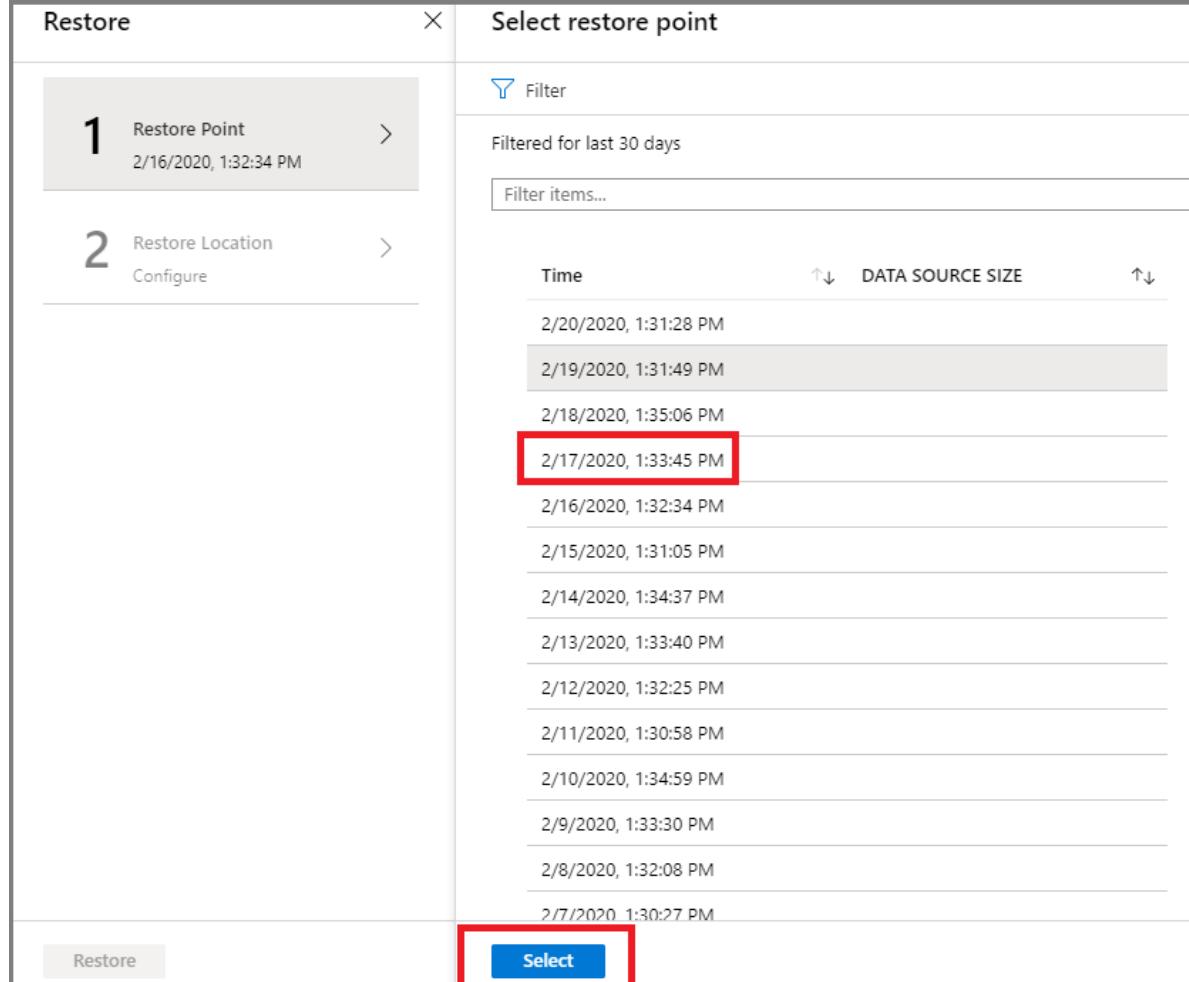
### Item-level recovery

You can use this restore option to restore individual files or folders in the original location or an alternate location.

1. Select the **File Recovery** option in the **Backup Item** pane that appears after you selected the file share to restore in step 5 of the [Select the file share to restore](#) section.



2. After you select **File Recovery**, the **Restore** pane opens with a **Restore point** menu that displays a list of restore points available for the selected file share.
3. Select the restore point you want to use to perform the restore operation, and select **OK**.

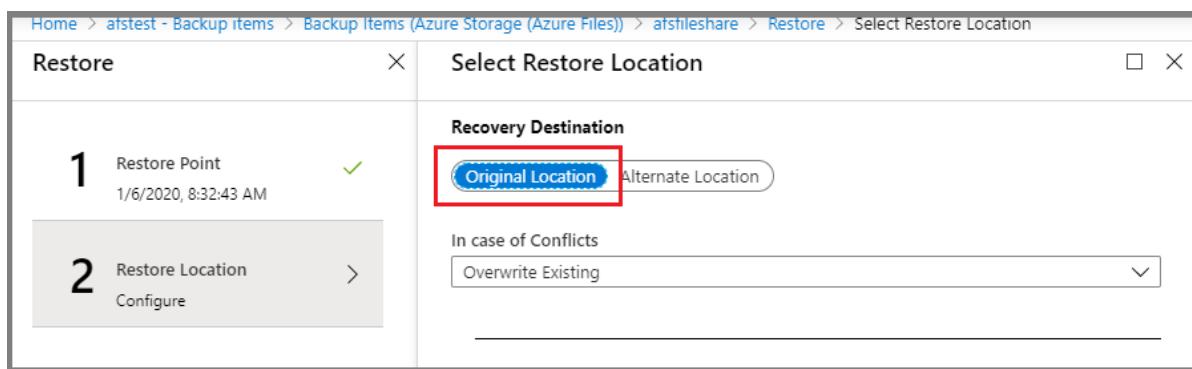


4. After you select **OK**, the restore pane menu switches to **Restore Location**. In **Restore Location**, specify where or how to restore the data. Select one of the following two options:

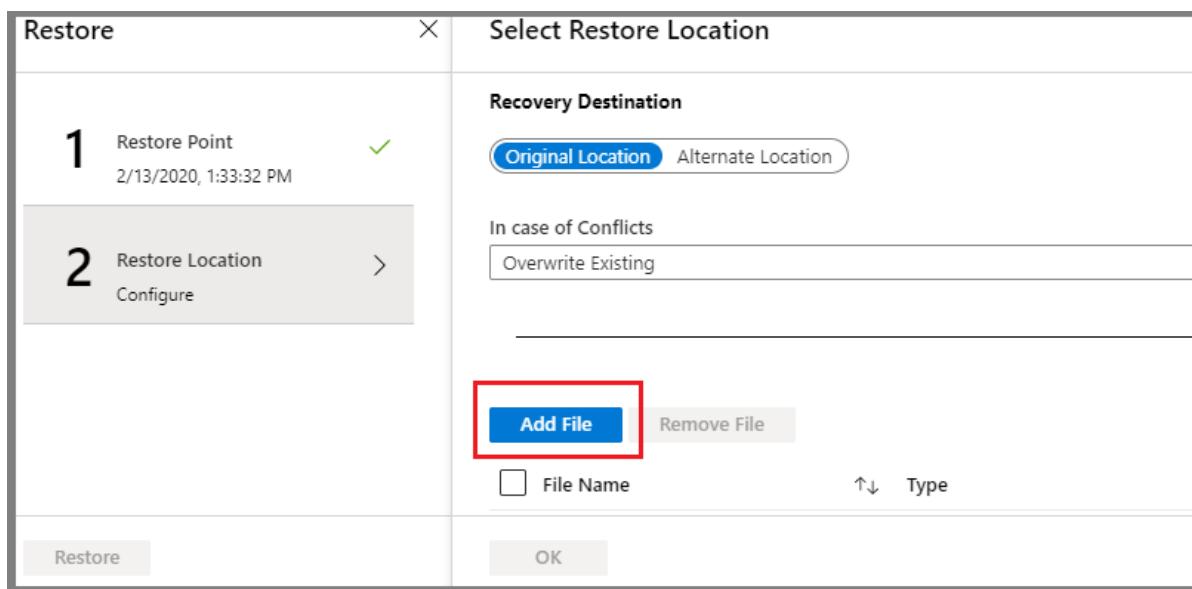
- **Original Location:** Restore selected files or folders to the same file share as the original source.
- **Alternate Location:** Restore selected files or folders to an alternate location and keep the original file share contents as is.

#### Restore to the original location

1. Select **Original Location** as the **Recovery Destination**, and select whether to skip or overwrite if there are conflicts.

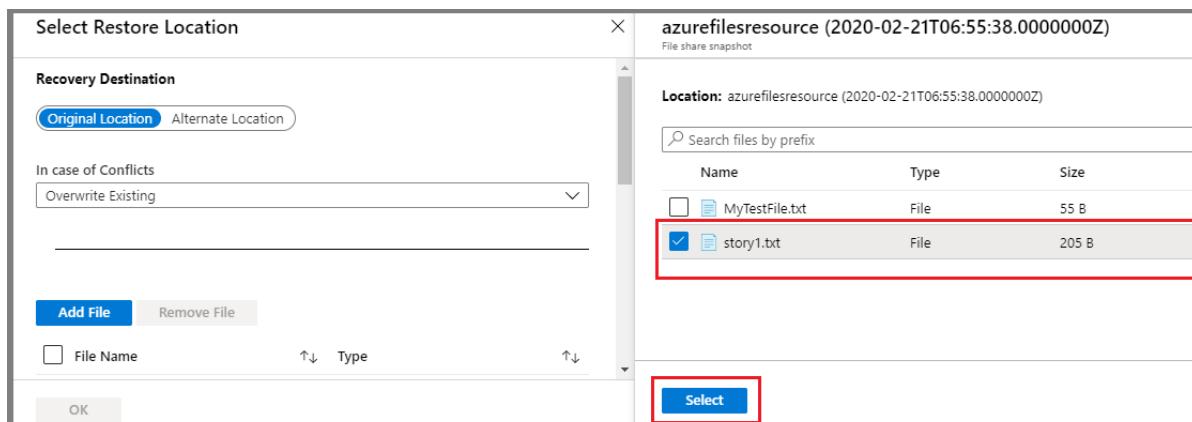


2. Choose **Select File** to select the files or folders you want to restore.



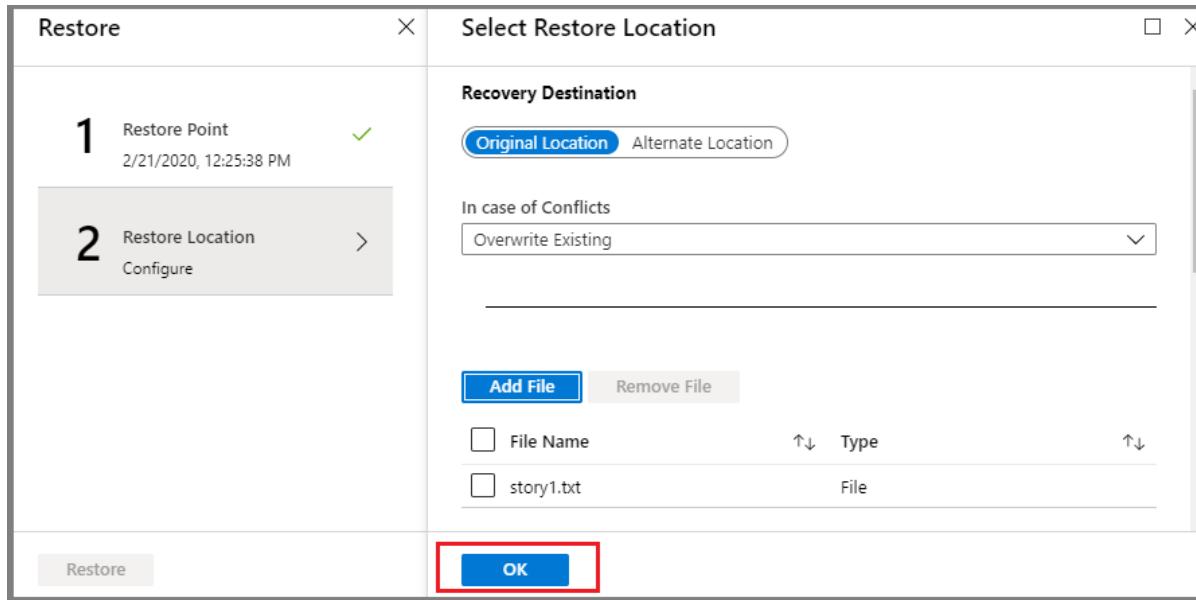
3. After you choose **Select File**, a file share pane displays the contents of the file share recovery point you selected for restore.

4. Select the check box that corresponds to the file or folder you want to restore, and choose **Select**.

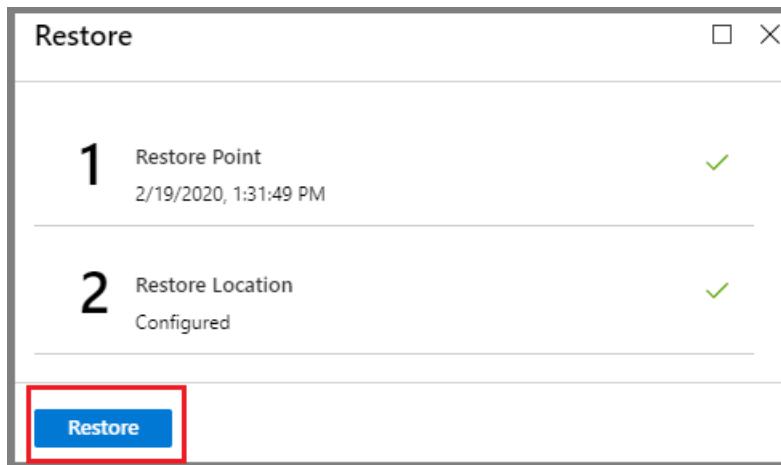


5. Repeat steps 2 through 4 to select multiple files or folders for restore.

6. After you select all the items you want to restore, select **OK**.

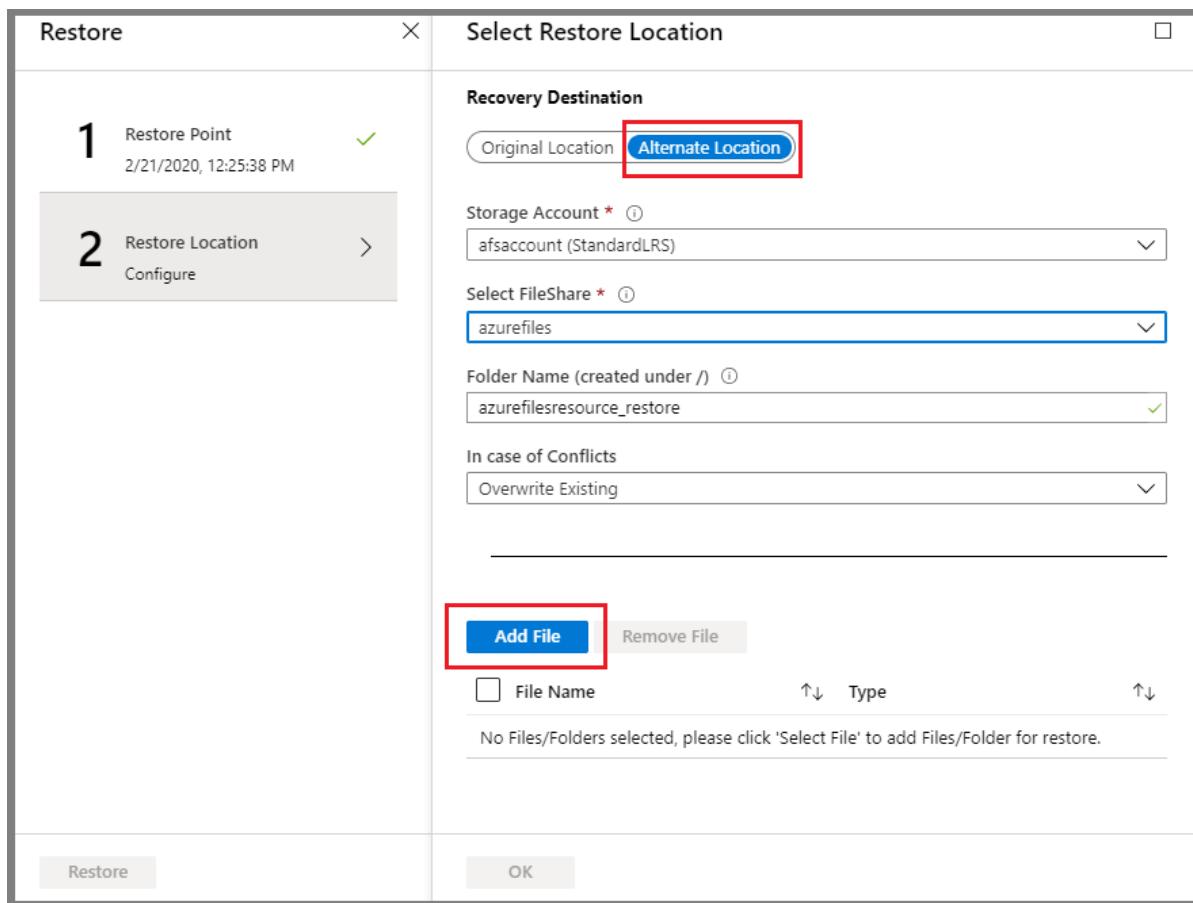


7. Select **Restore** to start the restore operation.

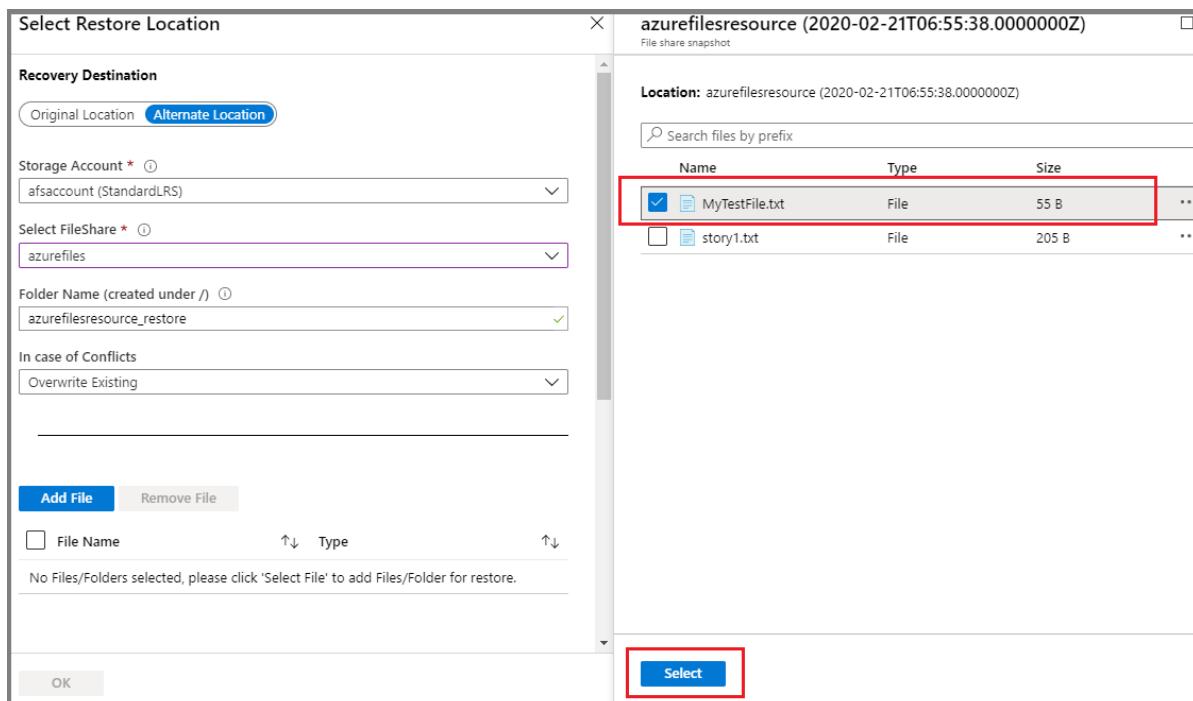


#### Restore to an alternate location

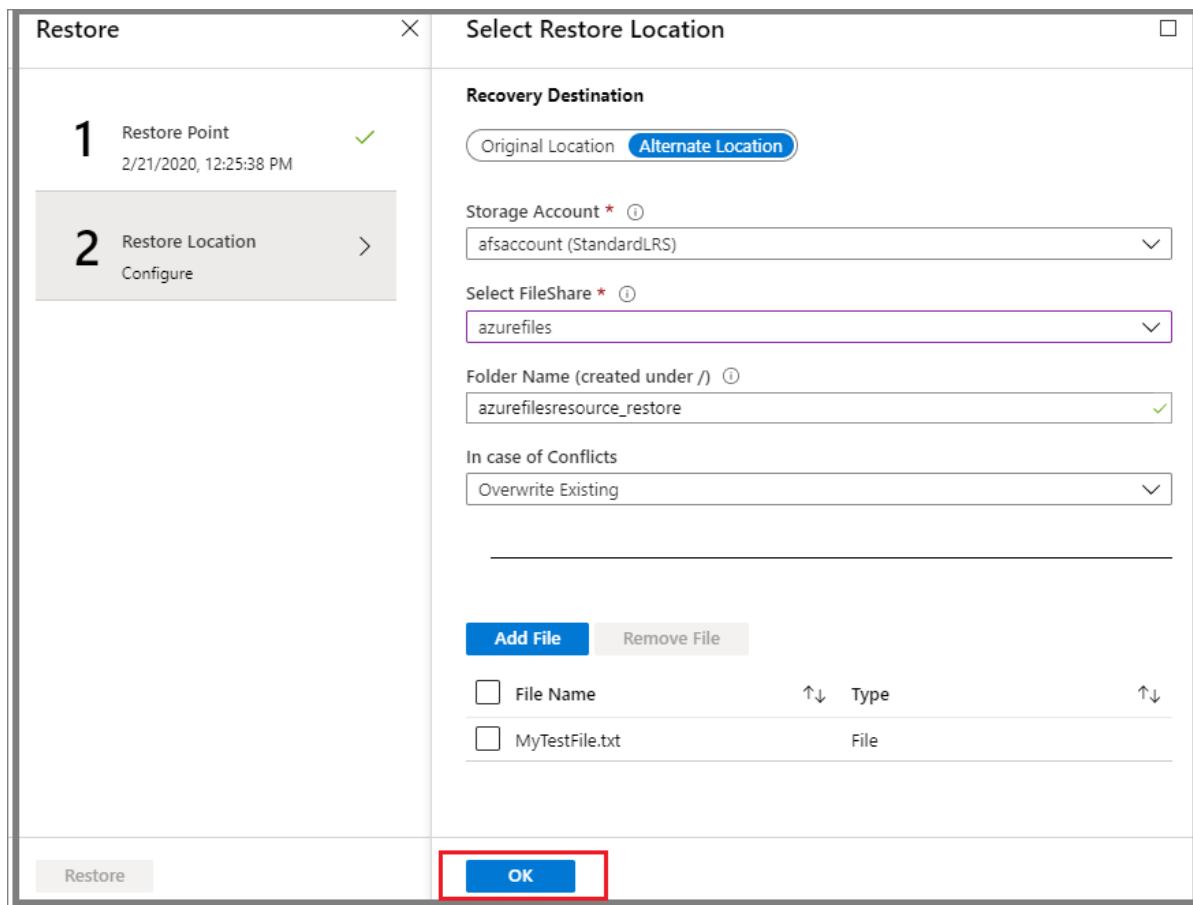
1. Select **Alternate Location** as the **Recovery Destination**.
2. Select the destination storage account where you want to restore the backed-up content from the **Storage Account** drop-down list.
3. The **Select File Share** drop-down list displays the file shares present in the storage account you selected in step 2. Select the file share where you want to restore the backed-up contents.
4. In the **Folder Name** box, specify a folder name you want to create in the destination file share with the restored contents.
5. Select whether to skip or overwrite if there are conflicts.
6. Choose **Select File** to select the files or folders you want to restore.



7. When you choose **Select File**, a file share pane displays the contents of the file share recovery point you selected for restore.
8. Select the check box that corresponds to the file or folder you want to restore, and choose **Select**.



9. Repeat steps 6 through 8 to select multiple files or folders for restore.
10. After you select all the items you want to restore, select **OK**.



11. Select **Restore** to start the restore operation.

## Track a restore operation

After you trigger the restore operation, the backup service creates a job for tracking. Azure Backup displays notifications about the job in the portal. To view operations for the job, select the notifications hyperlink.

You can also monitor restore progress from the Recovery Services vault:

1. Open the Recovery Services vault from where you triggered the restore operation.
2. In the overview pane, select **Backup Jobs** under the **Monitoring** section to see the status of operations running against different workloads.

Home > afstest - Backup Jobs

**afstest - Backup Jobs**

Recovery Services vault

Diagnose and solve problems

Settings

- Properties
- Locks
- Export template

Getting started

- Backup
- Site Recovery

Protected items

- Backup items
- Replicated items

Manage

- Backup policies
- Backup Infrastructure
- Site Recovery infrastructure
- Recovery Plans (Site Recovery)
- Backup Reports

Monitoring

- Alerts
- Diagnostic settings

Backup Jobs

Choose columns Filter Export jobs Refresh View jobs in secondary region

Filtered by: Item Type - All item types, Operation - All Operations, Status - All Status, Start Time - 1/7/2020, 7:17:41 PM, End Time - 1/8/2020, 7:17:41 PM

(i) Completed fetching data from the service.

Filter items...

| Workload name              | Operation      | Status    | Type         | Start time           | Duration |
|----------------------------|----------------|-----------|--------------|----------------------|----------|
| afsfileshare(filesync2901) | Restore        | Completed | AzureStorage | 1/8/2020, 5:56:51 PM | 00:02:21 |
| test1(filesync2901)        | Disable backup | Completed | AzureStorage | 1/8/2020, 4:33:19 PM | 00:00:46 |
| test1(filesync2901)        | Backup         | Completed | AzureStorage | 1/8/2020, 4:30:30 PM | 00:01:51 |
| afsfileshare(filesync2901) | Backup         | Completed | AzureStorage | 1/8/2020, 8:30:07 AM | 00:00:55 |

3. Select the workload name that corresponds to your file share to view more details about the restore operation, like **Data Transferred** and **Number of Restored Files**.

Restore  
afsfileshare(filesync2901)

Cancel  Deploy Template

Job Details

|                             |                                                               |
|-----------------------------|---------------------------------------------------------------|
| Source File Share Name      | afsfileshare                                                  |
| Source Storage Account Name | filesync2901                                                  |
| RestoreRecoveryPointTime    | 1/6/2020 3:03:15 AM                                           |
| Target File Share Name      | afsfileshare                                                  |
| Target Storage Account Name | filesync2901                                                  |
| Job Type                    | Recover to an alternate file share                            |
| RestoreDestination          | filesync2901/afsfileshare/afsfileshare_restore                |
| Data Transferred (in MB)    | 3                                                             |
| Number Of Restored Files    | 1                                                             |
| Number Of Skipped Files     | 0                                                             |
| Number Of Failed Files      | 0                                                             |
| Activity ID                 | 3f2818c9-5902-461f-b352-9ca134b6f049-2020-01-08T12:26:50Z-lbz |

## Next steps

- Learn how to [Manage Azure file share backups](#).

# Manage Azure file share backups

1/31/2020 • 5 minutes to read • [Edit Online](#)

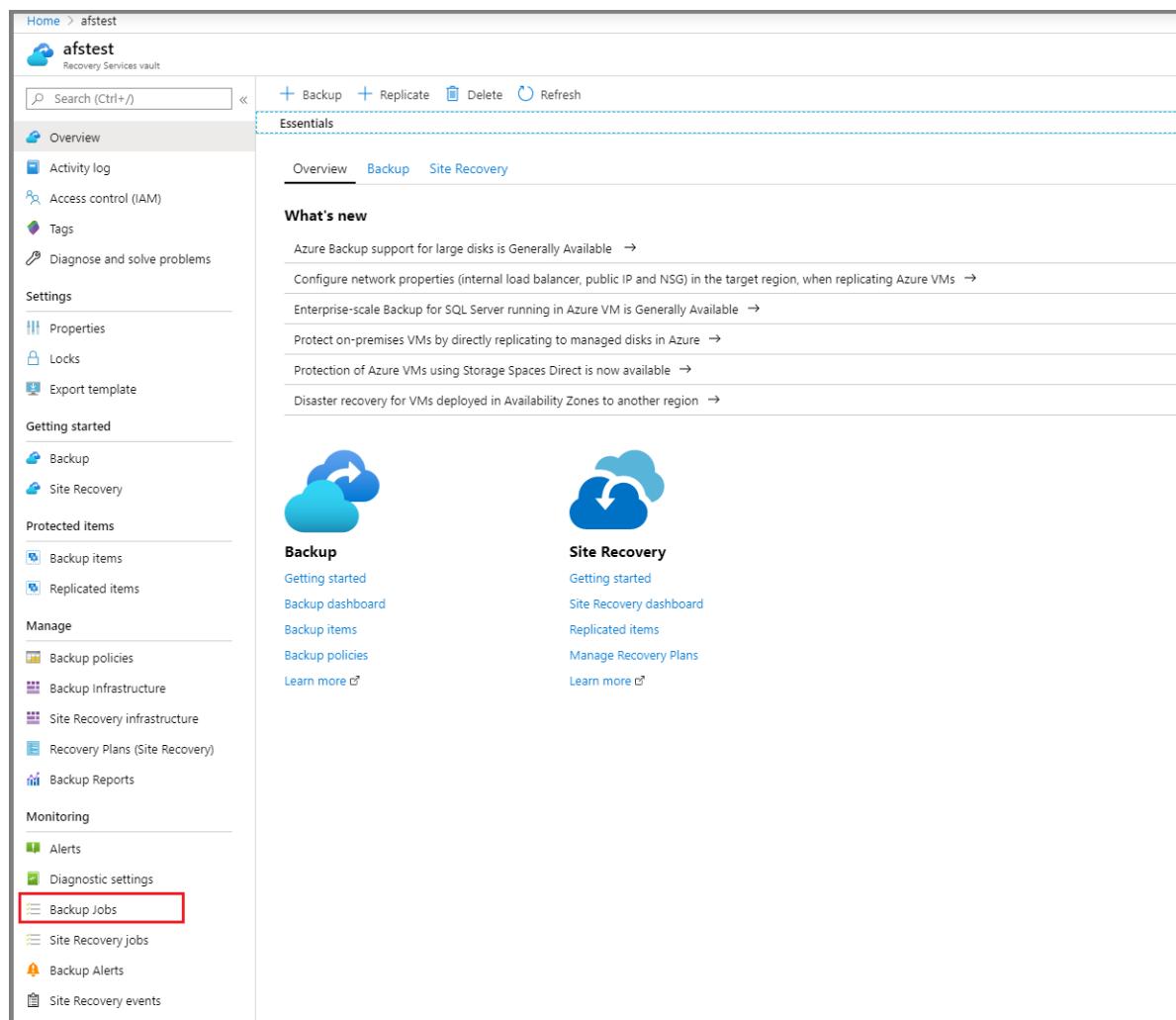
This article describes common tasks for managing and monitoring the Azure file shares that are backed up by [Azure Backup](#). You'll learn how to do management tasks in the Recovery Services vault.

## Monitor jobs

When you trigger a backup or restore operation, the backup service creates a job for tracking. You can monitor the progress of all jobs on the **Backup Jobs** page.

To open the **Backup Jobs** page:

1. Open the Recovery Services vault you used to configure backup for your file shares. In the **Overview** pane, select **Backup Jobs** under the **Monitoring** section.



2. After you select **OK**, the **Backup Jobs** pane lists the status of all jobs. Select the workload name that corresponds to the file share you want to monitor.

The screenshot shows the 'Backup Jobs' section of the 'afstest - Backup Jobs' page. On the left, there's a navigation menu with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Properties, and Locks. The main area displays a table of backup jobs. The table has columns: Workload name, Operation, Status, Type, Start time, Duration, and three dots for more options. Two rows are shown: 'afsfileshare(filesync2901)' and 'test1(filesync2901)', both of which are completed backups to Azure Storage.

## Create a new policy

You can create a new policy to back up Azure file shares from the **Backup policies** section of the Recovery Services vault. All policies created when you configured backup for file shares show up with the **Policy Type** as **Azure File Share**.

To view the existing backup policies:

1. Open the Recovery Services vault you used to configure the backup for the file share. On the Recovery Services vault menu, select **Backup policies** under the **Manage** section. All the backup policies configured in the vault appear.

The screenshot shows the 'Backup policies' section of the 'afstest - Backup policies' page. On the left, there's a navigation menu with sections like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Properties, Locks, Export template, Getting started (Backup, Site Recovery), Protected items (Backup items, Replicated items), and Manage (Backup policies, Backup Infrastructure, Site Recovery infrastructure, Recovery Plans (Site Recovery)). The 'Backup policies' item is highlighted with a red box. The main area displays a table of backup policies. The table has columns: Name, Policy Type, and three dots for more options. Four policies are listed: 'HourlyLogBackup' (SQL Server in Azure VM), 'Schedule2' (Azure File Share), 'DefaultPolicy' (Azure Virtual Machine), and 'Schedule1' (Azure File Share).

2. To view policies specific to **Azure File Share**, select **Azure File Share** from the drop-down list on the upper right.

The screenshot shows the 'Backup policies' pane in the Azure portal. On the left, there's a navigation menu with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Properties, Locks, Export template, Getting started (Backup, Site Recovery), Protected items (Backup items, Replicated items), and Manage (Backup policies, Backup Infrastructure, Site Recovery infrastructure, Recovery Plans (Site Recovery), Backup Reports). The 'Backup policies' item is selected. On the right, there's a search bar and a list of policy types. A red box highlights the 'Azure File Share' option in the list.

To create a new backup policy:

1. In the **Backup policies** pane, select **+ Add**.

The screenshot shows the 'Backup policies' pane in the Azure portal. The left navigation menu is identical to the previous screenshot. The right pane displays a list of existing backup policies. A red box highlights the '+ Add' button at the top. Another red box highlights the 'Backup policies' item in the Manage section of the left menu. The table lists five policies:

| Name            | Policy Type            | Actions |
|-----------------|------------------------|---------|
| HourlyLogBackup | SQL Server in Azure VM | ...     |
| Schedule2       | Azure File Share       | ...     |
| DefaultPolicy   | Azure Virtual Machine  | ...     |
| Schedule1       | Azure File Share       | ...     |

2. In the **Add** pane, select **Azure File Share** as the **Policy Type**. The **Backup policy** pane for **Azure File Share** opens. Specify the policy name, backup frequency, and retention range for the recovery points. After you define the policy, select **OK**.

Home > afstest - Backup policies > Add > Backup policy

| Add                                                                                                                                      | Backup policy                                                                                                                                   |
|------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Policy Type</p> <p>Azure Virtual Machine</p> <p><b>Azure File Share</b></p> <p>SQL Server in Azure VM</p> <p>SAP HANA in Azure VM</p> | <p>Policy name * ⓘ<br/>Scheduled</p> <p>Backup schedule<br/>Daily 8:30 AM (UTC) Coordinated Universal Ti...</p> <p>Retain for<br/>30 Day(s)</p> |
| <b>OK</b>                                                                                                                                |                                                                                                                                                 |

## Modify policy

You can modify a backup policy to change the backup frequency or retention range.

To modify a policy:

1. Open the Recovery Services vault you used to configure the backup for the file share. On the Recovery Services vault menu, select **Backup policies** under the **Manage** section. All the backup policies configured in the vault appear.

| Name            | Schedule      | Policy Type            |
|-----------------|---------------|------------------------|
| HourlyLogBackup | Schedule2     | SQL Server in Azure VM |
| Schedule2       | DefaultPolicy | Azure File Share       |
| DefaultPolicy   | Schedule1     | Azure Virtual Machine  |
| Schedule1       |               | Azure File Share       |

2. To view policies specific to an Azure file share, select **Azure File Share** from the drop-down list on the upper right. Select the backup policy you want to modify.

| Name      | Schedule | Policy Type            |
|-----------|----------|------------------------|
| Schedule2 | All      | Azure Virtual Machine  |
| Schedule1 | All      | SQL Server in Azure VM |
|           | All      | SAP HANA in Azure VM   |
|           | All      | Azure File Share       |

3. The **Schedule** pane opens. Edit the **Backup schedule** and **Retention range** as required, and select **Save**. You'll see an "Update in Progress" message in the pane. After the policy changes update successfully, you'll see the message "Successfully updated the backup policy."

The screenshot shows the 'Schedule2' configuration page for backup policies. At the top, there are buttons for 'Associated items', 'Delete', 'Discard', and 'Save'. The 'Save' button is highlighted with a red box. Below this, there's a section for the 'Backup schedule' with dropdowns for 'Daily', '11:00 AM', and '(UTC) Coordinated Universal Ti...'. Under 'Retention range', it says 'Retain for 20 Day(s)'.

## Stop protection on a file share

There are two ways to stop protecting Azure file shares:

- Stop all future backup jobs, and *delete all recovery points*.
- Stop all future backup jobs, but *leave the recovery points*.

There might be a cost associated with leaving the recovery points in storage, because the underlying snapshots created by Azure Backup will be retained. The benefit of leaving the recovery points is that you can restore the file share later. For information about the cost of leaving the recovery points, see the [pricing details](#). If you decide to delete all the recovery points, you can't restore the file share.

To stop protection for an Azure file share:

1. Open the Recovery Services vault that contains the file share recovery points. Select **Backup Items** under the **Protected Items** section. The list of backup item types appears.

| BACKUP MANAGEMENT TYPE      | BACKUP ITEM COUNT |
|-----------------------------|-------------------|
| SQL in Azure VM             | 4                 |
| Azure Backup Server         | 3                 |
| Azure Storage (Azure Files) | 3                 |
| Azure Virtual Machine       | 1                 |
| Azure Backup Agent          | 1                 |

2. In the **Backup Management Type** list, select **Azure Storage (Azure Files)**. The **Backup Items (Azure Storage (Azure Files))** list appears.

| Name             | Storage Account | Resource Group | Last Backup Status | Last Backup Time     | ... |
|------------------|-----------------|----------------|--------------------|----------------------|-----|
| afstestfileshare | filesync2901    | afstesting     | Success            | 1/8/2020, 8:30:07 AM | ... |
| test1            | filesync2901    | afstesting     | Success            | 1/7/2020, 4:33:08 PM | ... |

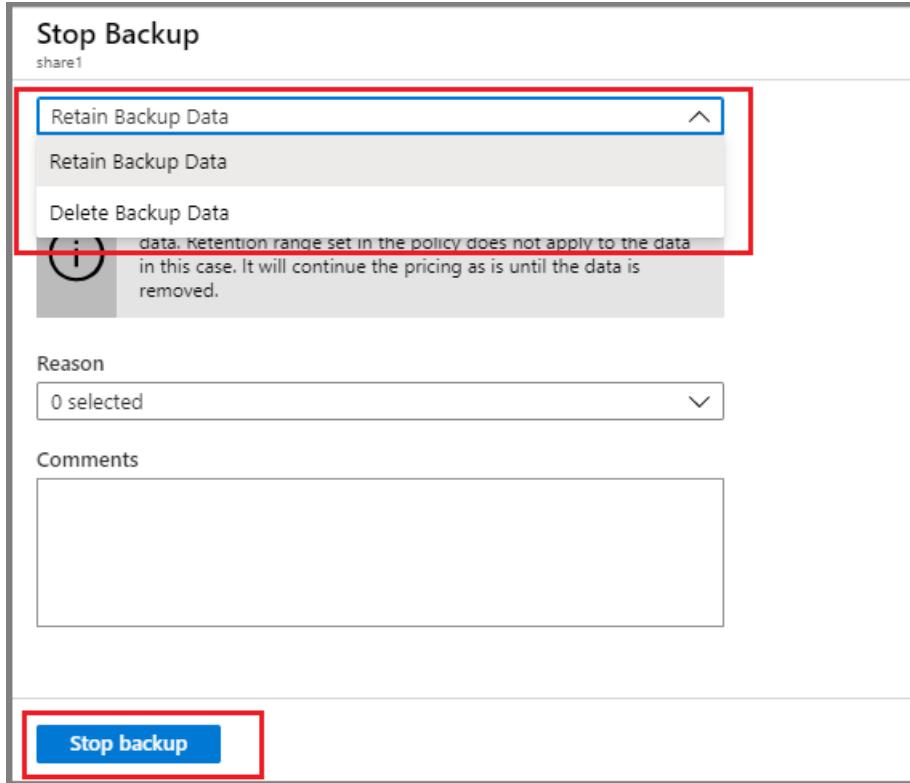
3. In the **Backup Items (Azure Storage (Azure Files))** list, select the backup item for which you want to

stop protection.

4. Select the **Stop backup** option.



5. In the **Stop Backup** pane, select **Retain Backup Data** or **Delete Backup Data**. Then select **Stop backup**.

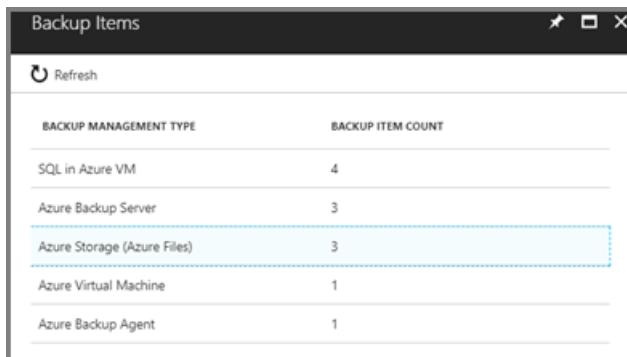


## Resume protection on a file share

If the **Retain Backup Data** option was selected when protection for the file share was stopped, it's possible to resume protection. If the **Delete Backup Data** option was selected, protection for the file share can't resume.

To resume protection for the Azure file share:

1. Open the Recovery Services vault that contains the file share recovery points. Select **Backup Items** under the **Protected Items** section. The list of backup item types appears.



2. In the **Backup Management Type** list, select **Azure Storage (Azure Files)**. The **Backup Items (Azure Storage (Azure Files))** list appears.

| Name         | Storage Account | Resource Group | Last Backup Status | Last Backup Time     |
|--------------|-----------------|----------------|--------------------|----------------------|
| afsfileshare | filesync2901    | afstesting     | Success            | 1/8/2020, 8:30:07 AM |
| test1        | filesync2901    | afstesting     | Success            | 1/7/2020, 4:33:08 PM |

3. In the **Backup Items (Azure Storage (Azure Files))** list, select the backup item for which you want to resume protection.

4. Select the **Resume backup** option.

5. The **Backup Policy** pane opens. Select a policy of your choice to resume backup.

6. After you select a backup policy, select **Save**. You'll see an "Update in Progress" message in the portal. After the backup successfully resumes, you'll see the message "Successfully updated backup policy for the Protected Azure File Share."

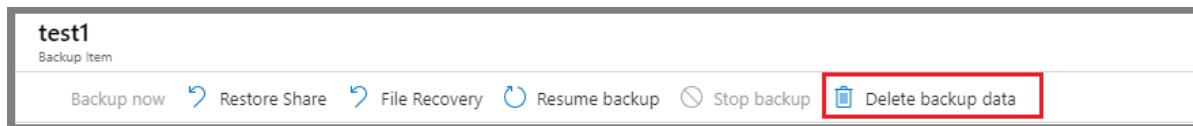
## Delete backup data

You can delete the backup of a file share during the **Stop backup** job, or any time after you stop protection. It might be beneficial to wait days or even weeks before you delete the recovery points. When you delete backup data, you can't choose specific recovery points to delete. If you decide to delete your backup data, you delete all recovery points associated with the file share.

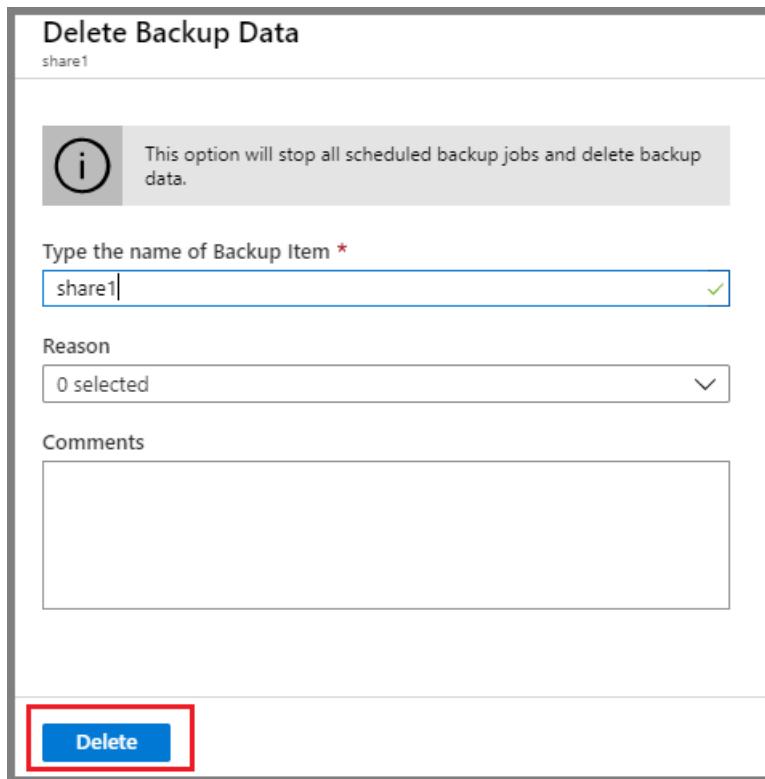
The following procedure assumes that the protection was stopped for the file share.

To delete backup data for the Azure file share:

1. After the backup job is stopped, the **Resume backup** and **Delete backup data** options are available in the **Backup Item** dashboard. Select the **Delete backup data** option.



2. The **Delete Backup Data** pane opens. Enter the name of the file share to confirm deletion. Optionally, provide more information in the **Reason** or **Comments** boxes. After you're sure about deleting the backup data, select **Delete**.



## Unregister a storage account

To protect your file shares in a particular storage account by using a different recovery services vault, first [stop protection for all file shares](#) in that storage account. Then unregister the account from the current recovery services vault used for protection.

The following procedure assumes that the protection was stopped for all file shares in the storage account you want to unregister.

To unregister the storage account:

1. Open the Recovery Services vault where your storage account is registered.
2. On the **Overview** pane, select the **Backup Infrastructure** option under the **Manage** section.

The screenshot shows the Azure Backup service interface for a vault named 'azurefilesvault'. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Properties, Locks, Export template), Getting started (Backup, Site Recovery), Protected Items (Backup items, Replicated items), Manage (Backup policies, Backup Infrastructure, Site Recovery infrastructure, Recovery Plans (Site Recovery), Backup Reports). The 'Backup Infrastructure' link is highlighted with a red box. The main content area shows 'What's new' with several bullet points about backup support for large disks, network properties, enterprise-scale backup for SQL Server, protecting on-premises VMs, protection of Azure VMs using Storage Spaces Direct, and disaster recovery for VMs in Availability Zones. Below this are two sections: 'Backup' and 'Site Recovery', each with their own 'Getting started', 'Backup dashboard', 'Backup items', 'Backup policies', and 'Learn more' links.

3. The **Backup Infrastructure** pane opens. Select **Storage Accounts** under the **Azure Storage Accounts** section.

The screenshot shows the 'Backup Infrastructure - Storage Accounts' page for the 'azurefilesvault'. The left sidebar has 'Overview', 'Management servers' (Backup Management Servers, Protected Servers), and 'Azure Storage Accounts' (Storage Accounts, highlighted with a red box). The main content area displays a table with columns 'BACKUP MANAGEMENT TYPE' and 'PROTECTED SERVER COUNT'. It lists four entries: 'Workload in Azure VM' (0), 'Azure Backup Agent' (0), 'DPM' (0), and 'Azure Backup Server' (0). A message at the top says 'Fetching data from service completed.'

| BACKUP MANAGEMENT TYPE | PROTECTED SERVER COUNT |
|------------------------|------------------------|
| Workload in Azure VM   | 0                      |
| Azure Backup Agent     | 0                      |
| DPM                    | 0                      |
| Azure Backup Server    | 0                      |

4. After you select **Storage Accounts**, a list of storage accounts registered with the vault appears.

5. Right-click the storage account you want to unregister, and select **Unregister**.

The screenshot shows the 'Backup Infrastructure - Storage Accounts' page for the 'azurefilesvault'. The left sidebar has 'Overview', 'Management servers' (Backup Management Servers, Protected Servers), and 'Azure Storage Accounts' (Storage Accounts, highlighted with a red box). The main content area shows a table with one entry: 'afaccount1'. A context menu is open over this entry, with options 'Pin to dashboard' (highlighted with a red box) and 'Unregister' (also highlighted with a red box).

## Next steps

For more information, see [Troubleshoot Azure file shares backup](#).

# Back up Azure file shares with CLI

1/29/2020 • 5 minutes to read • [Edit Online](#)

The Azure command-line interface (CLI) provides a command-line experience for managing Azure resources. It's a great tool for building custom automation to use Azure resources. This article details how to back up Azure file shares with Azure CLI. You can also perform these steps with [Azure PowerShell](#) or in the [Azure portal](#).

By the end of this tutorial, you will learn how to perform below operations with Azure CLI:

- Create a recovery services vault
- Enable backup for Azure file shares
- Trigger an on-demand backup for file shares

## Use Azure Cloud Shell

Azure hosts Azure Cloud Shell, an interactive shell environment that you can use through your browser. You can use either Bash or PowerShell with Cloud Shell to work with Azure services. You can use the Cloud Shell preinstalled commands to run the code in this article without having to install anything on your local environment.

To start Azure Cloud Shell:

| OPTION                                                                                                                                                    | EXAMPLE/LINK                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Select <b>Try It</b> in the upper-right corner of a code block.<br>Selecting <b>Try It</b> doesn't automatically copy the code to Cloud Shell.            |  |
| Go to <a href="https://shell.azure.com">https://shell.azure.com</a> , or select the <b>Launch Cloud Shell</b> button to open Cloud Shell in your browser. |  |
| Select the <b>Cloud Shell</b> button on the menu bar at the upper right in the <a href="#">Azure portal</a> .                                             |  |

To run the code in this article in Azure Cloud Shell:

1. Start Cloud Shell.
2. Select the **Copy** button on a code block to copy the code.
3. Paste the code into the Cloud Shell session by selecting **Ctrl+Shift+V** on Windows and Linux or by selecting **Cmd+Shift+V** on macOS.
4. Select **Enter** to run the code.

To install and use the CLI locally, you must run Azure CLI version 2.0.18 or later. To find the CLI version, `run az --version`. If you need to install or upgrade, see [Install the Azure CLI](#).

## Create a Recovery Services Vault

A recovery service vault is an entity that gives you a consolidated view and management capability across all backup items. 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.

Follow these steps to create a recovery services vault:

1. A vault is placed in a resource group. If you don't have an existing resource group, create a new one with [az group create](#). In this tutorial, we create the new resource group *azurefiles* in the East US region.

```
az group create --name AzureFiles --location eastus --output table
```

| Location | Name       |
|----------|------------|
| eastus   | AzureFiles |

2. Use the [az backup vault create](#) cmdlet to create the vault. Specify the same location for the vault as was used for the resource group.

The following example creates a recovery services vault named *azurefilesvault* in the East US region.

```
az backup vault create --resource-group azurefiles --name azurefilesvault --location eastus --output table
```

| Location | Name            | ResourceGroup |
|----------|-----------------|---------------|
| eastus   | azurefilesvault | azurefiles    |

3. Specify the type of redundancy to use for the vault storage. You can use [locally redundant storage](#) or [geo-redundant storage](#).

The following example sets storage redundancy option for *azurefilesvault* to **Georedundant** using the [az backup vault backup-properties set](#) cmdlet.

```
az backup vault backup-properties set --name azurefilesvault --resource-group azurefiles --backup-storage-redundancy Georedundant
```

To check if the vault is created successfully, you can use the [az backup vault show](#) cmdlet to get details of your vault. The following example displays the details of the *azurefilesvault* we created in the steps above.

```
az backup vault show --name azurefilesvault --resource-group azurefiles --output table
```

The output will be similar to the following response:

| Location | Name            | ResourceGroup |
|----------|-----------------|---------------|
| eastus   | azurefilesvault | azurefiles    |

## Enable backup for Azure file shares

This section assumes that you already have an Azure file share for which you want to configure backup. If you don't have one, create an Azure file share using the [az storage share create](#) command.

To enable backup for file shares, you need to create a protection policy that defines when a backup job runs and how long recovery points are stored. You can create a backup policy using the [az backup policy create](#) cmdlet.

The following example uses the [az backup protection enable-for-azurefileshare](#) cmdlet to enable backup for the

*azurefiles* file share in the *afsaccount* storage account using the *schedule 1* backup policy:

```
az backup protection enable-for-azurefileshare --vault-name azurefilesvault --resource-group azurefiles --policy-name schedule1 --storage-account afsaccount --azure-file-share azurefiles --output table
```

| Name                                 | ResourceGroup |
|--------------------------------------|---------------|
| 0caa93f4-460b-4328-ac1d-8293521dd928 | azurefiles    |

The **Name** attribute in the output corresponds to the name of the job that is created by the backup service for your **enable backup** operation. To track status of the job, use the [az backup job show](#) cmdlet.

## Trigger an on-demand backup for file share

If you want to trigger an on-demand backup for your file share instead of waiting for the backup policy to run the job at the scheduled time, use the [az backup protection backup-now](#) cmdlet.

You need to define the following parameters to trigger an on-demand backup:

- **--container-name** is the name of the storage account hosting the file share. To retrieve the **name** or **friendly name** of your container, use the [az backup container list](#) command.
- **--item-name** is the name of the file share for which you want to trigger an on-demand backup. To retrieve the **name** or **friendly name** of your backed-up item, use the [az backup item list](#) command.
- **--retain-until** specifies the date until when you want to retain the recovery point. The value should be set in UTC time format (dd-mm-yyyy).

The following example triggers an on-demand backup for the *azuresfiles* fileshare in the *afsaccount* storage account with retention until *20-01-2020*.

```
az backup protection backup-now --vault-name azurefilesvault --resource-group azurefiles --container-name "StorageContainer;Storage;AzureFiles;afsaccount" --item-name "AzureFileShare;azuresfiles" --retain-until 20-01-2020 --output table
```

| Name                                 | ResourceGroup |
|--------------------------------------|---------------|
| 9f026b4f-295b-4fb8-aae0-4f058124cb12 | azurefiles    |

The **Name** attribute in the output corresponds to the name of the job that is created by the backup service for your “on-demand backup” operation. To track the status of a job, use the [az backup job show](#) cmdlet.

## Next steps

- Learn how to [Restore Azure file shares with CLI](#)
- Learn how to [Manage Azure file share backups with CLI](#)

# Restore Azure file shares with the Azure CLI

1/31/2020 • 7 minutes to read • [Edit Online](#)

The Azure CLI provides a command-line experience for managing Azure resources. It's a great tool for building custom automation to use Azure resources. This article explains how to restore an entire file share or specific files from a restore point created by [Azure Backup](#) by using the Azure CLI. You can also perform these steps with [Azure PowerShell](#) or in the [Azure portal](#).

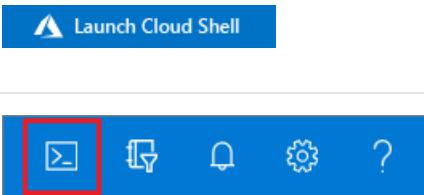
By the end of this article, you'll learn how to perform the following operations with the Azure CLI:

- View restore points for a backed-up Azure file share.
- Restore a full Azure file share.
- Restore individual files or folders.

## Use Azure Cloud Shell

Azure hosts Azure Cloud Shell, an interactive shell environment that you can use through your browser. You can use either Bash or PowerShell with Cloud Shell to work with Azure services. You can use the Cloud Shell preinstalled commands to run the code in this article without having to install anything on your local environment.

To start Azure Cloud Shell:

| OPTION                                                                                                                                                    | EXAMPLE/LINK                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Select <b>Try It</b> in the upper-right corner of a code block. Selecting <b>Try It</b> doesn't automatically copy the code to Cloud Shell.               |  |
| Go to <a href="https://shell.azure.com">https://shell.azure.com</a> , or select the <b>Launch Cloud Shell</b> button to open Cloud Shell in your browser. |  |
| Select the <b>Cloud Shell</b> button on the menu bar at the upper right in the <a href="#">Azure portal</a> .                                             |                                                                                      |

To run the code in this article in Azure Cloud Shell:

1. Start Cloud Shell.
2. Select the **Copy** button on a code block to copy the code.
3. Paste the code into the Cloud Shell session by selecting **Ctrl+Shift+V** on Windows and Linux or by selecting **Cmd+Shift+V** on macOS.
4. Select **Enter** to run the code.

To install and use the CLI locally, you must run Azure CLI version 2.0.18 or later. To find the CLI version, run `az --version`. If you need to install or upgrade, see [Install the Azure CLI](#).

## Prerequisites

This article assumes that you already have an Azure file share that's backed up by Azure Backup. If you don't have one, see [Back up Azure file shares with the CLI](#) to configure backup for your file share. For this article, you use the

following resources:

| FILE SHARE         | STORAGE ACCOUNT   | REGION | DETAILS                                                 |
|--------------------|-------------------|--------|---------------------------------------------------------|
| <i>azurefiles</i>  | <i>afsaccount</i> | EastUS | Original source backed up by using Azure Backup         |
| <i>azurefiles1</i> | <i>afaccount1</i> | EastUS | Destination source used for alternate location recovery |

You can use a similar structure for your file shares to try out the different types of restores explained in this article.

## Fetch recovery points for the Azure file share

Use the [az backup recoverypoint list](#) cmdlet to list all recovery points for the backed-up file share.

The following example fetches the list of recovery points for the *azurefiles* file share in the *afsaccount* storage account.

```
az backup recoverypoint list --vault-name azurefilesvault --resource-group azurefiles --container-name "StorageContainer;Storage;AzureFiles;afsaccount" --backup-management-type azurestorage --item-name "AzureFileShare;azurefiles" --workload-type azurefileshare --out table
```

You can also run the previous cmdlet by using the friendly name for the container and the item by providing the following two additional parameters:

- **--backup-management-type:** *azurestorage*
- **--workload-type:** *azurefileshare*

```
az backup recoverypoint list --vault-name azurefilesvault --resource-group azurefiles --container-name afsaccount --backup-management-type azurestorage --item-name azurefiles --workload-type azurefileshare --out table
```

The result set is a list of recovery points with time and consistency details for each restore point.

| Name               | Time                      | Consistency          |
|--------------------|---------------------------|----------------------|
| 932887541532871865 | 2020-01-05T07:08:23+00:00 | FileSystemConsistent |
| 932885927361238054 | 2020-01-05T07:08:10+00:00 | FileSystemConsistent |
| 932879614553967772 | 2020-01-04T21:33:04+00:00 | FileSystemConsistent |

The **Name** attribute in the output corresponds to the recovery point name that can be used as a value for the **--rp-name** parameter in recovery operations.

## Full share recovery by using the Azure CLI

You can use this restore option to restore the complete file share in the original or an alternate location.

Define the following parameters to perform restore operations:

- **--container-name:** The name of the storage account that hosts the backed-up original file share. To retrieve the name or friendly name of your container, use the [az backup container list](#) command.
- **--item-name:** The name of the backed-up original file share you want to use for the restore operation. To retrieve the name or friendly name of your backed-up item, use the [az backup item list](#) command.

### Restore a full share to the original location

When you restore to an original location, you don't need to specify target-related parameters. Only **Resolve Conflict** must be provided.

The following example uses the [az backup restore restore-azurefileshare](#) cmdlet with restore mode set to *originalallocation* to restore the *azurefiles* file share in the original location. You use the recovery point 932883129628959823, which you obtained in [Fetch recovery points for the Azure file share](#):

```
az backup restore restore-azurefileshare --vault-name azurefilesvault --resource-group azurefiles --rp-name 932887541532871865 --container-name "StorageContainer;Storage;AzureFiles;afsaccount" --item-name "AzureFileShare;azurefiles" --restore-mode originalallocation --resolve-conflict overwrite --out table
```

| Name                                 | ResourceGroup |
|--------------------------------------|---------------|
| 6a27cc23-9283-4310-9c27-dcfb81b7b4bb | azurefiles    |

The **Name** attribute in the output corresponds to the name of the job that's created by the backup service for your restore operation. To track the status of the job, use the [az backup job show](#) cmdlet.

### Restore a full share to an alternate location

You can use this option to restore a file share to an alternate location and keep the original file share as is. Specify the following parameters for alternate location recovery:

- **--target-storage-account**: The storage account to which the backed-up content is restored. The target storage account must be in the same location as the vault.
- **--target-file-share**: The file share within the target storage account to which the backed-up content is restored.
- **--target-folder**: The folder under the file share to which data is restored. If the backed-up content is to be restored to a root folder, give the target folder values as an empty string.
- **--resolve-conflict**: Instruction if there's a conflict with the restored data. Accepts **Overwrite** or **Skip**.

The following example uses [az backup restore restore-azurefileshare](#) with restore mode as *alternatelocation* to restore the *azurefiles* file share in the *afsaccount* storage account to the *azurefiles1* file share in the *afaccount1* storage account.

```
az backup restore restore-azurefileshare --vault-name azurefilesvault --resource-group azurefiles --rp-name 932883129628959823 --container-name "StorageContainer;Storage;AzureFiles;afsaccount" --item-name "AzureFileShare;azurefiles" --restore-mode alternatelocation --target-storage-account afaccount1 --target-file-share azurefiles1 --target-folder restoredata --resolve-conflict overwrite --out table
```

| Name                                 | ResourceGroup |
|--------------------------------------|---------------|
| babeb61c-d73d-4b91-9830-b8bfa83c349a | azurefiles    |

The **Name** attribute in the output corresponds to the name of the job that's created by the backup service for your restore operation. To track the status of the job, use the [az backup job show](#) cmdlet.

## Item-level recovery

You can use this restore option to restore individual files or folders in the original or an alternate location.

Define the following parameters to perform restore operations:

- **--container-name**: The name of the storage account that hosts the backed-up original file share. To retrieve the name or friendly name of your container, use the [az backup container list](#) command.
- **--item-name**: The name of the backed-up original file share you want to use for the restore operation. To

retrieve the name or friendly name of your backed-up item, use the [az backup item list](#) command.

Specify the following parameters for the items you want to recover:

- **SourceFilePath**: The absolute path of the file, to be restored within the file share, as a string. This path is the same path used in the [az storage file download](#) or [az storage file show](#) CLI commands.
- **SourceFileType**: Choose whether a directory or a file is selected. Accepts **Directory** or **File**.
- **ResolveConflict**: Instruction if there's a conflict with the restored data. Accepts **Overwrite** or **Skip**.

#### Restore individual files or folders to the original location

Use the [az backup restore restore-azurefiles](#) cmdlet with restore mode set to *originallocation* to restore specific files or folders to their original location.

The following example restores the *RestoreTest.txt* file in its original location: the *azurefiles* file share.

```
az backup restore restore-azurefiles --vault-name azurefilesvault --resource-group azurefiles --rp-name 932881556234035474 --container-name "StorageContainer;Storage;AzureFiles;afsaccount" --item-name "AzureFileShare;azurefiles" --restore-mode originallocation --source-file-type file --source-file-path "Restore/RestoreTest.txt" --resolve-conflict overwrite --out table
```

| Name                                 | ResourceGroup |
|--------------------------------------|---------------|
| df4d9024-0dcb-4edc-bf8c-0a3d18a25319 | azurefiles    |

The **Name** attribute in the output corresponds to the name of the job that's created by the backup service for your restore operation. To track the status of the job, use the [az backup job show](#) cmdlet.

#### Restore individual files or folders to an alternate location

To restore specific files or folders to an alternate location, use the [az backup restore restore-azurefiles](#) cmdlet with restore mode set to *alternatelocation* and specify the following target-related parameters:

- **--target-storage-account**: The storage account to which the backed-up content is restored. The target storage account must be in the same location as the vault.
- **--target-file-share**: The file share within the target storage account to which the backed-up content is restored.
- **--target-folder**: The folder under the file share to which data is restored. If the backed-up content is to be restored to a root folder, give the target folder's value as an empty string.

The following example restores the *RestoreTest.txt* file originally present in the *azurefiles* file share to an alternate location: the *restoreddata* folder in the *azurefiles1* file share hosted in the *afaccount1* storage account.

```
az backup restore restore-azurefiles --vault-name azurefilesvault --resource-group azurefiles --rp-name 932881556234035474 --container-name "StorageContainer;Storage;AzureFiles;afsaccount" --item-name "AzureFileShare;azurefiles" --restore-mode alternatelocation --target-storage-account afaccount1 --target-file-share azurefiles1 --target-folder restoreddata --resolve-conflict overwrite --source-file-type file --source-file-path "Restore/RestoreTest.txt" --out table
```

| Name                                 | ResourceGroup |
|--------------------------------------|---------------|
| df4d9024-0dcb-4edc-bf8c-0a3d18a25319 | azurefiles    |

The **Name** attribute in the output corresponds to the name of the job that's created by the backup service for your restore operation. To track the status of the job, use the [az backup job show](#) cmdlet.

## Next steps

Learn how to [Manage Azure file share backups with the Azure CLI](#).

# Manage Azure file share backups with the Azure CLI

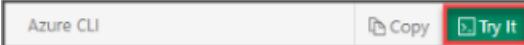
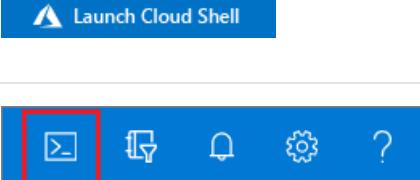
1/31/2020 • 7 minutes to read • [Edit Online](#)

The Azure CLI provides a command-line experience for managing Azure resources. It's a great tool for building custom automation to use Azure resources. This article explains how to perform tasks for managing and monitoring the Azure file shares that are backed up by [Azure Backup](#). You can also perform these steps with the [Azure portal](#).

## Use Azure Cloud Shell

Azure hosts Azure Cloud Shell, an interactive shell environment that you can use through your browser. You can use either Bash or PowerShell with Cloud Shell to work with Azure services. You can use the Cloud Shell preinstalled commands to run the code in this article without having to install anything on your local environment.

To start Azure Cloud Shell:

| OPTION                                                                                                                                                    | EXAMPLE/LINK                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Select <b>Try It</b> in the upper-right corner of a code block.<br>Selecting <b>Try It</b> doesn't automatically copy the code to Cloud Shell.            |    |
| Go to <a href="https://shell.azure.com">https://shell.azure.com</a> , or select the <b>Launch Cloud Shell</b> button to open Cloud Shell in your browser. |  |
| Select the <b>Cloud Shell</b> button on the menu bar at the upper right in the <a href="#">Azure portal</a> .                                             |                                                                                      |

To run the code in this article in Azure Cloud Shell:

1. Start Cloud Shell.
2. Select the **Copy** button on a code block to copy the code.
3. Paste the code into the Cloud Shell session by selecting **Ctrl+Shift+V** on Windows and Linux or by selecting **Cmd+Shift+V** on macOS.
4. Select **Enter** to run the code.

To install and use the CLI locally, you must run the Azure CLI version 2.0.18 or later. To find the CLI version, run `az --version`. If you need to install or upgrade, see [Install the Azure CLI](#).

## Prerequisites

This article assumes you already have an Azure file share backed up by [Azure Backup](#). If you don't have one, see [Back up Azure file shares with the CLI](#) to configure backup for your file shares. For this article, you use the following resources:

- **Resource group:** `azurefiles`
- **RecoveryServicesVault:** `azurefilesvault`
- **Storage Account:** `afsaccount`
- **File Share:** `azurefiles`

## Monitor jobs

When you trigger backup or restore operations, the backup service creates a job for tracking. To monitor completed or currently running jobs, use the [az backup job list](#) cmdlet. With the CLI, you also can [suspend a currently running job](#) or [wait until a job finishes](#).

The following example displays the status of backup jobs for the *azurefilesvault* Recovery Services vault:

```
az backup job list --resource-group azurefiles --vault-name azurefilesvault
```

```
[
 {
 "eTag": null,
 "id": "/Subscriptions/ef4ab5a7-c2c0-4304-af80-
af49f48af3d1/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupJobs/
d477dfb6-b292-4f24-bb43-6b14e9d06ab5",
 "location": null,
 "name": "d477dfb6-b292-4f24-bb43-6b14e9d06ab5",
 "properties": {
 "actionsInfo": null,
 "activityId": "3cef43ed-0af4-43e2-b9cb-1322c496ccb4",
 "backupManagementType": "AzureStorage",
 "duration": "0:00:29.718011",
 "endTime": "2020-01-13T08:05:29.180606+00:00",
 "entityFriendlyName": "azurefiles",
 "errorDetails": null,
 "extendedInfo": null,
 "jobType": "AzureStorageJob",
 "operation": "Backup",
 "startTime": "2020-01-13T08:04:59.462595+00:00",
 "status": "Completed",
 "storageAccountName": "afsaccount",
 "storageAccountVersion": "MicrosoftStorage"
 },
 "resourceGroup": "azurefiles",
 "tags": null,
 "type": "Microsoft.RecoveryServices/vaults/backupJobs"
 },
 {
 "eTag": null,
 "id": "/Subscriptions/ef4ab5a7-c2c0-4304-af80-
af49f48af3d1/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupJobs/
1b9399bf-c23c-4caa-933a-5fc2bf884519",
 "location": null,
 "name": "1b9399bf-c23c-4caa-933a-5fc2bf884519",
 "properties": {
 "actionsInfo": null,
 "activityId": "2663449c-94f1-4735-aaf9-5bb991e7e00c",
 "backupManagementType": "AzureStorage",
 "duration": "0:00:28.145216",
 "endTime": "2020-01-13T08:05:27.519826+00:00",
 "entityFriendlyName": "azurefilesresource",
 "errorDetails": null,
 "extendedInfo": null,
 "jobType": "AzureStorageJob",
 "operation": "Backup",
 "startTime": "2020-01-13T08:04:59.374610+00:00",
 "status": "Completed",
 "storageAccountName": "afsaccount",
 "storageAccountVersion": "MicrosoftStorage"
 },
 "resourceGroup": "azurefiles",
 "tags": null,
 "type": "Microsoft.RecoveryServices/vaults/backupJobs"
 }
]
```

## Modify policy

You can modify a backup policy to change backup frequency or retention range by using [az backup item set-policy](#).

To change the policy, define the following parameters:

- **--container-name:** The name of the storage account that hosts the file share. To retrieve the **name** or **friendly name** of your container, use the [az backup container list](#) command.

- **--name:** The name of the file share for which you want to change the policy. To retrieve the **name** or **friendly name** of your backed-up item, use the [az backup item list](#) command.
- **--policy-name:** The name of the backup policy you want to set for your file share. You can use [az backup policy list](#) to view all the policies for your vault.

The following example sets the *schedule2* backup policy for the *azurefiles* file share present in the *afsaccount* storage account.

```
az backup item set-policy --policy-name schedule2 --name azurefiles --vault-name azurefilesvault --resource-group azurefiles --container-name "StorageContainer;Storage;AzureFiles;afsaccount" --name "AzureFileShare;azurefiles" --backup-management-type azurestorage --out table
```

You can also run the previous command by using the friendly names for the container and the item by providing the following two additional parameters:

- **--backup-management-type:** *azurestorage*
- **--workload-type:** *azurefileshare*

```
az backup item set-policy --policy-name schedule2 --name azurefiles --vault-name azurefilesvault --resource-group azurefiles --container-name afsaccount --name azurefiles --backup-management-type azurestorage --out table
```

| Name                                 | ResourceGroup |
|--------------------------------------|---------------|
| fec6f004-0e35-407f-9928-10a163f123e5 | azurefiles    |

The **Name** attribute in the output corresponds to the name of the job that's created by the backup service for your change policy operation. To track the status of the job, use the [az backup job show](#) cmdlet.

## Stop protection on a file share

There are two ways to stop protecting Azure file shares:

- Stop all future backup jobs and *delete* all recovery points.
- Stop all future backup jobs but *leave* the recovery points.

There might be a cost associated with leaving the recovery points in storage, because the underlying snapshots created by Azure Backup will be retained. The benefit of leaving the recovery points is the option to restore the file share later, if you want. For information about the cost of leaving the recovery points, see the [pricing details](#). If you choose to delete all recovery points, you can't restore the file share.

To stop protection for the file share, define the following parameters:

- **--container-name:** The name of the storage account that hosts the file share. To retrieve the **name** or **friendly name** of your container, use the [az backup container list](#) command.
- **--item-name:** The name of the file share for which you want to stop protection. To retrieve the **name** or **friendly name** of your backed-up item, use the [az backup item list](#) command.

### Stop protection and retain recovery points

To stop protection while retaining data, use the [az backup protection disable](#) cmdlet.

The following example stops protection for the *azurefiles* file share but retains all recovery points.

```
az backup protection disable --vault-name azurefilesvault --resource-group azurefiles --container-name "StorageContainer;Storage;AzureFiles;afsaccount" --item-name "AzureFileShare;azurefiles" --out table
```

You can also run the previous command by using the friendly name for the container and the item by providing the following two additional parameters:

- **--backup-management-type**: *azurestorage*
- **--workload-type**: *azurefileshare*

```
az backup protection disable --vault-name azurefilesvault --resource-group azurefiles --container-name afsaccount --item-name azurefiles --workload-type azurefileshare --backup-management-type Azurestorage --out table
```

| Name                                 | ResourceGroup |
|--------------------------------------|---------------|
| fec6f004-0e35-407f-9928-10a163f123e5 | azurefiles    |

The **Name** attribute in the output corresponds to the name of the job that's created by the backup service for your stop protection operation. To track the status of the job, use the [az backup job show](#) cmdlet.

### Stop protection without retaining recovery points

To stop protection without retaining recovery points, use the [az backup protection disable](#) cmdlet with the **delete-backup-data** option set to **true**.

The following example stops protection for the *azurefiles* file share without retaining recovery points.

```
az backup protection disable --vault-name azurefilesvault --resource-group azurefiles --container-name "StorageContainer;Storage;AzureFiles;afsaccount" --item-name "AzureFileShare;azurefiles" --delete-backup-data true --out table
```

You can also run the previous command by using the friendly name for the container and the item by providing the following two additional parameters:

- **--backup-management-type**: *azurestorage*
- **--workload-type**: *azurefileshare*

```
az backup protection disable --vault-name azurefilesvault --resource-group azurefiles --container-name afsaccount --item-name azurefiles --workload-type azurefileshare --backup-management-type Azurestorage --delete-backup-data true --out table
```

## Resume protection on a file share

If you stopped protection for an Azure file share but retained recovery points, you can resume protection later. If you don't retain the recovery points, you can't resume protection.

To resume protection for the file share, define the following parameters:

- **--container-name**: The name of the storage account that hosts the file share. To retrieve the **name** or **friendly name** of your container, use the [az backup container list](#) command.
- **--item-name**: The name of the file share for which you want to resume protection. To retrieve the **name** or **friendly name** of your backed-up item, use the [az backup item list](#) command.
- **--policy-name**: The name of the backup policy for which you want to resume the protection for the file share.

The following example uses the [az backup protection resume](#) cmdlet to resume protection for the *azurefiles* file share by using the *schedule1* backup policy.

```
az backup protection resume --vault-name azurefilesvault --resource-group azurefiles --container-name "StorageContainer;Storage;AzureFiles;afsaccount" --item-name "AzureFileShare;azurefiles" --policy-name schedule2 --out table
```

You can also run the previous command by using the friendly name for the container and the item by providing the following two additional parameters:

- **--backup-management-type**: *azurestorage*
- **--workload-type**: *azurefileshare*

```
az backup protection resume --vault-name azurefilesvault --resource-group azurefiles --container-name afsaccount --item-name azurefiles --workload-type azurefileshare --backup-management-type Azurestorage --policy-name schedule2 --out table
```

| Name                                 | ResourceGroup |
|--------------------------------------|---------------|
| 75115ab0-43b0-4065-8698-55022a234b7f | azurefiles    |

The **Name** attribute in the output corresponds to the name of the job that's created by the backup service for your resume protection operation. To track the status of the job, use the [az backup job show](#) cmdlet.

## Unregister a storage account

If you want to protect your file shares in a particular storage account by using a different Recovery Services vault, first [stop protection for all file shares](#) in that storage account. Then unregister the account from the Recovery Services vault currently used for protection.

You need to provide a container name to unregister the storage account. To retrieve the **name** or the **friendly name** of your container, use the [az backup container list](#) command.

The following example unregisters the *afsaccount* storage account from *azurefilesvault* by using the [az backup container unregister](#) cmdlet.

```
az backup container unregister --vault-name azurefilesvault --resource-group azurefiles --container-name "StorageContainer;Storage;AzureFiles;afsaccount" --out table
```

You can also run the previous cmdlet by using the friendly name for the container by providing the following additional parameter:

- **--backup-management-type**: *azurestorage*

```
az backup container unregister --vault-name azurefilesvault --resource-group azurefiles --container-name afsaccount --backup-management-type Azurestorage --out table
```

## Next steps

For more information, see [Troubleshoot Azure file shares backup](#).

# Back up Azure Files with PowerShell

2/10/2020 • 9 minutes to read • [Edit Online](#)

This article describes how to use Azure PowerShell to back up an Azure Files file share using an [Azure Backup Recovery Services vault](#).

This article explains how to:

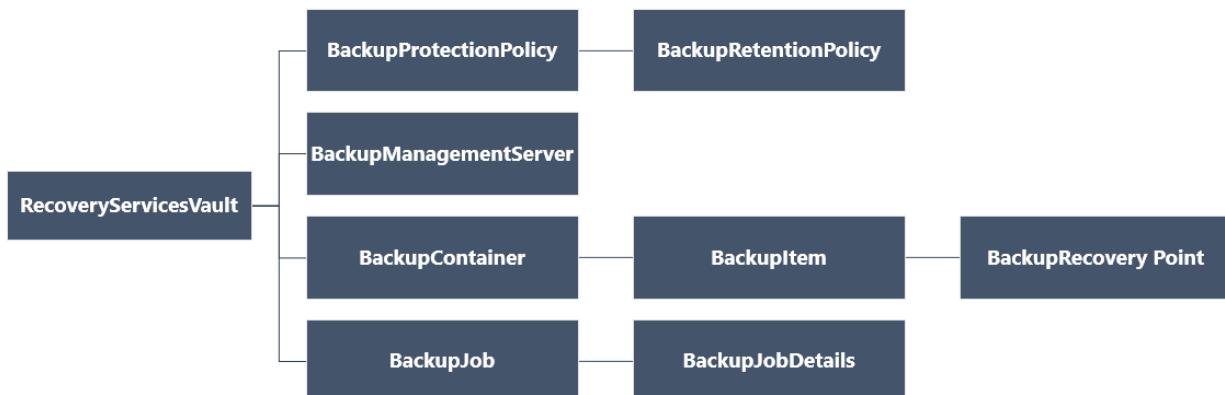
- Set up PowerShell and register the Azure Recovery Services Provider.
- Create a Recovery Services vault.
- Configure backup for an Azure file share.
- Run a backup job.

## Before you start

- [Learn more](#) about Recovery Services vaults.
- Read about the preview capabilities for [backing up Azure file shares](#).
- Review the PowerShell object hierarchy for Recovery Services.

## Recovery Services object hierarchy

The object hierarchy is summarized in the following diagram.



Review the [Az.RecoveryServices cmdlet reference](#) reference in the Azure library.

## Set up and install

### NOTE

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

Set up PowerShell as follows:

1. [Download the latest version of Az PowerShell](#). The minimum version required is 1.0.0.

**WARNING**

The minimum version of PS required for preview was 'Az 1.0.0'. Due to upcoming changes for GA, the minimum PS version required will be 'Az.RecoveryServices 2.6.0'. It is very important to upgrade all existing PS versions to this version. Otherwise, the existing scripts will break after GA. Install the minimum version with the following PS commands

```
Install-Module -Name Az.RecoveryServices -RequiredVersion 2.6.0
```

2. Find the Azure Backup PowerShell cmdlets with this command:

```
Get-Command *azrecoveryservices*
```

3. Review the aliases and cmdlets for Azure Backup, Azure Site Recovery, and the Recovery Services vault appear. Here's an example of what you might see. It's not a complete list of cmdlets.

| CommandType | Name                                               | Version | Source              |
|-------------|----------------------------------------------------|---------|---------------------|
| Alias       | Get-AzRecoveryServicesAsrNotificationSetting       | 0.7.0   | Az.RecoveryServices |
| Alias       | Get-AzRecoveryServicesAsrVaultSettings             | 0.7.0   | Az.RecoveryServices |
| Alias       | Get-AzRecoveryServicesBackupProperties             | 0.7.0   | Az.RecoveryServices |
| Alias       | Set-AzRecoveryServicesAsrNotificationSetting       | 0.7.0   | Az.RecoveryServices |
| Alias       | Set-AzRecoveryServicesAsrVaultSettings             | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Backup-AzRecoveryServicesBackupItem                | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Disable-AzRecoveryServicesBackupProtection         | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Disable-AzRecoveryServicesBackupRPMountScript      | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Edit-AzRecoveryServicesAsrRecoveryPlan             | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Enable-AzRecoveryServicesBackupProtection          | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrAlertSetting              | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrEvent                     | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrFabric                    | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrJob                       | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrNetwork                   | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrNetworkMapping            | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrPolicy                    | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrProtectableItem           | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrProtectionContainer       | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrProtectionContainerMap... | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrRecoveryPlan              | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrRecoveryPoint             | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrReplicationProtectedItem  | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrServicesProvider          | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrStorageClassification     | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrStorageClassificationM... | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrVaultContext              | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrvCenter                   | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupContainer              | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupItem                   | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupJob                    | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupJobDetails             | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupManagementServer       | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupProperty               | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupProtectionPolicy       | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupRecoveryPoint          | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupRetentionPolicyObject  | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupRPMountScript          | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupSchedulePolicyObject   | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupStatus                 | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesVault                        | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesVaultSettingsFile            | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Import-AzRecoveryServicesAsrVaultSettingsFile      | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesAsrAzureToAzureDiskReplic... | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesAsrFabric                    | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesAsrNetworkMapping            | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesAsrPolicy                    | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesAsrProtectableItem           | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesAsrProtectionContainer       | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesAsrProtectionContainerMap... | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesAsrRecoveryPlan              | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesAsrReplicationProtectedItem  | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesAsrStorageClassificationM... | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesAsrvCenter                   | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesBackupProtectionPolicy       | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesVault                        | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Remove-AzRecoveryServicesAsrFabric                 | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Remove-AzRecoveryServicesAsrNetworkMapping         | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Remove-AzRecoveryServicesAsrPolicy                 | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Remove-AzRecoveryServicesAsrProtectionContainer    | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Remove-AzRecoveryServicesAsrProtectionContainer... | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Remove-AzRecoveryServicesAsrRecoveryPlan           | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Remove-AzRecoveryServicesAsrReplicationProtecte... | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Remove-AzRecoveryServicesAsrServicesProvider       | 0.7.0   | Az.RecoveryServices |

4. Sign in to your Azure account with **Connect-AzAccount**.
5. On the web page that appears, you're prompted to input your account credentials.
  - Alternately, you can include your account credentials as a parameter in the **Connect-AzAccount** cmdlet with **-Credential**.
  - If you're a CSP partner working on behalf of a tenant, specify the customer as a tenant, using their tenantID or tenant primary domain name. An example is **Connect-AzAccount -Tenant** fabrikam.com.
6. Associate the subscription you want to use with the account, because an account can have several subscriptions.

```
Select-AzSubscription -SubscriptionName $SubscriptionName
```

7. If you're using Azure Backup for the first time, use the **Register-AzResourceProvider** cmdlet to register the Azure Recovery Services provider with your subscription.

```
Register-AzResourceProvider -ProviderNamespace "Microsoft.RecoveryServices"
```

8. Verify that the providers registered successfully:

```
Get-AzResourceProvider -ProviderNamespace "Microsoft.RecoveryServices"
```

9. In the command output, verify that **RegistrationState** changes to **Registered**. If it doesn't, run the **Register-AzResourceProvider** cmdlet again.

## Create a Recovery Services vault

The Recovery Services vault is a Resource Manager resource, so you must place it within a resource group. You can use an existing resource group, or you can create a resource group with the **New-AzResourceGroup** cmdlet. When you create a resource group, specify the name and location for the resource group.

Follow these steps to create a Recovery Services vault.

1. A vault is placed in a resource group. If you don't have an existing resource group, create a new one with the **New-AzResourceGroup**. In this example, we create a new resource group in the West US region.

```
New-AzResourceGroup -Name "test-rg" -Location "West US"
```

2. Use the **New-AzRecoveryServicesVault** cmdlet to create the vault. Specify the same location for the vault as was used for the resource group.

```
New-AzRecoveryServicesVault -Name "testvault" -ResourceGroupName "test-rg" -Location "West US"
```

3. Specify the type of redundancy to use for the vault storage.

- You can use [locally redundant storage](#) or [geo-redundant storage](#).
- The following example sets the **-BackupStorageRedundancy** option for the [Set-AzRecoveryServicesBackupProperties](#) cmd for **testvault** set to **GeoRedundant**.

```
$vault1 = Get-AzRecoveryServicesVault -Name "testvault"
Set-AzRecoveryServicesBackupProperties -Vault $vault1 -BackupStorageRedundancy GeoRedundant
```

## View the vaults in a subscription

To view all vaults in the subscription, use [Get-AzRecoveryServicesVault](#).

```
Get-AzRecoveryServicesVault
```

The output is similar to the following. Note that the associated resource group and location are provided.

```
Name : Contoso-vault
ID : /subscriptions/1234
Type : Microsoft.RecoveryServices/vaults
Location : WestUS
ResourceGroupName : Contoso-docs-rg
SubscriptionId : 1234-567f-8910-abc
Properties : Microsoft.Azure.Commands.RecoveryServices.ARSVaultProperties
```

## Set the vault context

Store the vault object in a variable, and set the vault context.

- Many Azure Backup cmdlets require the Recovery Services vault object as an input, so it's convenient to store the vault object in a variable.
- The vault context is the type of data protected in the vault. Set it with [Set-AzRecoveryServicesVaultContext](#). After the context is set, it applies to all subsequent cmdlets.

The following example sets the vault context for **testvault**.

```
Get-AzRecoveryServicesVault -Name "testvault" | Set-AzRecoveryServicesVaultContext
```

## Fetch the vault ID

We plan on deprecating the vault context setting in accordance with Azure PowerShell guidelines. Instead, you can store or fetch the vault ID, and pass it to relevant commands. So, if you haven't set the vault context or want to specify the command to run for a certain vault, pass the vault ID as "-vaultID" to all relevant command as follows:

```
$vaultID = Get-AzRecoveryServicesVault -ResourceGroupName "Contoso-docs-rg" -Name "testvault" | select -
ExpandProperty ID
New-AzRecoveryServicesBackupProtectionPolicy -Name "NewAFSPolicy" -WorkloadType "AzureFiles" -RetentionPolicy
$retPol -SchedulePolicy $schPol -VaultID $vaultID
```

## Configure a backup policy

A backup policy specifies the schedule for backups, and how long backup recovery points should be kept:

- A backup policy is associated with at least one retention policy. A retention policy defines how long a recovery point is kept before it's deleted.
- View the default backup policy retention using [Get-AzRecoveryServicesBackupRetentionPolicyObject](#).
- View the default backup policy schedule using [Get-AzRecoveryServicesBackupSchedulePolicyObject](#).
- You use the [New-AzRecoveryServicesBackupProtectionPolicy](#) cmdlet to create a new backup policy. You input the schedule and retention policy objects.

By default, a start time is defined in the Schedule Policy Object. Use the following example to change the start time to the desired start time. The desired start time should be in UTC as well. The below example assumes the desired start time is 01:00 AM UTC for daily backups.

```
$schPol = Get-AzRecoveryServicesBackupSchedulePolicyObject -WorkloadType "AzureFiles"
$UtcTime = Get-Date -Date "2019-03-20 01:30:00Z"
$UtcTime = $UtcTime.ToUniversalTime()
$schpol.ScheduleRunTimes[0] = $UtcTime
```

## IMPORTANT

You need to provide the start time in 30 minute multiples only. In the above example, it can be only "01:00:00" or "02:30:00". The start time cannot be "01:15:00"

The following example stores the schedule policy and the retention policy in variables. It then uses those variables as parameters for a new policy (**NewAFSPolicy**). **NewAFSPolicy** takes a daily backup and retains it for 30 days.

```
$schPol = Get-AzRecoveryServicesBackupSchedulePolicyObject -WorkloadType "AzureFiles"
$retPol = Get-AzRecoveryServicesBackupRetentionPolicyObject -WorkloadType "AzureFiles"
New-AzRecoveryServicesBackupProtectionPolicy -Name "NewAFSPolicy" -WorkloadType "AzureFiles" -RetentionPolicy
$retPol -SchedulePolicy $schPol
```

The output is similar to the following.

| Name         | WorkloadType | BackupManagementType | BackupTime            | DaysOfWeek |
|--------------|--------------|----------------------|-----------------------|------------|
| ---          | -----        | -----                | -----                 | -----      |
| NewAFSPolicy | AzureFiles   | AzureStorage         | 10/24/2019 1:30:00 AM |            |

## Enable backup

After you define the backup policy, you can enable the protection for the Azure file share using the policy.

### Retrieve a backup policy

You fetch the relevant policy object with [Get-AzRecoveryServicesBackupProtectionPolicy](#). Use this cmdlet to get a specific policy, or to view the policies associated with a workload type.

#### Retrieve a policy for a workload type

The following example retrieves policies for the workload type **AzureFiles**.

```
Get-AzRecoveryServicesBackupProtectionPolicy -WorkloadType "AzureFiles"
```

The output is similar to the following.

| Name     | WorkloadType | BackupManagementType | BackupTime            | DaysOfWeek |
|----------|--------------|----------------------|-----------------------|------------|
| ---      | -----        | -----                | -----                 | -----      |
| dailyafs | AzureFiles   | AzureStorage         | 1/10/2018 12:30:00 AM |            |

## NOTE

The time zone of the **BackupTime** field in PowerShell is Universal Coordinated Time (UTC). When the backup time is shown in the Azure portal, the time is adjusted to your local time zone.

### Retrieve a specific policy

The following policy retrieves the backup policy named **dailyafs**.

```
$afsPol = Get-AzRecoveryServicesBackupProtectionPolicy -Name "dailyafs"
```

### Enable backup and apply policy

Enable protection with [Enable-AzRecoveryServicesBackupProtection](#). After the policy is associated with the vault, backups are triggered in accordance with the policy schedule.

The following example enables protection for the Azure file share **testAzureFileShare** in storage account **testStorageAcct**, with the policy **dailyafs**.

```
Enable-AzRecoveryServicesBackupProtection -StorageAccountName "testStorageAcct" -Name "testAzureFS" -Policy $afsPol
```

The command waits until the configure protection job is finished and gives a similar output, as shown.

| WorkloadName | Operation       | Status    | StartTime             | EndTime               | JobID                                |
|--------------|-----------------|-----------|-----------------------|-----------------------|--------------------------------------|
| -----        | -----           | -----     | -----                 | -----                 | -----                                |
| testAzureFS  | ConfigureBackup | Completed | 11/12/2018 2:15:26 PM | 11/12/2018 2:16:11 PM | ec7d4f1d-40bd-46a4-9edb-3193c41f6bf6 |

## Important notice - Backup item identification for AFS backups

This section outlines an important change in AFS backup in preparation for GA.

While enabling the backup for AFS, user supplies the customer friendly File share name as the entity name and a backup item is created. The backup item's 'name' is a unique identifier created by Azure Backup service. Usually the identifier involves user friendly name. But to handle the important scenario of soft-delete, where a file share can be deleted and another file-share can be created with the same name, the unique identity of Azure file share will now be an ID instead of customer friendly name. In order to know the unique identity/name of each item, just run the `Get-AzRecoveryServicesBackupItem` command with the relevant filters for `backupManagementType` and `WorkloadType` to get all the relevant items and then observe the name field in the returned PS object/response. It is always recommended to list items and then retrieve their unique name from 'name' field in response. Use this value to filter the items with the 'Name' parameter. Otherwise use the `FriendlyName` parameter to retrieve the item with it's customer friendly name/identifier.

### WARNING

Make sure the PS version is upgraded to the minimum version for 'Az.RecoveryServices 2.6.0' for AFS backups. With this version, the 'friendlyName' filter is available for `Get-AzRecoveryServicesBackupItem` command. Pass the Azure File Share name to `friendlyName` parameter. If you pass the Azure File Share name to the 'Name' parameter, this version throws a warning to pass this friendly name to the friendly name parameter. Not installing this minimum version might result in failure of existing scripts. Install the minimum version of PS with the following command.

```
Install-module -Name Az.RecoveryServices -RequiredVersion 2.6.0
```

## Trigger an on-demand backup

Use `Backup-AzRecoveryServicesBackupItem` to run an on-demand backup for a protected Azure file share.

1. Retrieve the storage account from the container in the vault that holds your backup data with [Get-AzRecoveryServicesBackupContainer](#).
2. To start a backup job, you obtain information about the Azure file share with [Get-AzRecoveryServicesBackupItem](#).
3. Run an on-demand backup with[Backup-AzRecoveryServicesBackupItem](#).

Run the on-demand backup as follows:

```
$afsContainer = Get-AzRecoveryServicesBackupContainer -FriendlyName "testStorageAcct" -ContainerType AzureStorage
$afsBkpItem = Get-AzRecoveryServicesBackupItem -Container $afsContainer -WorkloadType "AzureFiles" -
FriendlyName "testAzureFS"
$job = Backup-AzRecoveryServicesBackupItem -Item $afsBkpItem
```

The command returns a job with an ID to be tracked, as shown in the following example.

| WorkloadName                         | Operation | Status    | StartTime             | EndTime               |
|--------------------------------------|-----------|-----------|-----------------------|-----------------------|
| JobID                                |           |           |                       |                       |
| -----                                | -----     | -----     | -----                 | -----                 |
| testAzureFS                          | Backup    | Completed | 11/12/2018 2:42:07 PM | 11/12/2018 2:42:11 PM |
| 8bdfe3ab-9bf7-4be6-83d6-37ff1ca13ab6 |           |           |                       |                       |

Azure file share snapshots are used while the backups are taken, so usually the job completes by the time the command returns this output.

### Using on-demand backups to extend retention

On-demand backups can be used to retain your snapshots for 10 years. Schedulers can be used to run on-demand PowerShell scripts with chosen retention and thus take snapshots at regular intervals every week, month, or year. While taking regular snapshots, refer to the [limitations of on-demand backups](#) using Azure backup.

If you are looking for sample scripts, you can refer to the sample script on GitHub (<https://github.com/Azure-Samples/Use-PowerShell-for-long-term-retention-of-Azure-Files-Backup>) using Azure Automation runbook that enables you to schedule backups on a periodic basis and retain them even up to 10 years.

#### WARNING

Make sure the PS version is upgraded to the minimum version for 'Az.RecoveryServices 2.6.0' for AFS backups in your automation runbooks. You will have to replace the old 'AzureRM' module with 'Az' module. With this version, the 'friendlyName' filter is available for `Get-AzRecoveryServicesBackupItem` command. Pass the azure file share name to friendlyName parameter. If you pass the azure file share name to the 'Name' parameter, this version throws a warning to pass this friendly name to the friendly name parameter.

## Next steps

[Learn about](#) backing up Azure Files in the Azure portal.

# Restore Azure Files with PowerShell

2/7/2020 • 3 minutes to read • [Edit Online](#)

This article explains how to restore an entire file share, or specific files, from a restore point created by the [Azure Backup](#) service using Azure Powershell.

You can restore an entire file share or specific files on the share. You can restore to the original location, or to an alternate location.

## WARNING

Make sure the PS version is upgraded to the minimum version for 'Az.RecoveryServices 2.6.0' for AFS backups. For more details, refer to [the section](#) outlining the requirement for this change.

## Fetch recovery points

Use [Get-AzRecoveryServicesBackupRecoveryPoint](#) to list all recovery points for the backed-up item.

In the following script:

- The variable **\$rp** is an array of recovery points for the selected backup item from the past seven days.
- The array is sorted in reverse order of time with the latest recovery point at index **0**.
- Use standard PowerShell array indexing to pick the recovery point.
- In the example, **\$rp[0]** selects the latest recovery point.

```
$startDate = (Get-Date).AddDays(-7)
$endDate = Get-Date
$rp = Get-AzRecoveryServicesBackupRecoveryPoint -Item $afsBkpItem -StartDate $startdate.ToUniversalTime() -
EndDate $enddate.ToUniversalTime()

$rp[0] | fl
```

The output is similar to the following.

```
FileShareSnapshotUri : https://testStorageAcct.file.core.windows.net/testAzureFS?sharesnapshot=2018-11-
20T00:31:04.00000
 00Z
RecoveryPointType : FileSystemConsistent
RecoveryPointTime : 11/20/2018 12:31:05 AM
RecoveryPointId : 86593702401459
ItemName : testAzureFS
Id : /Subscriptions/00000000-0000-0000-0000-
000000000000/resourceGroups/testVaultRG/providers/Micros
oft.RecoveryServices/vaults/testVault/backupFabrics/Azure/protectionContainers/StorageContainer;storage;teststo
rageRG;testStorageAcct/protectedItems/AzureFileShare;testAzureFS/recoveryPoints/86593702401462
WorkloadType : AzureFiles
ContainerName : storage;teststorageRG;testStorageAcct
ContainerType : AzureStorage
BackupManagementType : AzureStorage
```

After the relevant recovery point is selected, you restore the file share or file to the original location, or to an alternate location.

## Restore an Azure file share to an alternate location

Use the [Restore-AzRecoveryServicesBackupItem](#) to restore to the selected recovery point. Specify these parameters to identify the alternate location:

- **TargetStorageAccountName:** The storage account to which the backed-up content is restored. The target storage account must be in the same location as the vault.
- **TargetFileShareName:** The file shares within the target storage account to which the backed-up content is restored.
- **TargetFolder:** The folder under the file share to which data is restored. If the backed-up content is to be restored to a root folder, give the target folder values as an empty string.
- **ResolveConflict:** Instruction if there's a conflict with the restored data. Accepts **Overwrite** or **Skip**.

Run the cmdlet with the parameters as follows:

```
Restore-AzRecoveryServicesBackupItem -RecoveryPoint $rp[0] -TargetStorageAccountName "TargetStorageAcct" -
TargetFileShareName "DestAFS" -TargetFolder "testAzureFS_restored" -ResolveConflict Overwrite
```

The command returns a job with an ID to be tracked, as shown in the following example.

| WorkloadName                                        | Operation | Status     | StartTime             | EndTime |
|-----------------------------------------------------|-----------|------------|-----------------------|---------|
| JobID                                               |           |            |                       |         |
| -----                                               | -----     | -----      | -----                 | -----   |
| testAzureFS<br>9fd34525-6c46-496e-980a-3740ccb2ad75 | Restore   | InProgress | 12/10/2018 9:56:38 AM |         |

## Restore an Azure file to an alternate location

Use the [Restore-AzRecoveryServicesBackupItem](#) to restore to the selected recovery point. Specify these parameters to identify the alternate location, and to uniquely identify the file you want to restore.

- **TargetStorageAccountName:** The storage account to which the backed-up content is restored. The target storage account must be in the same location as the vault.
- **TargetFileShareName:** The file shares within the target storage account to which the backed-up content is restored.
- **TargetFolder:** The folder under the file share to which data is restored. If the backed-up content is to be restored to a root folder, give the target folder values as an empty string.
- **SourceFilePath:** The absolute path of the file, to be restored within the file share, as a string. This path is the same path used in the **Get-AzStorageFile** PowerShell cmdlet.
- **SourceFileType:** Whether a directory or a file is selected. Accepts **Directory** or **File**.
- **ResolveConflict:** Instruction if there's a conflict with the restored data. Accepts **Overwrite** or **Skip**.

The additional parameters (SourceFilePath and SourceFileType) are related only to the individual file you want to restore.

```
Restore-AzRecoveryServicesBackupItem -RecoveryPoint $rp[0] -TargetStorageAccountName "TargetStorageAcct" -
TargetFileShareName "DestAFS" -TargetFolder "testAzureFS_restored" -SourceFileType File -SourceFilePath
"TestDir/TestDoc.docx" -ResolveConflict Overwrite
```

This command returns a job with an ID to be tracked, as shown in the previous section.

## Restore Azure file shares and files to the original location

When you restore to an original location, you don't need to specify destination- and target-related parameters. Only **ResolveConflict** must be provided.

#### Overwrite an Azure file share

```
Restore-AzRecoveryServicesBackupItem -RecoveryPoint $rp[0] -ResolveConflict Overwrite
```

#### Overwrite an Azure file

```
Restore-AzRecoveryServicesBackupItem -RecoveryPoint $rp[0] -SourceFileType File -SourceFilePath "TestDir/TestDoc.docx" -ResolveConflict Overwrite
```

## Next steps

[Learn about](#) restoring Azure Files in the Azure portal.

# Manage Azure file share backups with PowerShell

2/7/2020 • 2 minutes to read • [Edit Online](#)

This article describes how to use Azure PowerShell to manage and monitor the Azure file shares that are backed up by the Azure Backup service.

## WARNING

Make sure the PS version is upgraded to the minimum version for 'Az.RecoveryServices 2.6.0' for AFS backups. For more details, refer to [the section](#) outlining the requirement for this change.

## Modify the protection policy

To change the policy used for backing up the Azure file share, use [Enable-AzRecoveryServicesBackupProtection](#). Specify the relevant backup item and the new backup policy.

The following example changes the **testAzureFS** protection policy from **dailyafs** to **monthlyafs**.

```
$monthlyafsPol = Get-AzRecoveryServicesBackupProtectionPolicy -Name "monthlyafs"
$afsContainer = Get-AzRecoveryServicesBackupContainer -FriendlyName "testStorageAcct" -ContainerType
AzureStorage
$afsBkpItem = Get-AzRecoveryServicesBackupItem -Container $afsContainer -WorkloadType AzureFiles -Name
"testAzureFS"
Enable-AzRecoveryServicesBackupProtection -Item $afsBkpItem -Policy $monthlyafsPol
```

## Track backup and restore jobs

On-demand backup and restore operations return a job along with an ID, as shown when you [run an on-demand backup](#). Use the [Get-AzRecoveryServicesBackupJobDetails](#) cmdlet to track the job progress and details.

```
$job = Get-AzRecoveryServicesBackupJob -JobId 00000000-6c46-496e-980a-3740ccb2ad75 -VaultId $vaultID

$job | fl

IsCancellable : False
IsRetriable : False
ErrorDetails :
{Microsoft.Azure.Commands.RecoveryServices.Backup.Cmdlets.Models.AzureFileShareJobErrorInfo}
ActivityId : 00000000-5b71-4d73-9465-8a4a91f13a36
JobId : 00000000-6c46-496e-980a-3740ccb2ad75
Operation : Restore
Status : Failed
WorkloadName : testAFS
StartTime : 12/10/2018 9:56:38 AM
EndTime : 12/10/2018 11:03:03 AM
Duration : 01:06:24.4660027
BackupManagementType : AzureStorage

$job.ErrorDetails

 ErrorCode ErrorMessage Recommendations
----- -----
1073871825 Microsoft Azure Backup encountered an internal error. Wait for a few minutes and then try the operation again. If the issue persists, please contact Microsoft support.
```

## Stop protection on a file share

There are two ways to stop protecting Azure file shares:

- Stop all future backup jobs and *delete* all recovery points
- Stop all future backup jobs but *leave* the recovery points

There may be a cost associated with leaving the recovery points in storage, as the underlying snapshots created by Azure Backup will be retained. However, the benefit of leaving the recovery points is you can restore the file share later, if desired. For information about the cost of leaving the recovery points, see the [pricing details](#). If you choose to delete all recovery points, you can't restore the file share.

## Stop protection and retain recovery points

To stop protection while retaining data, use the [Disable-AzRecoveryServicesBackupProtection](#) cmdlet.

The following example stops protection for the *afsfileshare* file share but retains all recovery points:

```
$vaultID = Get-AzRecoveryServicesVault -ResourceGroupName "afstesting" -Name "afstest" | select -ExpandProperty ID
$bkpItem = Get-AzRecoveryServicesBackupItem -BackupManagementType AzureStorage -WorkloadType AzureFiles -Name "afsfileshare" -VaultId $vaultID
Disable-AzRecoveryServicesBackupProtection -Item $b kpItem -VaultId $vaultID
```

| WorkloadName | Operation     | Status    | StartTime            | EndTime              | JobID                                |
|--------------|---------------|-----------|----------------------|----------------------|--------------------------------------|
| -----        | -----         | -----     | -----                | -----                | -----                                |
| afsfileshare | DisableBackup | Completed | 1/26/2020 2:43:59 PM | 1/26/2020 2:44:21 PM | 98d9f8a1-54f2-4d85-8433-c32eafbd793f |

The Job ID attribute in the output corresponds to the Job ID of the job that is created by the backup service for your “stop protection” operation. To track the status of the job, use the [Get-AzRecoveryServicesBackupJob](#) cmdlet.

## Stop protection without retaining recovery points

To stop protection without retaining recovery points, use the [Disable-AzRecoveryServicesBackupProtection](#) cmdlet and add the **-RemoveRecoveryPoints** parameter.

The following example stops protection for the *afsfileshare* file share without retaining recovery points:

```
$vaultID = Get-AzRecoveryServicesVault -ResourceGroupName "afstesting" -Name "afstest" | select -ExpandProperty ID
$bkpItem = Get-AzRecoveryServicesBackupItem -BackupManagementType AzureStorage -WorkloadType AzureFiles -Name "afsfileshare" -VaultId $vaultID
Disable-AzRecoveryServicesBackupProtection -Item $bkpItem -VaultId $vaultID -RemoveRecoveryPoints
```

| WorkloadName | Operation        | Status    | StartTime            | EndTime              | JobID                                |
|--------------|------------------|-----------|----------------------|----------------------|--------------------------------------|
| -----        | -----            | -----     | -----                | -----                | -----                                |
| afsfileshare | DeleteBackupData | Completed | 1/26/2020 2:50:57 PM | 1/26/2020 2:51:39 PM | b1a61c0b-548a-4687-9d15-9db1cc5bcc85 |

## Next steps

[Learn about](#) managing Azure file share backups in the Azure portal.

# Backup Azure file share using Azure Backup via Rest API

2/18/2020 • 9 minutes to read • [Edit Online](#)

This article describes how to back up an Azure File share using Azure Backup via REST API.

This article assumes you've already created a recovery services vault and policy for configuring backup for your file share. If you haven't, refer to the [create vault](#) and [create policy](#) REST API tutorials for creating new vaults and policies.

For this article, we'll use the following resources:

- **RecoveryServicesVault:** *azurefilesvault*
- **Policy:** *schedule1*
- **Resource group:** *azurefiles*
- **Storage Account:** *testvault2*
- **File Share:** *testshare*

## Configure backup for an unprotected Azure file share using REST API

### Discover storage accounts with unprotected Azure file shares

The vault needs to discover all Azure storage accounts in the subscription with file shares that can be backed up to the Recovery Services Vault. This is triggered using the [refresh operation](#). It's an asynchronous *POST* operation that ensures the vault gets the latest list of all unprotected Azure File shares in the current subscription and 'caches' them. Once the file share is 'cached', Recovery services can access the file share and protect it.

```
POST
https://management.azure.com/Subscriptions/{subscriptionId}/resourceGroups/{vaultresourceGroupName}/providers/Microsoft.RecoveryServices/vaults/{vaultName}/backupFabrics/{fabricName}/refreshContainers?api-version=2016-12-01&$filter={$filter}
```

The POST URI has `{subscriptionId}` , `{vaultName}` , `{vaultresourceGroupName}` , and `{fabricName}` parameters. In our example, the value for the different parameters would be as follows:

- `{fabricName}` is *Azure*
- `{vaultName}` is *azurefilesvault*
- `{vaultresourceGroupName}` is *azurefiles*
- `$filter=backupManagementType eq 'AzureStorage'`

Since all the required parameters are given in the URI, there's no need for a separate request body.

```
POST https://management.azure.com/Subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/refreshContainers?api-version=2016-12-01&$filter=backupManagementType eq 'AzureStorage'
```

### Responses

The 'refresh' operation is an [asynchronous operation](#). It means this operation creates another operation that needs to be tracked separately.

It returns two responses: 202 (Accepted) when another operation is created, and 200 (OK) when that operation completes.

#### Example responses

Once the *POST* request is submitted, a 202 (Accepted) response is returned.

```
HTTP/1.1 202 Accepted
'Pragma': 'no-cache'
'Expires': '-1'
'Location': 'https://management.azure.com/Subscriptions/00000000-0000-0000-0000-000000000000/ResourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/operationResults/cca47745-12d2-42f9-b3a4-75335f18fdf6?api-version=2016-12-01'
'Retry-After': '60'
'X-Content-Type-Options': 'nosniff'
'x-ms-request-id': '6cc12ceb-90a2-430d-a1ec-9b6b6fdea92b'
'x-ms-client-request-id': '3da383a5-d66d-4b7c-982a-bc8d94798d61,3da383a5-d66d-4b7c-982a-bc8d94798d61'
'Strict-Transport-Security': 'max-age=31536000; includeSubDomains'
'X-Powered-By': 'ASP.NET'
'x-ms-ratelimit-remaining-subscription-reads': '11996'
'x-ms-correlation-request-id': '6cc12ceb-90a2-430d-a1ec-9b6b6fdea92b'
'x-ms-routing-request-id': 'CENTRALUSEUAP:20200203T091326Z:6cc12ceb-90a2-430d-a1ec-9b6b6fdea92b'
'Date': 'Mon, 03 Feb 2020 09:13:25 GMT'
```

Track the resulting operation using the "Location" header with a simple *GET* command

```
GET https://management.azure.com/Subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/operationResults/cca47745-12d2-42f9-b3a4-75335f18fdf6?api-version=2016-12-01
```

Once all the Azure Storage accounts are discovered, the *GET* command returns a 200 (No Content) response. The vault is now able to discover any storage account with file shares that can be backed up within the subscription.

```
HTTP/1.1 200 NoContent
Cache-Control : no-cache
Pragma : no-cache
X-Content-Type-Options : nosniff
x-ms-request-id : d9bdb266-8349-4dbd-9688-de52f07648b2
x-ms-client-request-id : 3da383a5-d66d-4b7c-982a-bc8d94798d61,3da383a5-d66d-4b7c-982a-bc8d94798d61
Strict-Transport-Security : max-age=31536000; includeSubDomains
X-Powered-By : ASP.NET
x-ms-ratelimit-remaining-subscription-reads: 11933
x-ms-correlation-request-id : d9bdb266-8349-4dbd-9688-de52f07648b2
x-ms-routing-request-id : CENTRALUSEUAP:20200127T105304Z:d9bdb266-8349-4dbd-9688-de52f07648b2
Date : Mon, 27 Jan 2020 10:53:04 GMT
```

## Get List of storage accounts that can be protected with Recovery Services vault

To confirm that "caching" is done, list all protectable storage accounts under the subscription. Then locate the desired storage account in the response. This is done using the [GET ProtectableContainers](#) operation.

```
GET https://management.azure.com/Subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/protectableContainers?api-version=2016-12-01$filter=backupManagementType eq 'AzureStorage'
```

The *GET* URI has all the required parameters. No additional request body is needed.

Example of response body:

```
{
 "value": [
 {
 "id": "/Subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/protectableContainers/StorageContainer;Storage;AzureFiles;testvault2",
 "name": "StorageContainer;Storage;AzureFiles;testvault2",
 "type": "Microsoft.RecoveryServices/vaults/backupFabrics/protectableContainers",
 "properties": {
 "friendlyName": "testvault2",
 "backupManagementType": "AzureStorage",
 "protectableContainerType": "StorageContainer",
 "healthStatus": "Healthy",
 "containerId": "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/AzureFiles/providers/Microsoft.Storage/storageAccounts/testvault2"
 }
 }
]
}
```

Since we can locate the *testvault2* storage account in the response body with the friendly name, the refresh operation performed above was successful. The recovery services vault can now successfully discover storage accounts with unprotected files shares in the same subscription.

### **Register storage account with Recovery Services vault**

This step is only needed if you didn't register the storage account with the vault earlier. You can register the vault via the [ProtectionContainers-Register operation](#).

```
PUT
https://management.azure.com/Subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.RecoveryServices/vaults/{vaultName}/backupFabrics/{fabricName}/protectionContainers/{containerName}?api-version=2016-12-01
```

Set the variables for the URI as follows:

- {resourceGroupName} - *azurefiles*
- {fabricName} - *Azure*
- {vaultName} - *azurefilesvault*
- {containerName} - This is the name attribute in the response body of the GET ProtectableContainers operation. In our example, it's *StorageContainer;Storage;AzureFiles;testvault2*

**NOTE**

Always take the name attribute of the response and fill it in this request. Do NOT hard-code or create the container-name format. If you create or hard-code it, the API call will fail if the container-name format changes in the future.

```
PUT https://management.azure.com/Subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/AzureFiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/protectionContainers/StorageContainer;Storage;AzureFiles;testvault2?api-version=2016-12-01
```

The create request body is as follows:

```
{
 "properties": {

 "containerType": "StorageContainer",

 "sourceResourceId": "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/AzureFiles/providers/Microsoft.Storage/storageAccounts/testvault2",

 "resourceGroup": "AzureFiles",

 "friendlyName": "testvault2",

 "backupManagementType": "AzureStorage"

 }
}
```

For the complete list of definitions of the request body and other details, refer to [ProtectionContainers-Register](#).

This is an asynchronous operation and returns two responses: "202 Accepted" when the operation is accepted and "200 OK" when the operation is complete. To track the operation status, use the location header to get the latest status of the operation.

```
GET https://management.azure.com/Subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/AzureFiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/protectionContainers/StorageContainer;Storage;AzureFiles;testvault2/operationresults/1a3c8ee7-e0e5-43ed-b8b3-73cc992b6db9?api-version=2016-12-01
```

Example of response body when operation is complete:

```
{
 "id": "/Subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/AzureFiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/
protectionContainers/StorageContainer;Storage;AzureFiles;testvault2",
 "name": "StorageContainer;Storage;AzureFiles;testvault2",
 "properties": {
 "sourceResourceId": "/subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/AzureFiles/providers/Microsoft.Storage/storageAccounts/testvault2",
 "protectedItemCount": 0,
 "friendlyName": "testvault2",
 "backupManagementType": "AzureStorage",
 "registrationStatus": "Registered",
 "healthStatus": "Healthy",
 "containerType": "StorageContainer",
 "protectableObjectType": "StorageContainer"
 }
}
```

You can verify if the registration was successful from the value of the *registrationstatus* parameter in the response body. In our case, it shows the status as registered for *testvault2*, so the registration operation was successful.

### Inquire all unprotected files shares under a storage account

You can inquire about protectable items in a storage account using the [Protection Containers-Inquire](#) operation. It's an asynchronous operation and the results should be tracked using the location header.

```
POST
https://management.azure.com/Subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.RecoveryServices/vaults/{vaultName}/backupFabrics/{fabricName}/protectionContainers/{containerName}/inquire
?api-version=2016-12-01
```

Set the variables for the above URI as follows:

- {vaultName} - *azurefilesvault*
- {fabricName} - *Azure*
- {containerName}- Refer to the name attribute in the response body of the GET ProtectableContainers operation. In our example, it's *StorageContainer;Storage;AzureFiles;testvault2*

```
https://management.azure.com/Subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/protectionContainers/StorageContainer;Storage;AzureFiles;testvault2/inquire?api-version=2016-12-01
```

Once the request is successful, it returns the status code "OK"

```
Cache-Control : no-cache
Pragma : no-cache
X-Content-Type-Options: nosniff
x-ms-request-id : 68727f1e-b8cf-4bf1-bf92-8e03a9d96c46
x-ms-client-request-id : 3da383a5-d66d-4b7c-982a-bc8d94798d61,3da383a5-d66d-4b7c-982a-bc8d94798d61
Strict-Transport-Security: max-age=31536000; includeSubDomains
Server : Microsoft-IIS/10.0
X-Powered-B : ASP.NET
x-ms-ratelimit-remaining-subscription-reads: 11932
x-ms-correlation-request-id : 68727f1e-b8cf-4bf1-bf92-8e03a9d96c46
x-ms-routing-request-id : CENTRALUSEUAP:20200127T105305Z:68727f1e-b8cf-4bf1-bf92-8e03a9d96c46
Date : Mon, 27 Jan 2020 10:53:05 GMT
```

### Select the file share you want to back up

You can list all protectable items under the subscription and locate the desired file share to be backed up using the [GET backupprotectableItems](#) operation.

```
GET
```

```
https://management.azure.com/Subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.RecoveryServices/vaults/{vaultName}/backupProtectableItems?api-version=2016-12-01&$filter={$filter}
```

Construct the URI as follows:

- {vaultName} - *azurefilesvault*
- {\$filter} - *backupManagementType eq 'AzureStorage'*

```
GET https://management.azure.com/Subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupProtectableItems?$filter=backupManagementType eq 'AzureStorage'&api-version=2016-12-01
```

Sample response:

Status Code:200

```
{
 "value": [
 {
 "id": "/Subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/protectionContainers/storagecontainer;storage;azurefiles;afaccount1/protectableItems/azurefileshare;azurefiles1",
 "name": "azurefileshare;azurefiles1",
 "type": "Microsoft.RecoveryServices/vaults/backupFabrics/protectionContainers/protectableItems",
 "properties": {
 "parentContainerFabricId": "/subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/AzureFiles/providers/Microsoft.Storage/storageAccounts/afaccount1",
 "parentContainerFriendlyName": "afaccount1",
 "azureFileShareType": "XSMB",
 "backupManagementType": "AzureStorage",
 "workloadType": "AzureFileShare",
 "protectableItemType": "AzureFileShare",
 "friendlyName": "azurefiles1",
 "protectionState": "NotProtected"
 }
 },
 {
 "id": "/Subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/protectionContainers/storagecontainer;storage;azurefiles;afsaccount/protectableItems/azurefileshare;afsresource",
 "name": "azurefileshare;afsresource",
 "type": "Microsoft.RecoveryServices/vaults/backupFabrics/protectionContainers/protectableItems",
 "properties": {
 "parentContainerFabricId": "/subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/AzureFiles/providers/Microsoft.Storage/storageAccounts/afsaccount",
 "parentContainerFriendlyName": "afsaccount",
 "azureFileShareType": "XSMB",
 "backupManagementType": "AzureStorage",
 "workloadType": "AzureFileShare",
 "protectableItemType": "AzureFileShare",
 "friendlyName": "afsresource",
 "protectionState": "NotProtected"
 }
 },
 {
 "id": "/Subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/protectionContainers/storagecontainer;storage;azurefiles;testvault2/protectableItems/azurefileshare;testshare",
 "name": "azurefileshare;testshare",
 "type": "Microsoft.RecoveryServices/vaults/backupFabrics/protectionContainers/protectableItems",
 "properties": {
 "parentContainerFabricId": "/subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/AzureFiles/providers/Microsoft.Storage/storageAccounts/testvault2",
 "parentContainerFriendlyName": "testvault2",
 "azureFileShareType": "XSMB",
 "backupManagementType": "AzureStorage",
 "workloadType": "AzureFileShare",
 "protectableItemType": "AzureFileShare",
 "friendlyName": "testshare",
 "protectionState": "NotProtected"
 }
 }
]
}
```

The response contains the list of all unprotected file shares and contains all the information required by the Azure Recovery Service to configure the backup.

## Enable backup for the file share

After the relevant file share is "identified" with the friendly name, select the policy to protect. To learn more about existing policies in the vault, refer to [list Policy API](#). Then select the [relevant policy](#) by referring to the policy name. To create policies, refer to [create policy tutorial](#).

Enabling protection is an asynchronous *PUT* operation that creates a "protected item".

```
PUT
```

```
https://management.azure.com/Subscriptions/{subscriptionId}/resourceGroups/{vaultresourceGroupName}/providers/Microsoft.RecoveryServices/vaults/{vaultName}/backupFabrics/{fabricName}/protectionContainers/{containerName}/protectedItems/{protectedItemName}?api-version=2019-05-13
```

Set the **containername** and **protecteditemName** variables using the ID attribute in the response body of the GET `backupprotectableitems` operation.

In our example, the ID of file share we want to protect is:

```
"/Subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/protectionContainers/storagecontainer;storage;azurefiles;testvault2/protectableItems/azurefileshare;testshare
```

- {containername} - *storagecontainer;storage;azurefiles;testvault2*
- {protectedItemName} - *azurefileshare;testshare*

Or you can refer to the **name** attribute of the protection container and protectable item responses.

### NOTE

Always take the name attribute of the response and fill it in this request. Do NOT hard-code or create the container-name format or protected item name format. If you create or hard-code it, the API call will fail if the container-name format or protected item name format changes in the future.

```
PUT https://management.azure.com/Subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/protectionContainers/StorageContainer;Storage;AzureFiles;testvault2/protectedItems/azurefileshare;testshare?api-version=2016-12-01
```

Create a request body:

The following request body defines properties required to create a protected item.

```
{
 "properties": {
 "protectedItemType": "AzureFileShareProtectedItem",
 "sourceResourceId": "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/AzureFiles/providers/Microsoft.Storage/storageAccounts/testvault2",
 "policyId": "/Subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupPolicies/schedule1"
 }
}
```

The **sourceResourceId** is the **parentcontainerFabricID** in response of GET `backupprotectableitems`.

## Sample Response

The creation of a protected item is an asynchronous operation, which creates another operation that needs to be tracked. It returns two responses: 202 (Accepted) when another operation is created and 200 (OK) when that operation completes.

Once you submit the *PUT* request for protected item creation or update, the initial response is 202 (Accepted) with a location header.

```
HTTP/1.1 202 Accepted
Cache-Control : no-cache
Pragma : no-cache
Location : https://management.azure.com/Subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabric
s/Azure/protectionContainers/StorageContainer;Storage;AzureFiles;testvault2/protectedItems/azurefileshare;tests
hare/operationResults/c3a52d1d-0853-4211-8141-477c65740264?api-version=2016-12-01
Retry-After : 60
Azure-AsyncOperation : https://management.azure.com/Subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabric
s/Azure/protectionContainers/StorageContainer;Storage;AzureFiles;testvault2/protectedItems/azurefileshare;tests
hare/operationResults/c3a52d1d-0853-4211-8141-477c65740264?api-version=2016-12-01
X-Content-Type-Options : nosniff
x-ms-request-id : b55527fa-f473-4f09-b169-9cc3a7a39065
x-ms-client-request-id: 3da383a5-d66d-4b7c-982a-bc8d94798d61,3da383a5-d66d-4b7c-982a-bc8d94798d61
Strict-Transport-Security : max-age=31536000; includeSubDomains
X-Powered-By : ASP.NET
x-ms-ratelimit-remaining-subscription-writes: 1198
x-ms-correlation-request-id : b55527fa-f473-4f09-b169-9cc3a7a39065
x-ms-routing-request-id : CENTRALUSEUAP:20200127T105412Z:b55527fa-f473-4f09-b169-9cc3a7a39065
Date : Mon, 27 Jan 2020 10:54:12 GMT
```

Then track the resulting operation using the location header or Azure-AsyncOperation header with a *GET* command.

```
GET https://management.azure.com/Subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupOperat
ions/c3a52d1d-0853-4211-8141-477c65740264?api-version=2016-12-01
```

Once the operation completes, it returns 200 (OK) with the protected item content in the response body.

Sample Response Body:

```
{
 "id": "c3a52d1d-0853-4211-8141-477c65740264",
 "name": "c3a52d1d-0853-4211-8141-477c65740264",
 "status": "Succeeded",
 "startTime": "2020-02-03T18:10:48.296012Z",
 "endTime": "2020-02-03T18:10:48.296012Z",
 "properties": {
 "objectType": "OperationStatusJobExtendedInfo",
 "jobId": "e2ca2cf4-2eb9-4d4b-b16a-8e592d2a658b"
 }
}
```

This confirms that protection is enabled for the file share and the first backup will be triggered according to the policy schedule.

## Trigger an on-demand backup for file share

Once an Azure file share is configured for backup, backups run according to the policy schedule. You can wait for

the first scheduled backup or trigger an on-demand backup anytime.

Triggering an on-demand backup is a POST operation.

```
POST
```

```
https://management.azure.com/Subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.RecoveryServices/vaults/{vaultName}/backupFabrics/{fabricName}/protectionContainers/{containerName}/protectedItems/{protectedItemName}/backup?api-version=2016-12-01
```

{containerName} and {protectedItemName} are as constructed above while enabling backup. For our example, this translates to:

```
POST https://management.azure.com/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/protectionContainers/StorageContainer;storage;azurefiles;testvault2/protectedItems/AzureFileShare;testsshare/backup?api-version=2017-07-01
```

## Create request body

To trigger an on-demand backup, following are the components of the request body.

| NAME       | TYPE                       | DESCRIPTION                      |
|------------|----------------------------|----------------------------------|
| Properties | AzurefilesharebackupReques | BackupRequestResource properties |

For the complete list of definitions of the request body and other details, refer to [trigger backups for protected items REST API document](#).

## Request Body example

```
{
 "properties":{
 "objectType":"AzureFileShareBackupRequest",
 "recoveryPointExpiryTimeInUTC":"2020-03-07T18:29:59.000Z"
 }
}
```

## Responses

Triggering an on-demand backup is an [asynchronous operation](#). It means this operation creates another operation that needs to be tracked separately.

It returns two responses: 202 (Accepted) when another operation is created and 200 (OK) when that operation completes.

## Example responses

Once you submit the *POST* request for an on-demand backup, the initial response is 202 (Accepted) with a location header or Azure-async-header.

```
'Cache-Control': 'no-cache'
'Pragma': 'no-cache'
'Expires': '-1'
'Location': https://management.azure.com/subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabric
s/Azure/protectionContainers/StorageContainer;storage;azurefiles;testvault2/protectedItems/AzureFileShare;tests
hare/operationResults/dc62d524-427a-4093-968d-e951c0a0726e?api-version=2017-07-01
'Retry-After': '60'
'Azure-AsyncOperation': https://management.azure.com/subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabric
s/Azure/protectionContainers/StorageContainer;storage;azurefiles;testvault2/protectedItems/AzureFileShare;tests
hare/operationsStatus/dc62d524-427a-4093-968d-e951c0a0726e?api-version=2017-07-01
'X-Content-Type-Options': 'nosniff'
'x-ms-request-id': '2e03b8d4-66b1-48cf-8094-aa8bff57e8fb'
'x-ms-client-request-id': 'a644712a-4895-11ea-ba57-0a580af42708, a644712a-4895-11ea-ba57-0a580af42708'
'Strict-Transport-Security': 'max-age=31536000; includeSubDomains'
'X-Powered-By': 'ASP.NET'
'x-ms-ratelimit-remaining-subscription-writes': '1199'
'x-ms-correlation-request-id': '2e03b8d4-66b1-48cf-8094-aa8bff57e8fb'
'x-ms-routing-request-id': 'WESTEUROPE:20200206T040339Z:2e03b8d4-66b1-48cf-8094-aa8bff57e8fb'
'Date': 'Thu, 06 Feb 2020 04:03:38 GMT'
'Content-Length': '0'
```

Then track the resulting operation using the location header or Azure-AsyncOperation header with a *GET* command.

```
GET https://management.azure.com/Subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupOperat
ions/dc62d524-427a-4093-968d-e951c0a0726e?api-version=2016-12-01
```

Once the operation completes, it returns 200 (OK) with the ID of the resulting backup job in the response body.

#### Sample response body

```
{
 "id": "dc62d524-427a-4093-968d-e951c0a0726e",
 "name": "dc62d524-427a-4093-968d-e951c0a0726e",
 "status": "Succeeded",
 "startTime": "2020-02-06T11:06:02.1327954Z",
 "endTime": "2020-02-06T11:06:02.1327954Z",
 "properties": {
 "objectType": "OperationStatusJobExtendedInfo",
 "jobId": "39282261-cb52-43f5-9dd0-ffaf66beeaef"
 }
}
```

Since the backup job is a long running operation, it needs to be tracked as explained in the [monitor jobs using REST API document](#).

## Next steps

- Learn how to [restore Azure file shares using Rest API](#).

# Restore Azure File Shares using REST API

2/18/2020 • 6 minutes to read • [Edit Online](#)

This article explains how to restore an entire file share or specific files from a restore point created by [Azure Backup](#) by using the REST API.

By the end of this article, you'll learn how to perform the following operations using REST API:

- View restore points for a backed-up Azure file share.
- Restore a full Azure file share.
- Restore individual files or folders.

## Prerequisites

We assume that you already have a backed-up file share you want to restore. If you don't, check [Backup Azure file share using REST API](#) to learn how to create one.

For this article, we'll use the following resources:

- **RecoveryServicesVault:** *azurefilesvault*
- **Resource group:** *azurefiles*
- **Storage Account:** *afsaccount*
- **File Share:** *azurefiles*

## Fetch ContainerName and ProtectedItemName

For most of the restore related API calls, you need to pass values for the {containerName} and {protectedItemName} URI parameters. Use the ID attribute in the response body of the [GET backupprotectableitems](#) operation to retrieve values for these parameters. In our example, the ID of the file share we want to protect is:

```
"/Subscriptions/ef4ab5a7-c2c0-4304-af80-af49f48af3d1/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/protectionContainers/storagecontainer;storage;azurefiles;afsaccount/pr
```

So the values translate as follows:

- {containername} - *storagecontainer;storage;azurefiles;afsaccount*
- {protectedItemName} - *azurefileshare;azurefiles*

## Fetch recovery points for backed up Azure file share

To restore any backed-up file share or files, first select a recovery point to perform the restore operation. The available recovery points of a backed-up item can be listed using the [Recovery Point-List](#) REST API call. It's a GET operation with all the relevant values.

```
GET
https://management.azure.com/Subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.RecoveryServices/vaults/{vaultName}/backupFabrics/{fabricName}/protectionContainers/{containerName}/protectedItems/{protectedItemName}/recoveryPoints?api-version=2019-05-13&$filter={$filter}
```

Set the URI values as follows:

- {fabricName}: *Azure*
- {vaultName}: *azurefilesvault*
- {containername}: *storagecontainer;storage;azurefiles;afsaccount*
- {protectedItemName}: *azurefileshare;azurefiles*
- {ResourceGroupName}: *azurefiles*

The GET URI has all the required parameters. There's no need for an additional request body.

```
GET https://management.azure.com/Subscriptions/ef4ab5a7-c2c0-4304-af80-af49f48af3d1/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/protectionContainers/StorageContainer;storage;azur
efiles;afsaccount/protectedItems/AzureFileShare;azurefiles/recoveryPoints?api-version=2019-05-13
```

## Example response

Once the GET URI is submitted, a 200 response is returned:

```

HTTP/1.1" 200 None
'Cache-Control': 'no-cache'
'Pragma': 'no-cache'
'Transfer-Encoding': 'chunked'
'Content-Type': 'application/json'
'Content-Encoding': 'gzip'
'Expires': '-1'
'Vary': 'Accept-Encoding'
'X-Content-Type-Options': 'nosniff'
'x-ms-request-id': '6d8d7951-7d97-4c49-9a2d-7fbaab55233a'
'x-ms-client-request-id': '4edb5a58-47ea-11ea-a27a-0a580af41908', 4edb5a58-47ea-11ea-a27a-0a580af41908'
'Strict-Transport-Security': 'max-age=31536000; includeSubDomains'
'Server': 'Microsoft-IIS/10.0'
'X-Powered-By': 'ASP.NET'
'x-ms-ratelimit-remainging-subscription-reads': '11998'
'x-ms-correlation-request-id': '6d8d7951-7d97-4c49-9a2d-7fbaab55233a'
'x-ms-routing-request-id': 'WESTEUROPE:20200205T073708Z:d68d7951-7d97-4c49-9a2d-7fbaab55233a'
'Date': 'Wed, 05 Feb 2020 07:37:08 GMT'
{
 "value": [
 {
 "eTag": null,
 "id": "/Subscriptions/ef4ab5a7-c2c0-4304-af80-
af49f48af3d1/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/protectionContainers/StorageContainer;storage;azur
efiles;afsaccount/protectedItems/AzureFileShare;azurefiles/recoveryPoints/932881138555802864",
 "location": null,
 "name": "932881138555802864",
 "properties": {
 "fileShareSnapshotUri": "https://afsaccount.file.core.windows.net/azurefiles?sharesnapshot=2020-02-04T08:01:35.0000000Z",
 "objectType": "AzureFileShareRecoveryPoint",
 "recoveryPointSizeInGb": 1,
 "recoveryPointTime": "2020-02-04T08:01:35+00:00",
 "recoveryPointType": "FileSystemConsistent"
 },
 "resourceGroup": "azurefiles",
 "tags": null,
 "type": "Microsoft.RecoveryServices/vaults/backupFabrics/protectionContainers/protectedItems/recoveryPoints"
 },
 {
 "eTag": null,
 "id": "/Subscriptions/ef4ab5a7-c2c0-4304-af80-
af49f48af3d1/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/protectionContainers/StorageContainer;storage;azur
efiles;afsaccount/protectedItems/AzureFileShare;azurefiles/recoveryPoints/932878582606969225",
 "location": null,
 "name": "932878582606969225",
 "properties": {
 "fileShareSnapshotUri": "https://afsaccount.file.core.windows.net/azurefiles?sharesnapshot=2020-02-03T08:05:30.0000000Z",
 "objectType": "AzureFileShareRecoveryPoint",
 "recoveryPointSizeInGb": 1,
 "recoveryPointTime": "2020-02-03T08:05:30+00:00",
 "recoveryPointType": "FileSystemConsistent"
 },
 "resourceGroup": "azurefiles",
 "tags": null,
 "type": "Microsoft.RecoveryServices/vaults/backupFabrics/protectionContainers/protectedItems/recoveryPoints"
 },
 {
 "eTag": null,
 "id": "/Subscriptions/ef4ab5a7-c2c0-4304-af80-
af49f48af3d1/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/protectionContainers/StorageContainer;storage;azur
efiles;afsaccount/protectedItems/AzureFileShare;azurefiles/recoveryPoints/932890167574511261",
 "location": null,
 "name": "932890167574511261",
 "properties": {
 "fileShareSnapshotUri": "https://afsaccount.file.core.windows.net/azurefiles?sharesnapshot=2020-02-02T08:03:50.0000000Z",
 "objectType": "AzureFileShareRecoveryPoint",
 "recoveryPointSizeInGb": 1,
 "recoveryPointTime": "2020-02-02T08:03:50+00:00",
 "recoveryPointType": "FileSystemConsistent"
 },
 "resourceGroup": "azurefiles",
 "tags": null,
 "type": "Microsoft.RecoveryServices/vaults/backupFabrics/protectionContainers/protectedItems/recoveryPoints"
 }
]
}

```

The recovery point is identified with the {name} field in the response above.

## Full share recovery using REST API

Use this restore option to restore the complete file share in the original or an alternate location. Triggering restore is a POST request and you can perform this operation using the [trigger restore](#) REST API.

```

POST
https://management.azure.com/Subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.RecoveryServices/vaults/{vaultName}/backupFabrics/{fab
ricName}/protectionContainers/{containerName}/protectedItems/{protectedItemName}/recoveryPoints/{recoveryPointId}/restore?api-version=2019-05-13

```

The values {containerName} and {protectedItemName} are as set [here](#) and recoveryPointID is the {name} field of the recovery point mentioned above.

```

POST https://management.azure.com/Subscriptions/ef4ab5a7-c2c0-4304-af80-
af49f48af3d1/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/protectionContainers/StorageContainer;storage;azur
efiles;afsaccount/protectedItems/AzureFileShare%3Bazurefiles/recoveryPoints/932886657837421071/restore?api-version=2019-05-13

```

### Create request body

To trigger a restore for an Azure file share, the following are the components of the request body:

| NAME       | TYPE                         | DESCRIPTION                       |
|------------|------------------------------|-----------------------------------|
| Properties | AzureFileShareRestoreRequest | RestoreRequestResource properties |

For the complete list of definitions of the request body and other details, refer to the [trigger Restore REST API document](#).

## Restore to original location

### Request body example

The following request body defines properties required to trigger an Azure file share restore:

```
{
 "properties": {
 "objectType": "AzureFileShareRestoreRequest",
 "recoveryType": "Originallocation",
 "sourceResourceId": "/subscriptions/ef4ab5a7-c2c0-4304-af80-af49f48af3d1/resourceGroups/AzureFiles/providers/Microsoft.Storage/storageAccounts/afsaccount",
 "copyOptions": "Overwrite",
 "restoreRequestType": "FullShareRestore"
 }
}
```

## Restore to alternate location

Specify the following parameters for alternate location recovery:

- **targetResourceId**: The storage account to which the backed-up content is restored. The target storage account must be in the same location as the vault.
- **name**: The file share within the target storage account to which the backed-up content is restored.
- **targetFolderPath**: The folder under the file share to which data is restored.

### Request body example

The following request body restores the *azurefiles* file share in the *afsaccount* storage account to the *azurefiles1* file share in the *afaccount1* storage account.

```
{
 "properties": {
 "objectType": "AzureFileShareRestoreRequest",
 "recoveryType": "AlternateLocation",
 "sourceResourceId": "/subscriptions/ef4ab5a7-c2c0-4304-af80-af49f48af3d1/resourceGroups/AzureFiles/providers/Microsoft.Storage/storageAccounts/afsaccount",
 "copyOptions": "Overwrite",
 "restoreRequestType": "FullShareRestore",
 "restoreFileSpecs": [
 {
 "targetFolderPath": "restoredata"
 }
],
 "targetDetails": {
 "name": "azurefiles1",
 "targetResourceId": "/subscriptions/ef4ab5a7-c2c0-4304-af80-af49f48af3d1/resourceGroups/AzureFiles/providers/Microsoft.Storage/storageAccounts/afaccount1"
 }
 }
}
```

## Response

The triggering of a restore operation is an [asynchronous operation](#). This operation creates another operation that needs to be tracked separately. It returns two responses: 202 (Accepted) when another operation is created, and 200 (OK) when that operation completes.

### Response example

Once you submit the *POST* URI for triggering a restore, the initial response is 202 (Accepted) with a location header or Azure-async-header.

```
HTTP/1.1" 202
'Cache-Control': 'no-cache'
'Pragma': 'no-cache'
'Expires': '-1'
'Location': 'https://management.azure.com/Subscriptions/ef4ab5a7-c2c0-4304-af80-af49f48af3d1/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/protectionContainers/StorageContainer;storage;azurefiles;afsaccount/protectedItems/AzureFileShare;azurefiles/operationsResults/68ccfb1-a64f-4b29-b955-314b5790cfa9?api-version=2019-05-13'
'Retry-After': '60'
'Azure-AsyncOperation': 'https://management.azure.com/Subscriptions/ef4ab5a7-c2c0-4304-af80-af49f48af3d1/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/protectionContainers/StorageContainer;storage;azurefiles;afsaccount/protectedItems/AzureFileShare;azurefiles/operationsStatus/68ccfb1-a64f-4b29-b955-314b5790cfa9?api-version=2019-05-13'
'X-Content-Type-Options': 'nosniff'
'x-ms-request-id': '2426777d-c5ec-44b6-a324-384f8947460c'
'x-ms-client-request-id': '3c743096-47eb-11ea-ae90-0a580af41908, 3c743096-47eb-11ea-ae90-0a580af41908'
'Strict-Transport-Security': 'max-age=31536000; includeSubDomains'
'X-Powered-By': 'ASP.NET'
'X-ms-ratelimit-remaining-subscription-writes': '1199'
'x-ms-correlation-request-id': '2426777d-c5ec-44b6-a324-384f8947460c'
'x-ms-routing-request-id': 'WESTEUROPE:20200205T074347Z:2426777d-c5ec-44b6-a324-384f8947460c'
'Date': 'Wed, 05 Feb 2020 07:43:47 GMT'
```

Then track the resulting operation using the location header or the Azure-AsyncOperation header with a GET command.

```
GET https://management.azure.com/Subscriptions/ef4ab5a7-c2c0-4304-af80-af49f48af3d1/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupOperations/68ccfb1-a64f-4b29-b955-314b5790cfa9?api-version=2016-12-01
```

Once the operation completes, it returns 200 (OK) with the ID of the resulting restore job in the response body.

```

HTTP/1.1" 200
'Cache-Control': 'no-cache'
'Pragma': 'no-cache'
'Transfer-Encoding': 'chunked'
'Content-Type': 'application/json'
'Content-Encoding': 'gzip'
'Expires': '-1'
'Vary': 'Accept-Encoding'
'X-Content-Type-Options': 'nosniff'
'x-ms-request-id': '41ee89b2-3be4-40d8-8ff6-f5592c2571e3'
'x-ms-client-request-id': '3c743096-47eb-11ea-ae90-0a580af41908, 3c743096-47eb-11ea-ae90-0a580af41908'
'Strict-Transport-Security': 'max-age=31536000; includeSubDomains'
'Server': 'Microsoft-IIS/10.0'
'X-Powered-By': 'ASP.NET'
'x-ms-ratelimit-remaining-subscription-reads': '11998'
'x-ms-correlation-request-id': '41ee89b2-3be4-40d8-8ff6-f5592c2571e3'
'x-ms-routing-request-id': 'WESTEUROPE:20200205T074348Z:41ee89b2-3be4-40d8-8ff6-f5592c2571e3'
'Date': 'Wed, 05 Feb 2020 07:43:47 GMT'
{
 "id": "/Subscriptions/ef4ab5a7-c2c0-4304-af80-af49f48af3d1/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupJobs/a7e97e42-4e54-4d4b-b449-26fcf946f42c",
 "location": null,
 "name": "a7e97e42-4e54-4d4b-b449-26fcf946f42c",
 "properties": {
 "actionsInfo": [
 "Cancellable"
],
 "activityId": "3c743096-47eb-11ea-ae90-0a580af41908",
 "backupManagementType": "AzureStorage",
 "duration": "0:00:01.863098",
 "endTime": null,
 "entityFriendlyName": "azurefiles",
 "errorDetails": null,
 "extendedInfo": {
 "dynamicErrorMessage": null,
 "propertyBag": {},
 "tasksList": []
 },
 "jobType": "AzureStorageJob",
 "operation": "Restore",
 "startTime": "2020-02-05T07:43:47.144961+00:00",
 "status": "InProgress",
 "storageAccountName": "afsaccount",
 "storageAccountVersion": "Storage"
 },
 "resourceGroup": "azurefiles",
 "tags": null,
 "type": "Microsoft.RecoveryServices/vaults/backupJobs"
}

```

For alternate location recovery, the response body will be like this:

```

{
 "id": "/Subscriptions/ef4ab5a7-c2c0-4304-af80-af49f48af3d1/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupJobs/7e0ee41e-6e31-4728-a25c-98ff6b777641",
 "location": null,
 "name": "7e0ee41e-6e31-4728-a25c-98ff6b777641",
 "properties": {
 "actionsInfo": [
 "Cancellable"
],
 "activityId": "6077be6e-483a-11ea-a915-0a580af4ad72",
 "backupManagementType": "AzureStorage",
 "duration": "0:00:02.171965",
 "endTime": null,
 "entityFriendlyName": "azurefiles",
 "errorDetails": null,
 "extendedInfo": {
 "dynamicErrorMessage": null,
 "propertyBag": {
 "Data Transferred (in MB)": "0",
 "Job Type": "Recover to an alternate file share",
 "Number Of Failed Files": "0",
 "Number Of Restored Files": "0",
 "Number Of Skipped Files": "0",
 "RestoreDestination": "afsaccount1/azurefiles1/restoreddata",
 "Source File Share Name": "azurefiles",
 "Source Storage Account Name": "afsaccount",
 "Target File Share Name": "azurefiles1",
 "Target Storage Account Name": "afsaccount1"
 },
 "tasksList": []
 },
 "jobType": "AzureStorageJob",
 "operation": "Restore",
 "startTime": "2020-02-05T17:10:18.106532+00:00",
 "status": "InProgress",
 "storageAccountName": "afsaccount",
 "storageAccountVersion": "ClassicCompute"
 },
 "resourceGroup": "azurefiles",
 "tags": null,
 "type": "Microsoft.RecoveryServices/vaults/backupJobs"
}

```

Since the backup job is a long running operation, it should be tracked as explained in the [monitor jobs using REST API document](#).

## Item level recovery using REST API

You can use this restore option to restore individual files or folders in the original or an alternate location.

```

POST
https://management.azure.com/Subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.RecoveryServices/vaults/{vaultName}/backupFabrics/{fabricName}/protectionContainers/{containerName}/protectedItems/{protectedItemName}/recoveryPoints/{recoveryPointId}/restore?api-version=2019-05-13

```

The values {containerName} and {protectedItemName} are as set [here](#) and recoveryPointID is the {name} field of the recovery point mentioned above.

```

POST https://management.azure.com/Subscriptions/ef4ab5a7-c2c0-4304-af80-af49f48af3d1/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/protectionContainers/StorageContainer;storage;azurefiles;afsaccount/protectedItems/AzureFileShare%3Bazurefiles/recoveryPoints/932886657837421071/restore?api-version=2019-05-13

```

#### Create request body

To trigger a restore for an Azure file share, the following are the components of the request body:

| NAME       | TYPE                         | DESCRIPTION                       |
|------------|------------------------------|-----------------------------------|
| Properties | AzureFileShareRestoreRequest | RestoreRequestResource properties |

For the complete list of definitions of the request body and other details, refer to the [trigger Restore REST API document](#).

#### Restore to original location

The following request body is to restore the *Restoretest.txt* file in the *azurefiles* file share in the *afsaccount* storage account.

Create Request Body

```
{
 "properties": {
 "objectType": "AzureFileShareRestoreRequest",
 "copyOptions": "Overwrite",
 "recoveryType": "OriginalAllocation",
 "restoreFileSpecs": [
 {
 "fileSpecType": "File",
 "path": "RestoreTest.txt",
 "targetFolderPath": null
 }
],
 "restoreRequestType": "ItemLevelRestore",
 "sourceResourceId": "/subscriptions/ef4ab5a7-c2c0-4304-af80-af49f48af3d1/resourceGroups/azurefiles/providers/Microsoft.storage/storageAccounts/afsaccount",
 "targetDetails": null
 }
}
```

#### Restore to alternate location

The following request body is to restore the *Restoretest.txt* file in the *azurefiles* file share in the *afsaccount* storage account to the *restoredata* folder of the *azurefiles1* file share in the *afaccount1* storage account.

Create request body

```
{
 "properties": {
 "objectType": "AzureFileShareRestoreRequest",
 "recoveryType": "AlternateLocation",
 "sourceResourceId": "/subscriptions/ef4ab5a7-c2c0-4304-af80-af49f48af3d1/resourceGroups/AzureFiles/providers/Microsoft.Storage/storageAccounts/afsaccount",
 "copyOptions": "Overwrite",
 "restoreRequestType": "ItemLevelRestore",
 "restoreFileSpecs": [
 {
 "path": "Restore/RestoreTest.txt",
 "fileSpecType": "File",
 "targetFolderPath": "restoredata"
 }
],
 "targetDetails": {
 "name": "azurefiles1",
 "targetResourceId": "/subscriptions/ef4ab5a7-c2c0-4304-af80-af49f48af3d1/resourceGroups/AzureFiles/providers/Microsoft.Storage/storageAccounts/afaccount1"
 }
 }
}
```

The response should be handled in the same way as explained above for [full share restores](#).

## Next steps

- Learn how to [manage Azure file shares backup using Rest API](#).

# Manage Azure File share backup with REST API

2/18/2020 • 3 minutes to read • [Edit Online](#)

This article explains how to perform tasks for managing and monitoring the Azure file shares that are backed up by [Azure Backup](#).

## Monitor jobs

The Azure Backup service triggers jobs that run in the background. This includes scenarios such as triggering backup, restore operations, and disabling backup. These jobs can be tracked using their IDs.

### Fetch job information from operations

An operation such as triggering backup will always return a jobID in the response.

For example, the final response of a [trigger backup REST API](#) operation is as follows:

```
{
 "id": "c3a52d1d-0853-4211-8141-477c65740264",
 "name": "c3a52d1d-0853-4211-8141-477c65740264",
 "status": "Succeeded",
 "startTime": "2020-02-03T18:10:48.296012Z",
 "endTime": "2020-02-03T18:10:48.296012Z",
 "properties": {
 "objectType": "OperationStatusJobExtendedInfo",
 "jobId": "e2ca2cf4-2eb9-4d4b-b16a-8e592d2a658b"
 }
}
```

The Azure file share backup job is identified by the  **jobId** field and can be tracked as mentioned [here](#) using a GET request.

### Tracking the job

```
GET
https://management.azure.com/Subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.RecoveryServices/vaults/{vaultName}/backupJobs/{jobName}?api-version=2019-05-13
```

The {jobName} is the "jobId" mentioned above. The response is always "200 OK" with the **status** field indicating the status of the job. Once it is "Completed" or "CompletedWithWarnings", the **extendedInfo** section reveals more details about the job.

```
GET https://management.azure.com/Subscriptions/ef4ab5a7-c2c0-4304-af80-
af49f48af3d1/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupJobs/
e2ca2cf4-2eb9-4d4b-b16a-8e592d2a658b?api-version=2019-05-13'
```

### Response

| NAME   | TYPE        | DESCRIPTION |
|--------|-------------|-------------|
| 200 OK | JobResource | OK          |

### Response example

Once the *GET* URL is submitted, a 200 response is returned.

```

HTTP/1.1" 200
'Cache-Control': 'no-cache'
'Pragma': 'no-cache'
'Transfer-Encoding': 'chunked'
'Content-Type': 'application/json'
'Content-Encoding': 'gzip'
'Expires': '-1'
'Vary': 'Accept-Encoding'
'Server': 'Microsoft-IIS/10.0, Microsoft-IIS/10.0'
'X-Content-Type-Options': 'nosniff'
'x-ms-request-id': 'dba43f00-5cdb-43b1-a9ec-23e419db67c5'
'x-ms-client-request-id': 'a644712a-4895-11ea-ba57-0a580af42708, a644712a-4895-11ea-ba57-0a580af42708'
'X-Powered-By': 'ASP.NET'
'Strict-Transport-Security': 'max-age=31536000; includeSubDomains'
'x-ms-ratelimit-remaining-subscription-reads': '11999'
'x-ms-correlation-request-id': 'dba43f00-5cdb-43b1-a9ec-23e419db67c5'
'x-ms-routing-request-id': 'WESTEUROPE:20200206T040341Z:dba43f00-5cdb-43b1-a9ec-23e419db67c5'
'Date': 'Thu, 06 Feb 2020 04:03:40 GMT'
{
 "id": "/Subscriptions/ef4ab5a7-c2c0-4304-af80-
af49f48af3d1/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupJobs/
e2ca2cf4-2eb9-4d4b-b16a-8e592d2a658b",
 "name": "e2ca2cf4-2eb9-4d4b-b16a-8e592d2a658b",
 "type": "Microsoft.RecoveryServices/vaults/backupJobs",
 "properties": {
 "jobType": "AzureStorageJob",
 "duration": "00:00:43.1809140",
 "storageAccountName": "testvault2",
 "storageAccountVersion": "Storage",
 "extendedInfo": {
 "tasksList": [],
 "propertyBag": {
 "File Share Name": "testshare",
 "Storage Account Name": "testvault2",
 "Policy Name": "schedule1"
 }
 },
 "entityFriendlyName": "testshare",
 "backupManagementType": "AzureStorage",
 "operation": "ConfigureBackup",
 "status": "Completed",
 "startTime": "2020-02-03T18:10:48.296012Z",
 "endTime": "2020-02-03T18:11:31.476926Z",
 "activityId": "3677cec0-942d-4eac-921f-8f3c873140d7"
 }
}

```

## Modify policy

To change the policy with which the file share is protected, you can use the same format as enabling protection. Just provide the new policy ID in the request policy and submit the request.

For example: To change the protection policy of *testshare* from *schedule1* to *schedule2*, provide the *schedule2* ID in the request body.

```
{
 "properties": {
 "protectedItemType": "AzureFileShareProtectedItem",
 "sourceResourceId": "/subscriptions/ef4ab5a7-c2c0-4304-af80-
af49f48af3d1/resourceGroups/AzureFiles/providers/Microsoft.Storage/storageAccounts/testvault2",
 "policyId": "/Subscriptions/ef4ab5a7-c2c0-4304-af80-
af49f48af3d1/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupPolicies/schedule2"
 }
}
```

## Stop protection but retain existing data

You can remove protection on a protected file share but retain the data already backed up. To do so, remove the policy in the request body you used to enable backup and submit the request. Once the association with the policy is removed, backups are no longer triggered, and no new recovery points are created.

```
{
 "properties": {
 "protectedItemType": "AzureFileShareProtectedItem",
 "sourceResourceId": "/subscriptions/ef4ab5a7-c2c0-4304-af80-
af49f48af3d1/resourceGroups/AzureFiles/providers/Microsoft.Storage/storageAccounts/testvault2",
 "policyId": "",
 "protectionState": "ProtectionStopped"
 }
}
```

### Sample response

Stopping protection for a file share is an asynchronous operation. The operation creates another operation that needs to be tracked. It returns two responses: 202 (Accepted) when another operation is created, and 200 when that operation completes.

Response header when operation is successfully accepted:

```
HTTP/1.1" 202
'Cache-Control': 'no-cache'
'Pragma': 'no-cache'
'Expires': '-1'
'Location': 'https://management.azure.com/Subscriptions/ef4ab5a7-c2c0-4304-af80-
af49f48af3d1/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/protectionContainers/StorageContainer;storage;azurefiles;testvault2/protectedItems/AzureFileShare;testshare/operationResults/b300922a-ad9c-4181-b4cd-d42ea780ad77?api-version=2019-05-13'
'Retry-After': '60'
msrest.http_logger : 'Azure-AsyncOperation': 'https://management.azure.com/Subscriptions/ef4ab5a7-c2c0-
4304-af80-
af49f48af3d1/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/protectionContainers/StorageContainer;storage;azurefiles;testvault2/protectedItems/AzureFileShare;testshare/operationsStatus/b300922a-ad9c-4181-b4cd-d42ea780ad77?api-version=2019-05-13'
'X-Content-Type-Options': 'nosniff'
'x-ms-request-id': '3895e8a1-e4b9-4da5-bec7-2cf0266405f8'
'x-ms-client-request-id': 'd331c15e-48ab-11ea-84c0-0a580af46a50, d331c15e-48ab-11ea-84c0-0a580af46a50'
'Strict-Transport-Security': 'max-age=31536000; includeSubDomains'
'X-Powered-By': 'ASP.NET'
'x-ms-ratelimit-remaining-subscription-writes': '1199'
'x-ms-correlation-request-id': '3895e8a1-e4b9-4da5-bec7-2cf0266405f8'
'x-ms-routing-request-id': 'WESTEUROPE:20200206T064224Z:3895e8a1-e4b9-4da5-bec7-2cf0266405f8'
'Date': 'Thu, 06 Feb 2020 06:42:24 GMT'
'Content-Length': '0'
```

Then track the resulting operation using the location header or Azure-AsyncOperation header with a GET

command:

```
GET https://management.azure.com/Subscriptions/ef4ab5a7-c2c0-4304-af80-af49f48af3d1/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupoperations/b300922a-ad9c-4181-b4cd-d42ea780ad77?api-version=2016-12-01
```

## Response body

```
{
 "id": "b300922a-ad9c-4181-b4cd-d42ea780ad77",
 "name": "b300922a-ad9c-4181-b4cd-d42ea780ad77",
 "status": "Succeeded",
 "startTime": "2020-02-06T06:42:24.4001299Z",
 "endTime": "2020-02-06T06:42:24.4001299Z",
 "properties": {
 "objectType": "OperationStatusJobExtendedInfo",
 "jobId": "7816fca8-d5be-4c41-b911-1bbd922e5826"
 }
}
```

## Stop protection and delete data

To remove the protection on a protected file share and delete the backup data as well, perform a delete operation as detailed [here](#).

```
DELETE
https://management.azure.com/Subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.RecoveryServices/vaults/{vaultName}/backupFabrics/{fabricName}/protectionContainers/{containerName}/protectedItems/{protectedItemName}?api-version=2019-05-13
```

The parameters {containerName} and {protectedItemName} are as set [here](#).

The following example triggers an operation to stop protection for the *testshare* file share protected with *azurefilesvault*.

```
DELETE https://management.azure.com/Subscriptions/ef4ab5a7-c2c0-4304-af80-af49f48af3d1/resourceGroups/azurefiles/providers/Microsoft.RecoveryServices/vaults/azurefilesvault/backupFabrics/Azure/protectionContainers/StorageContainer;Storage;AzureFiles;testvault2/protectedItems/azurefileshare;testshare?api-version=2016-12-01
```

## Responses

Delete protection is an asynchronous operation. The operation creates another operation that needs to be tracked separately. It returns two responses: 202 (Accepted) when another operation is created and 204 (NoContent) when that operation completes.

## Next steps

- Learn how to [troubleshoot problems while configuring backup for Azure File shares](#).

# About SAP HANA database backup in Azure VMs

2/28/2020 • 2 minutes to read • [Edit Online](#)

SAP HANA databases are mission critical workloads that require a low recovery point objective (RPO) and a fast recovery time objective (RTO). You can now [back up SAP HANA databases running on Azure VMs](#) using [Azure Backup](#).

Azure Backup is [Backint certified](#) by SAP, to provide native backup support by leveraging SAP HANA's native APIs. This offering from Azure Backup aligns with Azure Backup's mantra of **zero-infrastructure** backups, eliminating the need to deploy and manage backup infrastructure. You can now seamlessly back up and restore SAP HANA databases running on Azure VMs ([M series VMs](#) also supported now!) and leverage enterprise management capabilities that Azure Backup provides.

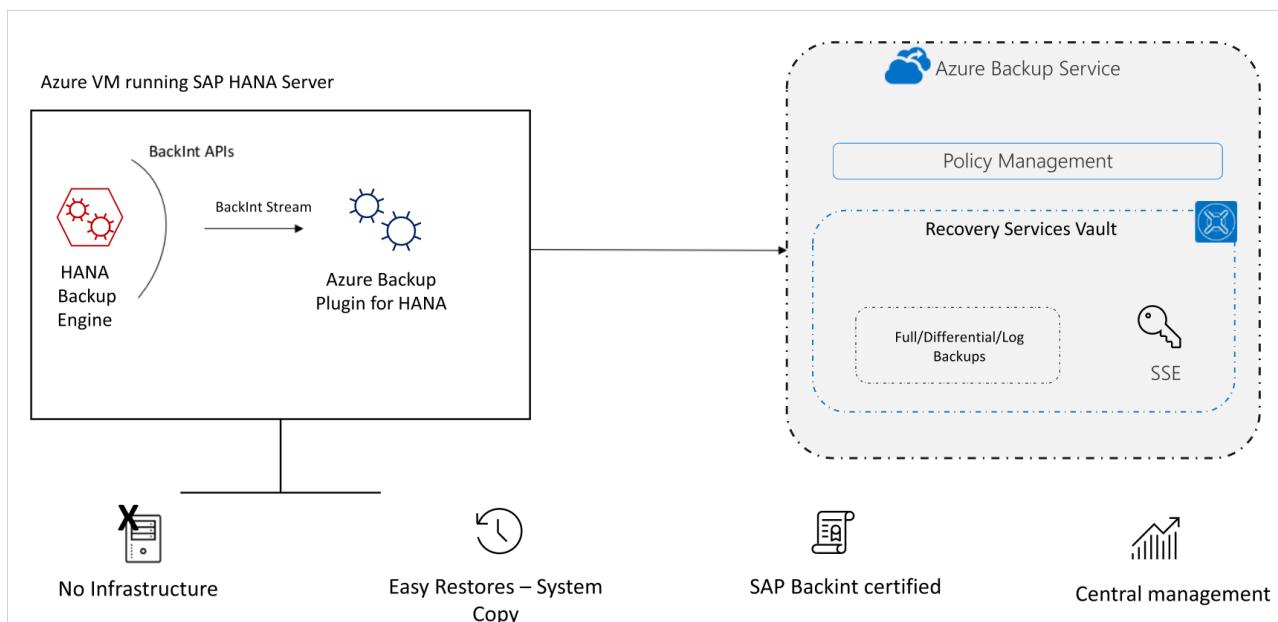
## Added value

Using Azure Backup to back up and restore SAP HANA databases, gives the following advantages:

- **15-minute Recovery Point Objective (RPO):** Recovery of critical data of up to 15 minutes is now possible.
- **One-click, point-in-time restores:** Restore of production data to alternate HANA servers is made easy. Chaining of backups and catalogs to perform restores is all managed by Azure behind the scenes.
- **Long-term retention:** For rigorous compliance and audit needs. Retain your backups for years, based on the retention duration, beyond which the recovery points will be pruned automatically by the built-in lifecycle management capability.
- **Backup Management from Azure:** Use Azure Backup's management and monitoring capabilities for improved management experience. Azure CLI is also supported.

To view the backup and restore scenarios that we support today, refer to the [SAP HANA scenario support matrix](#).

## Backup architecture



- The backup process begins by [creating a Recovery services vault](#) in Azure. This vault will be used to store the backups and recovery points created over time.
- The Azure VM running SAP HANA server is registered with the vault, and the databases to be backed-up

are discovered. To enable the Azure Backup service to discover databases, a [preregistration script](#) must be run on the HANA server as a root user.

- This script creates **AZUREWLBACKUPHANAUSER** DB user and a corresponding key with the same name in **hdbuserstore**. Refer to the [setting up permissions section](#) to understand more about what the script does.
- Azure Backup Service now installs the **Azure Backup Plugin for HANA** on the registered SAP HANA server.
- The **AZUREWLBACKUPHANAUSER** DB user created by the preregistration script is used by the **Azure Backup Plugin for HANA** to perform all backup and restore operations. If you attempt to configure backup for SAP HANA DBs without running this script, you might receive the following error: **UserErrorHanaScriptNotRun**.
- To [configure backup](#) on the databases that are discovered, choose the required backup policy and enable backups.
- Once the backup is configured, Azure Backup service sets up the following Backint parameters at the DATABASE level on the protected SAP HANA server:
  - [catalog\_backup\_using\_backint:true]
  - [enable\_accumulated\_catalog\_backup:false]
  - [parallel\_data\_backup\_backint\_channels:1]
  - [log\_backup\_timeout\_s:900])
  - [backint\_response\_timeout:7200]

#### NOTE

Ensure that these parameters are *not* present at HOST level. Host-level parameters will override these parameters and might cause unexpected behavior.

- The **Azure Backup Plugin for HANA** maintains all the backup schedules and policy details. It triggers the scheduled backups and communicates with the **HANA Backup Engine** through the Backint APIs.
- The **HANA Backup Engine** returns a Backint stream with the data to be backed up.
- All the scheduled backups and on-demand backups (triggered from the Azure portal) that are either full or differential are initiated by the **Azure Backup Plugin for HANA**. However, log backups are managed and triggered by **HANA Backup Engine** itself.

## Next steps

- Learn how to [restore an SAP HANA database running on an Azure VM](#)
- Learn how to [manage SAP HANA databases that are backed up using Azure Backup](#)

# Back up SAP HANA databases in Azure VMs

2/27/2020 • 11 minutes to read • [Edit Online](#)

SAP HANA databases are critical workloads that require a low recovery-point objective (RPO) and long-term retention. You can back up SAP HANA databases running on Azure virtual machines (VMs) by using [Azure Backup](#).

This article shows how to back up SAP HANA databases that are running on Azure VMs to an Azure Backup Recovery Services vault.

In this article, you will learn how to:

- Create and configure a vault
- Discover databases
- Configure backups
- Run an on-demand backup job

## NOTE

**Soft delete for SQL server in Azure VM and soft delete for SAP HANA in Azure VM workloads** is now available in preview.

To sign up for the preview, write to us at [AskAzureBackupTeam@microsoft.com](mailto:AskAzureBackupTeam@microsoft.com)

## Prerequisites

Refer to the [prerequisites](#) and the [What the pre-registration script does](#) sections to set up the database for backup.

### Set up network connectivity

For all operations, the SAP HANA VM requires connectivity to Azure public IP addresses. VM operations (database discovery, configure backups, schedule backups, restore recovery points, and so on) fail without connectivity to Azure public IP addresses.

Establish connectivity by using one of the following options:

#### Allow the Azure datacenter IP ranges

This option allows the [IP ranges](#) in the downloaded file. To access a network security group (NSG), use the `Set-AzureNetworkSecurityRule` cmdlet. If your safe recipients list only includes region-specific IPs, you'll also need to update the safe recipients list the Azure Active Directory (Azure AD) service tag to enable authentication.

#### Allow access using NSG tags

If you use NSG to restrict connectivity, then you should use AzureBackup service tag to allow outbound access to Azure Backup. In addition, you should also allow connectivity for authentication and data transfer by using [rules](#) for Azure AD and Azure Storage. This can be done from the Azure portal or via PowerShell.

To create a rule using the portal:

1. In **All Services**, go to **Network security groups** and select the network security group.
2. Select **Outbound security rules** under **Settings**.
3. Select **Add**. Enter all the required details for creating a new rule as described in [security rule settings](#). Ensure the option **Destination** is set to **Service Tag** and **Destination service tag** is set to **AzureBackup**.
4. Click **Add**, to save the newly created outbound security rule.

To create a rule using PowerShell:

1. Add Azure account credentials and update the national clouds

```
Add-AzureRmAccount
```

2. Select the NSG subscription

```
Select-AzureRmSubscription "<Subscription Id>"
```

3. Select the NSG

```
$nsg = Get-AzureRmNetworkSecurityGroup -Name "<NSG name>" -ResourceGroupName "<NSG resource group name>"
```

4. Add allow outbound rule for Azure Backup service tag

```
Add-AzureRmNetworkSecurityRuleConfig -NetworkSecurityGroup $nsg -Name "AzureBackupAllowOutbound" -Access Allow -Protocol * -Direction Outbound -Priority <priority> -SourceAddressPrefix * -SourcePortRange * -DestinationAddressPrefix "AzureBackup" -DestinationPortRange 443 -Description "Allow outbound traffic to Azure Backup service"
```

5. Add allow outbound rule for Storage service tag

```
Add-AzureRmNetworkSecurityRuleConfig -NetworkSecurityGroup $nsg -Name "StorageAllowOutbound" -Access Allow -Protocol * -Direction Outbound -Priority <priority> -SourceAddressPrefix * -SourcePortRange * -DestinationAddressPrefix "Storage" -DestinationPortRange 443 -Description "Allow outbound traffic to Azure Backup service"
```

6. Add allow outbound rule for AzureActiveDirectory service tag

```
Add-AzureRmNetworkSecurityRuleConfig -NetworkSecurityGroup $nsg -Name "AzureActiveDirectoryAllowOutbound" -Access Allow -Protocol * -Direction Outbound -Priority <priority> -SourceAddressPrefix * -SourcePortRange * -DestinationAddressPrefix "AzureActiveDirectory" -DestinationPortRange 443 -Description "Allow outbound traffic to AzureActiveDirectory service"
```

7. Save the NSG

```
Set-AzureRmNetworkSecurityGroup -NetworkSecurityGroup $nsg
```

**Allow access by using Azure Firewall tags.** If you're using Azure Firewall, create an application rule by using the AzureBackup [FQDN tag](#). This allows outbound access to Azure Backup.

**Deploy an HTTP proxy server to route traffic.** When you back up an SAP HANA database on an Azure VM, the backup extension on the VM uses the HTTPS APIs to send management commands to Azure Backup and data to Azure Storage. The backup extension also uses Azure AD for authentication. Route the backup extension traffic for these three services through the HTTP proxy. The extensions are the only component that's configured for access to the public internet.

Connectivity options include the following advantages and disadvantages:

| OPTION                       | ADVANTAGES                                                                            | DISADVANTAGES                                                                                                                         |
|------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Allow IP ranges              | No additional costs                                                                   | Complex to manage because the IP address ranges change over time<br><br>Provides access to the whole of Azure, not just Azure Storage |
| Use NSG service tags         | Easier to manage as range changes are automatically merged<br><br>No additional costs | Can be used with NSGs only<br><br>Provides access to the entire service                                                               |
| Use Azure Firewall FQDN tags | Easier to manage as the required FQDNs are automatically managed                      | Can be used with Azure Firewall only                                                                                                  |

| OPTION            | ADVANTAGES                                                                                                                                                  | DISADVANTAGES                                        |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| Use an HTTP proxy | Granular control in the proxy over the storage URLs is allowed<br><br>Single point of internet access to VMs<br><br>Not subject to Azure IP address changes | Additional costs to run a VM with the proxy software |

## Onboard to the public preview

Onboard to the public preview as follows:

- In the portal, register your subscription ID to the Recovery Services service provider by [following this article](#).
- For 'Az' module in PowerShell, run this cmdlet . It should complete as "Registered".

```
Register-AzProviderFeature -FeatureName "HanaBackup" -ProviderNamespace Microsoft.RecoveryServices
```

- If you are using 'AzureRM' module in PowerShell, run this cmdlet. It should complete as "Registered".

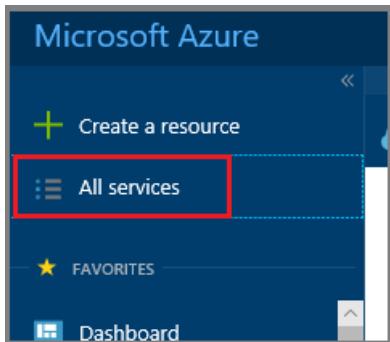
```
Register-AzureRmProviderFeature -FeatureName "HanaBackup" -ProviderNamespace Microsoft.RecoveryServices
```

## Create a Recovery Services vault

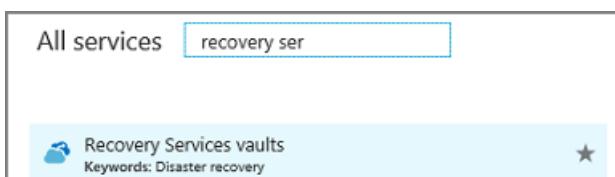
A Recovery Services vault is an entity that stores backups and recovery points created over time. The Recovery Services vault also contains the backup policies that are associated with the protected virtual machines.

To create a Recovery Services vault, follow these steps.

1. Sign in to your subscription in the [Azure portal](#).
2. On the left menu, select **All services**.

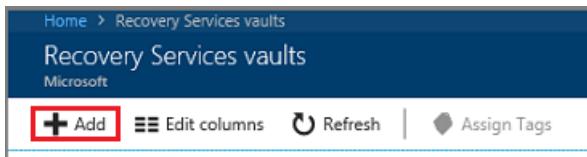


3. In the **All services** dialog box, enter *Recovery Services*. The list of resources filters according to your input. In the list of resources, select **Recovery Services vaults**.

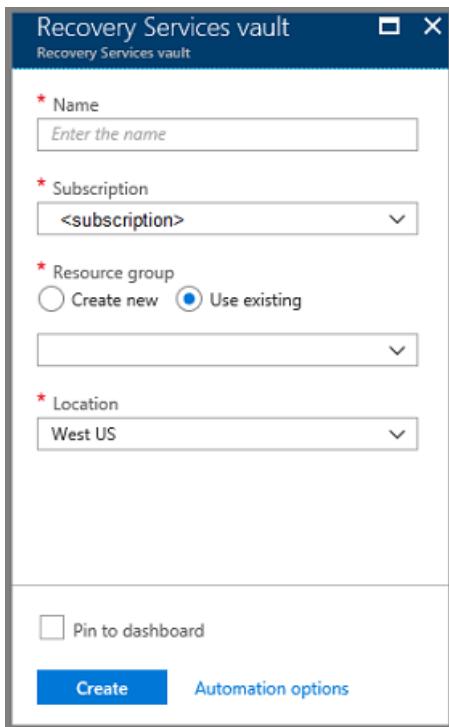


The list of Recovery Services vaults in the subscription appears.

4. On the **Recovery Services vaults** dashboard, select **Add**.



The **Recovery Services vault** dialog box opens. Provide values for the **Name**, **Subscription**, **Resource group**, and **Location**.

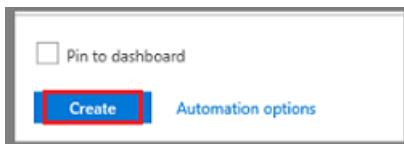


- **Name:** Enter a friendly name to identify the vault. The name must be unique to the Azure subscription. Specify a name that has at least 2 but not more than 50 characters. The name must start with a letter and consist only of letters, numbers, and hyphens.
- **Subscription:** Choose the subscription to use. If you're a member of only one subscription, you'll see that name. If you're not sure which subscription to use, use the default (suggested) subscription. There are multiple choices only if your work or school account is associated with more than one Azure subscription.
- **Resource group:** Use an existing resource group or create a new one. To see the list of available resource groups in your subscription, select **Use existing**, and then select a resource from the drop-down list. To create a new resource group, select **Create new** and enter the name. For more information about resource groups, see [Azure Resource Manager overview](#).
- **Location:** Select the geographic region for the vault. To create a vault to protect virtual machines, the vault *must* be in the same region as the virtual machines.

#### IMPORTANT

If you're not sure of the location of your VM, close the dialog box. Go to the list of virtual machines in the portal. If you have virtual machines in several regions, create a Recovery Services vault in each region. Create the vault in the first location, before you create the vault for another location. There's no need to specify storage accounts to store the backup data. The Recovery Services vault and Azure Backup handle that automatically.

5. When you're ready to create the Recovery Services vault, select **Create**.



It can take a while to create the Recovery Services vault. Monitor the status notifications in the **Notifications** area at the upper-right corner of the portal. After your vault is created, it's visible in the list of Recovery Services vaults. If you don't see your vault, select **Refresh**.

## Discover the databases

1. In the vault, in **Getting Started**, click **Backup**. In **Where is your workload running?**, select **SAP HANA in Azure VM**.
2. Click **Start Discovery**. This initiates discovery of unprotected Linux VMs in the vault region.
  - After discovery, unprotected VMs appear in the portal, listed by name and resource group.
  - If a VM isn't listed as expected, check whether it's already backed up in a vault.
  - Multiple VMs can have the same name but they belong to different resource groups.
3. In **Select Virtual Machines**, click the link to download the script that provides permissions for the Azure Backup service to access the SAP HANA VMs for database discovery.
4. Run the script on each VM hosting SAP HANA databases that you want to back up.
5. After running the script on the VMs, in **Select Virtual Machines**, select the VMs. Then click **Discover DBs**.
6. Azure Backup discovers all SAP HANA databases on the VM. During discovery, Azure Backup registers the VM with the vault, and installs an extension on the VM. No agent is installed on the database.

The screenshot shows the Azure portal interface for managing a Recovery Services vault named 'ReadyDemoVault'. On the left, the main vault settings page is displayed, with the 'Backup' section highlighted. In the center, a modal dialog titled 'Select Virtual Machines' is open, showing a list of VMs and a dropdown menu set to 'SAP HANA in Azure VM'. At the bottom of the dialog, there is a note: 'Azure backup requires permissions to able to discover SAP HANA DBs and perform backup and restore operations. Run this script on the SAP HANA VMs to provide these permissions to Azure Backup service. Learn More'.

## Configure backup

Now enable backup.

1. In Step 2, click **Configure Backup**.

Home > ignitedemovault > Backup Goal

## Backup Goal

Where is your workload running?

Azure

What do you want to backup?

SAP HANA in Azure VM (Preview)

**Step 1: Discover DBs in VMs**

**Start Discovery**

**View details**

**Step 2: Configure Backup**

**Configure Backup**

2. In **Select items to back up**, select all the databases you want to protect > **OK**.

| Backup                                               |                     | Select items to backup                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |  |             |      |                  |                                                      |                     |                                                                                             |                                           |          |  |                                          |          |  |                                      |          |  |                                           |                     |                                                                                             |
|------------------------------------------------------|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|-------------|------|------------------|------------------------------------------------------|---------------------|---------------------------------------------------------------------------------------------|-------------------------------------------|----------|--|------------------------------------------|----------|--|--------------------------------------|----------|--|-------------------------------------------|---------------------|---------------------------------------------------------------------------------------------|
| <b>1</b> Items to backup ><br>Select                 |                     | <a href="#">Refresh</a> <a href="#">Rediscover DBs</a><br> To discover more SAP HANA servers go back to Start Discovery<br><input type="text"/> Filter items...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |  |  |             |      |                  |                                                      |                     |                                                                                             |                                           |          |  |                                          |          |  |                                      |          |  |                                           |                     |                                                                                             |
| <b>2</b> Backup policy ><br>Select                   |                     | <table border="1"> <thead> <tr> <th>HANA System</th> <th>TYPE</th> <th>BACKUP READINESS</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> HANADemoIDC3\H22</td> <td>Standalone Instance</td> <td> Ready</td> </tr> <tr> <td><input type="checkbox"/> H22 IGNITE_BOOTH</td> <td>Database</td> <td></td> </tr> <tr> <td><input type="checkbox"/> H22_IGNITEBOOTH</td> <td>Database</td> <td></td> </tr> <tr> <td><input type="checkbox"/> H22_RESTORE</td> <td>Database</td> <td></td> </tr> <tr> <td><input type="checkbox"/> HANADemoIDC4\H21</td> <td>Standalone Instance</td> <td> Ready</td> </tr> </tbody> </table> <p>Selected items<br/>0 database(s)</p> |  |  | HANA System | TYPE | BACKUP READINESS | <input checked="" type="checkbox"/> HANADemoIDC3\H22 | Standalone Instance |  Ready | <input type="checkbox"/> H22 IGNITE_BOOTH | Database |  | <input type="checkbox"/> H22_IGNITEBOOTH | Database |  | <input type="checkbox"/> H22_RESTORE | Database |  | <input type="checkbox"/> HANADemoIDC4\H21 | Standalone Instance |  Ready |
| HANA System                                          | TYPE                | BACKUP READINESS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |  |  |             |      |                  |                                                      |                     |                                                                                             |                                           |          |  |                                          |          |  |                                      |          |  |                                           |                     |                                                                                             |
| <input checked="" type="checkbox"/> HANADemoIDC3\H22 | Standalone Instance |  Ready                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |  |  |             |      |                  |                                                      |                     |                                                                                             |                                           |          |  |                                          |          |  |                                      |          |  |                                           |                     |                                                                                             |
| <input type="checkbox"/> H22 IGNITE_BOOTH            | Database            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |  |  |             |      |                  |                                                      |                     |                                                                                             |                                           |          |  |                                          |          |  |                                      |          |  |                                           |                     |                                                                                             |
| <input type="checkbox"/> H22_IGNITEBOOTH             | Database            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |  |  |             |      |                  |                                                      |                     |                                                                                             |                                           |          |  |                                          |          |  |                                      |          |  |                                           |                     |                                                                                             |
| <input type="checkbox"/> H22_RESTORE                 | Database            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |  |  |             |      |                  |                                                      |                     |                                                                                             |                                           |          |  |                                          |          |  |                                      |          |  |                                           |                     |                                                                                             |
| <input type="checkbox"/> HANADemoIDC4\H21            | Standalone Instance |  Ready                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |  |  |             |      |                  |                                                      |                     |                                                                                             |                                           |          |  |                                          |          |  |                                      |          |  |                                           |                     |                                                                                             |
| <input type="button" value="Enable backup"/>         |                     | <input type="button" value="OK"/>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |  |  |             |      |                  |                                                      |                     |                                                                                             |                                           |          |  |                                          |          |  |                                      |          |  |                                           |                     |                                                                                             |

3. In **Backup Policy > Choose backup policy**, create a new backup policy for the databases, in accordance with the instructions below.

**Backup**

**Backup policy**

1 Items to backup ✓  
1 database(s)

2 Backup policy >  
Select

Choose backup policy ⓘ  
DailyFullLog2

**FULL BACKUP**

**Backup Frequency**  
Daily at 2:30 AM UTC

**Retention of daily backup point**  
Retain backup taken every day at 2:30 AM for 180 Day(s)

**Retention of weekly backup point**  
Retain backup taken every week on Sunday at 2:30 AM for 104 Week(s)

**Retention of monthly backup point**  
Retain backup taken every month on First Sunday at 2:30 AM for 60 Month(s)

**Retention of yearly backup point**  
Retain backup taken every year in January on First Sunday at 2:30 AM for 10 Year(s)

**LOG BACKUP**

Enable backup

OK

4. After creating the policy, on the **Backup** menu, click **Enable backup**.

**Backup**

1 Items to backup ✓  
1 database(s)

2 Backup policy ✓  
DailyFullLog2

Enable backup

5. Track the backup configuration progress in the **Notifications** area of the portal.

### Create a backup policy

A backup policy defines when backups are taken, and how long they're retained.

- A policy is created at the vault level.
- Multiple vaults can use the same backup policy, but you must apply the backup policy to each vault.

Specify the policy settings as follows:

1. In **Policy name**, enter a name for the new policy.

|                                                                                                                                   |                                                                                                                                                                                   |               |
|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Add                                                                                                                               | X                                                                                                                                                                                 | Backup policy |
| <p>Policy Type</p> <p>Azure Virtual Machine</p> <p>SAP HANA in Azure VM</p> <p>SQL Server in Azure VM</p> <p>Azure File Share</p> | <p>Policy name * ⓘ</p> <hr/> <p>Full Backup ⓘ &gt;</p> <p>Daily</p> <hr/> <p>*Differential Backup ⓘ &gt;</p> <p>Disabled</p> <hr/> <p>*Log Backup ⓘ &gt;</p> <p>Every 2 hours</p> | <p>Create</p> |

2. In **Full Backup policy**, select a **Backup Frequency**, choose **Daily** or **Weekly**.

- **Daily:** Select the hour and time zone in which the backup job begins.
    - You must run a full backup. You can't turn off this option.
    - Click **Full Backup** to view the policy.
    - You can't create differential backups for daily full backups.
  - **Weekly:** Select the day of the week, hour, and time zone in which the backup job runs.

## Full Backup Policy

Backup Frequency

Daily  11:30 AM  (UTC) Coordinated Univer...

**RETENTION RANGE**

Retention of daily backup point.

At \*  Retained for  
11:30 AM  180 Day(s)

Retention of weekly backup point.

On \*  At \*  Retained for  
Sunday  11:30 AM  104 Week(s)

Retention of monthly backup point.

Week Based  Day Based

On \*  Day \*  At \*  Retained for  
First  Sunday  11:30 AM  60 Month(s)

Retention of yearly backup point.

Week Based  Day Based

In \*  On \*  Day \*  At \*  Retained for  
January  First  Sunday  11:30 AM  10 Year(s)

**OK**

3. In **Retention Range**, configure retention settings for the full backup.

- By default all options are selected. Clear any retention range limits you don't want to use, and set those that you do.
- The minimum retention period for any type of backup (full/differential/log) is seven days.
- Recovery points are tagged for retention based on their retention range. For example, if you select a daily full backup, only one full backup is triggered each day.
- The backup for a specific day is tagged and retained based on the weekly retention range and setting.
- The monthly and yearly retention ranges behave in a similar way.

4. In the **Full Backup policy** menu, click **OK** to accept the settings.

5. Select **Differential Backup** to add a differential policy.

6. In **Differential Backup policy**, select **Enable** to open the frequency and retention controls.

- At most, you can trigger one differential backup per day.
- Differential backups can be retained for a maximum of 180 days. If you need longer retention, you must

use full backups.

**Differential Backup Policy**

**Differential Backup** ⓘ

**Enable** **Disable**

**Backup Frequency**

Sunday **▼** 2:00 AM **▼** (UTC) Coordinated  
Universal Time

**Retained for**

30 **Day(s)**

**NOTE**

Incremental backups aren't currently supported.

7. Click **OK** to save the policy and return to the main **Backup policy** menu.

8. Select **Log Backup** to add a transactional log backup policy,

- In **Log Backup**, select **Enable**. This cannot be disabled as SAP HANA manages all log backups.
- Set the frequency and retention controls.

**NOTE**

Log backups only begin to flow after a successful full backup is completed.

9. Click **OK** to save the policy and return to the main **Backup policy** menu.

10. After you finish defining the backup policy, click **OK**.

**NOTE**

Each log backup is chained to the previous full backup to form a recovery chain. This full backup will be retained until the retention of the last log backup has expired. This might mean that the full backup is retained for an extra period to make sure all the logs can be recovered. Let's assume user has a weekly full backup, daily differential and 2 hour logs. All of them are retained for 30 days. But, the weekly full can be really cleaned up/deleted only after the next full backup is available i.e., after 30 + 7 days. Say, a weekly full backup happens on Nov 16th. As per the retention policy, it should be retained until Dec 16th. The last log backup for this full happens before the next scheduled full, on Nov 22nd. Until this log is available until Dec 22nd, the Nov 16th full can't be deleted. So, the Nov 16th full is retained until Dec 22nd.

## Run an on-demand backup

Backups run in accordance with the policy schedule. You can run a backup on-demand as follows:

1. In the vault menu, click **Backup items**.
2. In **Backup Items**, select the VM running the SAP HANA database, and then click **Backup now**.
3. In **Backup Now**, use the calendar control to select the last day that the recovery point should be retained. Then click **OK**.
4. Monitor the portal notifications. You can monitor the job progress in the vault dashboard > **Backup Jobs** > **In**

**progress.** Depending on the size of your database, creating the initial backup may take a while.

## Run SAP HANA Studio backup on a database with Azure Backup enabled

If you want to take a local backup (using HANA Studio) of a database that's being backed up with Azure Backup, do the following:

1. Wait for any full or log backups for the database to finish. Check the status in SAP HANA Studio / Cockpit.
2. Disable log backups, and set the backup catalog to the file system for relevant database.
3. To do this, double-click **systemdb** > **Configuration** > **Select Database** > **Filter (Log)**.
4. Set **enable\_auto\_log\_backup** to **No**.
5. Set **log\_backup\_using\_backint** to **False**.
6. Take an on-demand full backup of the database.
7. Wait for the full backup and catalog backup to finish.
8. Revert the previous settings back to those for Azure:
  - Set **enable\_auto\_log\_backup** to **Yes**.
  - Set **log\_backup\_using\_backint** to **True**.

## Next steps

- Learn how to [restore SAP HANA databases running on Azure VMs](#)
- Learn how to [manage SAP HANA databases that are backed up using Azure Backup](#)

# Restore SAP HANA databases on Azure VMs

11/21/2019 • 3 minutes to read • [Edit Online](#)

This article describes how to restore SAP HANA databases that are running on Azure Virtual Machine (VM), that the Azure Backup service has backed up to an Azure Backup Recovery Services vault. Restores can be used to create copies of the data for dev / test scenarios or to return to a previous state.

For more information, on how to back up SAP HANA databases, see [Back up SAP HANA databases on Azure VMs](#).

## Restore to a point in time or to a recovery point

Azure Backup can restore SAP HANA databases that are running on Azure VMs as follows:

- Restore to a specific date or time (to the second) by using log backups. Azure Backup automatically determines the appropriate full, differential backups and the chain of log backups that are required to restore based on the selected time.
- Restore to a specific full or differential backup to restore to a specific recovery point.

## Prerequisites

Before restoring a database, note the following:

- You can restore the database only to an SAP HANA instance that is in the same region
- The target instance must be registered with the same vault as the source
- Azure Backup cannot identify two different SAP HANA instances on the same VM. Therefore, restoring data from one instance to another on the same VM is not possible
- To ensure that the target SAP HANA instance is ready for restore, check its **Backup readiness** status:
  - Open the vault in which the target SAP HANA instance is registered
  - On the vault dashboard, under **Getting started**, choose **Backup**

The screenshot shows the Microsoft Azure (Preview) portal interface. The top navigation bar displays the URL <https://ms.portal.azure.com/#@microsoft.onmicrosoft.com/resource/subscriptions/e3d2d341-4ddb-4c5d-9121-69b7e719485e/re>. The main content area is titled "ignitedemovault" and shows the "Recovery Services vault". On the left, a sidebar menu includes "Overview", "Activity log", "Access control (IAM)", "Tags", "Diagnose and solve problems", "Settings" (with "Properties", "Locks", and "Export template"), and "Getting started" (with "Backup" and "Site Recovery"). The "Backup" option is highlighted with a red box. The main content area has a header "Essentials" with tabs for "Overview", "Backup", and "Site Recovery". The "Backup" tab is selected. Below it, a "What's new" section lists several Azure Backup features with links: "Azure Backup support for large disks is Generally Available →", "Configure network properties (internal load balancer, public IP and NSG) in the target region...", "Enterprise-scale Backup for SQL Server running in Azure VM is Generally Available →", "Protect on-premises VMs by directly replicating to managed disks in Azure →", "Protection of Azure VMs using Storage Spaces Direct is now available →", and "Disaster recovery for VMs deployed in Availability Zones to another region →". Two blue cloud icons with arrows are displayed at the bottom.

- In **Backup**, under **What do you want to backup?** choose **SAP HANA in Azure VM**

The screenshot shows the "ignitedemovault - Backup" page. The left sidebar menu is identical to the previous screenshot, with "Backup" highlighted. The main content area has a header "Where is your workload running?" with a dropdown set to "Azure". Below it, a box contains the question "What do you want to backup?" with the option "SAP HANA in Azure VM (Preview)" selected, also highlighted with a red box. The page then splits into two sections: "Step 1: Discover DBs in VMs" with a "Start Discovery" button, and "Step 2: Configure Backup" with a "Configure Backup" button.

- Under **Discover DBs in VMs** click on **View details**

ignitedemovault - Backup

Recovery Services vault

Search (Ctrl+ /)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Properties

Locks

Export template

Getting started

Backup

Where is your workload running?

Azure

What do you want to backup?

SAP HANA in Azure VM (Preview)

Step 1: Discover DBs in VMs

Start Discovery

View details

Step 2: Configure Backup

Configure Backup

- Review the **Backup Readiness** of the target VM

Protected Servers

ignitedemovault

Refresh Filter

Fetching data from service completed.

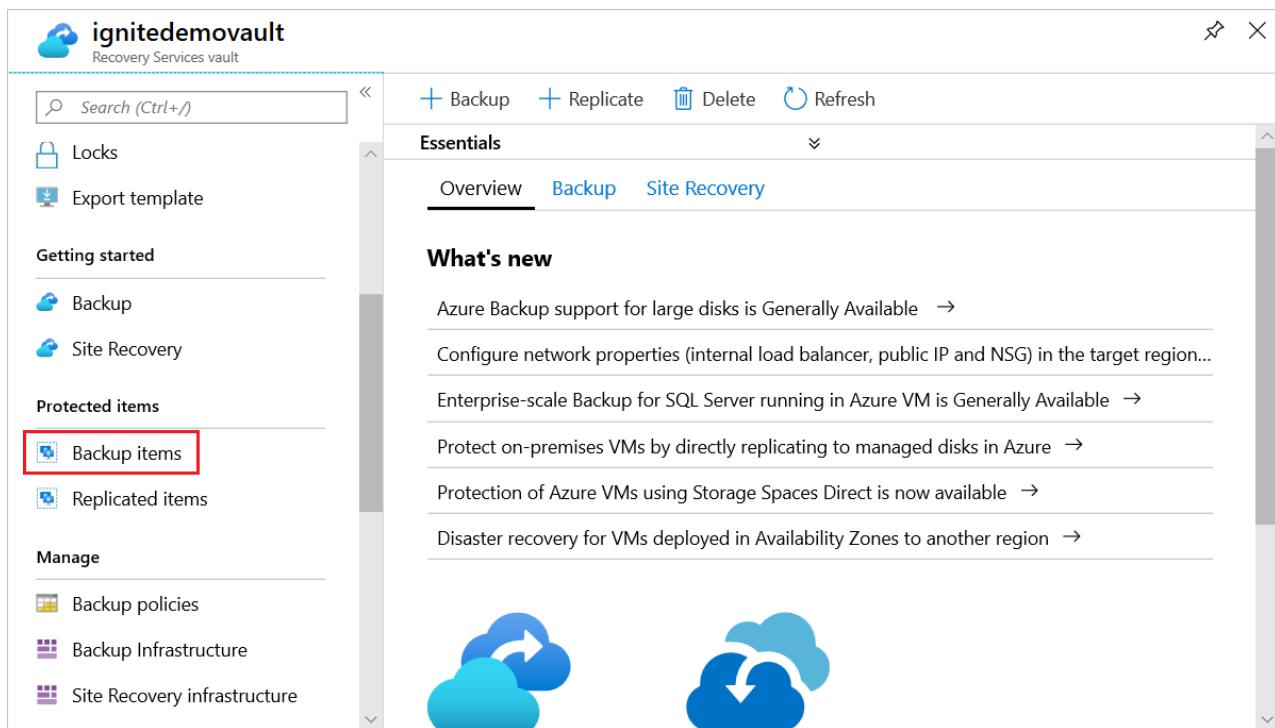
| VM Name      | VM RG   | Server       | Backup Readiness | Details       |
|--------------|---------|--------------|------------------|---------------|
| HANADemoIDC3 | IDCDemo | HANADemoIDC3 | Ready            | 5 DB(s) Found |
| HANADemoIDC4 | IDCDemo | HANADemoIDC4 | Ready            | 2 DB(s) Found |

- To learn more about the restore types that SAP HANA supports, refer to the SAP HANA Note [1642148](#)

## Restore a database

- Open the vault in which the SAP HANA database to be restored is registered
- On the vault dashboard, under **Protected Items**, choose **Backup Items**

Screenshot of the Azure portal showing the 'ignitedemovault' Recovery Services vault. The 'Backup items' section is selected and highlighted with a red box. The 'Essentials' blade shows the 'Backup' tab selected. A 'What's new' section lists several updates related to Azure Backup.



**What's new**

- Azure Backup support for large disks is Generally Available →
- Configure network properties (internal load balancer, public IP and NSG) in the target region...
- Enterprise-scale Backup for SQL Server running in Azure VM is Generally Available →
- Protect on-premises VMs by directly replicating to managed disks in Azure →
- Protection of Azure VMs using Storage Spaces Direct is now available →
- Disaster recovery for VMs deployed in Availability Zones to another region →

- In **Backup Items**, under **Backup Management Type** select **SAP HANA in Azure VM**

Screenshot of the 'ignitedemovault - Backup items' page. The 'Backup items' section is selected and highlighted with a red box. The 'Backup Management Type' table shows the count of backup items for different management types. The 'SAP HANA in Azure VM' row is highlighted with a red box.

| BACKUP MANAGEMENT TYPE      | BACKUP ITEM COUNT |
|-----------------------------|-------------------|
| SAP HANA in Azure VM        | 4                 |
| SQL in Azure VM             | 0                 |
| Azure Storage (Azure Files) | 0                 |
| DPM                         | 0                 |
| Azure Backup Server         | 0                 |
| Azure Backup Agent          | 0                 |
| Azure Virtual Machine       | 0                 |

- Select the database to be restored

**Backup Items (SAP HANA in Azure VM)**

ignitedemovault

Refresh Add Filter

**i** Fetching data from service completed.

Filter items ...

| Database | HANA System      | Type        | Backup Status | ... |
|----------|------------------|-------------|---------------|-----|
| h22      | HANADemoIDC3\H22 | HANA System | Healthy       | ... |
| systemdb | HANADemoIDC3\H22 | HANA System | Healthy       | ... |
| systemdb | HANADemoIDC4\H21 | HANA System | Healthy       | ... |
| h21      | HANADemoIDC4\H21 | HANA System | Healthy       | ... |

- Review the database menu. It provides information about database backup, including:
  - The oldest and latest restore points
  - The log backup status for the last 24 and 72 hours for the database

Home > ignitedemovault - Backup items > Backup Items (SAP HANA in Azure VM) > h22

## h22

Backup now Restore DB Stop backup Delete backup data Resume backup

Essentials

|                                                          |                                                               |
|----------------------------------------------------------|---------------------------------------------------------------|
| Recovery services vault<br><b>ignitedemovault</b>        | Backup Status<br><b>Healthy</b>                               |
| Subscription name<br><b>Backup_Canary_PM_Prod_Demo-1</b> | Latest restore point<br>11/6/2019, 9:06:39 AM (1 hour(s) ago) |
| Subscription ID<br>e3d2d341-4ddb-4c5d-9121-69b7e719485e  | Oldest restore point<br>10/29/2019, 1:09:02 PM (7 day(s) ago) |
| Host name<br>HANADemoIDC3                                | Backup policy<br><b>DailyFullLog2</b>                         |
| Item type<br>SAP HANA in Azure VM                        | HANA System<br>H22                                            |

Restore points

Logs in last 24 hours

24 hours 72 hours

Tue 12:00 PM Tue 6:00 PM Wed 12:00 AM Wed 6:00 AM

LOG (POINT IN TIME) NO LOGS AVAILABLE

- Select **Restore DB**
- Under **Restore Configuration**, specify where (or how) to restore data:
  - Alternate Location:** Restore the database to an alternate location and keep the original source database.
  - Overwrite DB:** Restore the data to the same SAP HANA instance as the original source. This option overwrites the original database.

Home > ignitedemovault - Backup items > Backup Items (SAP HANA in Azure VM) > h22 > Restore >

| Restore                                                                     | Restore Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>1 Choose Destination<br/>Configure</p> <p>2 Restore Point<br/>Select</p> | <p>Where to Restore?</p> <p><input checked="" type="radio"/> Alternate Location    <input type="radio"/> Overwrite DB</p> <p><b>i</b> If you don't see your SAP HANA Server in the below list go to 'Getting Started' &gt; 'Backup' &gt; 'Start Discovery'</p> <p><b>Host (Can't find Host?) *</b><br/>HANADemoIDC3</p> <p><b>HANA System *</b><br/>H22</p> <p><b>Restored DB Name *</b><br/>h22</p> <p><input type="checkbox"/> Overwrite if the DB with same name already exists on selected HANA instance</p> |
| <b>Restore</b>                                                              | <b>OK</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

#### Restore to alternate location

- In the **Restore Configuration** menu, under **Where to Restore**, select **Alternate Location**.

Home > ignitedemovault - Backup items > Backup Items (SAP HANA in Azure VM) > h22 > Restore >

| Restore                                                                                                   | Restore Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>1</b> Choose Destination &gt;<br/>Configure</p> <hr/> <p><b>2</b> Restore Point &gt;<br/>Select</p> | <p>Where to Restore?</p> <p><input checked="" type="radio"/> Alternate Location    <input type="radio"/> Overwrite DB</p> <div style="background-color: #f0f0f0; padding: 10px;"> <p><b>i</b> If you don't see your SAP HANA Server in the below list go to 'Getting Started' &gt; 'Backup' &gt; 'Start Discovery'</p> </div> <p><b>Host (Can't find Host?) *</b><br/>HANADemoIDC3</p> <p><b>HANA System *</b><br/>H22</p> <p><b>Restored DB Name *</b><br/>h22</p> <p><input type="checkbox"/> Overwrite if the DB with same name already exists on selected HANA instance</p> |
| <b>Restore</b>                                                                                            | <b>OK</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

- Select the SAP HANA host name and instance name to which you want to restore the database.
- Check if the target SAP HANA instance is ready for restore by ensuring its **Backup Readiness**. Refer to the [prerequisites section](#) for more details.
- In the **Restored DB Name** box, enter the name of the target database.

**NOTE**

Single Database Container (SDC) restores must follow these [checks](#).

- If applicable, select **Overwrite if the DB with the same name already exists on selected HANA instance**.
- Select **OK**.

|                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <h3>Restore</h3> <p><b>1</b> Choose Destination &gt;<br/>Configure</p> <p><b>2</b> Restore Point &gt;<br/>Select</p> | <h3>Restore Configuration</h3> <p>If you don't see your SAP HANA Server in the below list go to 'Getting Started' &gt; 'Backup' &gt; 'Start Discovery'</p> <p><b>Host (Can't find Host?) *</b><br/>HANADemoIDC3</p> <p><b>HANA System *</b><br/>H22</p> <p><b>Restored DB Name *</b><br/>h22_restore</p> <p><input type="checkbox"/> Overwrite if the DB with same name already exists on selected HANA instance</p> |
| <p>Restore</p>                                                                                                       | <p><b>OK</b></p>                                                                                                                                                                                                                                                                                                                                                                                                     |

- In **Select restore point**, select **Logs (Point in Time)** to **restore to a specific point in time**. Or select **Full & Differential** to **restore to a specific recovery point**.

#### Restore and overwrite

- In the **Restore Configuration** menu, under **Where to Restore**, select **Overwrite DB** > **OK**.

|                                                                                                                      |                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <h3>Restore</h3> <p><b>1</b> Choose Destination &gt;<br/>Configure</p> <p><b>2</b> Restore Point &gt;<br/>Select</p> | <h3>Restore Configuration</h3> <p>Where to Restore?</p> <p>Alternate Location      <b>Overwrite DB</b></p> <p>We'll overwrite the original DB to:<br/>HANADemoIDC3\H22\h22</p> |
| <p>Restore</p>                                                                                                       | <p><b>OK</b></p>                                                                                                                                                               |

- In **Select restore point**, select **Logs (Point in Time)** to **restore to a specific point in time**. Or select **Full & Differential** to **restore to a specific recovery point**.

**Restore to a specific point in time**

If you've selected **Logs (Point in Time)** as the restore type, do the following:

- Select a recovery point from the log graph and select **OK** to choose the point of restore.

The screenshot shows the 'Select restore point' dialog. On the left, a 'Restore' pane lists step 1 'Choose Destination' (HANADemoIDC3\H22\h22) with a green checkmark, and step 2 'Restore Point' (Select) with a grey arrow icon. On the right, the 'Select restore point' pane has a 'Logs (Point in Time)' tab selected, showing a message: 'Restores corresponding full, differential and log backups with minimal RTO'. Below it is a note: 'Log based restore is available from 10/29/2019, 13:09:02 . To restore from older or Full/Differential backup, click on "Full & differential" above.' A 'Restore Date/Time' section shows 11/07/2019 at 11:06:48 AM in local time (UTC +0530). A timeline graph shows a green bar labeled 'LOG (POINT IN TIME)' from 00 AM to 12:00:00 PM, followed by a grey bar labeled 'NO LOGS AVAILABLE' from 12:00:00 PM to 6:00:00 PM. At the bottom are 'Restore' and 'OK' buttons, with 'OK' highlighted with a red border.

- On the **Restore** menu, select **Restore** to start the restore job.

The screenshot shows the 'Restore' dialog. It lists step 1 'Choose Destination' (HANADemoIDC3\H22\h22\_restore) with a green checkmark, and step 2 'Restore Point' (11/6/2019, 9:06:39 AM) with a green checkmark. At the bottom is a 'Restore' button.

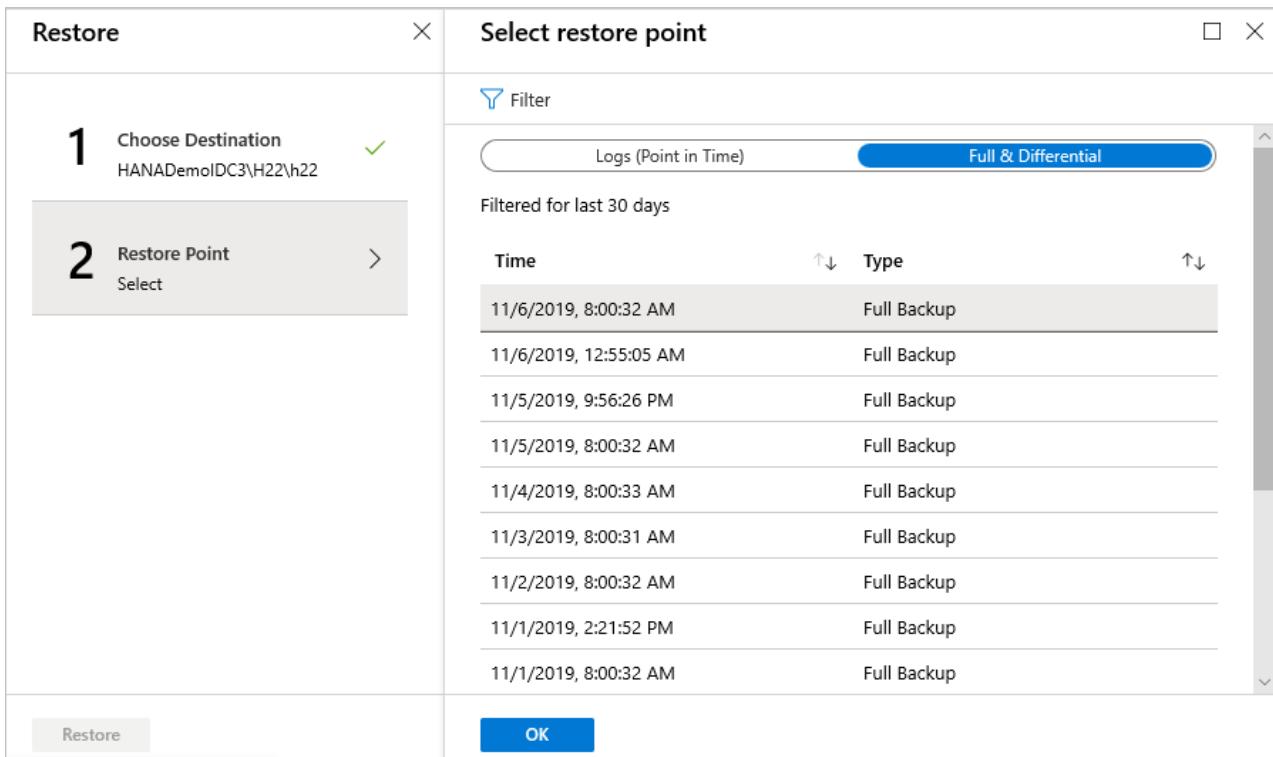
- Track the restore progress in the **Notifications** area or track it by selecting **Restore jobs** on the database menu.

The screenshot shows a notification message: 'Triggering restore for h22' at 5:10 PM. The message continues: 'Restore triggered successfully. Please monitor progress in backup jobs page.' with a small cursor icon pointing to the text.

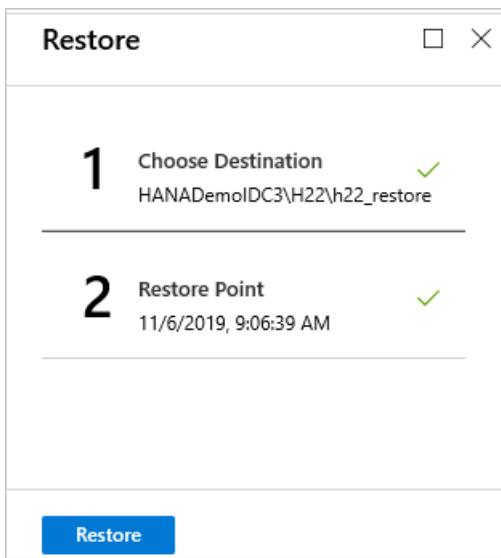
#### Restore to a specific recovery point

If you've selected **Full & Differential** as the restore type, do the following:

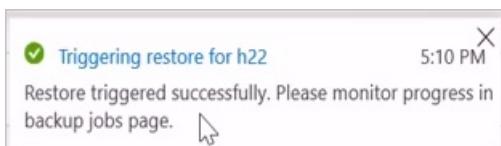
- Select a recovery point from the list and select **OK** to choose the point of restore.



- On the **Restore** menu, select **Restore** to start the restore job.



- Track the restore progress in the **Notifications** area or track it by selecting **Restore jobs** on the database menu.



#### NOTE

In Multiple Database Container (MDC) restores after the system DB is restored to a target instance, one needs to run the pre-registration script again. Only then the subsequent tenant DB restores will succeed. To learn more refer to [Troubleshooting – MDC Restore](#).

## Next steps

- [Learn how](#) to manage SAP HANA databases backed up using Azure Backup

# Manage and monitor backed up SAP HANA databases

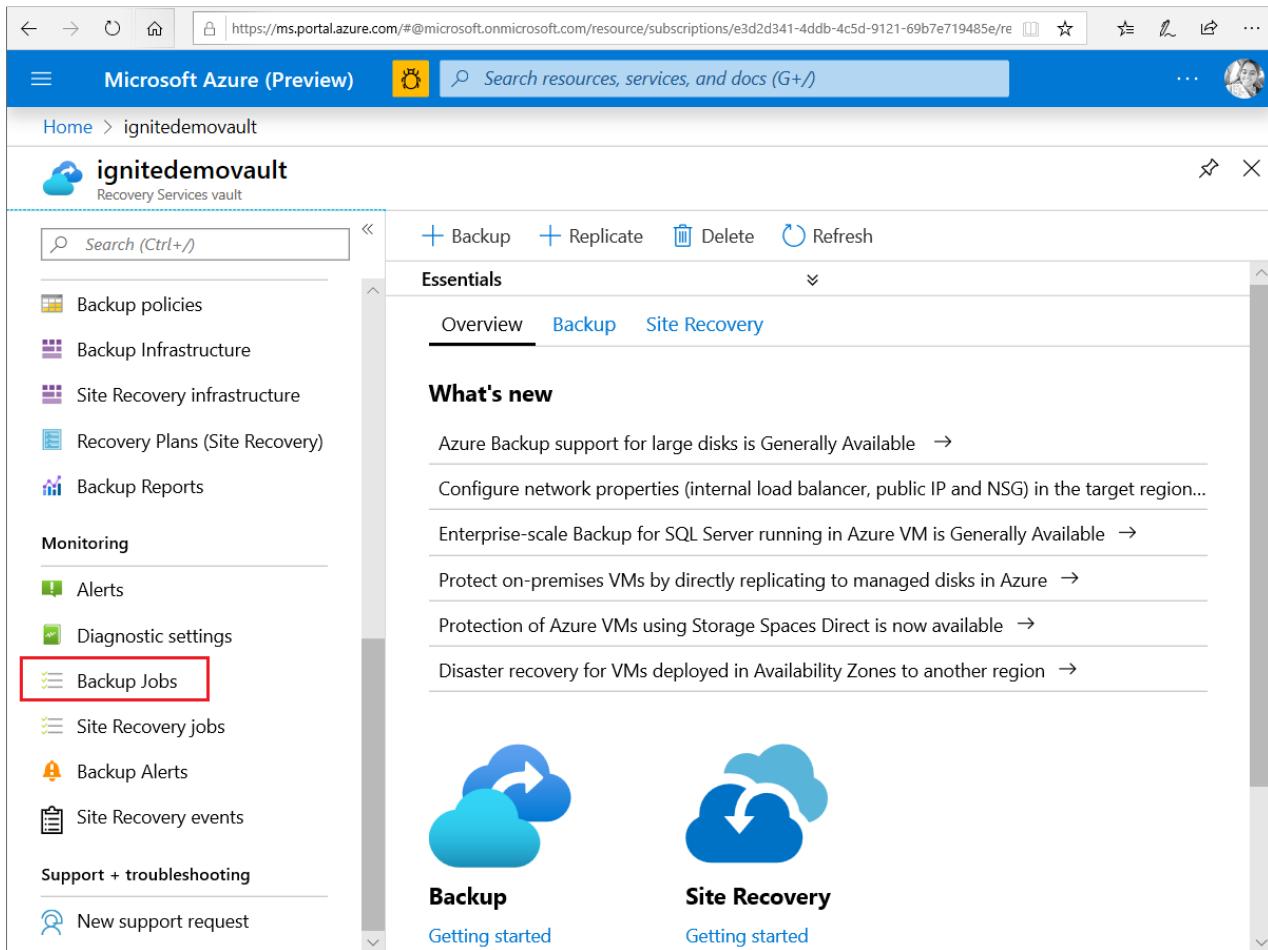
12/13/2019 • 5 minutes to read • [Edit Online](#)

This article describes common tasks for managing and monitoring SAP HANA databases that are running on an Azure virtual machine (VM) and that are backed up to an Azure Backup Recovery Services vault by the [Azure Backup](#) service. You'll learn how to monitor jobs and alerts, trigger an on-demand backup, edit policies, stop and resume database protection and unregister a VM from backups.

If you haven't configured backups yet for your SAP HANA databases, see [Back up SAP HANA databases on Azure VMs](#).

## Monitor manual backup jobs in the portal

Azure Backup shows all manually triggered jobs in the **Backup jobs** section on Azure portal.



The screenshot shows the Microsoft Azure (Preview) portal with the URL <https://ms.portal.azure.com/#@microsoft.onmicrosoft.com/resource/subscriptions/e3d2d341-4ddb-4c5d-9121-69b7e719485e/re>. The page title is "Microsoft Azure (Preview)" and the search bar contains "Search resources, services, and docs (G+/-)". The main content area shows a "Recovery Services vault" named "ignitedemovault". On the left, there's a sidebar with links for Home, ignitedemovault, Backup policies, Backup Infrastructure, Site Recovery infrastructure, Recovery Plans (Site Recovery), Backup Reports, Monitoring (Alerts, Diagnostic settings, Backup Jobs), Site Recovery jobs, Backup Alerts, Site Recovery events, Support + troubleshooting (New support request), and a Getting started button. The "Backup Jobs" link in the Monitoring section is highlighted with a red box. The main content area has tabs for Overview, Backup (which is selected), and Site Recovery. Below the tabs, there's a "What's new" section with several items. At the bottom, there are two large blue cloud icons with arrows, one labeled "Backup" and the other "Site Recovery", each with a "Getting started" button.

The jobs you see in this portal include database discovery and registering, and backup and restore operations. Scheduled jobs, including log backups aren't shown in this section. Manually triggered backups from the SAP HANA native clients (Studio/ Cockpit/ DBA Cockpit) also don't show up here.

ignitedemovault - Backup Jobs

Recovery Services vault

Properties Locks Export template

Getting started

- Backup
- Site Recovery

Protected items

- Backup items
- Replicated items

Manage

- Backup policies
- Backup Infrastructure
- Site Recovery infrastructure
- Recovery Plans (Site Recovery)
- Backup Reports

Filtered by: Item Type - All item types, Operation - All Operations, Status - All Status, Start Time - 10/8/2019, 12:30:31 PM, End Time - 11/7/2019, 12:30:31 PM

Completed fetching data from the service.

| Worklo...↑↓   | Operati...↑↓   | Status ↑↓    | Type ↑↓       | Start ti...↑↓  | Duration↑↓ | ... |
|---------------|----------------|--------------|---------------|----------------|------------|-----|
| H22/H22 [H... | Restore        | ✖ Failed     | AzureWorkl... | 11/6/2019, ... | 00:03:03   | ... |
| H22/H22 [H... | Restore (Full) | ✓ Complet... | AzureWorkl... | 11/1/2019, ... | 00:09:06   | ... |
| H22/H22 [H... | Restore (Log)  | ✓ Complet... | AzureWorkl... | 10/30/2019...  | 00:09:07   | ... |
| H21/H21 [H... | Backup (Full)  | ✓ Complet... | AzureWorkl... | 10/29/2019...  | 00:04:03   | ... |
| H21/SYSTEM... | Backup (Full)  | ✓ Complet... | AzureWorkl... | 10/29/2019...  | 00:04:04   | ... |
| systemdb      | Configure b... | ✓ Complet... | AzureWorkl... | 10/29/2019...  | 00:01:13   | ... |
| h21           | Configure b... | ✓ Complet... | AzureWorkl... | 10/29/2019...  | 00:01:47   | ... |
| HANADemo...   | Register       | ✓ Complet... | AzureWorkl... | 10/29/2019...  | 00:01:38   | ... |
| H22/H22 [H... | Restore (Full) | ✓ Complet... | AzureWorkl... | 10/29/2019...  | 00:09:07   | ... |
| H22/H22 [H... | Backup (Full)  | ✖ Failed     | AzureWorkl... | 10/29/2019...  | 00:02:31   | ... |

To learn more about monitoring, go to [Monitoring in the Azure portal](#) and [Monitoring using Azure Monitor](#).

## View backup alerts

Alerts are an easy means of monitoring backups of SAP HANA databases. Alerts help you focus on the events you care about the most without getting lost in the multitude of events that a backup generates. Azure Backup allows you to set alerts, and they can be monitored as follows:

- Sign in to the [Azure portal](#).
- On the vault dashboard, select **Backup Alerts**.

The screenshot shows the Azure Recovery Services vault management interface for the 'ignitedemovault' recovery services vault. The left sidebar contains several navigation items:

- Manage**
  - Backup policies
  - Backup Infrastructure
  - Site Recovery infrastructure
  - Recovery Plans (Site Recovery)
  - Backup Reports
- Monitoring**
  - Alerts
  - Diagnostic settings
  - Backup Jobs
  - Site Recovery jobs
  - Backup Alerts** (highlighted with a red border)
  - Site Recovery events
- Support + troubleshooting**
  - New support request

A search bar at the top is labeled "Search (Ctrl+ /)".

- You will be able to see the alerts:

**ignitedemovault - Backup Alerts**  
Recovery Services vault

Search (Ctrl+)

Manage

- Backup policies
- Backup Infrastructure
- Site Recovery infrastructure
- Recovery Plans (Site Recovery)
- Backup Reports

Monitoring

- Alerts
- Diagnostic settings
- Backup Jobs
- Site Recovery jobs
- Backup Alerts**
- Site Recovery events

Support + troubleshooting

Choose columns Filter Configure notifications Refresh

Filtered by: Status - Status - All, Severity - All Severities, Start Time - 10/8/2019, 12:32:43 PM, End Time - 11/7/2019, 12:32:43 PM

Completed fetching data from the service.

Filter items...

| Alert           | Backup item | Protected server | Severity | Duration     | Created    | Status | ... |
|-----------------|-------------|------------------|----------|--------------|------------|--------|-----|
| Restore failure | H22/H22     | HANADe...        | Critical | 17:47:29     | 11/6/2019  | Active | ... |
| Backup failure  | H21/H21     | HANADe...        | Critical | 8 days 22... | 10/29/2019 | Active | ... |
| Backup failure  | H21/H21     | HANADe...        | Critical | 8 days 22... | 10/29/2019 | Active | ... |
| Backup failure  | H22/H22     | HANADe...        | Critical | 8 days 23... | 10/29/2019 | Active | ... |
| Backup failure  | H22/H22     | HANADe...        | Critical | 8 days 23... | 10/29/2019 | Active | ... |
| Backup failure  | H22/H22     | HANADe...        | Critical | 8 days 23... | 10/29/2019 | Active | ... |
| Backup failure  | H22/H22     | HANADe...        | Critical | 8 days 23... | 10/29/2019 | Active | ... |
| Backup failure  | H22/H22     | HANADe...        | Critical | 8 days 23... | 10/29/2019 | Active | ... |
| Backup failure  | H22/SYS...  | HANADe...        | Critical | 8 days 23... | 10/29/2019 | Active | ... |

- Click on the alerts to see more details:

**Details**

Inactivate

**Alert** Restore failure

|                               |                                                                                                                                                                                                                                                                                         |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Status</b>                 | Active                                                                                                                                                                                                                                                                                  |
| <b>Alert type</b>             | Recovery                                                                                                                                                                                                                                                                                |
| <b>Severity</b>               | Critical                                                                                                                                                                                                                                                                                |
| <b>Backup item</b>            | H22/H22                                                                                                                                                                                                                                                                                 |
| <b>Backup item type</b>       | AzureWorkload                                                                                                                                                                                                                                                                           |
| <b>Protected server</b>       | HANADemoIDC3                                                                                                                                                                                                                                                                            |
| <b>Creation time</b>          | 11/7/2019, 10:25:03 PM                                                                                                                                                                                                                                                                  |
| <b>Latest occurrence time</b> | 11/7/2019, 10:25:03 PM                                                                                                                                                                                                                                                                  |
| <b>Occurrence count</b>       | 1                                                                                                                                                                                                                                                                                       |
| <b>Description</b>            | Database with same name already exists at the target location.                                                                                                                                                                                                                          |
| <b>Recommended action</b>     | Please select overwrite option during restore, or select a different database name. For troubleshooting instructions, see <a href="https://aka.ms/AB-usererrorcannotrestoreexistingdbwithoutforceoverwrite">https://aka.ms/AB-usererrorcannotrestoreexistingdbwithoutforceoverwrite</a> |
| <b>Alert raised on</b>        | BackupItem                                                                                                                                                                                                                                                                              |

Today, Azure Backup allows the sending of alerts through email. These alerts are:

- Triggered for all backup failures.
- Consolidated at the database level by error code.
- Sent only for a database's first backup failure.

To learn more about monitoring, go to [Monitoring in the Azure portal](#) and [Monitoring using Azure Monitor](#).

## Management Operations

Azure Backup makes management of a backed-up SAP HANA database easy with an abundance of management operations that it supports. These operations are discussed in more detail in the following sections.

### Run an ad-hoc backup

Backups run in accordance with the policy schedule. You can run a backup on-demand as follows:

1. In the vault menu, click **Backup items**.
2. In **Backup Items**, select the VM running the SAP HANA database, and then click **Backup now**.
3. In **Backup Now**, use the calendar control to select the last day that the recovery point should be retained. Then click **OK**.
4. Monitor the portal notifications. You can monitor the job progress in the vault dashboard > **Backup Jobs** > **In progress**. Depending on the size of your database, creating the initial backup may take a while.

### Run SAP HANA native client backup on a database with Azure backup enabled

If you want to take a local backup (using HANA Studio / Cockpit) of a database that's being backed up with Azure Backup, do the following:

1. Wait for any full or log backups for the database to finish. Check the status in SAP HANA Studio/ Cockpit.
2. Disable log backups, and set the backup catalog to the file system for relevant database.
3. To do this, double-click **systemdb** > **Configuration** > **Select Database** > **Filter (Log)**.
4. Set **enable\_auto\_log\_backup** to **No**.
5. Set **log\_backup\_using\_backint** to **False**.
6. Take an on-demand full backup of the database.
7. Wait for the full backup and catalog backup to finish.
8. Revert the previous settings back to those for Azure:
  - Set **enable\_auto\_log\_backup** to **Yes**.
  - Set **log\_backup\_using\_backint** to **True**.

### Change policy

You can change the underlying policy for an SAP HANA backup item.

- In the vault dashboard, go to **Backup items**:

The screenshot shows the Azure portal interface for a Recovery Services vault named 'ignitedemovault'. The left sidebar contains several navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Properties, Locks, Export template, Backup, Site Recovery, and Backup items. The 'Backup items' link is highlighted with a red box.

- Choose **SAP HANA in Azure VM**

| BACKUP MANAGEMENT TYPE      | BACKUP ITEM COUNT |
|-----------------------------|-------------------|
| SAP HANA in Azure VM        | 4                 |
| SQL in Azure VM             | 0                 |
| Azure Storage (Azure Files) | 0                 |
| DPM                         | 0                 |
| Azure Backup Server         | 0                 |
| Azure Backup Agent          | 0                 |
| Azure Virtual Machine       | 0                 |

- Choose the backup item whose underlying policy you want to change
- Click on the existing Backup policy

h22

Backup now Restore Stop backup Delete backup data Resume backup

Essentials ^

|                                                          |                                                                 |
|----------------------------------------------------------|-----------------------------------------------------------------|
| Recovery services vault<br><b>ignitedemovault</b>        | Backup Status<br>Unhealthy                                      |
| Subscription name<br><b>Backup_Canary_PM_Prod_Demo-1</b> | Latest restore point<br>12/6/2019, 11:32:05 PM (3 day(s) ago)   |
| Subscription ID<br>e3d2d341-4ddb-4c5d-9121-69b7e719485e  | Oldest restore point<br>10/29/2019, 1:09:02 PM (1 month(s) ago) |
| Host name<br>HANADemoDC3                                 | Backup policy<br><b>DailyFullLog2</b>                           |
| Item type<br>SAP HANA in Azure VM                        | HANA System<br>H22                                              |

Restore points

Logs in last 24 hours

Mon 12:00 PM Mon 6:00 PM Tue 12:00 AM Tue 01:29:00 AM Tue 6:00 AM

**LOG (POINT IN TIME)** NO LOGS AVAILABLE

24 hours 72 hours

- Change the policy, choosing from the list. [Create a new backup policy](#) if needed.

### Backup Policy

**i** Please choose a policy from below drop down and click on save to apply changes.

DailyFullLog2

**Backup Frequency**  
Daily at 2:30 AM UTC

**Retention of daily backup point**  
Retain backup taken every day at 2:30 AM for 180 Day(s)

**Retention of weekly backup point**  
Retain backup taken every week on Sunday at 2:30 AM for 104 Week(s)

**Retention of monthly backup point**  
Retain backup taken every month on First Sunday at 2:30 AM for 60 Month(s)

**Retention of yearly backup point**  
Retain backup taken every year in January on First Sunday at 2:30 AM for 10 Year(s)

**LOG BACKUP**

**Backup schedule**  
Every 2 hours

**Retained for**  
15 days

- Save the changes

**Backup Policy**

 Save  Discard

**Information:** Please choose a policy from below drop down and click on save to apply changes.

demopolicy

**FULL BACKUP**

**Backup Frequency**  
Daily at 2:30 AM UTC

**Retention of daily backup point**  
Retain backup taken every day at 2:30 AM for 180 Day(s)

**Retention of weekly backup point**  
Retain backup taken every week on Sunday at 2:30 AM for 104 Week(s)

**Retention of monthly backup point**  
Retain backup taken every month on First Sunday at 2:30 AM for 60 Month(s)

**Retention of yearly backup point**  
Retain backup taken every year in January on First Sunday at 2:30 AM for 10 Year(s)

**LOG BACKUP**

**Backup schedule**  
Every 2 hours

**Retained for**  
15 days

- Policy modification will impact all the associated Backup Items and trigger corresponding **configure protection** jobs.

#### NOTE

Any change in the retention period will be applied retrospectively to all the older recovery points besides the new ones.

Incremental backup policies cannot be used for SAP HANA databases. Incremental backup is not currently supported for these databases.

#### Stop protection for an SAP HANA database

You can stop protecting an SAP HANA database in a couple of ways:

- Stop all future backup jobs and delete all recovery points.
- Stop all future backup jobs and leave the recovery points intact.

If you choose to leave recovery points, keep these details in mind:

- All recovery points will remain intact forever, all pruning shall stop at stop protection with retain data.
- You will be charged for the protected instance and the consumed storage. For more information, see [Azure Backup pricing](#).
- If you delete a data source without stopping backups, new backups will fail.

To stop protection for a database:

- On the vault dashboard, select **Backup Items**.

- Under **Backup Management Type**, select **SAP HANA in Azure VM**

| BACKUP MANAGEMENT TYPE      | BACKUP ITEM COUNT |
|-----------------------------|-------------------|
| SAP HANA in Azure VM        | 4                 |
| SQL in Azure VM             | 0                 |
| Azure Storage (Azure Files) | 0                 |
| DPM                         | 0                 |
| Azure Backup Server         | 0                 |
| Azure Backup Agent          | 0                 |
| Azure Virtual Machine       | 0                 |

- Select the database for which you want to stop protection on:

**Backup Items (SAP HANA in Azure VM)**

ignitedemovault

⟳ Refresh + Add Filter

(i) Fetching data from service completed.

🔍 Filter items ...

| Database | HANA System      | Type        | Backup Status |     |
|----------|------------------|-------------|---------------|-----|
| h22      | HANADemoIDC3\H22 | HANA System | ✓ Healthy     | ... |
| systemdb | HANADemoIDC3\H22 | HANA System | ✓ Healthy     | ... |
| systemdb | HANADemoIDC4\H21 | HANA System | ✓ Healthy     | ... |
| h21      | HANADemoIDC4\H21 | HANA System | ✓ Healthy     | ... |

- On the database menu, select **Stop backup**.

**h22**

Backup now    Restore DB    Stop backup    Delete backup data    Resume backup

Essentials ^

|                                                          |                                                                |
|----------------------------------------------------------|----------------------------------------------------------------|
| Recovery services vault<br><b>ignitedemovault</b>        | Backup Status<br>Healthy                                       |
| Subscription name<br><b>Backup_Canary_PM_Prod_Demo-1</b> | Latest restore point<br>11/7/2019, 11:06:48 AM (1 hour(s) ago) |
| Subscription ID<br>e3d2d341-4ddb-4c5d-9121-69b7e719485e  | Oldest restore point<br>10/29/2019, 1:09:02 PM (8 day(s) ago)  |
| Host name<br>HANADemo1DC3                                | Backup policy<br><b>DailyFullLog2</b>                          |
| Item type<br>SAP HANA in Azure VM                        | HANA System<br>H22                                             |

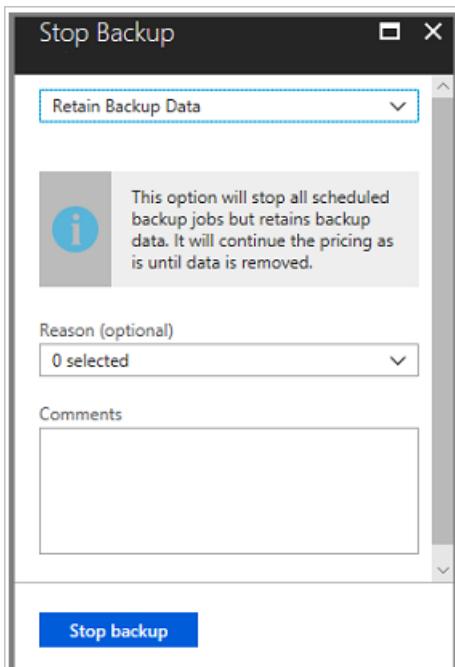
Restore points

Logs in last 24 hours

24 hours    72 hours

Wed 6:00 PM    Thu 12:00 AM    Thu 6:00 AM    Thu 12:00 PM

- On the **Stop Backup** menu, select whether to retain or delete data. If you want, provide a reason and comment.



- Select **Stop backup**.

#### Resume protection for an SAP HANA database

When you stop protection for the SAP HANA database, if you select the **Retain Backup Data** option, you can later resume protection. If you don't retain the backed-up data, you will not be able to resume protection.

To resume protection for an SAP HANA database:

- Open the backup item and select **Resume backup**.



- On the **Backup policy** menu, select a policy, and then select **Save**.

## Upgrading from SAP HANA 1.0 to 2.0

Learn how to continue backup for an SAP HANA database [after upgrading from SAP HANA 1.0 to 2.0](#).

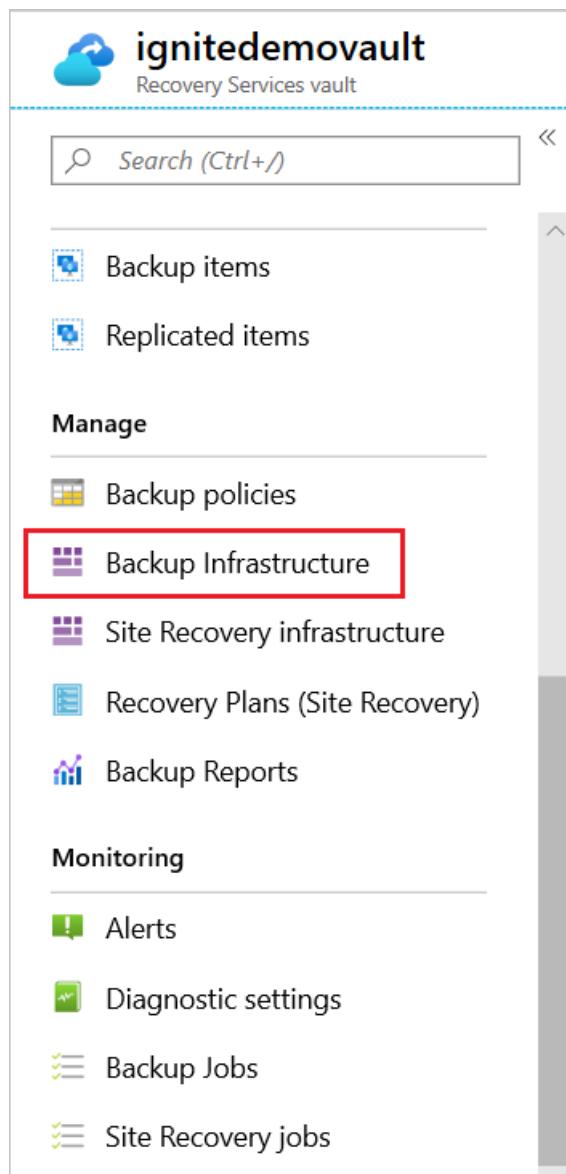
## Upgrading without a SID change

Learn how to continue backup of an SAP HANA database whose [SID has not changed after upgrade](#).

## Unregister an SAP HANA database

Unregister an SAP HANA instance after you disable protection but before you delete the vault:

- On the vault dashboard, under **Manage**, select **Backup Infrastructure**.



- Select the **Backup Management type** as **Workload in Azure VM**

| BACKUP MANAGEMENT TYPE | PROTECTED SERVER COUNT |
|------------------------|------------------------|
| Workload in Azure VM   | 2                      |
| Azure Backup Agent     | 0                      |
| DPM                    | 0                      |
| Azure Backup Server    | 0                      |

- In **Protected Servers**, select the instance to unregister. To delete the vault, you must unregister all servers/instances.
- Right-click the protected instance and select **Unregister**.

**Protected Servers (Workload in Azure VM)**  
ignitedemovault

⟳ Refresh ⌂ Filter

**i** Fetching data from service completed.

Filter items ...

| VM Name      | ↑↓ VM RG | ↑↓ Server | ↑↓  |
|--------------|----------|-----------|-----|
| HANADemoIDC3 | IDCDemo  |           | ... |
| HANADemoIDC4 | IDCDemo  |           | ... |

Pin to dashboard ⚡

Rediscover DBs

**Unregister**

Re-register

## Next steps

- Learn how to [troubleshoot common issues when backing up SAP HANA databases](#).

# Azure Backup Server protection matrix

2/18/2020 • 15 minutes to read • [Edit Online](#)

This article lists the various servers and workloads that you can protect with Azure Backup Server. The following matrix lists what can be protected with Azure Backup Server.

## Protection support matrix

| WORKLOAD                             | VERSION     | AZURE BACKUP SERVER INSTALLATION                                             | SUPPORTED AZURE BACKUP SERVER | PROTECTION AND RECOVERY                                                                                                                                                                                                                                                                                    |
|--------------------------------------|-------------|------------------------------------------------------------------------------|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Client computers (64-bit and 32-bit) | Windows 10  | Physical server<br><br>Hyper-V virtual machine<br><br>VMware virtual machine | V3, V2                        | Volume, share, folder, files, deduped volumes<br><br>Protected volumes must be NTFS. FAT and FAT32 aren't supported.<br><br>Volumes must be at least 1 GB. Azure Backup Server uses Volume Shadow Copy Service (VSS) to take the data snapshot and the snapshot only works if the volume is at least 1 GB. |
| Client computers (64-bit and 32-bit) | Windows 8.1 | Physical server<br><br>Hyper-V virtual machine                               | V3, V2                        | Files<br><br>Protected volumes must be NTFS. FAT and FAT32 aren't supported.<br><br>Volumes must be at least 1 GB. Azure Backup Server uses Volume Shadow Copy Service (VSS) to take the data snapshot and the snapshot only works if the volume is at least 1 GB.                                         |

| Workload                             | Version     | Azure Backup Server Installation                                                                    | Supported Azure Backup Server | Protection and Recovery                                                                                                                                                                                                                                                                                           |
|--------------------------------------|-------------|-----------------------------------------------------------------------------------------------------|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Client computers (64-bit and 32-bit) | Windows 8.1 | Windows virtual machine in VMWare (protects workloads running in Windows virtual machine in VMWare) | V3, V2                        | <p>Volume, share, folder, files, deduped volumes</p> <p>Protected volumes must be NTFS. FAT and FAT32 aren't supported.</p> <p>Volumes must be at least 1 GB. Azure Backup Server uses Volume Shadow Copy Service (VSS) to take the data snapshot and the snapshot only works if the volume is at least 1 GB.</p> |
| Client computers (64-bit and 32-bit) | Windows 8   | Physical server<br><br>On-premises Hyper-V virtual machine                                          | V3, V2                        | <p>Volume, share, folder, files, deduped volumes</p> <p>Protected volumes must be NTFS. FAT and FAT32 aren't supported.</p> <p>Volumes must be at least 1 GB. Azure Backup Server uses Volume Shadow Copy Service (VSS) to take the data snapshot and the snapshot only works if the volume is at least 1 GB.</p> |
| Client computers (64-bit and 32-bit) | Windows 8   | Windows virtual machine in VMWare (protects workloads running in Windows virtual machine in VMWare) | V3, V2                        | <p>Volume, share, folder, files, deduped volumes</p> <p>Protected volumes must be NTFS. FAT and FAT32 aren't supported.</p> <p>Volumes must be at least 1 GB. Azure Backup Server uses Volume Shadow Copy Service (VSS) to take the data snapshot and the snapshot only works if the volume is at least 1 GB.</p> |

| Workload                             | Version             | Azure Backup Server Installation                                                                                                                                                                                                                                                 | Supported Azure Backup Server | Protection and Recovery                                                                                                                                                                                                                                                                                           |
|--------------------------------------|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Client computers (64-bit and 32-bit) | Windows 7           | Physical server<br><br>On-premises Hyper-V virtual machine                                                                                                                                                                                                                       | V3, V2                        | <p>Volume, share, folder, files, deduped volumes</p> <p>Protected volumes must be NTFS. FAT and FAT32 aren't supported.</p> <p>Volumes must be at least 1 GB. Azure Backup Server uses Volume Shadow Copy Service (VSS) to take the data snapshot and the snapshot only works if the volume is at least 1 GB.</p> |
| Client computers (64-bit and 32-bit) | Windows 7           | Windows virtual machine in VMWare (protects workloads running in Windows virtual machine in VMWare)                                                                                                                                                                              | V3, V2                        | <p>Volume, share, folder, files, deduped volumes</p> <p>Protected volumes must be NTFS. FAT and FAT32 aren't supported.</p> <p>Volumes must be at least 1 GB. Azure Backup Server uses Volume Shadow Copy Service (VSS) to take the data snapshot and the snapshot only works if the volume is at least 1 GB.</p> |
| Servers (64-bit)                     | Windows Server 2019 | <p>Azure virtual machine (when workload is running as Azure virtual machine)</p> <p>Windows virtual machine in VMWare (protects workloads running in Windows virtual machine in VMWare)</p> <p>Physical server</p> <p>On-premises Hyper-V virtual machine</p> <p>Azure Stack</p> | V3<br><br>Not Nano server     | Volume, share, folder, file, system state/bare metal), deduped volumes                                                                                                                                                                                                                                            |

| WORKLOAD                    | VERSION                                                     | AZURE BACKUP SERVER INSTALLATION                                                                                                                                                                                                                                          | SUPPORTED AZURE BACKUP SERVER | PROTECTION AND RECOVERY                                                                                                                                                            |
|-----------------------------|-------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Servers (32-bit and 64-bit) | Windows Server 2016                                         | Azure virtual machine (when workload is running as Azure virtual machine)<br><br>Windows virtual machine in VMWare (protects workloads running in Windows virtual machine in VMWare)<br><br>Physical server<br><br>On-premises Hyper-V virtual machine<br><br>Azure Stack | V3, V2<br>Not Nano server     | Volume, share, folder, file, system state/bare metal), deduped volumes                                                                                                             |
| Servers (32-bit and 64-bit) | Windows Server 2012 R2 - Datacenter and Standard            | Azure virtual machine (when workload is running as Azure virtual machine)<br><br>Azure Stack                                                                                                                                                                              | V3, V2                        | Volume, share, folder, file<br><br>Azure Backup Server must be running on at least Windows Server 2012 R2 to protect Windows Server 2012 deduped volumes.                          |
| Servers (32-bit and 64-bit) | Windows Server 2012 R2 - Datacenter and Standard            | Windows virtual machine in VMWare (protects workloads running in Windows virtual machine in VMWare)<br><br>Azure Stack                                                                                                                                                    | V3, V2                        | Volume, share, folder, file, system state/bare metal)<br><br>Azure Backup Server must be running on Windows Server 2012 or 2012 R2 to protect Windows Server 2012 deduped volumes. |
| Servers (32-bit and 64-bit) | Windows Server 2012/2012 with SP1 - Datacenter and Standard | Physical server<br><br>On-premises Hyper-V virtual machine<br><br>Azure Stack                                                                                                                                                                                             | V3, V2                        | Volume, share, folder, file, system state/bare metal<br><br>Azure Backup Server must be running on at least Windows Server 2012 R2 to protect Windows Server 2012 deduped volumes. |

| Workload                    | Version                                                     | Azure Backup Server Installation                                                                                       | Supported Azure Backup Server                                                                 | Protection and Recovery                                                                                                                                                            |
|-----------------------------|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Servers (32-bit and 64-bit) | Windows Server 2012/2012 with SP1 - Datacenter and Standard | Azure virtual machine (when workload is running as Azure virtual machine)<br><br>Azure Stack                           | V3, V2                                                                                        | Volume, share, folder, file<br><br>Azure Backup Server must be running on at least Windows Server 2012 R2 to protect Windows Server 2012 deduped volumes.                          |
| Servers (32-bit and 64-bit) | Windows Server 2012/2012 with SP1 - Datacenter and Standard | Windows virtual machine in VMWare (protects workloads running in Windows virtual machine in VMWare)<br><br>Azure Stack | V3, V2                                                                                        | Volume, share, folder, file, system state/bare metal<br><br>Azure Backup Server must be running on at least Windows Server 2012 R2 to protect Windows Server 2012 deduped volumes. |
| Servers (32-bit and 64-bit) | Windows Server 2008 R2 SP1 - Standard and Enterprise        | Physical server<br><br>On-premises Hyper-V virtual machine<br><br>Azure Stack                                          | V3, V2<br>You need to be running SP1 and install <a href="#">Windows Management Frame 4.0</a> | Volume, share, folder, file, system state/bare metal                                                                                                                               |
| Servers (32-bit and 64-bit) | Windows Server 2008 R2 SP1 - Standard and Enterprise        | Azure virtual machine (when workload is running as Azure virtual machine)<br><br>Azure Stack                           | V3, V2<br>You need to be running SP1 and install <a href="#">Windows Management Frame 4.0</a> | Volume, share, folder, file                                                                                                                                                        |
| Servers (32-bit and 64-bit) | Windows Server 2008 R2 SP1 - Standard and Enterprise        | Windows virtual machine in VMWare (protects workloads running in Windows virtual machine in VMWare)<br><br>Azure Stack | V3, V2<br>You need to be running SP1 and install <a href="#">Windows Management Frame 4.0</a> | Volume, share, folder, file, system state/bare metal                                                                                                                               |
| Servers (32-bit and 64-bit) | Windows Server 2008 SP2                                     | Physical server<br><br>On-premises Hyper-V virtual machine<br><br>Azure Stack                                          | Not supported                                                                                 | Volume, share, folder, file, system state/bare metal                                                                                                                               |

| WORKLOAD                    | VERSION                     | AZURE BACKUP SERVER INSTALLATION                                                                                                                                                                                                                                          | SUPPORTED AZURE BACKUP SERVER | PROTECTION AND RECOVERY                              |
|-----------------------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|------------------------------------------------------|
| Servers (32-bit and 64-bit) | Windows Server 2008 SP2     | Windows virtual machine in VMWare (protects workloads running in Windows virtual machine in VMWare)<br><br>Azure Stack                                                                                                                                                    | V3, V2                        | Volume, share, folder, file, system state/bare metal |
| Servers (32-bit and 64-bit) | Windows Storage Server 2008 | Physical server<br><br>On-premises Hyper-V virtual machine<br><br>Azure Stack                                                                                                                                                                                             | V3, V2                        | Volume, share, folder, file, system state/bare metal |
| SQL Server                  | SQL Server 2019             | Physical server<br><br>On-premises Hyper-V virtual machine<br><br>Azure virtual machine (when workload is running as Azure virtual machine)<br><br>Windows virtual machine in VMWare (protects workloads running in Windows virtual machine in VMWare)<br><br>Azure Stack | V3                            | All deployment scenarios: database                   |
| SQL Server                  | SQL Server 2017             | Physical server<br><br>On-premises Hyper-V virtual machine<br><br>Azure virtual machine (when workload is running as Azure virtual machine)<br><br>Windows virtual machine in VMWare (protects workloads running in Windows virtual machine in VMWare)<br><br>Azure Stack | V3                            | All deployment scenarios: database                   |

| <b>WORKLOAD</b> | <b>VERSION</b>      | <b>AZURE BACKUP SERVER INSTALLATION</b>                                                                                                                                                                               | <b>SUPPORTED AZURE BACKUP SERVER</b> | <b>PROTECTION AND RECOVERY</b>     |
|-----------------|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|------------------------------------|
| SQL Server      | SQL Server 2016 SP2 | Physical server<br><br>On-premises Hyper-V virtual machine<br><br>Azure virtual machine<br><br>Windows virtual machine in VMWare (protects workloads running in Windows virtual machine in VMWare)<br><br>Azure Stack | V3, V2                               | All deployment scenarios: database |
| SQL Server      | SQL Server 2016 SP1 | Physical server<br><br>On-premises Hyper-V virtual machine<br><br>Azure virtual machine<br><br>Windows virtual machine in VMWare (protects workloads running in Windows virtual machine in VMWare)<br><br>Azure Stack | V3, V2                               | All deployment scenarios: database |
| SQL Server      | SQL Server 2016     | Physical server<br><br>On-premises Hyper-V virtual machine<br><br>Azure virtual machine<br><br>Windows virtual machine in VMWare (protects workloads running in Windows virtual machine in VMWare)<br><br>Azure Stack | V3, V2                               | All deployment scenarios: database |
| SQL Server      | SQL Server 2014     | Azure virtual machine (when workload is running as Azure virtual machine)<br><br>Azure Stack                                                                                                                          | V3, V2                               | All deployment scenarios: database |

| <b>WORKLOAD</b> | <b>VERSION</b>                            | <b>AZURE BACKUP SERVER INSTALLATION</b>                                                                                | <b>SUPPORTED AZURE BACKUP SERVER</b> | <b>PROTECTION AND RECOVERY</b>     |
|-----------------|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------|--------------------------------------|------------------------------------|
| SQL Server      | SQL Server 2014                           | Windows virtual machine in VMWare (protects workloads running in Windows virtual machine in VMWare)<br><br>Azure Stack | V3, V2                               | All deployment scenarios: database |
| SQL Server      | SQL Server 2012 with SP2                  | Physical server<br><br>On-premises Hyper-V virtual machine<br><br>Azure Stack                                          | V3, V2                               | All deployment scenarios: database |
| SQL Server      | SQL Server 2012 with SP2                  | Azure virtual machine (when workload is running as Azure virtual machine)<br><br>Azure Stack                           | V3, V2                               | All deployment scenarios: database |
| SQL Server      | SQL Server 2012 with SP2                  | Windows virtual machine in VMWare (protects workloads running in Windows virtual machine in VMWare)<br><br>Azure Stack | V3, V2                               | All deployment scenarios: database |
| SQL Server      | SQL Server 2012, SQL Server 2012 with SP1 | Physical server<br><br>On-premises Hyper-V virtual machine<br><br>Azure Stack                                          | V3, V2                               | All deployment scenarios: database |
| SQL Server      | SQL Server 2012, SQL Server 2012 with SP1 | Azure virtual machine (when workload is running as Azure virtual machine)<br><br>Azure Stack                           | V3, V2                               | All deployment scenarios: database |
| SQL Server      | SQL Server 2012, SQL Server 2012 with SP1 | Windows virtual machine in VMWare (protects workloads running in Windows virtual machine in VMWare)<br><br>Azure Stack | V3, V2                               | All deployment scenarios: database |

| WORKLOAD   | VERSION            | AZURE BACKUP SERVER INSTALLATION                                                                                       | SUPPORTED AZURE BACKUP SERVER | PROTECTION AND RECOVERY            |
|------------|--------------------|------------------------------------------------------------------------------------------------------------------------|-------------------------------|------------------------------------|
| SQL Server | SQL Server 2008 R2 | Physical server<br><br>On-premises Hyper-V virtual machine<br><br>Azure Stack                                          | V3, V2                        | All deployment scenarios: database |
| SQL Server | SQL Server 2008 R2 | Azure virtual machine (when workload is running as Azure virtual machine)<br><br>Azure Stack                           | V3, V2                        | All deployment scenarios: database |
| SQL Server | SQL Server 2008 R2 | Windows virtual machine in VMWare (protects workloads running in Windows virtual machine in VMWare)<br><br>Azure Stack | V3, V2                        | All deployment scenarios: database |
| SQL Server | SQL Server 2008    | Physical server<br><br>On-premises Hyper-V virtual machine<br><br>Azure Stack                                          | V3, V2                        | All deployment scenarios: database |
| SQL Server | SQL Server 2008    | Azure virtual machine (when workload is running as Azure virtual machine)<br><br>Azure Stack                           | V3, V2                        | All deployment scenarios: database |
| SQL Server | SQL Server 2008    | Windows virtual machine in VMWare (protects workloads running in Windows virtual machine in VMWare)<br><br>Azure Stack | V3, V2                        | All deployment scenarios: database |

| WORKLOAD | VERSION       | AZURE BACKUP SERVER INSTALLATION                                                                                                                                      | SUPPORTED AZURE BACKUP SERVER | PROTECTION AND RECOVERY                                                                                                                                                                                                                                       |
|----------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Exchange | Exchange 2016 | <p>Physical server</p> <p>On-premises Hyper-V virtual machine</p> <p>Azure Stack</p> <p>Azure virtual machine (when workload is running as Azure virtual machine)</p> | V3, V2                        | <p>Protect (all deployment scenarios): Standalone Exchange server, database under a database availability group (DAG)</p> <p>Recover (all deployment scenarios): Mailbox, mailbox databases under a DAG</p> <p>Backup of Exchange over ReFS not supported</p> |
| Exchange | Exchange 2016 | <p>Windows virtual machine in VMWare (protects workloads running in Windows virtual machine in VMWare)</p> <p>Azure Stack</p>                                         | V3, V2                        | <p>Protect (all deployment scenarios): Standalone Exchange server, database under a database availability group (DAG)</p> <p>Recover (all deployment scenarios): Mailbox, mailbox databases under a DAG</p> <p>Backup of Exchange over ReFS not supported</p> |
| Exchange | Exchange 2013 | <p>Physical server</p> <p>On-premises Hyper-V virtual machine</p> <p>Azure Stack</p>                                                                                  | V3, V2                        | <p>Protect (all deployment scenarios): Standalone Exchange server, database under a database availability group (DAG)</p> <p>Recover (all deployment scenarios): Mailbox, mailbox databases under a DAG</p> <p>Backup of Exchange over ReFS not supported</p> |

| WORKLOAD | VERSION       | AZURE BACKUP SERVER INSTALLATION                                                                                              | SUPPORTED AZURE BACKUP SERVER | PROTECTION AND RECOVERY                                                                                                                                                                                                                                       |
|----------|---------------|-------------------------------------------------------------------------------------------------------------------------------|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Exchange | Exchange 2013 | <p>Windows virtual machine in VMWare (protects workloads running in Windows virtual machine in VMWare)</p> <p>Azure Stack</p> | V3, V2                        | <p>Protect (all deployment scenarios): Standalone Exchange server, database under a database availability group (DAG)</p> <p>Recover (all deployment scenarios): Mailbox, mailbox databases under a DAG</p> <p>Backup of Exchange over ReFS not supported</p> |
| Exchange | Exchange 2010 | <p>Physical server</p> <p>On-premises Hyper-V virtual machine</p> <p>Azure Stack</p>                                          | V3, V2                        | <p>Protect (all deployment scenarios): Standalone Exchange server, database under a database availability group (DAG)</p> <p>Recover (all deployment scenarios): Mailbox, mailbox databases under a DAG</p> <p>Backup of Exchange over ReFS not supported</p> |
| Exchange | Exchange 2010 | <p>Windows virtual machine in VMWare (protects workloads running in Windows virtual machine in VMWare)</p> <p>Azure Stack</p> | V3, V2                        | <p>Protect (all deployment scenarios): Standalone Exchange server, database under a database availability group (DAG)</p> <p>Recover (all deployment scenarios): Mailbox, mailbox databases under a DAG</p> <p>Backup of Exchange over ReFS not supported</p> |

| WORKLOAD   | VERSION         | AZURE BACKUP SERVER INSTALLATION                                                                                                                                                                                                                                                 | SUPPORTED AZURE BACKUP SERVER | PROTECTION AND RECOVERY                                                                                                                                                                                                                                                                                                                                       |
|------------|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SharePoint | SharePoint 2016 | <p>Physical server</p> <p>On-premises Hyper-V virtual machine</p> <p>Azure virtual machine (when workload is running as Azure virtual machine)</p> <p>Windows virtual machine in VMWare (protects workloads running in Windows virtual machine in VMWare)</p> <p>Azure Stack</p> | V3, V2                        | <p>Protect (all deployment scenarios): Farm, frontend web server content</p> <p>Recover (all deployment scenarios): Farm, database, web application, file or list item, SharePoint search, frontend web server</p> <p>Note that protecting a SharePoint farm that's using the SQL Server 2012 AlwaysOn feature for the content databases isn't supported.</p> |
| SharePoint | SharePoint 2013 | <p>Physical server</p> <p>On-premises Hyper-V virtual machine</p> <p>Azure Stack</p>                                                                                                                                                                                             | V3, V2                        | <p>Protect (all deployment scenarios): Farm, frontend web server content</p> <p>Recover (all deployment scenarios): Farm, database, web application, file or list item, SharePoint search, frontend web server</p> <p>Note that protecting a SharePoint farm that's using the SQL Server 2012 AlwaysOn feature for the content databases isn't supported.</p> |

| WORKLOAD   | VERSION         | AZURE BACKUP SERVER INSTALLATION                                                                                       | SUPPORTED AZURE BACKUP SERVER | PROTECTION AND RECOVERY                                                                                                                                                                                                                                                                                                                                                          |
|------------|-----------------|------------------------------------------------------------------------------------------------------------------------|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SharePoint | SharePoint 2013 | Azure virtual machine (when workload is running as Azure virtual machine) -<br><br>Azure Stack                         | V3, V2                        | <p>Protect (all deployment scenarios): Farm, SharePoint search, frontend web server content</p> <p>Recover (all deployment scenarios): Farm, database, web application, file or list item, SharePoint search, frontend web server</p> <p>Note that protecting a SharePoint farm that's using the SQL Server 2012 AlwaysOn feature for the content databases isn't supported.</p> |
| SharePoint | SharePoint 2013 | Windows virtual machine in VMWare (protects workloads running in Windows virtual machine in VMWare)<br><br>Azure Stack | V3, V2                        | <p>Protect (all deployment scenarios): Farm, SharePoint search, frontend web server content</p> <p>Recover (all deployment scenarios): Farm, database, web application, file or list item, SharePoint search, frontend web server</p> <p>Note that protecting a SharePoint farm that's using the SQL Server 2012 AlwaysOn feature for the content databases isn't supported.</p> |

| WORKLOAD                                                                    | VERSION             | AZURE BACKUP SERVER INSTALLATION                                                                                       | SUPPORTED AZURE BACKUP SERVER | PROTECTION AND RECOVERY                                                                                                                                                                                                        |
|-----------------------------------------------------------------------------|---------------------|------------------------------------------------------------------------------------------------------------------------|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SharePoint                                                                  | SharePoint 2010     | Physical server<br><br>On-premises Hyper-V virtual machine<br><br>Azure Stack                                          | V3, V2                        | Protect (all deployment scenarios): Farm, SharePoint search, frontend web server content<br><br>Recover (all deployment scenarios): Farm, database, web application, file or list item, SharePoint search, frontend web server |
| SharePoint                                                                  | SharePoint 2010     | Azure virtual machine (when workload is running as Azure virtual machine)<br><br>Azure Stack                           | V3, V2                        | Protect (all deployment scenarios): Farm, SharePoint search, frontend web server content<br><br>Recover (all deployment scenarios): Farm, database, web application, file or list item, SharePoint search, frontend web server |
| SharePoint                                                                  | SharePoint 2010     | Windows virtual machine in VMWare (protects workloads running in Windows virtual machine in VMWare)<br><br>Azure Stack | V3, V2                        | Protect (all deployment scenarios): Farm, SharePoint search, frontend web server content<br><br>Recover (all deployment scenarios): Farm, database, web application, file or list item, SharePoint search, frontend web server |
| Hyper-V host - MABS protection agent on Hyper-V host server, cluster, or VM | Windows Server 2019 | Physical server<br><br>On-premises Hyper-V virtual machine                                                             | V3                            | Protect: Hyper-V computers, cluster shared volumes (CSVs)<br><br>Recover: Virtual machine, Item-level recovery of files and folder, volumes, virtual hard drives                                                               |

| Workload                                                                    | Version                                              | Azure Backup Server Installation                           | Supported Azure Backup Server | Protection and Recovery                                                                                                                                          |
|-----------------------------------------------------------------------------|------------------------------------------------------|------------------------------------------------------------|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hyper-V host - MABS protection agent on Hyper-V host server, cluster, or VM | Windows Server 2016                                  | Physical server<br><br>On-premises Hyper-V virtual machine | V3, V2                        | Protect: Hyper-V computers, cluster shared volumes (CSVs)<br><br>Recover: Virtual machine, Item-level recovery of files and folder, volumes, virtual hard drives |
| Hyper-V host - MABS protection agent on Hyper-V host server, cluster, or VM | Windows Server 2012 R2 - Datacenter and Standard     | Physical server<br><br>On-premises Hyper-V virtual machine | V3, V2                        | Protect: Hyper-V computers, cluster shared volumes (CSVs)<br><br>Recover: Virtual machine, Item-level recovery of files and folder, volumes, virtual hard drives |
| Hyper-V host - MABS protection agent on Hyper-V host server, cluster, or VM | Windows Server 2012 - Datacenter and Standard        | Physical server<br><br>On-premises Hyper-V virtual machine | V3, V2                        | Protect: Hyper-V computers, cluster shared volumes (CSVs)<br><br>Recover: Virtual machine, Item-level recovery of files and folder, volumes, virtual hard drives |
| Hyper-V host - MABS protection agent on Hyper-V host server, cluster, or VM | Windows Server 2008 R2 SP1 - Enterprise and Standard | Physical server<br><br>On-premises Hyper-V virtual machine | V3, V2                        | Protect: Hyper-V computers, cluster shared volumes (CSVs)<br><br>Recover: Virtual machine, Item-level recovery of files and folder, volumes, virtual hard drives |
| Hyper-V host - MABS protection agent on Hyper-V host server, cluster, or VM | Windows Server 2008 SP2                              | Physical server<br><br>On-premises Hyper-V virtual machine | Not supported                 | Protect: Hyper-V computers, cluster shared volumes (CSVs)<br><br>Recover: Virtual machine, Item-level recovery of files and folder, volumes, virtual hard drives |

| WORKLOAD   | VERSION                                                      | AZURE BACKUP SERVER INSTALLATION                              | SUPPORTED AZURE BACKUP SERVER | PROTECTION AND RECOVERY                                                                                                                                                                                                                                                                                                                                           |
|------------|--------------------------------------------------------------|---------------------------------------------------------------|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VMware VMs | VMware vCenter/vSphere ESX/ESXi Licensed Version 5.5/6.0/6.5 | Physical server, On-premises Hyper-V VM, Windows VM in VMWare | V3, V2                        | VMware VMs on cluster-shared volumes (CSVs), NFS, and SAN storage Item-level recovery of files and folders is available only for Windows VMs, VMware vApps are not supported.                                                                                                                                                                                     |
| VMware VMs | VMware vSphere Licensed Version 6.7                          | Physical server, On-premises Hyper-V VM, Windows VM in VMWare | V3                            | VMware VMs on cluster-shared volumes (CSVs), NFS, and SAN storage Item-level recovery of files and folders is available only for Windows VMs, VMware vApps are not supported.                                                                                                                                                                                     |
| Linux      | Linux running as Hyper-V or VMware guest                     | Physical server, On-premises Hyper-V VM, Windows VM in VMWare | V3, V2                        | <p>Hyper-V must be running on Windows Server 2012 R2 or Windows Server 2016. Protect: Entire virtual machine</p> <p>Recover: Entire virtual machine</p> <p>Only file-consistent snapshots are supported.</p> <p>For a complete list of supported Linux distributions and versions, see the article, <a href="#">Linux on distributions endorsed by Azure</a>.</p> |

## Azure ExpressRoute support

You can back up your data over Azure ExpressRoute with public peering (available for old circuits) and Microsoft peering. Backup over private peering is not supported.

With public peering: Ensure access to the following domains/addresses:

- <http://www.msftncsi.com/ncsi.txt>
- [microsoft.com](http://microsoft.com)
- [WindowsAzure.com](http://WindowsAzure.com)
- [microsoftonline.com](http://microsoftonline.com)
- [windows.net](http://windows.net)

With Microsoft peering, please select the following services/regions and relevant community values:

- Azure Active Directory (12076:5060)
- Microsoft Azure Region (according to the location of your Recovery Services vault)
- Azure Storage (according to the location of your Recovery Services vault)

For more details, see the [ExpressRoute routing requirements](#).

**NOTE**

Public Peering is deprecated for new circuits.

## Cluster support

Azure Backup Server can protect data in the following clustered applications:

- File servers
- SQL Server
- Hyper-V - If you protect a Hyper-V cluster using scaled-out MABS protection agent, you can't add secondary protection for the protected Hyper-V workloads.

If you run Hyper-V on Windows Server 2008 R2, make sure to install the update described in KB [975354](#).

If you run Hyper-V on Windows Server 2008 R2 in a cluster configuration, make sure you install SP2 and KB [971394](#).

- Exchange Server - Azure Backup Server can protect non-shared disk clusters for supported Exchange Server versions (cluster-continuous replication), and can also protect Exchange Server configured for local continuous replication.
- SQL Server - Azure Backup Server doesn't support backing up SQL Server databases hosted on cluster-shared volumes (CSVs).

Azure Backup Server can protect cluster workloads that are located in the same domain as the MABS server, and in a child or trusted domain. If you want to protect data sources in untrusted domains or workgroups, use NTLM or certificate authentication for a single server, or certificate authentication only for a cluster.

# Install and upgrade Azure Backup Server

2/25/2020 • 18 minutes to read • [Edit Online](#)

Applies To: MABS v3. (MABS v2 is no longer supported. If you are using a version earlier than MABS v3, please upgrade to the latest version.)

This article explains how to prepare your environment to back up workloads using Microsoft Azure Backup Server (MABS). With Azure Backup Server, you can protect application workloads such as Hyper-V VMs, Microsoft SQL Server, SharePoint Server, Microsoft Exchange, and Windows clients from a single console.

## NOTE

Azure Backup Server can now protect VMware VMs and provides improved security capabilities. Install the product as explained in the sections below and the latest Azure Backup Agent. To learn more about backing up VMware servers with Azure Backup Server, see the article, [Use Azure Backup Server to back up a VMware server](#). To learn about security capabilities, refer to [Azure backup security features documentation](#).

MABS deployed in an Azure VM can back up VMs in Azure but they should be in same domain to enable backup operation. The process to back an Azure VM remains same as backing up VMs on premises, however deploying MABS in Azure has some limitations. For more information on limitation, see [DPM as an Azure virtual machine](#)

## NOTE

Azure has two deployment models for creating and working with resources: [Resource Manager and classic](#). This article provides the information and procedures for restoring VMs deployed using the Resource Manager model.

Azure Backup Server inherits much of the workload backup functionality from Data Protection Manager (DPM). This article links to DPM documentation to explain some of the shared functionality. Though Azure Backup Server shares much of the same functionality as DPM, Azure Backup Server does not back up to tape, nor does it integrate with System Center.

## Choose an installation platform

The first step towards getting the Azure Backup Server up and running is to set up a Windows Server. Your server can be in Azure or on-premises.

### Using a server in Azure

When choosing a server for running Azure Backup Server, it is recommended you start with a gallery image of Windows Server 2016 Datacenter or Windows Server 2019 Datacenter. The article, [Create your first Windows virtual machine in the Azure portal](#), provides a tutorial for getting started with the recommended virtual machine in Azure, even if you've never used Azure before. The recommended minimum requirements for the server virtual machine (VM) should be: Standard\_A4\_v2 with four cores and 8-GB RAM.

Protecting workloads with Azure Backup Server has many nuances. The article, [Install DPM as an Azure virtual machine](#), helps explain these nuances. Before deploying the machine, read this article completely.

### Using an on-premises server

If you do not want to run the base server in Azure, you can run the server on a Hyper-V VM, a VMware VM, or a

physical host. The recommended minimum requirements for the server hardware are two cores and 8-GB RAM. The supported operating systems are listed in the following table:

| OPERATING SYSTEM                   | PLATFORM | SKU                              |
|------------------------------------|----------|----------------------------------|
| Windows Server 2019                | 64 bit   | Standard, Datacenter, Essentials |
| Windows Server 2016 and latest SPs | 64 bit   | Standard, Datacenter, Essentials |

You can deduplicate the DPM storage using Windows Server Deduplication. Learn more about how [DPM and deduplication](#) work together when deployed in Hyper-V VMs.

#### NOTE

Azure Backup Server is designed to run on a dedicated, single-purpose server. You cannot install Azure Backup Server on:

- A computer running as a domain controller
- A computer on which the Application Server role is installed
- A computer that is a System Center Operations Manager management server
- A computer on which Exchange Server is running
- A computer that is a node of a cluster

Installing Azure Backup Server is not supported on Windows Server Core or Microsoft Hyper-V Server.

Always join Azure Backup Server to a domain. If you plan to move the server to a different domain, install Azure Backup Server first, then join the server to the new domain. Moving an existing Azure Backup Server machine to a new domain after deployment is *not supported*.

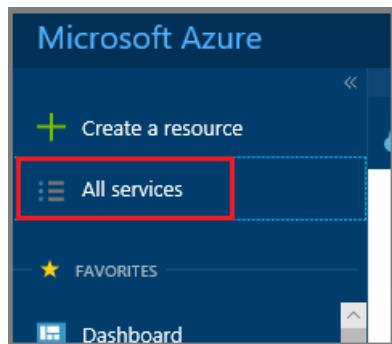
Whether you send backup data to Azure, or keep it locally, Azure Backup Server must be registered with a Recovery Services vault.

## Create a Recovery Services vault

A Recovery Services vault is an entity that stores backups and recovery points created over time. The Recovery Services vault also contains the backup policies that are associated with the protected virtual machines.

To create a Recovery Services vault, follow these steps.

1. Sign in to your subscription in the [Azure portal](#).
2. On the left menu, select **All services**.



3. In the **All services** dialog box, enter *Recovery Services*. The list of resources filters according to your input. In the list of resources, select **Recovery Services vaults**.

The screenshot shows the Azure portal interface. At the top, there's a search bar with 'recovery ser' typed into it. Below the search bar, a navigation bar has 'All services' selected. Underneath, a section titled 'Recovery Services vaults' is shown, with the subtitle 'Keywords: Disaster recovery'. There's also a star icon for favoriting.

The list of Recovery Services vaults in the subscription appears.

4. On the **Recovery Services vaults** dashboard, select **Add**.

This screenshot shows the 'Recovery Services vaults' dashboard. The 'Add' button, which is red with a white plus sign, is highlighted with a red box. Other buttons like 'Edit columns', 'Refresh', and 'Assign Tags' are visible at the bottom of the dashboard area.

The **Recovery Services vault** dialog box opens. Provide values for the **Name**, **Subscription**, **Resource group**, and **Location**.

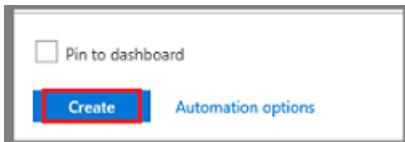
This screenshot shows the 'Recovery Services vault' dialog box. It contains fields for Name, Subscription, Resource group, and Location. The 'Name' field is labeled with a red asterisk and has a placeholder 'Enter the name'. The 'Subscription' field shows '<subscription>' with a dropdown arrow. The 'Resource group' section has two options: 'Create new' (radio button) and 'Use existing' (radio button, which is selected). The 'Location' field shows 'West US' with a dropdown arrow. At the bottom, there's a checkbox for 'Pin to dashboard' and two buttons: 'Create' (blue) and 'Automation options'.

- **Name:** Enter a friendly name to identify the vault. The name must be unique to the Azure subscription. Specify a name that has at least 2 but not more than 50 characters. The name must start with a letter and consist only of letters, numbers, and hyphens.
- **Subscription:** Choose the subscription to use. If you're a member of only one subscription, you'll see that name. If you're not sure which subscription to use, use the default (suggested) subscription. There are multiple choices only if your work or school account is associated with more than one Azure subscription.
- **Resource group:** Use an existing resource group or create a new one. To see the list of available resource groups in your subscription, select **Use existing**, and then select a resource from the drop-down list. To create a new resource group, select **Create new** and enter the name. For more information about resource groups, see [Azure Resource Manager overview](#).
- **Location:** Select the geographic region for the vault. To create a vault to protect virtual machines, the vault *must* be in the same region as the virtual machines.

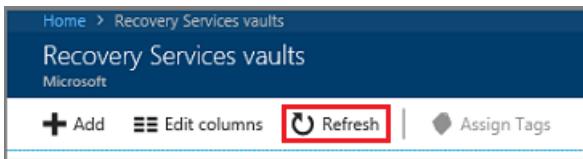
### IMPORTANT

If you're not sure of the location of your VM, close the dialog box. Go to the list of virtual machines in the portal. If you have virtual machines in several regions, create a Recovery Services vault in each region. Create the vault in the first location, before you create the vault for another location. There's no need to specify storage accounts to store the backup data. The Recovery Services vault and Azure Backup handle that automatically.

- When you're ready to create the Recovery Services vault, select **Create**.



It can take a while to create the Recovery Services vault. Monitor the status notifications in the **Notifications** area at the upper-right corner of the portal. After your vault is created, it's visible in the list of Recovery Services vaults. If you don't see your vault, select **Refresh**.



### Set Storage Replication

The storage replication option allows you to choose between geo-redundant storage and locally redundant storage. By default, Recovery Services vaults use geo-redundant storage. If this vault is your primary vault, leave the storage option set to geo-redundant storage. Choose locally redundant storage if you want a cheaper option that isn't quite as durable. Read more about [geo-redundant](#) and [locally redundant](#) storage options in the [Azure Storage replication overview](#).

To edit the storage replication setting:

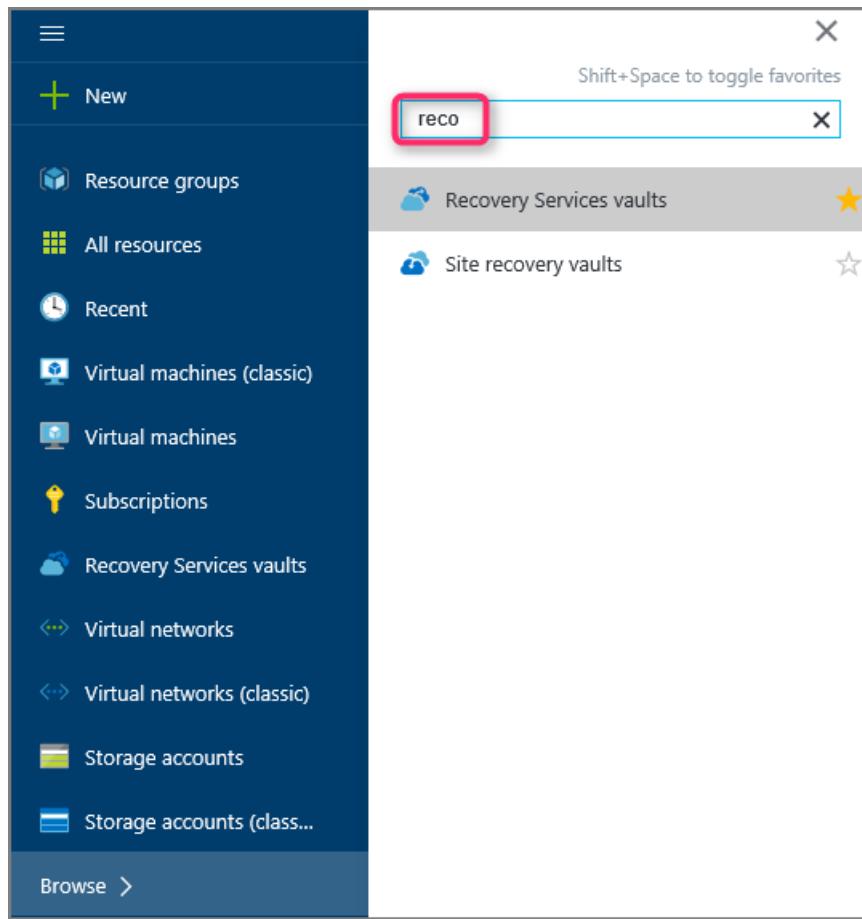
- From the **Recovery Services vaults** blade, click the new vault. Under the **Settings** section, click **Properties**.
- In **Properties**, under **Backup Configuration**, click **Update**.
- Select the storage replication type, and click **Save**.

The screenshot shows the Azure Recovery Services vault Properties page. On the left, there's a navigation pane with links like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (with Properties highlighted), Locks, Automation script, Getting started (with Backup and Site Recovery), Protected items (with Backup items and Replicated items), Manage (with Backup policies and Backup infrastructure), and a large 'Update' button. On the right, there's a 'Backup Configuration' section with tabs for DemoVault and DemoVault - Properties. It shows the vault is Active, located in Central India, and part of the mayurssg01 resource group. It also lists Subscription Name, Subscription ID, and Diagnostic settings. Under the 'Backup' section, 'Backup Configuration' is selected (highlighted with a red box) and has an 'Update' link. Other options like Security Settings and another 'Update' link are also present.

## Software package

### Downloading the software package

1. Sign in to the [Azure portal](#).
2. If you already have a Recovery Services vault open, proceed to step 3. If you do not have a Recovery Services vault open, but are in the Azure portal, on the main menu, click **Browse**.
  - In the list of resources, type **Recovery Services**.
  - As you begin typing, the list will filter based on your input. When you see **Recovery Services vaults**, click it.



The list of Recovery Services vaults appears.

- From the list of Recovery Services vaults, select a vault.

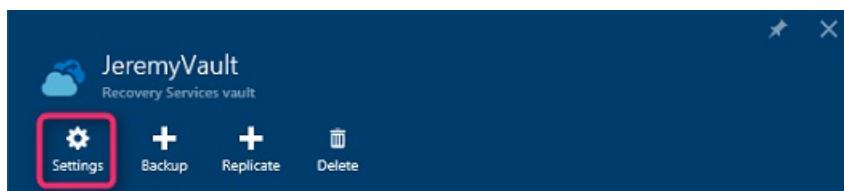
The selected vault dashboard opens.

The screenshot shows the Azure Recovery Services vault interface for 'JeremyVault'. At the top, there's a navigation bar with icons for Settings, Backup, Replicate, and Delete. Below this is a section titled 'Essentials' with a 'Monitoring' card showing 'Site Recovery Health' status (Unhealthy services: 0, Events: 0). There are also 'Backup' and 'Site Recovery' cards, each with three sub-sections and a 'Add tiles' button.

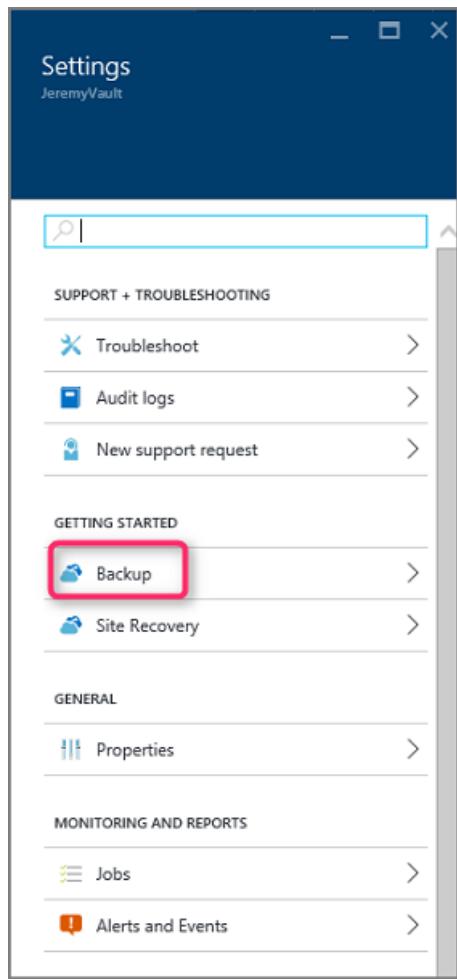
| Backup                 |                         |                      |
|------------------------|-------------------------|----------------------|
| Backup Items           | Backup Jobs             | Backup Usage         |
| Azure Virtual Machines | Azure virtual mach... 4 | Cloud - LRS 0 B      |
| File-Folders           |                         | Cloud - GRS 40.96 GB |
|                        |                         |                      |

| Site Recovery    |                |                                                  |
|------------------|----------------|--------------------------------------------------|
| Replicated items | Recovery plans | Site Recovery jobs                               |
| 0                | 0              | Failed 0<br>Waiting for input 0<br>In progress 0 |
|                  |                |                                                  |

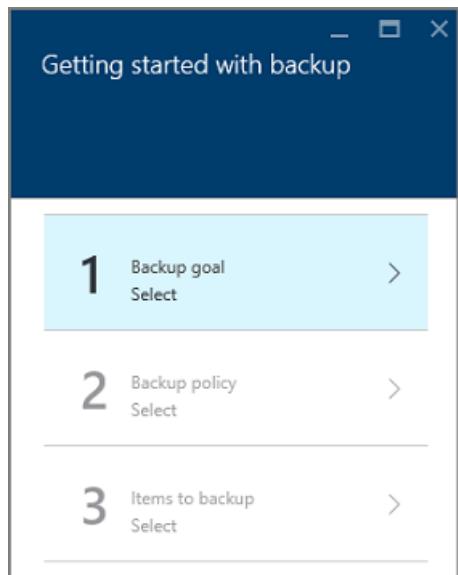
3. The **Settings** blade opens up by default. If it is closed, click on **Settings** to open the settings blade.



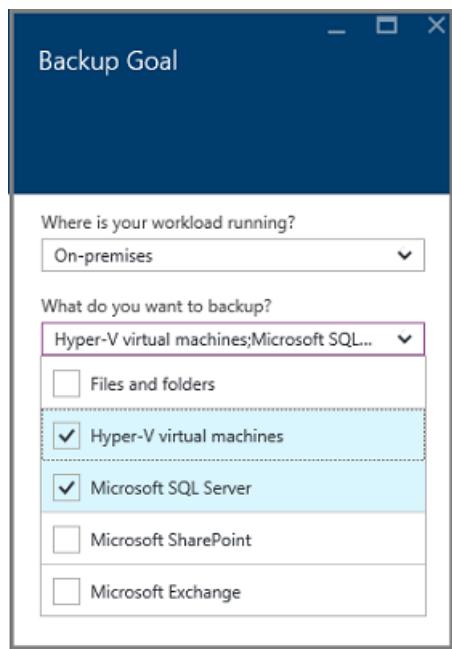
4. Click **Backup** to open the Getting Started wizard.



In the **Getting Started with backup** blade that opens, **Backup Goals** will be auto-selected.



5. In the **Backup Goal** blade, from the **Where is your workload running** menu, select **On-premises**.

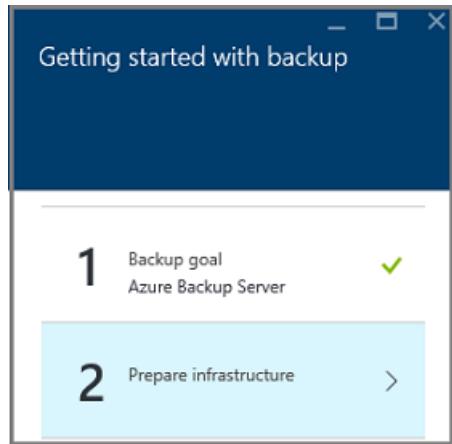


From the **What do you want to back up?** drop-down menu, select the workloads you want to protect using Azure Backup Server, and then click **OK**.

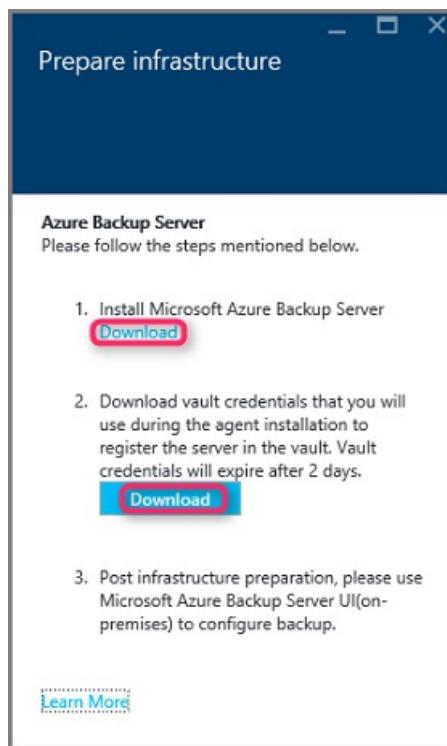
The **Getting Started with backup** wizard switches the **Prepare infrastructure** option to back up workloads to Azure.

**NOTE**

If you only want to back up files and folders, we recommend using the Azure Backup agent and following the guidance in the article, [First look: back up files and folders](#). If you are going to protect more than files and folders, or you are planning to expand the protection needs in the future, select those workloads.



6. In the **Prepare infrastructure** blade that opens, click the **Download** links for Install Azure Backup Server and Download vault credentials. You use the vault credentials during registration of Azure Backup Server to the recovery services vault. The links take you to the Download Center where the software package can be downloaded.



7. Select all the files and click **Next**. Download all the files coming in from the Microsoft Azure Backup download page, and place all the files in the same folder.

This screenshot shows a download interface. On the left, a table lists files with checkboxes and sizes. On the right, a summary shows the total size and a 'Next' button.

| <input checked="" type="checkbox"/> File Name                           | Size     |
|-------------------------------------------------------------------------|----------|
| <input checked="" type="checkbox"/> MicrosoftAzureBackupInstaller.exe   | 484 KB   |
| <input checked="" type="checkbox"/> MicrosoftAzureBackupInstaller-1.bin | 701.4 MB |
| <input checked="" type="checkbox"/> MicrosoftAzureBackupInstaller-2.bin | 701.9 MB |
| <input checked="" type="checkbox"/> MicrosoftAzureBackupInstaller-3.bin | 701.9 MB |
| <input checked="" type="checkbox"/> MicrosoftAzureBackupInstaller-4.bin | 701.9 MB |
| <input checked="" type="checkbox"/> MicrosoftAzureBackupInstaller-5.bin | 446.1 MB |

Download Summary:  
1. MicrosoftAzureBackupInstaller.exe  
2. MicrosoftAzureBackupInstaller-1.bin  
3. MicrosoftAzureBackupInstaller-2.bin  
4. MicrosoftAzureBackupInstaller-3.bin  
5. MicrosoftAzureBackupInstaller-4.bin  
6. MicrosoftAzureBackupInstaller-5.bin

Total Size: 3.2 GB

**Next**

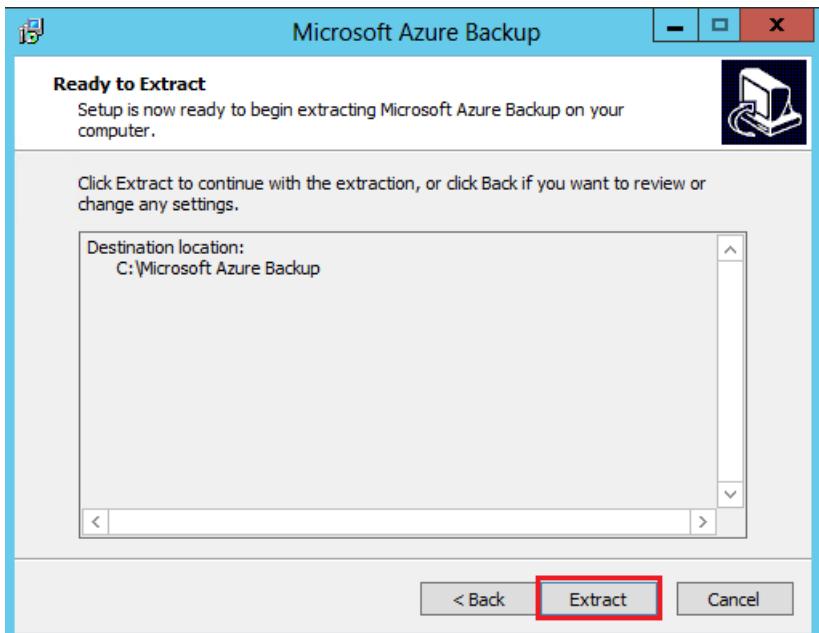
Since the download size of all the files together is > 3G, on a 10-Mbps download link it may take up to 60 minutes for the download to complete.

### Extracting the software package

After you've downloaded all the files, click **MicrosoftAzureBackupInstaller.exe**. This will start the **Microsoft Azure Backup Setup Wizard** to extract the setup files to a location specified by you. Continue through the wizard and click on the **Extract** button to begin the extraction process.

#### WARNING

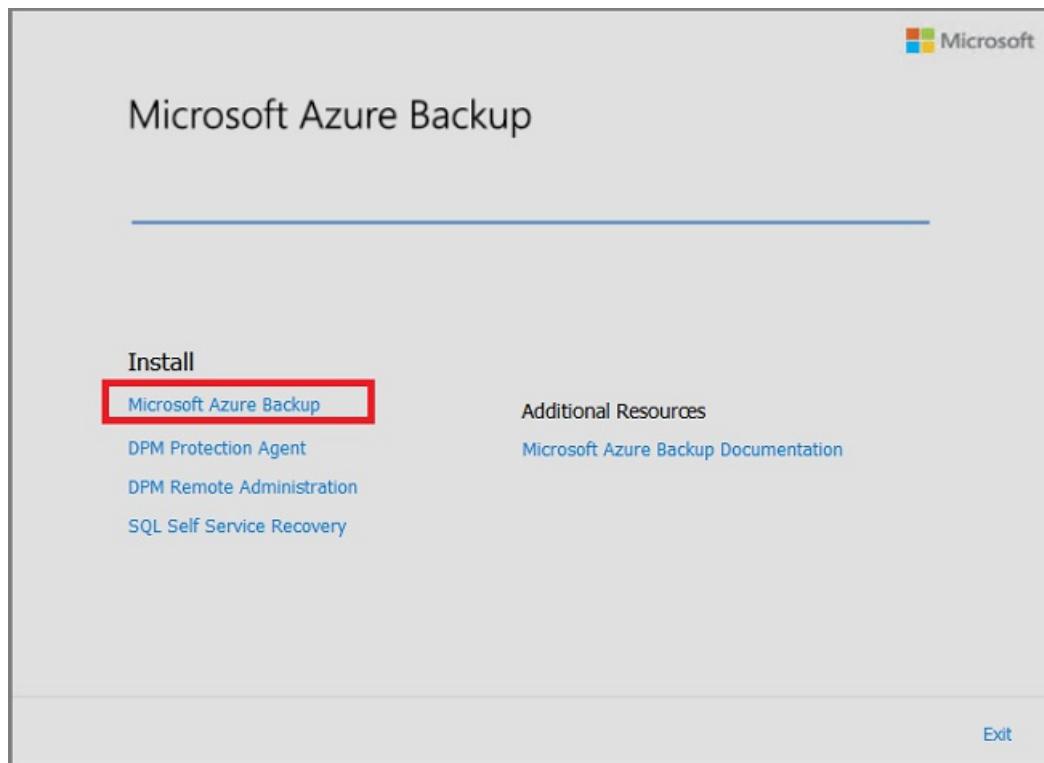
At least 4 GB of free space is required to extract the setup files.



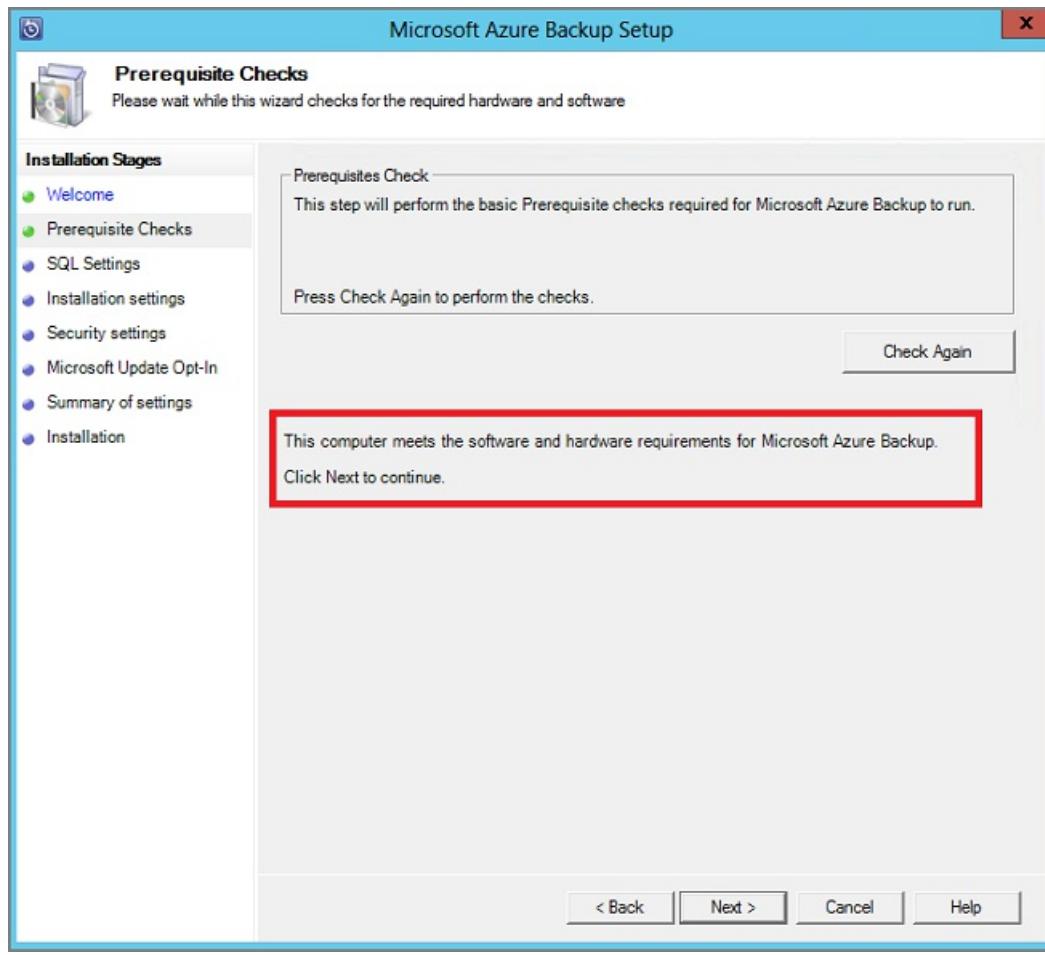
Once the extraction process complete, check the box to launch the freshly extracted *setup.exe* to begin installing Microsoft Azure Backup Server and click on the **Finish** button.

### Installing the software package

1. Click **Microsoft Azure Backup** to launch the setup wizard.



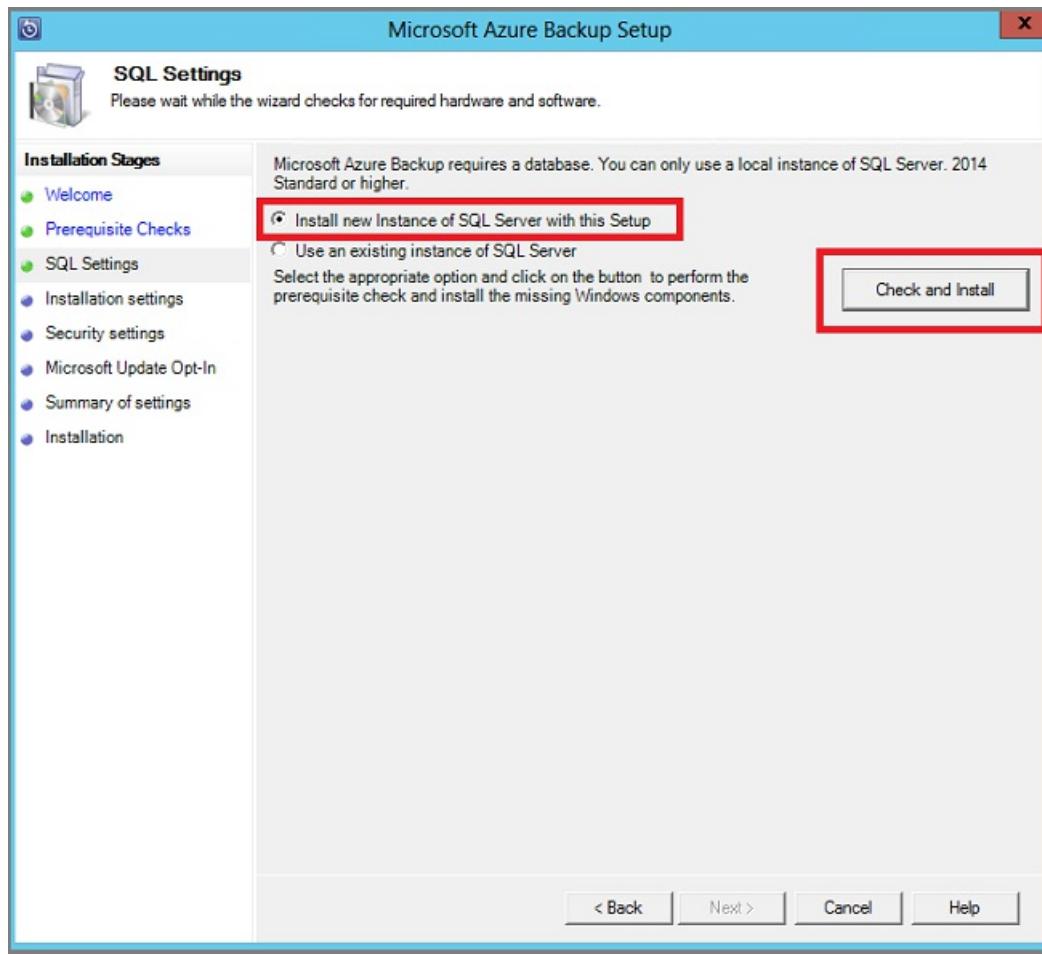
2. On the Welcome screen, click the **Next** button. This takes you to the *Prerequisite Checks* section. On this screen, click **Check** to determine if the hardware and software prerequisites for Azure Backup Server have been met. If all prerequisites are met successfully, you will see a message indicating that the machine meets the requirements. Click on the **Next** button.



3. The Azure Backup Server installation package comes bundled with the appropriate SQL Server binaries needed. When starting a new Azure Backup Server installation, pick the option **Install new Instance of SQL Server with this Setup** and click the **Check and Install** button. Once the prerequisites are successfully installed, click **Next**.

#### NOTE

If you wish to use your own SQL server, the supported SQL Server versions are SQL Server 2014 SP1 or higher, 2016 and 2017. All SQL Server versions should be Standard or Enterprise 64-bit. Azure Backup Server will not work with a remote SQL Server instance. The instance being used by Azure Backup Server needs to be local. If you are using an existing SQL server for MABS, the MABS setup only supports the use of *named instances* of SQL server.



If a failure occurs with a recommendation to restart the machine, do so and click **Check Again**. If there are any SQL configuration issues, reconfigure SQL as per the SQL guidelines and retry to install/upgrade MABS using the existing instance of SQL.

### Manual configuration

When you use your own instance of SQL, make sure you add `builtin\Administrators` to `sysadmin` role to master DB.

### SSRS Configuration with SQL 2017

When you are using your own instance of SQL 2017, you need to manually configure SSRS. After SSRS configuration, ensure that `IsInitialized` property of SSRS is set to `True`. When this is set to True, MABS assumes that SSRS is already configured and will skip the SSRS configuration.

Use the following values for SSRS configuration:

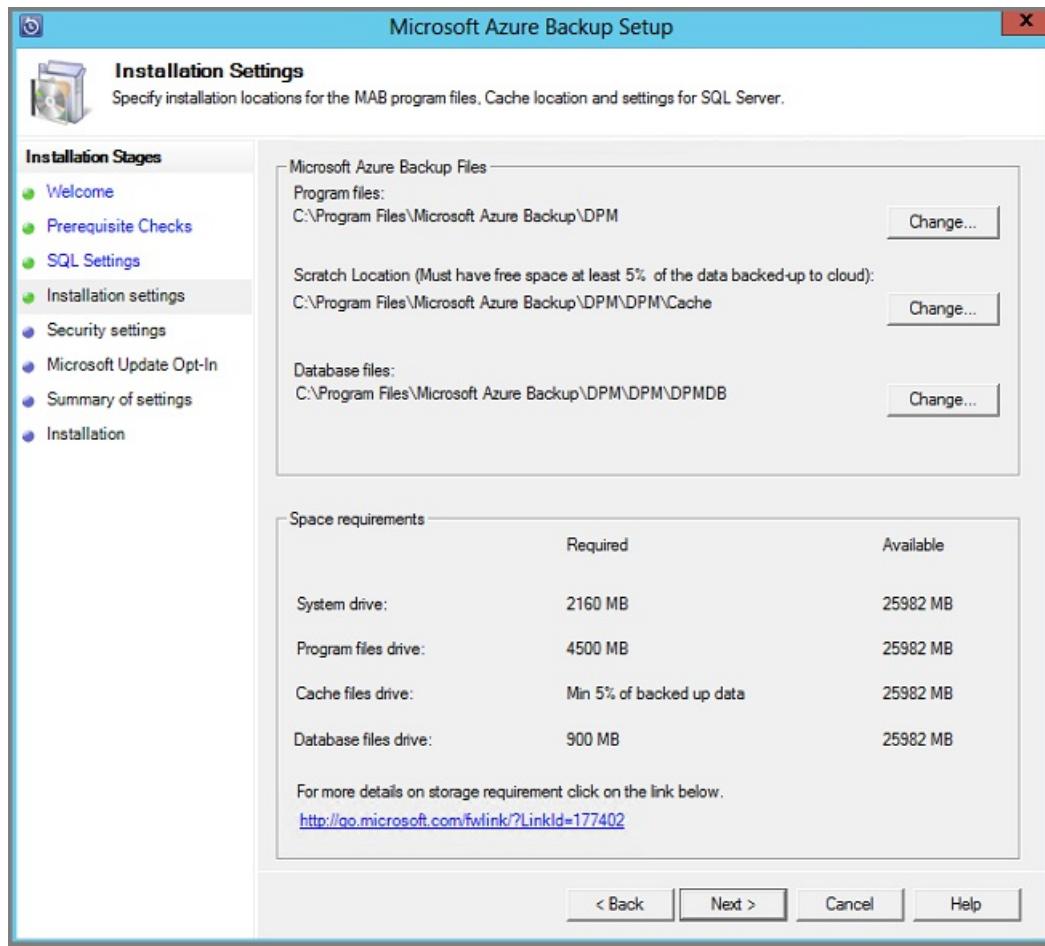
- Service Account: 'Use built-in account' should be Network Service
- Web Service URL: 'Virtual Directory' should be `ReportServer_<SQLInstanceName>`
- Database: `DatabaseName` should be `ReportServer$<SQLInstanceName>`
- Web Portal URL: 'Virtual Directory' should be `Reports_<SQLInstanceName>`

[Learn more about SSRS configuration.](#)

#### NOTE

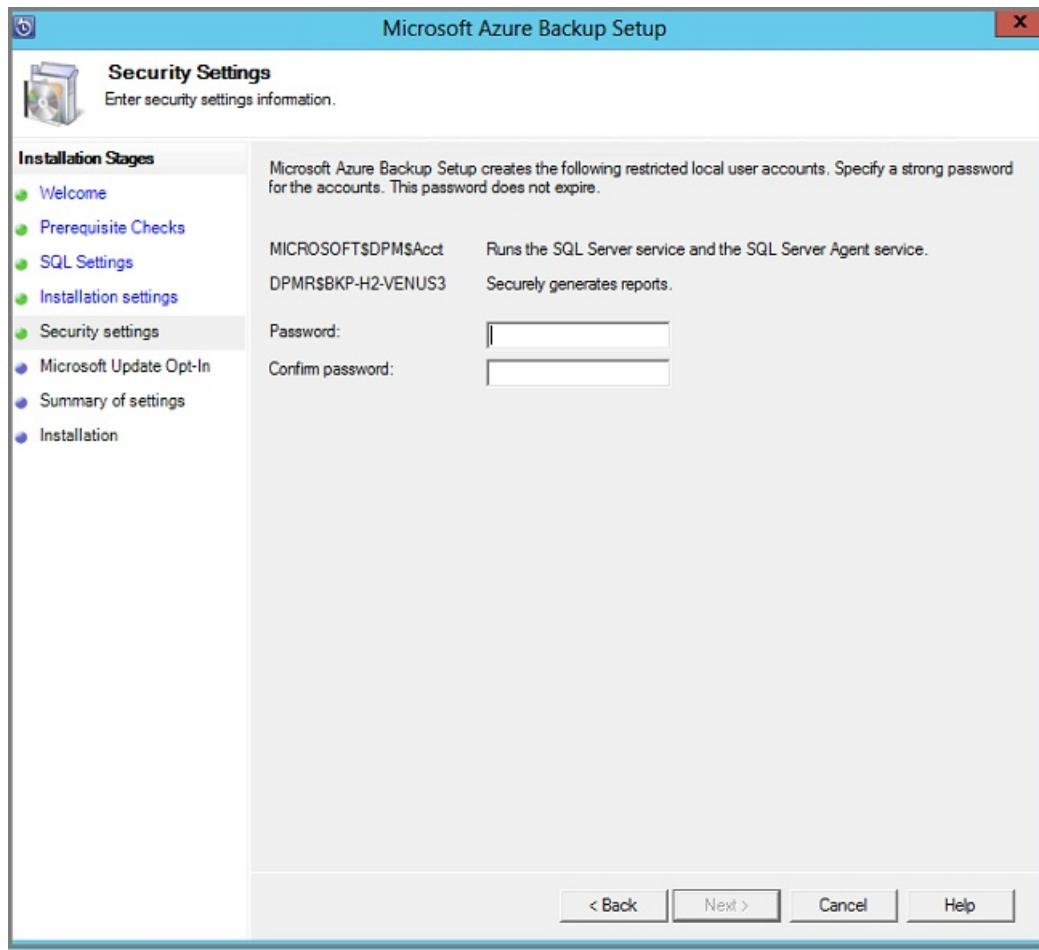
Licensing for SQL Server used as the database for MABS is governed by [Microsoft Online Services Terms \(OST\)](#). According to OST, SQL Server bundled with MABS can be used only as the database for MABS.

4. Provide a location for the installation of Microsoft Azure Backup server files and click **Next**.



The scratch location is a requirement for back up to Azure. Ensure the scratch location is at least 5% of the data planned to be backed up to the cloud. For disk protection, separate disks need to be configured once the installation completes. For more information regarding storage pools, see [Configure storage pools and disk storage](#).

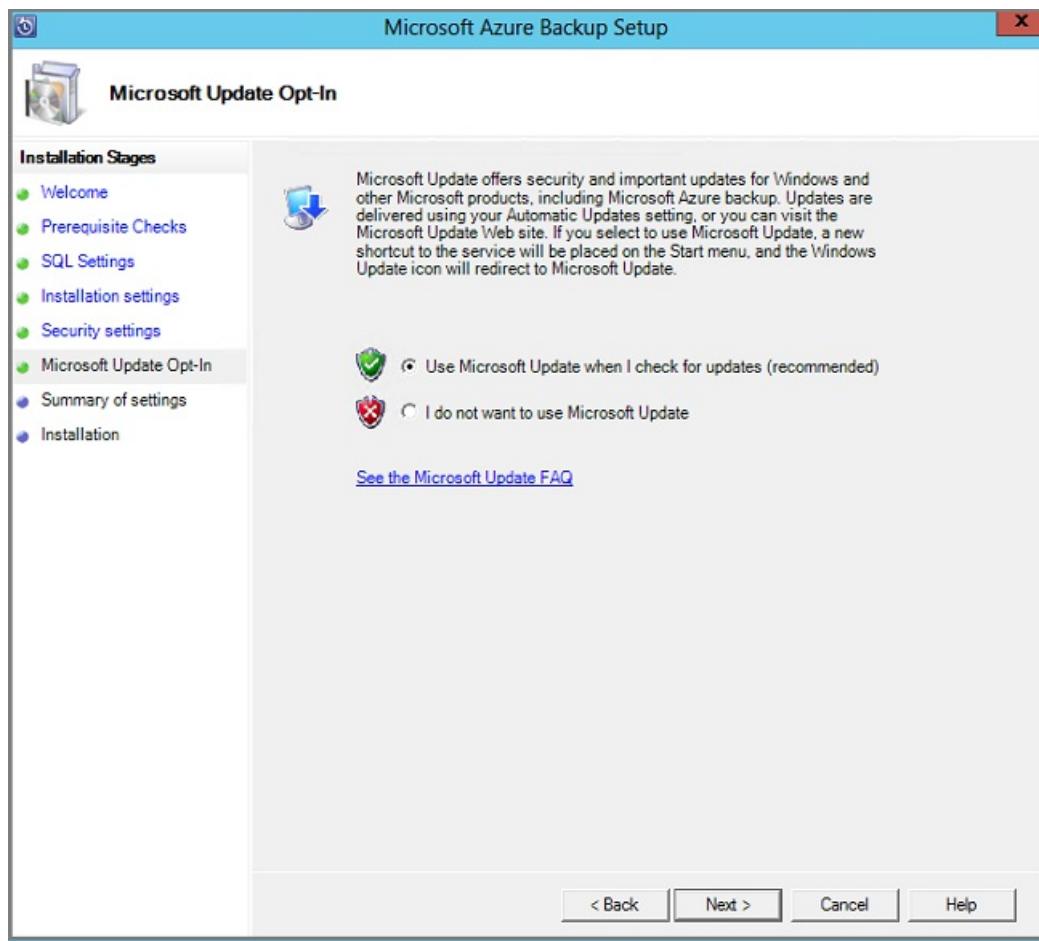
5. Provide a strong password for restricted local user accounts and click **Next**.



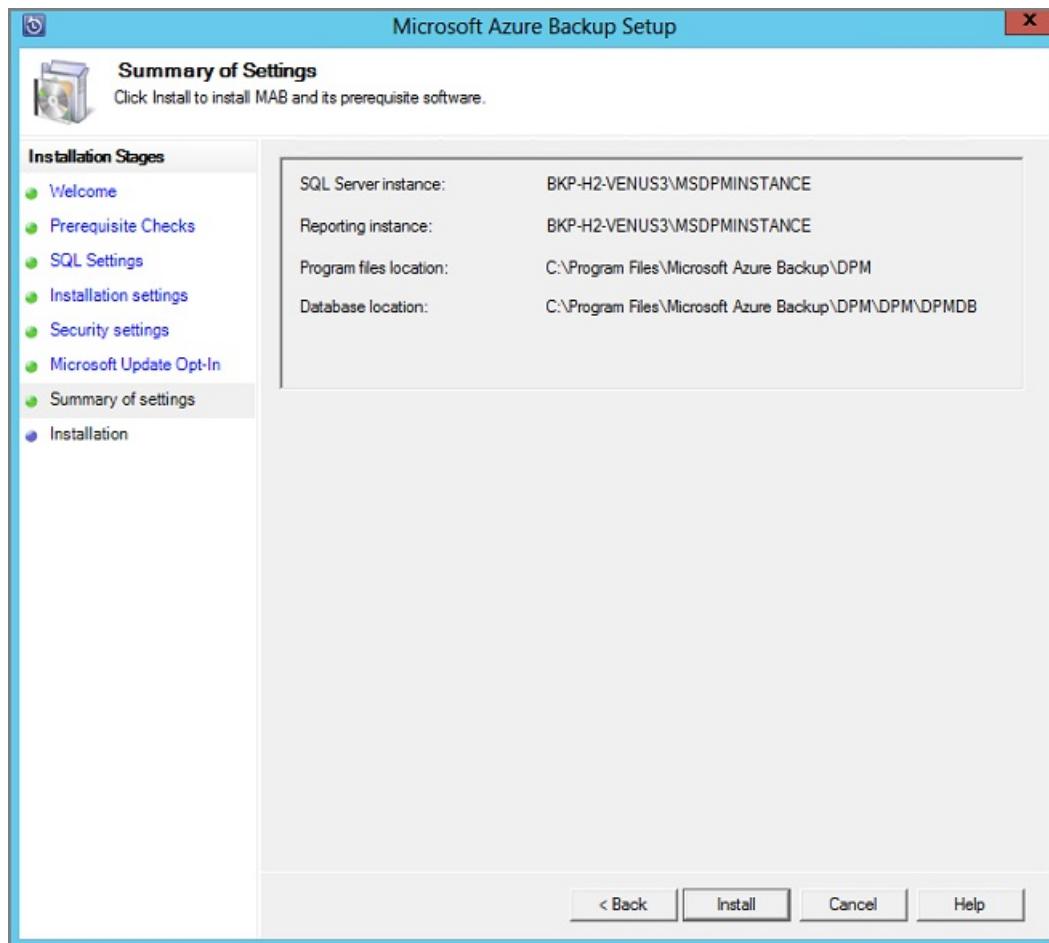
6. Select whether you want to use *Microsoft Update* to check for updates and click **Next**.

**NOTE**

We recommend having Windows Update redirect to Microsoft Update, which offers security and important updates for Windows and other products like Microsoft Azure Backup Server.



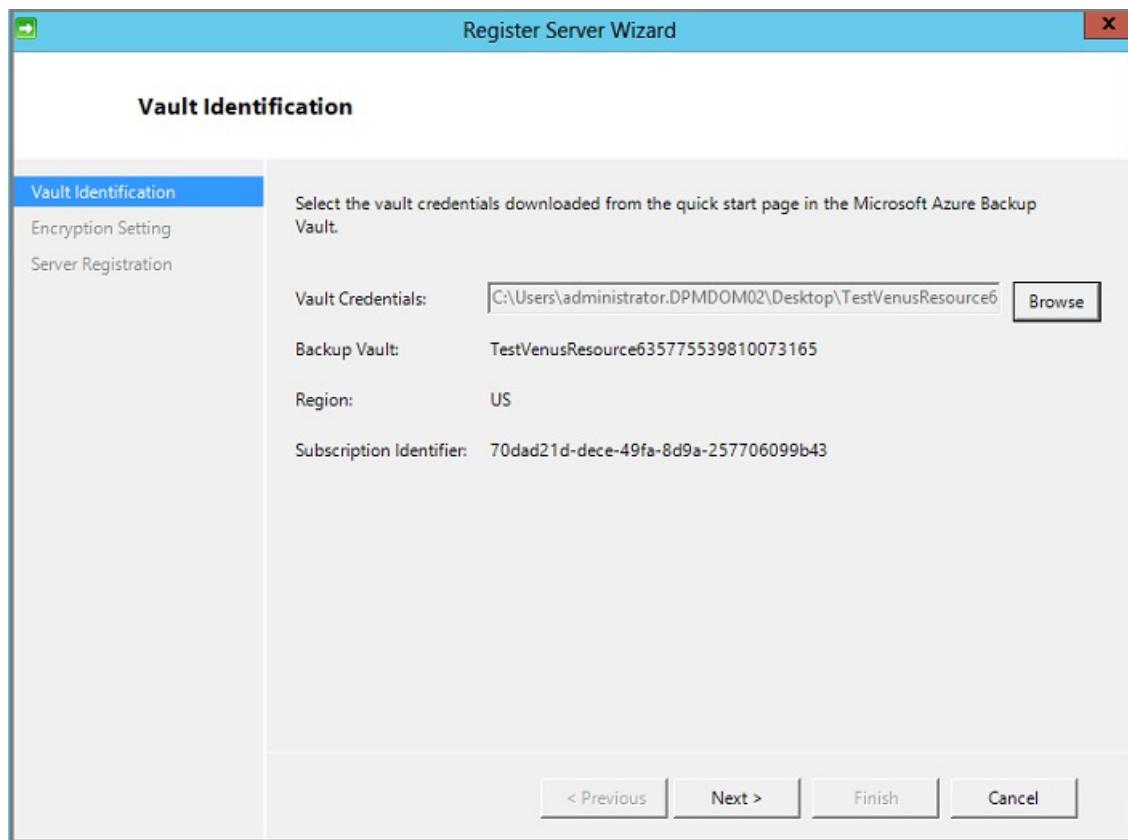
7. Review the *Summary of Settings* and click **Install**.



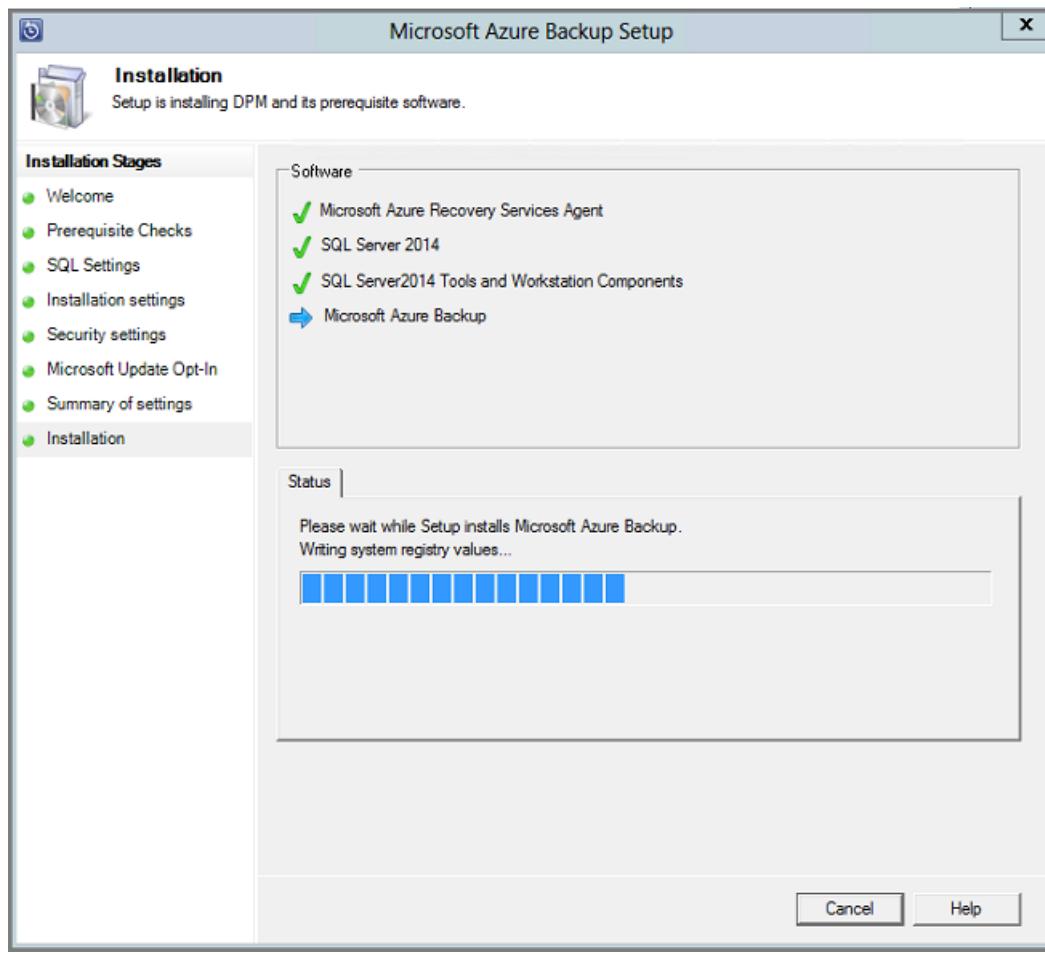
8. The installation happens in phases. In the first phase, the Microsoft Azure Recovery Services Agent is installed on the server. The wizard also checks for Internet connectivity. If Internet connectivity is available

you can proceed with installation, if not, you need to provide proxy details to connect to the Internet.

The next step is to configure the Microsoft Azure Recovery Services Agent. As a part of the configuration, you will have to provide your vault credentials to register the machine to the recovery services vault. You will also provide a passphrase to encrypt/decrypt the data sent between Azure and your premises. You can automatically generate a passphrase or provide your own minimum 16-character passphrase. Continue with the wizard until the agent has been configured.



- Once registration of the Microsoft Azure Backup server successfully completes, the overall setup wizard proceeds to the installation and configuration of SQL Server and the Azure Backup Server components. Once the SQL Server component installation completes, the Azure Backup Server components are installed.



When the installation step has completed, the product's desktop icons will have been created as well. Just double-click the icon to launch the product.

### Add backup storage

The first backup copy is kept on storage attached to the Azure Backup Server machine. For more information about adding disks, see [Configure storage pools and disk storage](#).

#### NOTE

You need to add backup storage even if you plan to send data to Azure. In the current architecture of Azure Backup Server, the Azure Backup vault holds the *second* copy of the data while the local storage holds the first (and mandatory) backup copy.

### Install and update the Data Protection Manager protection agent

MABS uses the System Center Data Protection Manager protection agent. [Here are the steps](#) to install the Protection Agent on your Protection Servers.

The following sections describe how to update protection agents for client computers.

1. In the Backup Server Administrator Console, select **Management > Agents**.
2. In the display pane, select the client computers for which you want to update the protection agent.

#### NOTE

The **Agent Updates** column indicates when a protection agent update is available for each protected computer. In the **Actions** pane, the **Update** action is available only when a protected computer is selected and updates are available.

3. To install updated protection agents on the selected computers, in the **Actions** pane, select **Update**.

4. For a client computer that is not connected to the network, until the computer is connected to the network, the **Agent Status** column shows a status of **Update Pending**.

After a client computer is connected to the network, the **Agent Updates** column for the client computer shows a status of **Updating**.

## Move MABS to a new server

Here are the steps if you need to move MABS to a new server, while retaining the storage. This can be done only if all the data is on Modern Backup Storage.

### IMPORTANT

- The new server name must be the same name as the original Azure Backup Server instance. You can't change the name of the new Azure Backup Server instance if you want to use the previous storage pool and MABS Database (DPMDB) to retain recovery points.
- You must have a backup of the MABS Database (DPMDB). You'll need to restore the database.

1. In the display pane, select the client computers for which you want to update the protection agent.
2. Shut down the original Azure backup server or take it off the wire.
3. Reset the machine account in active directory.
4. Install Server 2016 on new machine and name it the same machine name as the original Azure Backup server.
5. Join the Domain
6. Install Azure Backup server V3 or later (move MABS Storage pool disks from old server and import)
7. Restore the DPMDB taken in step 1.
8. Attach the storage from the original backup server to the new server.
9. From SQL Restore the DPMDB
10. From admin command line on new server cd to Microsoft Azure Backup install location and bin folder  
Path example: C:\windows\system32>cd "c:\Program Files\Microsoft Azure Backup\DPM\DPMSync\bin"
11. To Azure backup, Run DPMSYNC -SYNC

If you have added NEW disks to the DPM Storage pool instead of moving the old ones, then run  
DPMSYNC -Reallocatereplica

## Network connectivity

Azure Backup Server requires connectivity to the Azure Backup service for the product to work successfully. To validate whether the machine has the connectivity to Azure, use the `Get-DPMCcloudConnection` cmdlet in the Azure Backup Server PowerShell console. If the output of the cmdlet is TRUE, then connectivity exists, else there is no connectivity.

At the same time, the Azure subscription needs to be in a healthy state. To find out the state of your subscription and to manage it, sign in to the [subscription portal](#).

Once you know the state of the Azure connectivity and of the Azure subscription, you can use the table below to

find out the impact on the backup/restore functionality offered.

| CONNECTIVITY STATE          | AZURE SUBSCRIPTION | BACK UP TO AZURE | BACK UP TO DISK | RESTORE FROM AZURE                        | RESTORE FROM DISK |
|-----------------------------|--------------------|------------------|-----------------|-------------------------------------------|-------------------|
| Connected                   | Active             | Allowed          | Allowed         | Allowed                                   | Allowed           |
| Connected                   | Expired            | Stopped          | Stopped         | Allowed                                   | Allowed           |
| Connected                   | Deprovisioned      | Stopped          | Stopped         | Stopped and Azure recovery points deleted | Stopped           |
| Lost connectivity > 15 days | Active             | Stopped          | Stopped         | Allowed                                   | Allowed           |
| Lost connectivity > 15 days | Expired            | Stopped          | Stopped         | Allowed                                   | Allowed           |
| Lost connectivity > 15 days | Deprovisioned      | Stopped          | Stopped         | Stopped and Azure recovery points deleted | Stopped           |

### Recovering from loss of connectivity

If you have a firewall or a proxy that is preventing access to Azure, you need to allow the following domain addresses in the firewall/proxy profile:

- `http://www.msftncsi.com/ncsi.txt`
- \*.Microsoft.com
- \*.WindowsAzure.com
- \*.microsoftonline.com
- \*.windows.net

If you are using ExpressRoute Microsoft peering, please select the following services/regions:

- Azure Active Directory (12076:5060)
- Microsoft Azure Region (as per the location of your Recovery Services vault)
- Azure Storage (as per the location of your Recovery Services vault)

For more details, visit [ExpressRoute routing requirements](#).

Once connectivity to Azure has been restored to the Azure Backup Server machine, the operations that can be performed are determined by the Azure subscription state. The table above has details about the operations allowed once the machine is "Connected".

### Handling subscription states

It is possible to take an Azure subscription from an *Expired* or *Deprovisioned* state to the *Active* state. However, this has some implications on the product behavior while the state is not *Active*:

- A *Deprovisioned* subscription loses functionality for the period that it is deprovisioned. On turning *Active*, the product functionality of backup/restore is revived. The backup data on the local disk also can be retrieved if it was kept with a sufficiently large retention period. However, the backup data in Azure is irretrievably lost once the subscription enters the *Deprovisioned* state.
- An *Expired* subscription only loses functionality for until it has been made *Active* again. Any backups scheduled for the period that the subscription was *Expired* will not run.

# Upgrade MABS

Use the following procedures to upgrade MABS.

## Upgrade from MABS V2 to V3

### NOTE

MABS V2 is not a prerequisite for installing MABS V3. However, you can upgrade to MABS V3 only from MABS V2.

Use the following steps to upgrade MABS:

1. To upgrade from MABS V2 to MABS V3, upgrade your OS to Windows Server 2016 or Windows Server 2019 if needed.
2. Upgrade your server. The steps are similar to [installation](#). However, for SQL settings, you will get an option to upgrade your SQL instance to SQL 2017, or to use your own instance of SQL server 2017.

### NOTE

Do not exit while your SQL instance is being upgraded, exiting will uninstall the SQL reporting instance and hence an attempt to re-upgrade MABS will fail.

### IMPORTANT

As part of SQL 2017 upgrade, we backup the SQL encryption keys and uninstall the reporting services. After SQL server upgrade, reporting service(14.0.6827.4788) is installed & encryption keys are restored.

When configuring SQL 2017 manually, refer to *SSRS configuration with SQL 2017* section under Install instructions.

3. Update the protection agents on the protected servers.
4. Backups should continue without the need to restart your production servers.
5. You can begin protecting your data now. If you are upgrading to Modern Backup Storage, while protecting, you can also choose the volumes you wish to store the backups in, and check for under provisioned space. [Learn more](#).

## Troubleshooting

If Microsoft Azure Backup server fails with errors during the setup phase (or backup or restore), refer to this [error codes document](#) for more information. You can also refer to [Azure Backup related FAQs](#)

## Next steps

You can get detailed information here about [preparing your environment for DPM](#). It also contains information about supported configurations on which Azure Backup Server can be deployed and used. You can use a series of [PowerShell cmdlet](#) for performing various operations.

You can use these articles to gain a deeper understanding of workload protection using Microsoft Azure Backup server.

- [SQL Server backup](#)
- [SharePoint server backup](#)
- [Alternate server backup](#)



# Add storage to Azure Backup Server

11/18/2019 • 4 minutes to read • [Edit Online](#)

Azure Backup Server V2 and later supports Modern Backup Storage that offers storage savings of 50 percent, backups that are three times faster, and more efficient storage. It also offers workload-aware storage.

## NOTE

To use Modern Backup Storage, you must run Backup Server V2 or V3 on Windows Server 2016 or V3 on Windows Server 2019. If you run Backup Server V2 on an earlier version of Windows Server, Azure Backup Server can't take advantage of Modern Backup Storage. Instead, it protects workloads as it does with Backup Server V1. For more information, see the Backup Server version [protection matrix](#).

To achieve enhanced backup performances we recommend to deploy MABS v3 with tiered storage on Windows Server 2019. Please refer to the DPM article "[Set up MBS with Tiered Storage](#)" for steps to configure tiered storage.

## Volumes in Backup Server

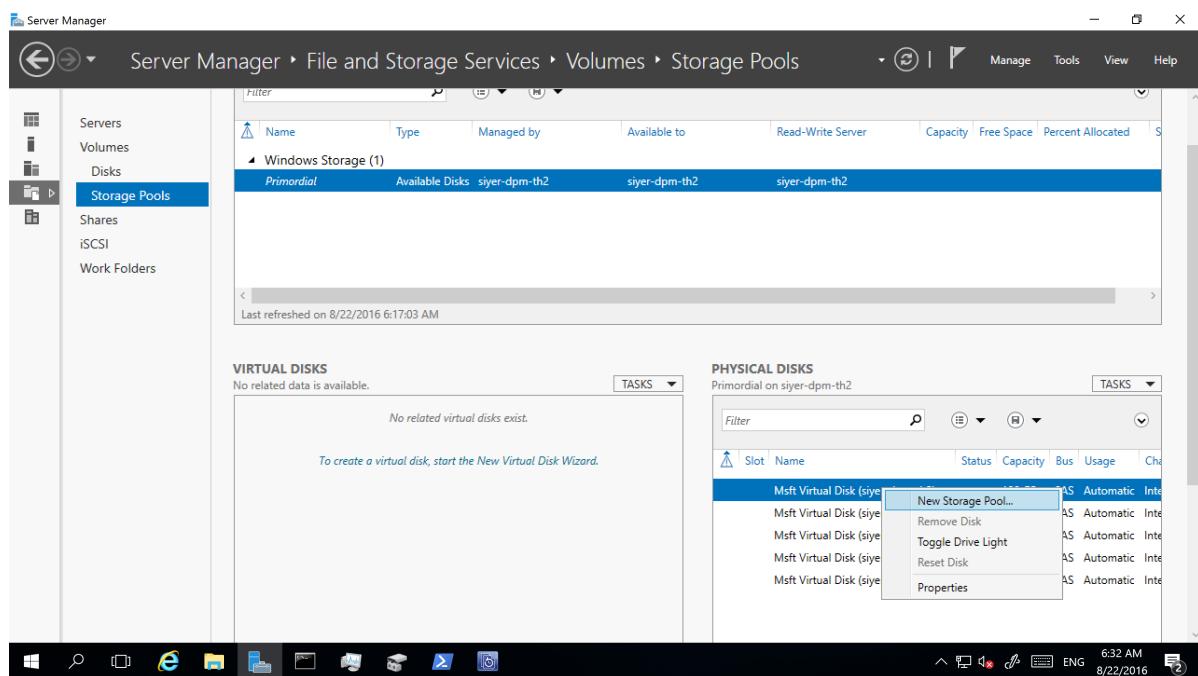
Backup Server V2 or later accepts storage volumes. When you add a volume, Backup Server formats the volume to Resilient File System (ReFS), which Modern Backup Storage requires. To add a volume, and to expand it later if you need to, we suggest that you use this workflow:

1. Set up Backup Server on a VM.
2. Create a volume on a virtual disk in a storage pool:
  - a. Add a disk to a storage pool and create a virtual disk with simple layout.
  - b. Add any additional disks, and extend the virtual disk.
  - c. Create volumes on the virtual disk.
3. Add the volumes to Backup Server.
4. Configure workload-aware storage.

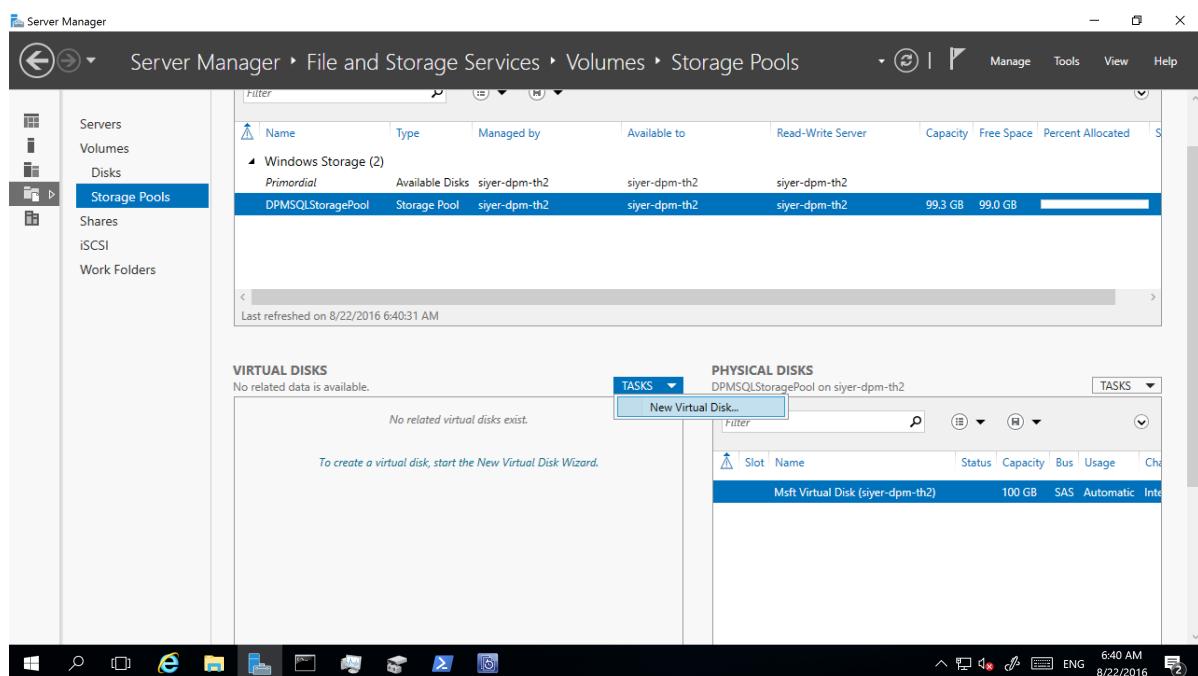
## Create a volume for Modern Backup Storage

Using Backup Server V2 or later with volumes as disk storage can help you maintain control over storage. A volume can be a single disk. However, if you want to extend storage in the future, create a volume out of a disk created by using storage spaces. This can help if you want to expand the volume for backup storage. This section offers best practices for creating a volume with this setup.

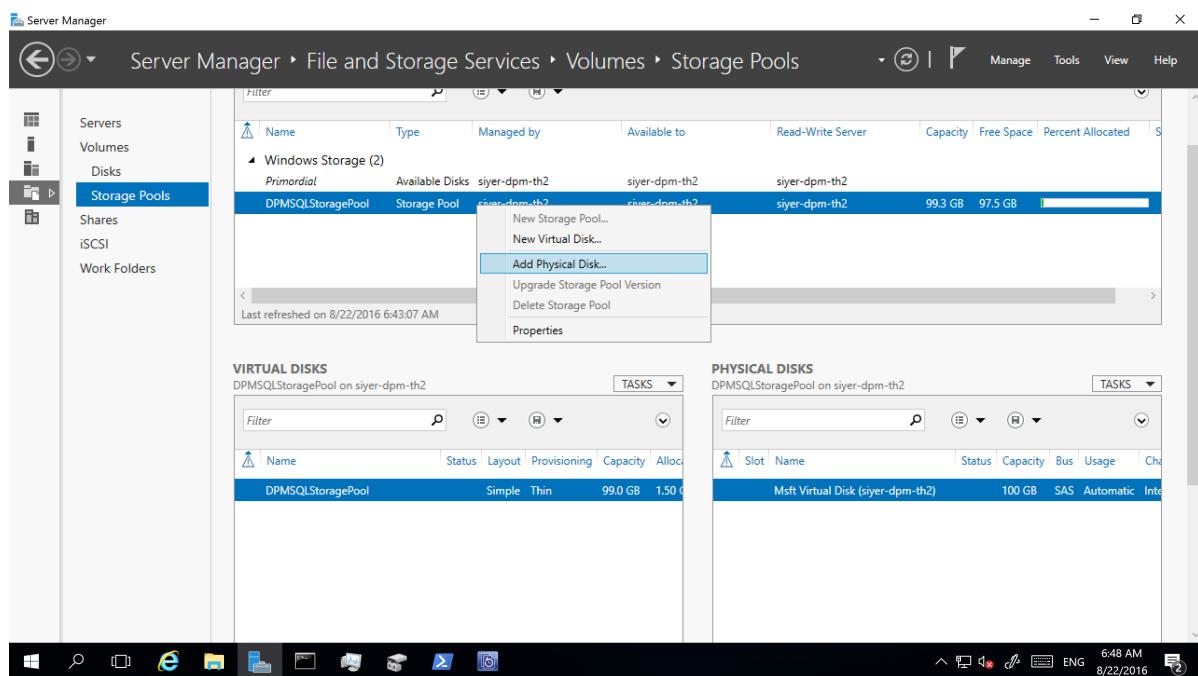
1. In Server Manager, select **File and Storage Services > Volumes > Storage Pools**. Under **PHYSICAL DISKS**, select **New Storage Pool**.



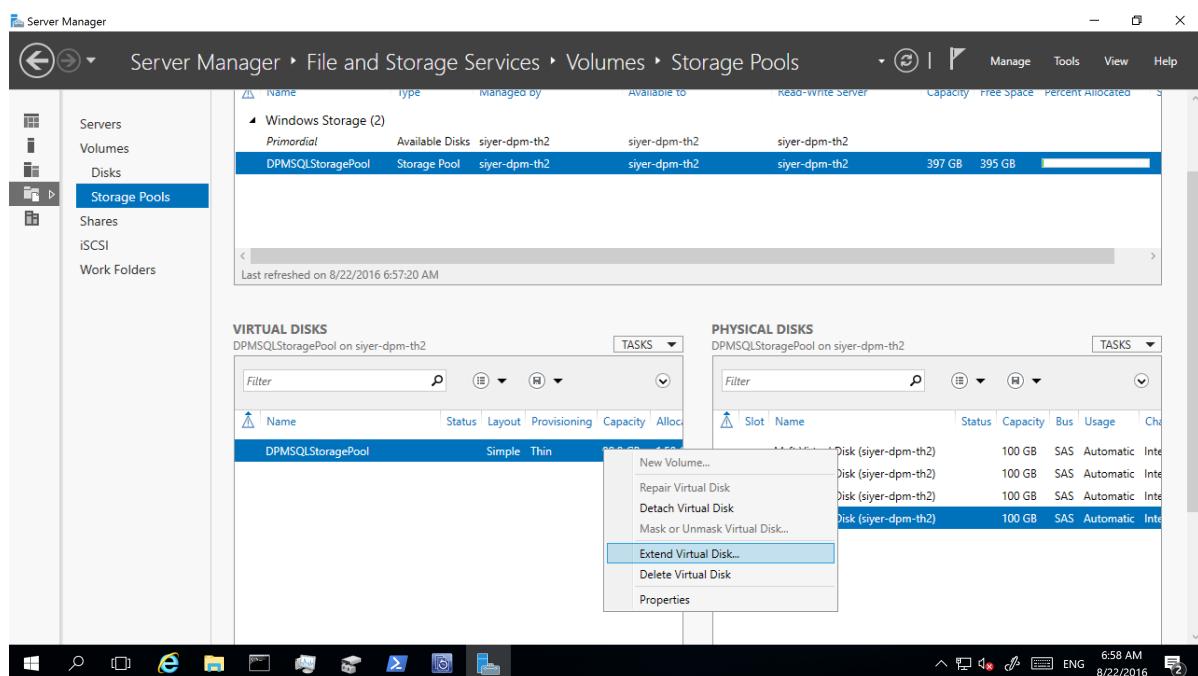
2. In the **TASKS** drop-down box, select **New Virtual Disk**.



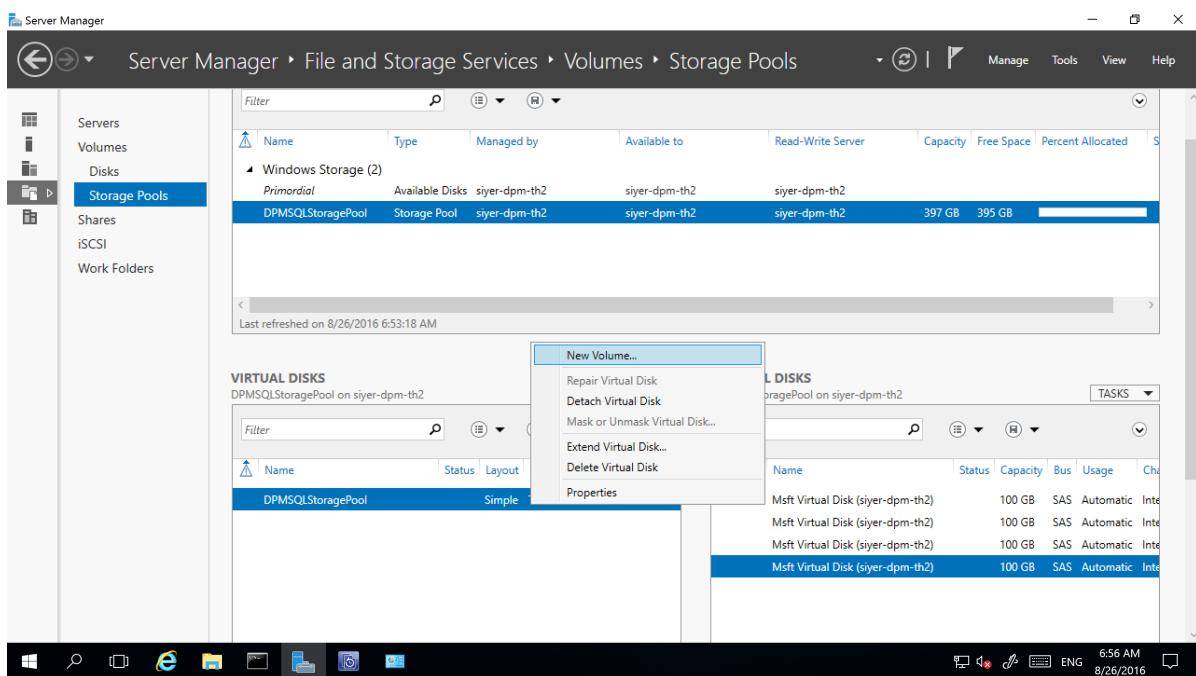
3. Select the storage pool, and then select **Add Physical Disk**.



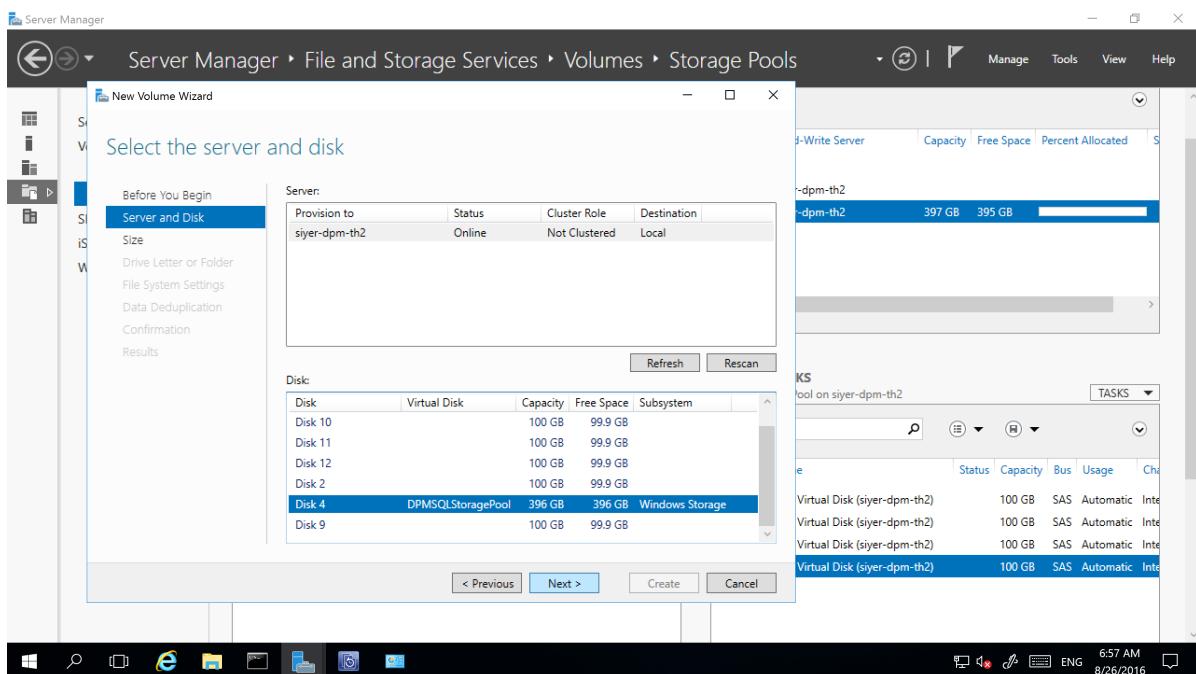
4. Select the physical disk, and then select **Extend Virtual Disk**.



5. Select the virtual disk, and then select **New Volume**.



6. In the **Select the server and disk** dialog, select the server and the new disk. Then, select **Next**.

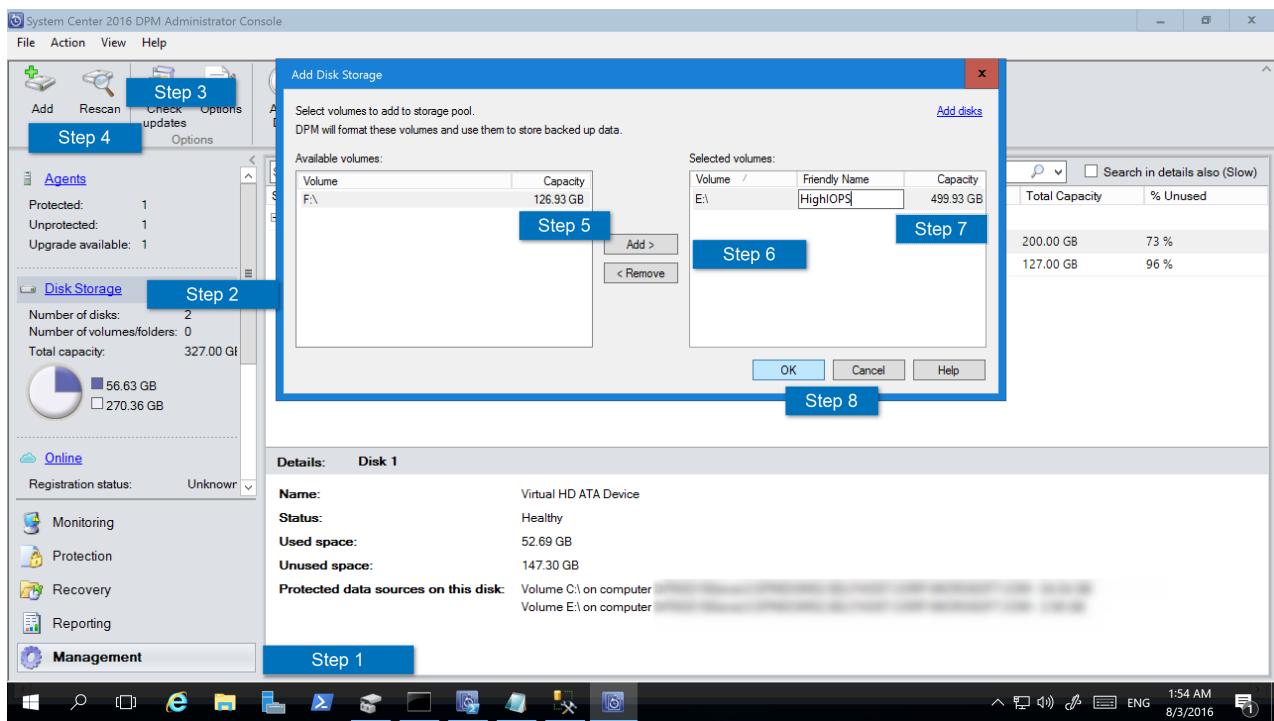


## Add volumes to Backup Server disk storage

### NOTE

- Add only one disk to the pool to keep the column count to 1. You can then add disks as needed afterwards.
- If you add multiple disks to the storage pool at a go, the number of disks is stored as the number of columns. When more disks are added, they can only be a multiple of the number of columns.

To add a volume to Backup Server, in the **Management** pane, rescan the storage, and then select **Add**. A list of all the volumes available to be added for Backup Server Storage appears. After available volumes are added to the list of selected volumes, you can give them a friendly name to help you manage them. To format these volumes to ReFS so Backup Server can use the benefits of Modern Backup Storage, select **OK**.



## Set up workload-aware storage

With workload-aware storage, you can select the volumes that preferentially store certain kinds of workloads. For example, you can set expensive volumes that support a high number of input/output operations per second (IOPS) to store only the workloads that require frequent, high-volume backups. An example is SQL Server with transaction logs. Other workloads that are backed up less frequently, like VMs, can be backed up to low-cost volumes.

### **Update-DPMDiskStorage**

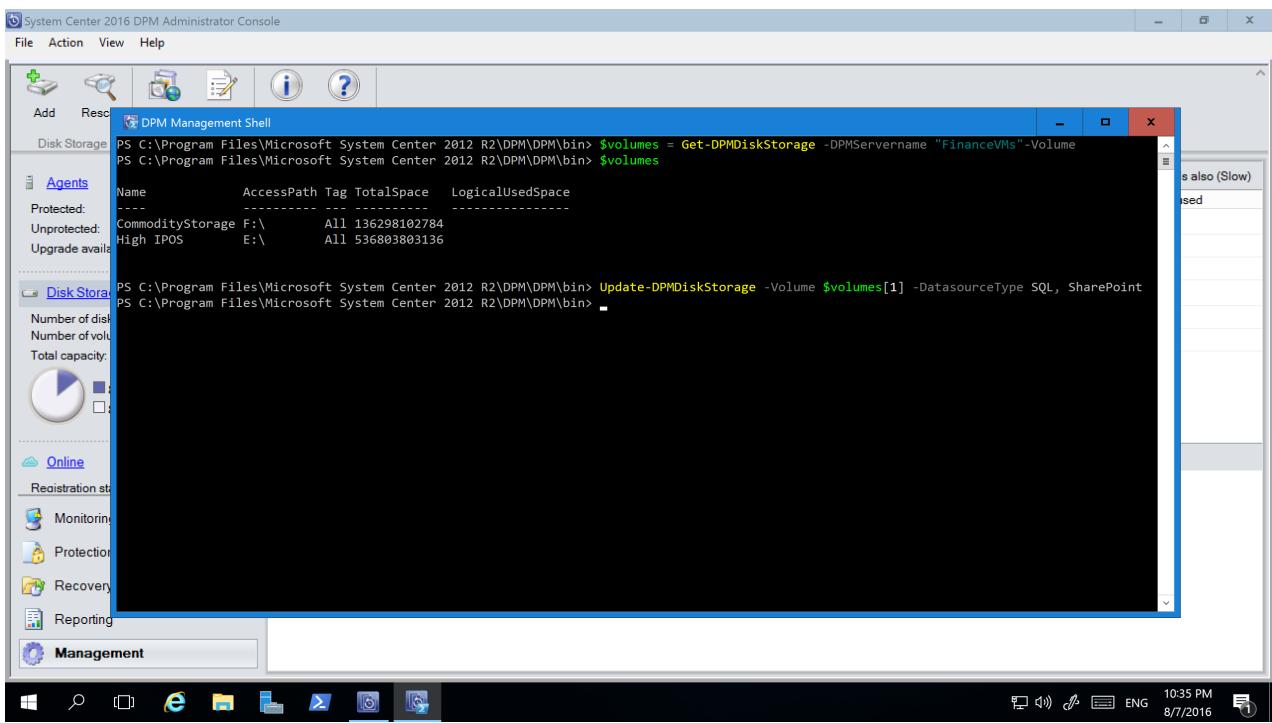
You can set up workload-aware storage by using the PowerShell cmdlet `Update-DPMDiskStorage`, which updates the properties of a volume in the storage pool on an Azure Backup Server.

Syntax:

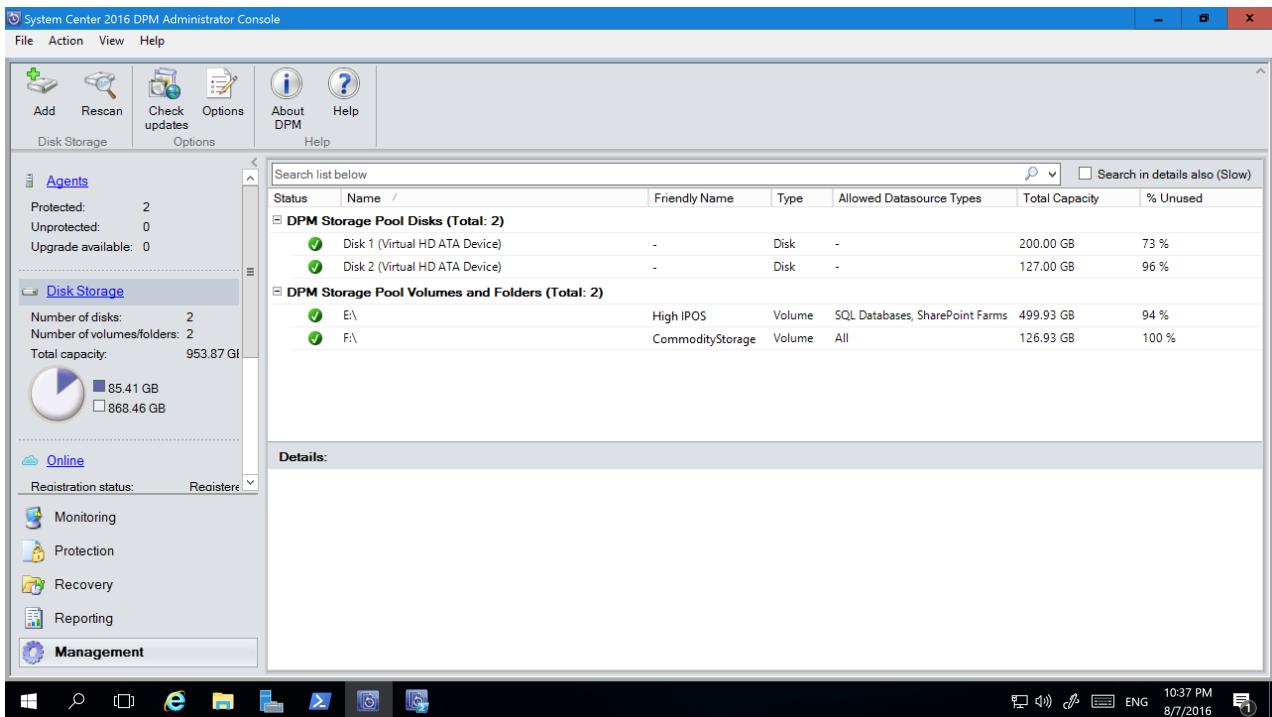
Parameter Set: Volume

```
Update-DPMDiskStorage [-Volume] <Volume> [[-FriendlyName] <String>] [[-DatasourceType] <VolumeTag[]>] [-Confirm] [-WhatIf] [<CommonParameters>]
```

The following screenshot shows the `Update-DPMDiskStorage` cmdlet in the PowerShell window.



The changes you make by using PowerShell are reflected in the Backup Server Administrator Console.

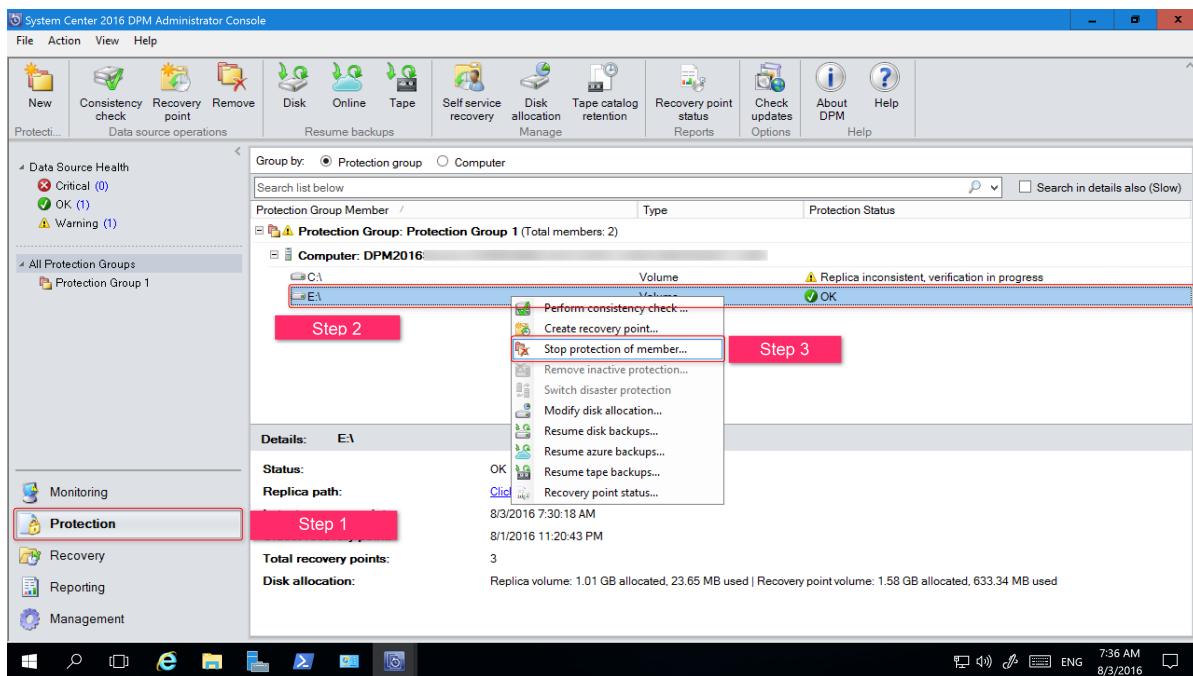


## Migrate legacy storage to Modern Backup Storage

After you upgrade to or install Backup Server V2 and upgrade the operating system to Windows Server 2016, update your protection groups to use Modern Backup Storage. By default, protection groups are not changed. They continue to function as they were initially set up.

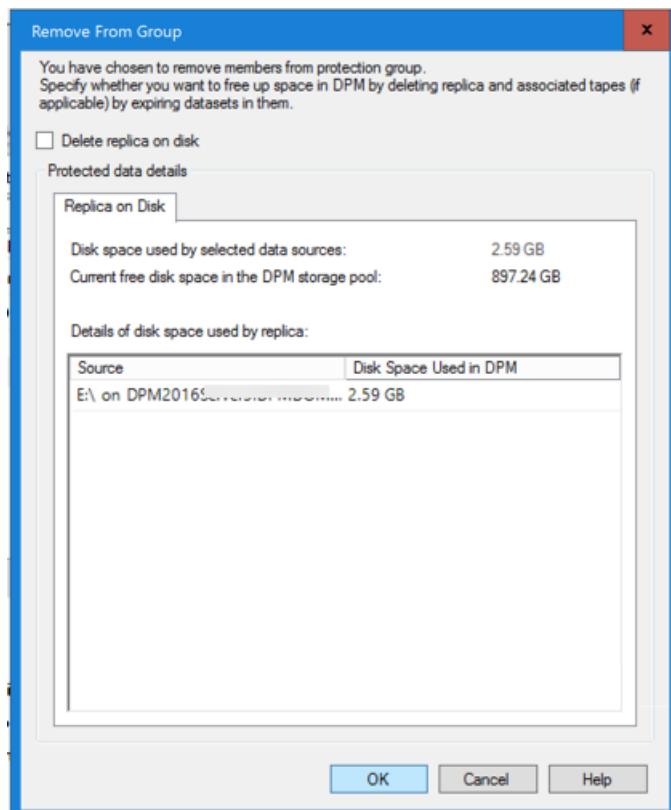
Updating protection groups to use Modern Backup Storage is optional. To update the protection group, stop protection of all data sources by using the retain data option. Then, add the data sources to a new protection group.

1. In the Administrator Console, select the **Protection** feature. In the **Protection Group Member** list, right-click the member, and then select **Stop protection of member**.



2. In the **Remove from Group** dialog box, review the used disk space and the available free space for the storage pool. The default is to leave the recovery points on the disk and allow them to expire per their associated retention policy. Click **OK**.

If you want to immediately return the used disk space to the free storage pool, select the **Delete replica on disk** check box to delete the backup data (and recovery points) associated with that member.



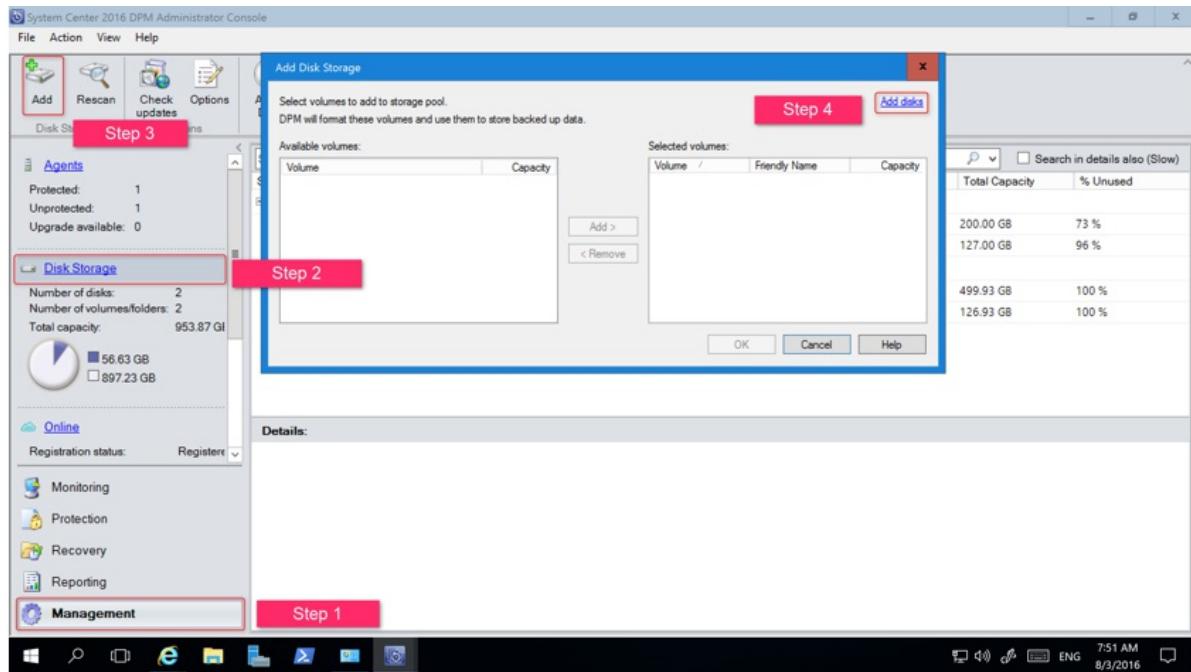
3. Create a protection group that uses Modern Backup Storage. Include the unprotected data sources.

## Add disks to increase legacy storage

If you want to use legacy storage with Backup Server, you might need to add disks to increase legacy storage.

To add disk storage:

1. In the Administrator Console, select **Management** > **Disk Storage** > **Add**.



2. In the **Add Disk Storage** dialog, select **Add disks**.
3. In the list of available disks, select the disks you want to add, select **Add**, and then select **OK**.

## Next steps

After you install Backup Server, learn how to prepare your server, or begin protecting a workload.

- [Prepare Backup Server workloads](#)
- [Use Backup Server to back up a VMware server](#)
- [Use Backup Server to back up SQL Server](#)

# What's new in Microsoft Azure Backup Server

2/24/2020 • 3 minutes to read • [Edit Online](#)

Microsoft Azure Backup Server version 3 (MABS V3) is the latest upgrade, and includes critical bug fixes, Windows Server 2019 support, SQL 2017 support, and other features and enhancements. To view the list of bugs fixed and the installation instructions for MABS V3, see KB article [4457852](#).

The following features are included in MABS V3:

## Volume to Volume migration

With Modern Backup Storage (MBS) in MABS V2, we announced Workload aware storage, where you configure certain workloads to be backed up to specific storage, based on storage properties. However, after configuration, you may find a need to move backups of certain data sources to other storage for optimized resource utilization. MABS V3 gives you the capability to migrate your backups and configure them to be stored to a different volume in [three steps](#).

## Prevent unexpected data loss

In enterprises, MABS is managed by a team of administrators. While there are guidelines on storage that should be used for backups, an incorrect volume given to MABS as backup storage may lead to loss of critical data. With MABS V3, you can prevent such scenarios by configuring those volumes as the ones that are not available for storage using [these PowerShell cmdlets](#).

## Custom size allocation

Modern Backup Storage (MBS) consumes storage thinly, as and when needed. To do so, MABS calculates the size of the data being backed up when it is configured for protection. However, if many files and folders are being backed up together, as in the case of a file server, size calculation can take long time. With MABS V3, you can configure MABS to accept the volume size as default, instead of calculating the size of each file, hence saving time.

## Optimized CC for RCT VMs

MABS uses RCT (the native change tracking in Hyper-V), which decreases the need for time-consuming consistency checks in scenarios as VM crashes. RCT provides better resiliency than the change tracking provided by VSS snapshot-based backups. MABS V3 optimizes network and storage consumption further by transferring only the changed data during any consistency checks.

## Support to TLS 1.2

TLS 1.2 is the secure way of communication suggested by Microsoft with best-in class encryption. MABS now supports TLS 1.2 communication between MABS and the protected servers, for certificate-based authentication, and for cloud backups.

## VMware VM protection support

VMware VM backup is now supported for production deployments. MABS V3 offers the following for VMware VM protection:

- Support for vCenter and ESXi 6.5, along with support for 5.5 and 6.0.

- Auto-protection of VMware VMs to cloud. If new VMware VMs are added to a protected folder, they are automatically protected to disk and cloud.
- Recovery efficiency improvements for VMware alternative location recovery.

## SQL 2017 support

MABS V3 can be installed with SQL 2017 as the MABS database. You can upgrade the SQL server from SQL 2016 to SQL 2017, or install it freshly. You can also back up SQL 2017 workload both in clustered and non-clustered environment with MABS V3.

## Windows Server 2019 support

MABS V3 can be installed on Windows Server 2019. To use MABS V3 with WS2019, you can either upgrade your OS to WS2019 before installing/upgrading to MABS V3 or you can upgrade your OS post installing/upgrading V3 on WS2016.

MABS V3 is a full release, and can be installed directly on Windows Server 2016, Windows Server 2019, or can be upgraded from MABS V2. Before you upgrade to or install Backup Server V3, read about the installation prerequisites. Find more information about the installation/upgrade steps for MABS [here](#).

### NOTE

MABS has the same code base as System Center Data Protection Manager. MABS v3 is equivalent to Data Protection Manager 1807.

## Next steps

Learn how to prepare your server or begin protecting a workload:

- [Known issues in MABS V3](#)
- [Prepare Backup Server workloads](#)
- [Use Backup Server to back up a VMware server](#)
- [Use Backup Server to back up SQL Server](#)
- [Use Modern Backup Storage with Backup Server](#)

# Release notes for Microsoft Azure Backup Server

11/18/2019 • 2 minutes to read • [Edit Online](#)

This article provides the known issues and workarounds for Microsoft Azure Backup Server (MABS) V3.

## Backup and recovery fails for clustered workloads

**Description:** Backup/restore fails for clustered data sources such as Hyper-V cluster or SQL cluster (SQL Always On) or Exchange in database availability group (DAG) after upgrading MABS V2 to MABS V3.

**Work around:** To prevent this, open SQL Server Management Studio (SSMS)) and run the following SQL script on the DPM DB:

```
IF EXISTS (SELECT * FROM dbo.sysobjects
 WHERE id = OBJECT_ID(N'[dbo].[tbl_PRM_DatasourceLastActiveServerMap]')
 AND OBJECTPROPERTY(id, N'IsUserTable') = 1)
DROP TABLE [dbo].[tbl_PRM_DatasourceLastActiveServerMap]
GO

CREATE TABLE [dbo].[tbl_PRM_DatasourceLastActiveServerMap] (
 [DatasourceId] [GUID] NOT NULL,
 [ActiveNode] [nvarchar](256) NULL,
 [IsGCed] [bit] NOT NULL
) ON [PRIMARY]
GO

ALTER TABLE [dbo].[tbl_PRM_DatasourceLastActiveServerMap] ADD
CONSTRAINT [pk_tbl_PRM_DatasourceLastActiveServerMap__DatasourceId] PRIMARY KEY NONCLUSTERED
(
 [DatasourceId]
) ON [PRIMARY],

CONSTRAINT [DF_tbl_PRM_DatasourceLastActiveServerMap_IsGCed] DEFAULT
(
 0
) FOR [IsGCed]
GO
```

## Upgrade to MABS V3 fails in Russian locale

**Description:** Upgrade from MABS V2 to MABS V3 in Russian locale fails with an error code **4387**.

**Work around:** Do the following steps to upgrade to MABS V3 using Russian install package:

1. [Backup](#) your SQL database and uninstall MABS V2 (choose to retain the protected data during uninstall).
2. Upgrade to SQL 2017 (Enterprise) and uninstall reporting as part of upgrade.
3. [Install](#) SQL Server Reporting Services (SSRS).
4. [Install](#) SQL Server Management Studio (SSMS).
5. Configure Reporting using the parameters as documented in [SSRS configuration with SQL 2017](#).
6. [Install](#) MABS V3.
7. [Restore](#) SQL using SSMS and run DPM-Sync tool as described [here](#).
8. Update the 'DataBaseVersion' property in dbo.tbl\_DLS\_GlobalSetting table using the following command:

```
UPDATE dbo.tbl_DLS_GlobalSetting
set PropertyValue = '13.0.415.0'
where PropertyName = 'DatabaseVersion'
```

9. Start MSDPM service.

## Next steps

[What's New in MABS V3](#)

# Run an unattended installation of Azure Backup Server

11/18/2019 • 2 minutes to read • [Edit Online](#)

Learn how to run an unattended installation of Azure Backup Server.

These steps don't apply if you're installing Azure Backup Server V1.

## Install Backup Server

1. On the server that hosts Azure Backup Server V2 or later, create a text file. (You can create the file in Notepad or in another text editor.) Save the file as MABSSetup.ini.
2. Paste the following code in the MABSSetup.ini file. Replace the text inside the brackets (< >) with values from your environment. The following text is an example:

```
[OPTIONS]
UserName=administrator
CompanyName=<Microsoft Corporation>
SQLMachineName=localhost
SQLInstanceName=<SQL instance name>
SQLMachineUserName=administrator
SQLMachinePassword=<admin password>
SQLMachineDomainName=<machine domain>
ReportingMachineName=localhost
ReportingInstanceName=<reporting instance name>
SqlAccountPassword=<admin password>
ReportingMachineUserName=<username>
ReportingMachinePassword=<reporting admin password>
ReportingMachineDomainName=<domain>
VaultCredentialFilePath=<vault credential full path and complete name>
SecurityPassphrase=<passphrase>
PassphraseSaveLocation=<passphrase save location>
UseExistingSQL=<1/0 use or do not use existing SQL>
```

3. Save the file. Then, at an elevated command prompt on the installation server, enter this command:

```
start /wait <cldlayout path>/Setup.exe /i /f <.ini file path>/setup.ini /L <log path>/setup.log
```

You can use these flags for the installation:

**/f:** .ini file path  
**/l:** Log path  
**/i:** Installation path  
**/x:** Uninstall path

## Next steps

After you install Backup Server, learn how to prepare your server, or begin protecting a workload.

- [Prepare Backup Server workloads](#)
- [Use Backup Server to back up a VMware server](#)
- [Use Backup Server to back up SQL Server](#)

- Add Modern Backup Storage to Backup Server

# Back up Hyper-V virtual machines with Azure Backup Server

2/24/2020 • 19 minutes to read • [Edit Online](#)

This article explains how to back up Hyper-V virtual machines using Microsoft Azure Backup Server (MABS).

## Supported scenarios

MABS can back up virtual machines running on Hyper-V host servers in the following scenarios:

- **Virtual machines with local or direct storage** - Back up virtual machines hosted on Hyper-V host standalone servers that have local or directly attached storage. For example: a hard drive, a storage area network (SAN) device, or a network attached storage (NAS) device. The MABS protection agent must be installed on all hosts.
- **Virtual machines in a cluster with CSV storage** - Back up virtual machines hosted on a Hyper-V cluster with Cluster Shared Volume (CSV) storage. The MABS protection agent is installed on each cluster node.

## Host versus guest backup

MABS can do a host or guest-level backup of Hyper-V VMs. At the host level, the MABS protection agent is installed on the Hyper-V host server or cluster and protects the entire VMs and data files running on that host. At the guest level, the agent is installed on each virtual machine and protects the workload present on that machine.

Both methods have pros and cons:

- Host-level backups are flexible because they work regardless of the type of OS running on the guest machines and don't require the installation of the MABS protection agent on each VM. If you deploy host level backup, you can recover an entire virtual machine, or files and folders (item-level recovery).
- Guest-level backup is useful if you want to protect specific workloads running on a virtual machine. At host-level you can recover an entire VM or specific files, but it won't provide recovery in the context of a specific application. For example, to recover specific SharePoint items from a backed-up VM, you should do guest-level backup of that VM. Use guest-level backup if you want to protect data stored on passthrough disks. Passthrough allows the virtual machine to directly access the storage device and doesn't store virtual volume data in a VHD file.

## How the backup process works

MABS performs backup with VSS as follows. The steps in this description are numbered to help with clarity.

1. The MABS block-based synchronization engine makes an initial copy of the protected virtual machine and ensures that the copy of the virtual machine is complete and consistent.
2. After the initial copy is made and verified, MABS uses the Hyper-V VSS writer to capture backups. The VSS writer provides a data-consistent set of disk blocks that are synchronized with the MABS server. This approach provides the benefit of a "full backup" with the MABS server, while minimizing the backup data that must be transferred across the network.
3. The MABS protection agent on a server that is running Hyper-V uses the existing Hyper-V APIs to determine whether a protected virtual machine also supports VSS.

- If a virtual machine complies with the requirements for online backup and has the Hyper-V integration services component installed, then the Hyper-V VSS writer recursively forwards the VSS request through to all VSS-aware processes on the virtual machine. This operation occurs without the MABS protection agent being installed on the virtual machine. The recursive VSS request allows the Hyper-V VSS writer to ensure that disk- write operations are synchronized so that a VSS snapshot is captured without the loss of data.

The Hyper-V integration services component invokes the Hyper-V VSS writer in Volume Shadow Copy Services (VSS) on virtual machines to ensure that their application data is in a consistent state.

- If the virtual machine doesn't comply with online backup requirements, MABS automatically uses the Hyper-V APIs to pause the virtual machine before they capture data files.
4. After the initial baseline copy of the virtual machine synchronizes with the MABS server, all changes that are made to the virtual machine resources are captured in a new recovery point. The recovery point represents the consistent state of the virtual machine at a specific time. Recovery point captures can occur at least one time a day. When a new recovery point is created, MABS uses block-level replication in conjunction with the Hyper-V VSS writer to determine which blocks have been altered on the server that is running Hyper-V after the last recovery point was created. These data blocks are then transferred to the MABS server and are applied to the replica of the protected data.
  5. The MABS server uses VSS on the volumes that host recovery data so that multiple shadow copies are available. Each of these shadow copies provides a separate recovery. VSS recovery points are stored on the MABS server. The temporary copy that is made on the server running Hyper-V, is only stored for the duration of the MABS synchronization.

#### **NOTE**

Starting in Windows Server 2016, Hyper-V virtual hard disks have built-in change tracking known as resilient change tracking (RCT). MABS uses RCT (the native change tracking in Hyper-V), which decreases the need for time-consuming consistency checks in scenarios such as VM crashes. RCT provides better resiliency than the change tracking provided by VSS snapshot-based backups. MABS V3 optimizes network and storage consumption further by transferring only the changed data during any consistency checks.

## Backup prerequisites

These are the prerequisites for backing up Hyper-V virtual machines with MABS:

| PREREQUISITE | DETAILS |
|--------------|---------|
|--------------|---------|

| PREREQUISITE                 | DETAILS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MABS prerequisites           | <ul style="list-style-type: none"> <li>- If you want to perform item-level recovery for virtual machines (recover files, folders, volumes), then you'll need to install the Hyper-V role on the MABS server. If you only want to recover the virtual machine and not item-level, then the role isn't required.</li> <li>- You can protect up to 800 virtual machines of 100 GB each on one MABS server and allow multiple MABS servers that support larger clusters.</li> <li>- MABS excludes the page file from incremental backups to improve virtual machine backup performance.</li> <li>- MABS can back up a Hyper-V server or cluster in the same domain as the MABS server, or in a child or trusted domain. If you want to back up Hyper-V in a workgroup or an untrusted domain, you'll need to set up authentication. For a single Hyper-V server, you can use NTLM or certificate authentication. For a cluster, you can use certificate authentication only.</li> <li>- Using host-level backup to back up virtual machine data on passthrough disks isn't supported. In this scenario, we recommend you use host-level backup to back up VHD files and guest-level backup to back up the other data that isn't visible on the host.</li> <li>- You can back up VMs stored on deduplicated volumes.</li> </ul> |
| Hyper-V VM prerequisites     | <ul style="list-style-type: none"> <li>- The version of Integration Components that is running on the virtual machine should be the same as the version of the Hyper-V host.</li> <li>- For each virtual machine backup you'll need free space on the volume hosting the virtual hard disk files to allow Hyper-V enough room for differencing disks (AVHD's) during backup. The space must be at least equal to the calculation <b>Initial disk size*Churn rate*Backup window time</b>. If you're running multiple backups on a cluster, you'll need enough storage capacity to accommodate the AVHDs for each of the virtual machines using this calculation.</li> <li>- To back up virtual machines located on Hyper-V host servers running Windows Server 2012 R2, the virtual machine should have a SCSI controller specified, even if it's not connected to anything. (In Windows Server 2012 R2 online backup, the Hyper-V host mounts a new VHD in the VM and then later dismounts it. Only the SCSI controller can support this and therefore is required for online backup of the virtual machine. Without this setting, event ID 10103 will be issued when you try to back up the virtual machine.)</li> </ul>                                                                                                  |
| Linux prerequisites          | <ul style="list-style-type: none"> <li>- You can back up Linux virtual machines using MABS. Only file-consistent snapshots are supported.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Back up VMs with CSV storage | <ul style="list-style-type: none"> <li>- For CSV storage, install the Volume Shadow Copy Services (VSS) hardware provider on the Hyper-V server. Contact your storage area network (SAN) vendor for the VSS hardware provider.</li> <li>- If a single node shuts down unexpectedly in a CSV cluster, MABS will perform a consistency check against the virtual machines that were running on that node.</li> <li>- If you need to restart a Hyper-V server that has BitLocker Drive Encryption enabled on the CSV cluster, you must run a consistency check for Hyper-V virtual machines.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| PREREQUISITE                 | DETAILS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Back up VMs with SMB storage | <ul style="list-style-type: none"> <li>- Turn on auto-mount on the server that is running Hyper-V to enable virtual machine protection.</li> <li>- Disable TCP Chimney Offload.</li> <li>- Ensure that all Hyper-V machine\$ accounts have full permissions on the specific remote SMB file shares.</li> <li>- Ensure that the file path for all virtual machine components during recovery to alternate location is fewer than 260 characters. If not, recovery might succeed, but Hyper-V won't be able to mount the virtual machine.</li> <li>- The following scenarios aren't supported:<br/>Deployments where some components of the virtual machine are on local volumes and some components are on remote volumes; an IPv4 or IPv6 address for storage location file server, and recovery of a virtual machine to a computer that uses remote SMB shares.</li> <li>- You'll need to enable the File Server VSS Agent service on each SMB server - Add it in <b>Add roles and features &gt; Select server roles &gt; File and Storage Services &gt; File Services &gt; File Service &gt; File Server VSS Agent Service</b>.</li> </ul> |

## Back up virtual machines

1. Set up your [MABS server](#) and [your storage](#). When setting up your storage, use these storage capacity guidelines.
  - Average virtual machine size - 100 GB
  - Number of virtual machines per MABS server - 800
  - Total size of 800 VMs - 80 TB
  - Required space for backup storage - 80 TB
2. Set up the MABS protection agent on the Hyper-V server or Hyper-V cluster nodes. If you're doing guest-level backup, you'll install the agent on the VMs you want to back up at the guest-level.
3. In the MABS Administrator console, click **Protection > Create protection group** to open the **Create New Protection Group** wizard.
4. On the **Select Group Members** page, select the VMs you want to protect from the Hyper-V host servers on which they're located. We recommend you put all VMs that will have the same protection policy into one protection group. To make efficient use of space, enable colocation. Colocation allows you to locate data from different protection groups on the same disk or tape storage, so that multiple data sources have a single replica and recovery point volume.
5. On the **Select Data Protection Method** page, specify a protection group name. Select **I want short-term protection using Disk** and select **I want online protection** if you want to back up data to Azure using the Azure Backup service.
6. In **Specify Short-Term Goals > Retention range**, specify how long you want to retain disk data. In **Synchronization frequency**, specify how often incremental backups of the data should run. Alternatively, instead of selecting an interval for incremental backups you can enable **Just before a recovery point**. With this setting enabled, MABS will run an express full backup just before each scheduled recovery point.

#### **NOTE**

If you're protecting application workloads, recovery points are created in accordance with Synchronization frequency, provided the application supports incremental backups. If it doesn't, then MABS runs an express full backup, instead of an incremental backup, and creates recovery points in accordance with the express backup schedule.

7. In the **Review disk allocation** page, review the storage pool disk space allocated for the protection group.

**Total Data size** is the size of the data you want to back up, and **Disk space to be provisioned on MABS** is the space that MABS recommends for the protection group. MABS chooses the ideal backup volume, based on the settings. However, you can edit the backup volume choices in the **Disk allocation details**. For the workloads, select the preferred storage in the dropdown menu. Your edits change the values for **Total Storage** and **Free Storage** in the **Available Disk Storage** pane. Underprovisioned space is the amount of storage MABS suggests you add to the volume, to continue with backups smoothly in the future.

8. On the **Choose Replica Creation Method** page, specify how the initial replication of data in the protection group will be performed. If you select to **Automatically replicate over the network**, we recommend you choose an off-peak time. For large amounts of data or less than optimal network conditions, consider selecting **Manually**, which requires replicating the data offline using removable media.
9. On the **Consistency Check Options** page, select how you want to automate consistency checks. You can enable a check to run only when replica data becomes inconsistent, or according to a schedule. If you don't want to configure automatic consistency checking, you can run a manual check at any time by right-clicking the protection group and selecting **Perform Consistency Check**.

After you create the protection group, initial replication of the data occurs in accordance with the method you selected. After initial replication, each backup takes place in line with the protection group settings. If you need to recover backed up data, note the following:

## Back up virtual machines configured for live migration

When virtual machines are involved in live migration, MABS continues to protect the virtual machines as long as the MABS protection agent is installed on the Hyper-V host. The way in which MABS protects the virtual machines depends on the type of live migration involved.

**Live migration within a cluster** - When a virtual machine is migrated within a cluster MABS detects the migration, and backs up the virtual machine from the new cluster node without any requirement for user intervention. Because the storage location hasn't changed, MABS continues with express full backups.

**Live migration outside the cluster** - When a virtual machine is migrated between stand-alone servers, different clusters, or between a stand-alone server and a cluster, MABS detects the migration, and can back up the virtual machine without user intervention.

### Requirements for maintaining protection

The following are requirements for maintaining protection during live migration:

- The Hyper-V hosts for the virtual machines must be located in a System Center VMM cloud, on a VMM server, running at least System Center 2012 with SP1.
- The MABS protection agent must be installed on all Hyper-V hosts.
- MABS servers must be connected to the VMM server. All Hyper-V host servers in the VMM cloud must also be connected to the MABS servers. This allows MABS to communicate with the VMM server so MABS can find out on which Hyper-V host server the virtual machine is currently running, and to create a new backup from that Hyper-V server. If a connection can't be established to the Hyper-V server, the backup fails with a message that the MABS protection agent is unreachable.

- All MABS servers, VMM servers, and Hyper-V host servers must be in the same domain.

## Details about live migration

Note the following for backup during live migration:

- If a live migration transfers storage, MABS performs a full consistency check of the virtual machine, and then continues with express full backups. When live migration of storage occurs, Hyper-V reorganizes the virtual hard disk (VHD) or VHDX, which causes a one-time spike in the size of the MABS backup data.
- On the virtual machine host, turn on auto-mount to enable virtual protection, and disable TCP Chimney Offload.
- MABS uses port 6070 as the default port for hosting the DPM-VMM Helper Service. To change the registry:
  - Navigate to **HKLM\Software\Microsoft\Microsoft Data Protection Manager\Configuration**.
  - Create a 32-bit DWORD value: DpmVmmHelperServicePort, and write the updated port number as part of the registry key.
  - Open `<Install directory>\Azure Backup Server\DP\DP\VmHelperService\VmHelperServiceHost.exe.config`, and change the port number from 6070 to the new port. For example:  
`<add baseAddress="net.tcp://localhost:6080/VmHelperService/" />`
  - Restart the DPM-VMM Helper service, and restart the DPM service.

## Set up protection for live migration

To set up protection for live migration:

- Set up the MABS server and its storage, and install the MABS protection agent on every Hyper-V host server or cluster node in the VMM cloud. If you're using SMB storage in a cluster, install the MABS protection agent on all cluster nodes.
- Install the VMM console as a client component on the MABS server so that MABS can communicate with the VMM server. The console should be the same version as the one running on the VMM server.
- Assign the MABSMachineName\$ account as a read-only administrator account on the VMM management server.
- Connect all Hyper-V host servers to all MABS servers with the `Set-DPMGlobalProperty` PowerShell cmdlet. The cmdlet accepts multiple MABS server names. Use the format:  
`Set-DPMGlobalProperty -dpmservername <MABSservername> -knownvmmservers <vmmservername>`. For more information, see [Set-DPMGlobalProperty](#).
- After all virtual machines running on the Hyper-V hosts in the VMM clouds are discovered in VMM, set up a protection group and add the virtual machines you want to protect. Automatic consistency checks should be enabled at the protection group level for protection under virtual machine mobility scenarios.
- After the settings are configured, when a virtual machine migrates from one cluster to another all backups continue as expected. You can verify live migration is enabled as expected as follows:
  - Check the DPM-VMM Helper Service is running. If it isn't, start it.
  - Open Microsoft SQL Server Management Studio and connect to the instance that hosts the MABS database (DPMDB). On DPMDB run the following query:  
`SELECT TOP 1000 [PropertyName] , [PropertyValue] FROM[DPMDB].[dbo].[tbl_DLS_GlobalSetting]`.

This query contains a property called `KnownVMMServer`. This value should be the same value you provided with the `Set-DPMGlobalProperty` cmdlet.

- c. Run the following query to validate the *VMMIdentifier* parameter in the `PhysicalPathXML` for a particular virtual machine. Replace `VMName` with the name of the virtual machine.

```
select cast(PhysicalPath as XML) from tbl_IM_ProtectedObject where DataSourceId in (select datasourceid from tbl_IM_DataSource where DataSourceName like '%<VMName>%')
```

- d. Open the .xml file that this query returns and validate that the *VMMIdentifier* field has a value.

### Run manual migration

After you complete the steps in the previous sections, and the MABS Summary Manager job completes, migration is enabled. By default, this job starts at midnight and runs every morning. If you want to run a manual migration, to check everything is working as expected, do the following:

1. Open SQL Server Management Studio and connect to the instance that hosts the MABS database.

2. Run the following query:

```
select * from tbl_SCH_ScheduleDefinition where JobDefinitionID='9B30D213-B836-4B9E-97C2-DB03C3EB39D7' .
```

This query returns the **ScheduleID**. Note this ID as you will use it in the next step.

3. In the SQL Server Management Studio, expand **SQL Server Agent**, and then expand **Jobs**. Right-click **ScheduleID** that you noted, and select **Start Job at Step**.

Backup performance is affected when the job runs. The size and scale of your deployment determines how much time the job takes to finish.

## Back up replica virtual machines

If MABS is running on Windows Server 2012 R2 or greater, then you can back up replica virtual machines. This is useful for several reasons:

**Reduces the impact of backups on the running workload** - Taking a backup of a virtual machine incurs some overhead as a snapshot is created. By offloading the backup process to a secondary remote site, the running workload is no longer affected by the backup operation. This is applicable only to deployments where the backup copy is stored on a remote site. For example, you might take daily backups and store data locally to ensure quick restore times, but take monthly or quarterly backups from replica virtual machines stored remotely for long-term retention.

**Saves bandwidth** - In a typical remote branch office/headquarters deployment you need an appropriate amount of provisioned bandwidth to transfer backup data between sites. If you create a replication and failover strategy, in addition to your data backup strategy, you can reduce the amount of redundant data sent over the network. By backing up the replica virtual machine data rather than the primary, you save the overhead of sending the backed-up data over the network.

**Enables hoster backup** - You can use a hosted datacenter as a replica site, with no need for a secondary datacenter. In this case, the hoster SLA requires consistent backup of replica virtual machines.

A replica virtual machine is turned off until a failover is initiated, and VSS can't guarantee an application-consistent backup for a replica virtual machine. Thus the backup of a replica virtual machine will be crash-consistent only. If crash-consistency can't be guaranteed, then the backup will fail and this might occur in a number of conditions:

- The replica virtual machine isn't healthy and is in a critical state.
- The replica virtual machine is resynchronizing (in the Resynchronization in Progress or Resynchronization Required state).
- Initial replication between the primary and secondary site is in progress or pending for the virtual machine.

- .hrl logs are being applied to the replica virtual machine, or a previous action to apply the .hrl logs on the virtual disk failed, or was canceled or interrupted.
- Migration or failover of the replica virtual machine is in progress

## Recover backed up virtual machines

When you can recover a backed up virtual machine, you use the Recovery wizard to select the virtual machine and the specific recovery point. To open the Recovery Wizard and recover a virtual machine:

1. In the MABS Administrator console, type the name of the VM, or expand the list of protected items and select the VM you want to recover.
2. In the **Recovery points for** pane, on the calendar, click any date to see the recovery points available. Then in the **Path** pane, select the recovery point you want to use in the Recovery wizard.
3. From the **Actions** menu, click **Recover** to open the Recovery Wizard.

The VM and recovery point you selected appear in the **Review Recovery Selection** screen. Click **Next**.

4. On the **Select Recovery Type** screen, select where you want to restore the data and then click **Next**.
  - **Recover to original instance:** When you recover to the original instance, the original VHD is deleted. MABS recovers the VHD and other configuration files to the original location using Hyper-V VSS writer. At the end of the recovery process, virtual machines are still highly available. The resource group must be present for recovery. If it isn't available, recover to an alternate location and then make the virtual machine highly available.
  - **Recover as virtual machine to any host:** MABS supports alternate location recovery (ALR), which provides a seamless recovery of a protected Hyper-V virtual machine to a different Hyper-V host, independent of processor architecture. Hyper-V virtual machines that are recovered to a cluster node will not be highly available. If you choose this option, the Recovery Wizard presents you with an additional screen for identifying the destination and destination path.
  - **Copy to a network folder:** MABS supports item-level recovery (ILR), which allows you to do item-level recovery of files, folders, volumes, and virtual hard disks (VHDs) from a host-level backup of Hyper-V virtual machines to a network share or a volume on a MABS protected server. The MABS protection agent doesn't have to be installed inside the guest to perform item-level recovery. If you choose this option, the Recovery Wizard presents you with an additional screen for identifying the destination and destination path.

5. In **Specify Recovery Options** configure the recovery options and click **Next**.
  - If you are recovering a VM over low bandwidth, click **Modify** to enable **Network bandwidth usage throttling**. After turning on the throttling option, you can specify the amount of bandwidth you want to make available and the time when that bandwidth is available.
  - Select **Enable SAN based recovery using hardware snapshots** if you have configured your network.
  - Select **Send an e-mail when the recovery completes** and then provide the email addresses, if you want email notifications sent once the recovery process completes.
6. In the Summary screen, make sure all details are correct. If the details aren't correct, or you want to make a change, click **Back**. If you are satisfied with the settings, click **Recover** to start the recovery process.
7. The **Recovery Status** screen provides information about the recovery job.

## Next steps

# Back up VMware VMs with Azure Backup Server

1/16/2020 • 12 minutes to read • [Edit Online](#)

This article explains how to back up VMware VMs running on VMware ESXi hosts/vCenter Server to Azure using Azure Backup Server.

This article explains how to:

- Set up a secure channel so that Azure Backup Server can communicate with VMware servers over HTTPS.
- Set up a VMware account that Azure Backup Server uses to access the VMware server.
- Add the account credentials to Azure Backup.
- Add the vCenter or ESXi server to Azure Backup Server.
- Set up a protection group that contains the VMware VMs you want to back up, specify backup settings, and schedule the backup.

## Before you start

- Verify that you're running a version of vCenter/ESXi that's supported for backup. Refer to the support matrix [here](#).
- Make sure you've set up Azure Backup Server. If you haven't, [do that](#) before you start. You should be running Azure Backup Server with the latest updates.

## Create a secure connection to the vCenter Server

By default, Azure Backup Server communicates with VMware servers over HTTPS. To set up the HTTPS connection, download the VMware Certificate Authority (CA) certificate, and import it on the Azure Backup Server.

### Before you begin

- If you don't want to use HTTPS, you can [disable HTTPS certificate validation for all VMware servers](#).
- You typically connect from a browser on the Azure Backup Server machine to the vCenter/ESXi server using the vSphere Web Client. The first time you do this, the connection isn't secure and will show the following.
- It's important to understand how Azure Backup Server handles backups.
  - As a first step Azure Backup Server backs up data to local disk storage. Azure Backup Server uses a storage pool, a set of disks and volumes on which Azure Backup Server stores disk recovery points for its protected data. The storage pool can be directly attached storage (DAS), a fiber channel SAN, or iSCSI storage device or SAN. It's important to ensure that you have sufficient storage for local backup of your VMware VM data.
  - Azure Backup Server then backs up from the local disk storage to Azure.
  - [Get help](#) to figure out how much storage space you need. The information is for DPM but can be used for Azure Backup Server too.

### Set up the certificate

Set up a secure channel as follows:

1. In the browser on Azure Backup Server, enter the vSphere Web Client URL. If the login page doesn't appear, verify the connection and browser proxy settings.

**Getting Started**

To access vSphere remotely, use the vSphere Web Client.

[Log in to vSphere Web Client](#)

For help, see  
[vSphere Documentation](#)

**vCenter Servers**

**For Administrators**

**Web-Based Datastore Browser**

Use your web browser to find and download files (for example, virtual machine and virtual disk files).

[Browse datastores in the vSphere inventory](#)

**For Developers**

**vSphere Web Services SDK**

Learn about our latest SDKs, Toolkits, and APIs for managing VMware ESX, ESXi, and VMware vCenter. Get sample code, reference documentation, participate in our Forum Discussions, and view our latest Sessions and Webinars.

[Learn more about the Web Services SDK](#)

[Browse objects managed by vSphere](#)

[Download trusted root CA certificates](#)

2. On the vSphere Web Client login page, click **Download trusted root CA certificates**.

**For Administrators**

**Web-Based Datastore Browser**

Use your web browser to find and download files (for example, virtual machine and virtual disk files).

[Browse datastores in the vSphere inventory](#)

**For Developers**

**vSphere Web Services SDK**

Learn about our latest SDKs, Toolkits, and APIs for managing VMware ESX, ESXi, and VMware vCenter. Get sample code, reference documentation, participate in our Forum Discussions, and view our latest Sessions and Webinars.

[Learn more about the Web Services SDK](#)

[Browse objects managed by vSphere](#)

[Download trusted root CA certificates](#)

3. A file named **download** is downloaded. Depending on your browser, you receive a message that asks whether to open or save the file.



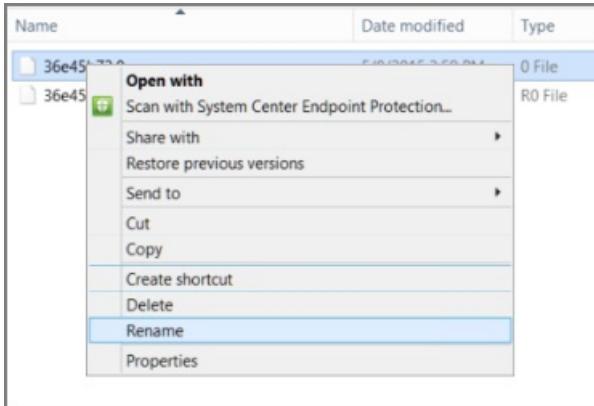
4. Save the file on the Azure Backup Server machine with a .zip extension.

5. Right-click **download.zip** > **Extract All**. The .zip file extracts its contents to the **certs** folder, which contains:

- The root certificate file with an extension that begins with a numbered sequence like .0 and .1.
- The CRL file has an extension that begins with a sequence like .r0 or .r1. The CRL file is associated with a certificate.

| Name        | Date modified     | Type    | Size |
|-------------|-------------------|---------|------|
| 36e45b73.0  | 5/8/2015 3:59 PM  | 0 File  | 2 KB |
| 36e45b73.r0 | 4/19/2017 3:01 AM | R0 File | 1 KB |

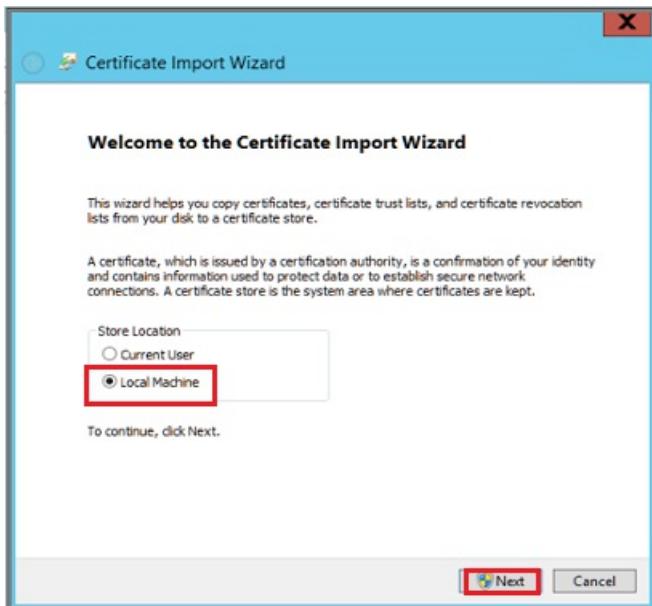
6. In the **certs** folder, right-click the root certificate file > **Rename**.



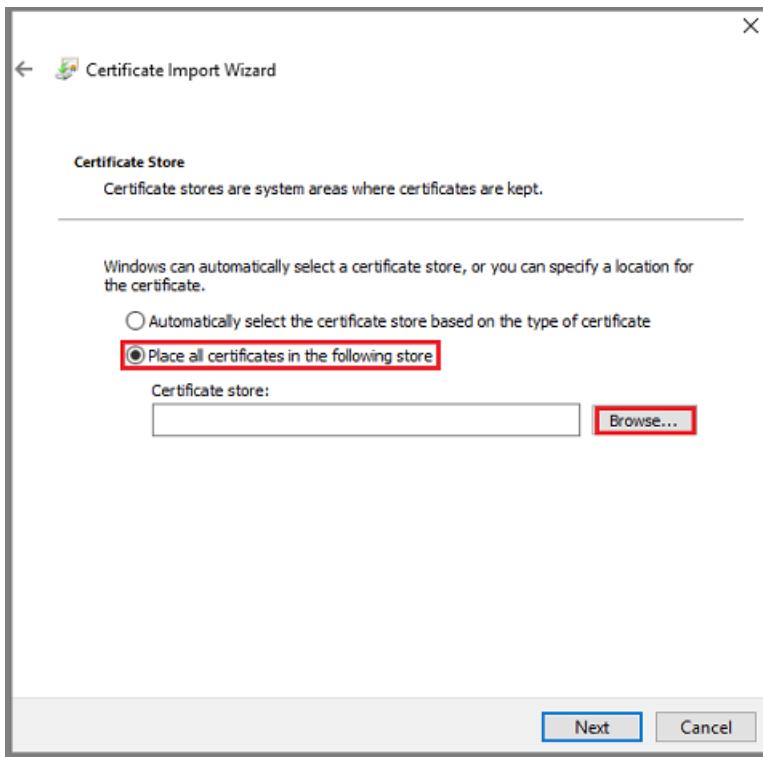
7. Change the root certificate's extension to .crt, and confirm. The file icon changes to one that represents a root certificate.

8. Right-click the root certificate and from the pop-up menu, select **Install Certificate**.

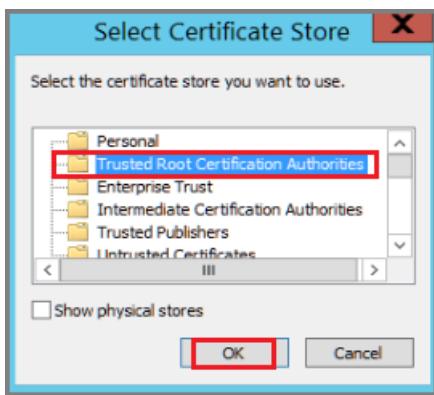
9. In **Certificate Import Wizard**, select **Local Machine** as the destination for the certificate, and then click **Next**. Confirm if you're asked if you want to allow changes to the computer.



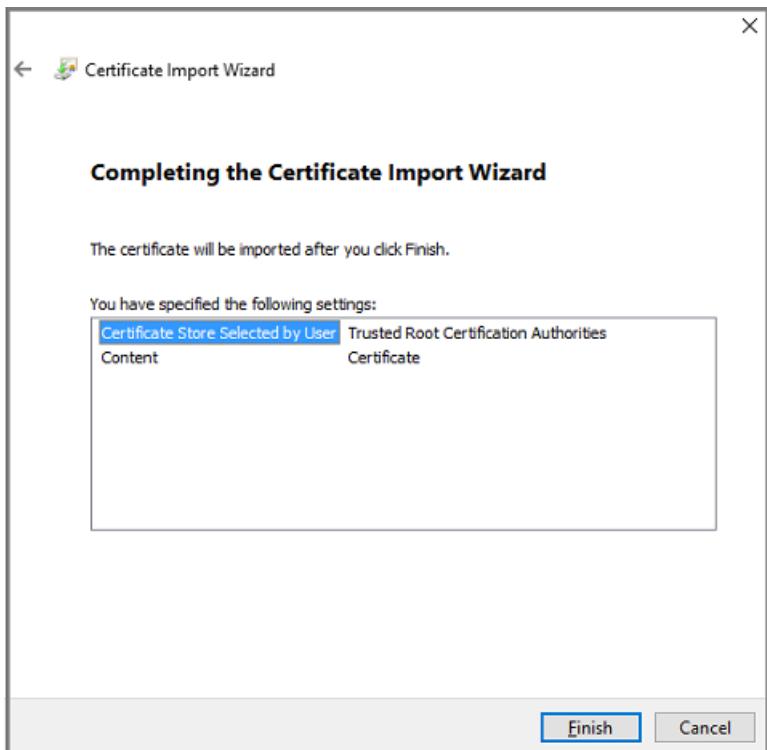
10. On the **Certificate Store** page, select **Place all certificates in the following store**, and then click **Browse** to choose the certificate store.



11. In **Select Certificate Store**, select **Trusted Root Certification Authorities** as the destination folder for the certificates, and then click **OK**.



12. In **Completing the Certificate Import Wizard**, verify the folder, and then click **Finish**.



13. After the certificate import is confirmed, sign in to the vCenter Server to confirm that your connection is secure.

#### Disable HTTPS certificate validation

If you have secure boundaries within your organization, and don't want to use the HTTPS protocol between VMware servers and the Azure Backup Server machine, disable HTTPS as follows:

1. Copy and paste the following text into a .txt file.

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\VMWare]
"IgnoreCertificateValidation"=dword:00000001
```

2. Save the file on the Azure Backup Server machine with the name **DisableSecureAuthentication.reg**.
3. Double-click the file to activate the registry entry.

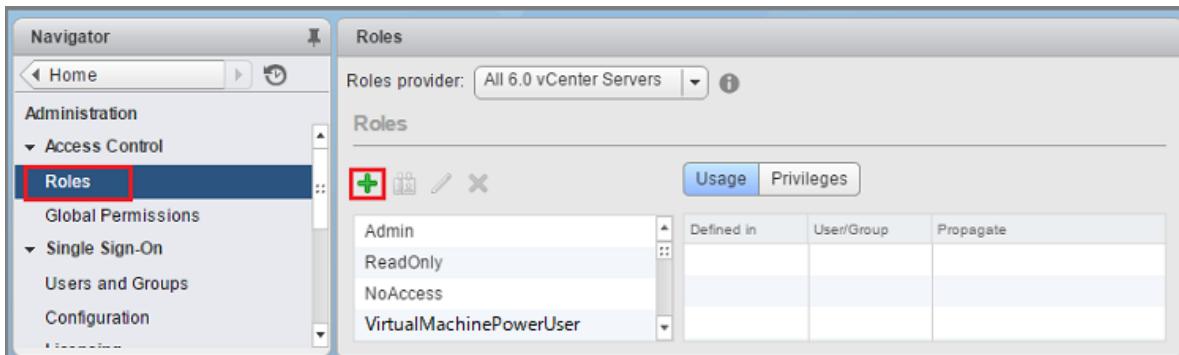
## Create a VMware role

The Azure Backup Server needs a user account with permissions to access v-Center Server/ESXi host. Create a VMware role with specific privileges, and then associate a user account with the role.

1. Sign in to the vCenter Server (or ESXi host if you're not using vCenter Server).
2. In the **Navigator** panel, click **Administration**.



3. In **Administration > Roles**, click the add role icon (the + symbol).



4. In **Create Role > Role name**, enter *BackupAdminRole*. The role name can be whatever you like, but it should be recognizable for the role's purpose.
5. Select the privileges as summarized in the table below, and then click **OK**. The new role appears on the list in the **Roles** panel.
- Click the icon next to the parent label to expand the parent and view the child privileges.
  - To select the VirtualMachine privileges, you need to go several levels into the parent child hierarchy.
  - You don't need to select all child privileges within a parent privilege.



## Role permissions

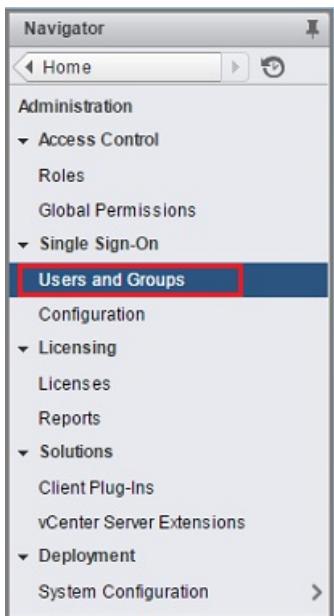
| PRIVILEGES FOR VCENTER 6.5 AND ABOVE<br>USER ACCOUNT | PRIVILEGES FOR VCENTER 6.0 USER<br>ACCOUNT | PRIVILEGES FOR VCENTER 5.5 USER<br>ACCOUNT |
|------------------------------------------------------|--------------------------------------------|--------------------------------------------|
| Datastore.AllocateSpace                              |                                            |                                            |
| Datastore.Browse datastore                           | Datastore.AllocateSpace                    | Network.Assign                             |

| PRIVILEGES FOR VCENTER 6.5 AND ABOVE<br>USER ACCOUNT                     | PRIVILEGES FOR VCENTER 6.0 USER<br>ACCOUNT                   | PRIVILEGES FOR VCENTER 5.5 USER<br>ACCOUNT     |
|--------------------------------------------------------------------------|--------------------------------------------------------------|------------------------------------------------|
| Datastore.Low-level file operations                                      | Global.Manage custom attributes                              | Datastore.AllocateSpace                        |
| Datastore cluster.Configure a<br>datastore cluster                       | Global.Set custom attribute                                  | VirtualMachine.Config.ChangeTracking           |
| Global.Disable methods                                                   | Host.Local operations.Create virtual<br>machine              | VirtualMachine.State.RemoveSnapshot            |
| Global.Enable methods                                                    | Network. Assign network                                      | VirtualMachine.State.CreateSnapshot            |
| Global.Licenses                                                          | Resource. Assign virtual machine to<br>resource pool         | VirtualMachine.Provisioning.DiskRando<br>mRead |
| Global.Log event                                                         | Virtual machine.Configuration.Add new<br>disk                | VirtualMachine.Interact.PowerOff               |
| Global.Manage custom attributes                                          | Virtual<br>machine.Configuration.Advanced                    | VirtualMachine.Inventory.Create                |
| Global.Set custom attribute                                              | Virtual machine.Configuration.Disk<br>change tracking        | VirtualMachine.Config.AddNewDisk               |
| Network.Assign network                                                   | Virtual machine.Configuration.Host<br>USB device             | VirtualMachine.Config.HostUSBDevice            |
| Resource. Assign virtual machine to<br>resource pool                     | Virtual machine.Configuration.Query<br>unowned files         | VirtualMachine.Config.AdvancedConfig           |
| Virtual machine.Configuration.Add new<br>disk                            | Virtual machine.Configuration.Swapfile<br>placement          | VirtualMachine.Config.SwapPlacement            |
| Virtual<br>machine.Configuration.Advanced                                | Virtual machine.Interaction.Power Off                        | Global.ManageCustomFields                      |
| Virtual machine.Configuration.Disk<br>change tracking                    | Virtual machine.Inventory. Create new                        |                                                |
| Virtual machine.Configuration.Disk<br>lease                              | Virtual machine.Provisioning.Allow disk<br>access            |                                                |
| Virtual machine.Configuration.Extend<br>virtual disk                     | Virtual machine.Provisioning. Allow<br>read-only disk access |                                                |
| Virtual machine.Guest<br>Operations.Guest Operation<br>Modifications     | Virtual machine.Snapshot<br>management.Create snapshot       |                                                |
| Virtual machine.Guest<br>Operations.Guest Operation Program<br>Execution | Virtual machine.Snapshot<br>management.Remove Snapshot       |                                                |
| Virtual machine.Guest<br>Operations.Guest Operation Queries              |                                                              |                                                |

| PRIVILEGES FOR VCENTER 6.5 AND ABOVE<br>USER ACCOUNT                       | PRIVILEGES FOR VCENTER 6.0 USER<br>ACCOUNT | PRIVILEGES FOR VCENTER 5.5 USER<br>ACCOUNT |
|----------------------------------------------------------------------------|--------------------------------------------|--------------------------------------------|
| Virtual machine .Interaction .Device connection                            |                                            |                                            |
| Virtual machine .Interaction .Guest operating system management by VIX API |                                            |                                            |
| Virtual machine .Inventory.Register                                        |                                            |                                            |
| Virtual machine .Inventory.Remove                                          |                                            |                                            |
| Virtual machine .Provisioning.Allow disk access                            |                                            |                                            |
| Virtual machine .Provisioning.Allow read-only disk access                  |                                            |                                            |
| Virtual machine .Provisioning.Allow virtual machine download               |                                            |                                            |
| Virtual machine .Snapshot management. Create snapshot                      |                                            |                                            |
| Virtual machine .Snapshot management.Remove Snapshot                       |                                            |                                            |
| Virtual machine .Snapshot management.Revert to snapshot                    |                                            |                                            |
| vApp.Add virtual machine                                                   |                                            |                                            |
| vApp.Assign resource pool                                                  |                                            |                                            |
| vApp.Unregister                                                            |                                            |                                            |

## Create a VMware account

1. In vCenter Server **Navigator** panel, click **Users and Groups**. If you don't use vCenter Server, create the account on the appropriate ESXi host.



The **vCenter Users and Groups** panel appear.

2. In the **vCenter Users and Groups** panel, select the **Users** tab, and then click the add users icon (the + symbol).

A screenshot of the vCenter Users and Groups interface. The top navigation bar has tabs for 'Users', 'Solution Users', and 'Groups'. Below it, a 'Domain' dropdown is set to 'Contoso.local'. A green plus sign icon is located in the top-left of the main table area. The table has columns: Username, First Name, Last Name, Email, Description, Locked, Disabled, and Domain. Three rows are visible: 'BackupAdmin6.0' (Maanas Saran), 'DPM-BACKUP' (DPM-BA...), and 'BackupAdmin001' (Mark Galioto). A 'Filter' search bar is at the top right.

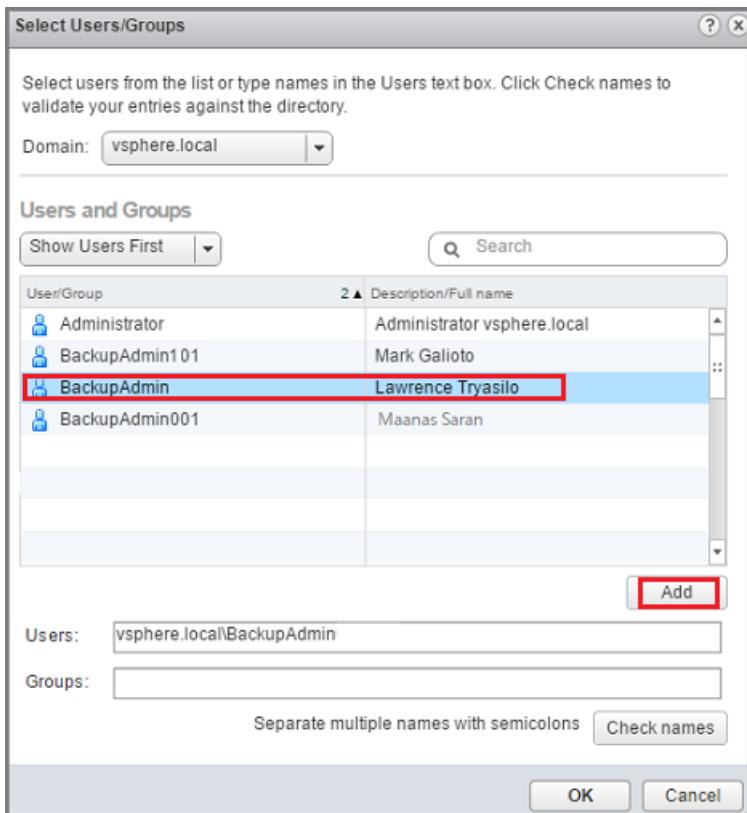
3. In **New User** dialog box, add the user information > **OK**. In this procedure, the username is BackupAdmin.

A screenshot of the 'New User' dialog box. It contains fields for User name ('BackupAdmin'), Password ('\*\*\*\*\*'), Confirm password ('\*\*\*\*\*'), First name ('Lawrence'), Last name ('Tryasilo'), Email address ('user@contoso.com'), and Description ('Testrole'). At the bottom are 'OK' and 'Cancel' buttons.

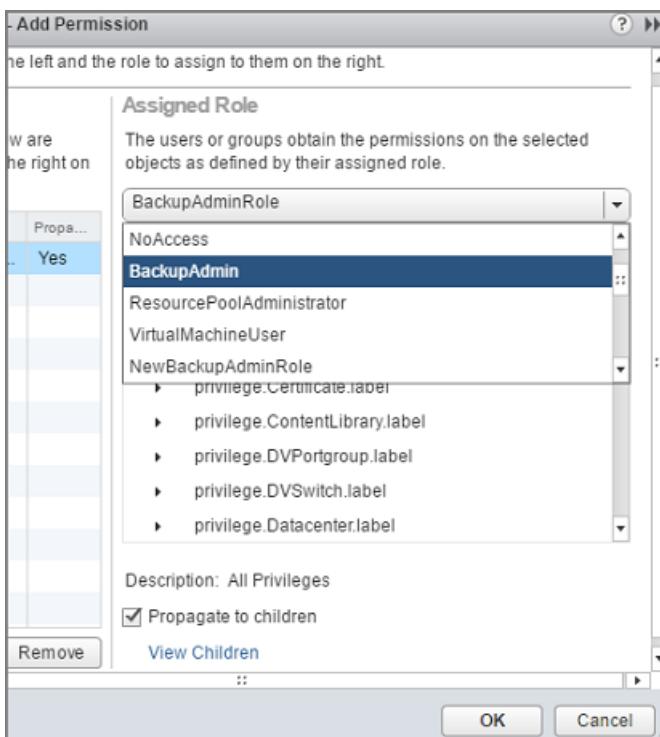
4. To associate the user account with the role, in the **Navigator** panel, click **Global Permissions**. In the **Global Permissions** panel, select the **Manage** tab, and then click the add icon (the + symbol).

5. In **Global Permission Root - Add Permission**, click **Add** to choose the user or group.

6. In **Select Users/Groups**, choose **BackupAdmin > Add**. In **Users**, the *domain\username* format is used for the user account. If you want to use a different domain, choose it from the **Domain** list. Click **OK** to add the selected users to the **Add Permission** dialog box.



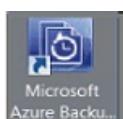
7. In **Assigned Role**, from the drop-down list, select **BackupAdminRole** > **OK**.



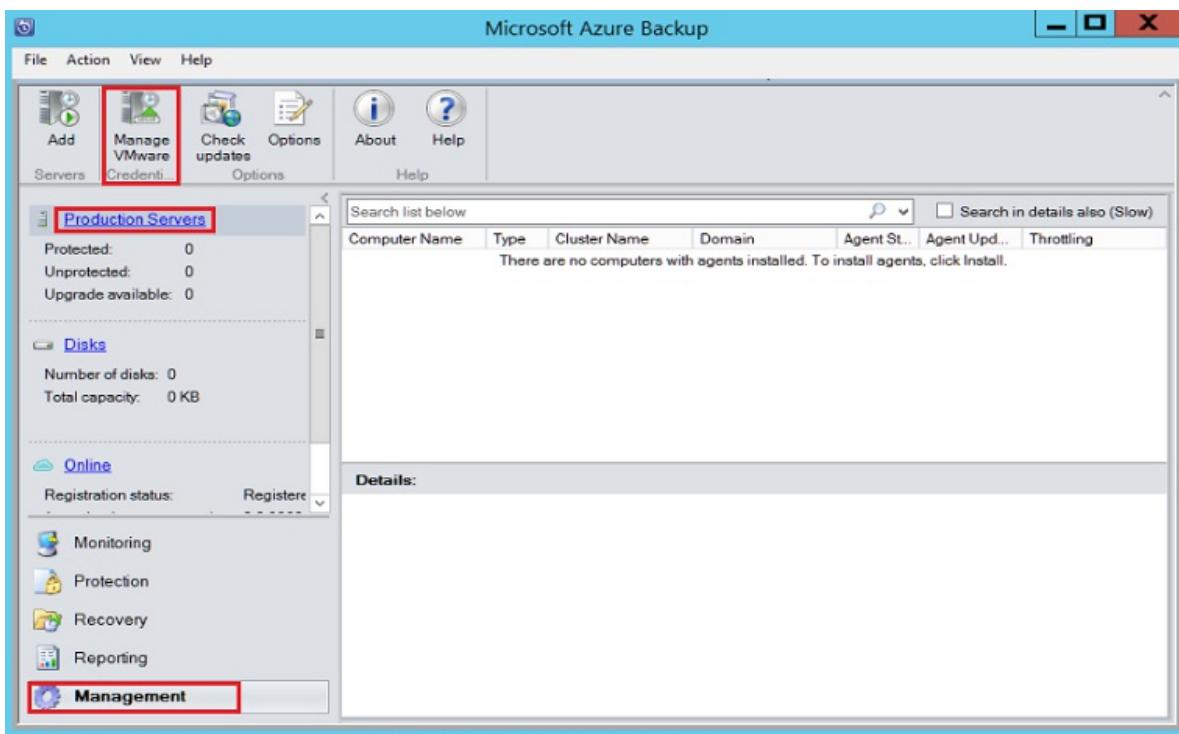
On the **Manage** tab in the **Global Permissions** panel, the new user account and the associated role appear in the list.

## Add the account on Azure Backup Server

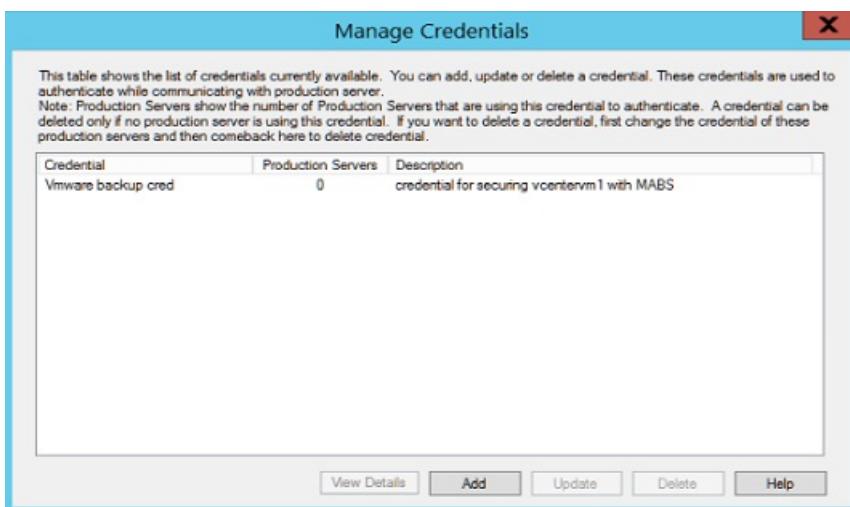
1. Open Azure Backup Server. If you can't find the icon on the desktop, open Microsoft Azure Backup from the apps list.



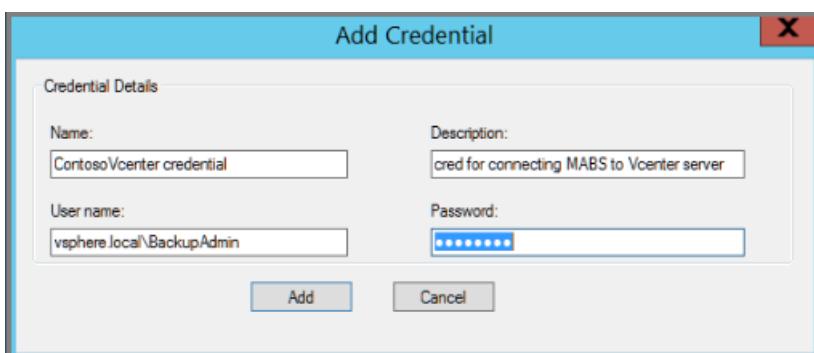
2. In the Azure Backup Server console, click **Management > Production Servers > Manage VMware**.



3. In the **Manage Credentials** dialog box, click **Add**.



4. In **Add Credential**, enter a name and a description for the new credential, and specify the username and password you defined on the VMware server. The name, *Contoso Vcenter credential* is used to identify the credential in this procedure. If the VMware server and Azure Backup Server aren't in the same domain, specify the domain in the user name.



5. Click **Add** to add the new credential.

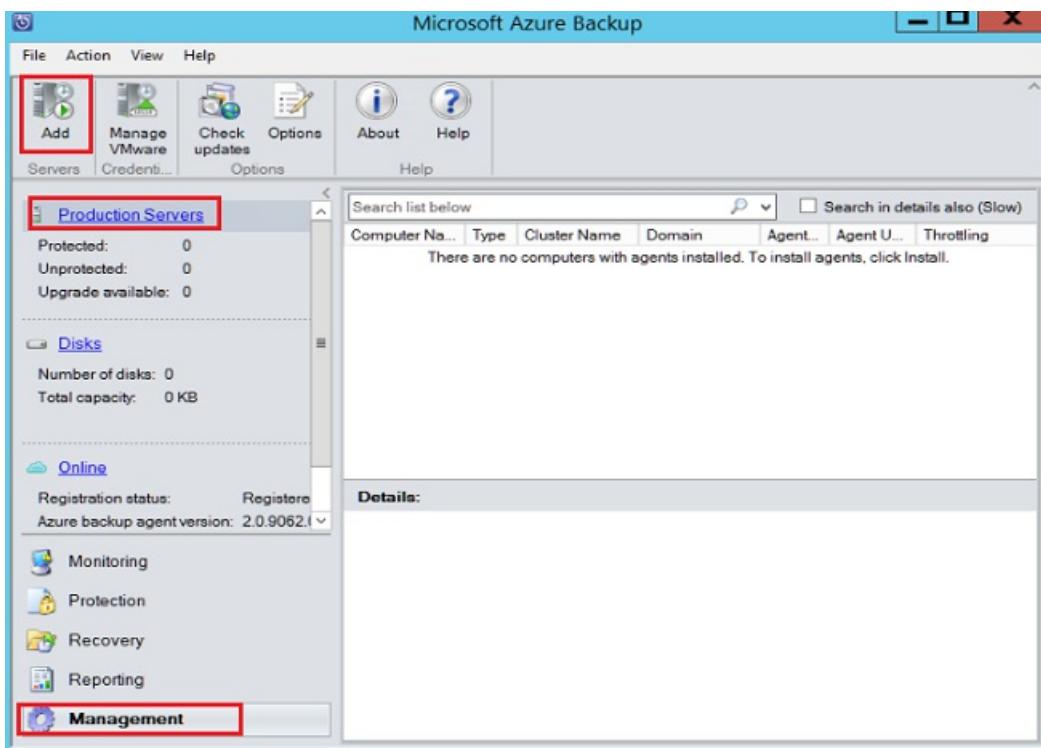
| Manage Credentials                                                                                                                                                                               |                    |                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|----------------------------------------------|
| This table shows the list of credentials currently available. You can add, update or delete a credential. These credentials are used to authenticate while communicating with production server. |                    |                                              |
| Credential                                                                                                                                                                                       | Production Servers | Description                                  |
| Contoso Vcenter credential                                                                                                                                                                       | 0                  | cred for connecting MABS to Vcenter server   |
| Vmware backup cred                                                                                                                                                                               | 0                  | credential for securing vcentervm1 with MABS |

[View Details](#) [Add](#) [Update](#) [Delete](#) [Help](#)

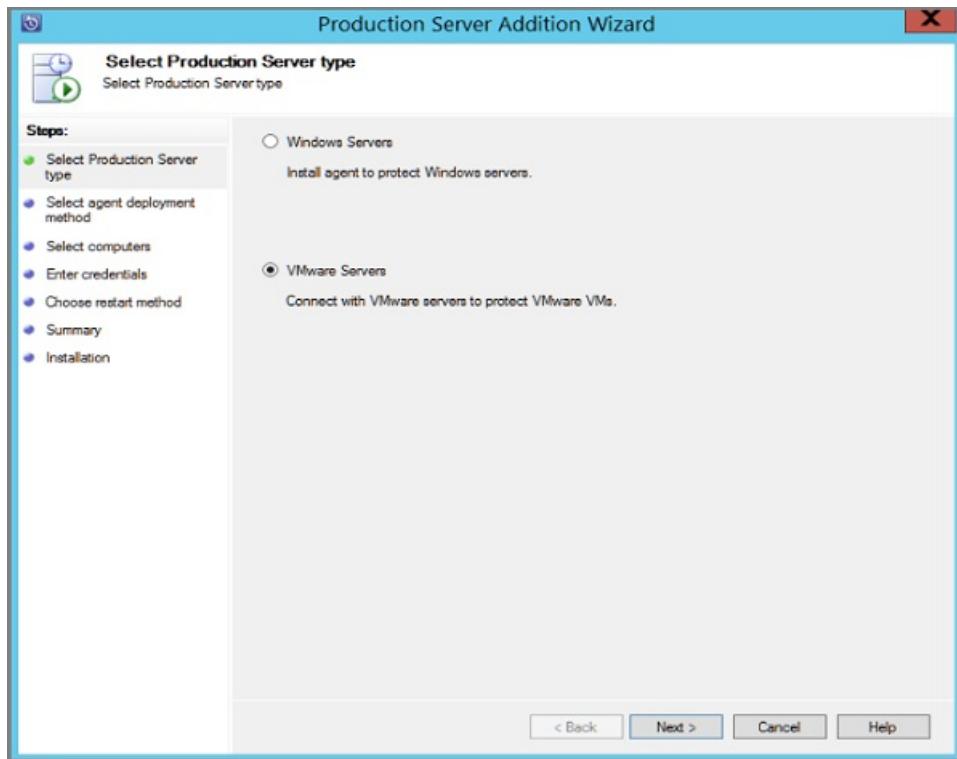
## Add the vCenter Server

Add the vCenter Server to Azure Backup Server.

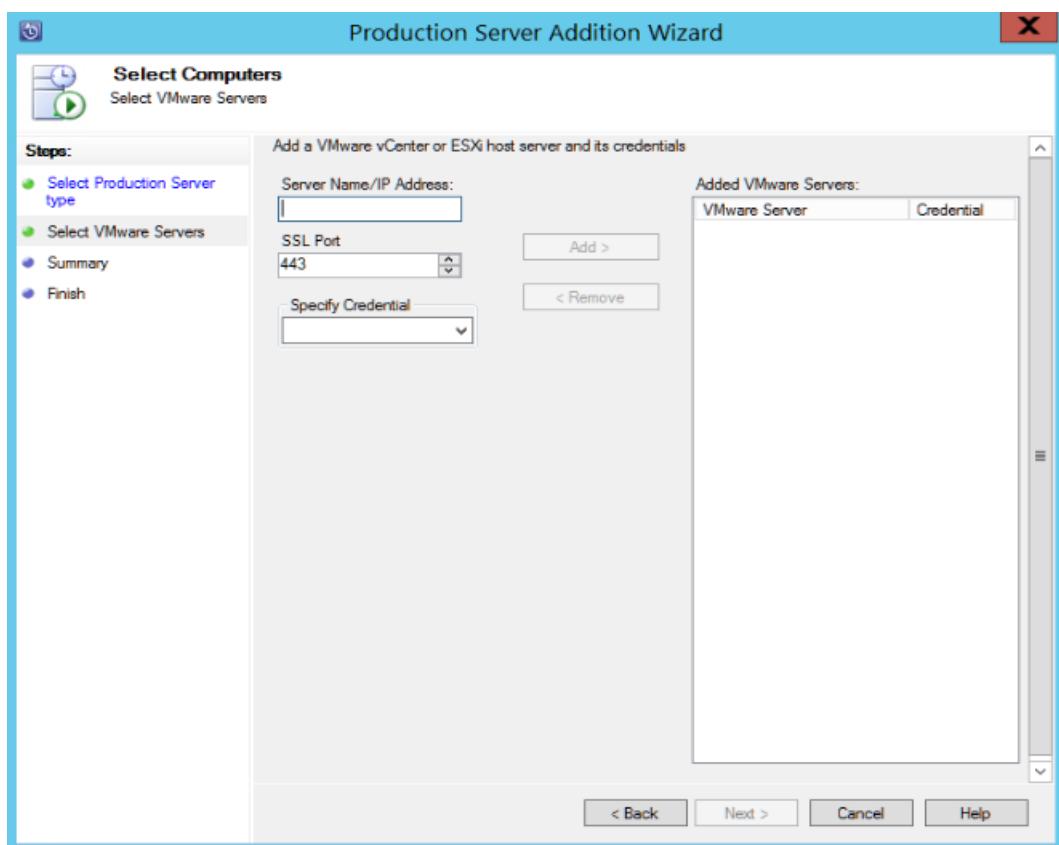
1. In the Azure Backup Server console, click **Management > Production Servers > Add**.



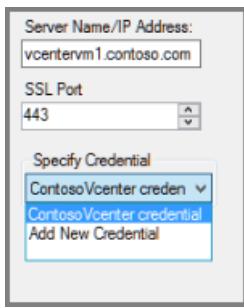
2. In **Production Server Addition Wizard > Select Production Server type** page, select **VMware Servers**, and then click **Next**.



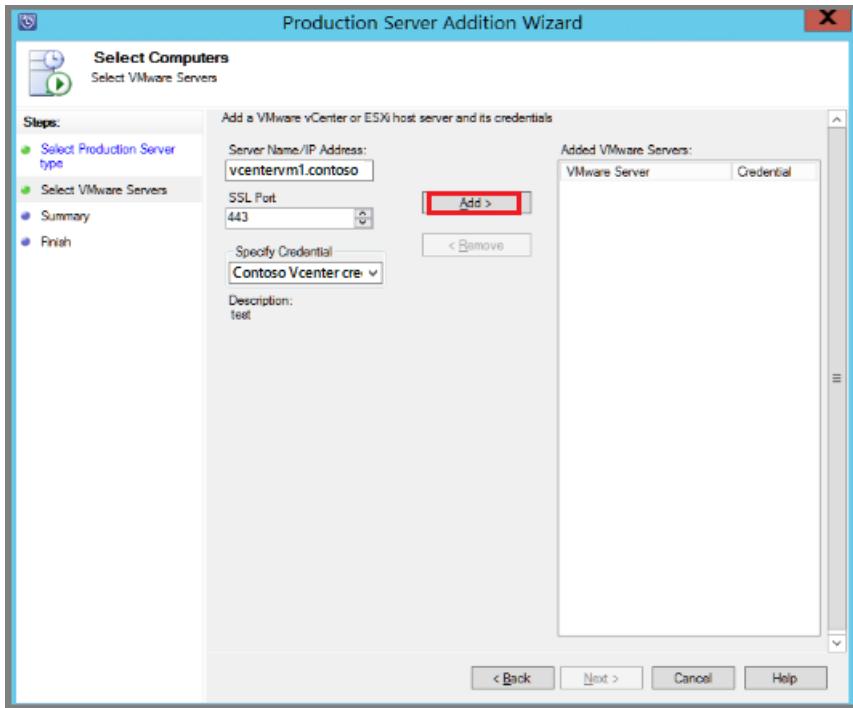
3. In **Select Computers Server Name/IP Address**, specify the FQDN or IP address of the VMware server. If all the ESXi servers are managed by the same vCenter, specify the vCenter name. Otherwise, add the ESXi host.



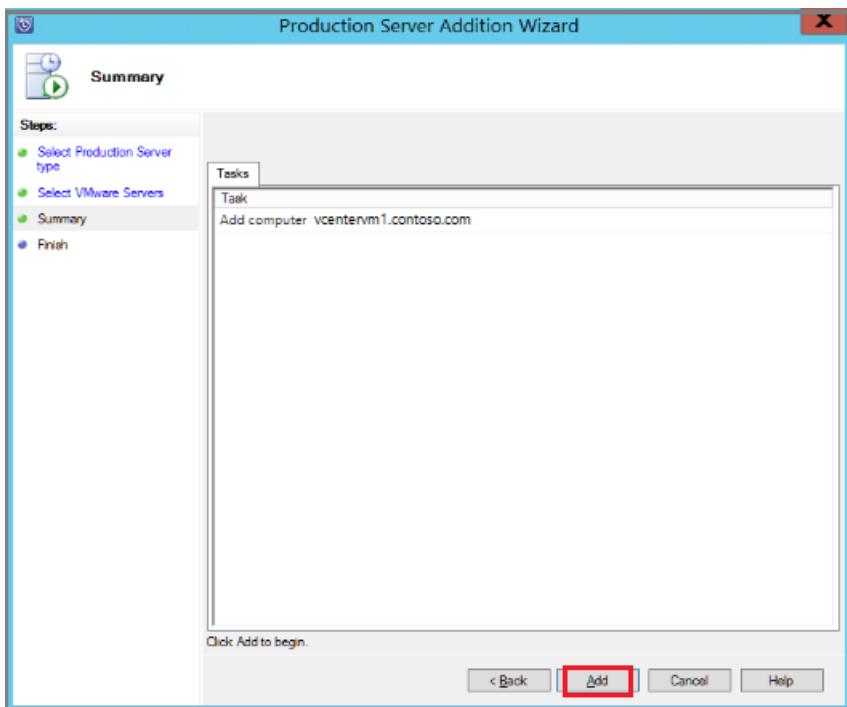
4. In **SSL Port**, enter the port that's used to communicate with the VMware server. 443 is the default port, but you can change it if your VMware server listens on a different port.
5. In **Specify Credential**, select the credential that you created earlier.



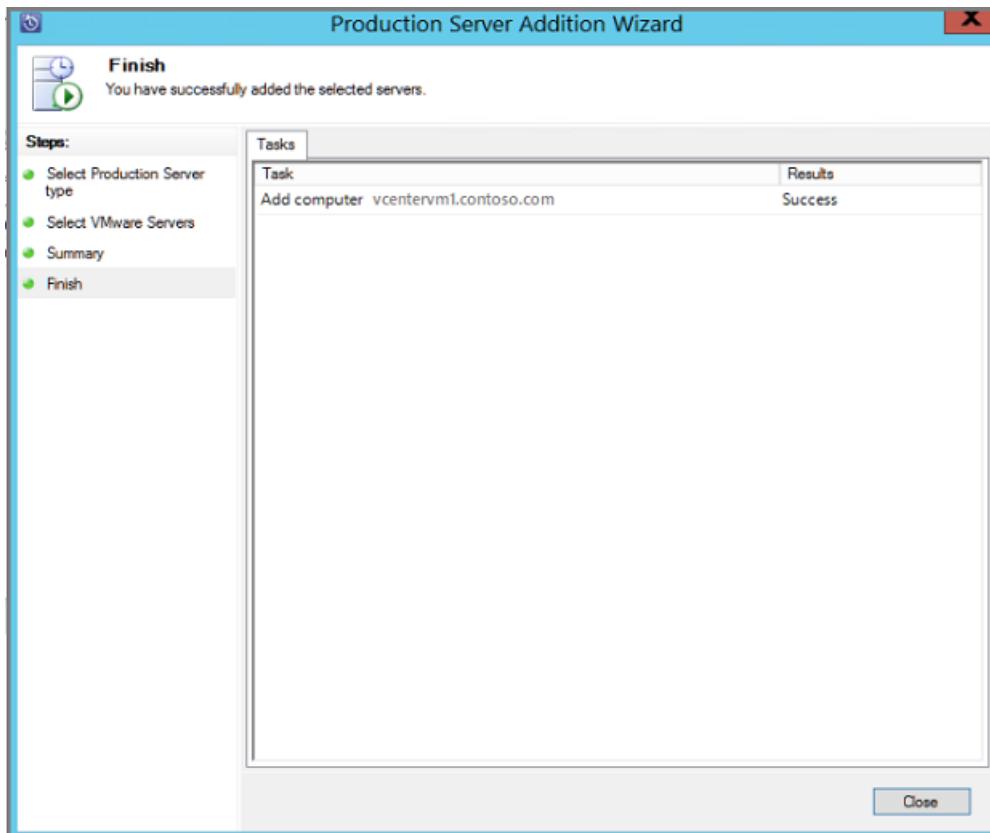
6. Click **Add** to add the VMware server to the servers list. Then click **Next**.



7. In the **Summary** page, click **Add** to add the VMware server to Azure Backup Server. The new server is added immediately, no agent is needed on the VMware server.



8. Verify settings on the **Finish** page.

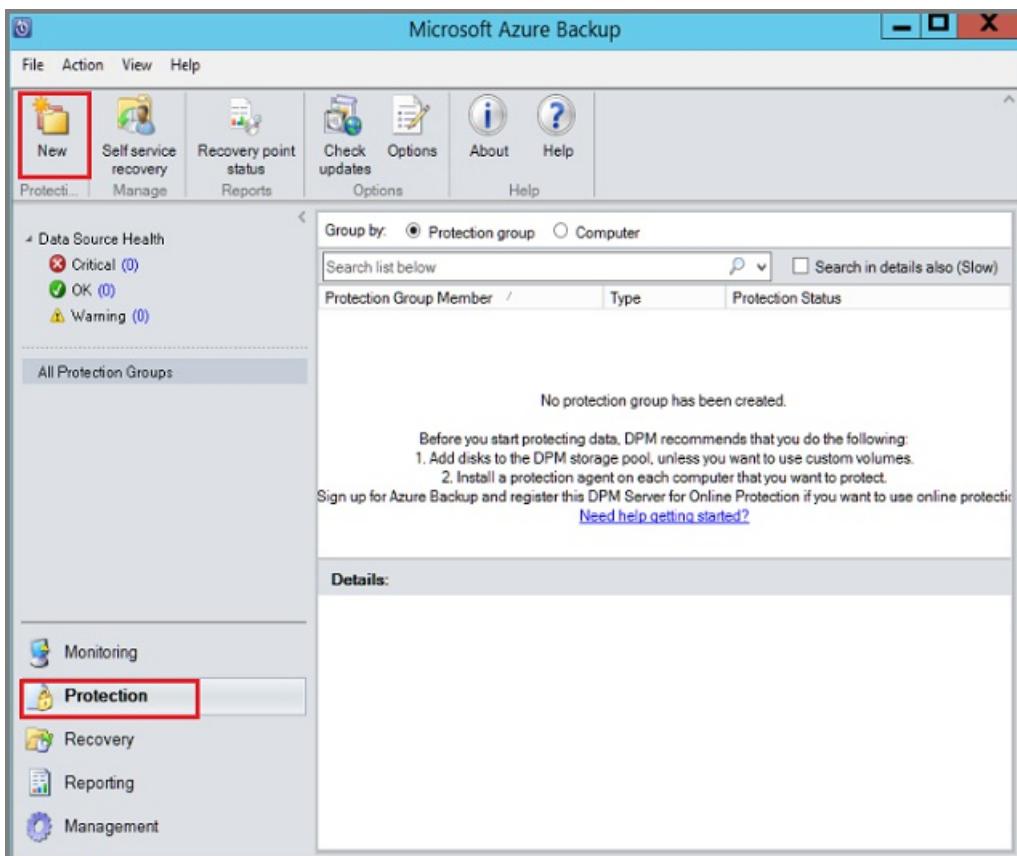


If you have multiple ESXi hosts that aren't managed by vCenter server, or you have multiple instances of vCenter Server, you need to rerun the wizard to add the servers.

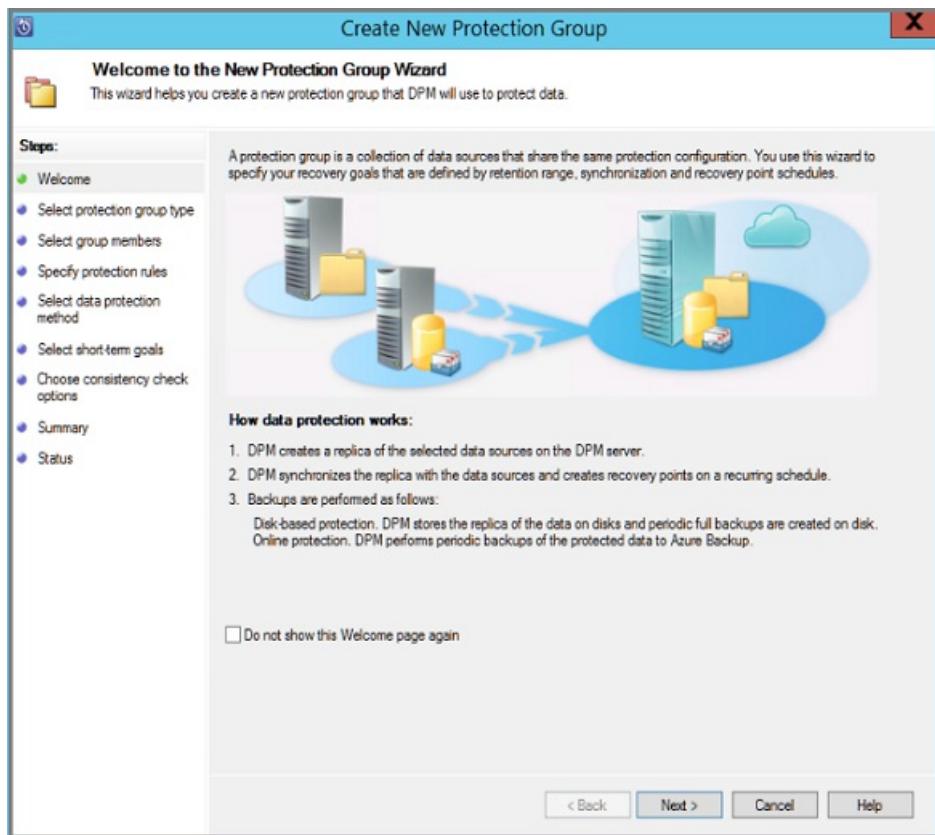
## Configure a protection group

Add VMware VMs for backup. Protection groups gather multiple VMs and apply the same data retention and backup settings to all VMs in the group.

1. In the Azure Backup Server console, click **Protection**, > **New**.



2. In the **Create New Protection Group** wizard welcome page, click **Next**.

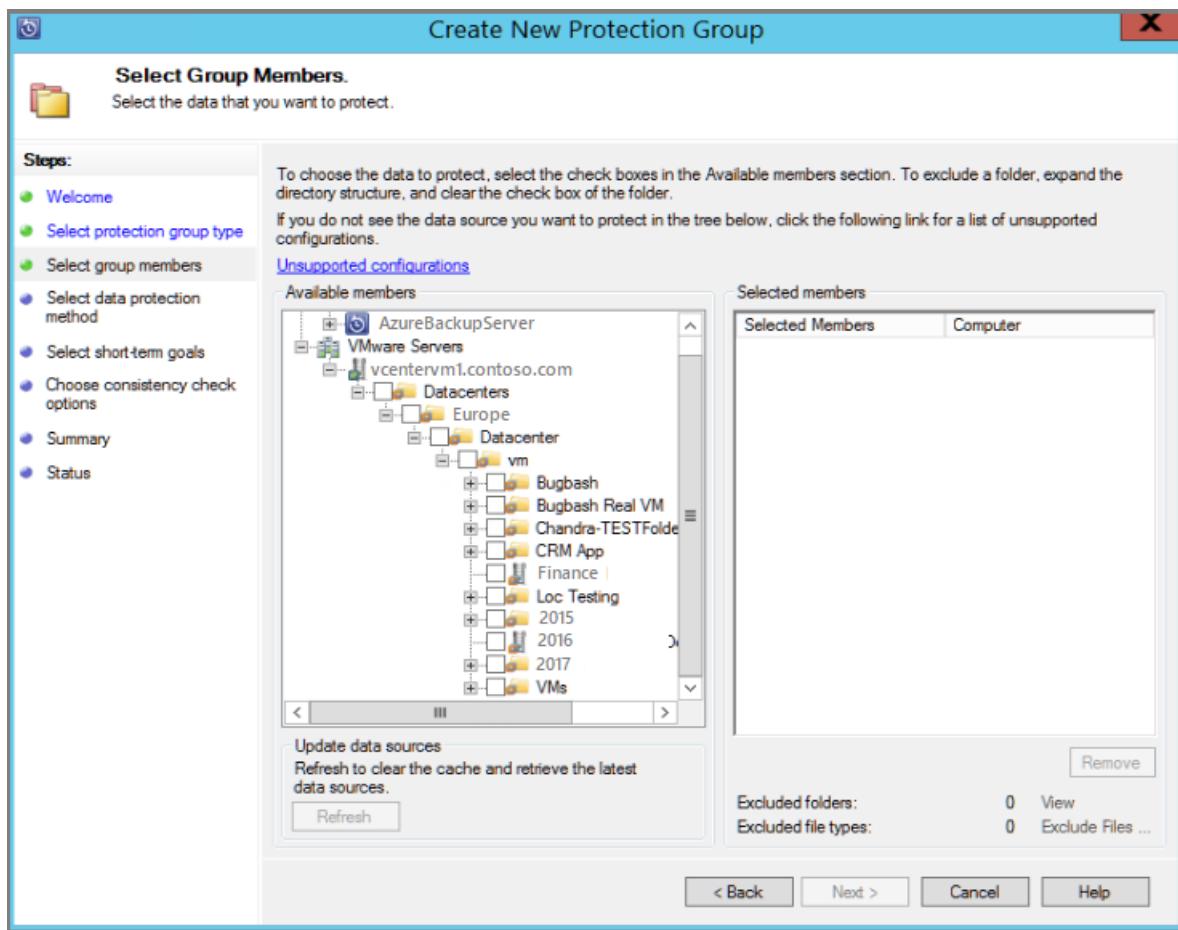


3. On the **Select Protection group type** page, select **Servers** and then click **Next**. The **Select group members** page appears.

4. In **Select group members**, select the VMs (or VM folders) that you want to back up. Then click **Next**.

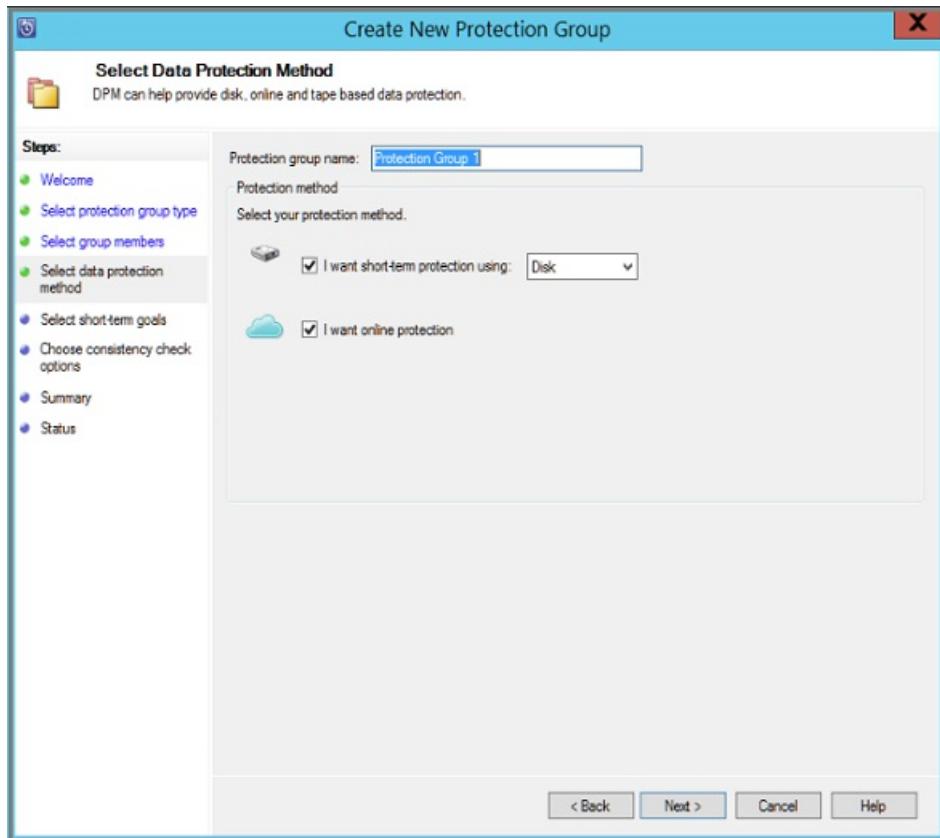
- When you select a folder, or VMs or folders inside that folder are also selected for backup. You can uncheck folders or VMs you don't want to back up.

5. If a VM or folder is already being backed up, you can't select it. This ensures that duplicate recovery points aren't created for a VM.



6. In **Select Data Protection Method** page, enter a name for the protection group, and protection settings.

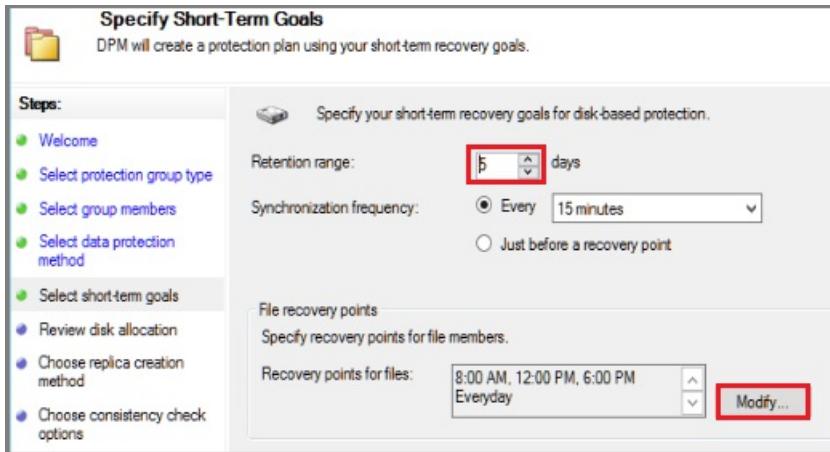
To back up to Azure, set short-term protection to **Disk** and enable online protection. Then click **Next**.



7. In **Specify Short-Term Goals**, specify how long you want to keep data backed up to disk.

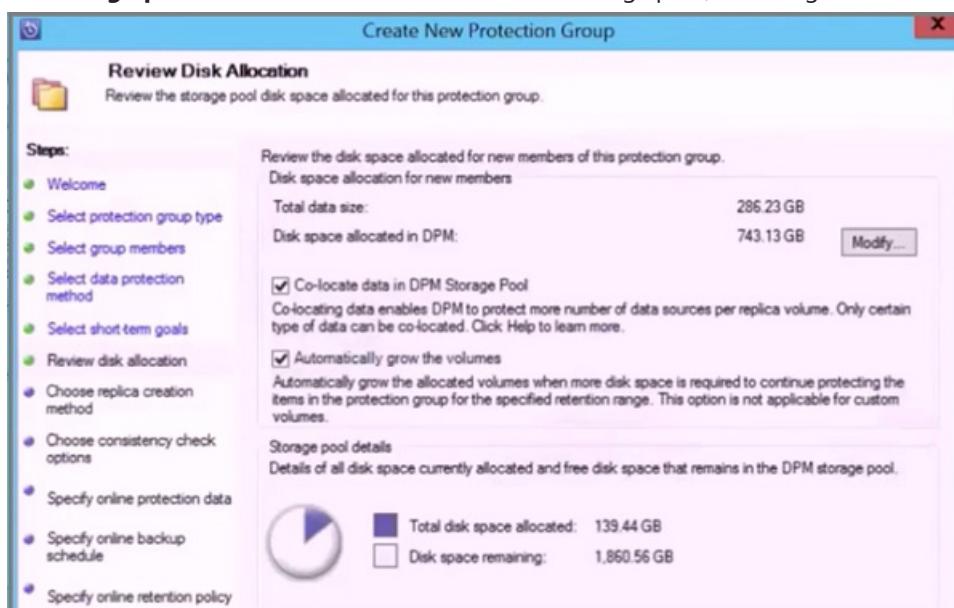
- In **Retention Range**, specify how many days disk recovery points should be kept.
- In **Synchronization frequency**, specify how often disk recovery points are taken.

- If you don't want to set a backup interval, you can check **Just before a recovery point** so that a backup runs just before each recovery point is scheduled.
- Short-term backups are full backups and not incremental.
- Click **Modify** to change the times/dates when short-term backups occur.



#### 8. In **Review Disk Allocation**, review the disk space provided for the VM backups. for the VMs.

- The recommended disk allocations are based on the retention range you specified, the type of workload, and the size of the protected data. Make any changes required, and then click **Next**.
- **Data size:** Size of the data in the protection group.
- **Disk space:** The recommended amount of disk space for the protection group. If you want to modify this setting, you should allocate total space that is slightly larger than the amount that you estimate each data source grows.
- **Colocate data:** If you turn on colocation, multiple data sources in the protection group can map to a single replica and recovery point volume. Colocation isn't supported for all workloads.
- **Automatically grow:** If you turn on this setting, if data in the protected group outgrows the initial allocation, Azure Backup Server tries to increase the disk size by 25 percent.
- **Storage pool details:** Shows the status of the storage pool, including total and remaining disk size.



#### 9. In **Choose Replica Creation Method** page, specify how you want to take the initial backup, and then click **Next**.

- The default is **Automatically over the network** and **Now**.
- If you use the default, we recommend that you specify an off-peak time. Choose **Later** and specify a

day and time.

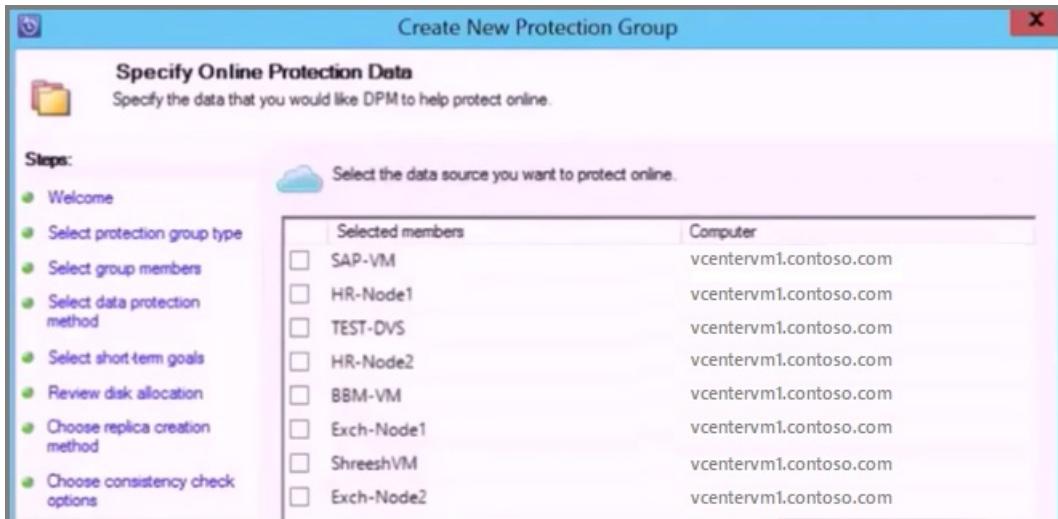
- For large amounts of data or less-than-optimal network conditions, consider replicating the data offline by using removable media.



10. In **Consistency Check Options**, select how and when to automate the consistency checks. Then click **Next**.

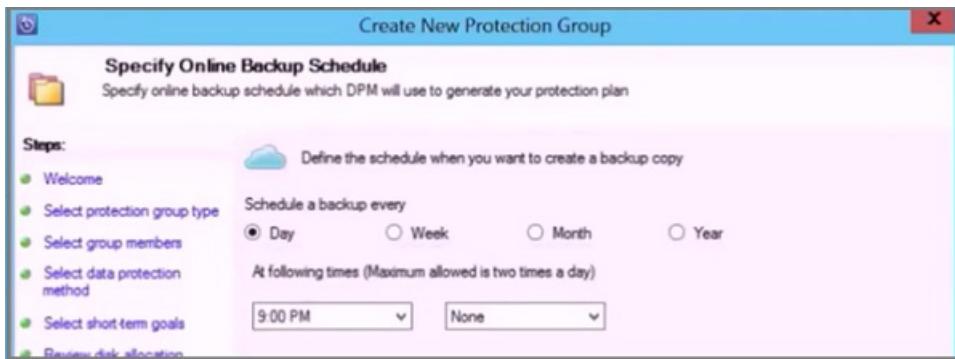
- You can run consistency checks when replica data becomes inconsistent, or on a set schedule.
- If you don't want to configure automatic consistency checks, you can run a manual check. To do this, right-click the protection group > **Perform Consistency Check**.

11. In **Specify Online Protection Data** page, select the VMs or VM folders that you want to back up. You can select the members individually, or click **Select All** to choose all members. Then click **Next**.



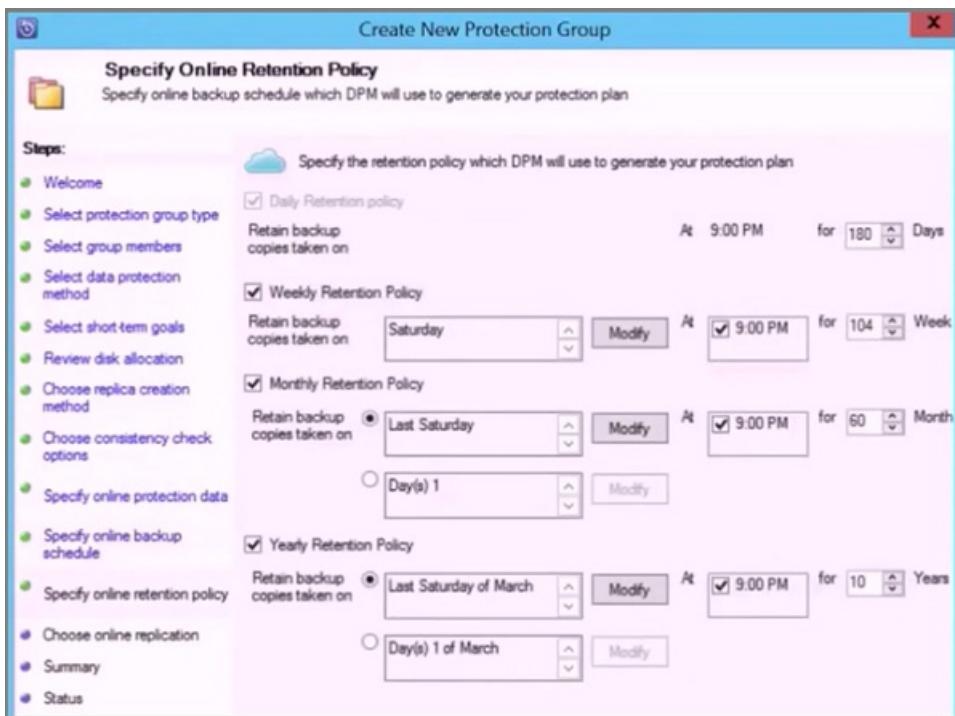
12. On the **Specify Online Backup Schedule** page, specify how often you want to back up data from local storage to Azure.

- Cloud recovery points for the data will be generated according to the schedule. Then click **Next**.
- After the recovery point is generated, it is transferred to the Recovery Services vault in Azure.

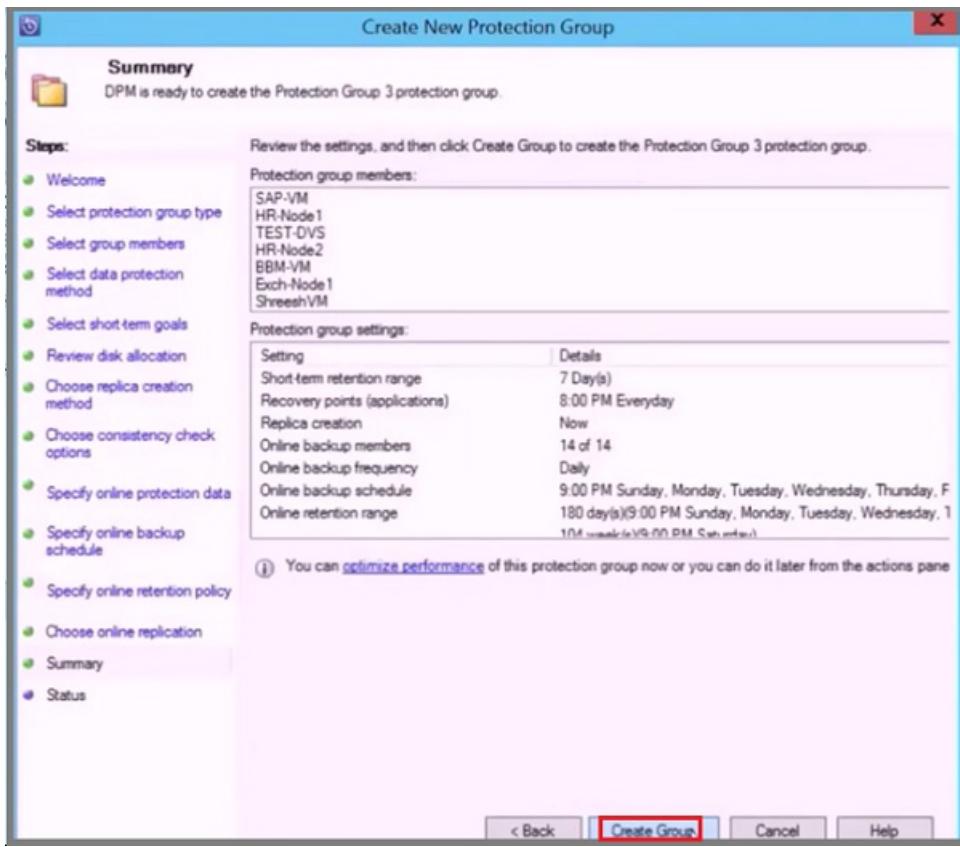


13. On the **Specify Online Retention Policy** page, indicate how long you want to keep the recovery points that are created from the daily/weekly/monthly/yearly backups to Azure. then click **Next**.

- There's no time limit for how long you can keep data in Azure.
- The only limit is that you can't have more than 9999 recovery points per protected instance. In this example, the protected instance is the VMware server.



14. On the **Summary** page, review the settings, and then click **Create Group**.



## VMWare vSphere 6.7

To back up vSphere 6.7, do the following:

- Enable TLS 1.2 on DPM Server

### NOTE

VMWare 6.7 onwards had TLS enabled as communication protocol.

- Set the registry keys as follows:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v2.0.50727]
"SystemDefaultTlsVersions"=dword:00000001
"SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v4.0.30319]
"SystemDefaultTlsVersions"=dword:00000001
"SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v2.0.50727]
"SystemDefaultTlsVersions"=dword:00000001
"SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
"SystemDefaultTlsVersions"=dword:00000001
"SchUseStrongCrypto"=dword:00000001
```

## Next steps

For troubleshooting issues when setting up backups, review the [troubleshooting guide for Azure Backup Server](#).

# Back up an Exchange server to Azure with Azure Backup Server

2/25/2020 • 3 minutes to read • [Edit Online](#)

This article describes how to configure Microsoft Azure Backup Server (MABS) to back up a Microsoft Exchange server to Azure.

## Prerequisites

Before you continue, make sure that Azure Backup Server is [installed and prepared](#).

## MABS protection agent

To install the MABS protection agent on the Exchange server, follow these steps:

1. Make sure that the firewalls are correctly configured. See [Configure firewall exceptions for the agent](#).
2. Install the agent on the Exchange server by clicking **Management > Agents > Install** in MABS Administrator Console. See [Install the MABS protection agent](#) for detailed steps.

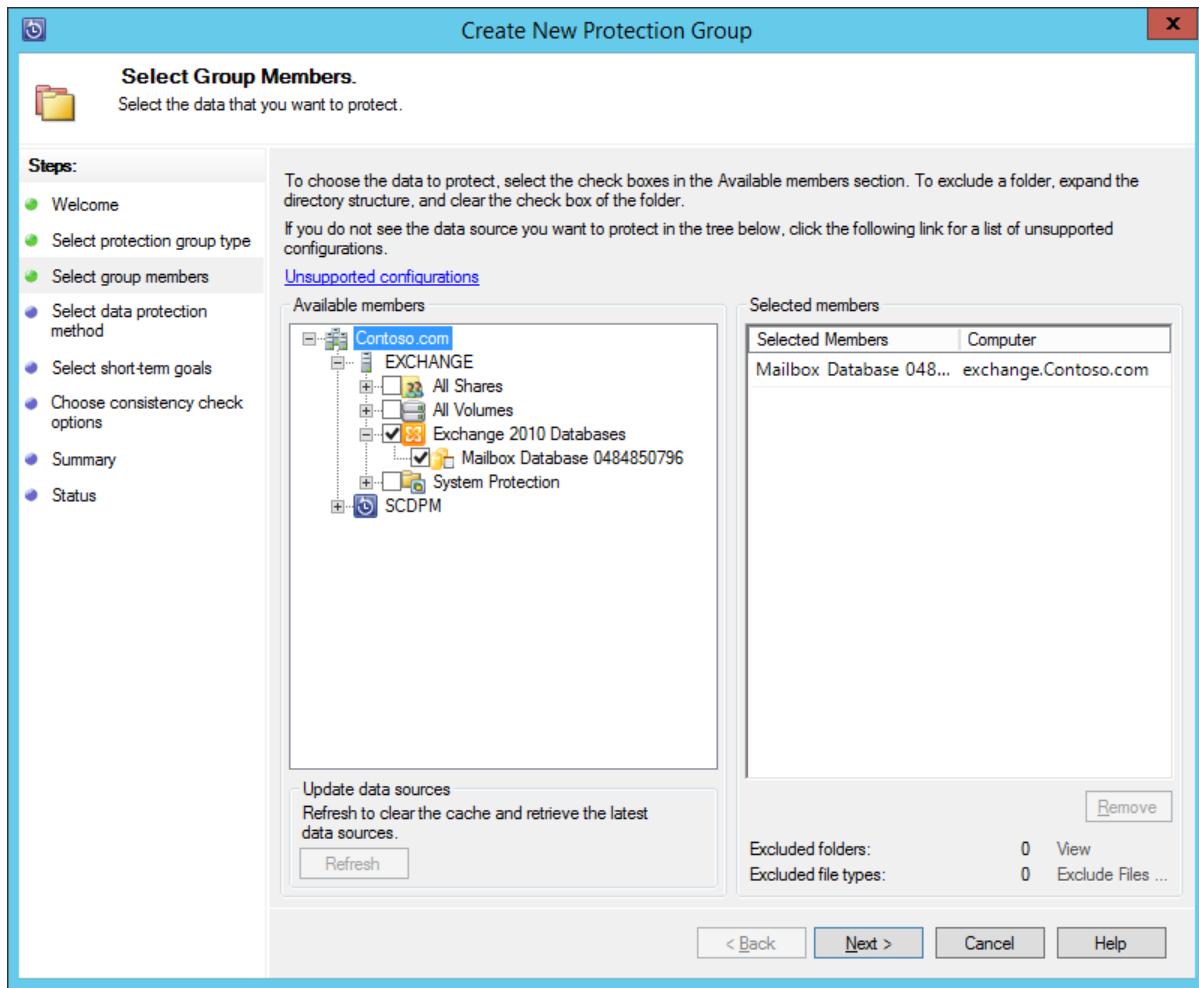
## Create a protection group for the Exchange server

1. In the MABS Administrator Console, click **Protection**, and then click **New** on the tool ribbon to open the **Create New Protection Group** wizard.
2. On the **Welcome** screen of the wizard, click **Next**.
3. On the **Select protection group type** screen, select **Servers** and click **Next**.
4. Select the Exchange server database that you want to protect and click **Next**.

### NOTE

If you are protecting Exchange 2013, check the [Exchange 2013 prerequisites](#).

In the following example, the Exchange 2010 database is selected.



5. Select the data protection method.

Name the protection group, and then select both of the following options:

- I want short-term protection using Disk.
- I want online protection.

6. Click **Next**.

7. Select the **Run Eseutil to check data integrity** option if you want to check the integrity of the Exchange Server databases.

After you select this option, backup consistency checking will be run on MABS to avoid the I/O traffic that's generated by running the **eseutil** command on the Exchange server.

#### NOTE

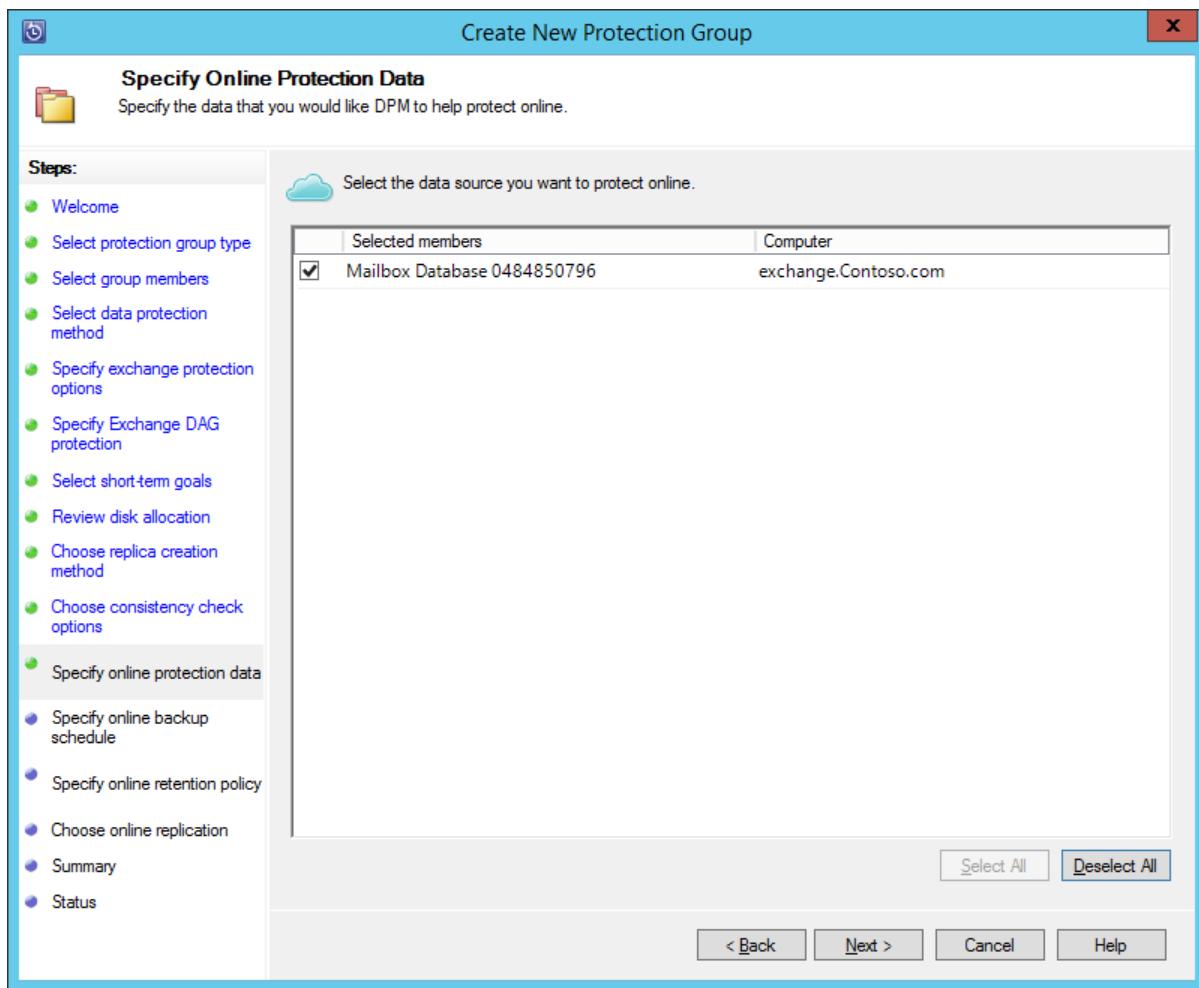
To use this option, you must copy the Ese.dll and Eseutil.exe files to the C:\Program Files\Microsoft Azure Backup\DPM\bin directory on the MAB server. Otherwise, the following error is triggered:



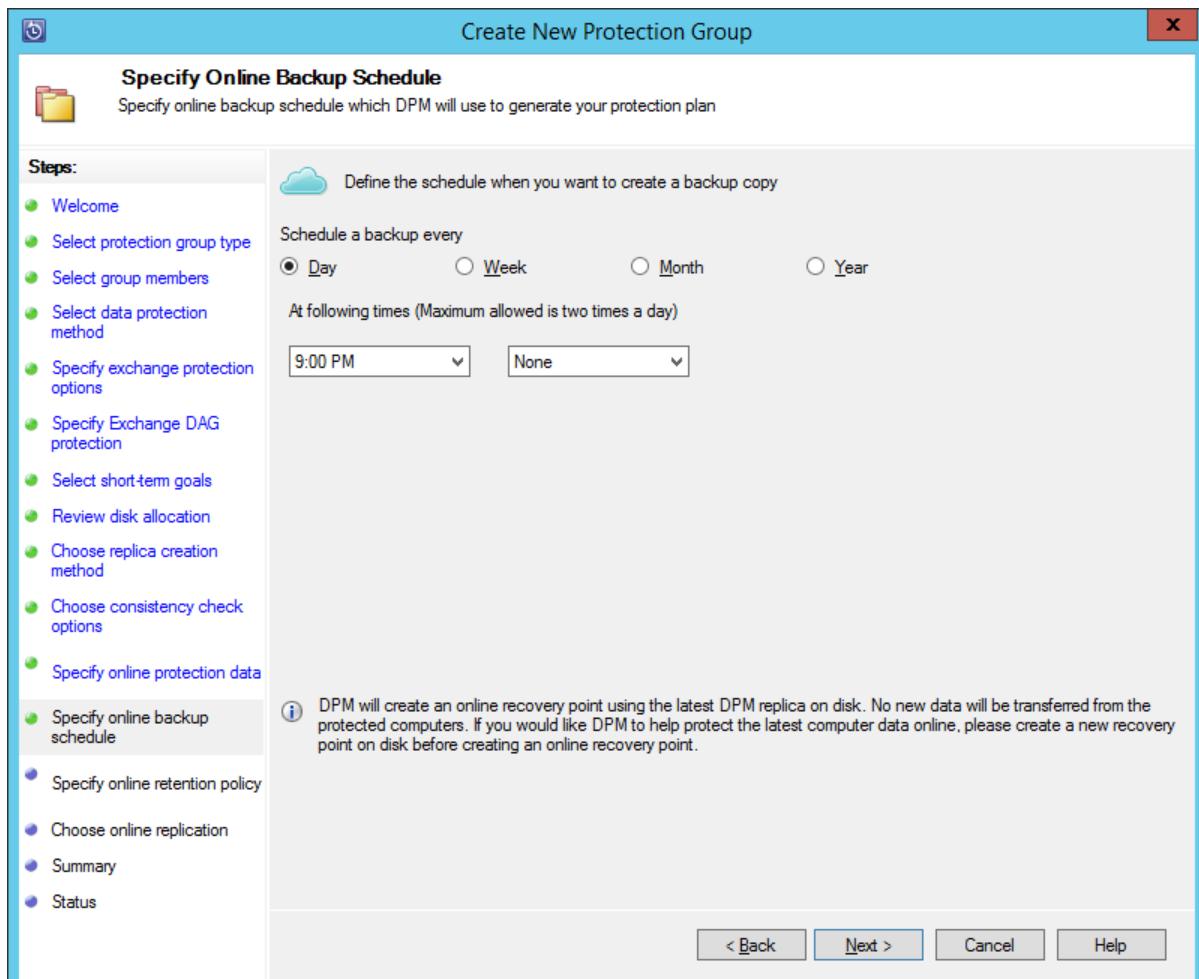
8. Click **Next**.
9. Select the database for **Copy Backup**, and then click **Next**.
10. Configure the goals for **Short-Term backup**, and then click **Next**.
11. Review the available disk space, and then click **Next**.
12. Select the time at which the MAB Server will create the initial replication, and then click **Next**.
13. Select the consistency check options, and then click **Next**.
14. Choose the database that you want to back up to Azure, and then click **Next**. For example:

#### NOTE

If you do not select "Full backup" for at least one DAG copy of a database, logs will not be truncated.



15. Define the schedule for **Azure Backup**, and then click **Next**. For example:



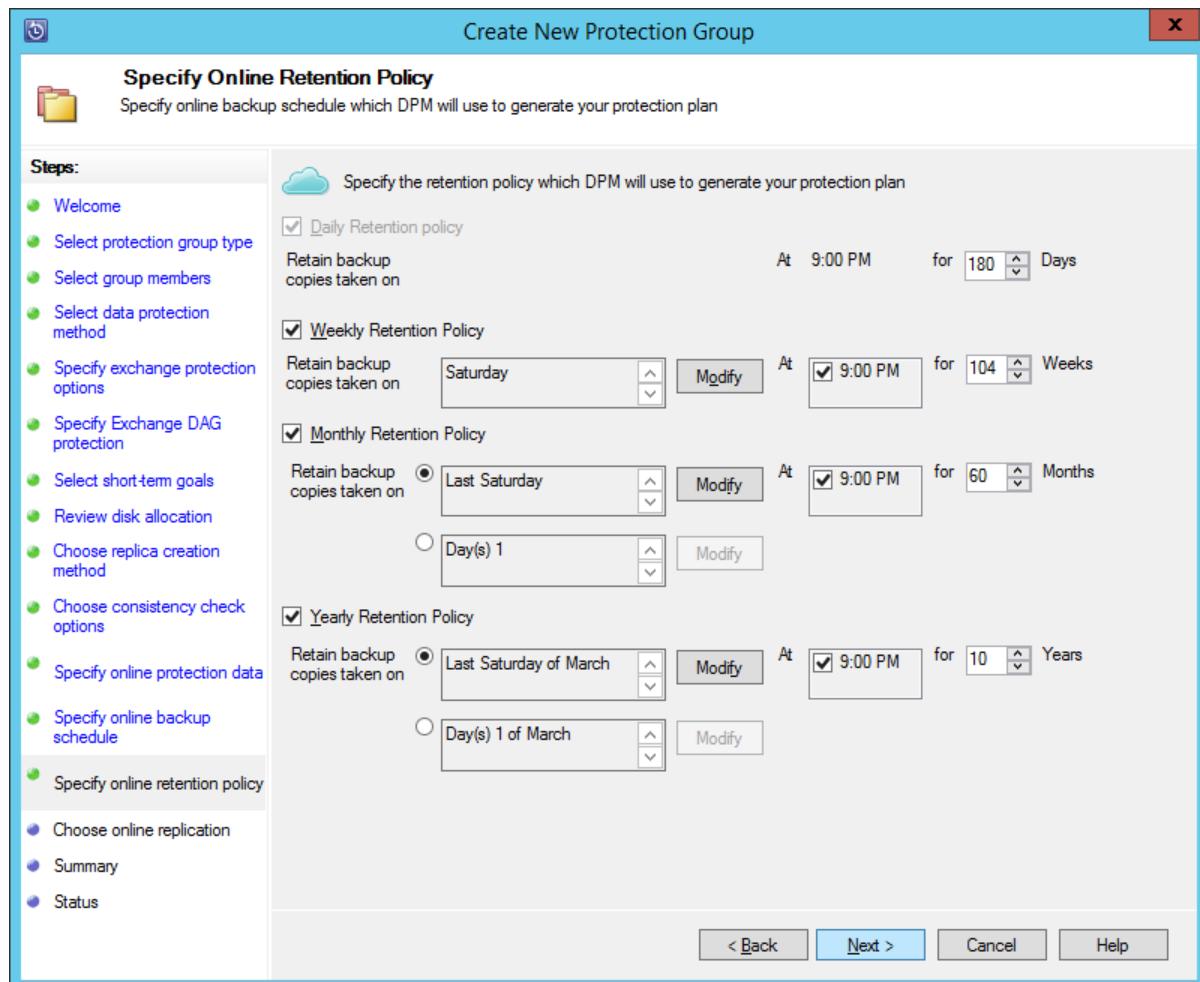
#### NOTE

Note Online recovery points are based on express full recovery points. Therefore, you must schedule the online recovery point after the time that's specified for the express full recovery point.

16. Configure the retention policy for **Azure Backup**, and then click **Next**.

17. Choose an online replication option and click **Next**.

If you have a large database, it could take a long time for the initial backup to be created over the network. To avoid this issue, you can create an offline backup.



18. Confirm the settings, and then click **Create Group**.

19. Click **Close**.

## Recover the Exchange database

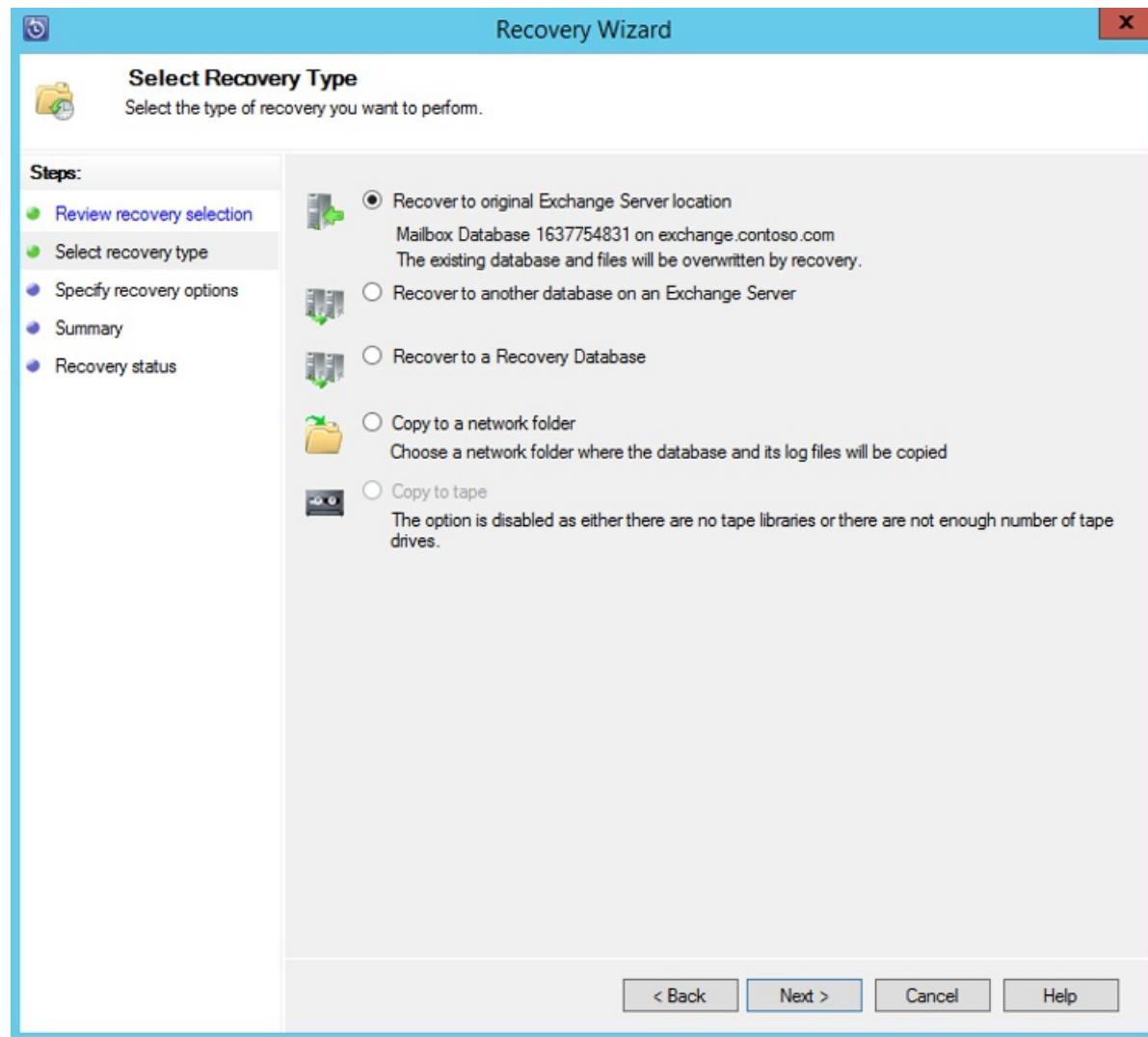
1. To recover an Exchange database, click **Recovery** in the MABS Administrator Console.
2. Locate the Exchange database that you want to recover.
3. Select an online recovery point from the *recovery time* drop-down list.
4. Click **Recover** to start the **Recovery Wizard**.

For online recovery points, there are five recovery types:

- **Recover to original Exchange Server location:** The data will be recovered to the original Exchange server.
- **Recover to another database on an Exchange Server:** The data will be recovered to another database

on another Exchange server.

- **Recover to a Recovery Database:** The data will be recovered to an Exchange Recovery Database (RDB).
- **Copy to a network folder:** The data will be recovered to a network folder.
- **Copy to tape:** If you have a tape library or a stand-alone tape drive attached and configured on MABS, the recovery point will be copied to a free tape.



## Next steps

- [Azure Backup FAQ](#)

# Back up a SharePoint farm to Azure with MABS

2/24/2020 • 8 minutes to read • [Edit Online](#)

You back up a SharePoint farm to Microsoft Azure by using Microsoft Azure Backup Server (MABS) in much the same way that you back up other data sources. Azure Backup provides flexibility in the backup schedule to create daily, weekly, monthly, or yearly backup points and gives you retention policy options for various backup points. It also provides the capability to store local disk copies for quick recovery-time objectives (RTO) and to store copies to Azure for economical, long-term retention.

## SharePoint supported versions and related protection scenarios

Azure Backup for DPM supports the following scenarios:

| WORKLOAD   | VERSION                                                                            | SHAREPOINT DEPLOYMENT                                                                               | PROTECTION AND RECOVERY                                                                                                                                                    |
|------------|------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SharePoint | SharePoint 2016, SharePoint 2013, SharePoint 2010, SharePoint 2007, SharePoint 3.0 | SharePoint deployed as a physical server or Hyper-V/VMware virtual machine<br>-----<br>SQL AlwaysOn | Protect SharePoint Farm recovery options: Recovery farm, database, and file or list item from disk recovery points. Farm and database recovery from Azure recovery points. |

## Before you start

There are a few things you need to confirm before you back up a SharePoint farm to Azure.

### Prerequisites

Before you proceed, make sure that you have [installed and prepared the Azure Backup Server](#) to protect workloads.

### Protection agent

The Azure Backup agent must be installed on the server that's running SharePoint, the servers that are running SQL Server, and all other servers that are part of the SharePoint farm. For more information about how to set up the protection agent, see [Setup Protection Agent](#). The one exception is that you install the agent only on a single web front end (WFE) server. Azure Backup Server needs the agent on one WFE server only to serve as the entry point for protection.

### SharePoint farm

For every 10 million items in the farm, there must be at least 2 GB of space on the volume where the MABS folder is located. This space is required for catalog generation. For MABS to recover specific items (site collections, sites, lists, document libraries, folders, individual documents, and list items), catalog generation creates a list of the URLs that are contained within each content database. You can view the list of URLs in the recoverable item pane in the **Recovery** task area of MABS Administrator Console.

### SQL Server

Azure Backup Server runs as a LocalSystem account. To back up SQL Server databases, MABS needs sysadmin privileges on that account for the server that's running SQL Server. Set NT AUTHORITY\SYSTEM to sysadmin on the server that's running SQL Server before you back it up.

If the SharePoint farm has SQL Server databases that are configured with SQL Server aliases, install the SQL

Server client components on the front-end Web server that MABS will protect.

## SharePoint Server

While performance depends on many factors such as size of SharePoint farm, as general guidance one MABS can protect a 25-TB SharePoint farm.

## What's not supported

- MABS that protects a SharePoint farm does not protect search indexes or application service databases. You will need to configure the protection of these databases separately.
- MABS does not provide backup of SharePoint SQL Server databases that are hosted on scale-out file server (SOFS) shares.

## Configure SharePoint protection

Before you can use MABS to protect SharePoint, you must configure the SharePoint VSS Writer service (WSS Writer service) by using **ConfigureSharePoint.exe**.

You can find **ConfigureSharePoint.exe** in the [MABS Installation Path]\bin folder on the front-end web server. This tool provides the protection agent with the credentials for the SharePoint farm. You run it on a single WFE server. If you have multiple WFE servers, select just one when you configure a protection group.

### To configure the SharePoint VSS Writer service

1. On the WFE server, at a command prompt, go to [MABS installation location]\bin\
2. Enter ConfigureSharePoint -EnableSharePointProtection.
3. Enter the farm administrator credentials. This account should be a member of the local Administrator group on the WFE server. If the farm administrator isn't a local admin grant the following permissions on the WFE server:
  - Grant the WSS\_Admin\_WPG group full control to the DPM folder (%Program Files%\Microsoft Azure Backup\DPM).
  - Grant the WSS\_Admin\_WPG group read access to the DPM Registry key (HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager).

#### NOTE

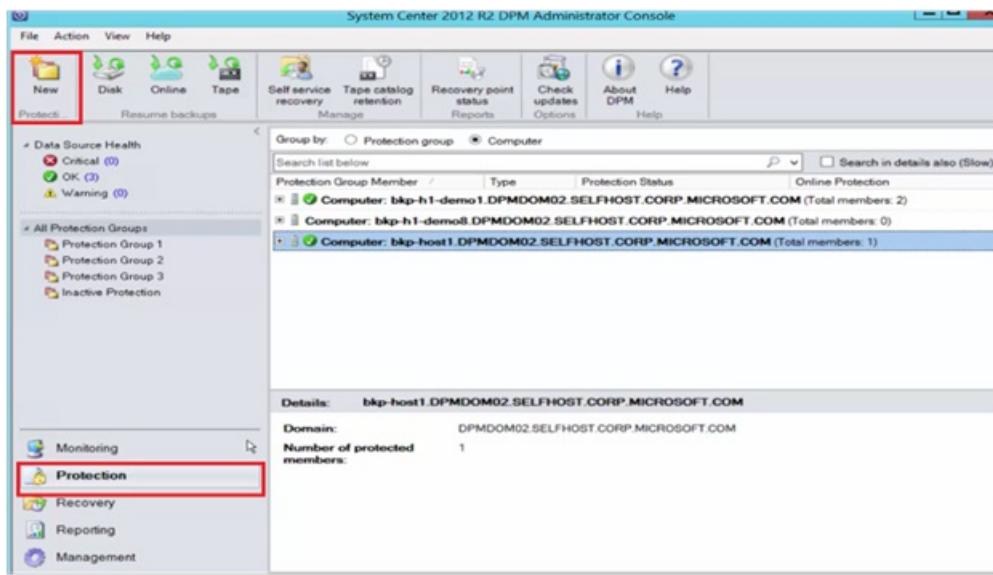
You'll need to rerun ConfigureSharePoint.exe whenever there's a change in the SharePoint farm administrator credentials.

## Back up a SharePoint farm by using MABS

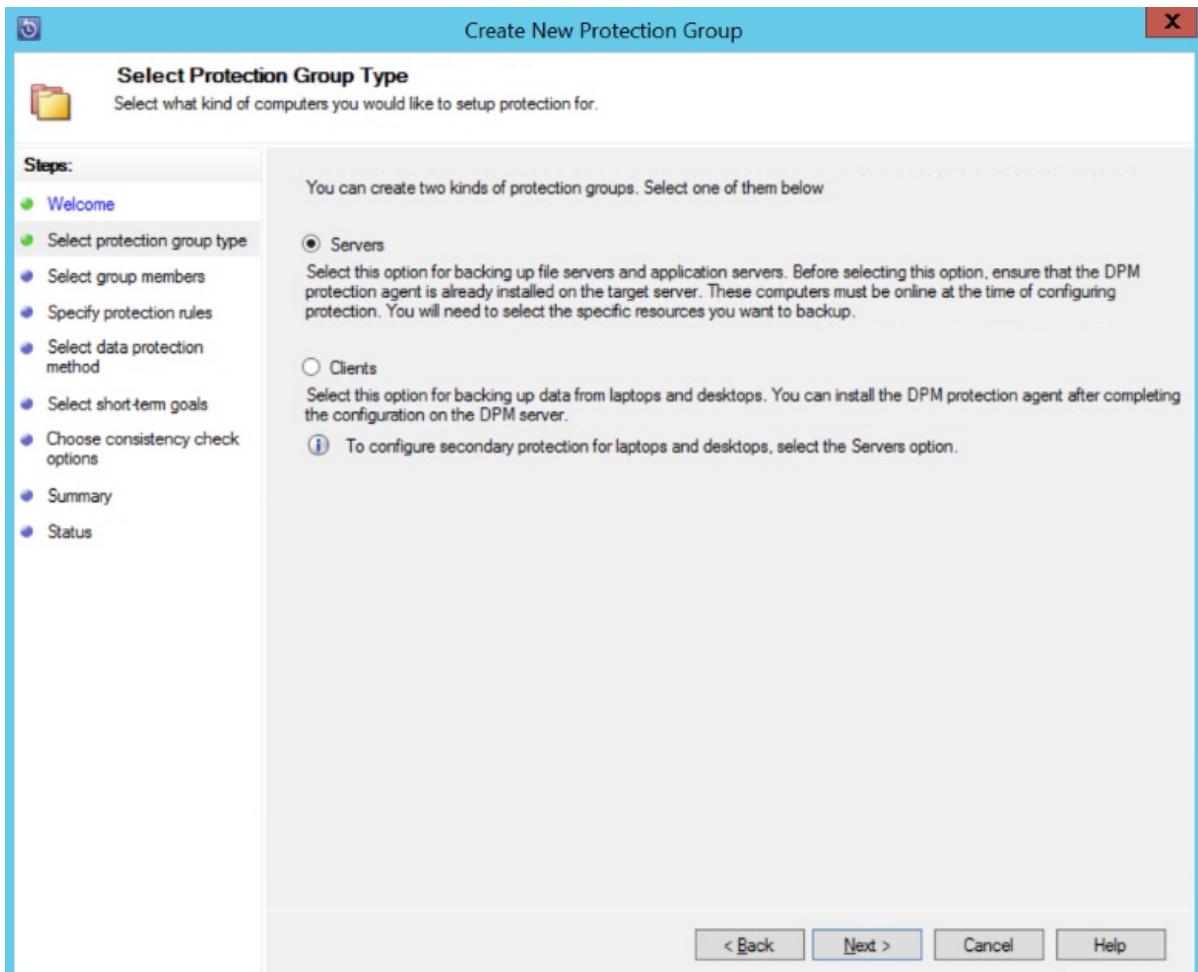
After you have configured MABS and the SharePoint farm as explained previously, SharePoint can be protected by MABS.

### To protect a SharePoint farm

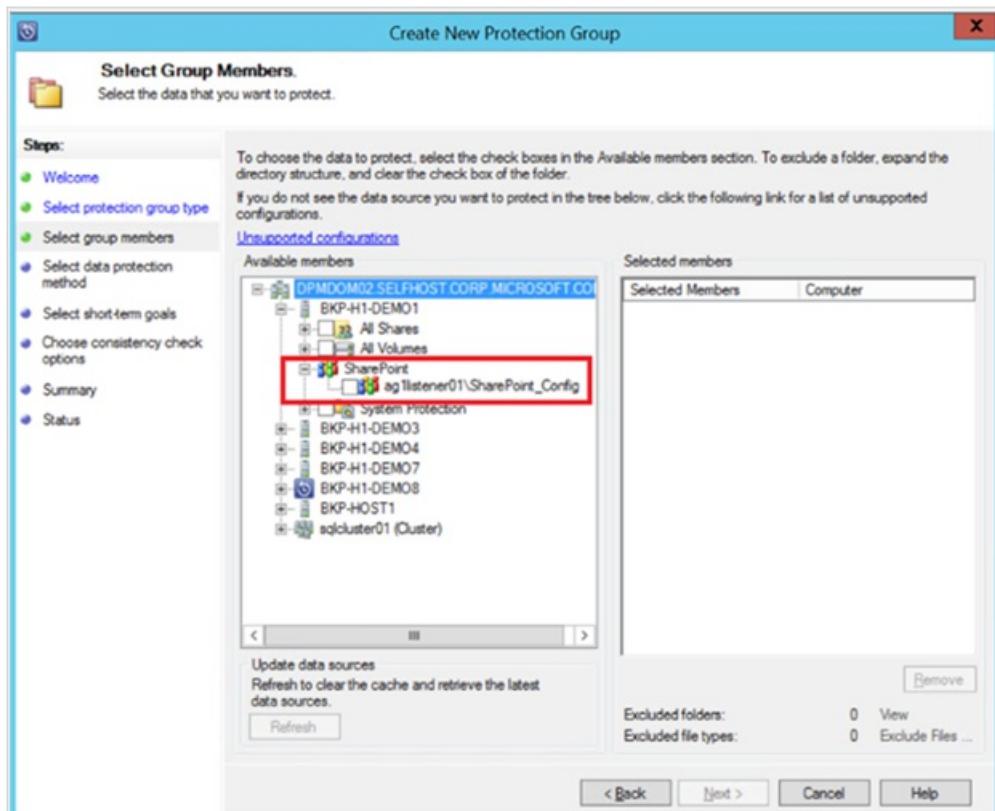
1. From the **Protection** tab of the MABS Administrator Console, click **New**.



2. On the **Select Protection Group Type** page of the **Create New Protection Group** wizard, select **Servers**, and then click **Next**.



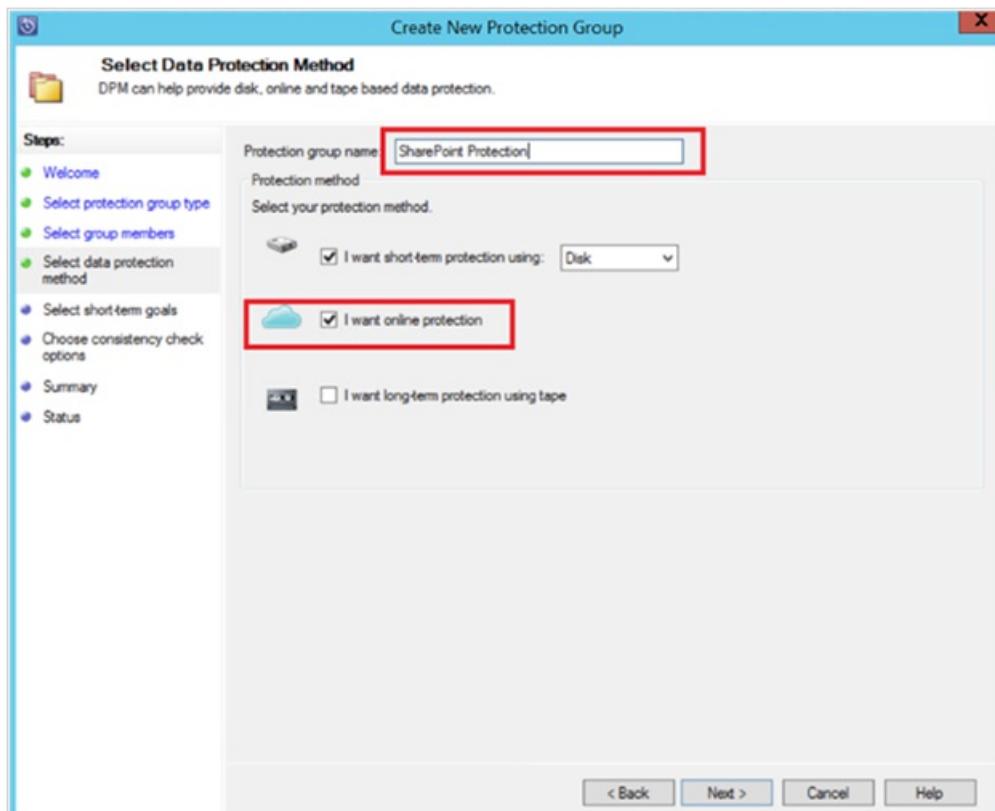
3. On the **Select Group Members** screen, select the check box for the SharePoint server you want to protect and click **Next**.



#### NOTE

With the protection agent installed, you can see the server in the wizard. MABS also shows its structure. Because you ran ConfigureSharePoint.exe, MABS communicates with the SharePoint VSS Writer service and its corresponding SQL Server databases and recognizes the SharePoint farm structure, the associated content databases, and any corresponding items.

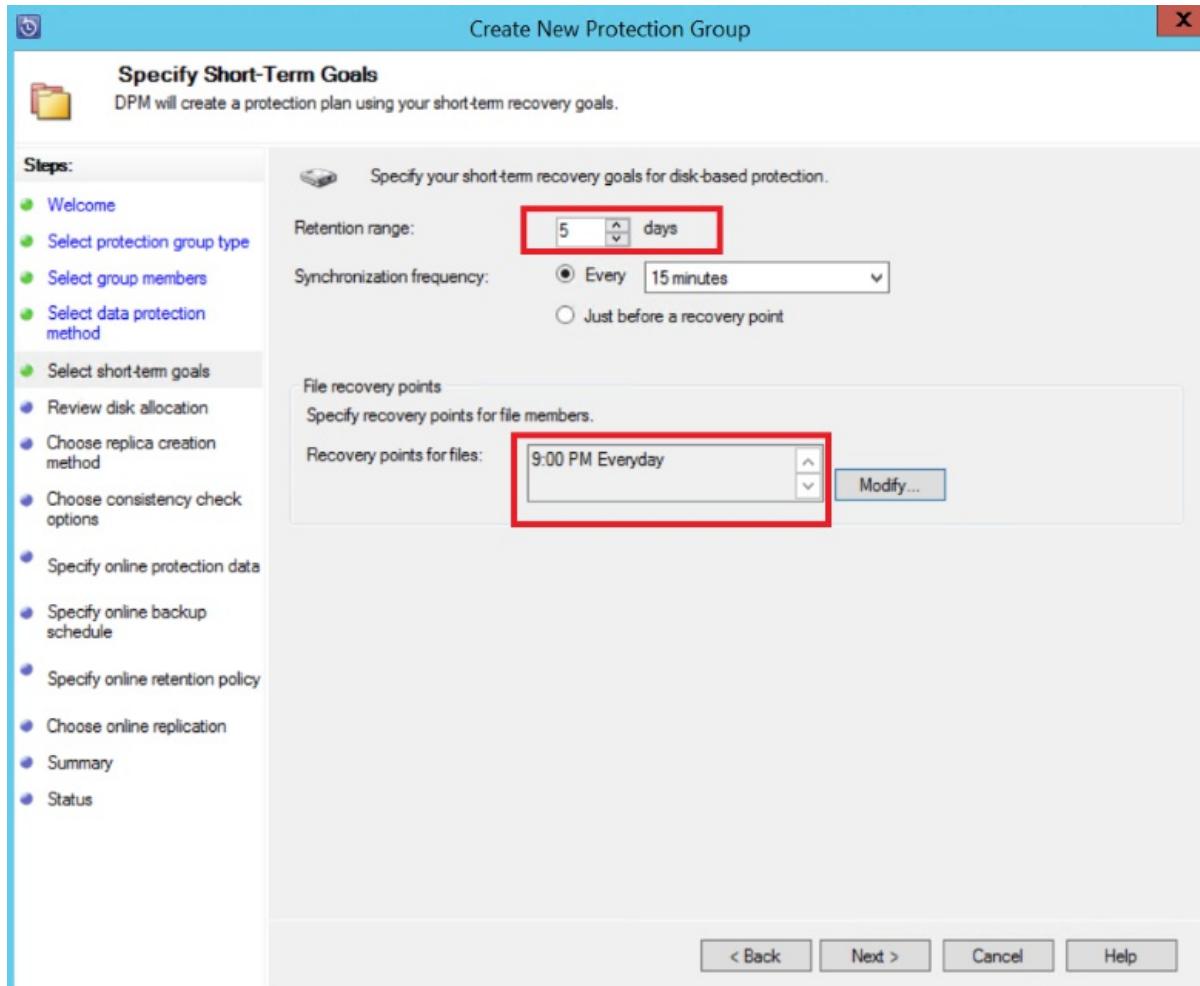
- On the **Select Data Protection Method** page, enter the name of the **Protection Group**, and select your preferred *protection methods*. Click **Next**.



#### NOTE

The disk protection method helps to meet short recovery-time objectives.

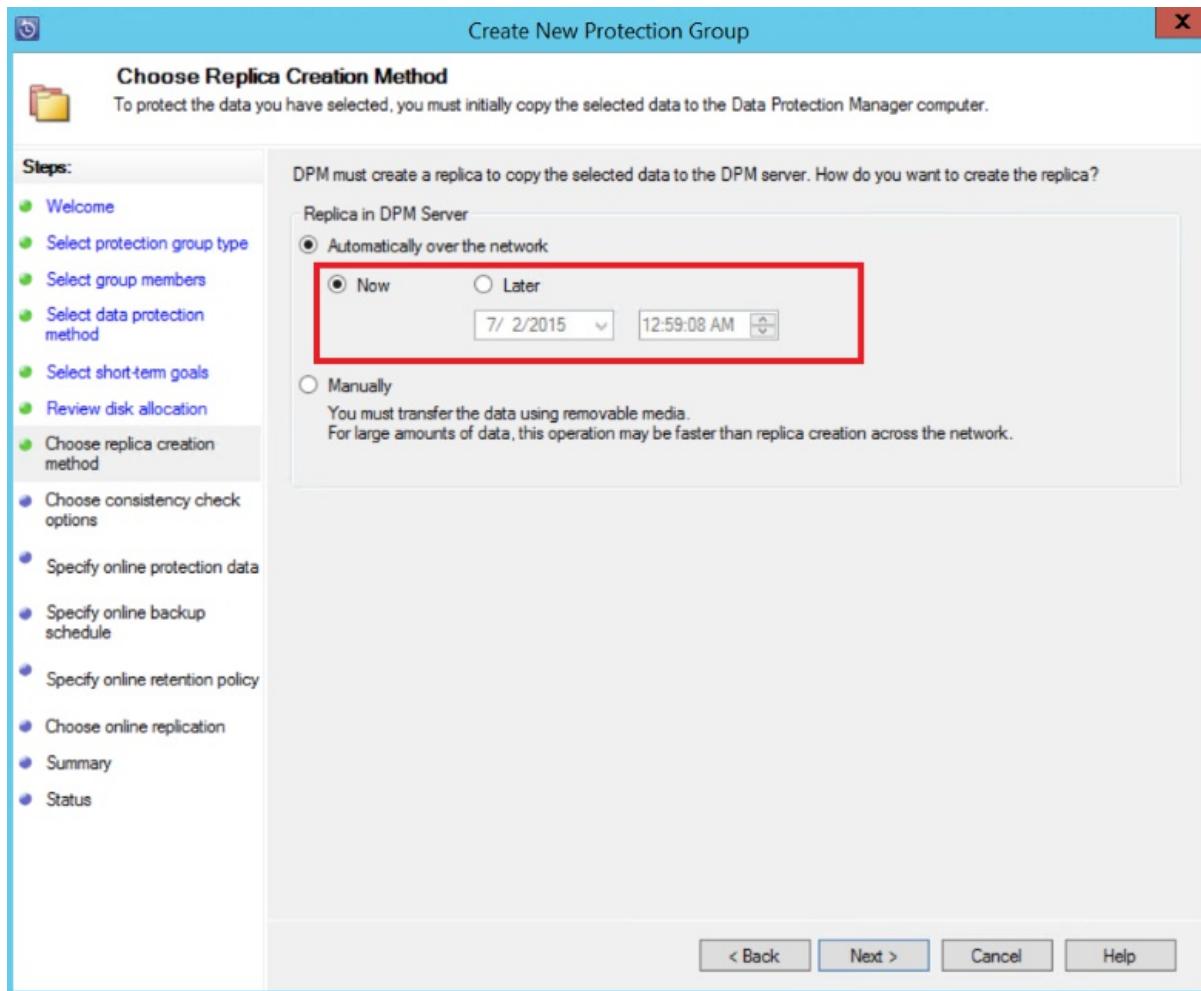
5. On the **Specify Short-Term Goals** page, select your preferred **Retention range** and identify when you want backups to occur.



#### NOTE

Because recovery is most often required for data that's less than five days old, we selected a retention range of five days on disk and ensured that the backup happens during non-production hours, for this example.

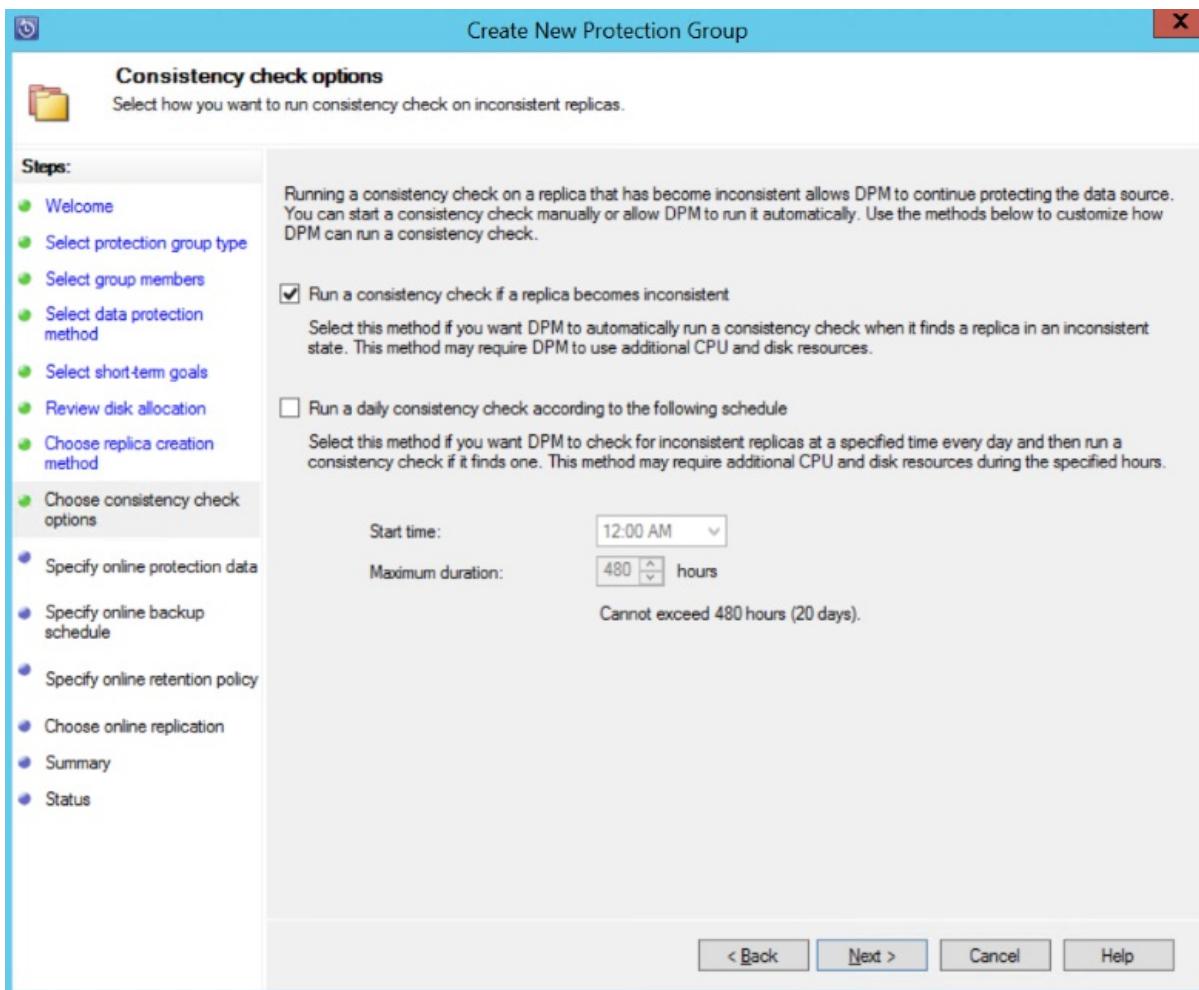
6. Review the storage pool disk space allocated for the protection group, and click then **Next**.
7. For every protection group, MABS allocates disk space to store and manage replicas. At this point, MABS must create a copy of the selected data. Select how and when you want the replica created, and then click **Next**.



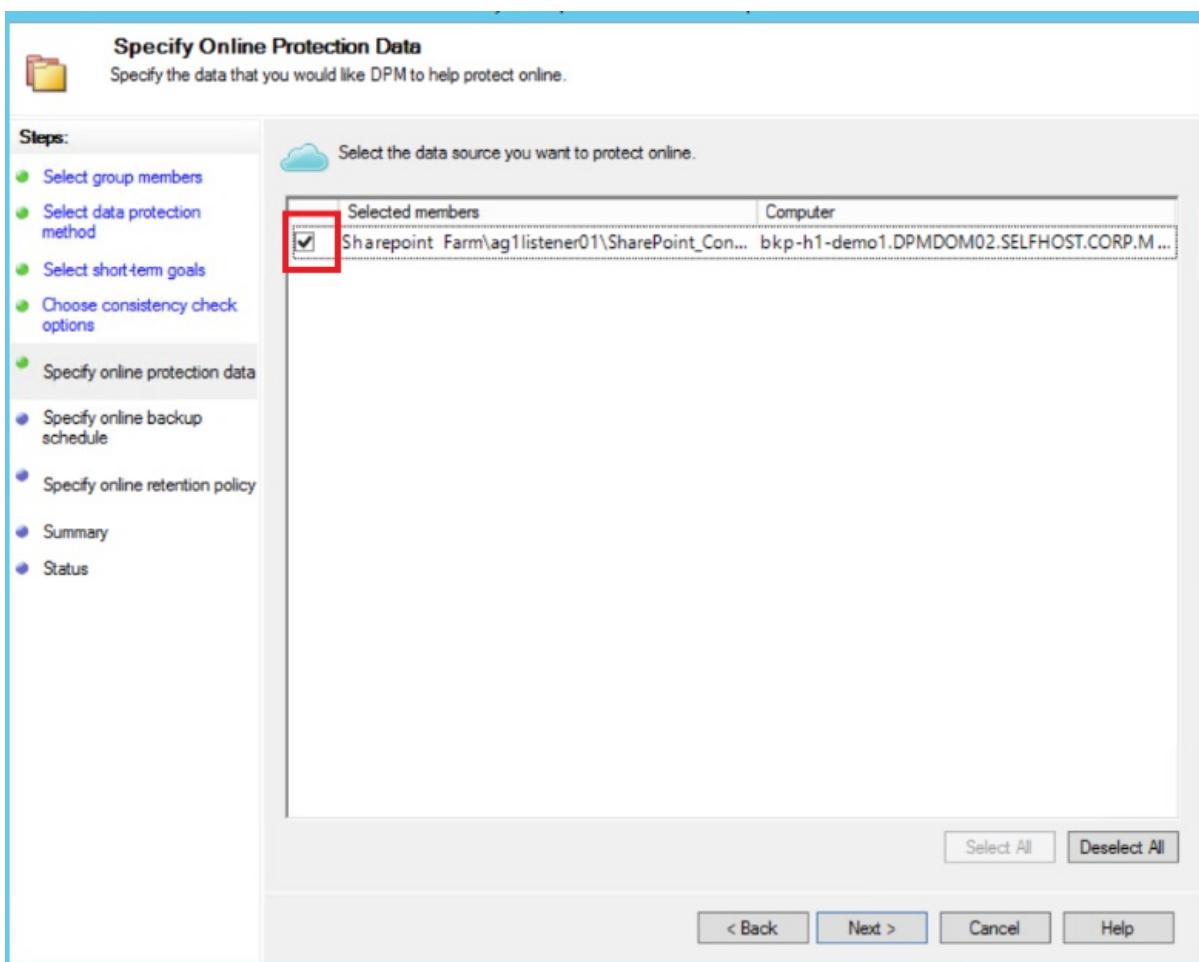
**NOTE**

To make sure that network traffic is not effected, select a time outside production hours.

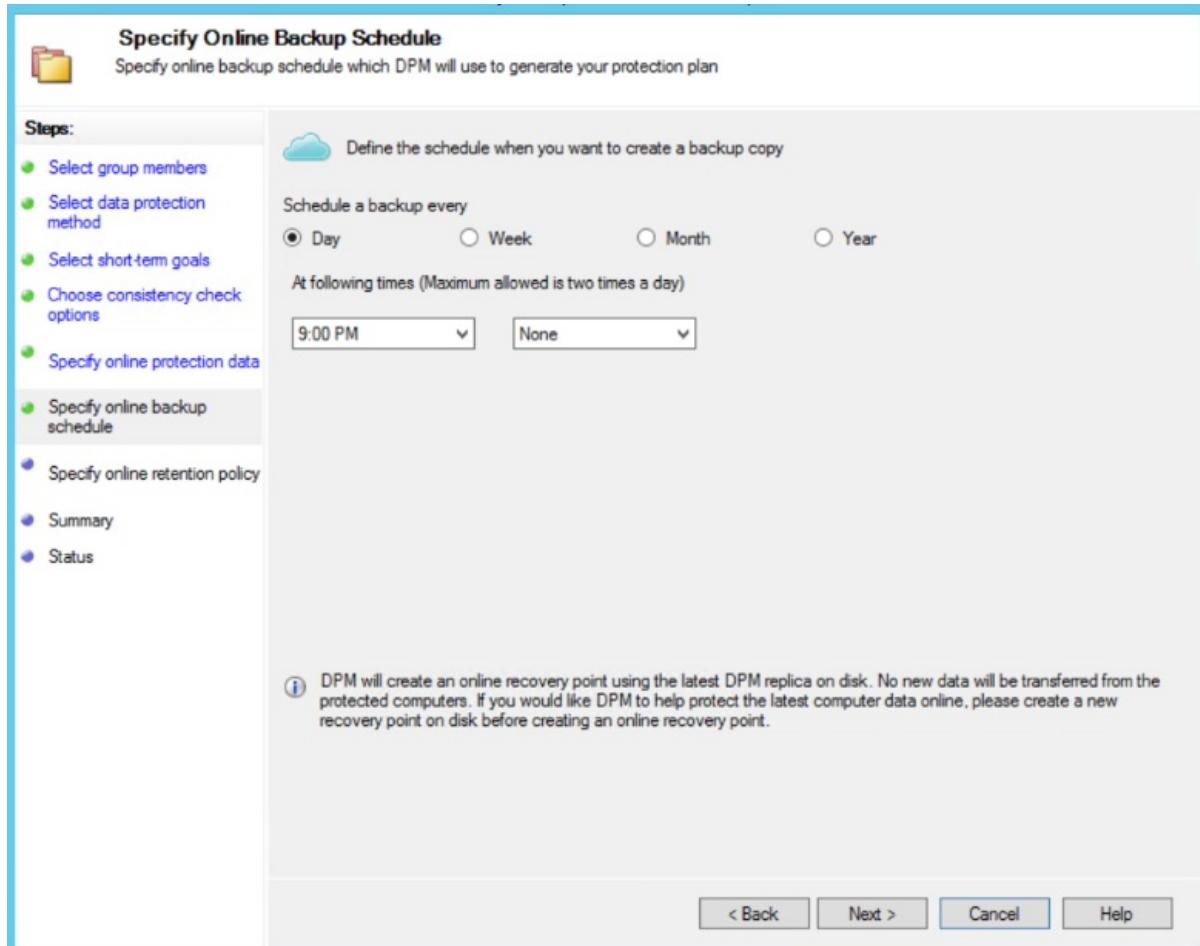
8. MABS ensures data integrity by performing consistency checks on the replica. There are two available options. You can define a schedule to run consistency checks, or DPM can run consistency checks automatically on the replica whenever it becomes inconsistent. Select your preferred option, and then click **Next**.



9. On the **Specify Online Protection Data** page, select the SharePoint farm that you want to protect, and then click **Next**.



10. On the **Specify Online Backup Schedule** page, select your preferred schedule, and then click **Next**.



**NOTE**

MABS provides a maximum of two daily backups to Azure from the then available latest disk backup point. Azure Backup can also control the amount of WAN bandwidth that can be used for backups in peak and off-peak hours by using [Azure Backup Network Throttling](#).

11. Depending on the backup schedule that you selected, on the **Specify Online Retention Policy** page, select the retention policy for daily, weekly, monthly, and yearly backup points.

**Specify Online Retention Policy**

Specify online backup schedule which DPM will use to generate your protection plan

**Steps:**

- Select group members
- Select data protection method
- Select short-term goals
- Choose consistency check options
- Specify online protection data
- Specify online backup schedule
- **Specify online retention policy**
- Summary
- Status

**Specify the retention policy which DPM will use to generate your protection plan**

Daily Retention policy  
Retain backup copies taken on At 9:00 PM for 180 Days

Weekly Retention Policy  
Retain backup copies taken on Sat At  9:00 PM for 104 Weeks

Monthly Retention Policy  
Retain backup copies taken on Last Sat At  9:00 PM for 60 Months

Day(s) 1 At  9:00 PM

Yearly Retention Policy  
Retain backup copies taken on Last Sat of Mar At  9:00 PM for 10 Years

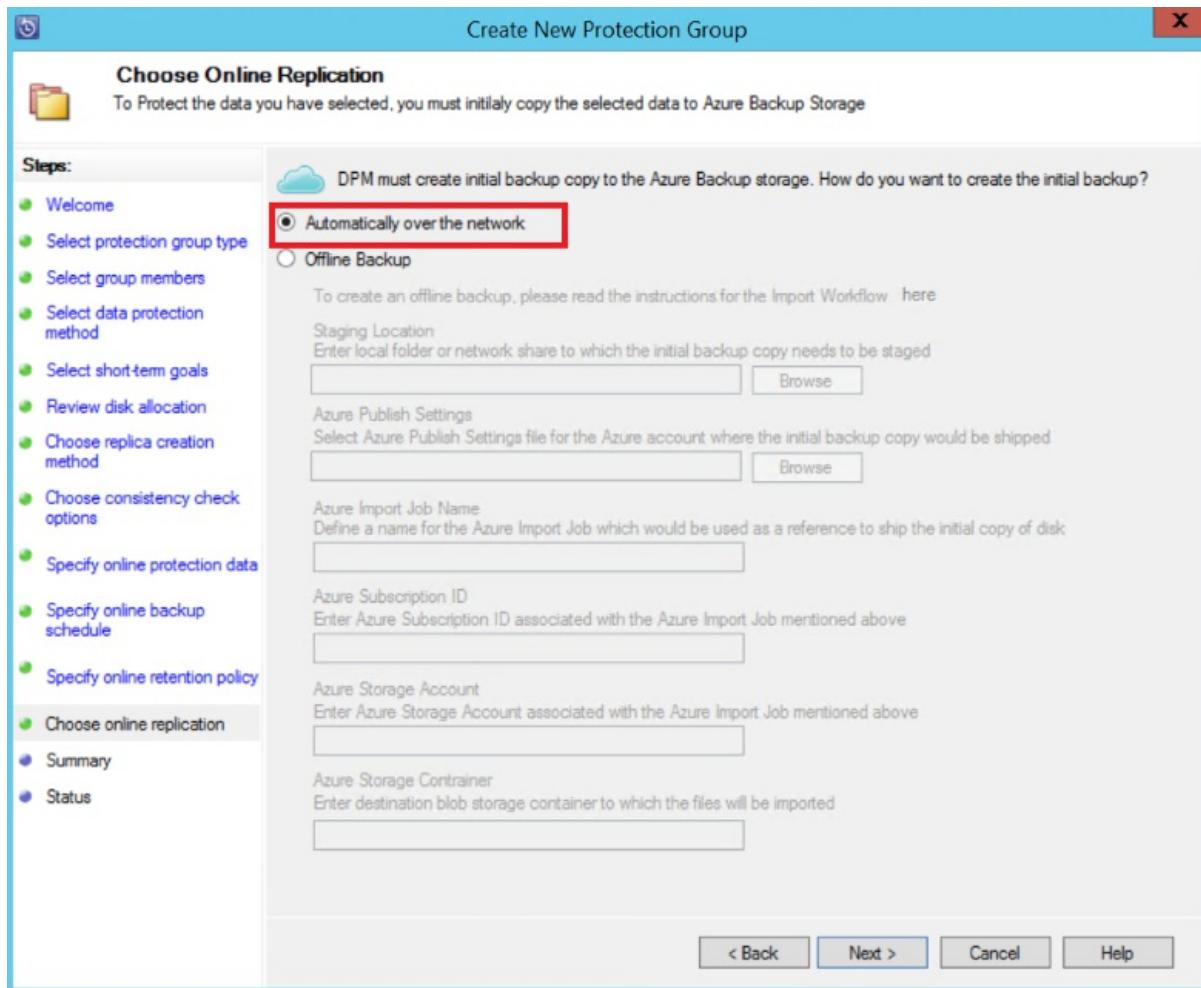
Day(s) 1 of Mar At  9:00 PM

**< Back** **Next >** **Cancel** **Help**

#### NOTE

MABS uses a grandfather-father-son retention scheme in which a different retention policy can be chosen for different backup points.

12. Similar to disk, an initial reference point replica needs to be created in Azure. Select your preferred option to create an initial backup copy to Azure, and then click **Next**.



13. Review your selected settings on the **Summary** page, and then click **Create Group**. You will see a success message after the protection group has been created.

Create New Protection Group

**Summary**  
DPM is ready to create the SharePoint Protection protection group.

**Steps:**

- Welcome
- Select protection group type
- Select group members
- Select data protection method
- Select short-term goals
- Review disk allocation
- Choose replica creation method
- Choose consistency check options
- Specify online protection data
- Specify online backup schedule
- Specify online retention policy
- Choose online replication
- Summary
- Status

**Protection group members:**  
Sharepoint Farm\ag1\listener01\SharePoint\_Config

**Protection group settings:**

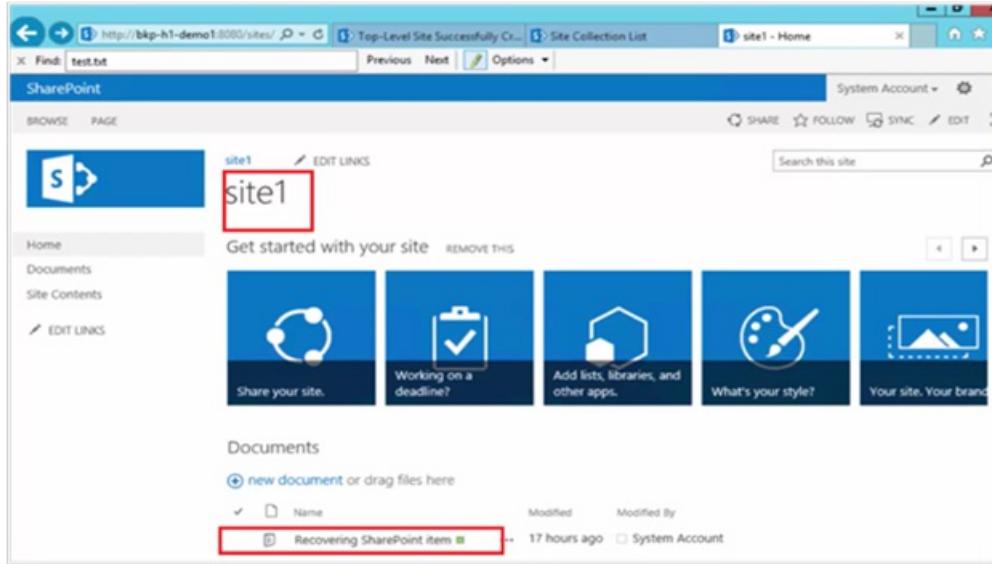
| Setting                 | Details                              |
|-------------------------|--------------------------------------|
| Online backup frequency | Daily                                |
| Online backup schedule  | 9:00 PM Everyday                     |
| Online retention range  | 180 day(s)(9:00 PM Everyday)         |
|                         | 104 week(s)(9:00 PM Sat)             |
|                         | 60 month(s)(Last Sat, 9:00 PM)       |
|                         | 10 year(s)(Last Sat of Mar, 9:00 PM) |
| Online Replica Creation | Network                              |

**Note:** You can [optimize performance](#) of this protection group now or you can do it later from the actions pane.

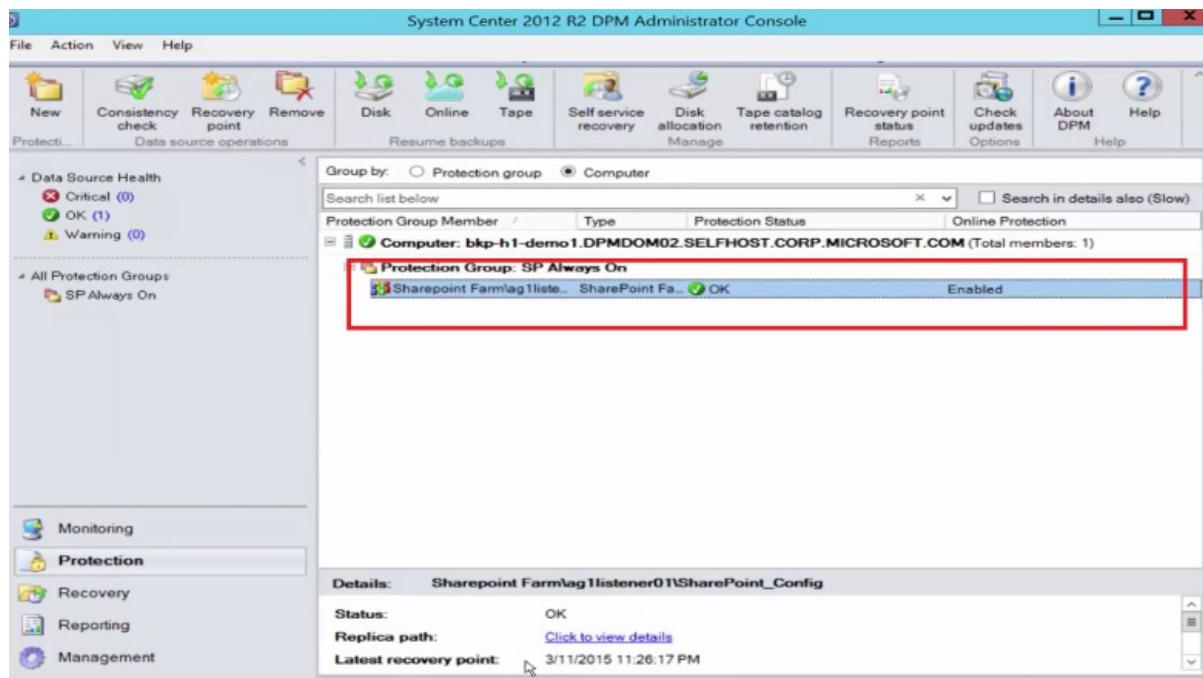
< Back      Create Group      Cancel      Help

## Restore a SharePoint item from disk by using MABS

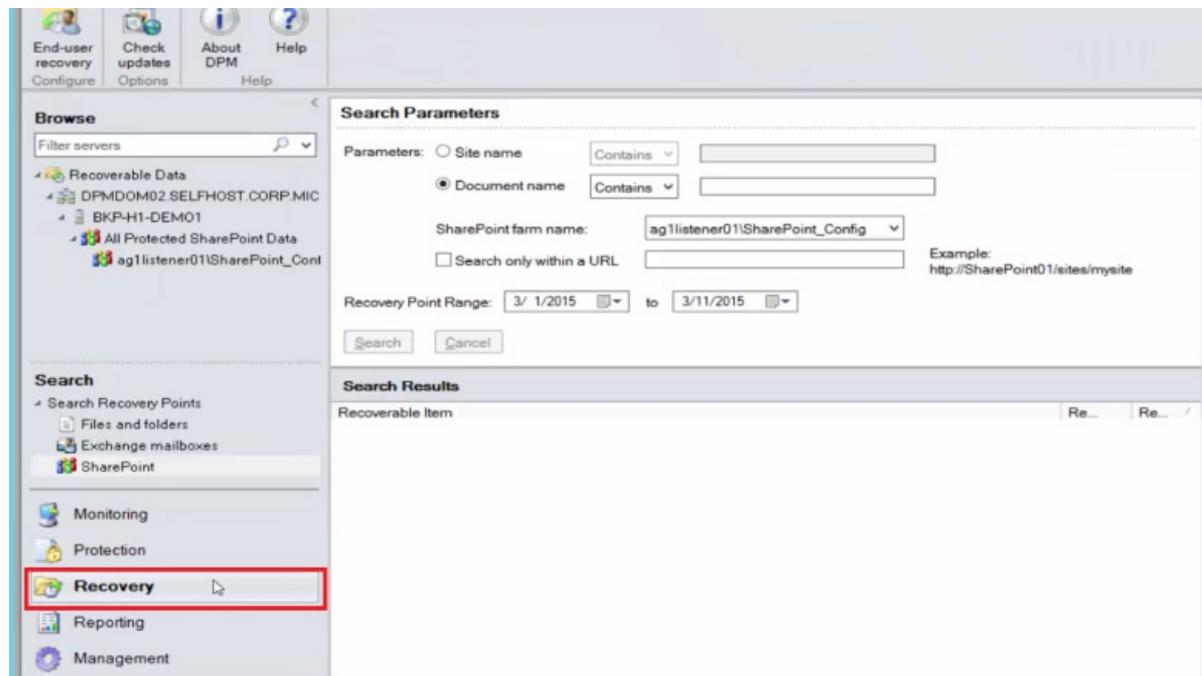
In the following example, the *Recovering SharePoint item* has been accidentally deleted and needs to be recovered.



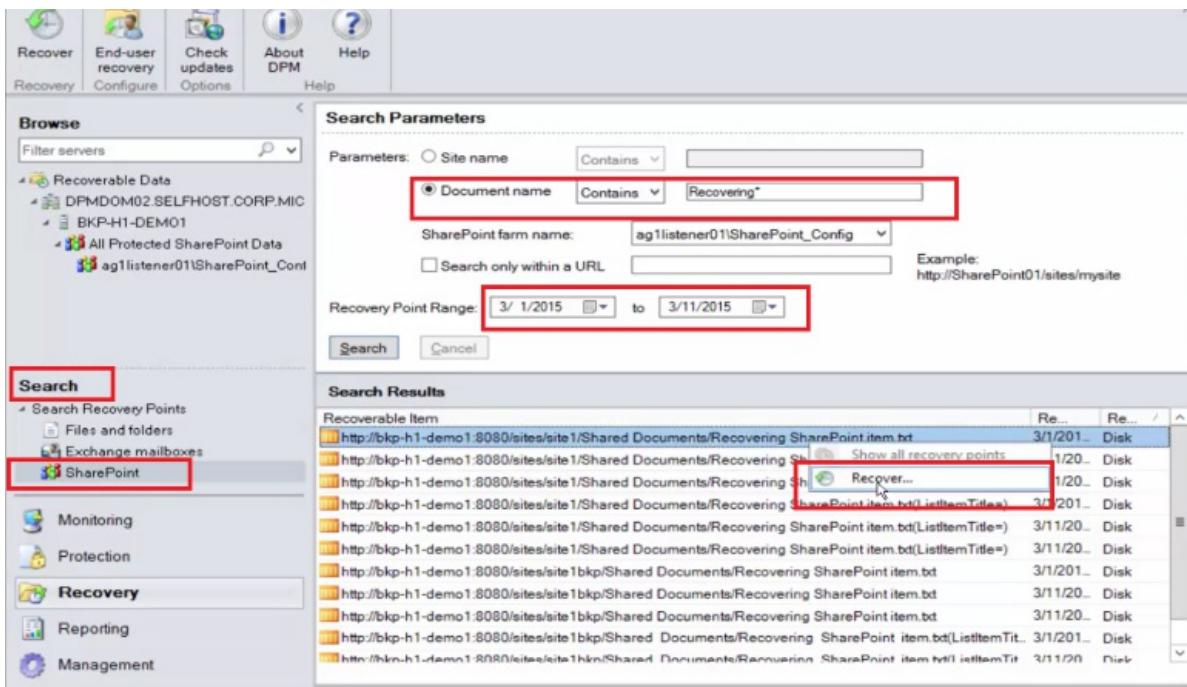
1. Open the **DPM Administrator Console**. All SharePoint farms that are protected by DPM are shown in the **Protection** tab.



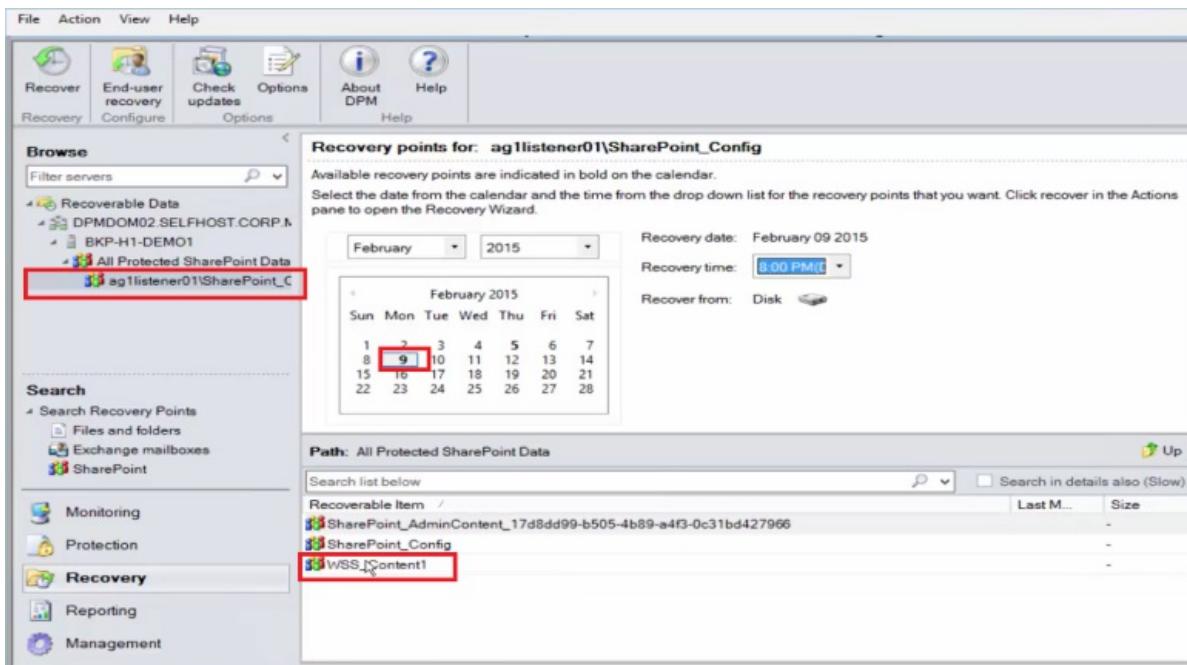
2. To begin to recover the item, select the **Recovery** tab.



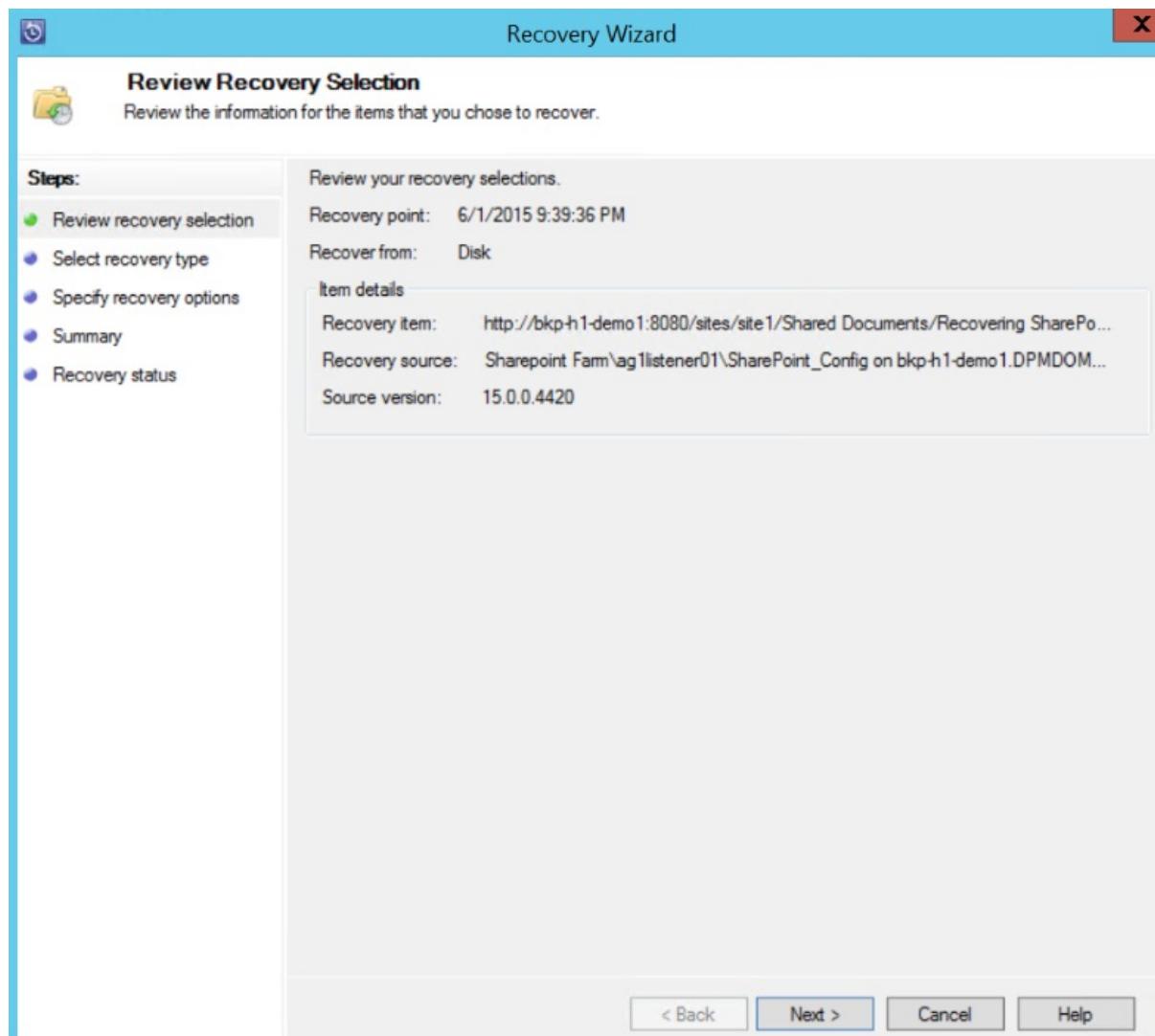
3. You can search SharePoint for *Recovering SharePoint item* by using a wildcard-based search within a recovery point range.



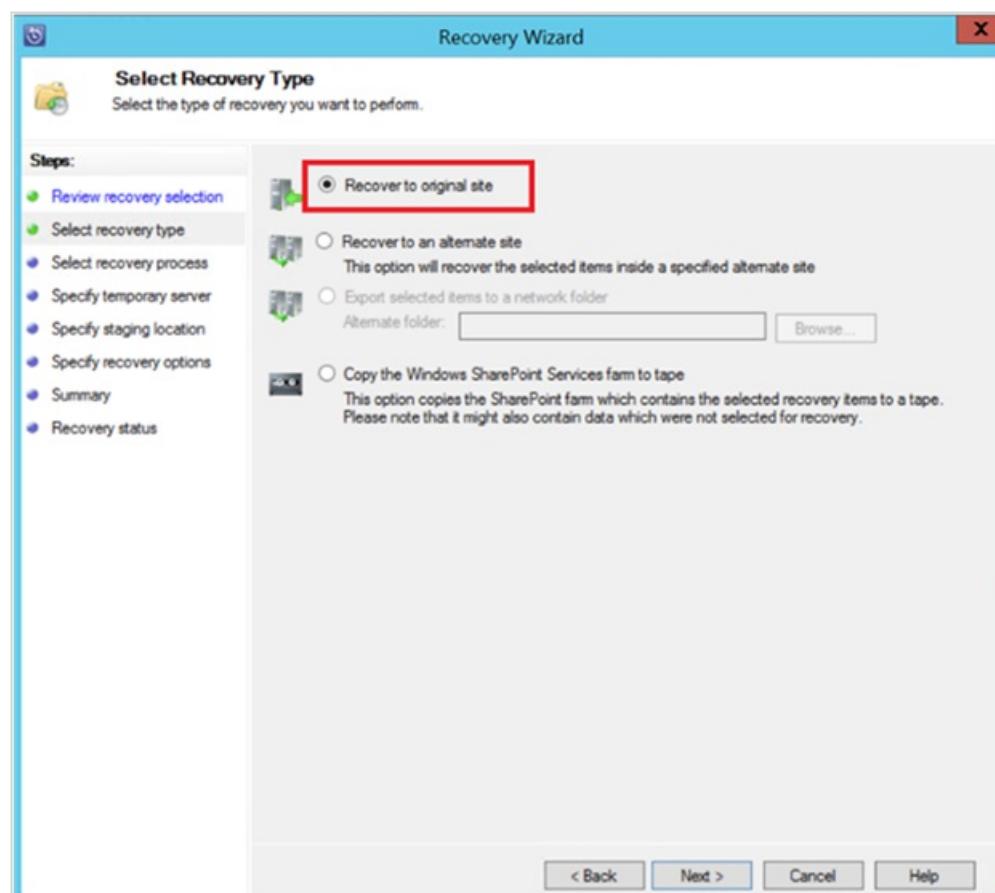
4. Select the appropriate recovery point from the search results, right-click the item, and then select **Recover**.
5. You can also browse through various recovery points and select a database or item to recover. Select **Date > Recovery time**, and then select the correct **Database > SharePoint farm > Recovery point > Item**.



6. Right-click the item, and then select **Recover** to open the **Recovery Wizard**. Click **Next**.



7. Select the type of recovery that you want to perform, and then click **Next**.

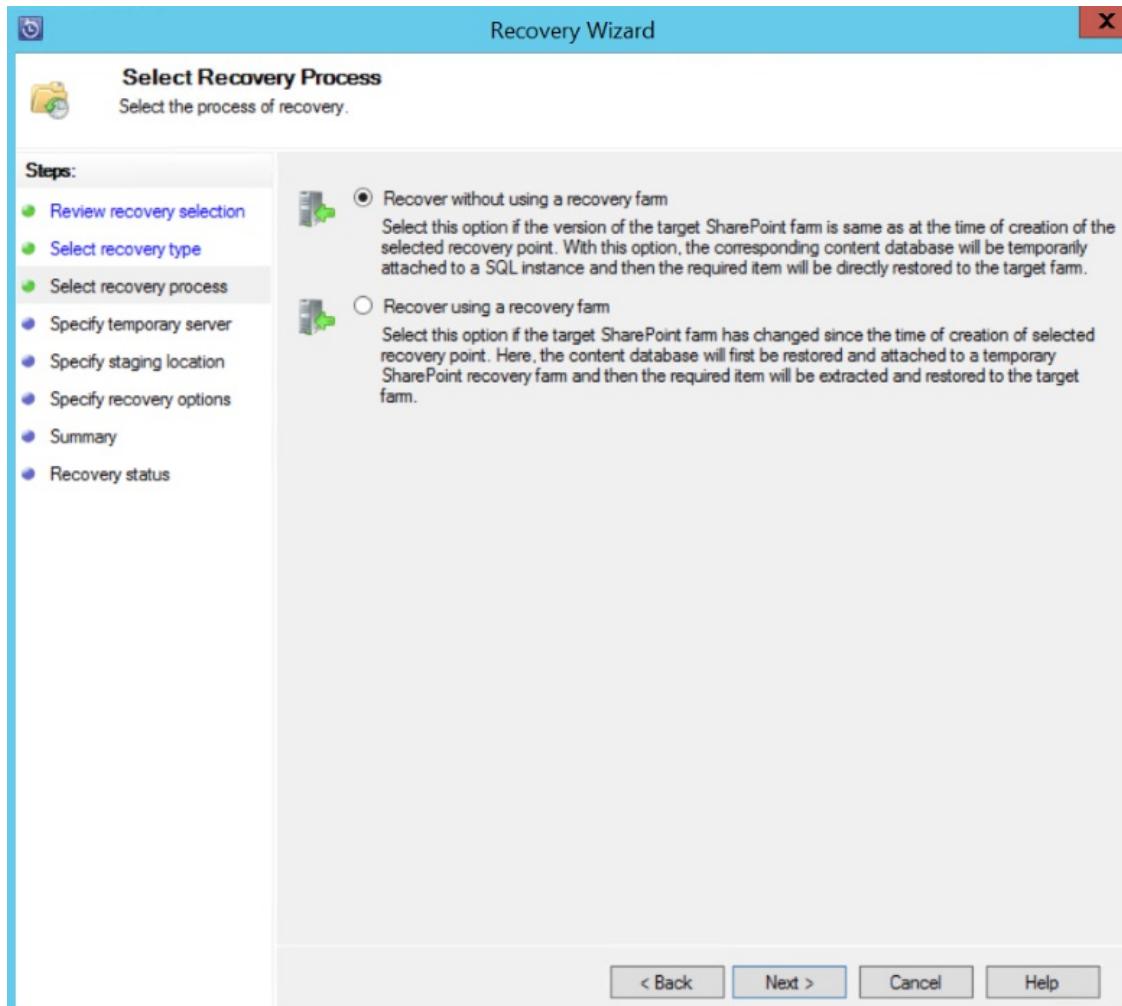


**NOTE**

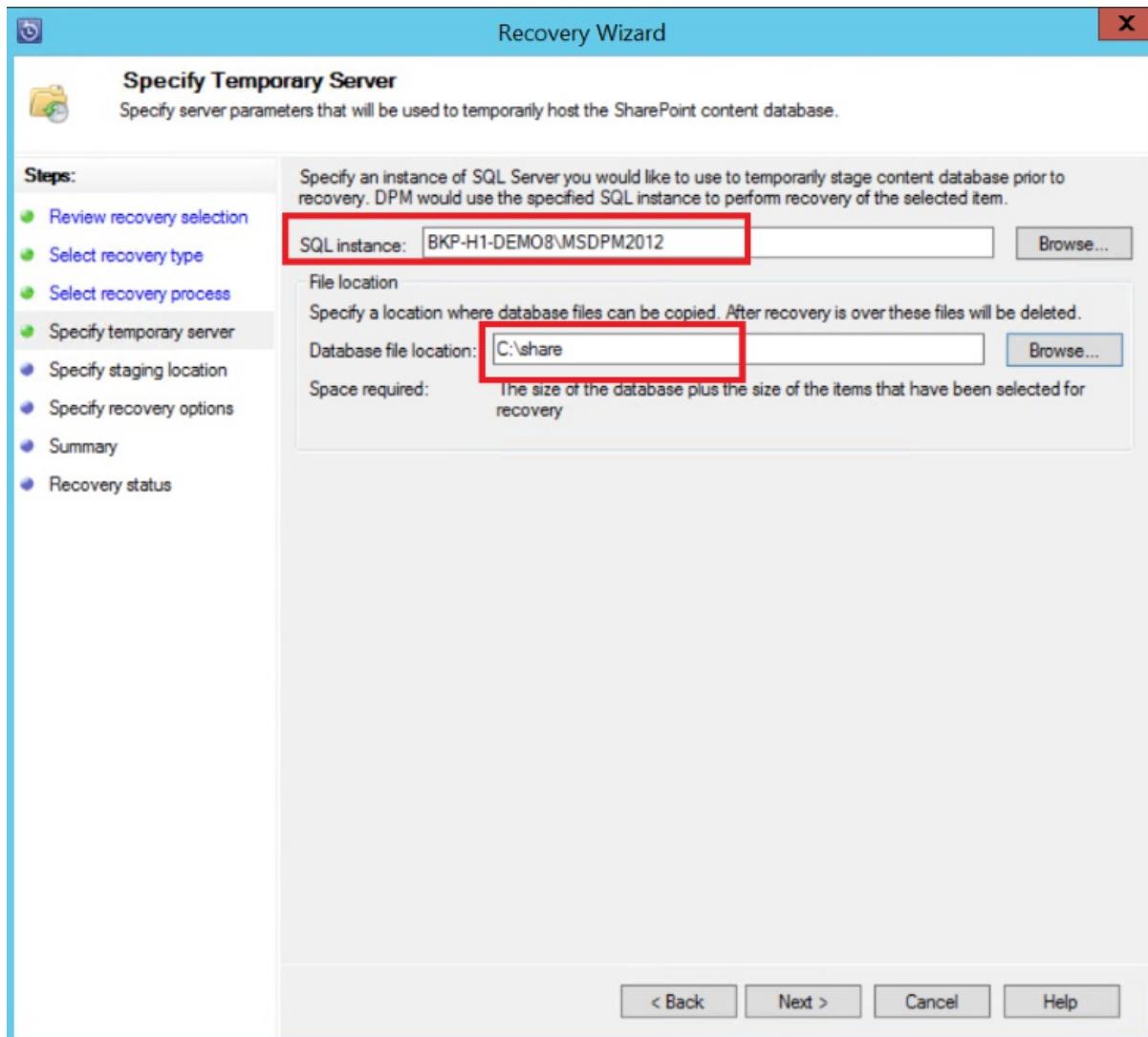
The selection of **Recover to original** in the example recovers the item to the original SharePoint site.

8. Select the **Recovery Process** that you want to use.

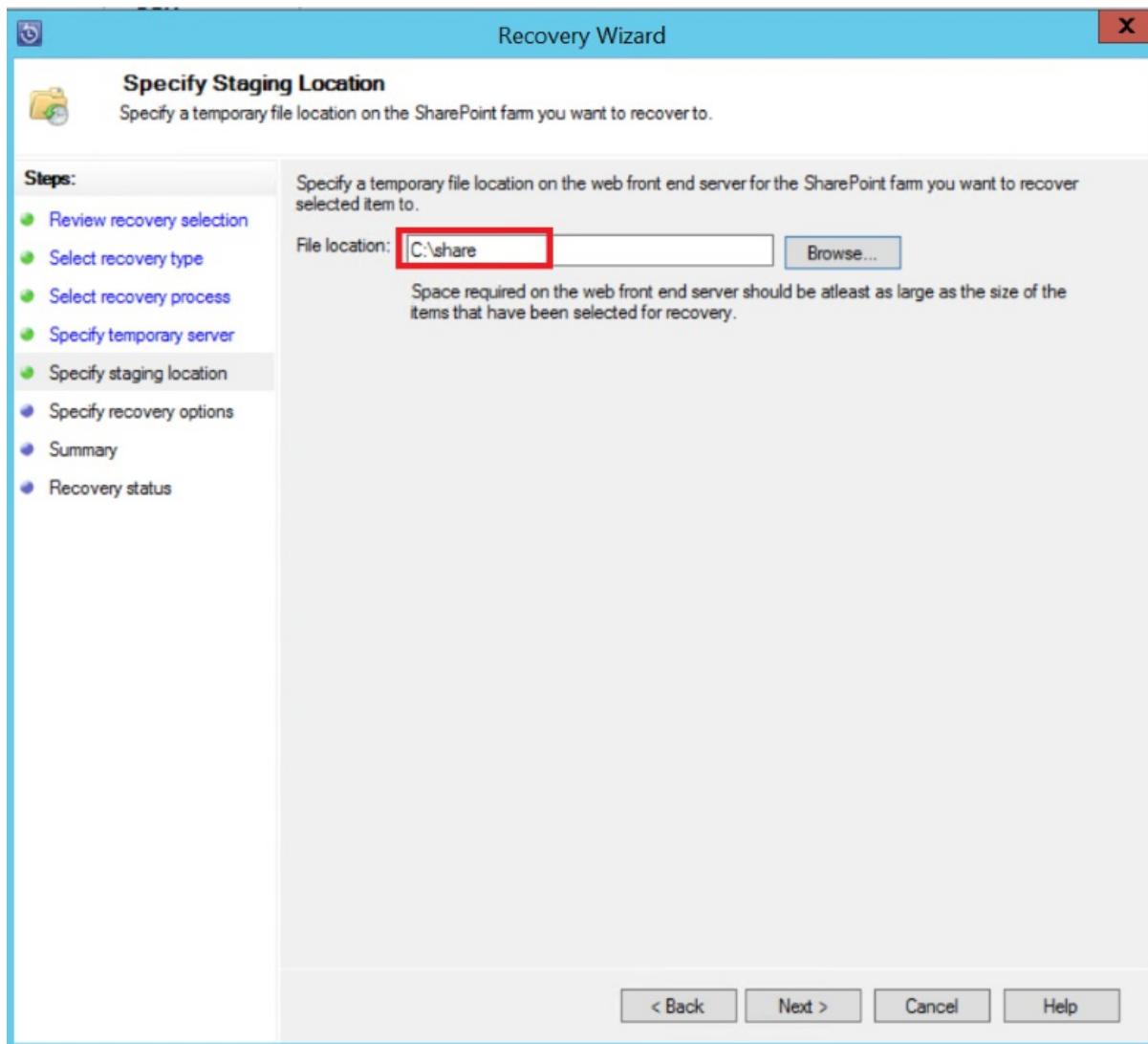
- Select **Recover without using a recovery farm** if the SharePoint farm has not changed and is the same as the recovery point that is being restored.
- Select **Recover using a recovery farm** if the SharePoint farm has changed since the recovery point was created.



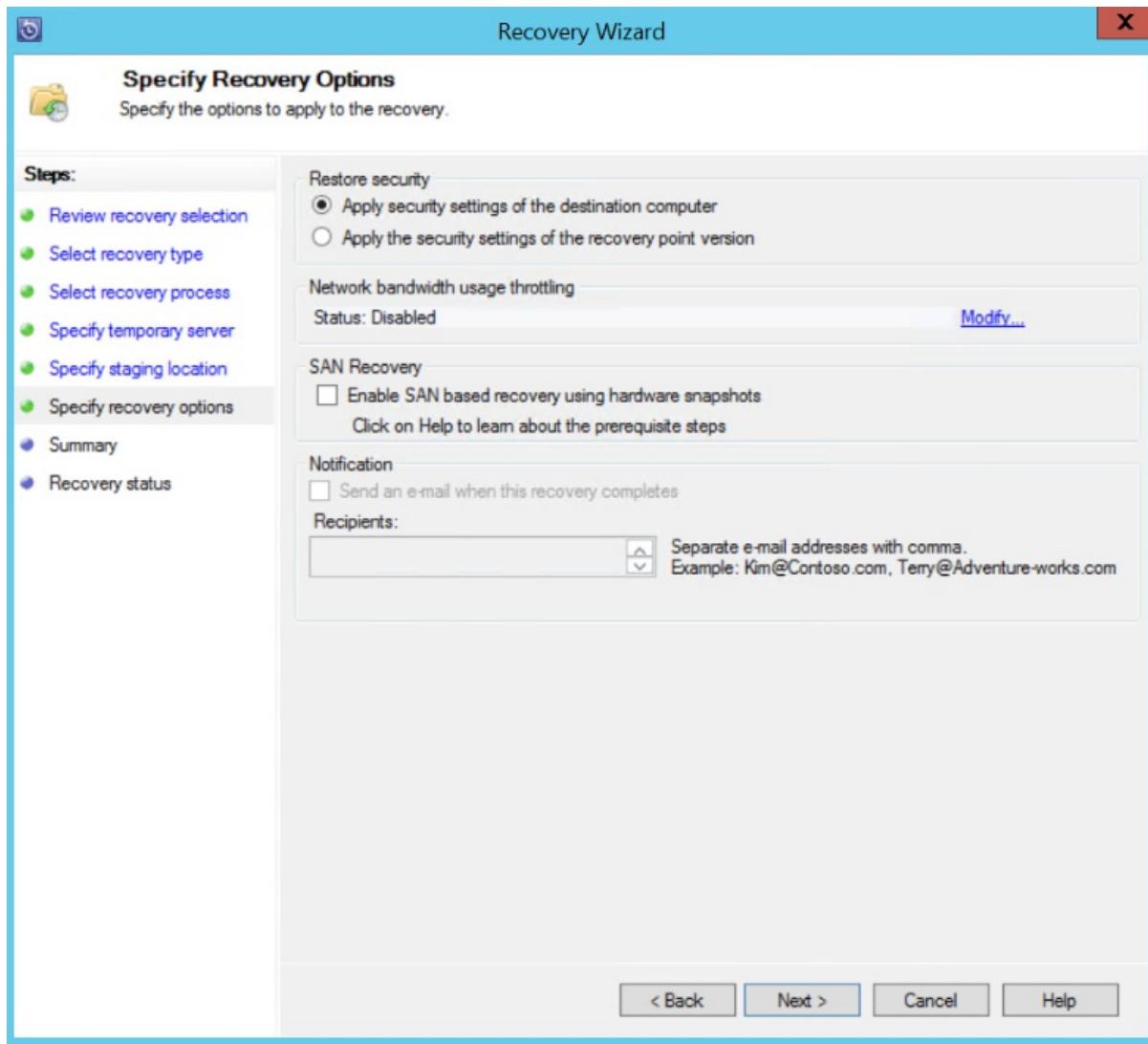
9. Provide a staging SQL Server instance location to recover the database temporarily, and provide a staging file share on MABS and the server that's running SharePoint to recover the item.



MABS attaches the content database that is hosting the SharePoint item to the temporary SQL Server instance. From the content database, it recovers the item and puts it on the staging file location on MABS. The recovered item that's on the staging location now needs to be exported to the staging location on the SharePoint farm.



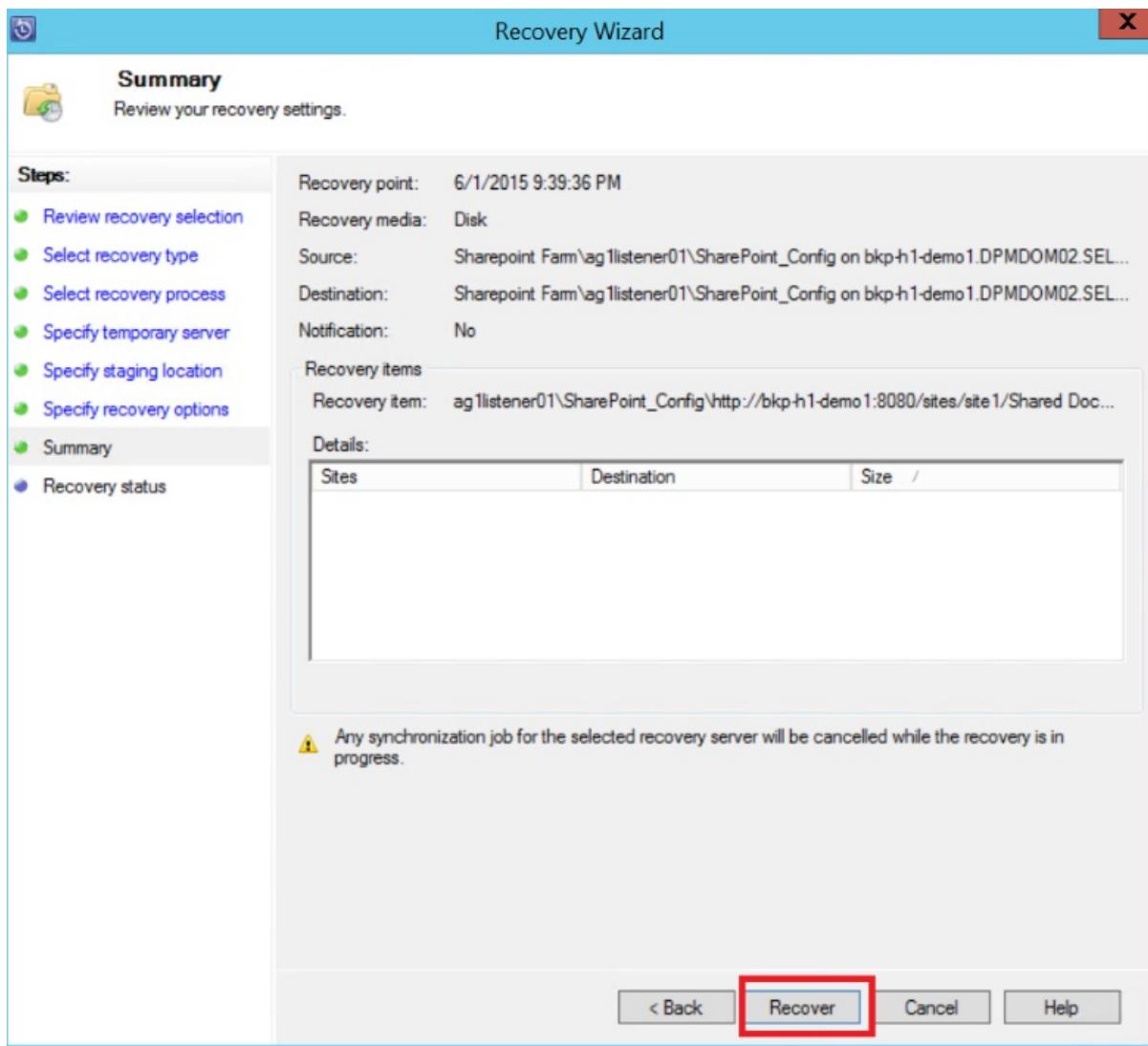
10. Select **Specify recovery options**, and apply security settings to the SharePoint farm or apply the security settings of the recovery point. Click **Next**.



#### NOTE

You can choose to throttle the network bandwidth usage. This minimizes impact to the production server during production hours.

11. Review the summary information, and then click **Recover** to begin recovery of the file.



12. Now select the **Monitoring** tab in the **MABS Administrator Console** to view the **Status** of the recovery.

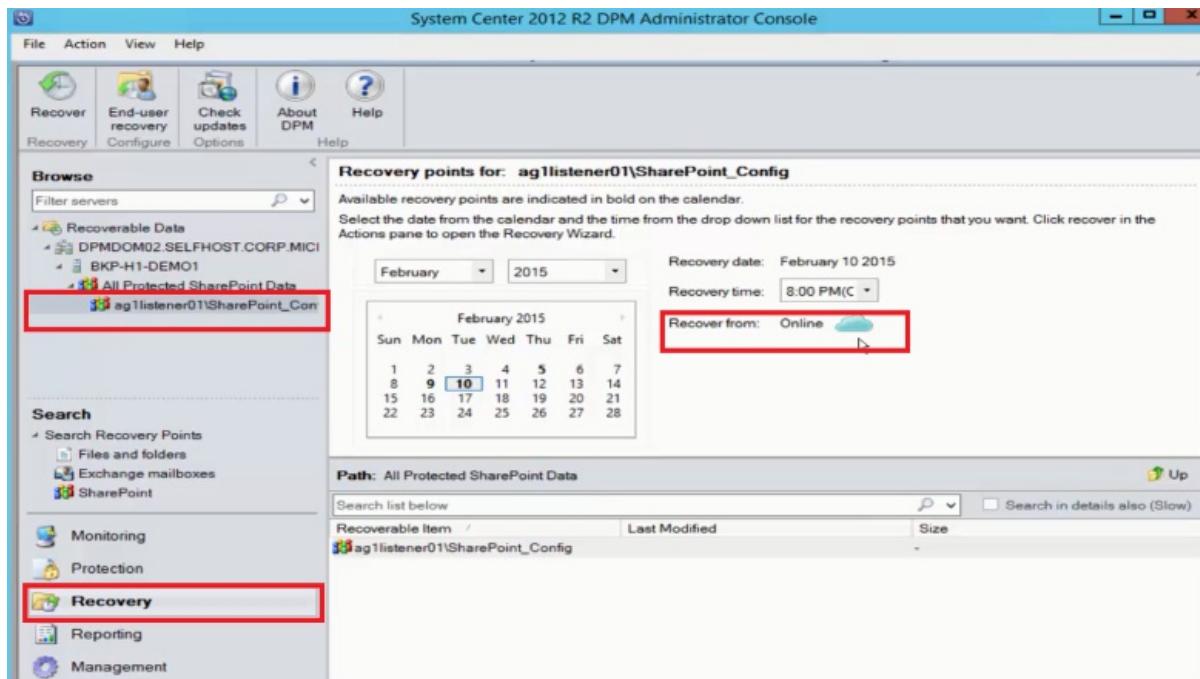
| Source             | Computer           | Protection Gr... | Type                              | Start Time           | End Time             | Duration |
|--------------------|--------------------|------------------|-----------------------------------|----------------------|----------------------|----------|
| bkp-h1-demo8.dp... | -                  | -                | SharePoint export and import task | 2/9/2015 11:24:42 PM | 2/9/2015 11:24:45 PM | 00:00:03 |
| bkp-h1-demo1.dp... | -                  | -                | SharePoint export and import task | 2/9/2015 11:24:42 PM | 2/9/2015 11:24:45 PM | 00:00:03 |
| ag1WSS...          | bkp-h1-demo8.dp... | -                | Disk recovery                     | 2/9/2015 11:24:42 PM | 2/9/2015 11:24:45 PM | 00:00:05 |
| bkp-h1-demo8.dp... | -                  | -                | SharePoint export and import task | 2/9/2015 10:00:00    | 2/9/2015 10:00:00    | 00:00:03 |
| bkp-h1-demo8.dp... | -                  | -                | SharePoint export and import task | 2/9/2015 10:00:00    | 2/9/2015 10:00:00    | 00:00:03 |
| bkp-h1-demo1.dp... | -                  | -                | SharePoint export and import task | 2/9/2015 10:00:00    | 2/9/2015 10:00:00    | 00:00:24 |
| ag1WSS...          | bkp-h1-demo8.dp... | -                | Disk recovery                     | 2/9/2015 10:00:00    | 2/9/2015 10:00:00    | 00:00:05 |
| bkp-h1-demo8.dp... | -                  | -                | SharePoint export and import task | 2/9/2015 10:00:00    | 2/9/2015 10:00:00    | 00:00:03 |
| bkp-h1-demo8.dp... | -                  | -                | SharePoint export and import task | 2/9/2015 9:38:00     | 2/9/2015 9:38:00     | 00:00:03 |

#### NOTE

The file is now restored. You can refresh the SharePoint site to check the restored file.

# Restore a SharePoint database from Azure by using DPM

1. To recover a SharePoint content database, browse through various recovery points (as shown previously), and select the recovery point that you want to restore.

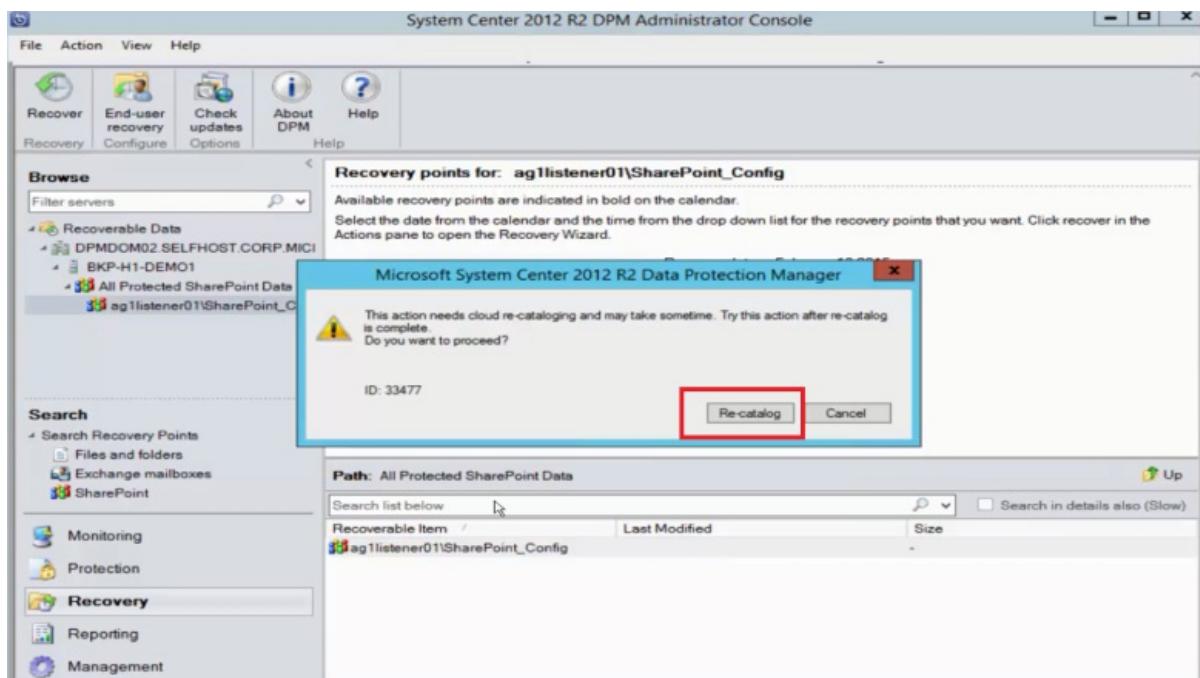


2. Double-click the SharePoint recovery point to show the available SharePoint catalog information.

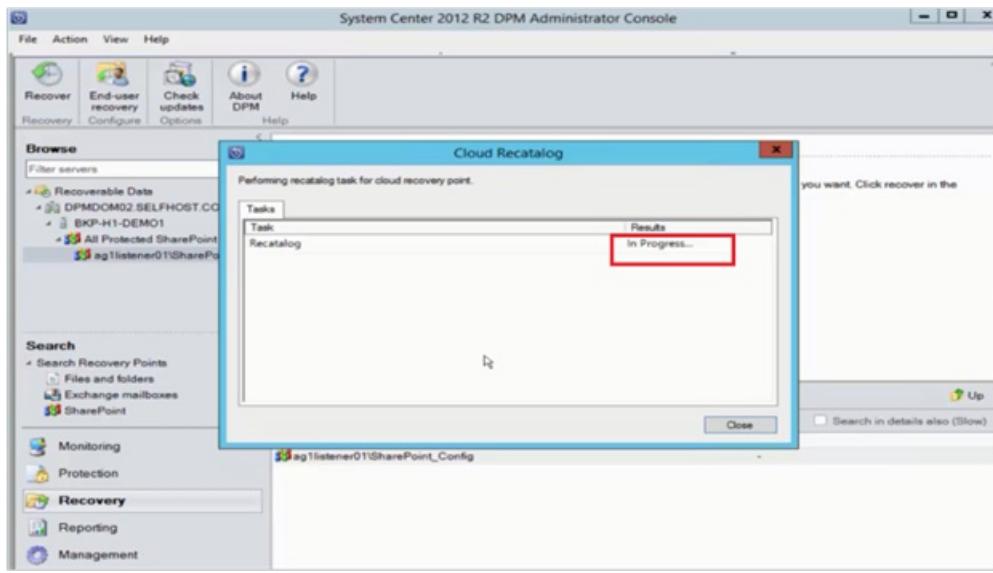
## NOTE

Because the SharePoint farm is protected for long-term retention in Azure, no catalog information (metadata) is available on MABS. As a result, whenever a point-in-time SharePoint content database needs to be recovered, you need to catalog the SharePoint farm again.

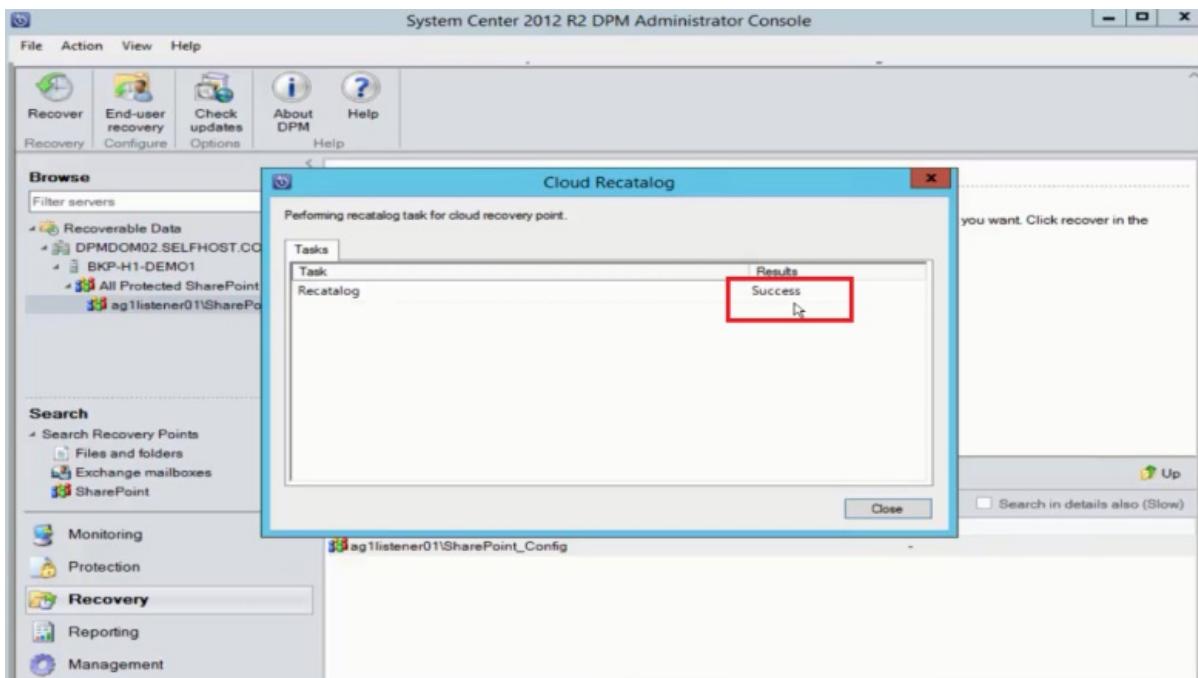
3. Click **Re-catalog**.



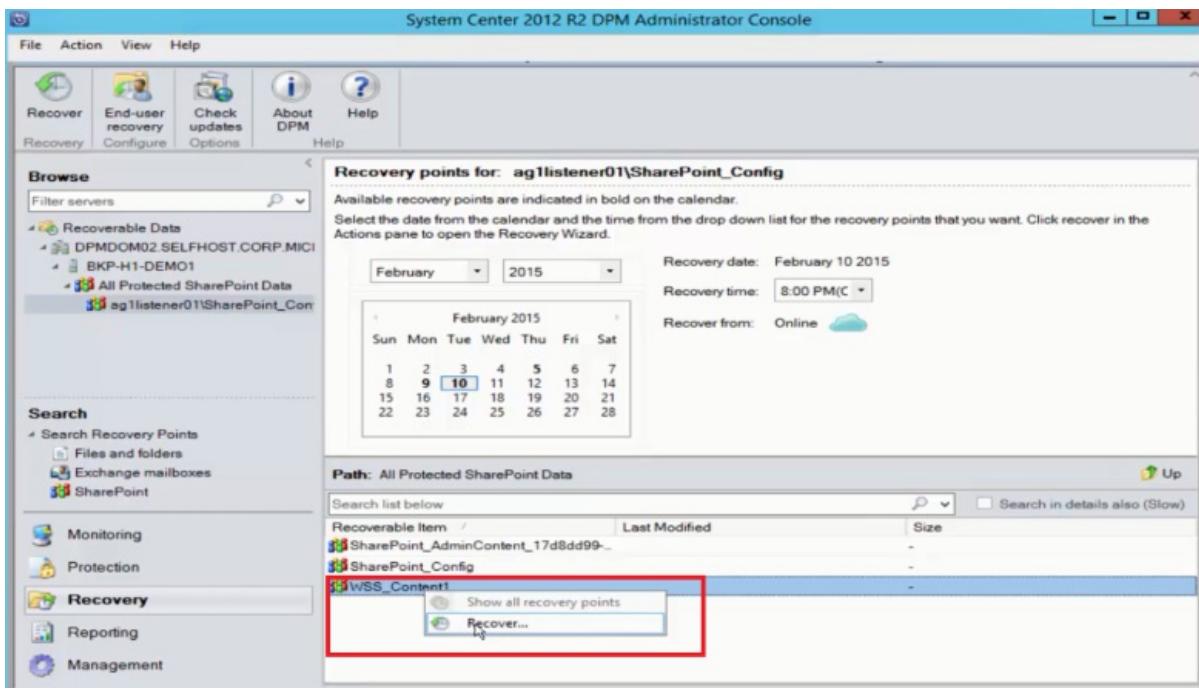
The **Cloud Recatalog** status window opens.



After cataloging is finished, the status changes to *Success*. Click **Close**.



4. Click the SharePoint object shown in the MABS **Recovery** tab to get the content database structure. Right-click the item, and then click **Recover**.



5. At this point, follow the recovery steps earlier in this article to recover a SharePoint content database from disk.

## Next steps

See the [Back up Exchange server](#) article. See the [Back up SQL Server](#) article.

# Back up SQL Server to Azure by using Azure Backup Server

2/20/2020 • 6 minutes to read • [Edit Online](#)

This article helps you set up backups of SQL Server databases by using Microsoft Azure Backup Server (MABS).

To back up a SQL Server database and recover it from Azure:

1. Create a backup policy to protect SQL Server databases in Azure.
2. Create on-demand backup copies in Azure.
3. Recover the database in Azure.

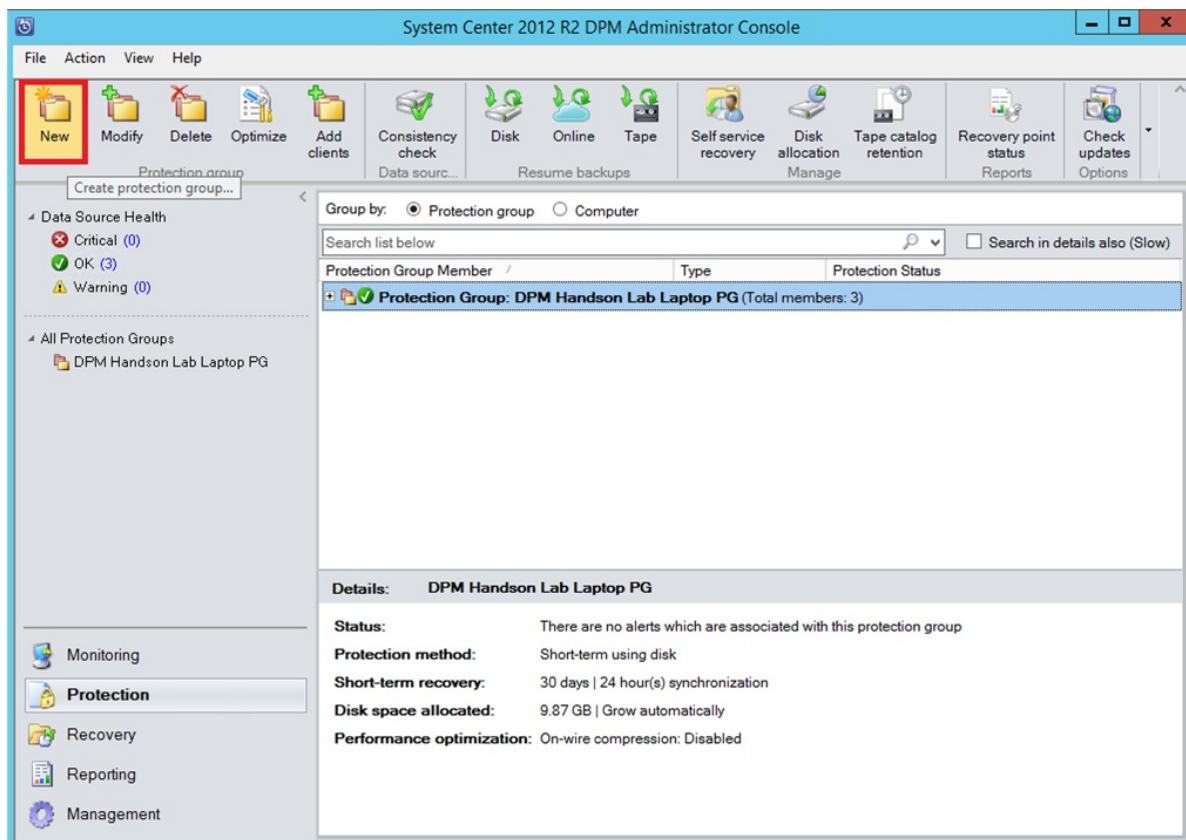
## Before you start

Before you begin, ensure that you have [installed and prepared Azure Backup Server](#).

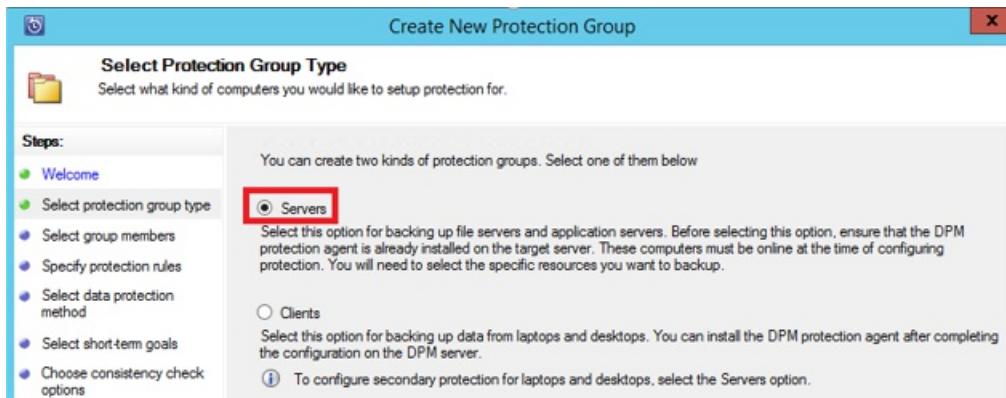
## Create a backup policy

To protect SQL Server databases in Azure, first create a backup policy:

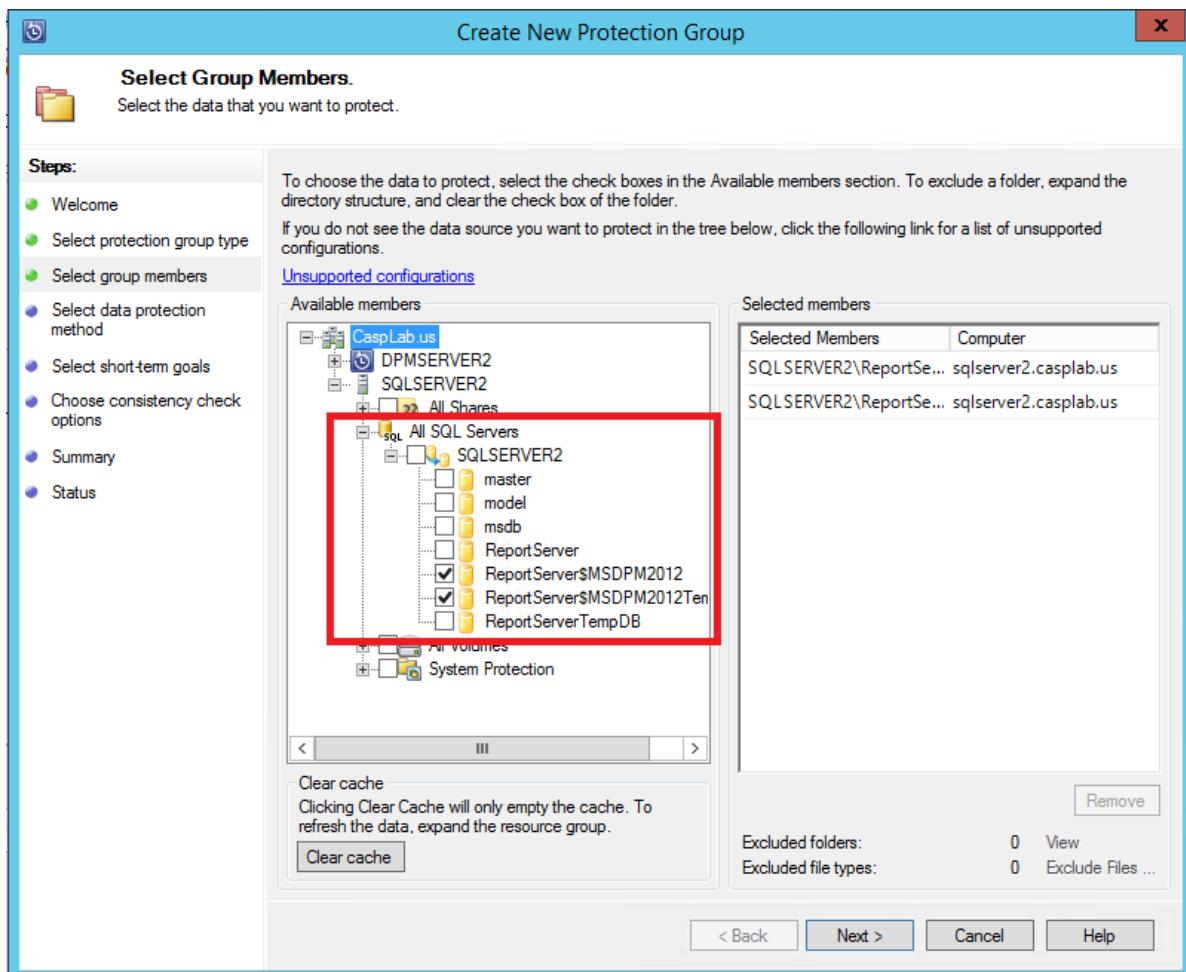
1. In Azure Backup Server, select the **Protection** workspace.
2. Select **New** to create a protection group.



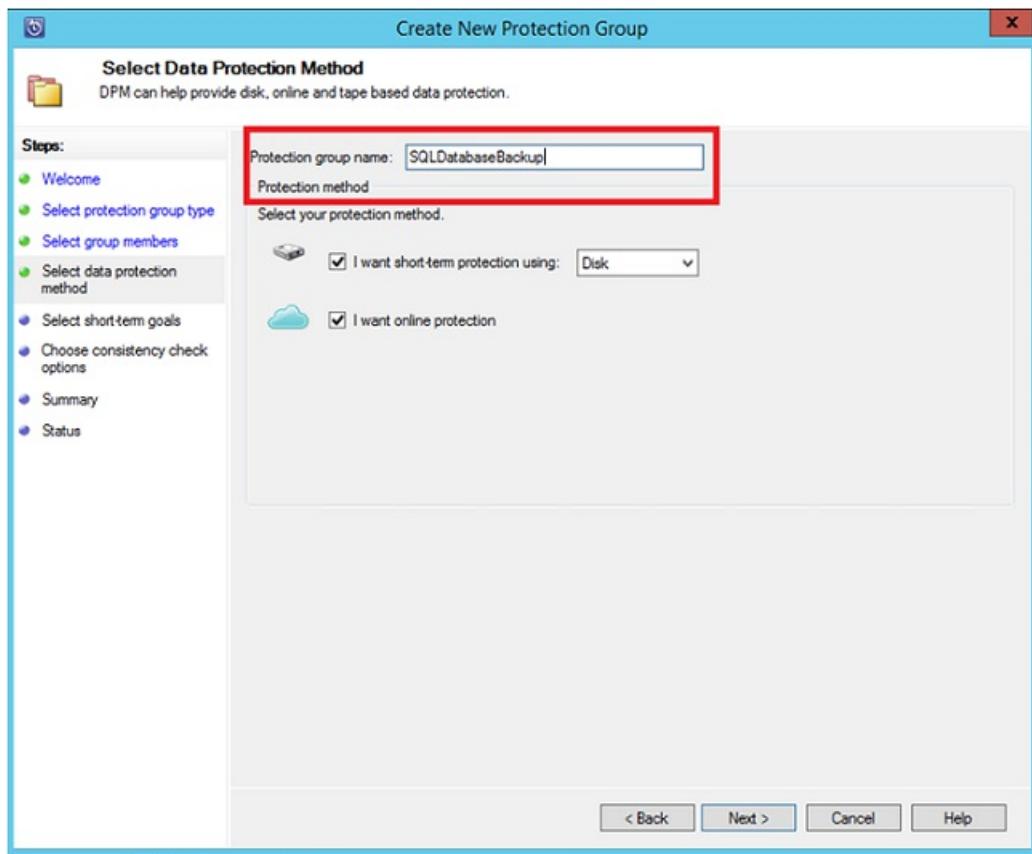
3. On the start page, review the guidance about creating a protection group. Then select **Next**.
4. For the protection group type, select **Servers**.



5. Expand the SQL Server machine where the databases that you want to back up are located. You see the data sources that can be backed up from that server. Expand **All SQL Shares** and then select the databases that you want to back up. In this example, we select ReportServer\$MSDPM2012 and ReportServer\$MSDPM2012TempDB. Select **Next**.

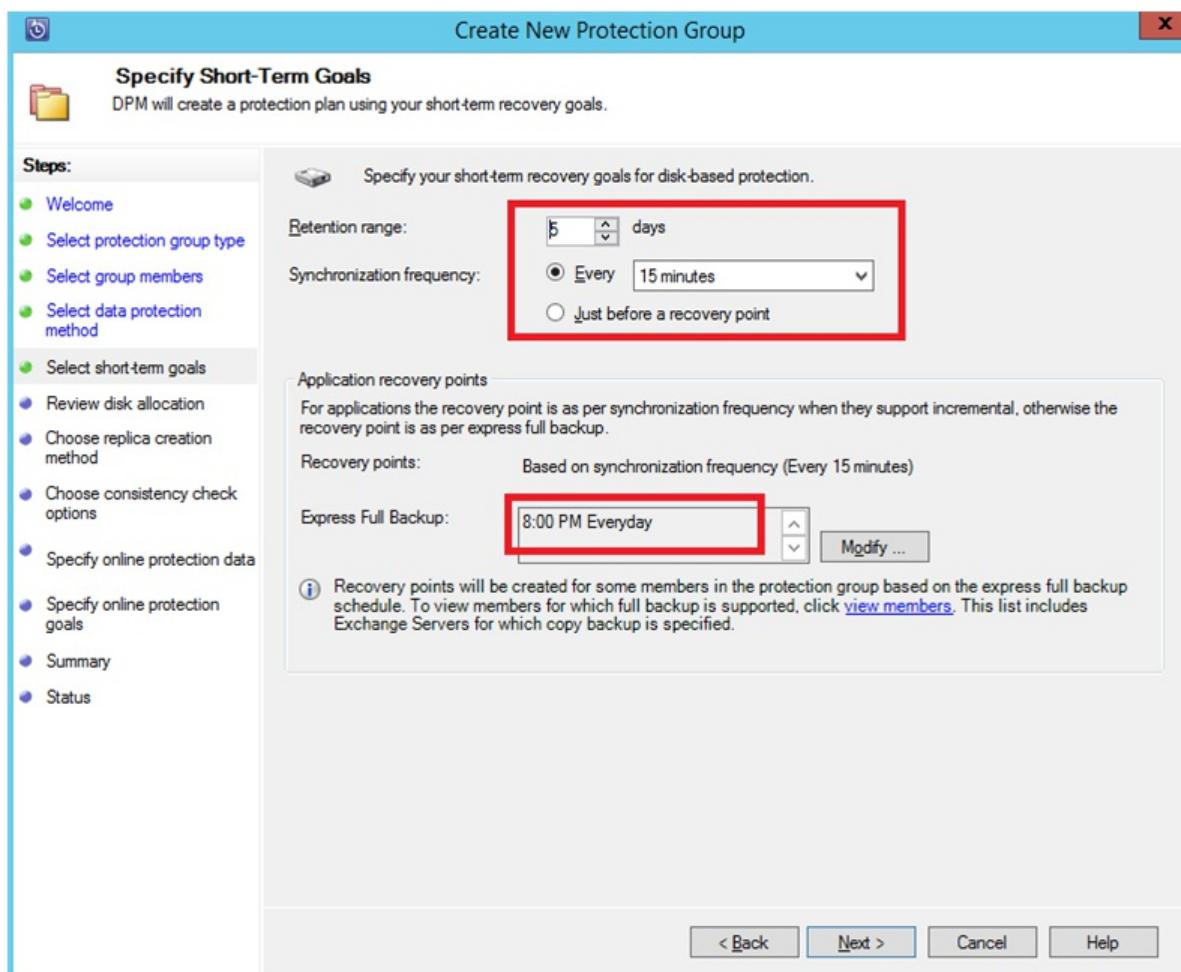


6. Name the protection group and then select **I want online protection**.



7. On the **Specify Short-Term Goals** page, include the necessary inputs to create backup points to the disk.

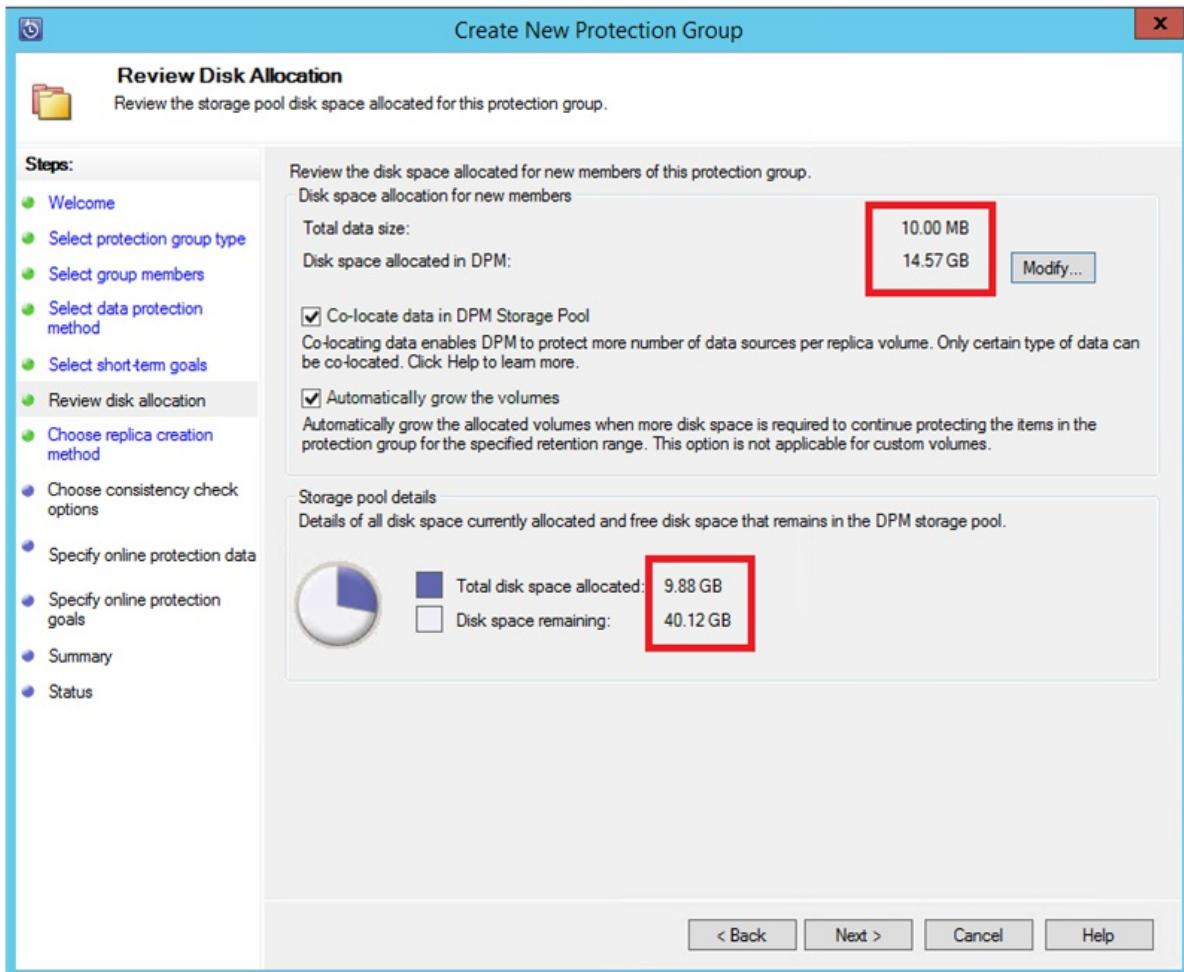
In this example, **Retention range** is set to 5 days. The backup **Synchronization frequency** is set to once every 15 minutes. **Express Full Backup** is set to 8:00 PM.



#### NOTE

In this example, a backup point is created at 8:00 PM every day. The data that has been modified since the previous day's 8:00 PM backup point is transferred. This process is called **Express Full Backup**. Although the transaction logs are synchronized every 15 minutes, if we need to recover the database at 9:00 PM, then the point is created by replaying the logs from the last express full backup point, which is 8:00 PM in this example.

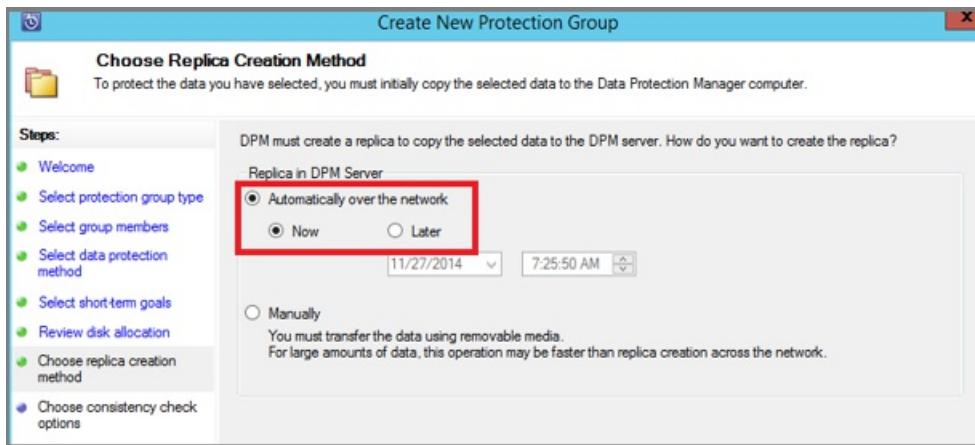
8. Select **Next**. MABS shows the overall storage space available. It also shows the potential disk space utilization.



By default, MABS creates one volume per data source (SQL Server database). The volume is used for the initial backup copy. In this configuration, Logical Disk Manager (LDM) limits MABS protection to 300 data sources (SQL Server databases). To work around this limitation, select **Co-locate data in DPM Storage Pool**. If you use this option, MABS uses a single volume for multiple data sources. This setup allows MABS to protect up to 2,000 SQL Server databases.

If you select **Automatically grow the volumes**, then MABS can account for the increased backup volume as the production data grows. If you don't select **Automatically grow the volumes**, then MABS limits the backup storage to the data sources in the protection group.

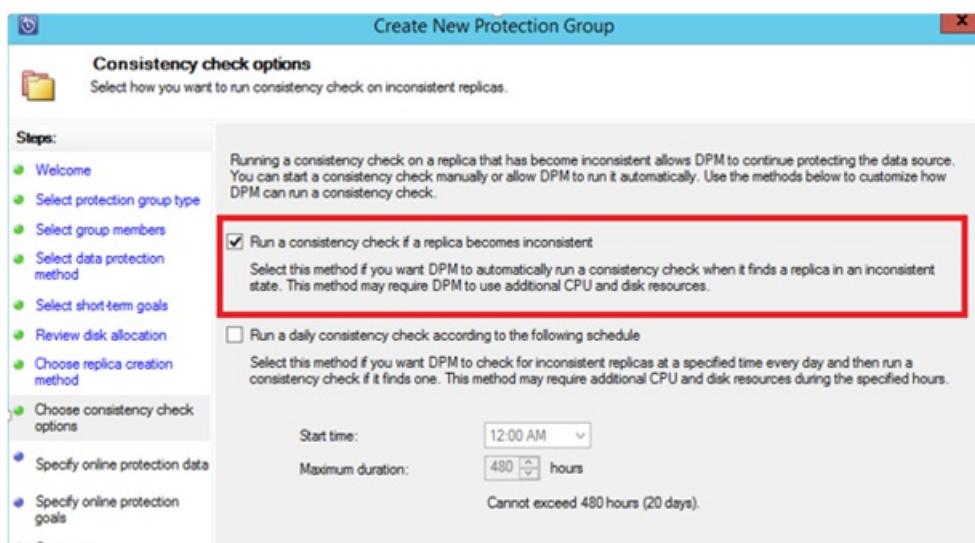
9. If you're an administrator, you can choose to transfer this initial backup**Automatically over the network** and choose the time of transfer. Or choose to **Manually** transfer the backup. Then select **Next**.



The initial backup copy requires the transfer of the entire data source (SQL Server database). The backup data moves from the production server (SQL Server machine) to MABS. If this backup is large, then transferring the data over the network could cause bandwidth congestion. For this reason, administrators can choose to use removable media to transfer the initial backup **Manually**. Or they can transfer the data **Automatically over the network** at a specified time.

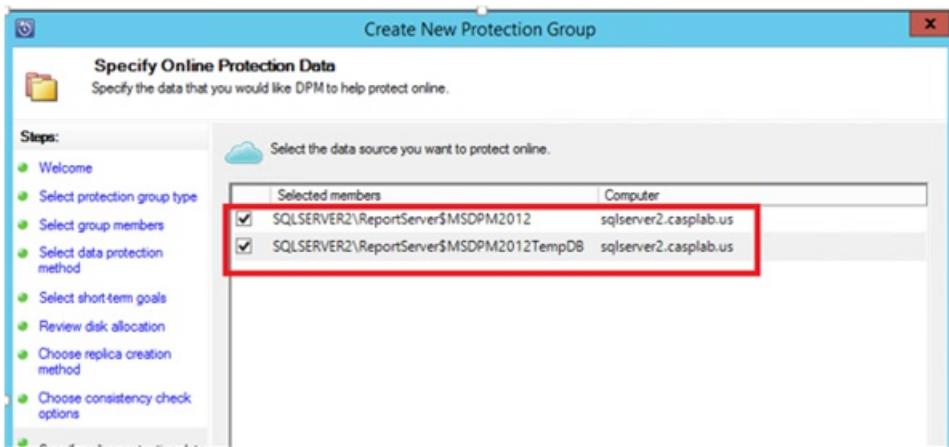
After the initial backup finishes, backups continue incrementally on the initial backup copy. Incremental backups tend to be small and are easily transferred across the network.

10. Choose when to run a consistency check. Then select **Next**.

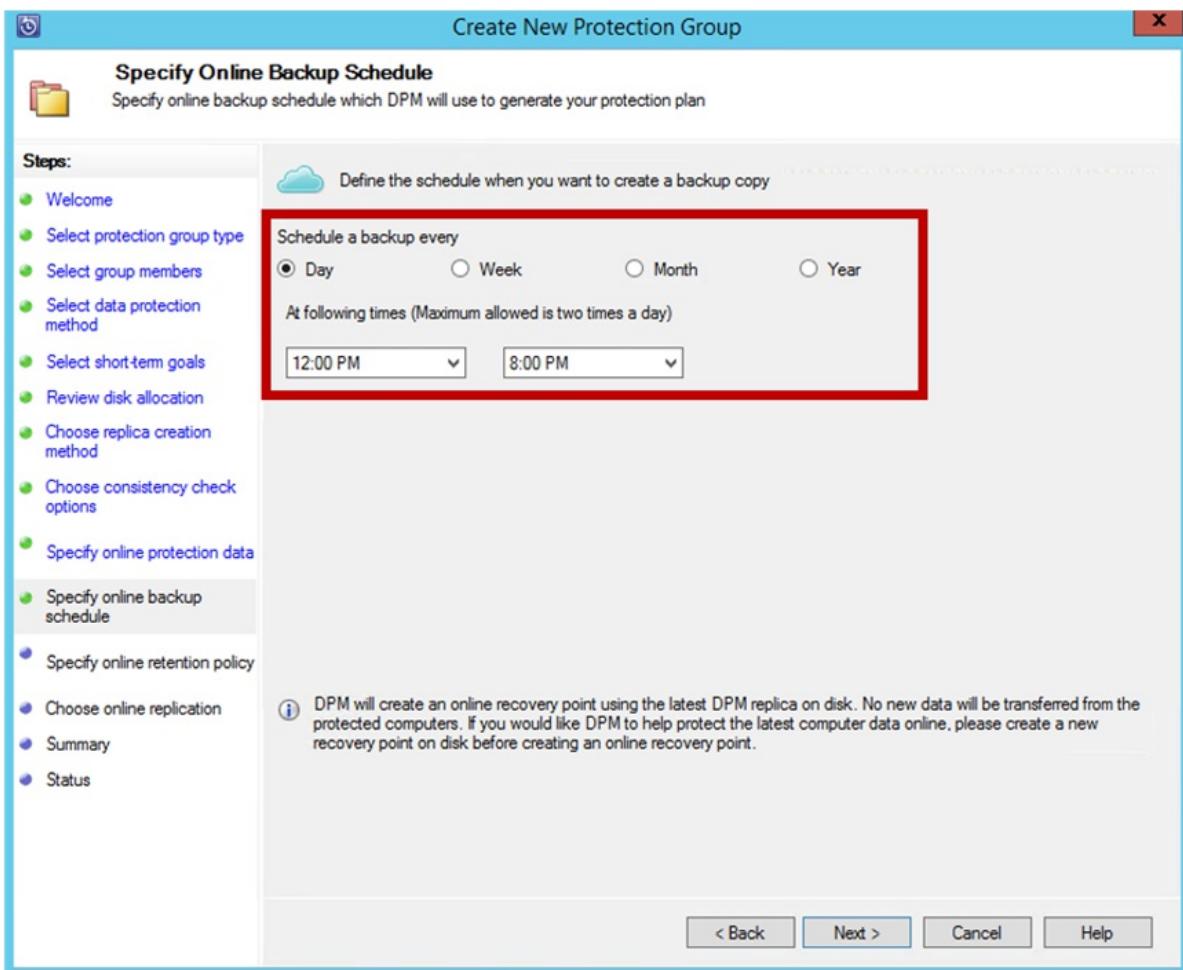


MABS can run a consistency check on the integrity of the backup point. It calculates the checksum of the backup file on the production server (the SQL Server machine in this example) and the backed-up data for that file in MABS. If the check finds a conflict, then the backed-up file in MABS is assumed to be corrupt. MABS fixes the backed-up data by sending the blocks that correspond to the checksum mismatch. Because the consistency check is a performance-intensive operation, administrators can choose to schedule the consistency check or run it automatically.

11. Select the data sources to protect in Azure. Then select **Next**.



12. If you're an administrator, you can choose backup schedules and retention policies that suit your organization's policies.



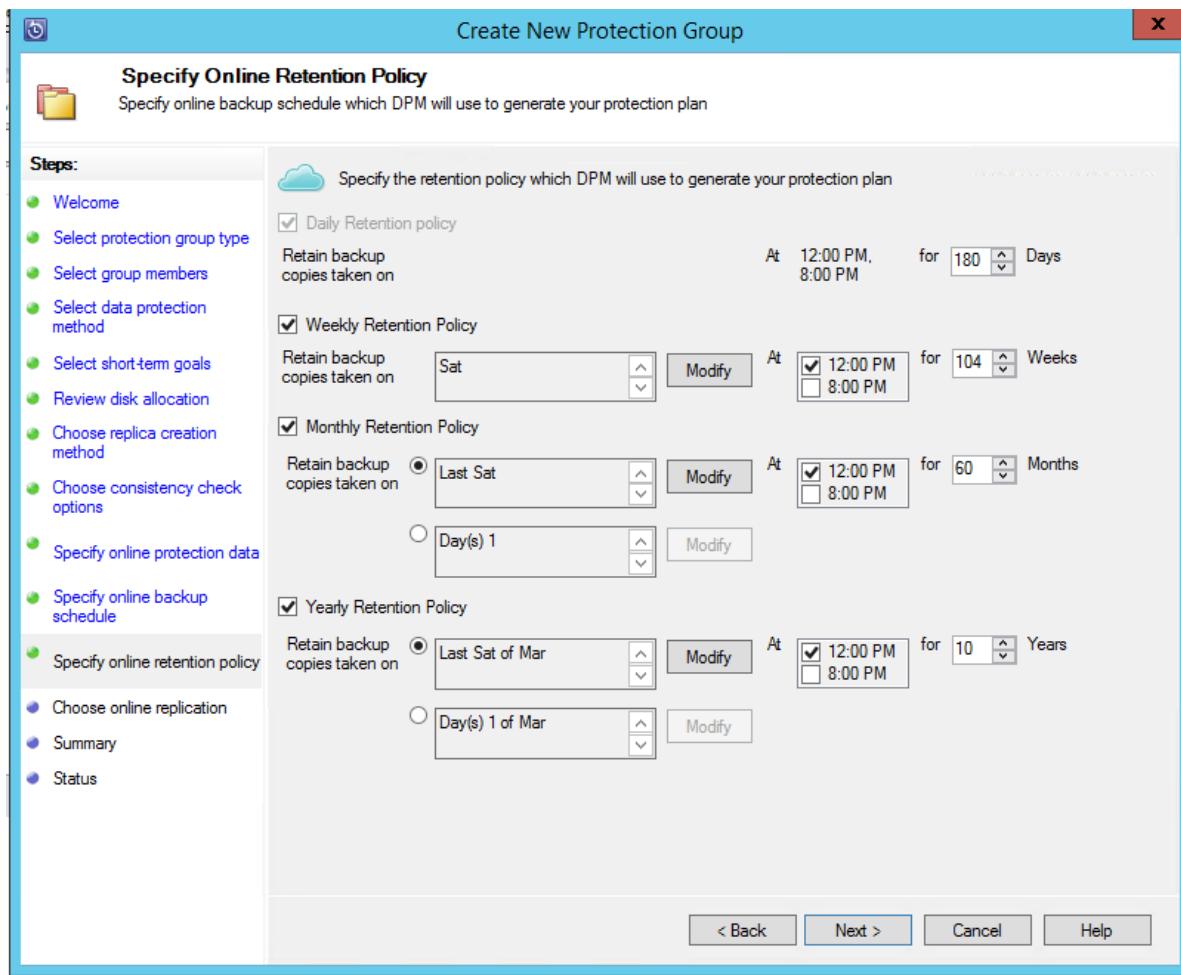
In this example, backups are taken daily at 12:00 PM and 8:00 PM.

#### TIP

For quick recovery, keep a few short-term recovery points on your disk. These recovery points are used for operational recovery. Azure serves as a good offsite location, providing higher SLAs and guaranteed availability.

Use Data Protection Manager (DPM) to schedule Azure Backups after the local disk backups finish. When you follow this practice, the latest disk backup is copied to Azure.

13. Choose the retention policy schedule. For more information about how the retention policy works, see [Use Azure Backup to replace your tape infrastructure](#).



In this example:

- Backups are taken daily at 12:00 PM and 8:00 PM. They're kept for 180 days.
- The backup on Saturday at 12:00 PM is kept for 104 weeks.
- The backup from the last Saturday of the month at 12:00 PM is kept for 60 months.
- The backup from the last Saturday of March at 12:00 PM is kept for 10 years.

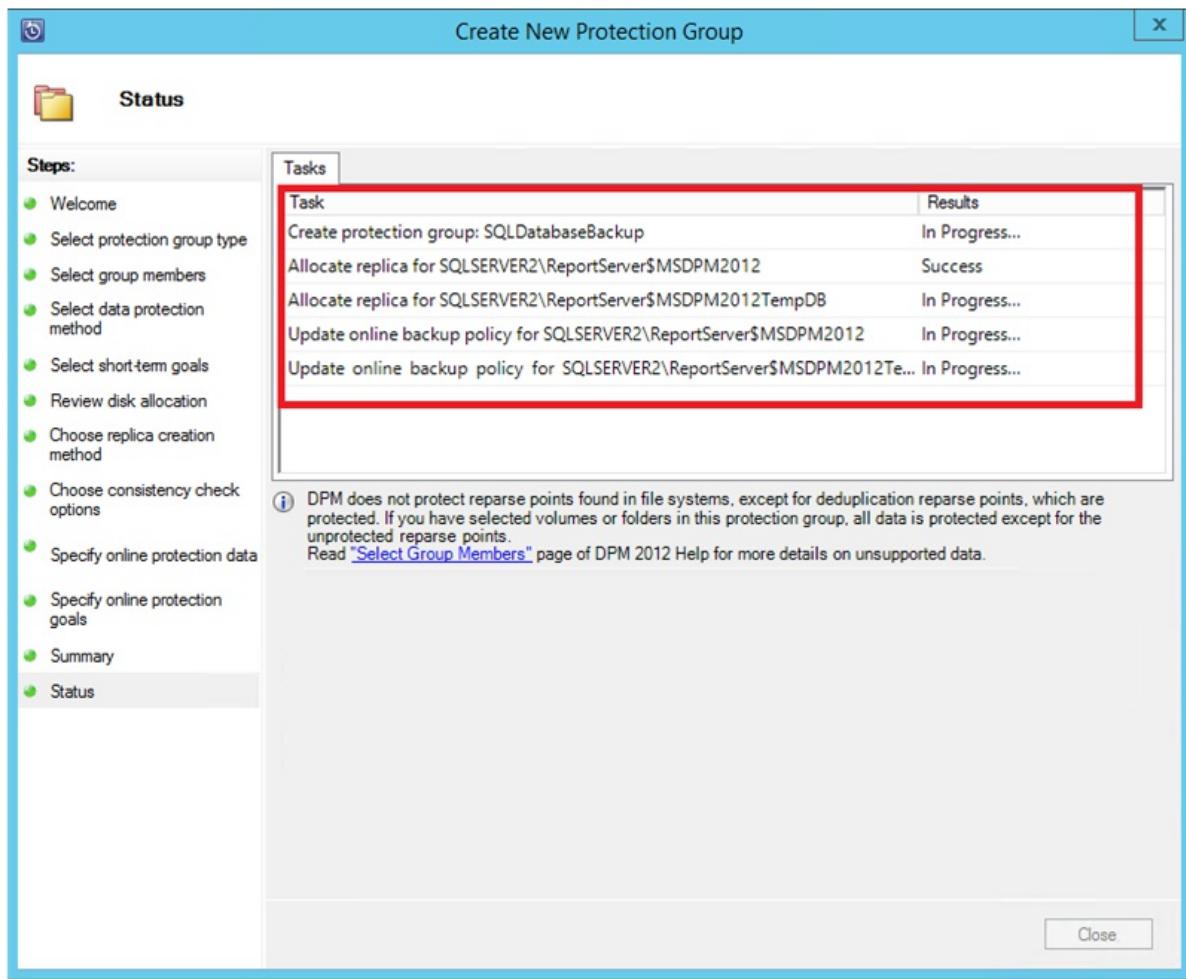
After you choose a retention policy, select **Next**.

14. Choose how to transfer the initial backup copy to Azure.

- The **Automatically over the network** option follows your backup schedule to transfer the data to Azure.
- For more information about **Offline Backup**, see [Overview of Offline Backup](#).

After you choose a transfer mechanism, select **Next**.

15. On the **Summary** page, review the policy details. Then select **Create group**. You can select **Close** and watch the job progress in the **Monitoring** workspace.



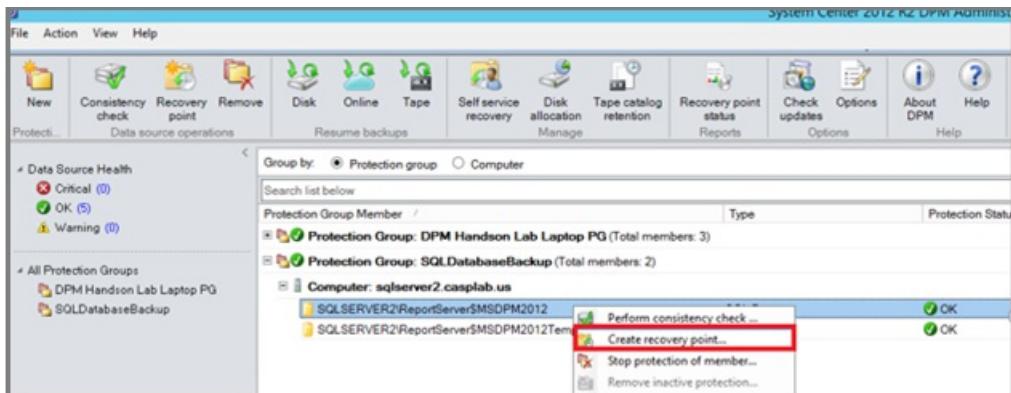
## Create on-demand backup copies of a SQL Server database

A recovery point is created when the first backup occurs. Rather than waiting for the schedule to run, you can manually trigger the creation of a recovery point:

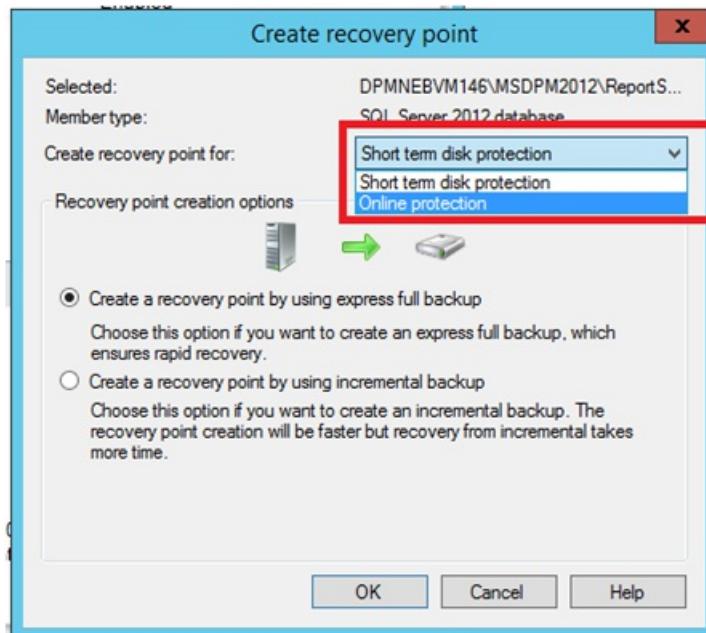
1. In the protection group, make sure the database status is **OK**.

| Protection Group Member                                        | Type     | Protection Status |
|----------------------------------------------------------------|----------|-------------------|
| Protection Group: DPM Handson Lab Laptop PG (Total members: 3) |          | Online Protection |
| Protection Group: SQLDatabaseBackup (Total members: 2)         |          |                   |
| Computer: sqlserver2.casplab.us                                |          |                   |
| SQLSERVER2\ReportSer...                                        | SQL Data | OK<br>Enabled     |
| SQLSERVER2\ReportSer...                                        | SQL Data | OK<br>Enabled     |

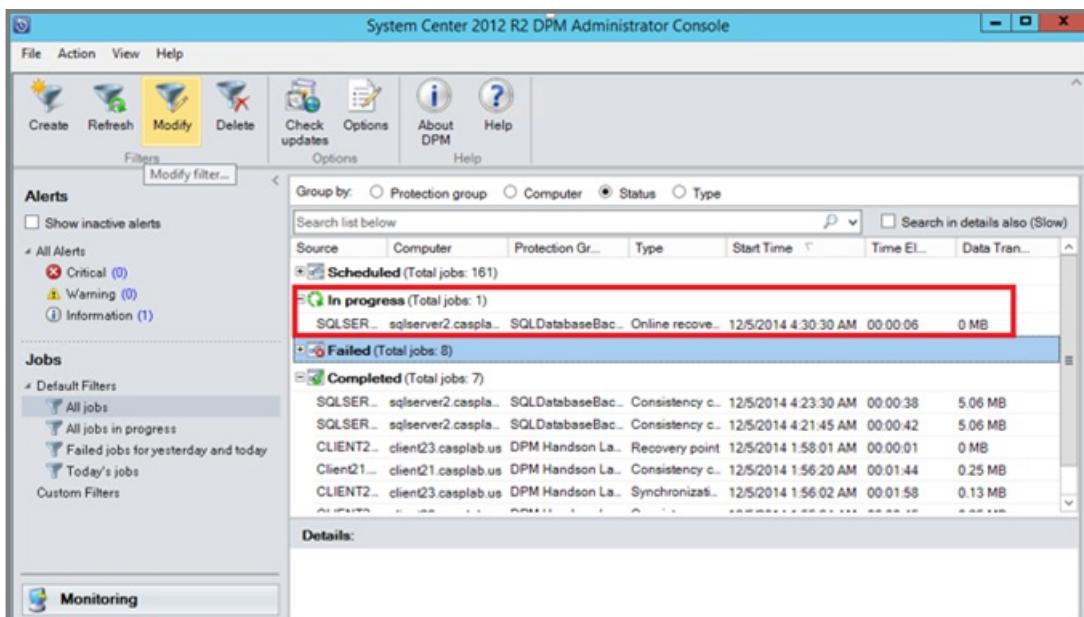
2. Right-click the database and then select **Create recovery point**.



3. In the drop-down menu, select **Online protection**. Then select **OK** to start the creation of a recovery point in Azure.



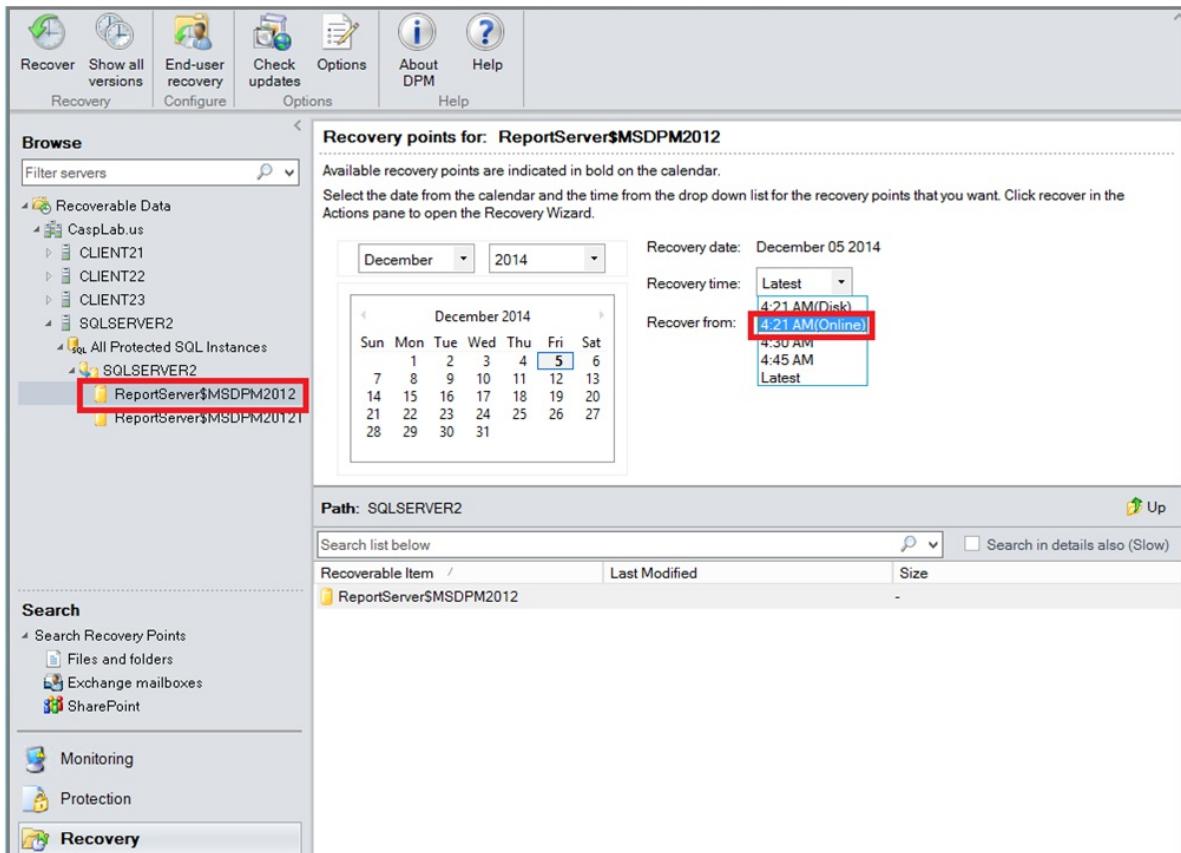
4. You can view the job progress in the **Monitoring** workspace.



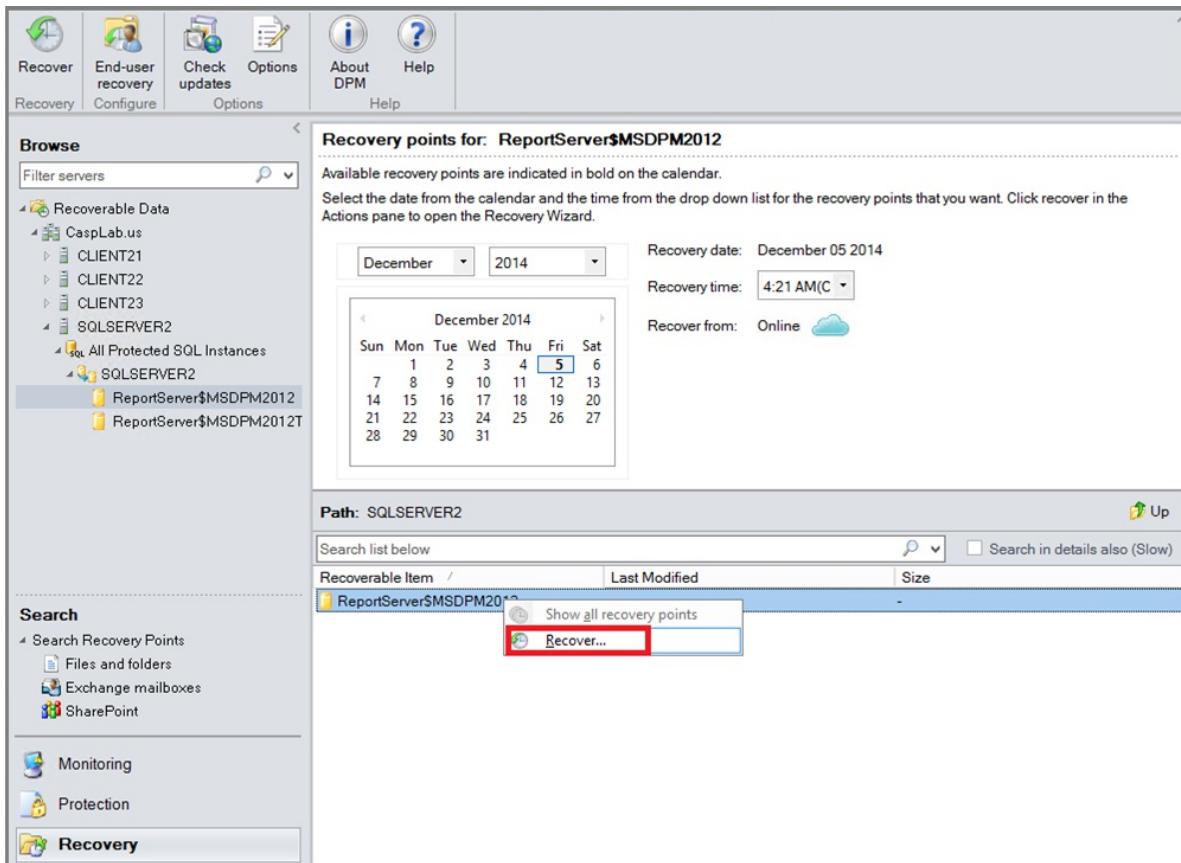
## Recover a SQL Server database from Azure

To recover a protected entity, such as a SQL Server database, from Azure:

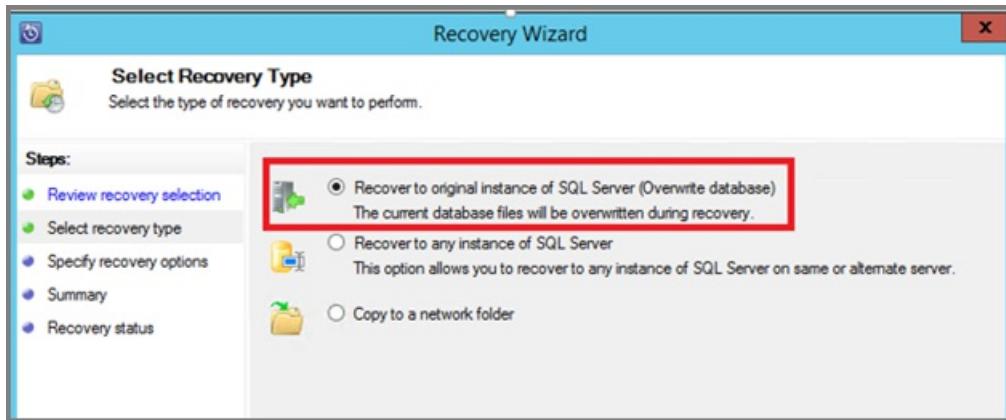
1. Open the DPM server management console. Go to the **Recovery** workspace to see the servers that DPM backs up. Select the database (in this example, ReportServer\$MSDPM2012). Select a **Recovery time** that ends with **Online**.



2. Right-click the database name and select **Recover**.



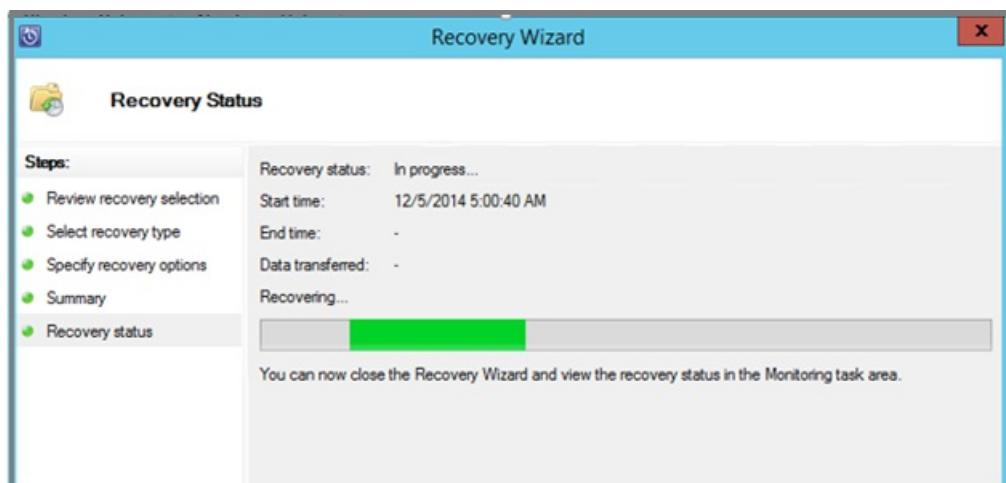
3. DPM shows the details of the recovery point. Select **Next**. To overwrite the database, select the recovery type **Recover to original instance of SQL Server**. Then select **Next**.



In this example, DPM allows the recovery of the database to another SQL Server instance or to a standalone network folder.

4. On the **Specify Recovery Options** page, you can select the recovery options. For example, you can choose **Network bandwidth usage throttling** to throttle the bandwidth that recovery uses. Then select **Next**.
5. On the **Summary** page, you see the current recovery configuration. Select **Recover**.

The recovery status shows the database being recovered. You can select **Close** to close the wizard and view the progress in the **Monitoring** workspace.



When the recovery is complete, the restored database is consistent with the application.

## Next steps

For more information, see [Azure Backup FAQ](#).

# Back up system state and restore to bare metal by using Azure Backup Server

2/20/2020 • 15 minutes to read • [Edit Online](#)

Azure Backup Server backs up system state and provides bare-metal recovery (BMR) protection.

- **System state backup:** Backs up operating system files. This backup allows you to recover when a computer starts, but system files and the registry are lost. A system state backup includes the following elements:
  - Domain member: Boot files, COM+ class registration database, registry
  - Domain controller: Windows Server Active Directory (NTDS), boot files, COM+ class registration database, registry, system volume (SYSVOL)
  - Computer that runs cluster services: Cluster server metadata
  - Computer that runs certificate services: Certificate data
- **Bare-metal backup:** Backs up operating system files and all data on critical volumes, except for user data. By definition, a BMR backup includes a system state backup. It provides protection when a computer won't start and you have to recover everything.

The following table summarizes what you can back up and recover. For information about app versions that system state and BMR can protect, see [What does Azure Backup Server back up?](#).

| BACKUP                                                                                         | ISSUE                             | RECOVER FROM AZURE BACKUP SERVER BACKUP | RECOVER FROM SYSTEM STATE BACKUP | BMR |
|------------------------------------------------------------------------------------------------|-----------------------------------|-----------------------------------------|----------------------------------|-----|
| <b>File data</b><br><br>Regular data backup<br><br>BMR/system state backup                     | Lost file data                    | Y                                       | N                                | N   |
| <b>File data</b><br><br>Azure Backup Server backup of file data<br><br>BMR/system state backup | Lost or damaged operating system  | N                                       | Y                                | Y   |
| <b>File data</b><br><br>Azure Backup Server backup of file data<br><br>BMR/system state backup | Lost server (data volumes intact) | N                                       | N                                | Y   |

| <b>BACKUP</b>                                                                                                                    | <b>ISSUE</b>                            | <b>RECOVER FROM AZURE BACKUP SERVER BACKUP</b> | <b>RECOVER FROM SYSTEM STATE BACKUP</b> | <b>BMR</b>                                                        |
|----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|------------------------------------------------|-----------------------------------------|-------------------------------------------------------------------|
| <b>File data</b><br><br>Azure Backup Server backup of file data<br><br>BMR/system state backup                                   | Lost server (data volumes lost)         | Y                                              | N                                       | Y<br><br>BMR, followed by regular recovery of backed-up file data |
| <b>SharePoint data</b><br><br>Azure Backup Server backup of farm data<br><br>BMR/system state backup                             | Lost site, lists, list items, documents | Y                                              | N                                       | N                                                                 |
| <b>SharePoint data</b><br><br>Azure Backup Server backup of farm data<br><br>BMR/system state backup                             | Lost or damaged operating system        | N                                              | Y                                       | Y                                                                 |
| <b>SharePoint data</b><br><br>Azure Backup Server backup of farm data<br><br>BMR/system state backup                             | Disaster recovery                       | N                                              | N                                       | N                                                                 |
| Windows Server 2012 R2 Hyper-V<br><br>Azure Backup Server backup of Hyper-V host or guest<br><br>BMR/system state backup of host | Lost VM                                 | Y                                              | N                                       | N                                                                 |
| Hyper-V<br><br>Azure Backup Server backup of Hyper-V host or guest<br><br>BMR/system state backup of host                        | Lost or damaged operating system        | N                                              | Y                                       | Y                                                                 |

| BACKUP                                                                                                    | ISSUE                                          | RECOVER FROM AZURE BACKUP SERVER BACKUP | RECOVER FROM SYSTEM STATE BACKUP | BMR                                                                     |
|-----------------------------------------------------------------------------------------------------------|------------------------------------------------|-----------------------------------------|----------------------------------|-------------------------------------------------------------------------|
| Hyper-V<br><br>Azure Backup Server backup of Hyper-V host or guest<br><br>BMR/system state backup of host | Lost Hyper-V host (VMs intact)                 | N                                       | N                                | Y                                                                       |
| Hyper-V<br><br>Azure Backup Server backup of Hyper-V host or guest<br><br>BMR/system state backup of host | Lost Hyper-V host (VMs lost)                   | N                                       | N                                | Y<br><br>BMR, followed by regular Azure Backup Server recovery          |
| SQL Server/Exchange<br><br>Azure Backup Server app backup<br><br>BMR/system state backup                  | Lost app data                                  | Y                                       | N                                | N                                                                       |
| SQL Server/Exchange<br><br>Azure Backup Server app backup<br><br>BMR/system state backup                  | Lost or damaged operating system               | N                                       | Y                                | Y                                                                       |
| SQL Server/Exchange<br><br>Azure Backup Server app backup<br><br>BMR/system state backup                  | Lost server (database/transaction logs intact) | N                                       | N                                | Y                                                                       |
| SQL Server/Exchange<br><br>Azure Backup Server app backup<br><br>BMR/system state backup                  | Lost server (database/transaction logs lost)   | N                                       | N                                | Y<br><br>BMR recovery, followed by regular Azure Backup Server recovery |

## How system state backup works

When a system state backup runs, Backup Server communicates with Windows Server Backup to request a backup of the server's system state. By default, Backup Server and Windows Server Backup use the drive that has the most available free space. Information about this drive is saved in the *PSDataSourceConfig.xml* file.

You can customize the drive that Backup Server uses for the system state backup:

1. On the protected server, go to `C:\Program Files\Microsoft Data Protection Manager\MABS\Datasources`.
2. Open the `PSDataSourceConfig.xml` file for editing.
3. Change the `<FilesToProtect>` value for the drive letter.
4. Save and close the file.

If a protection group is set to protect the system state of the computer, then run a consistency check. If an alert is generated, then select **Modify protection group** in the alert, and then complete the pages in the wizard. Then run another consistency check.

If the protection server is in a cluster, a cluster drive might be selected as the drive that has the most free space. If that drive ownership is switched to another node and a system state backup runs, then the drive is unavailable and the backup fails. In this scenario, modify `PSDataSourceConfig.xml` to point to a local drive.

Next, Windows Server Backup creates a folder called `WindowsImageBackup` in the root of the restore folder. As Windows Server Backup creates the backup, all the data is placed in this folder. When the backup finishes, the file is transferred to the Backup Server computer. Note the following information:

- This folder and its contents aren't cleaned up when the backup or transfer finishes. The best way to think of this is that the space is reserved for the next time a backup finishes.
- The folder is created for every backup. The time and date stamp reflect the time of your last system state backup.

## How BMR backup works

For BMR (including a system state backup), the backup job is saved directly to a share on the Backup Server computer. It's not saved to a folder on the protected server.

Backup Server calls Windows Server Backup and shares out the replica volume for that BMR backup. In this case, it doesn't require Windows Server Backup to use the drive that has the most free space. Instead, it uses the share that was created for the job.

When the backup finishes, the file is transferred to the Backup Server computer. Logs are stored in `C:\Windows\Logs\WindowsServerBackup`.

## Prerequisites and limitations

- BMR isn't supported for computers that run Windows Server 2003 or for computers that run a client operating system.
- You can't protect BMR and system state for the same computer in different protection groups.
- A Backup Server computer can't protect itself for BMR.
- Short-term protection to tape (disk to tape, or D2T) isn't supported for BMR. Long-term storage to tape (disk to disk to tape, or D2D2T) is supported.
- For BMR protection, Windows Server Backup must be installed on the protected computer.
- For BMR protection, unlike for system state protection, Backup Server has no space requirements on the protected computer. Windows Server Backup directly transfers backups to the Backup Server computer. The backup transfer job doesn't appear in the Backup Server **Jobs** view.
- Backup Server reserves 30 GB of space on the replica volume for BMR. You can change this space allotment on the **Disk Allocation** page in the Modify Protection Group Wizard. Or you can use the `Get-DatasourceDiskAllocation` and `Set-DatasourceDiskAllocation` PowerShell cmdlets. On the recovery point

volume, BMR protection requires about 6 GB for a retention of five days.

- You can't reduce the replica volume size to less than 15 GB.
- Backup Server doesn't calculate the size of the BMR data source. It assumes 30 GB for all servers. Change the value based on the size of BMR backups that you expect in your environment. You can roughly calculate the size of a BMR backup as the sum of used space on all critical volumes. Critical volumes = boot volume + system volume + volume hosting system state data, such as Active Directory.
- If you change from system state protection to BMR protection, then BMR protection requires less space on the *recovery point volume*. However, the extra space on the volume isn't reclaimed. You can manually shrink the volume size on the **Modify Disk Allocation** page of the Modify Protection Group Wizard. Or you can use the Get-DatasourceDiskAllocation and Set-DatasourceDiskAllocation PowerShell cmdlets.

If you change from system state protection to BMR protection, then BMR protection requires more space on the *replica volume*. The volume is automatically extended. If you want to change the default space allocations, then use the **Modify-DiskAllocation** PowerShell cmdlet.

- If you change from BMR protection to system state protection, then you need more space on the recovery point volume. Backup Server might try to automatically increase the volume. If the storage pool doesn't have sufficient space, an error occurs.

If you change from BMR protection to system state protection, then you need space on the protected computer. You need the space because system state protection first writes the replica to the local computer, and then it transfers the replica to the Backup Server computer.

## Before you begin

1. **Deploy Azure Backup Server.** Verify that Backup Server is correctly deployed. For more information, see:
  - [System requirements for Azure Backup Server](#)
  - [Backup Server protection matrix](#)
2. **Set up storage.** You can store backup data on disk, on tape, and in the cloud with Azure. For more information, see [Prepare data storage](#).
3. **Set up the protection agent.** Install the protection agent on the computer that you want to back up. For more information, see [Deploy the DPM protection agent](#).

## Back up system state and bare metal

To back up system state and bare metal:

1. To open the Create New Protection Group Wizard, in the Backup Server Administrator Console, select **Protection > Actions > Create Protection Group**.
2. On the **Select Protection Group Type** page, select **Servers**, and then select **Next**.
3. On the **Select Group Members** page, expand the computer, and then select either **BMR** or **system state**.

Remember that you can't protect both BMR and system state for the same computer in different groups. Also, when you select BMR, system state is automatically enabled. For more information, see [Deploy protection groups](#).

4. On the **Select Data Protection Method** page, choose how to handle short-term backup and long-term backup.

Short-term backup is always to disk first, with the option of backing up from the disk to Azure by using Azure Backup (short-term or long-term). An alternative to long-term backup to the cloud is to set up long-term backup to a standalone tape device or tape library that's connected to Backup Server.

5. On the **Select Short-Term Goals** page, choose how to back up to short-term storage on disk:
  - For **Retention range**, choose how long to keep the data on disk.
  - For **Synchronization frequency**, choose how often to run an incremental backup to disk. If you don't want to set a backup interval, you can select **Just before a recovery point**. Backup Server will run an express full backup just before each recovery point is scheduled.
6. If you want to store data on tape for long-term storage, then on the **Specify Long-Term Goals** page, choose how long to keep tape data (1 to 99 years).
  - a. For **Frequency of backup**, choose how often to run backup to tape. The frequency is based on the retention range you selected:
    - When the retention range is 1 to 99 years, you can back up daily, weekly, biweekly, monthly, quarterly, half-yearly, or yearly.
    - When the retention range is 1 to 11 months, you can back up daily, weekly, biweekly, or monthly.
    - When the retention range is 1 to 4 weeks, you can back up daily or weekly.
  - b. On the **Select Tape and Library Details** page, select the tape and library to use. Also choose whether data should be compressed and encrypted.
7. On the **Review Disk Allocation** page, review the storage pool disk space that's available for the protection group.
  - **Total Data size** is the size of the data you want to back up.
  - **Disk space to be provisioned on Azure Backup Server** is the space that Backup Server recommends for the protection group. Backup Server uses these settings to choose the ideal backup volume. You can edit the backup volume choices in **Disk allocation details**.
  - For workloads, in the drop-down menu, select the preferred storage. Your edits change the values for **Total Storage** and **Free Storage** in the **Available Disk Storage** pane. Underprovisioned space is the amount of storage that Backup Server suggests that you add to the volume to ensure smooth backups.
8. On the **Choose Replica Creation Method** page, select how to handle the initial full-data replication.

If you choose to replicate over the network, we recommend that you choose an off-peak time. For large amounts of data or for network conditions that are less than optimal, consider replicating the data offline by using removable media.
9. On the **Choose Consistency Check Options** page, select how to automate consistency checks.

You can choose to run a check only when replica data becomes inconsistent, or on a schedule. If you don't want to configure automatic consistency checking, then you can run a manual check at any time. To run a manual check, in the **Protection** area of the Backup Server Administrator Console, right-click the protection group, and then select **Perform Consistency Check**.
10. If you chose to back up to the cloud by using Azure Backup, on the **Specify Online Protection Data** page, select the workloads that you want to back up to Azure.
11. On the **Specify Online Backup Schedule** page, select how often to incrementally back up to Azure.

You can schedule backups to run every day, week, month, and year. You can also select the time and date at which backups should run. Backups can occur up to twice a day. Each time a backup runs, a data recovery point is created in Azure from the copy of the backup data that's stored on the Backup Server disk.
12. On the **Specify Online Retention Policy** page, select how the recovery points that are created from the daily, weekly, monthly, and yearly backups are kept in Azure.
13. On the **Choose Online Replication** page, select how the initial full replication of data occurs.

You can replicate over the network or back up offline (offline seeding). An offline backup uses the Azure

Import feature. For more information, see [Offline backup workflow in Azure Backup](#).

14. On the **Summary** page, review your settings. After you select **Create Group**, initial replication of the data occurs. When the data replication finishes, on the **Status** page, the protection group status is **OK**. Backups then happen according to the protection group settings.

## Recover system state or BMR

You can recover BMR or system state to a network location. If you backed up BMR, then use Windows Recovery Environment (WinRE) to start your system and connect it to the network. Then use Windows Server Backup to recover from the network location. If you backed up system state, then just use Windows Server Backup to recover from the network location.

### Restore BMR

To run recovery on the Backup Server computer:

1. In the **Recovery** pane, find the computer that you want to recover. Then select **Bare Metal Recovery**.
2. Available recovery points are indicated in bold on the calendar. Select the date and time for the recovery point that you want to use.
3. On the **Select Recovery Type** page, select **Copy to a network folder**.
4. On the **Specify Destination** page, select the destination for the copied data.

Remember, the destination needs to have enough room for the data. We recommend that you create a new folder for the destination.

5. On the **Specify Recovery Options** page, select the security settings. Then select whether to use storage area network (SAN)-based hardware snapshots, for quicker recovery. This option is available only if:
  - You have a SAN that provides this functionality.
  - You can create and split a clone to make it writable.
  - The protected computer and Backup Server computer are connected to the same network.
6. Set up notification options.

7. On the **Confirmation** page, select **Recover**.

To set up the share location:

1. In the restore location, go to the folder that has the backup.
2. Share the folder that's one level above *WindowsImageBackup* so that the root of the shared folder is the *WindowsImageBackup* folder.

If you don't share this folder, restore won't find the backup. To connect by using WinRE, you need a share that you can access in WinRE with the correct IP address and credentials.

To restore the system:

1. Start the computer on which you want to restore the image by using the Windows DVD for the system you're restoring.
2. On the first page, verify the settings for language and locale. On the **Install** page, select **Repair your computer**.
3. On the **System Recovery Options** page, select **Restore your computer using a system image that you created earlier**.
4. On the **Select a system image backup** page, select **Select a system image > Advanced > Search for a**

**system image on the network.** If a warning appears, select **Yes**. Go to the share path, enter the credentials, and then select the recovery point. The system scans for specific backups that are available in that recovery point. Select the recovery point that you want to use.

5. On the **Choose how to restore the backup** page, select **Format and repartition disks**. On the next page, verify the settings.
6. To begin the restore, select **Finish**. A restart is required.

### Restore system state

To run recovery in Backup Server:

1. In the **Recovery** pane, find the computer that you want to recover, and then select **Bare Metal Recovery**.
2. Available recovery points are indicated in bold on the calendar. Select the date and time for the recovery point that you want to use.
3. On the **Select Recovery Type** page, select **Copy to a network folder**.
4. On the **Specify Destination** page, select where to copy the data.

Remember, the destination you select needs to have enough room for the data. We recommend that you create a new folder for the destination.

5. On the **Specify Recovery Options** page, select the security settings. Then select whether to use SAN-based hardware snapshots, for quicker recovery. This option is available only if:
  - You have a SAN that provides this functionality.
  - You can create and split a clone to make it writable.
  - The protected computer and Backup Server server are connected to the same network.
6. Set up notification options.
7. On the **Confirmation** page, select **Recover**.

To run Windows Server Backup:

1. Select **Actions > Recover > This Server > Next**.
2. Select **Another Server**, select the **Specify Location Type** page, and then select **Remote shared folder**. Enter the path to the folder that contains the recovery point.
3. On the **Select Recovery Type** page, select **System state**.
4. On the **Select Location for System State Recovery** page, select **Original Location**.
5. On the **Confirmation** page, select **Recover**.
6. After the restore, restart the server.

You also can run the system state restore at a command prompt:

1. Start Windows Server Backup on the computer that you want to recover.
2. To get the version identifier, at a command prompt, enter:

```
wbadm get versions -backuptarget \<servername\sharename\>
```
3. Use the version identifier to start the system state restore. At the command prompt, enter:

```
wbadm start systemstaterecovery -version:<versionidentified> -backuptarget:<servername\sharename\>
```
4. Confirm that you want to start the recovery. You can see the process in the Command Prompt window. A

restore log is created.

5. After the restore, restart the server.

# Recover data from Azure Backup Server

11/18/2019 • 4 minutes to read • [Edit Online](#)

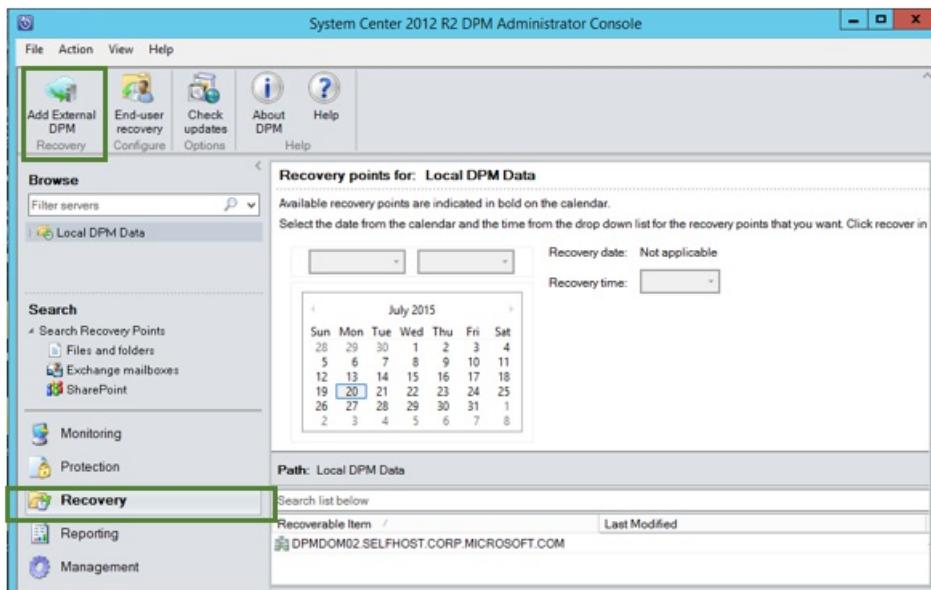
You can use Azure Backup Server to recover the data you've backed up to a Recovery Services vault. The process for doing so is integrated into the Azure Backup Server management console, and is similar to the recovery workflow for other Azure Backup components.

## NOTE

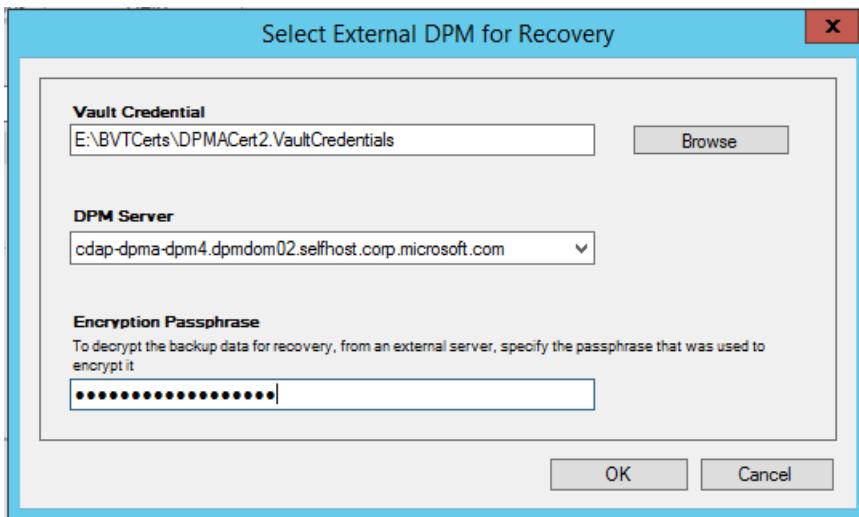
This article is applicable for [System Center Data Protection Manager 2012 R2 with UR7 or later](#), combined with the [latest Azure Backup agent](#).

To recover data from an Azure Backup Server:

1. From the **Recovery** tab of the Azure Backup Server management console, click '**Add External DPM**' (at the top left of the screen).



2. Download new **vault credentials** from the vault associated with the **Azure Backup Server** where the data is being recovered, choose the Azure Backup Server from the list of Azure Backup Servers registered with the Recovery Services vault, and provide the **encryption passphrase** associated with the server whose data is being recovered.

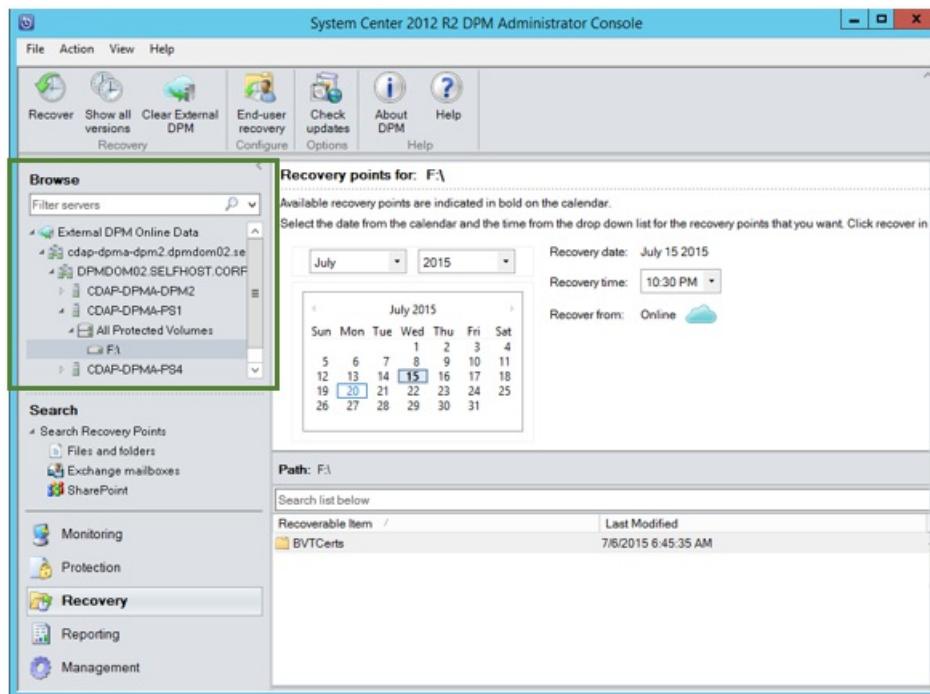


#### NOTE

Only Azure Backup Servers associated with the same registration vault can recover each other's data.

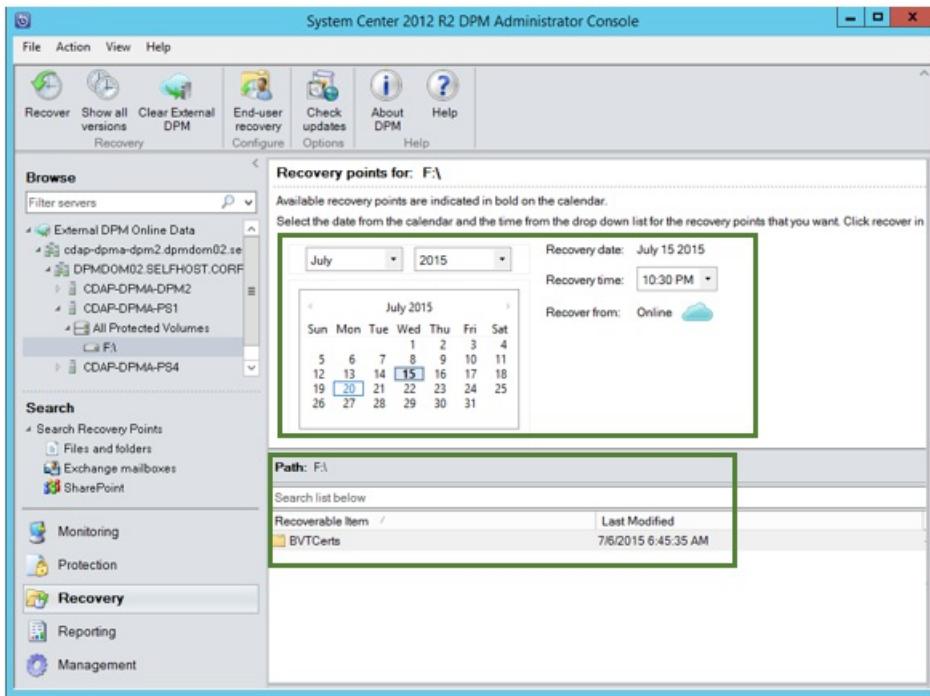
Once the External Azure Backup Server is successfully added, you can browse the data of the external server and the local Azure Backup Server from the **Recovery** tab.

3. Browse the available list of production servers protected by the external Azure Backup Server and select the appropriate data source.

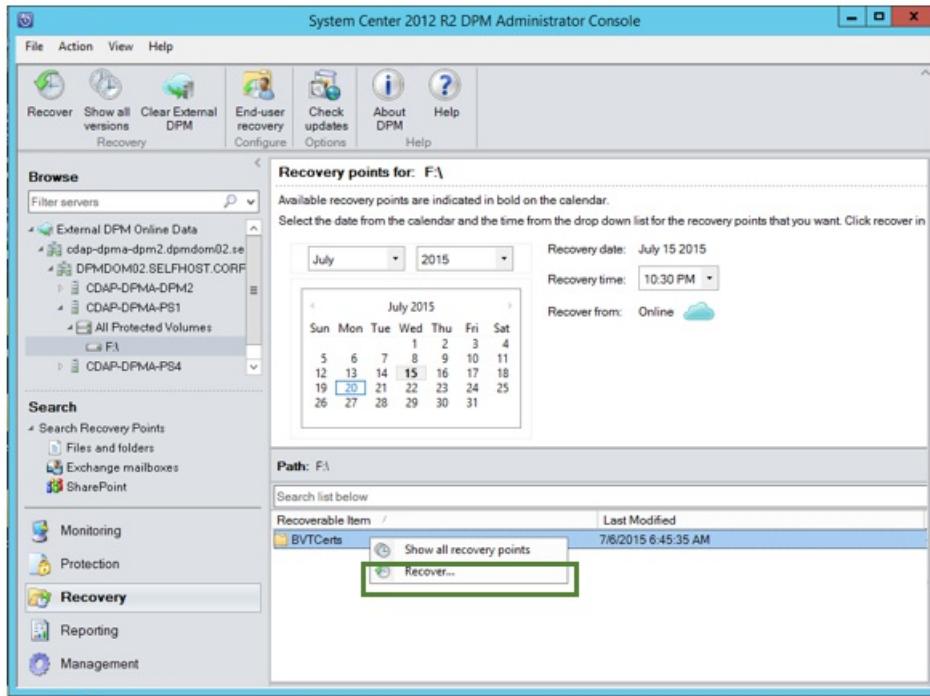


4. Select **the month and year** from the **Recovery points** drop down, select the required **Recovery date** for when the recovery point was created, and select the **Recovery time**.

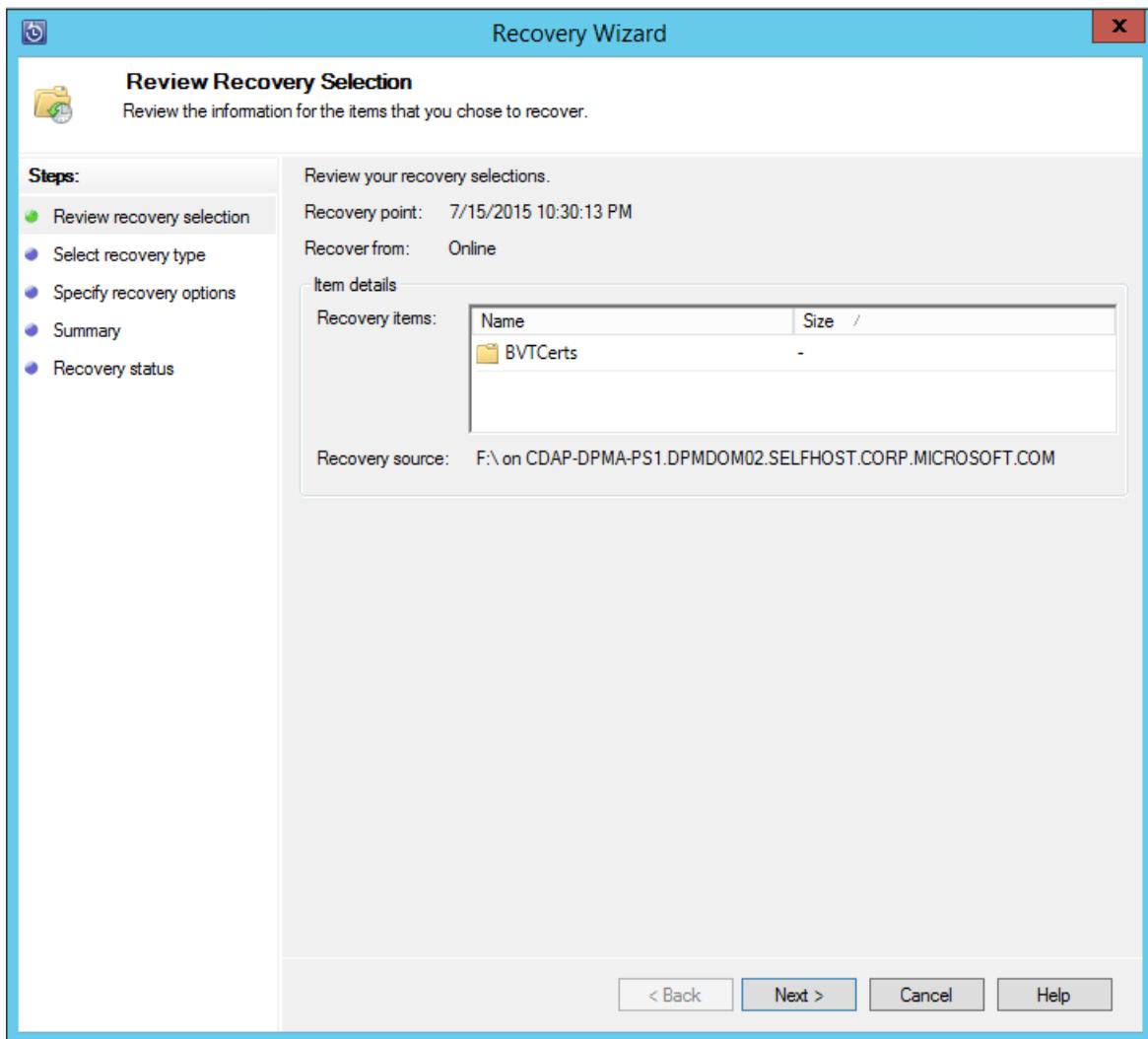
A list of files and folders appears in the bottom pane, which can be browsed and recovered to any location.



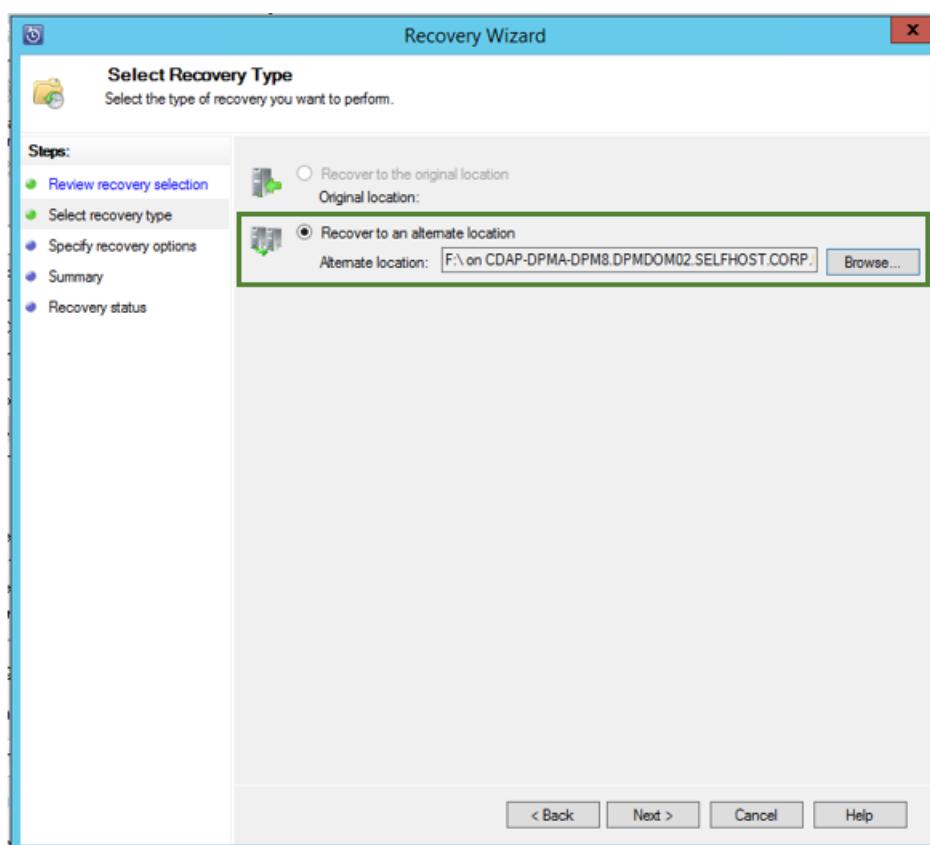
5. Right-click the appropriate item and click **Recover**.



6. Review the **Recover Selection**. Verify the data and time of the backup copy being recovered, as well as the source from which the backup copy was created. If the selection is incorrect, click **Cancel** to navigate back to recovery tab to select appropriate recovery point. If the selection is correct, click **Next**.



7. Select **Recover to an alternate location**. **Browse** to the correct location for the recovery.

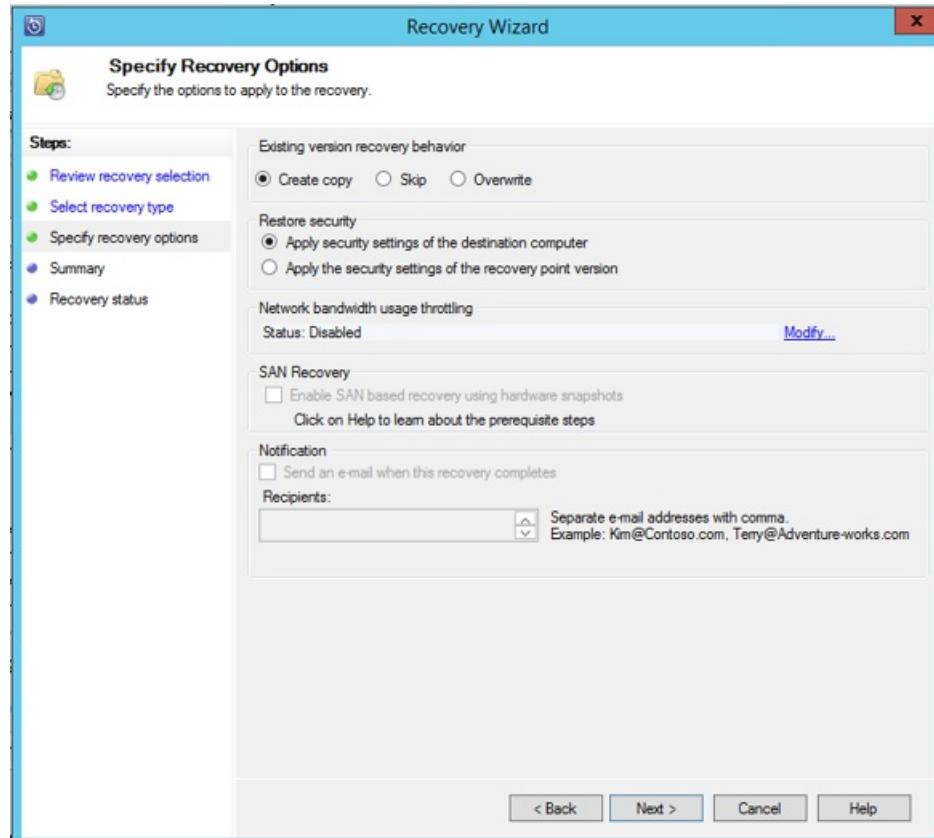


8. Choose the option related to **create copy**, **Skip**, or **Overwrite**.

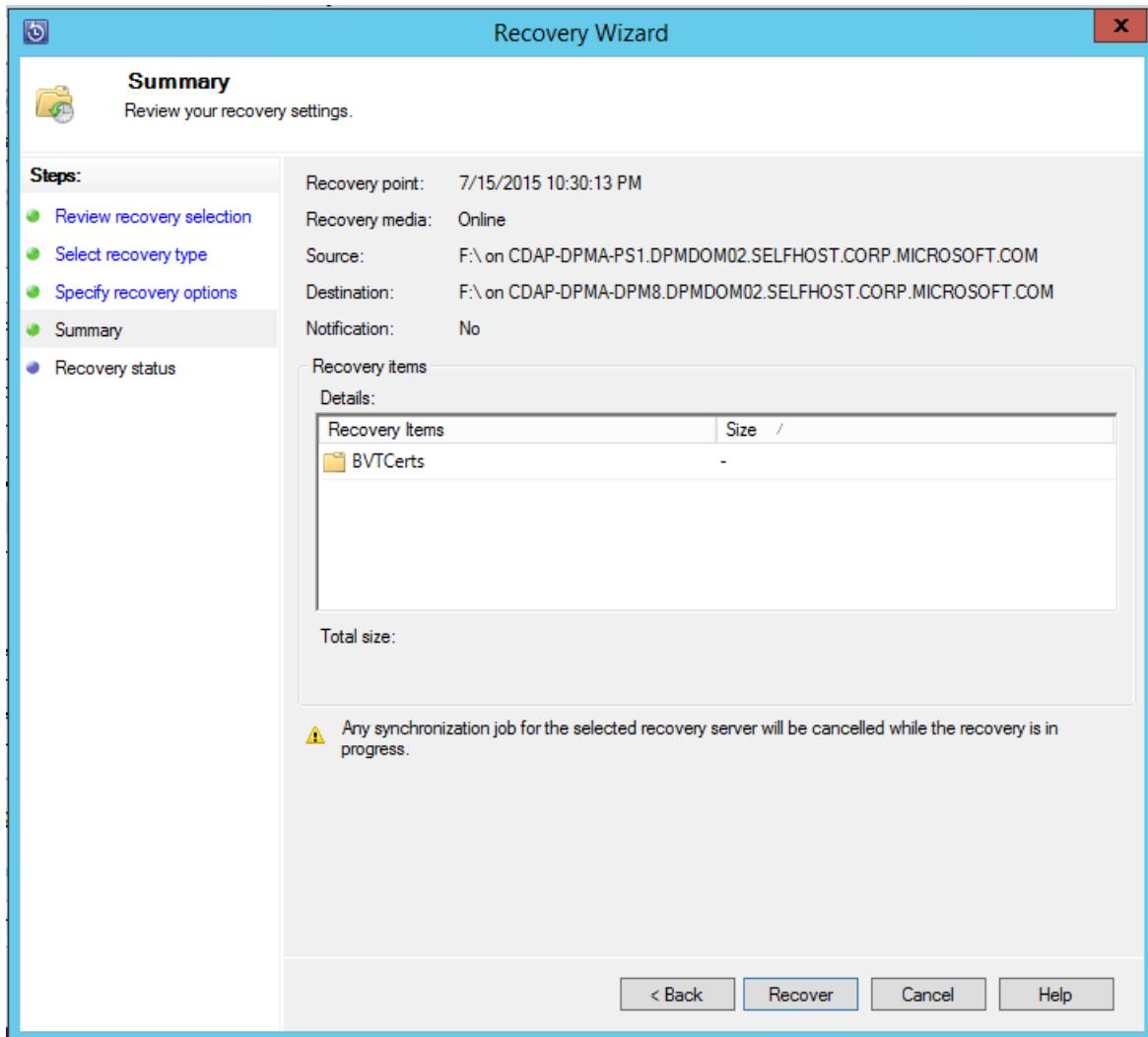
- **Create copy** - creates a copy of the file if there is a name collision.
- **Skip** - if there is a name collision, does not recover the file, which leaves the original file.
- **Overwrite** - if there is a name collision, overwrites the existing copy of the file.

Choose the appropriate option to **Restore security**. You can apply the security settings of the destination computer where the data is being recovered or the security settings that were applicable to product at the time the recovery point was created.

Identify whether a **Notification** is sent, once the recovery successfully completes.

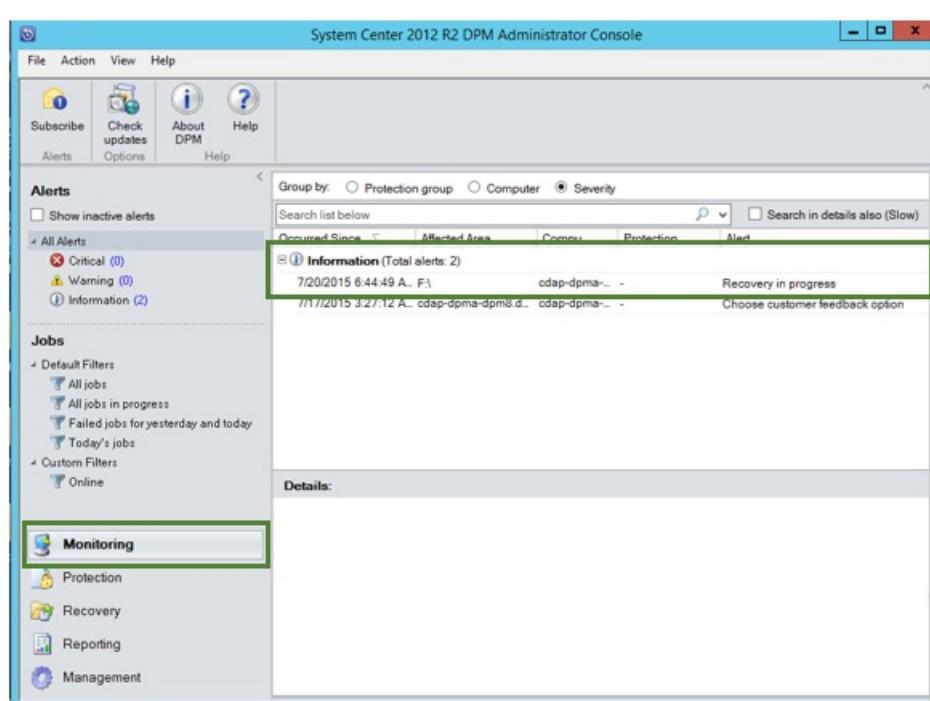


9. The **Summary** screen lists the options chosen so far. Once you click '**Recover**', the data is recovered to the appropriate on-premises location.

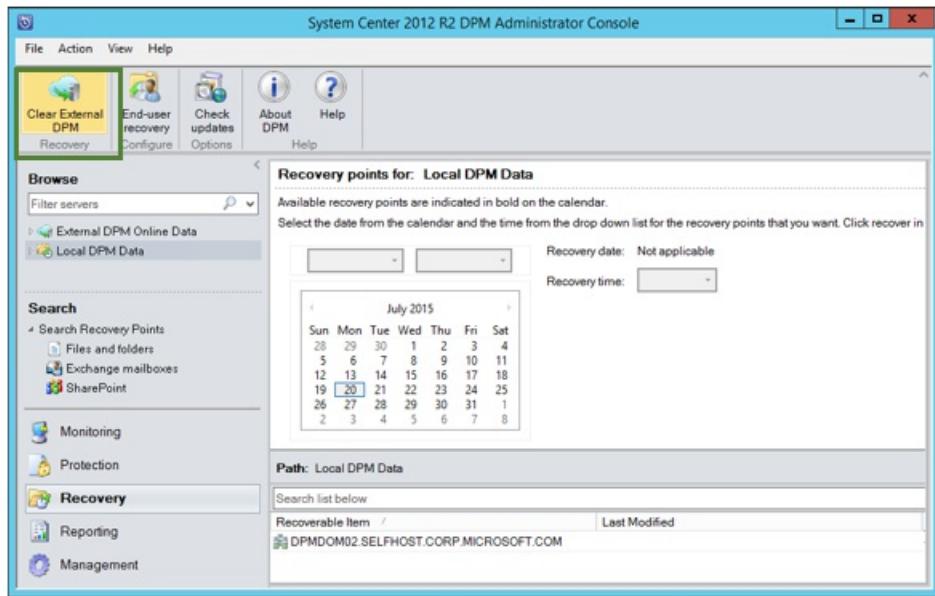


#### NOTE

The recovery job can be monitored in the **Monitoring** tab of the Azure Backup Server.



10. You can click **Clear External DPM** on the **Recovery** tab of the DPM server to remove the view of the external DPM server.



## Troubleshooting error messages

| NO. | ERROR MESSAGE                                                                            | TROUBLESHOOTING STEPS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.  | This server is not registered to the vault specified by the vault credential.            | <p><b>Cause:</b> This error appears when the vault credential file selected does not belong to the Recovery Services vault associated with Azure Backup Server on which the recovery is attempted.</p> <p><b>Resolution:</b> Download the vault credential file from the Recovery Services vault to which the Azure Backup Server is registered.</p>                                                                                                                                                                                                                                                                                                                                                         |
| 2.  | Either the recoverable data is not available or the selected server is not a DPM server. | <p><b>Cause:</b> There are no other Azure Backup Servers registered to the Recovery Services vault, or the servers have not yet uploaded the metadata, or the selected server is not an Azure Backup Server (using Windows Server or Windows Client).</p> <p><b>Resolution:</b> If there are other Azure Backup Servers registered to the Recovery Services vault, ensure that the latest Azure Backup agent is installed. If there are other Azure Backup Servers registered to the Recovery Services vault, wait for a day after installation to start the recovery process. The nightly job will upload the metadata for all the protected backups to cloud. The data will be available for recovery.</p> |

| No. | Error Message                                                                                                                         | Troubleshooting Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3.  | No other DPM server is registered to this vault.                                                                                      | <p><b>Cause:</b> There are no other Azure Backup Servers that are registered to the vault from which the recovery is being attempted.</p> <p><b>Resolution:</b> If there are other Azure Backup Servers registered to the Recovery Services vault, ensure that the latest Azure Backup agent is installed. If there are other Azure Backup Servers registered to the Recovery Services vault, wait for a day after installation to start the recovery process. The nightly job uploads the metadata for all protected backups to cloud. The data will be available for recovery.</p> |
| 4.  | The encryption passphrase provided does not match with passphrase associated with the following server:<br><b>&lt;server name&gt;</b> | <p><b>Cause:</b> The encryption passphrase used in the process of encrypting the data from the Azure Backup Server's data that is being recovered does not match the encryption passphrase provided. The agent is unable to decrypt the data. Hence the recovery fails.</p> <p><b>Resolution:</b> Please provide the exact same encryption passphrase associated with the Azure Backup Server whose data is being recovered.</p>                                                                                                                                                     |

## Next steps

Read the other FAQs:

- [Common questions about Azure VM backups](#)
- [Common questions about the Azure Backup agent](#)

# Restore VMware virtual machines

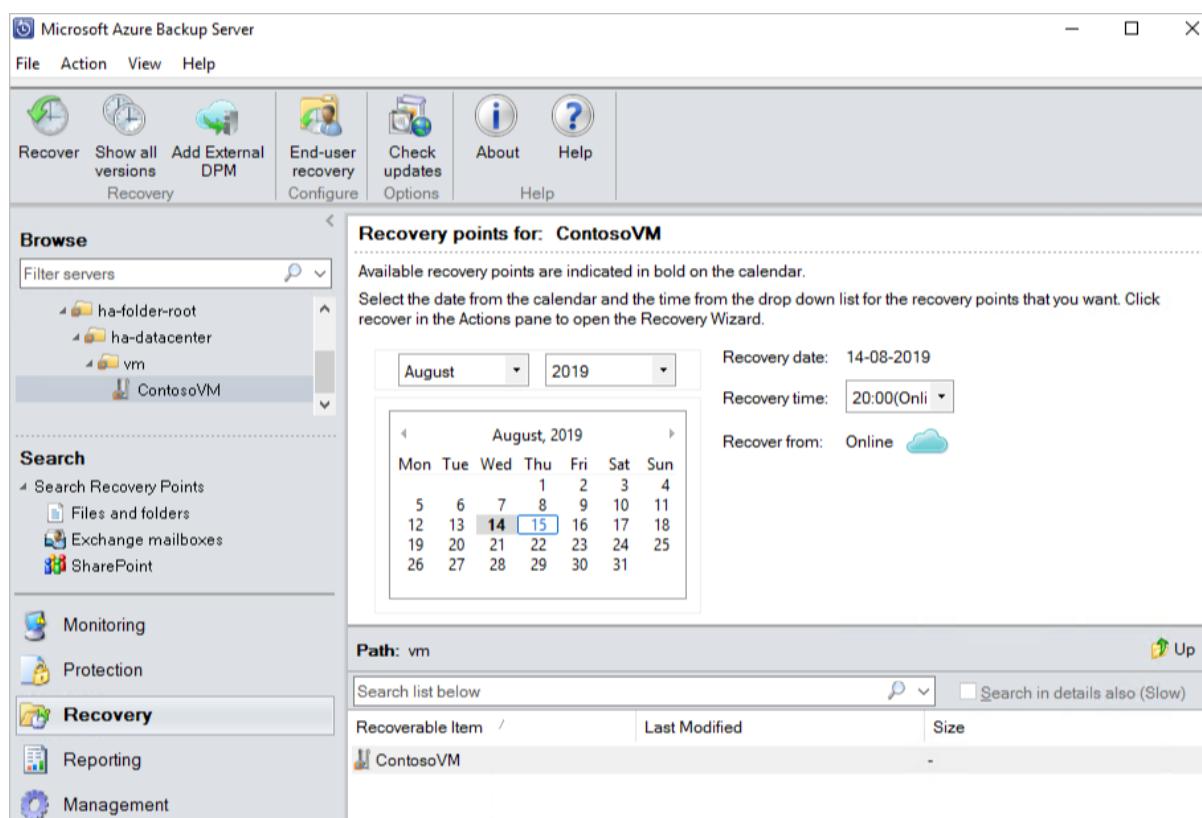
2/14/2020 • 5 minutes to read • [Edit Online](#)

This article explains how to use Microsoft Azure Backup Server (MABS) to restore VMware VM recovery points. For an overview on using MABS to recover data, see [Recover protected data](#). In the MABS Administrator Console, there are two ways to find recoverable data - search or browse. When recovering data, you may, or may not want to restore data or a VM to the same location. For this reason, MABS supports three recovery options for VMware VM backups:

- **Original location recovery (OLR)** - Use OLR to restore a protected VM to its original location. You can restore a VM to its original location only if no disks have been added or deleted, since the backup occurred. If disks have been added or deleted, you must use alternate location recovery.
- **Alternate location recovery (ALR)** - When the original VM is missing, or you don't want to disturb the original VM, recover the VM to an alternate location. To recover a VM to an alternate location, you must provide the location of an ESXi host, resource pool, folder, and the storage datastore and path. To help differentiate the restored VM from the original VM, MABS appends "-Recovered" to the name of the VM.
- **Individual file location recovery (ILR)** - If the protected VM is a Windows Server VM, individual files/folders inside the VM can be recovered using MABS's ILR capability. To recover individual files, see the procedure later in this article.

## Restore a recovery point

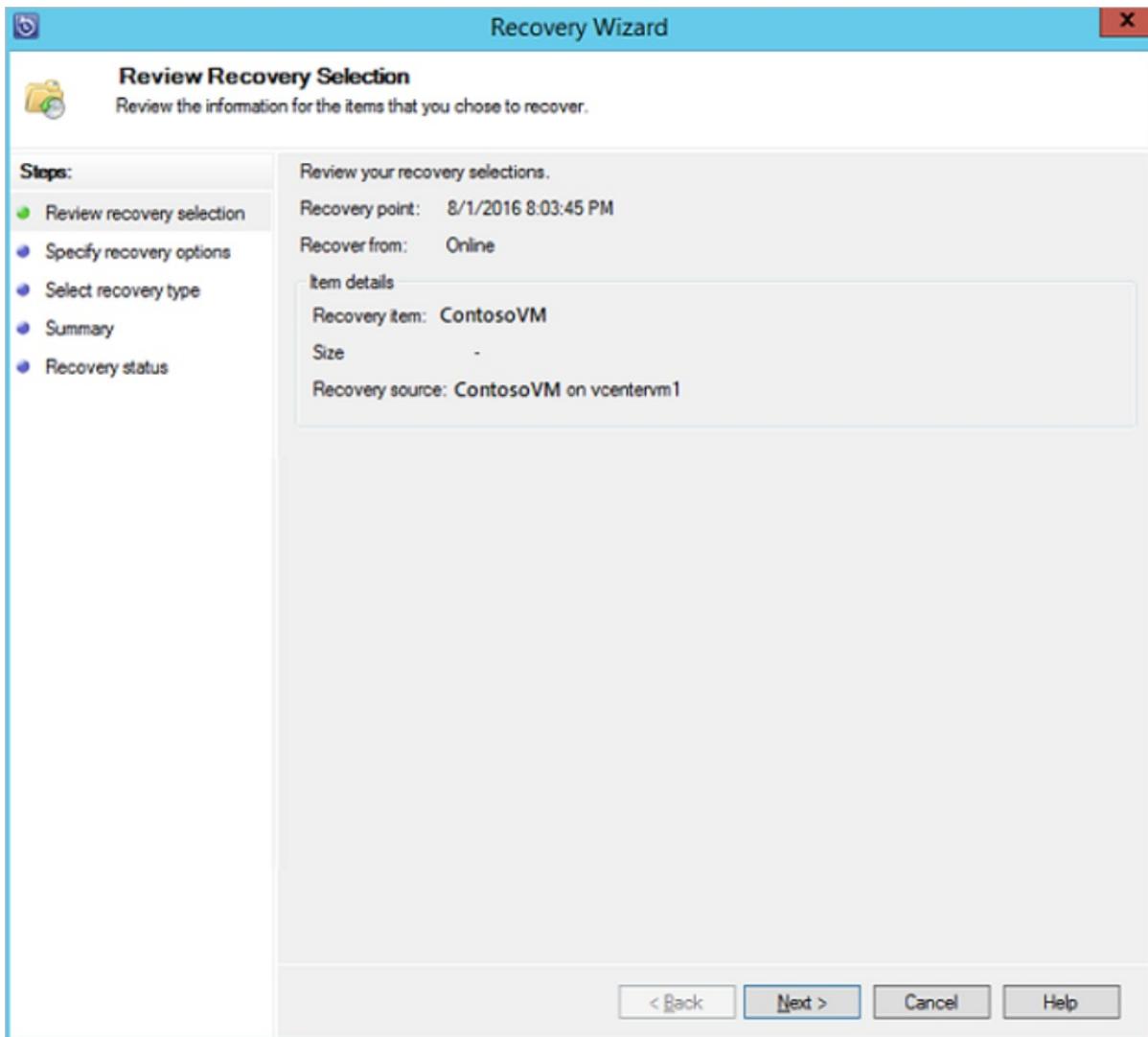
1. In the MABS Administrator Console, click Recovery view.
2. Using the Browse pane, browse or filter to find the VM you want to recover. Once you select a VM or folder, the Recovery points for pane displays the available recovery points.



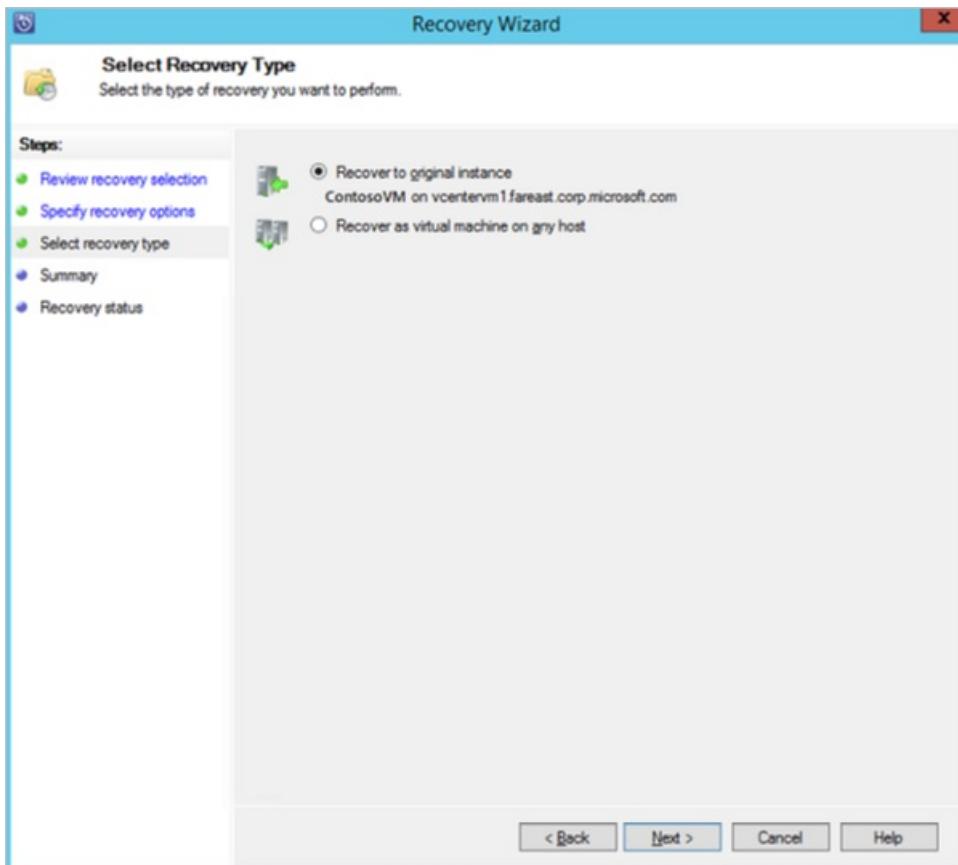
3. In the **Recovery points for** field, use the calendar and drop-down menus to select a date when a recovery

point was taken. Calendar dates in bold have available recovery points.

4. On the tool ribbon, click **Recover** to open the **Recovery Wizard**.



5. Click **Next** to advance to the **Specify Recovery Options** screen.
6. On the **Specify Recovery Options** screen, if you want to enable network bandwidth throttling, click **Modify**. To leave network throttling disabled, click **Next**. No other options on this wizard screen are available for VMware VMs. If you choose to modify the network bandwidth throttle, in the Throttle dialog, select **Enable network bandwidth usage throttling** to turn it on. Once enabled, configure the **Settings** and **Work Schedule**.
7. On the **Select Recovery Type** screen, choose whether to recover to the original instance, or to a new location, and click **Next**.
  - If you choose **Recover to original instance**, you don't need to make any more choices in the wizard. The data for the original instance is used.
  - If you choose **Recover as virtual machine on any host**, then on the **Specify Destination** screen, provide the information for **ESXi Host**, **Resource Pool**, **Folder**, and **Path**.



8. On the **Summary** screen, review your settings and click **Recover** to start the recovery process. The **Recovery status** screen shows the progression of the recovery operation.

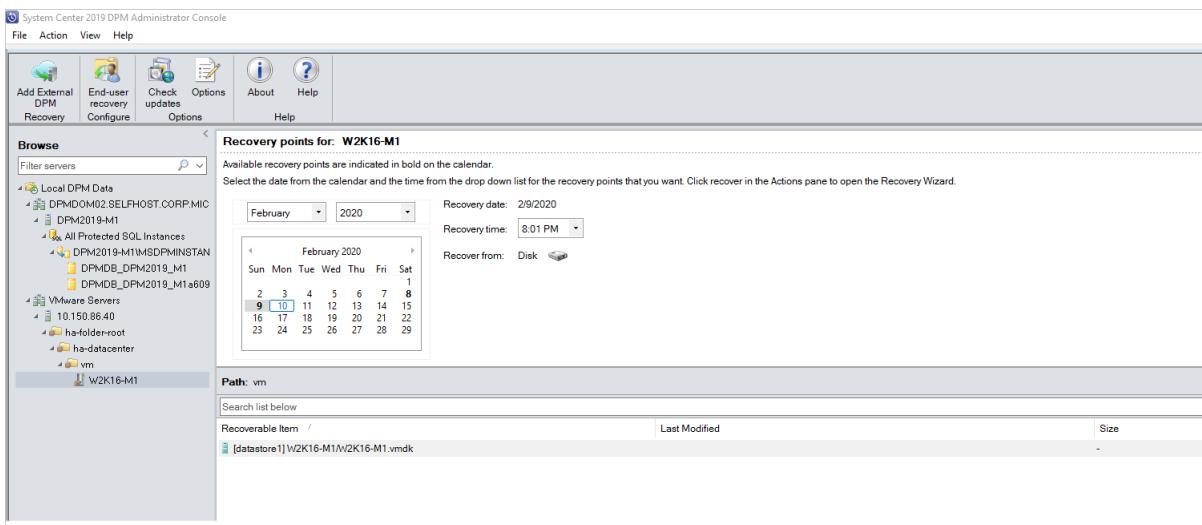
## Restore an individual file from a VM

You can restore individual files from a protected VM recovery point. This feature is only available for Windows Server VMs. Restoring individual files is similar to restoring the entire VM, except you browse into the VMDK and find the file(s) you want, before starting the recovery process. To recover an individual file or select files from a Windows Server VM:

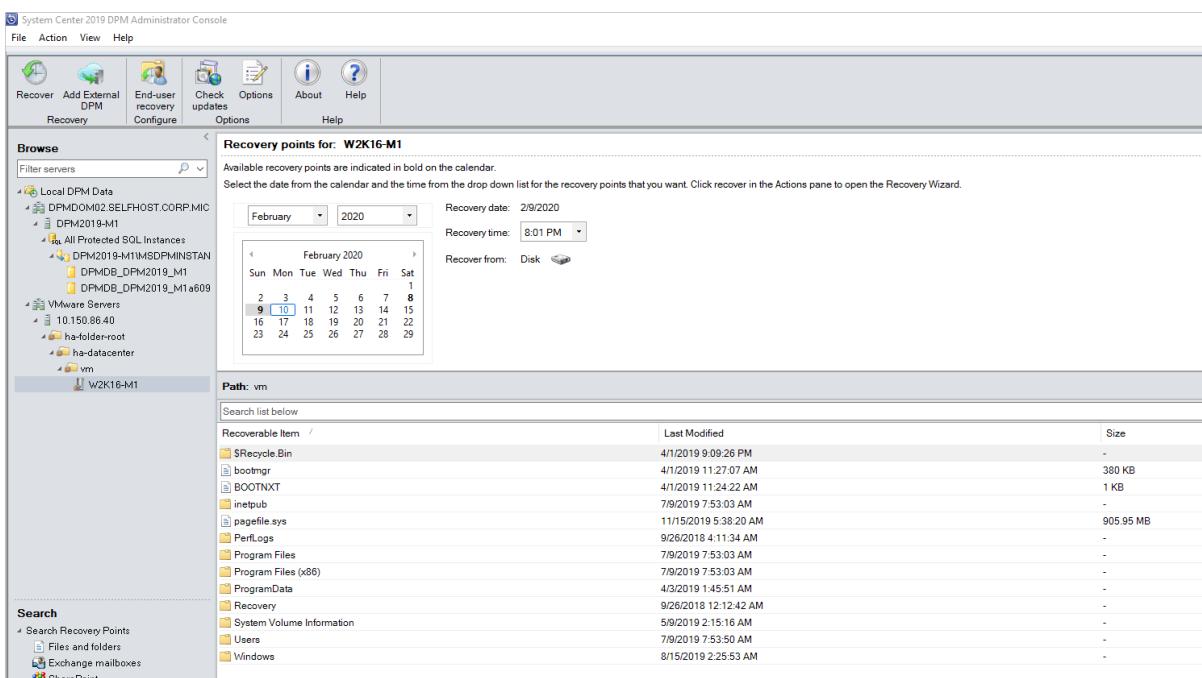
### NOTE

Restoring an individual file from a VM is available only for Windows VM and Disk Recovery Points.

1. In the MABS Administrator Console, click **Recovery** view.
2. Using the **Browse** pane, browse or filter to find the VM you want to recover. Once you select a VM or folder, the Recovery points for pane displays the available recovery points.



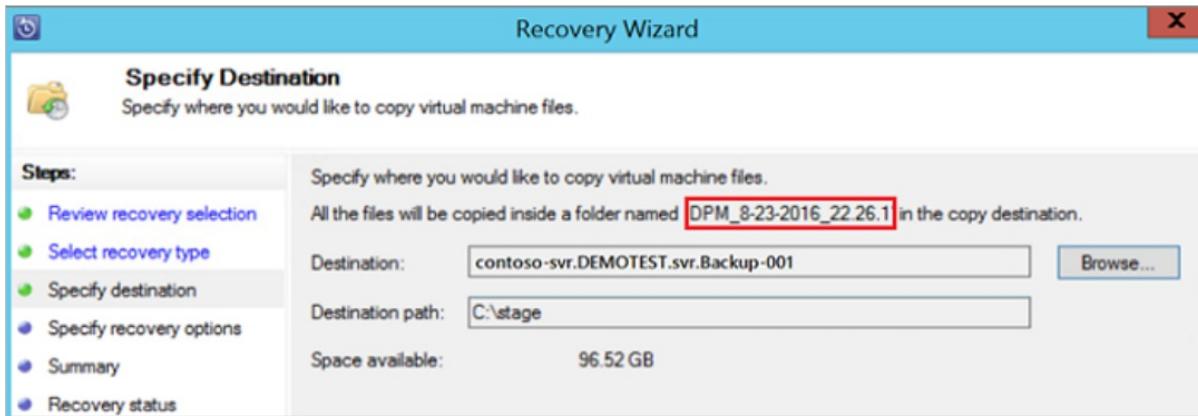
3. In the **Recovery Points for:** pane, use the calendar to select the date that contains the desired recovery point(s). Depending on how the backup policy has been configured, dates can have more than one recovery point. Once you've selected the day when the recovery point was taken, make sure you've chosen the correct **Recovery time**. If the selected date has multiple recovery points, choose your recovery point by selecting it in the Recovery time drop-down menu. Once you chose the recovery point, the list of recoverable items appears in the **Path:** pane.
4. To find the files you want to recover, in the **Path** pane, double-click the item in the **Recoverable item** column to open it. Select the file, files, or folders you want to recover. To select multiple items, press the **Ctrl** key while selecting each item. Use the **Path** pane to search the list of files or folders appearing in the **Recoverable Item** column. **Search list below** does not search into subfolders. To search through subfolders, double-click the folder. Use the **Up** button to move from a child folder into the parent folder. You can select multiple items (files and folders), but they must be in the same parent folder. You cannot recover items from multiple folders in the same recovery job.



5. When you have selected the item(s) for recovery, in the Administrator Console tool ribbon, click **Recover** to open the **Recovery Wizard**. In the Recovery Wizard, the **Review Recovery Selection** screen shows the selected items to be recovered.
6. On the **Specify Recovery Options** screen, if you want to enable network bandwidth throttling, click **Modify**. To leave network throttling disabled, click **Next**. No other options on this wizard screen are available for VMware VMs. If you choose to modify the network bandwidth throttle, in the Throttle dialog,

select **Enable network bandwidth usage throttling** to turn it on. Once enabled, configure the **Settings** and **Work Schedule**.

7. On the **Select Recovery Type** screen, click **Next**. You can only recover your file(s) or folder(s) to a network folder.
8. On the **Specify Destination** screen, click **Browse** to find a network location for your files or folders. MABS creates a folder where all recovered items are copied. The folder name has the prefix, MABS\_day-month-year. When you select a location for the recovered files or folder, the details for that location (Destination, Destination path, and available space) are provided.



9. On the **Specify Recovery Options** screen, choose which security setting to apply. You can opt to modify the network bandwidth usage throttling, but throttling is disabled by default. Also, **SAN Recovery** and **Notification** are not enabled.
10. On the **Summary** screen, review your settings and click **Recover** to start the recovery process. The **Recovery status** screen shows the progression of the recovery operation.

## Next steps

For troubleshooting issues when using Azure Backup Server, review the [troubleshooting guide for Azure Backup Server](#).

# Install Azure Backup Server on Azure Stack

2/24/2020 • 16 minutes to read • [Edit Online](#)

This article explains how to install Azure Backup Server on Azure Stack. With Azure Backup Server, you can protect Infrastructure as a Service (IaaS) workloads such as virtual machines running in Azure Stack. A benefit of using Azure Backup Server to protect your workloads is you can manage all workload protection from a single console.

## NOTE

To learn about security capabilities, refer to [Azure Backup security features documentation](#).

## Azure Backup Server protection matrix

Azure Backup Server protects the following Azure Stack virtual machine workloads.

| PROTECTED DATA SOURCE                                               | PROTECTION AND RECOVERY              |
|---------------------------------------------------------------------|--------------------------------------|
| Windows Server Semi Annual Channel - Datacenter/Enterprise/Standard | Volumes, files, folders              |
| Windows Server 2016 - Datacenter/Enterprise/Standard                | Volumes, files, folders              |
| Windows Server 2012 R2 - Datacenter/Enterprise/Standard             | Volumes, files, folders              |
| Windows Server 2012 - Datacenter/Enterprise/Standard                | Volumes, files, folders              |
| Windows Server 2008 R2 - Datacenter/Enterprise/Standard             | Volumes, files, folders              |
| SQL Server 2016                                                     | Database                             |
| SQL Server 2014                                                     | Database                             |
| SQL Server 2012 SP1                                                 | Database                             |
| SharePoint 2016                                                     | Farm, database, frontend, web server |
| SharePoint 2013                                                     | Farm, database, frontend, web server |
| SharePoint 2010                                                     | Farm, database, frontend, web server |

## Prerequisites for the Azure Backup Server environment

Consider the recommendations in this section when installing Azure Backup Server in your Azure Stack environment. The Azure Backup Server installer checks that your environment has the necessary prerequisites, but you'll save time by preparing before you install.

### Determining size of virtual machine

To run Azure Backup Server on an Azure Stack virtual machine, use size A2 or larger. For assistance in choosing a

virtual machine size, download the [Azure Stack VM size calculator](#).

## Virtual Networks on Azure Stack virtual machines

All virtual machines used in an Azure Stack workload must belong to the same Azure virtual network and Azure Subscription.

## Azure Backup Server VM performance

If shared with other virtual machines, the storage account size and IOPS limits impact Azure Backup Server VM performance. For this reason, you should use a separate storage account for the Azure Backup Server virtual machine. The Azure Backup agent running on the Azure Backup Server needs temporary storage for:

- its own use (a cache location),
- data restored from the cloud (local staging area)

## Configuring Azure Backup temporary disk storage

Each Azure Stack virtual machine comes with temporary disk storage, which is available to the user as volume `D:\`. The local staging area needed by Azure Backup can be configured to reside in `D:\`, and the cache location can be placed on `C:\`. In this way, no storage needs to be carved away from the data disks attached to the Azure Backup Server virtual machine.

## Storing backup data on local disk and in Azure

Azure Backup Server stores backup data on Azure disks attached to the virtual machine, for operational recovery. Once the disks and storage space are attached to the virtual machine, Azure Backup Server manages storage for you. The amount of backup data storage depends on the number and size of disks attached to each [Azure Stack virtual machine](#). Each size of Azure Stack VM has a maximum number of disks that can be attached to the virtual machine. For example, A2 is four disks. A3 is eight disks. A4 is 16 disks. Again, the size and number of disks determines the total backup storage pool.

### IMPORTANT

You should **not** retain operational recovery (backup) data on Azure Backup Server-attached disks for more than five days.

Storing backup data in Azure reduces backup infrastructure on Azure Stack. If data is more than five days old, it should be stored in Azure.

To store backup data in Azure, create or use a Recovery Services vault. When preparing to back up the Azure Backup Server workload, you [configure the Recovery Services vault](#). Once configured, each time a backup job runs, a recovery point is created in the vault. Each Recovery Services vault holds up to 9999 recovery points. Depending on the number of recovery points created, and how long they are retained, you can retain backup data for many years. For example, you could create monthly recovery points, and retain them for five years.

## Scaling deployment

If you want to scale your deployment, you have the following options:

- Scale up - Increase the size of the Azure Backup Server virtual machine from A series to D series, and increase the local storage [per the Azure Stack virtual machine instructions](#).
- Offload data - send older data to Azure and retain only the newest data on the storage attached to the Azure Backup Server.
- Scale out - Add more Azure Backup Servers to protect the workloads.

## .NET Framework

.NET Framework 3.5 SP1 or higher must be installed on the virtual machine.

## Joining a domain

The Azure Backup Server virtual machine must be joined to a domain. A domain user with administrator privileges must install Azure Backup Server on the virtual machine.

## Using an IaaS VM in Azure Stack

When choosing a server for Azure Backup Server, start with a Windows Server 2012 R2 Datacenter or Windows Server 2016 Datacenter gallery image. The article, [Create your first Windows virtual machine in the Azure portal](#), provides a tutorial for getting started with the recommended virtual machine. The recommended minimum requirements for the server virtual machine (VM) should be: A2 Standard with two cores and 3.5-GB RAM.

Protecting workloads with Azure Backup Server has many nuances. The article, [Install DPM as an Azure virtual machine](#), helps explain these nuances. Before deploying the machine, read this article completely.

### NOTE

Azure Backup Server is designed to run on a dedicated, single-purpose virtual machine. You cannot install Azure Backup Server on:

- A computer running as a domain controller
- A computer on which the Application Server role is installed
- A computer on which Exchange Server is running
- A computer that is a node of a cluster

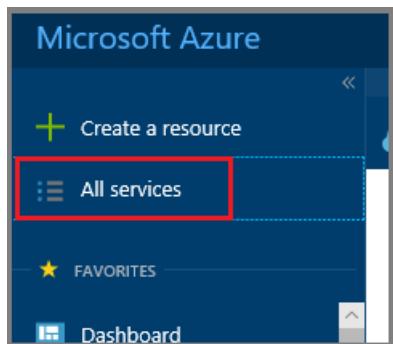
Always join Azure Backup Server to a domain. If you need to move Azure Backup Server to a different domain, first install Azure Backup Server, then join it to the new domain. Once you deploy Azure Backup Server, you can't move it to a new domain.

## Create a Recovery Services vault

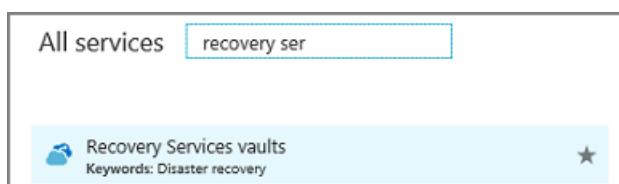
A Recovery Services vault is an entity that stores backups and recovery points created over time. The Recovery Services vault also contains the backup policies that are associated with the protected virtual machines.

To create a Recovery Services vault, follow these steps.

1. Sign in to your subscription in the [Azure portal](#).
2. On the left menu, select **All services**.

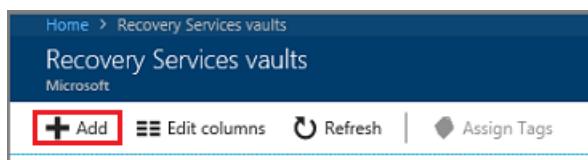


3. In the **All services** dialog box, enter *Recovery Services*. The list of resources filters according to your input. In the list of resources, select **Recovery Services vaults**.

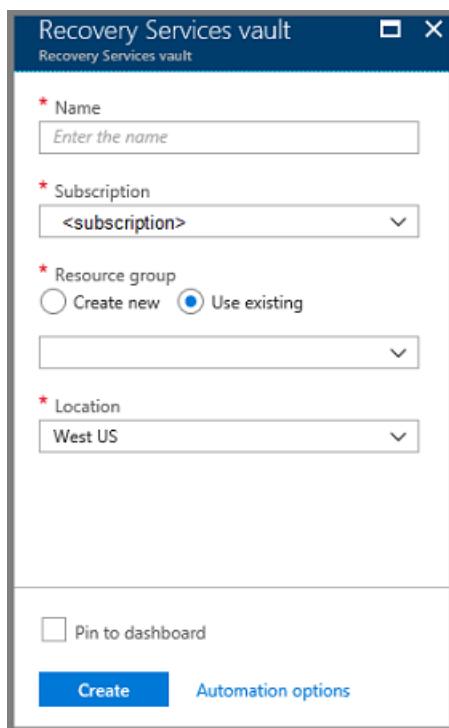


The list of Recovery Services vaults in the subscription appears.

4. On the **Recovery Services vaults** dashboard, select **Add**.



The **Recovery Services vault** dialog box opens. Provide values for the **Name**, **Subscription**, **Resource group**, and **Location**.

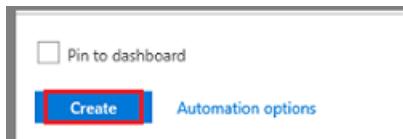


- **Name:** Enter a friendly name to identify the vault. The name must be unique to the Azure subscription. Specify a name that has at least 2 but not more than 50 characters. The name must start with a letter and consist only of letters, numbers, and hyphens.
- **Subscription:** Choose the subscription to use. If you're a member of only one subscription, you'll see that name. If you're not sure which subscription to use, use the default (suggested) subscription. There are multiple choices only if your work or school account is associated with more than one Azure subscription.
- **Resource group:** Use an existing resource group or create a new one. To see the list of available resource groups in your subscription, select **Use existing**, and then select a resource from the drop-down list. To create a new resource group, select **Create new** and enter the name. For more information about resource groups, see [Azure Resource Manager overview](#).
- **Location:** Select the geographic region for the vault. To create a vault to protect virtual machines, the vault *must* be in the same region as the virtual machines.

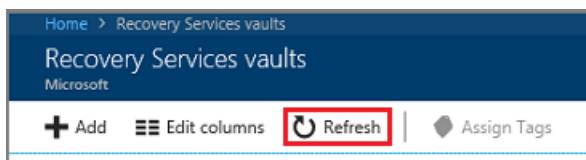
#### IMPORTANT

If you're not sure of the location of your VM, close the dialog box. Go to the list of virtual machines in the portal. If you have virtual machines in several regions, create a Recovery Services vault in each region. Create the vault in the first location, before you create the vault for another location. There's no need to specify storage accounts to store the backup data. The Recovery Services vault and Azure Backup handle that automatically.

5. When you're ready to create the Recovery Services vault, select **Create**.



It can take a while to create the Recovery Services vault. Monitor the status notifications in the **Notifications** area at the upper-right corner of the portal. After your vault is created, it's visible in the list of Recovery Services vaults. If you don't see your vault, select **Refresh**.

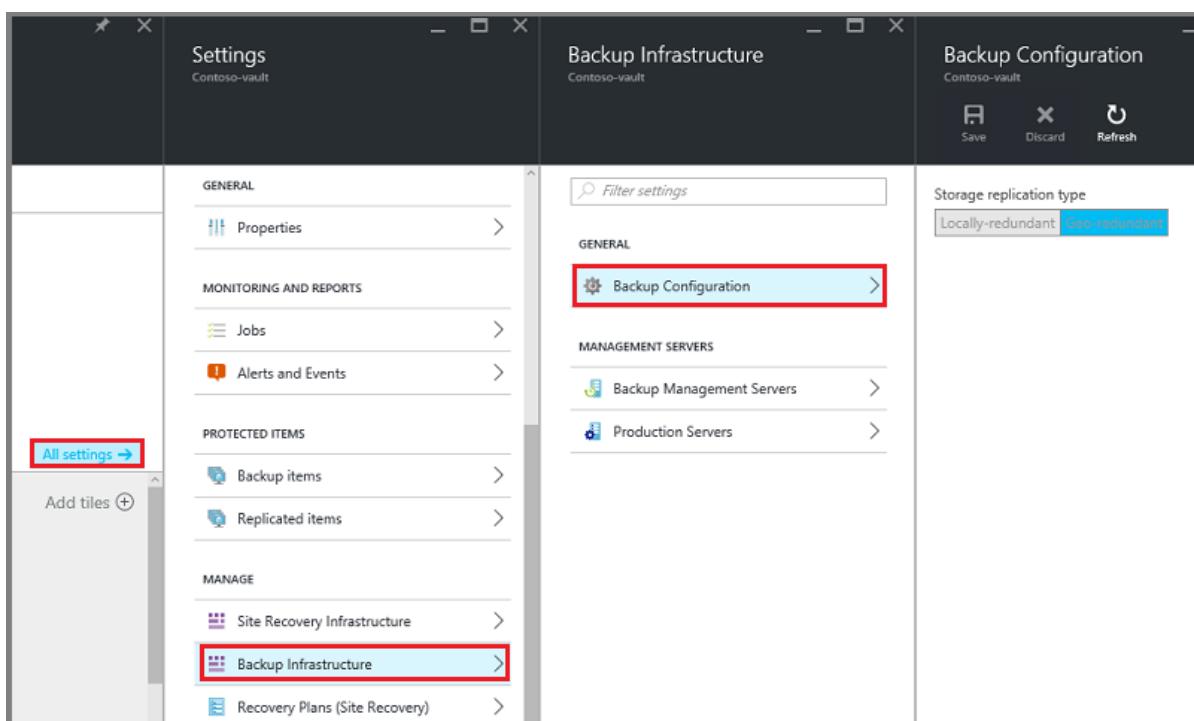


### Set Storage Replication

The Recovery Services vault storage replication option allows you to choose between geo-redundant storage and locally redundant storage. By default, Recovery Services vaults use geo-redundant storage. If this vault is your primary vault, leave the storage option set to geo-redundant storage. Choose locally redundant storage if you want a cheaper option that is less durable. Read more about [geo-redundant](#) and [locally redundant](#) storage options in the [Azure Storage replication overview](#).

To edit the storage replication setting:

1. Select your vault to open the vault dashboard and the Settings menu. If the **Settings** menu doesn't open, click **All settings** in the vault dashboard.
2. On the **Settings** menu, click **Backup Infrastructure** > **Backup Configuration** to open the **Backup Configuration** menu. On the **Backup Configuration** menu, choose the storage replication option for your vault.

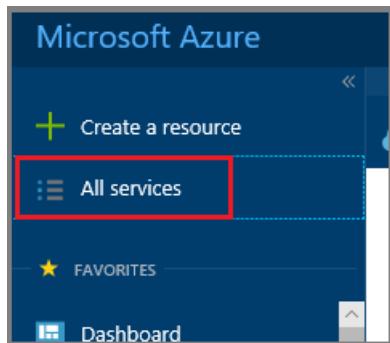


## Download Azure Backup Server installer

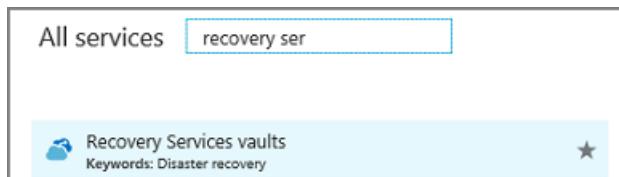
There are two ways to download the Azure Backup Server installer. You can download the Azure Backup Server installer from the [Microsoft Download Center](#). You can also download Azure Backup Server installer as you are

configuring a Recovery Services vault. The following steps walk you through downloading the installer from the Azure portal while configuring a Recovery Services vault.

1. From your Azure Stack virtual machine, [sign in to your Azure subscription in the Azure portal](#).
2. In the left-hand menu, select **All Services**.

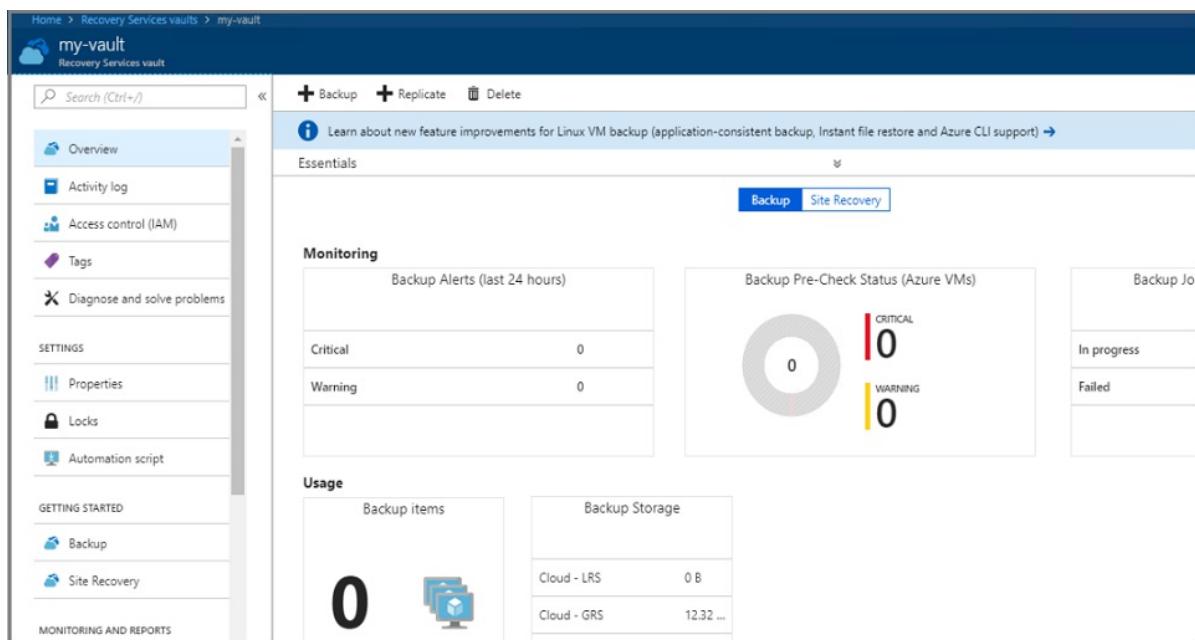


3. In the **All services** dialog, type *Recovery Services*. As you begin typing, your input filters the list of resources. Once you see it, select **Recovery Services vaults**.

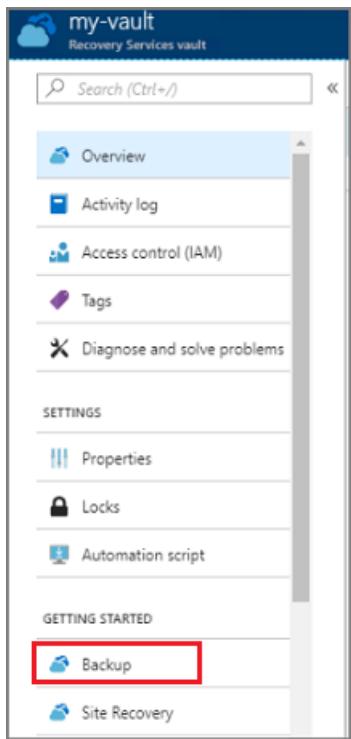


The list of Recovery Services vaults in the subscription appears.

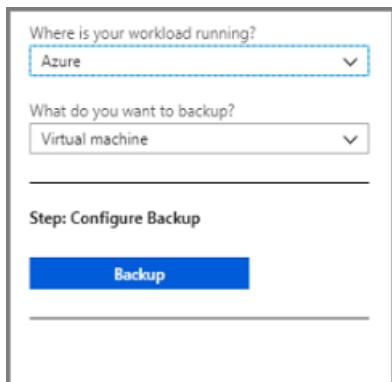
4. From the list of Recovery Services vaults, select your vault to open its dashboard.



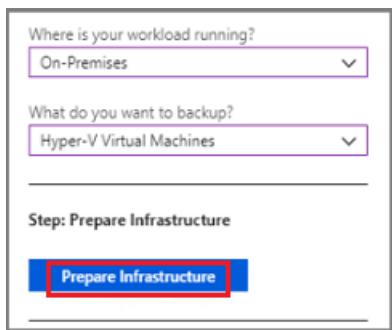
5. In the vault's Getting Started menu, click **Backup** to open the Getting Started wizard.



The backup menu opens.

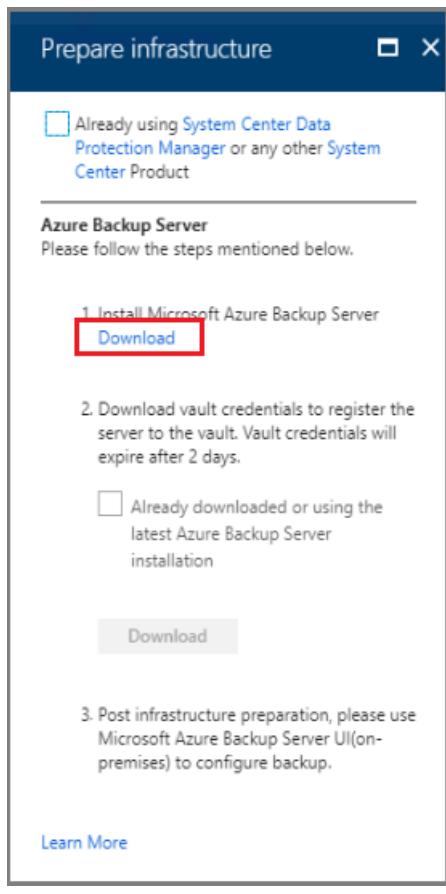


6. In the backup menu, from the **Where is your workload running** menu, select **On-premises**. From the **What do you want to backup?** drop-down menu, select the workloads you want to protect using Azure Backup Server. If you aren't sure which workloads to select, choose **Hyper-V Virtual Machines** and then click **Prepare Infrastructure**.



The **Prepare infrastructure** menu opens.

7. In the **Prepare infrastructure** menu, click **Download** to open a web page to download Azure Backup Server installation files.



The Microsoft web page that hosts the downloadable files for Azure Backup Server, opens.

8. In the Microsoft Azure Backup Server download page, select a language, and click **Download**.

The screenshot shows the Microsoft Azure Backup Server v2 download page. It features a language selection dropdown set to English and a prominent orange 'Download' button. Below the download area, there is descriptive text about the product's capabilities and links to 'Details', 'System Requirements', and 'Install Instructions' sections.

Important! Selecting a language below will dynamically change the complete page content to that language.

Select Language: English ▼

**Download**

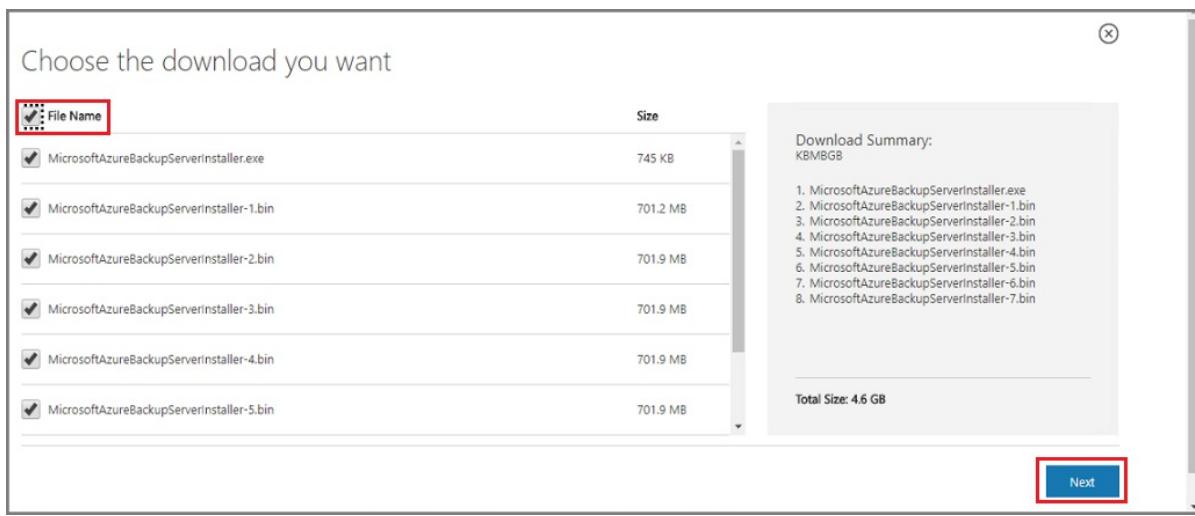
Microsoft Azure Backup provides backup for application workloads like Microsoft SQL Server, Hyper-V and VMware VMs, SharePoint Server, Exchange and Windows clients with support for both Disk to Disk backup for local copies and Disk to Disk to Cloud backup for long term retention. Azure Backup Server now supports Windows Server 2016 workloads as well as Modern Backup Storage as documented below.

**Details**

**System Requirements**

**Install Instructions**

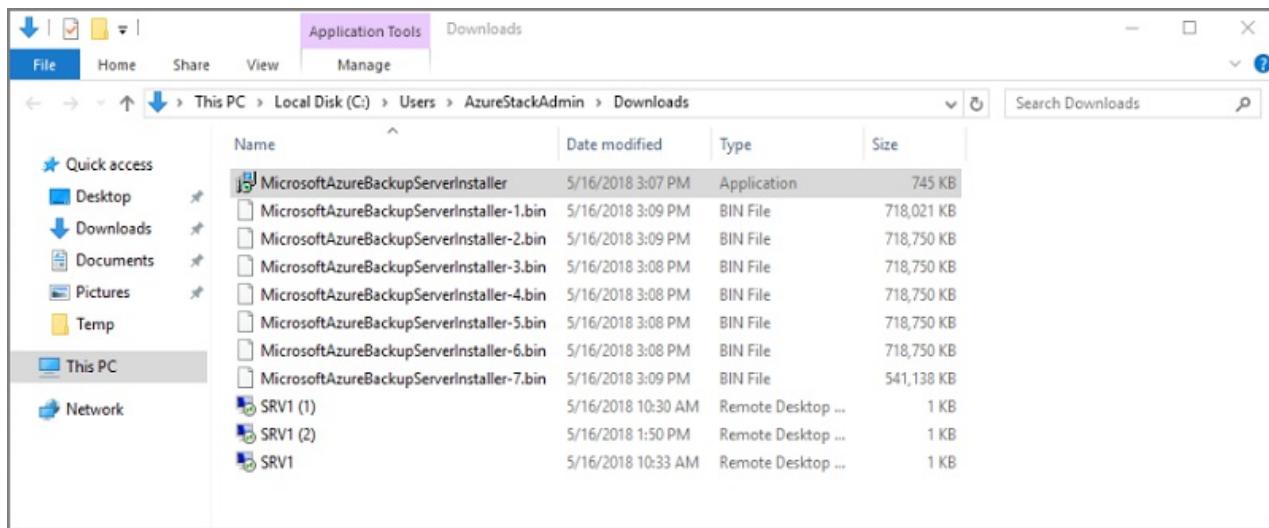
9. The Azure Backup Server installer is composed of eight files - an installer and seven .bin files. Check **File Name** to select all required files and click **Next**. Download all files to the same folder.



The download size of all installation files is larger than 3 GB. On a 10-Mbps download link, downloading all installation files may take up to 60 minutes. The files download to your specified download location.

## Extract Azure Backup Server install files

After you've downloaded all files to your Azure Stack virtual machine, go to the download location. The first phase of installing Azure Backup Server is to extract the files.

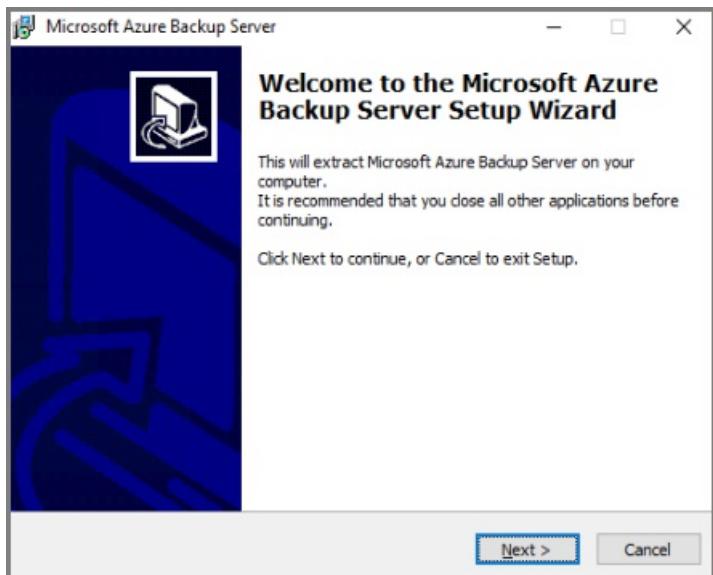


1. To start the installation, from the list of downloaded files, click **MicrosoftAzureBackupserverInstaller.exe**.

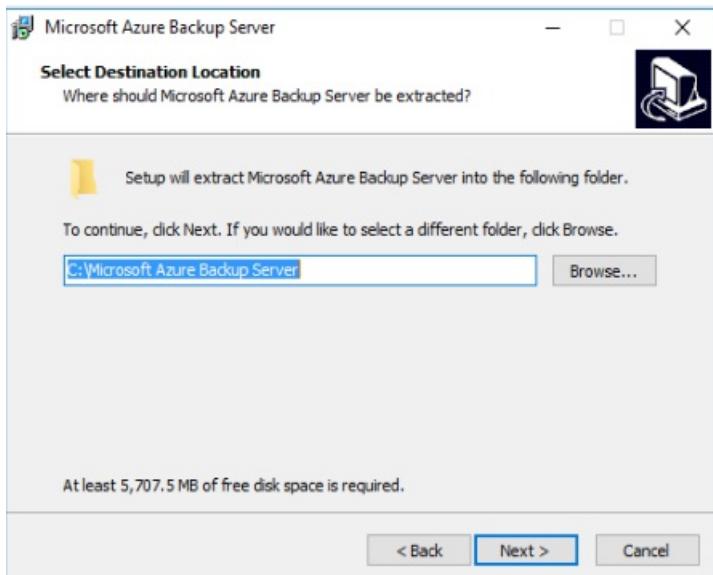
### WARNING

At least 4GB of free space is required to extract the setup files.

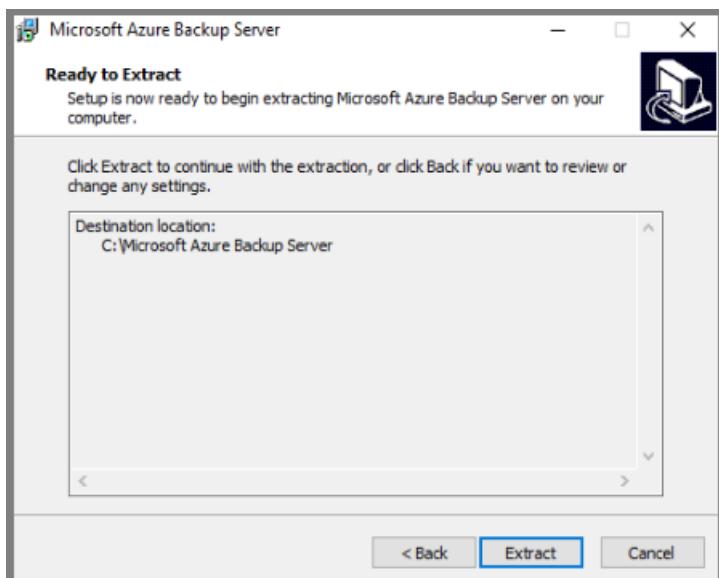
2. In the Azure Backup Server wizard, click **Next** to continue.



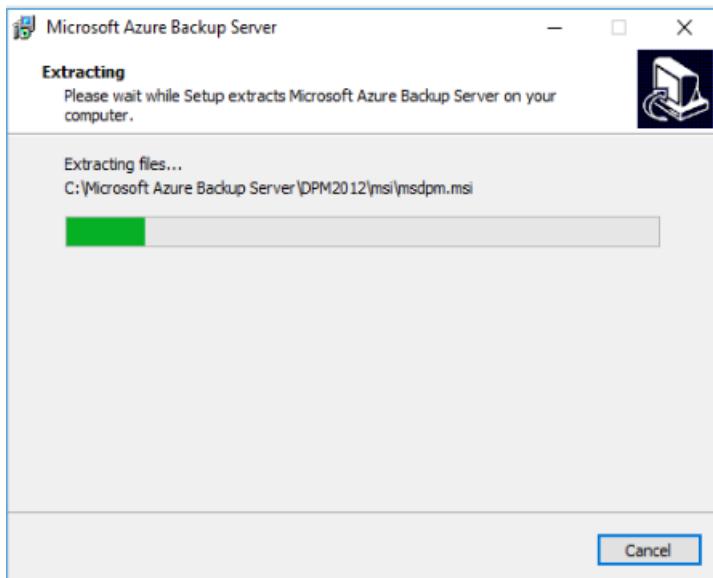
3. Choose the path for the Azure Backup Server files, and click **Next**.



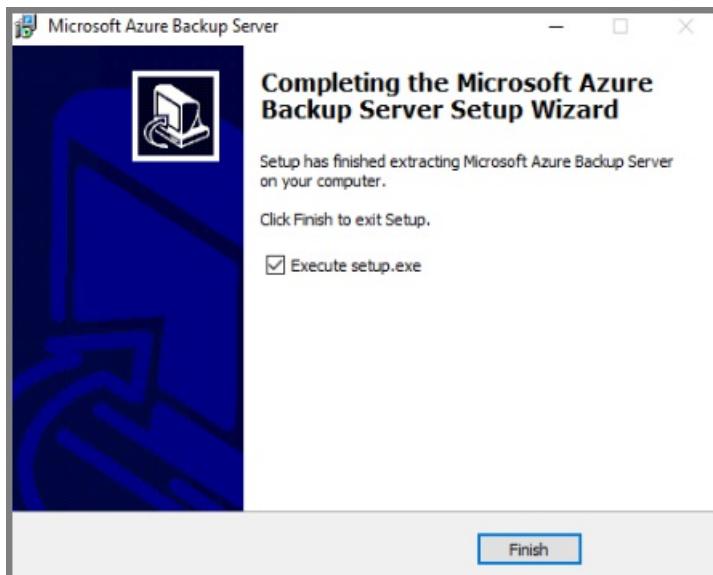
4. Verify the extraction location, and click **Extract**.



5. The wizard extracts the files and readies the installation process.

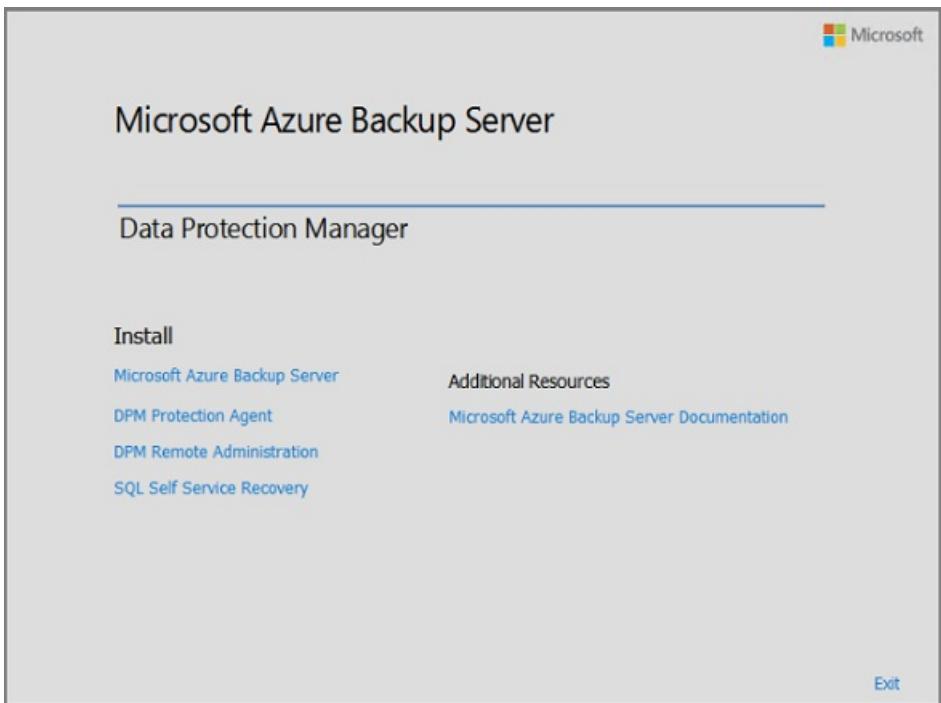


- Once the extraction process completes, click **Finish**. By default, **Execute setup.exe** is selected. When you click **Finish**, Setup.exe installs Microsoft Azure Backup Server to the specified location.



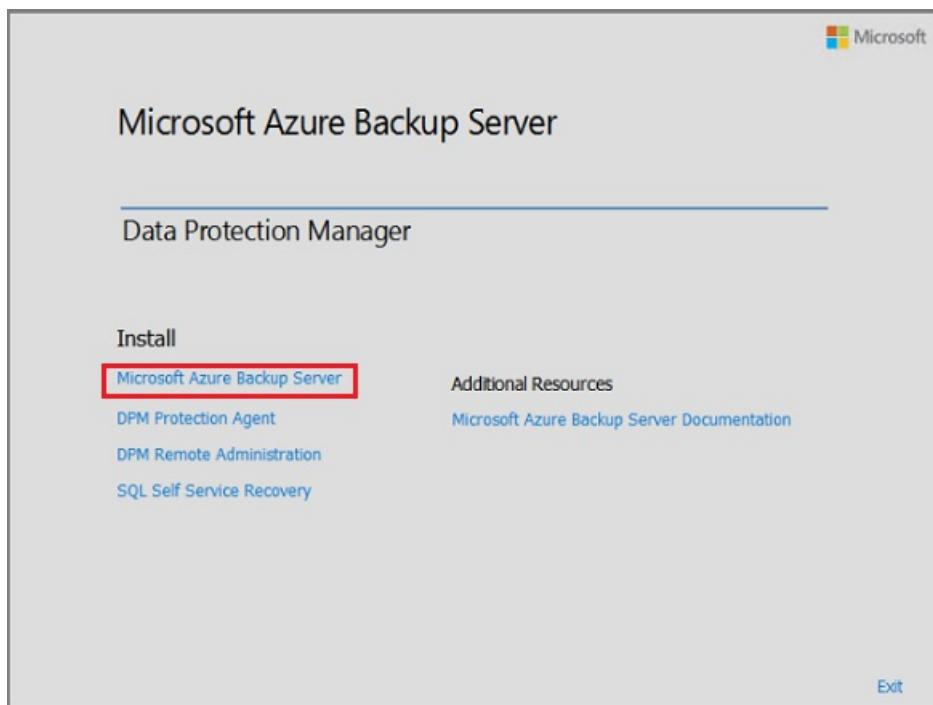
## Install the software package

In the previous step, you clicked **Finish** to exit the extraction phase, and start the Azure Backup Server setup wizard.

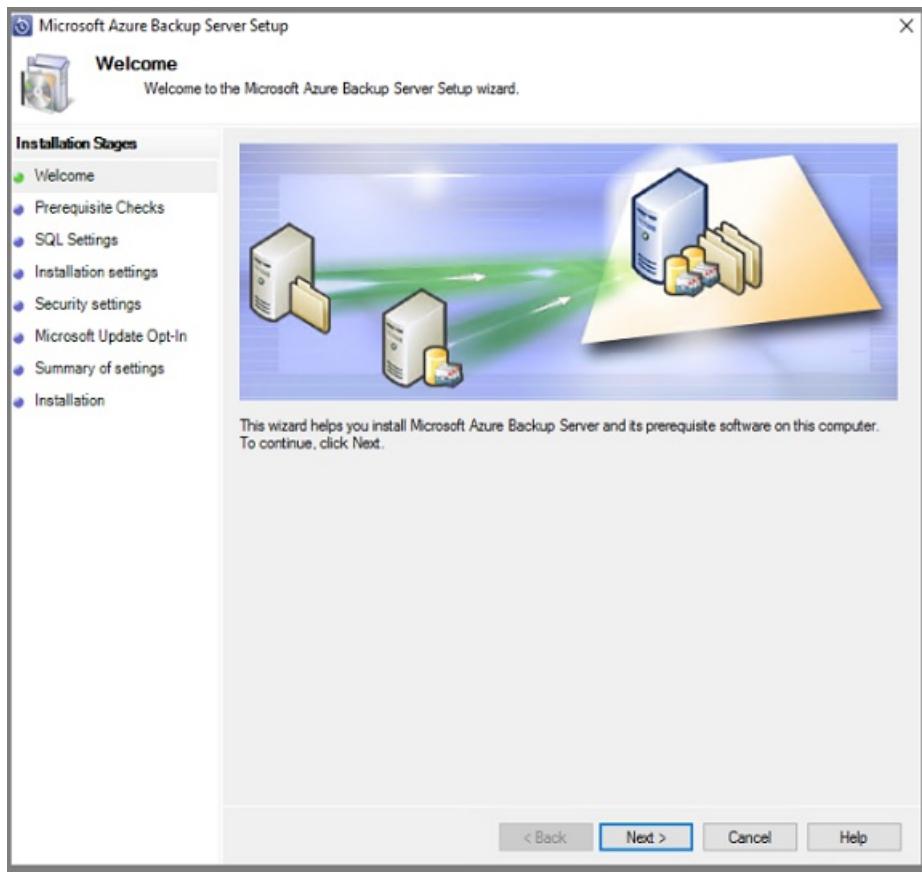


Azure Backup Server shares code with Data Protection Manager. You will see references to Data Protection Manager and DPM in the Azure Backup Server installer. Though Azure Backup Server and Data Protection Manager are separate products, these products are closely related.

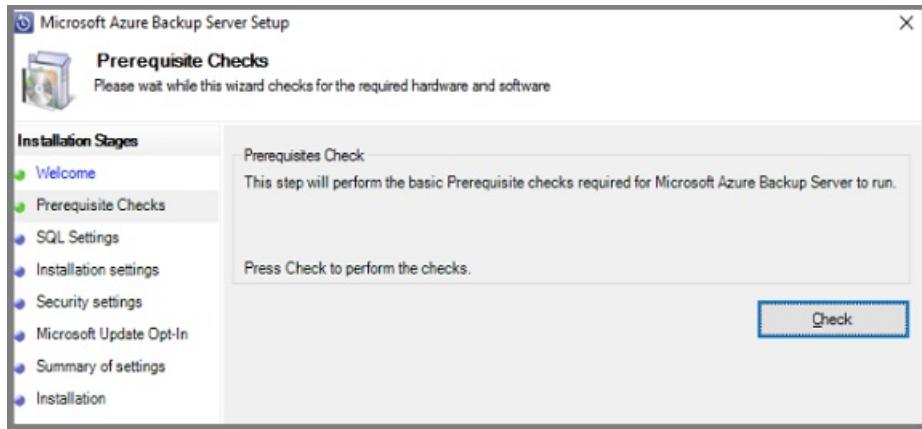
1. To launch the setup wizard, click **Microsoft Azure Backup Server**.



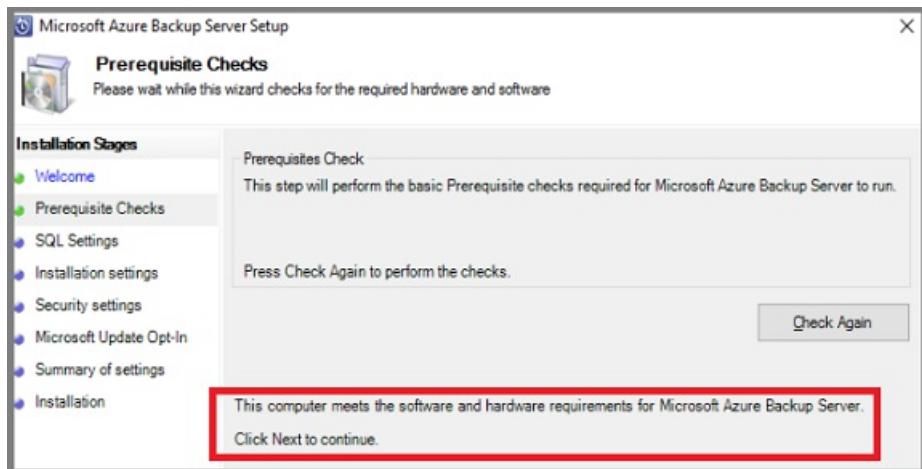
2. On the **Welcome** screen, click **Next**.



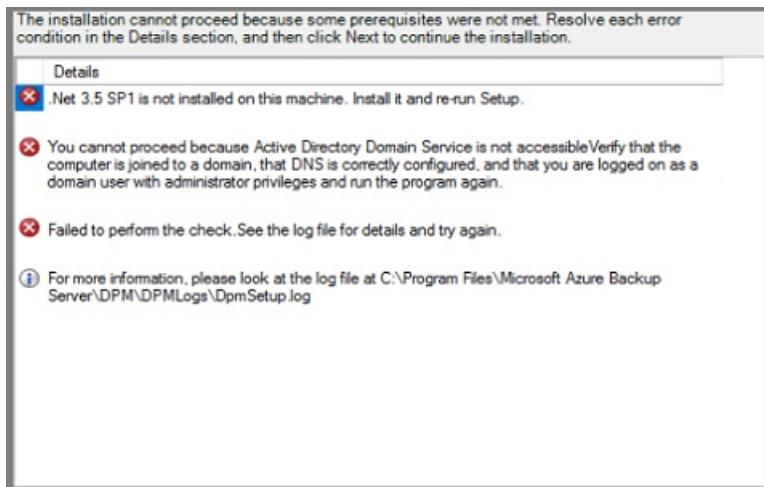
3. On the **Prerequisite Checks** screen, click **Check** to determine if the hardware and software prerequisites for Azure Backup Server have been met.



If your environment has the necessary prerequisites, you will see a message indicating that the machine meets the requirements. Click **Next**.



If your environment doesn't meet the necessary prerequisites, the issues will be specified. The prerequisites that were not met are also listed in the DpmSetup.log. Resolve the prerequisite errors, and then run **Check Again**. Installation can't proceed until all prerequisites are met.



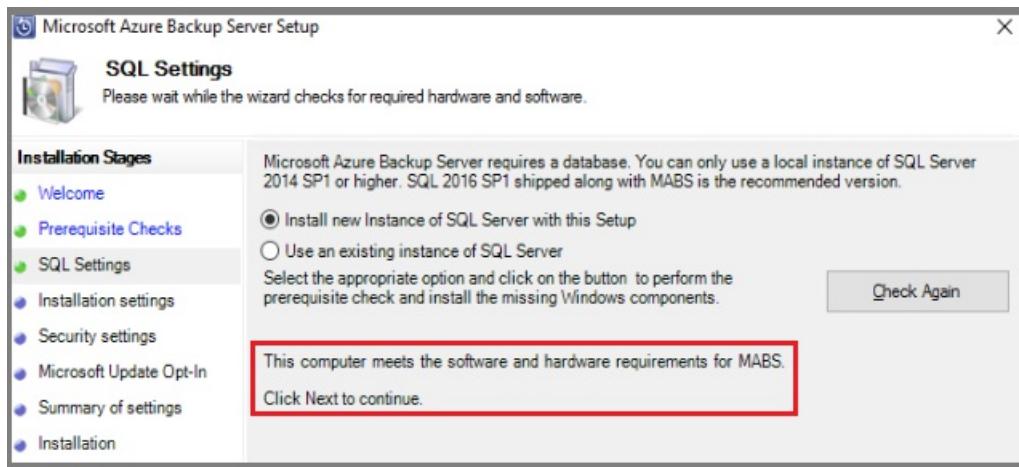
4. Microsoft Azure Backup Server requires SQL Server. The Azure Backup Server installation package comes bundled with the appropriate SQL Server binaries. If you want to use your own SQL installation, you can. However, the recommended choice is let the installer add a new instance of SQL Server. To ensure your choice works with your environment, click **Check and Install**.

#### NOTE

Azure Backup Server will not work with a remote SQL Server instance. The instance used by Azure Backup Server must be local.

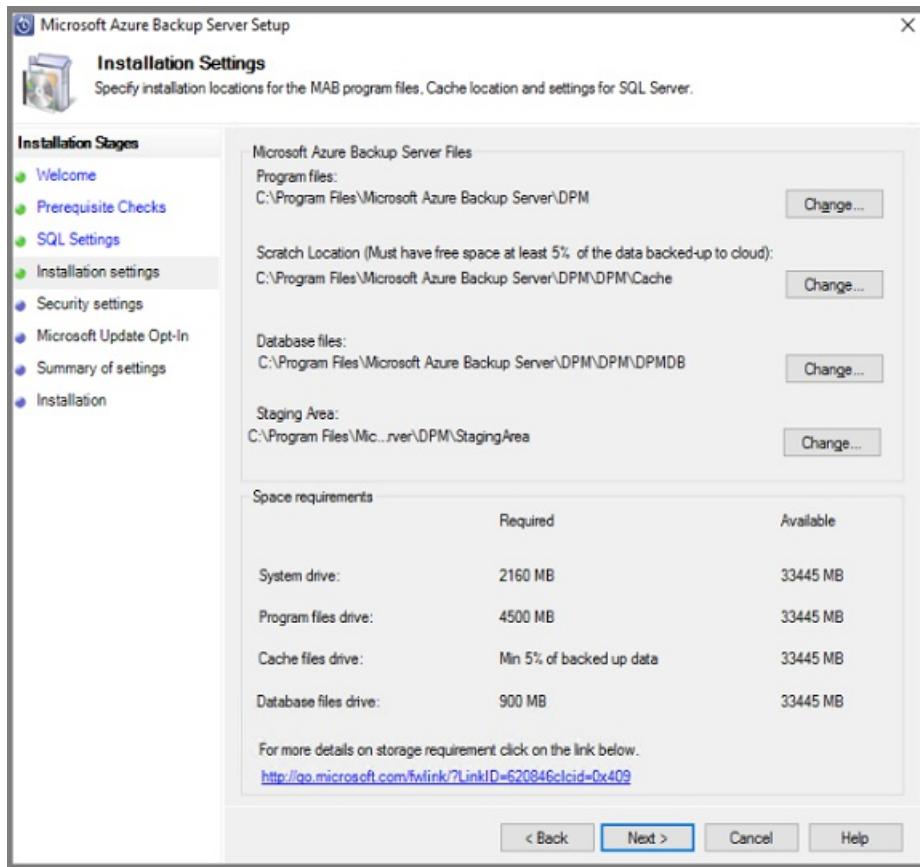


After checking, if the virtual machine has the necessary prerequisites to install Azure Backup Server, click **Next**.



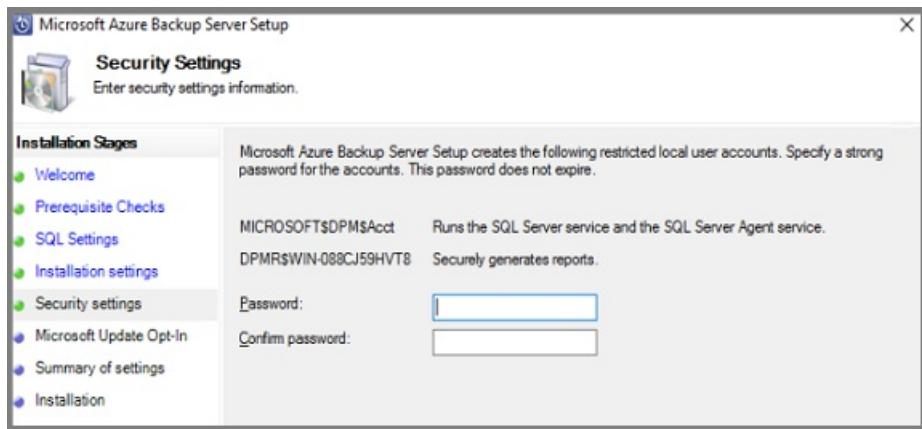
If a failure occurs with a recommendation to restart the machine, then restart the machine. After restarting the machine, restart the installer, and when you get to the **SQL Settings** screen, click **Check Again**.

5. In the **Installation Settings**, provide a location for the installation of Microsoft Azure Backup server files and click **Next**.



The scratch location is required to back up to Azure. Ensure the size of the scratch location is equivalent to at least 5% of the data planned to be backed up to Azure. For disk protection, separate disks need to be configured once the installation completes. For more information regarding storage pools, see [Configure storage pools and disk storage](#).

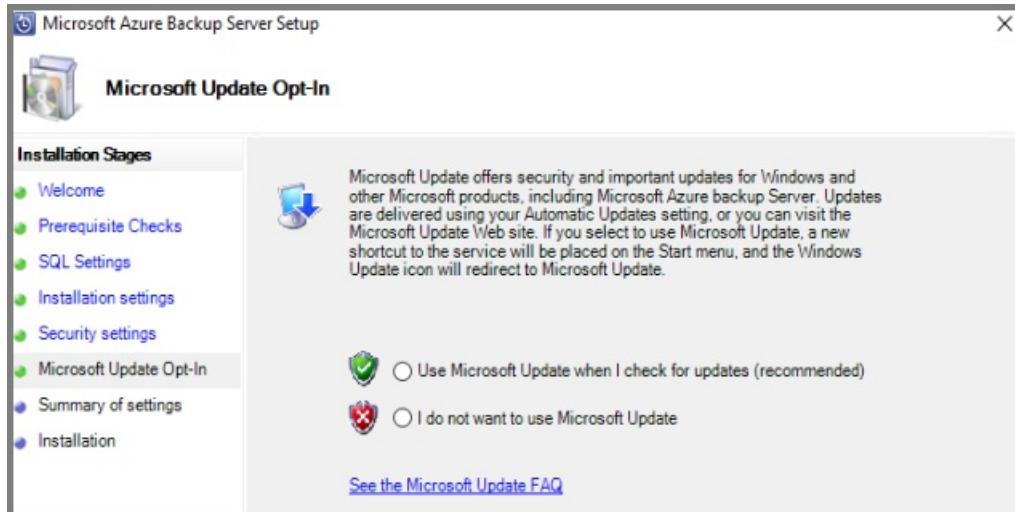
6. On the **Security Settings** screen, provide a strong password for restricted local user accounts and click **Next**.



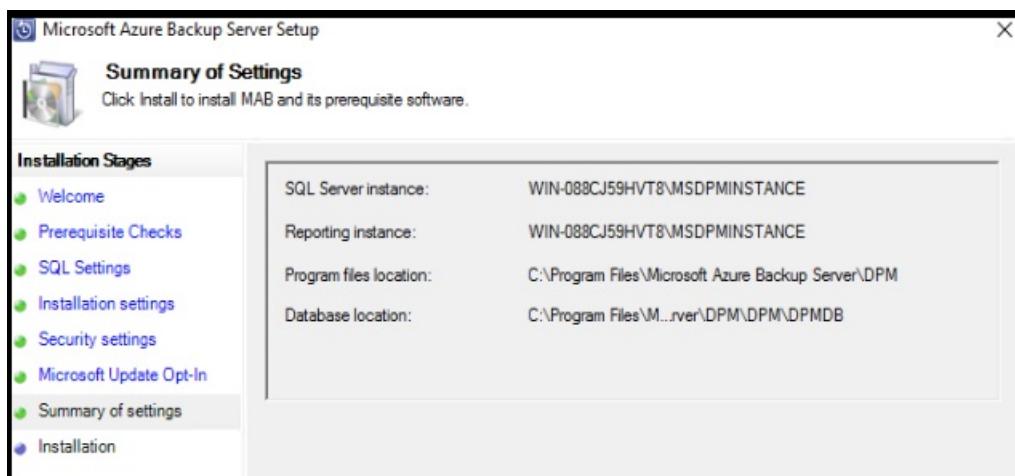
7. On the **Microsoft Update Opt-In** screen, select whether you want to use *Microsoft Update* to check for updates and click **Next**.

**NOTE**

We recommend having Windows Update redirect to Microsoft Update, which offers security and important updates for Windows and other products like Microsoft Azure Backup Server.



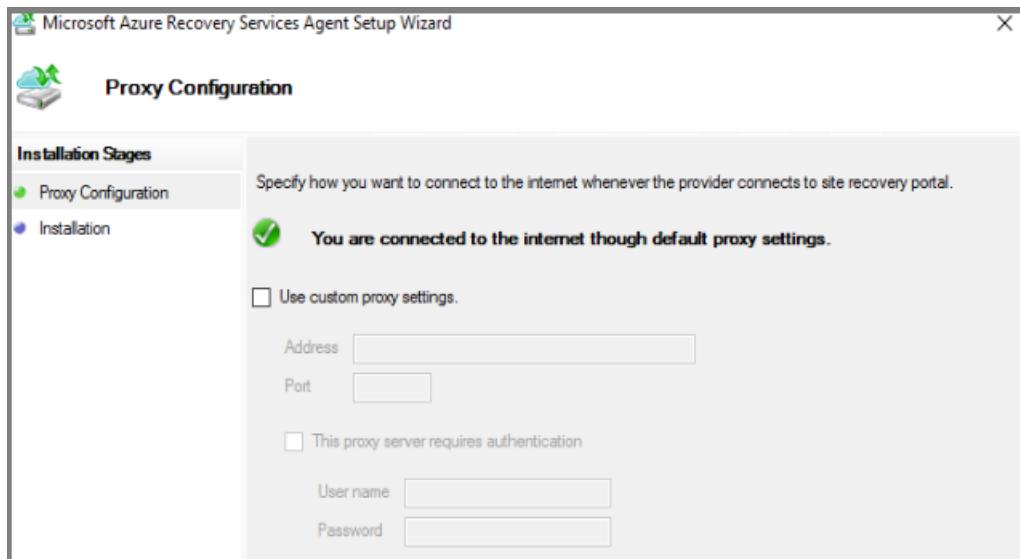
8. Review the *Summary of Settings* and click **Install**.



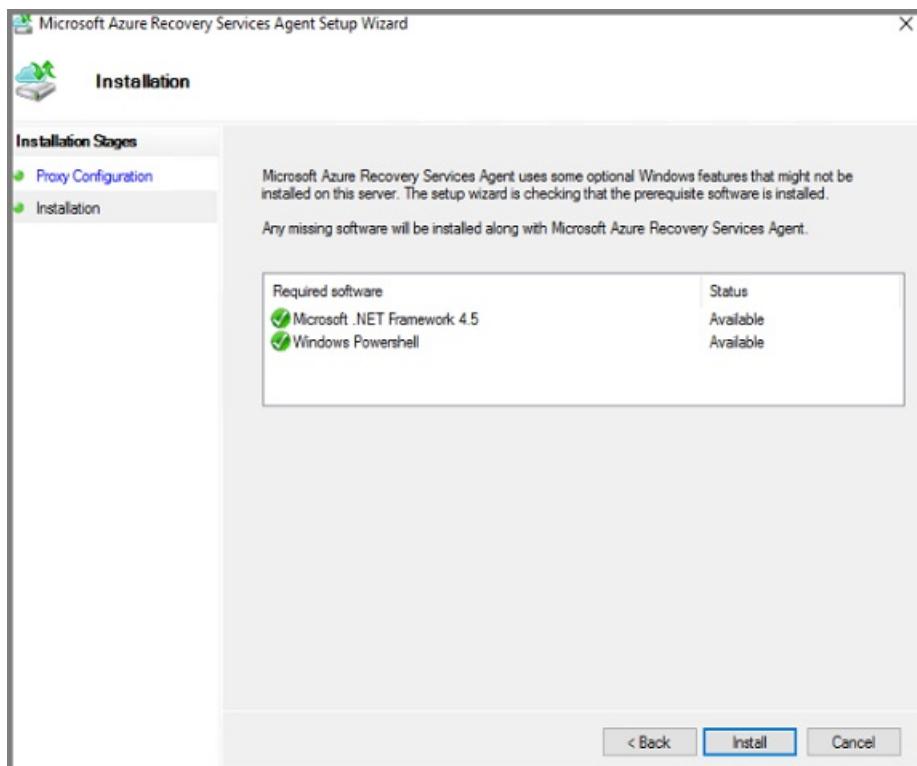
When Azure Backup Server finishes installing, the installer immediately launches the Microsoft Azure Recovery Services agent installer.

9. The Microsoft Azure Recovery Services Agent installer opens, and checks for Internet connectivity. If Internet connectivity is available, proceed with the installation. If there is no connectivity, provide proxy

details to connect to the Internet. Once you've specified your proxy settings, click **Next**.

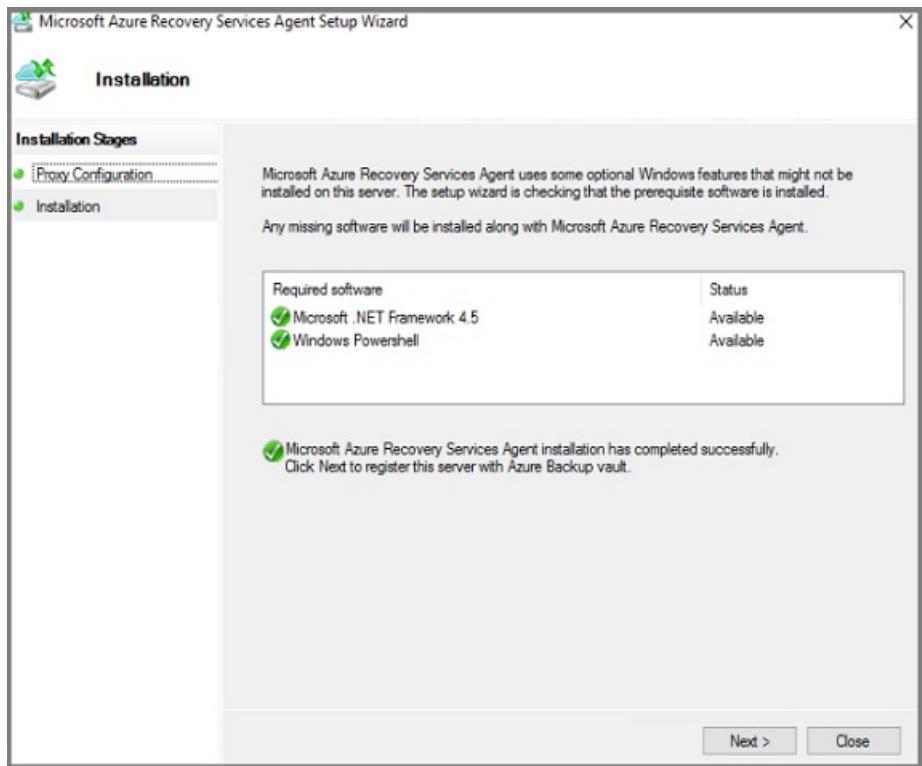


10. To install the Microsoft Azure Recovery Services Agent, click **Install**.



The Microsoft Azure Recovery Services agent, also called the Azure Backup agent, configures the Azure Backup Server to the Recovery Services vault. Once configured, Azure Backup Server will always backup data to the same Recovery Services vault.

11. Once the Microsoft Azure Recovery Services agent finishes installing, click **Next** to start the next phase: registering Azure Backup Server with the Recovery Services vault.



The installer launches the **Register Server Wizard**.

12. Switch to your Azure subscription and your Recovery Services vault. In the **Prepare Infrastructure** menu, click **Download** to download vault credentials. If the **Download** button in step 2 is not active, select **Already downloaded or using the latest Azure Backup Server installation** to activate the button. The vault credentials download to the location where you store downloads. Be aware of this location because you'll need it for the next step.

Where is your workload running?  
On-Premises

What do you want to backup?  
2 selected

**Step: Prepare Infrastructure**

**Prepare Infrastructure**

Already using System Center Data Protection Manager or any other System Center Product

**Azure Backup Server**  
Please follow the steps mentioned below.

1. Install Microsoft Azure Backup Server [Download](#)
2. Download vault credentials to register the server to the vault. Vault credentials will expire after 2 days.
- Already downloaded or using the latest Azure Backup Server installation

If you are downloading vault credentials for recovering data from an alternate server, ensure that your Azure Backup Server installation has the latest version of the Azure Recovery Services Agent. Click here to go to the latest release of the Azure Recovery Services Agent.

**Download**

3. Post infrastructure preparation, please use Microsoft Azure Backup Server UI(on-premises) to configure backup.

[Learn More](#)

13. In the **Vault Identification** menu, click **Browse** to find the Recovery Services vault credentials.

**Vault Identification**

Select the vault credentials downloaded from the quick start page in the Microsoft Azure Backup Vault.

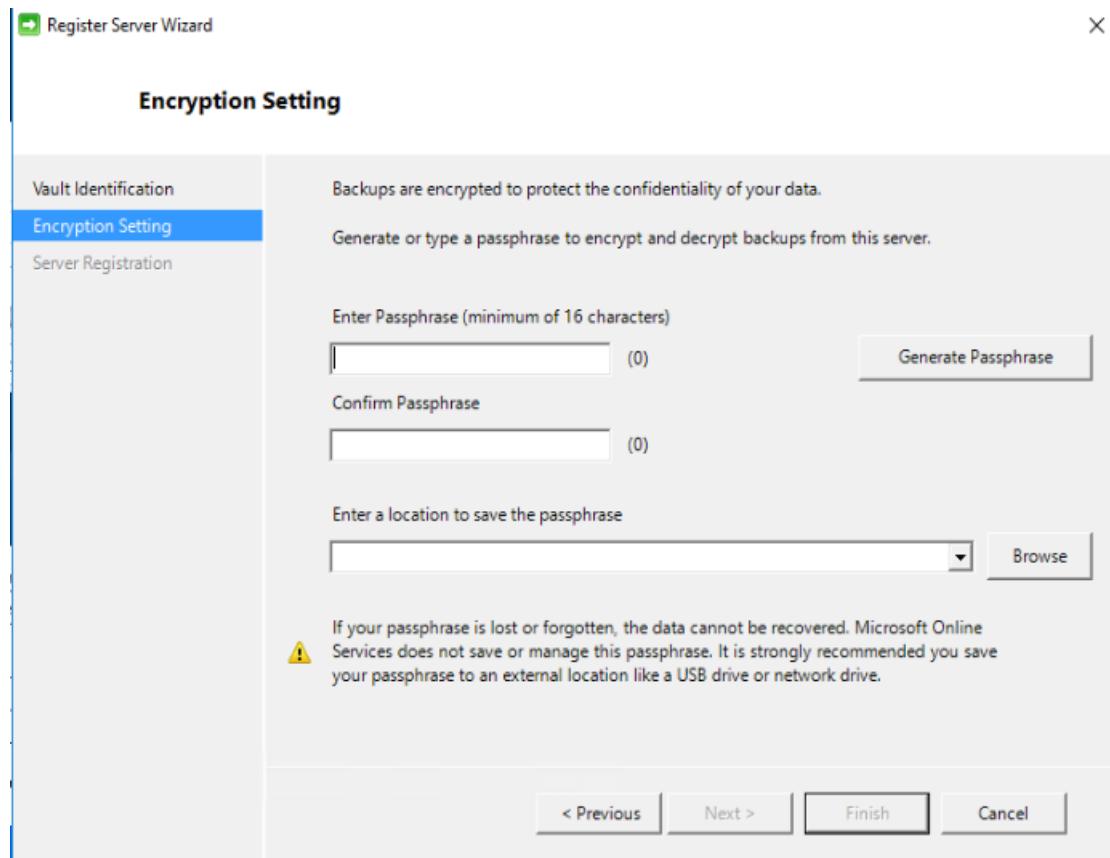
|                          |                                                             |                        |
|--------------------------|-------------------------------------------------------------|------------------------|
| Vault Credentials:       | C:\Users\AzureStackAdmin\Downloads\my-vault_Wed May 16 2018 | <a href="#">Browse</a> |
| Backup Vault:            | my-vault                                                    |                        |
| Region:                  | westus                                                      |                        |
| Subscription Identifier: | e3d2d341-4ddb-4c5d-9121-69b7e719485e                        |                        |

< Previous | Next > | Finish | Cancel

In the **Select Vault Credentials** dialog, go to the download location, select your vault credentials, and click **Open**.

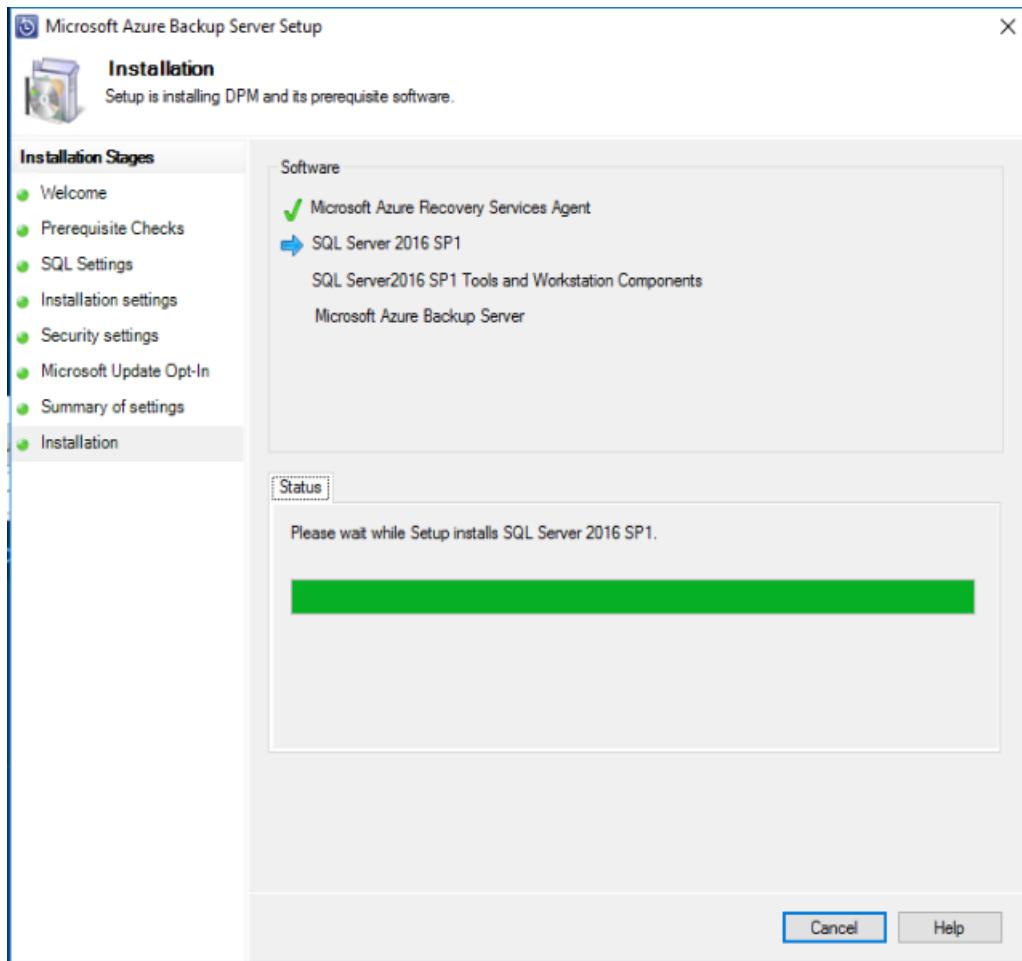
The path to the credentials appears in the Vault Identification menu. Click **Next** to advance to the Encryption Setting.

14. In the **Encryption Setting** dialog, provide a passphrase for the backup encryption, and a location to store the passphrase, and click **Next**.

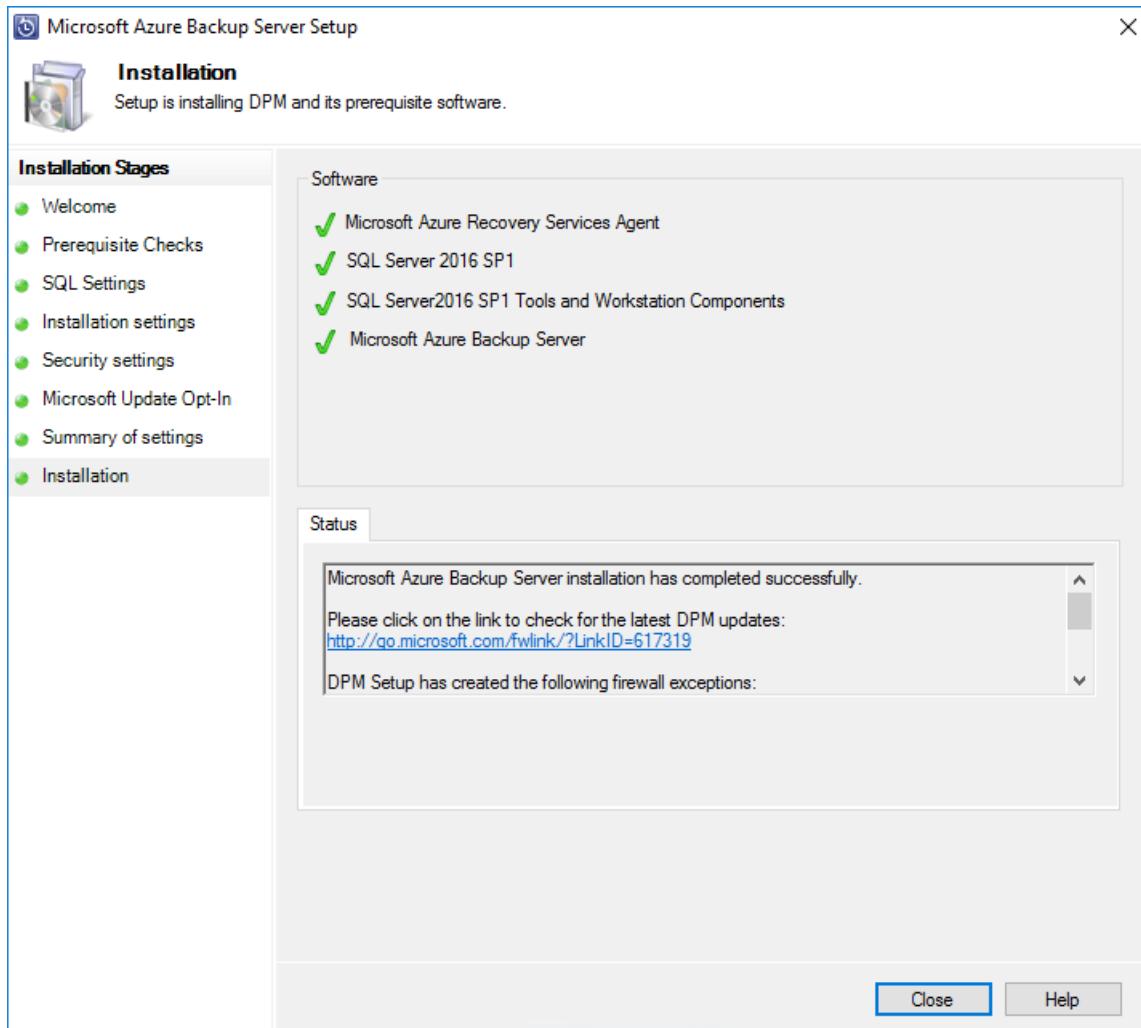


You can provide your own passphrase, or use the passphrase generator to create one for you. The passphrase is yours, and Microsoft does not save or manage this passphrase. To prepare for a disaster, save your passphrase to an accessible location.

Once you click **Next**, the Azure Backup Server is registered with the Recovery Services vault. The installer continues installing SQL Server and the Azure Backup Server.



15. When the installer completes, the Status shows that all software has been successfully installed.



When installation completes, the Azure Backup Server console and the Azure Backup Server PowerShell icons are created on the server desktop.

## Add backup storage

The first backup copy is kept on storage attached to the Azure Backup Server machine. For more information about adding disks, see [Add Modern Backup storage](#).

### NOTE

You need to add backup storage even if you plan to send data to Azure. In the Azure Backup Server architecture, the Recovery Services vault holds the *second* copy of the data while the local storage holds the first (and mandatory) backup copy.

## Network connectivity

Azure Backup Server requires connectivity to the Azure Backup service for the product to work successfully. To validate whether the machine has the connectivity to Azure, use the `Get-DPMCcloudConnection` cmdlet in the Azure Backup Server PowerShell console. If the output of the cmdlet is TRUE, then connectivity exists, else there is no connectivity.

At the same time, the Azure subscription needs to be in a healthy state. To find out the state of your subscription and to manage it, sign in to the [subscription portal](#).

Once you know the state of the Azure connectivity and of the Azure subscription, you can use the table below to find out the impact on the backup/restore functionality offered.

| CONNECTIVITY STATE          | AZURE SUBSCRIPTION | BACK UP TO AZURE | BACK UP TO DISK | RESTORE FROM AZURE                        | RESTORE FROM DISK |
|-----------------------------|--------------------|------------------|-----------------|-------------------------------------------|-------------------|
| Connected                   | Active             | Allowed          | Allowed         | Allowed                                   | Allowed           |
| Connected                   | Expired            | Stopped          | Stopped         | Allowed                                   | Allowed           |
| Connected                   | Deprovisioned      | Stopped          | Stopped         | Stopped and Azure recovery points deleted | Stopped           |
| Lost connectivity > 15 days | Active             | Stopped          | Stopped         | Allowed                                   | Allowed           |
| Lost connectivity > 15 days | Expired            | Stopped          | Stopped         | Allowed                                   | Allowed           |
| Lost connectivity > 15 days | Deprovisioned      | Stopped          | Stopped         | Stopped and Azure recovery points deleted | Stopped           |

### Recovering from loss of connectivity

If a firewall or a proxy is preventing access to Azure, add the following domain addresses in the firewall/proxy profile allow list:

- `http://www.msftncsi.com/ncsi.txt`
- \*.Microsoft.com

- \*.WindowsAzure.com
- \*.microsoftonline.com
- \*.windows.net

Once connectivity to Azure is restored to the Azure Backup Server, the Azure subscription state determines the operations that can be performed. Once the server is **Connected**, use the table in [Network connectivity](#) to see the available operations.

### Handling subscription states

It's possible to change an Azure subscription from *Expired* or *Deprovisioned* state to *Active* state. While the subscription state is not *Active*:

- While a subscription is *Deprovisioned*, it loses functionality. Restoring the subscription to *Active*, revives the backup/restore functionality. If backup data on the local disk was retained with a sufficiently large retention period, that backup data can be retrieved. However, backup data in Azure is irretrievably lost once the subscription enters the *Deprovisioned* state.
- While a subscription is *Expired*, it loses functionality. Scheduled backups do not run while a subscription is *Expired*.

## Troubleshooting

If Microsoft Azure Backup server fails with errors during the setup phase (or backup or restore), see the [error codes document](#). You can also refer to [Azure Backup related FAQs](#)

## Next steps

The article, [Preparing your environment for DPM](#), contains information about supported Azure Backup Server configurations.

You can use the following articles to gain a deeper understanding of workload protection using Microsoft Azure Backup Server.

- [SQL Server backup](#)
- [SharePoint server backup](#)
- [Alternate server backup](#)

# Back up files and applications on Azure Stack

11/18/2019 • 6 minutes to read • [Edit Online](#)

You can use Azure Backup to protect (or back up) files and applications on Azure Stack. To back up files and applications, install Microsoft Azure Backup Server as a virtual machine running on Azure Stack. You can protect the files on any Azure Stack server in the same virtual network. Once you have installed Azure Backup Server, add Azure disks to increase the local storage available for short-term backup data. Azure Backup Server uses Azure storage for long-term retention.

## NOTE

Though Azure Backup Server and System Center Data Protection Manager (DPM) are similar, DPM is not supported for use with Azure Stack.

This article does not cover installing Azure Backup Server in the Azure Stack environment. To install Azure Backup Server on Azure Stack, see the article, [Installing Azure Backup Server](#).

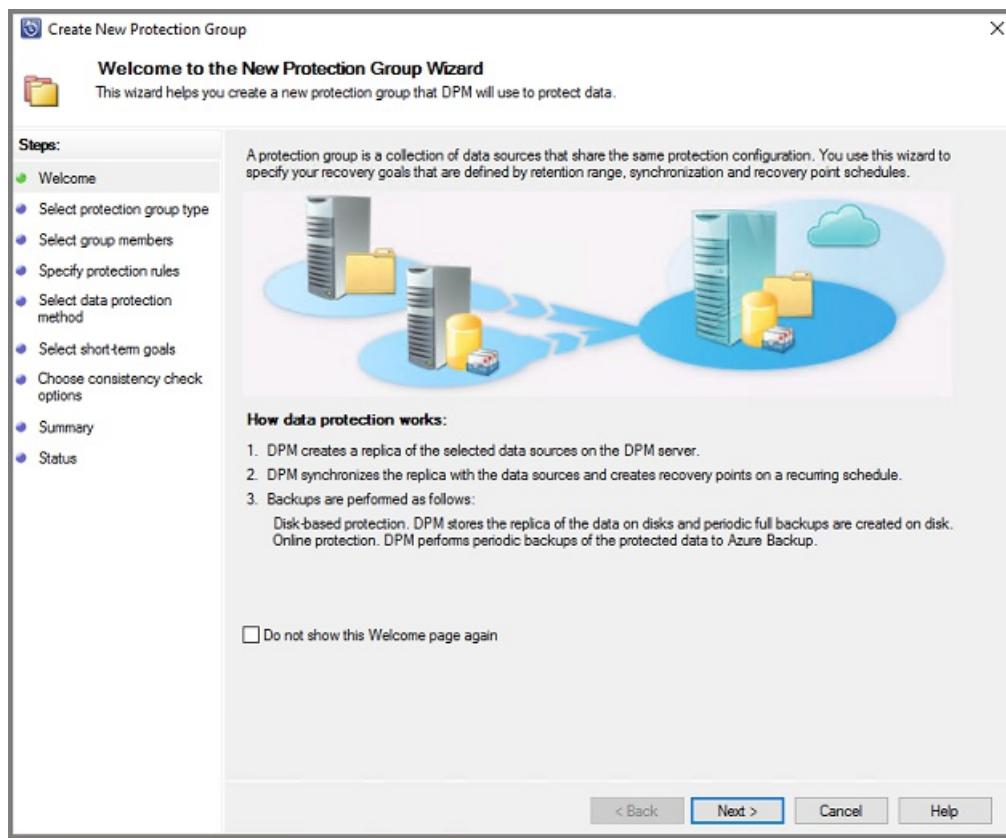
## Back up Files and Folders in Azure Stack VMs to Azure

To configure Azure Backup Server to protect Files in Azure Stack virtual machines, open the Azure Backup Server console. You'll use the console to configure protection groups and to protect the data on your virtual machines.

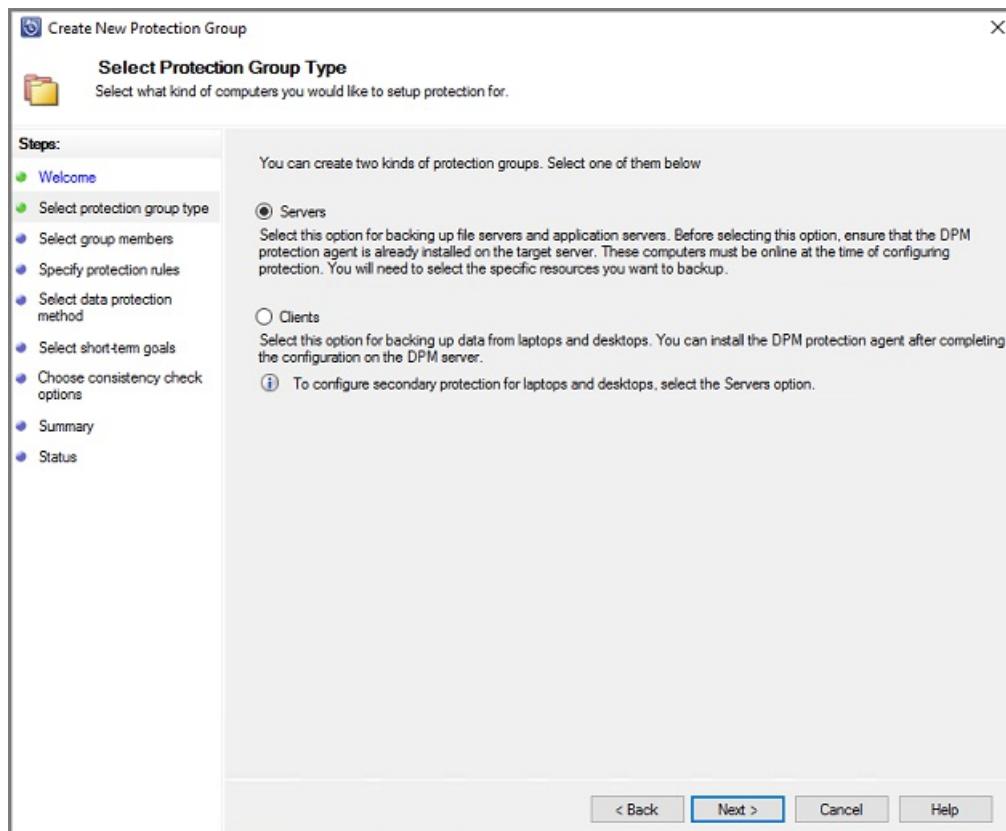
1. In the Azure Backup Server console, click **Protection** and in the toolbar, click **New** to open the **Create New Protection Group** wizard.



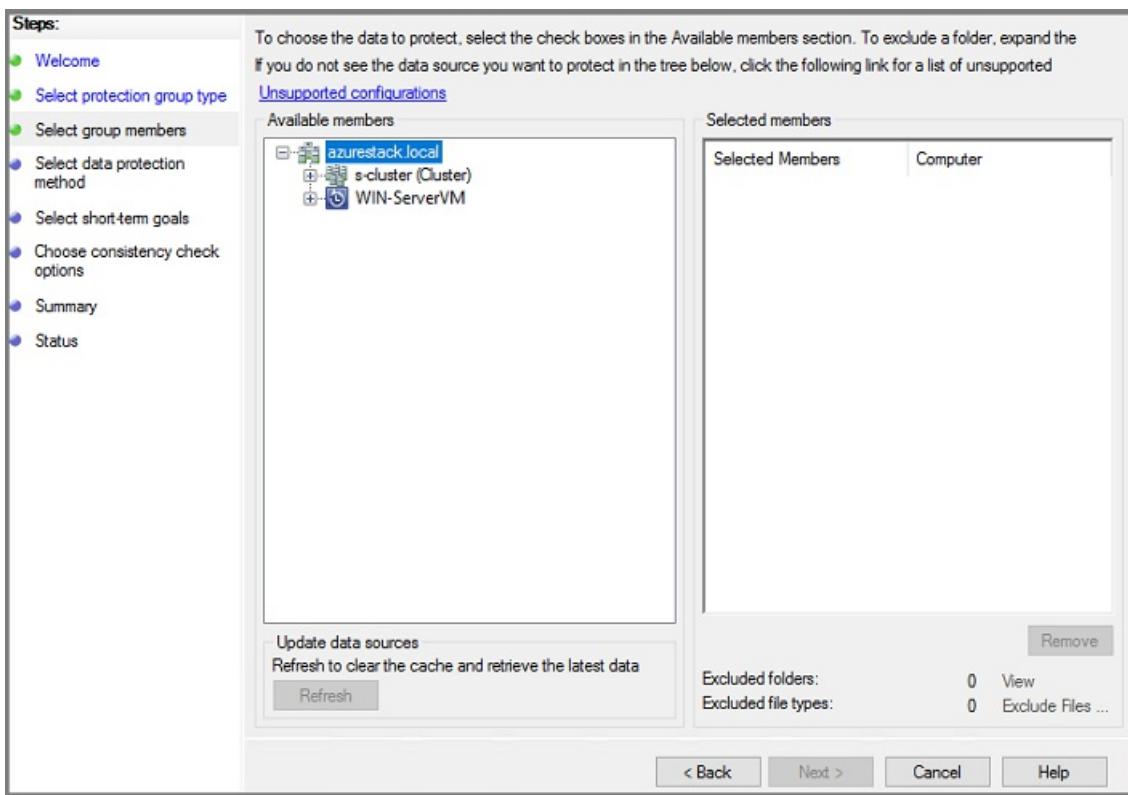
It may take a few seconds for the wizard to open. Once the wizard opens, click **Next** to advance to the **Select Protection Group Type** screen.



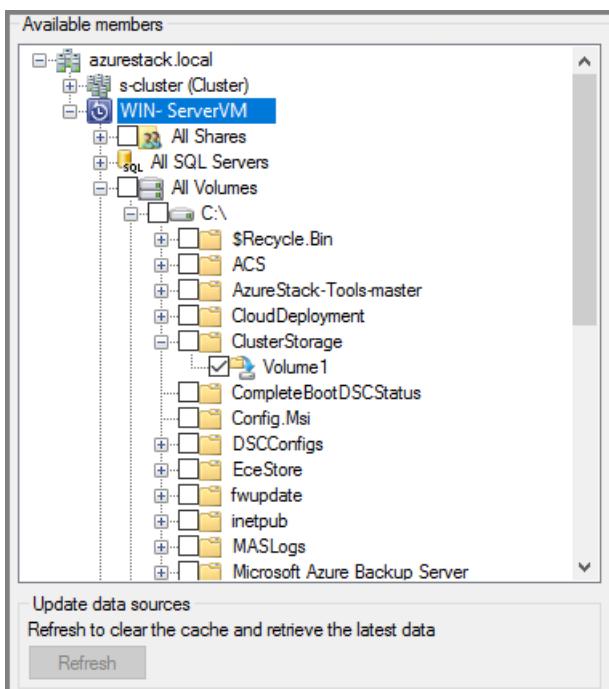
2. On the **Select Protection Group Type** screen, choose **Servers** and click **Next**.



The **Select Group Members** screen opens.

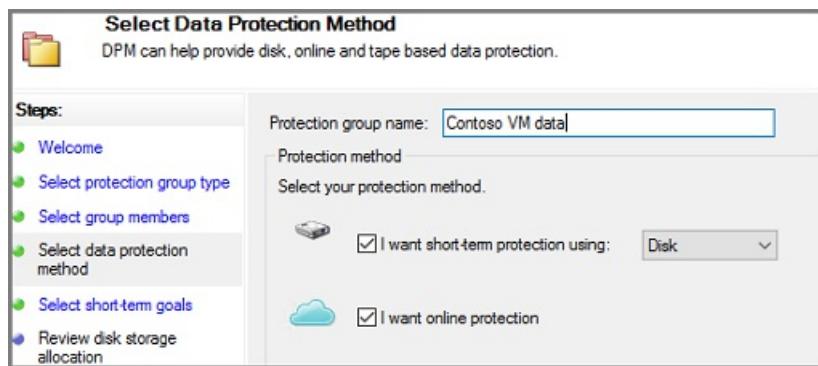


- In the **Select Group Members** screen, click + to expand the list of subitems. For all items that you want to protect, select the check box. Once all items have been selected, click **Next**.



Microsoft recommends putting all data that will share a protection policy, into one protection group. For complete information about planning and deploying protection groups, see the System Center DPM article, [Deploy Protection Groups](#).

- In the **Select Data Protection Method** screen, type a name for the protection group. Select the checkbox for **I want short-term protection using:** and **I want online protection**. Click **Next**.

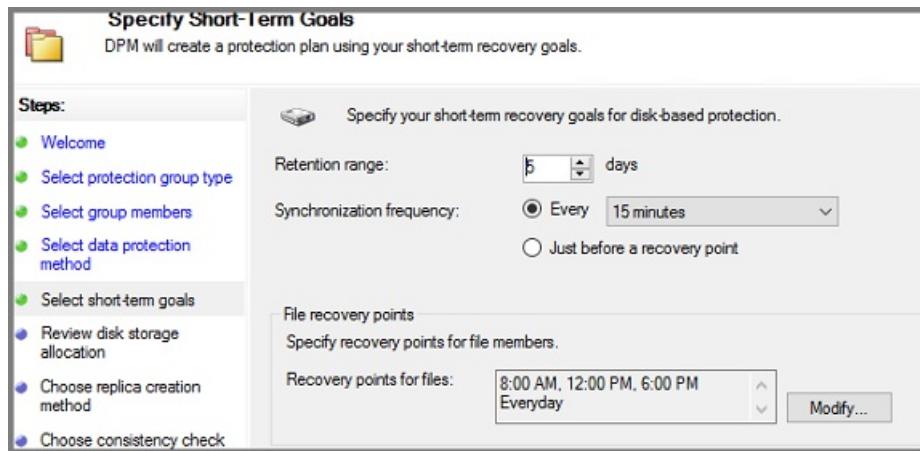


To select **I want online protection**, you must first select **I want short-term protection using:** Disk. Azure Backup Server does not protect to tape, so disk is the only choice for short-term protection.

5. In the **Specify Short-Term Goals** screen, choose how long to retain the recovery points saved to disk, and when to save incremental backups. Click **Next**.

#### IMPORTANT

You should **not** retain operational recovery (backup) data on Azure Backup Server-attached disks for more than five days.



Instead of selecting an interval for incremental backups, to run an express full backup just before each scheduled recovery point, click **Just before a recovery point**. If you're protecting application workloads, Azure Backup Server creates recovery points per the Synchronization frequency schedule (provided the application supports incremental backups). If the application doesn't support incremental backups, Azure Backup Server runs an express full backup.

For **File recovery points**, specify when to create recovery points. Click **Modify** to set the times and days of the week when recovery points are created.

6. In the **Review disk allocation** screen, review the storage pool disk space allocated for the protection group.

**Total Data size** is the size of the data you want to back up and **Disk space to be provisioned** on Azure Backup Server is the recommended space for the protection group. Azure Backup Server chooses the ideal backup volume, based on the settings. However, you can edit the backup volume choices in the Disk allocation details. For the workloads, select the preferred storage in the dropdown menu. Your edits change the values for Total Storage and Free Storage in the Available Disk Storage pane. Underprovisioned space is the amount of storage Azure Backup Server suggests you add to the volume, to continue with backups smoothly in the future.

7. In **Choose replica creation method**, select how you want to handle the initial full data replication. If you

decide to replicate over the network, Azure recommends you choose an off-peak time. For large amounts of data or less than optimal network conditions, consider replicating the data using removable media.

8. In **Choose consistency check options**, select how you want to automate consistency checks. Enable consistency checks to run only when data replication becomes inconsistent, or according to a schedule. If you don't want to configure automatic consistency checking, run a manual check at any time by:
  - In the **Protection** area of the Azure Backup Server console, right-click the protection group and select **Perform Consistency Check**.
9. If you choose to back up to Azure, on the **Specify online protection data** page make sure the workloads you want to back up to Azure are selected.
10. In **Specify online backup schedule**, specify when incremental backups to Azure should occur.

You can schedule backups to run every day/week/month/year and the time/date at which they should run. Backups can occur up to twice a day. Each time a backup job runs, a data recovery point is created in Azure from the copy of the backed-up data stored on the Azure Backup Server disk.
11. In **Specify online retention policy**, specify how the recovery points created from the daily/weekly/monthly/yearly backups are retained in Azure.
12. In **Choose online replication**, specify how the initial full replication of data occurs.
13. On **Summary**, review your settings. When you click **Create Group**, the initial data replication occurs. When the data replication finishes, on the **Status** page, the protection group status shows as **OK**. The initial backup job takes place in line with the protection group settings.

## Recover file data

Use Azure Backup Server console to recover data to your virtual machine.

1. In the Azure Backup Server console, on the navigation bar, click **Recovery** and browse for the data you want to recover. In the results pane, select the data.
2. On the calendar in the recovery points section, dates in bold indicate recovery points are available. Select the date to recover.
3. In the **Recoverable item** pane, select the item you want to recover.
4. In the **Actions** pane, click **Recover** to open the Recovery Wizard.
5. You can recover data as follows:
  - **Recover to the original location** - If the client computer is connected over VPN, this option doesn't work. Instead use an alternate location, and then copy data from that location.
  - **Recover to an alternate location**
6. Specify the recovery options:
  - For **Existing version recovery behavior**, select **Create copy**, **Skip**, or **Overwrite**. Overwrite is available only when recovering to the original location.
  - For **Restore security**, choose **Apply settings of the destination computer** or **Apply the security settings of the recovery point version**.
  - For **Network bandwidth usage throttling**, click **Modify** to enable network bandwidth usage throttling.
  - **Notification** Click **Send an e-mail when the recovery completes**, and specify the recipients who will receive the notification. Separate the e-mail addresses with commas.
  - After making the selections, click **Next**

7. Review your recovery settings, and click **Recover**.

**NOTE**

While the recovery job is in progress, all synchronization jobs for the selected recovery items are canceled.

If you're using Modern Backup Storage (MBS), File Server end-user recovery (EUR) isn't supported. File Server EUR has a dependency on Volume Shadow Copy Service (VSS), which Modern Backup Storage doesn't use. If EUR is enabled, use the following steps to recover data:

1. Navigate to the protected files, and right-click the file name and select **Properties**.
2. On the **Properties** menu, click **Previous Versions** and choose the version you want to recover.

## View Azure Backup Server with a vault

To view Azure Backup Server entities in the Azure portal, you can follow the following steps:

1. Open Recovery Services vault.
2. Click Backup Infrastructure.
3. View Backup Management Servers.

## Next steps

For information on using Azure Backup Server to protect other workloads, see one of the following articles:

- [Back up SharePoint farm](#)
- [Back up SQL server](#)

# Back up a SharePoint farm on Azure Stack

2/24/2020 • 9 minutes to read • [Edit Online](#)

You back up a SharePoint farm on Azure Stack to Microsoft Azure by using Microsoft Azure Backup Server (MABS) in much the same way that you back up other data sources. Azure Backup provides flexibility in the backup schedule to create daily, weekly, monthly, or yearly backup points and gives you retention policy options for various backup points. It also provides the capability to store local disk copies for quick recovery-time objectives (RTO) and to store copies to Azure for economical, long-term retention.

## SharePoint supported versions and related protection scenarios

Azure Backup for MABS supports the following scenarios:

| WORKLOAD   | VERSION                                           | SHAREPOINT DEPLOYMENT                                                          | PROTECTION AND RECOVERY                                                                                                                                                    |
|------------|---------------------------------------------------|--------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SharePoint | SharePoint 2016, SharePoint 2013, SharePoint 2010 | SharePoint deployed as an Azure Stack virtual machine<br>-----<br>SQL AlwaysOn | Protect SharePoint Farm recovery options: Recovery farm, database, and file or list item from disk recovery points. Farm and database recovery from Azure recovery points. |

## Before you start

There are a few things you need to confirm before you back up a SharePoint farm to Azure.

### Prerequisites

Before you proceed, make sure that you have [installed and prepared the Azure Backup Server](#) to protect workloads.

### Protection agent

The Azure Backup agent must be installed on the server that's running SharePoint, the servers that are running SQL Server, and all other servers that are part of the SharePoint farm. For more information about how to set up the protection agent, see [Setup Protection Agent](#). The one exception is that you install the agent only on a single web front end (WFE) server. Azure Backup Server needs the agent on one WFE server only to serve as the entry point for protection.

### SharePoint farm

For every 10 million items in the farm, there must be at least 2 GB of space on the volume where the MABS folder is located. This space is required for catalog generation. For MABS to recover specific items (site collections, sites, lists, document libraries, folders, individual documents, and list items), catalog generation creates a list of the URLs that are contained within each content database. You can view the list of URLs in the recoverable item pane in the **Recovery** task area of MABS Administrator Console.

### SQL Server

Azure Backup Server runs as a LocalSystem account. To back up SQL Server databases, MABS needs sysadmin privileges on that account for the server that's running SQL Server. Set NT AUTHORITY\SYSTEM to *sysadmin* on the server that's running SQL Server before you back it up.

If the SharePoint farm has SQL Server databases that are configured with SQL Server aliases, install the SQL

Server client components on the front-end Web server that MABS will protect.

### What's not supported

- MABS that protects a SharePoint farm does not protect search indexes or application service databases. You will need to configure the protection of these databases separately.
- MABS does not provide backup of SharePoint SQL Server databases that are hosted on scale-out file server (SOFS) shares.

## Configure SharePoint protection

Before you can use MABS to protect SharePoint, you must configure the SharePoint VSS Writer service (WSS Writer service) by using **ConfigureSharePoint.exe**.

You can find **ConfigureSharePoint.exe** in the [MABS Installation Path]\bin folder on the front-end web server. This tool provides the protection agent with the credentials for the SharePoint farm. You run it on a single WFE server. If you have multiple WFE servers, select just one when you configure a protection group.

### To configure the SharePoint VSS Writer service

1. On the WFE server, at a command prompt, go to [MABS installation location]\bin\
2. Enter ConfigureSharePoint -EnableSharePointProtection.
3. Enter the farm administrator credentials. This account should be a member of the local Administrator group on the WFE server. If the farm administrator isn't a local admin, grant the following permissions on the WFE server:
  - Grant the WSS\_Admin\_WPG group full control to the DPM folder (%Program Files%\Microsoft Azure Backup\DPM).
  - Grant the WSS\_Admin\_WPG group read access to the DPM Registry key (HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager).

#### NOTE

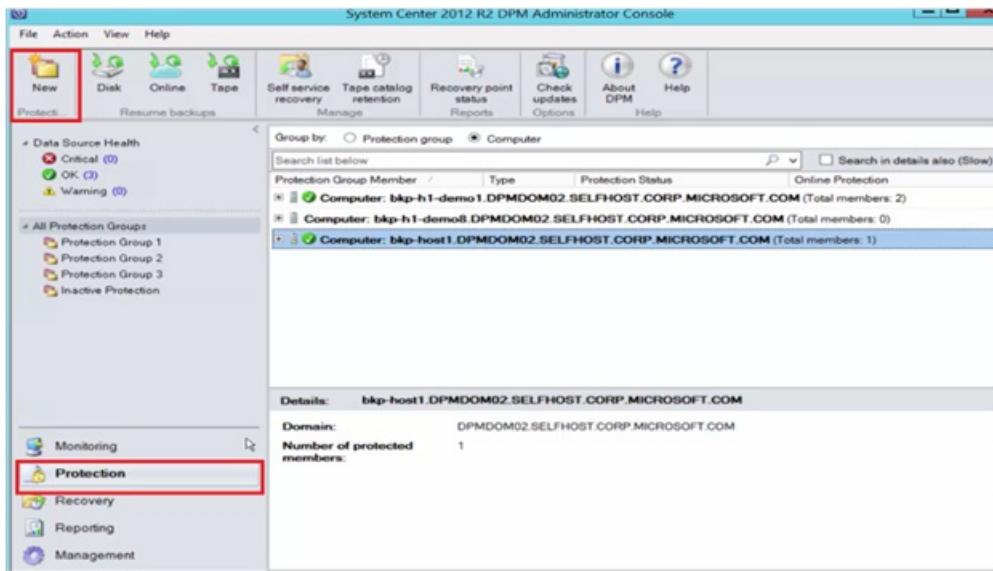
You'll need to rerun ConfigureSharePoint.exe whenever there's a change in the SharePoint farm administrator credentials.

## Back up a SharePoint farm by using MABS

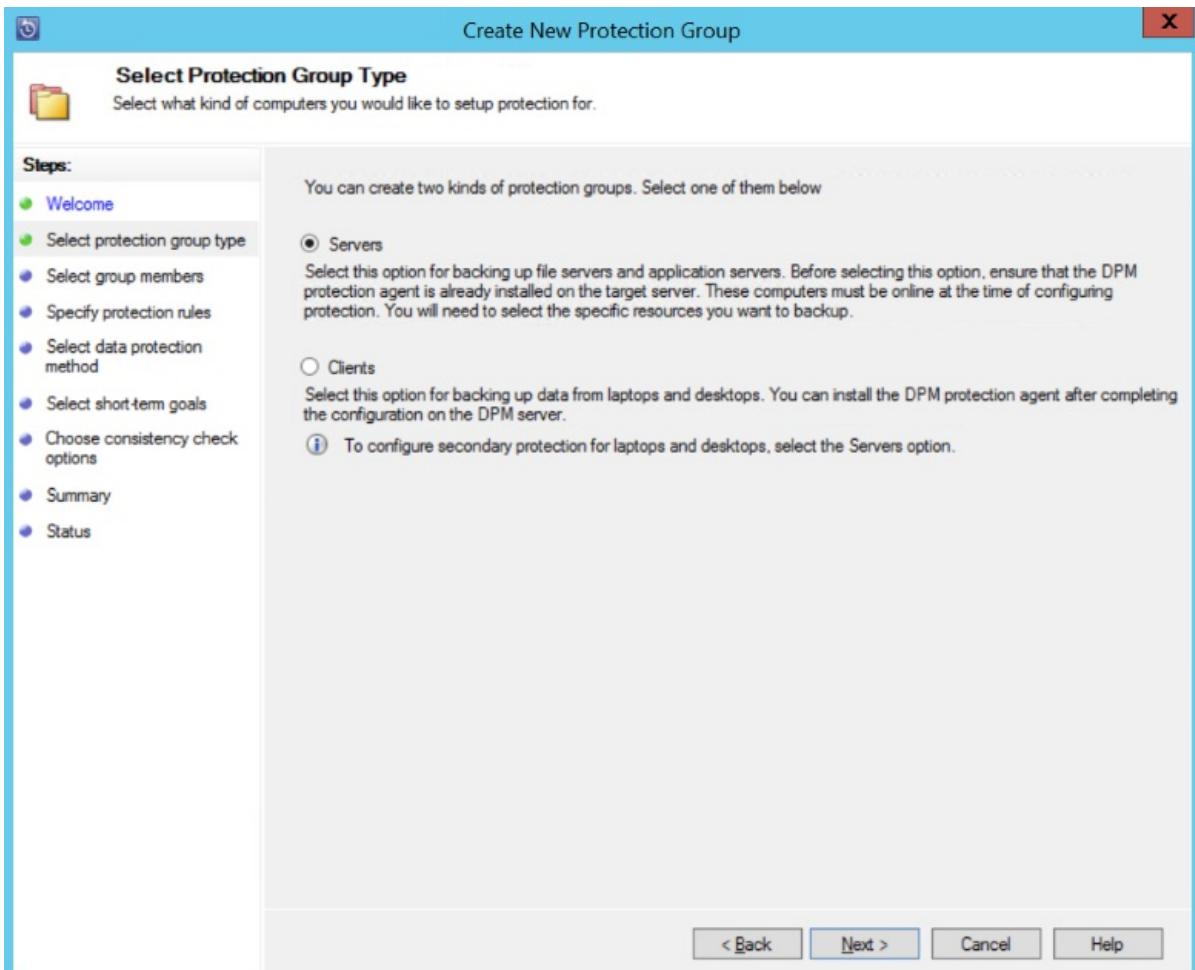
After you have configured MABS and the SharePoint farm as explained previously, SharePoint can be protected by MABS.

### To protect a SharePoint farm

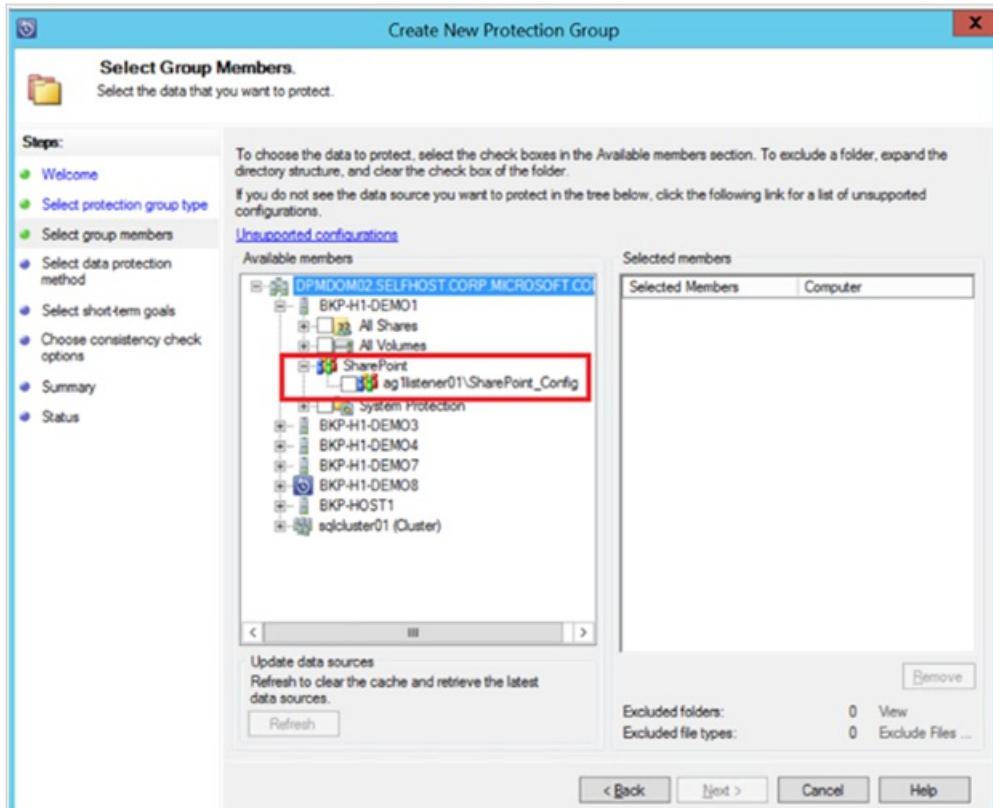
1. From the **Protection** tab of the MABS Administrator Console, click **New**.



2. On the **Select Protection Group Type** page of the **Create New Protection Group** wizard, select **Servers**, and then click **Next**.



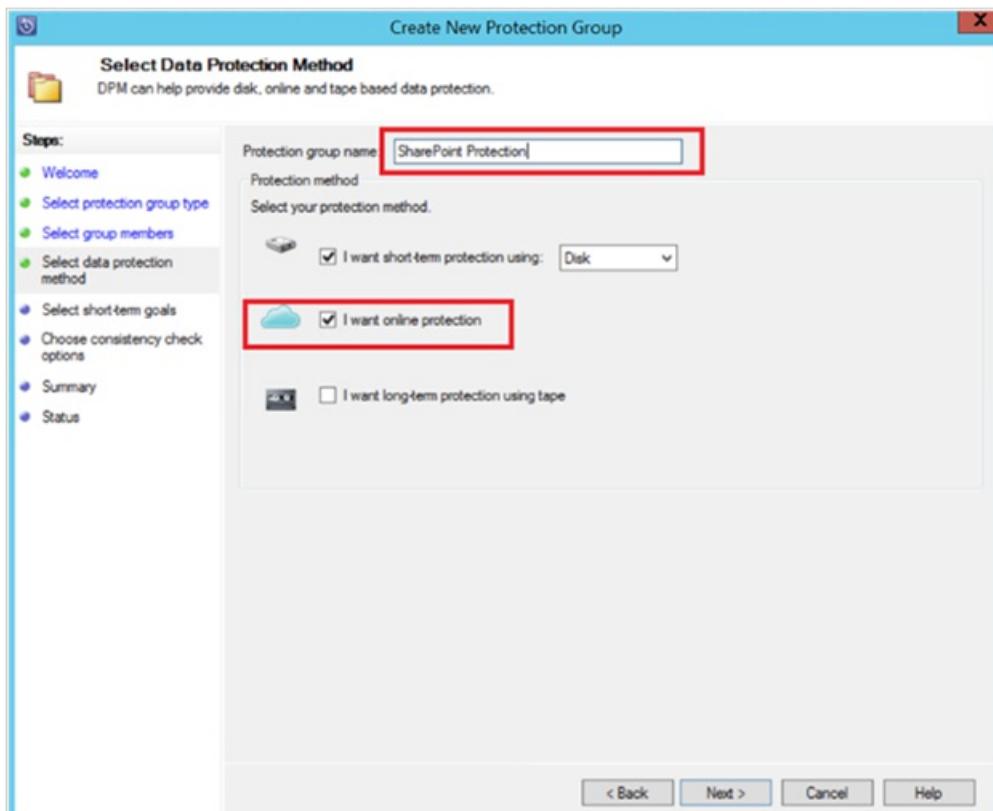
3. On the **Select Group Members** screen, select the check box for the SharePoint server you want to protect and click **Next**.



#### NOTE

With the protection agent installed, you can see the server in the wizard. MABS also shows its structure. Because you ran `ConfigureSharePoint.exe`, MABS communicates with the SharePoint VSS Writer service and its corresponding SQL Server databases and recognizes the SharePoint farm structure, the associated content databases, and any corresponding items.

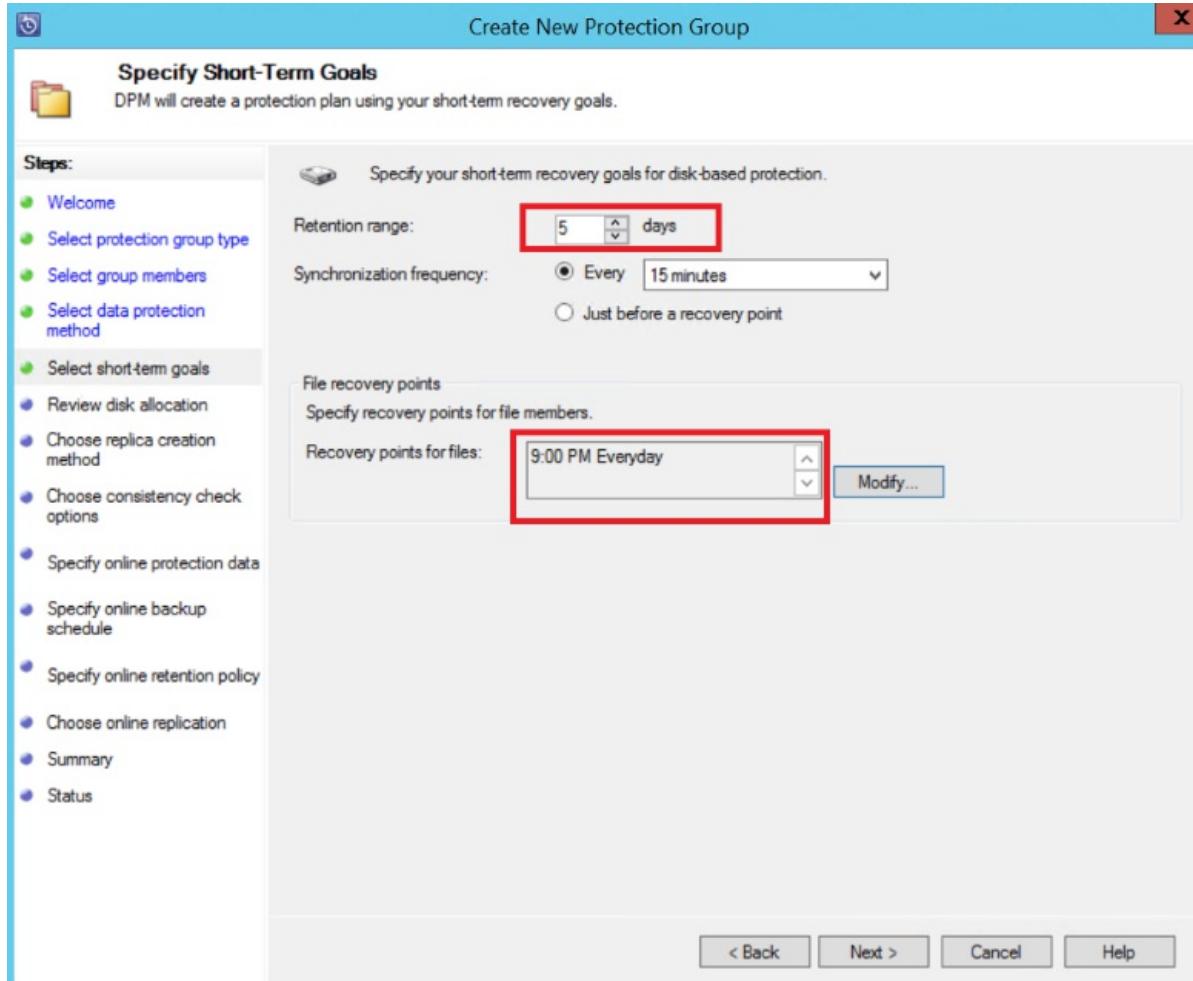
4. On the **Select Data Protection Method** page, enter the name of the **Protection Group**, and select your preferred *protection methods*. Click **Next**.



#### NOTE

The disk protection method helps to meet short recovery-time objectives.

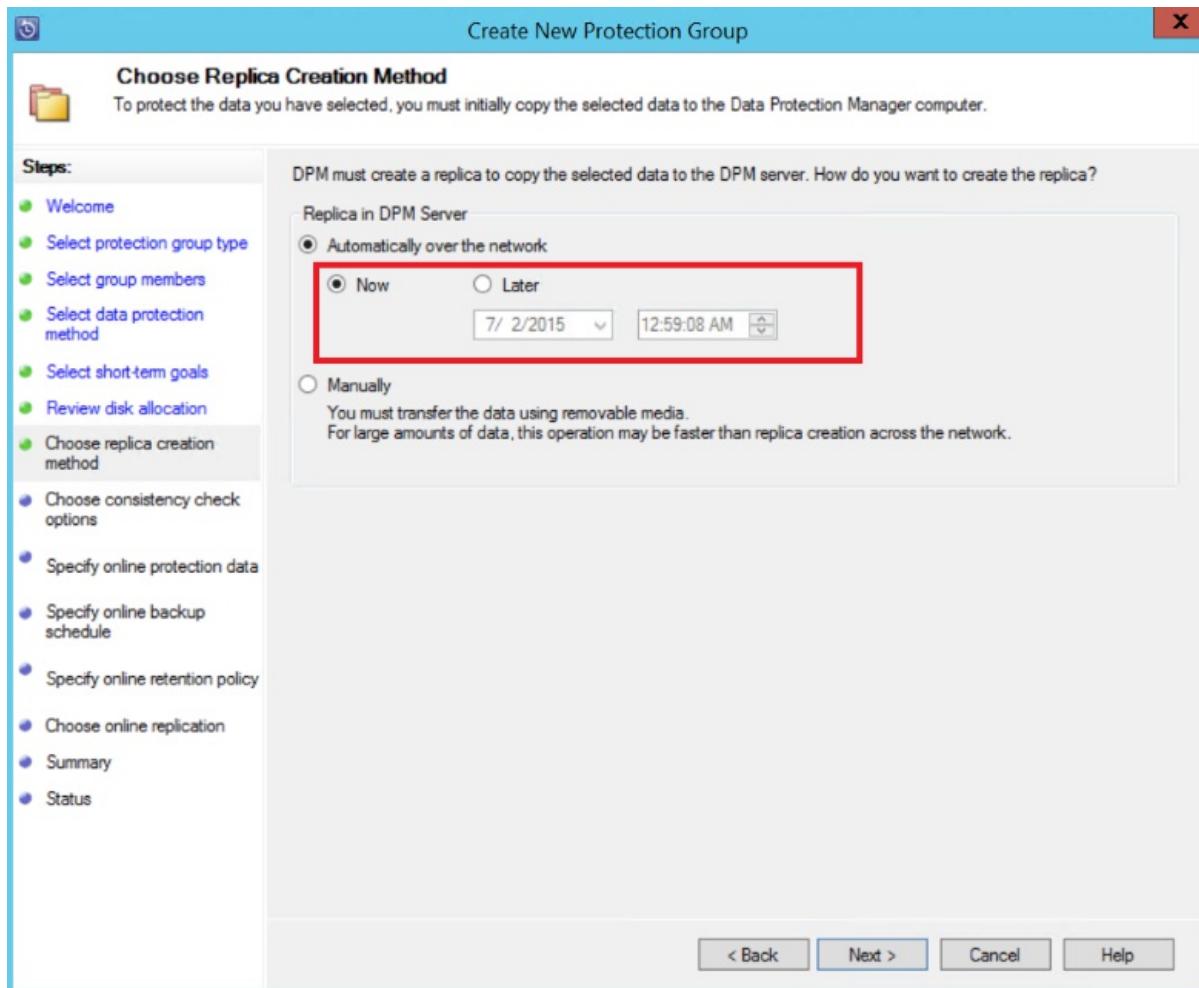
5. On the **Specify Short-Term Goals** page, select your preferred **Retention range**, and identify when you want backups to occur.



#### NOTE

Because recovery is most often required for data that's less than five days old, we selected a retention range of five days on disk and ensured that the backup happens during non-production hours, for this example.

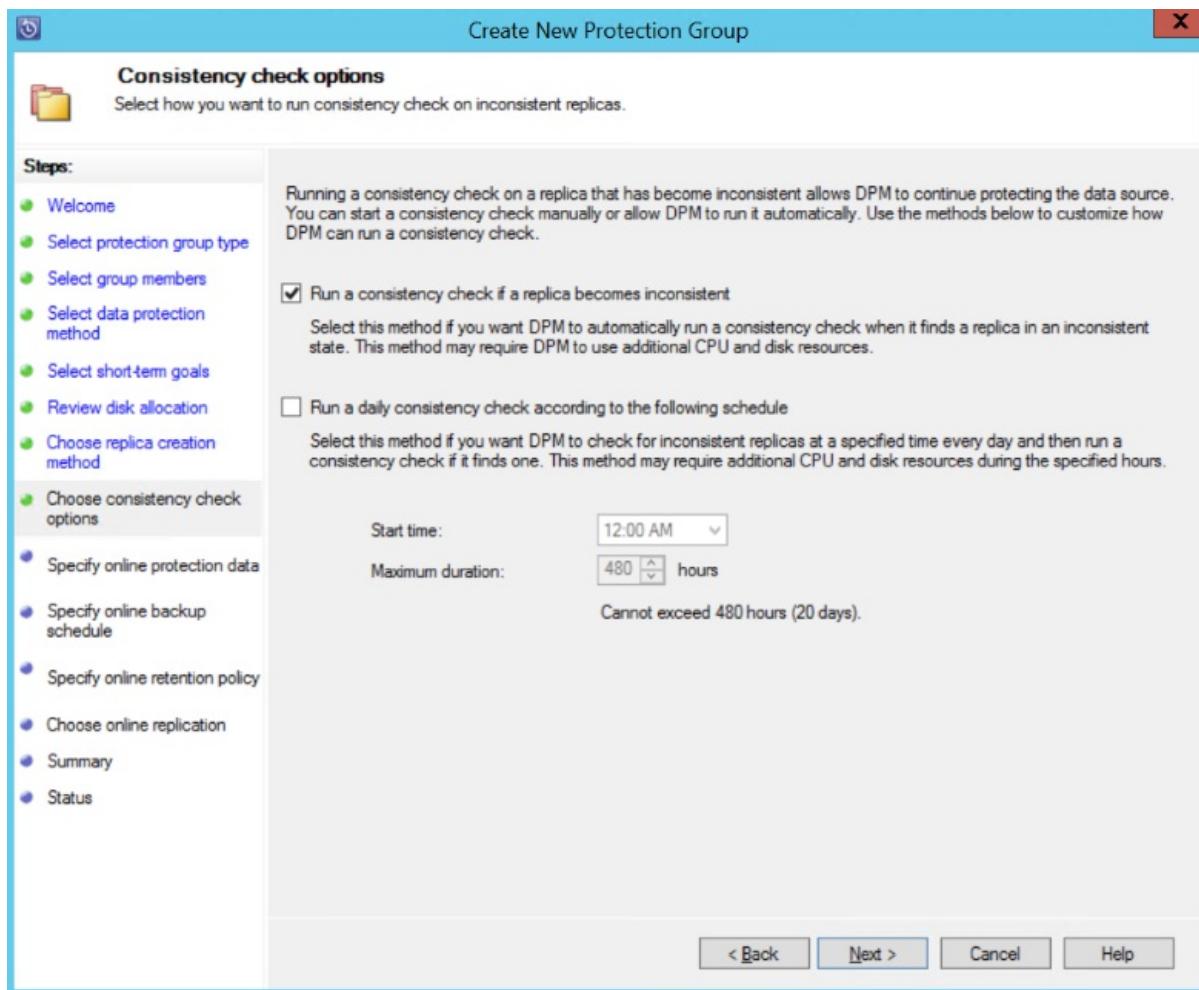
6. Review the storage pool disk space allocated for the protection group, and click then **Next**.
7. For every protection group, MABS allocates disk space to store and manage replicas. At this point, MABS must create a copy of the selected data. Select how and when you want the replica created, and then click **Next**.



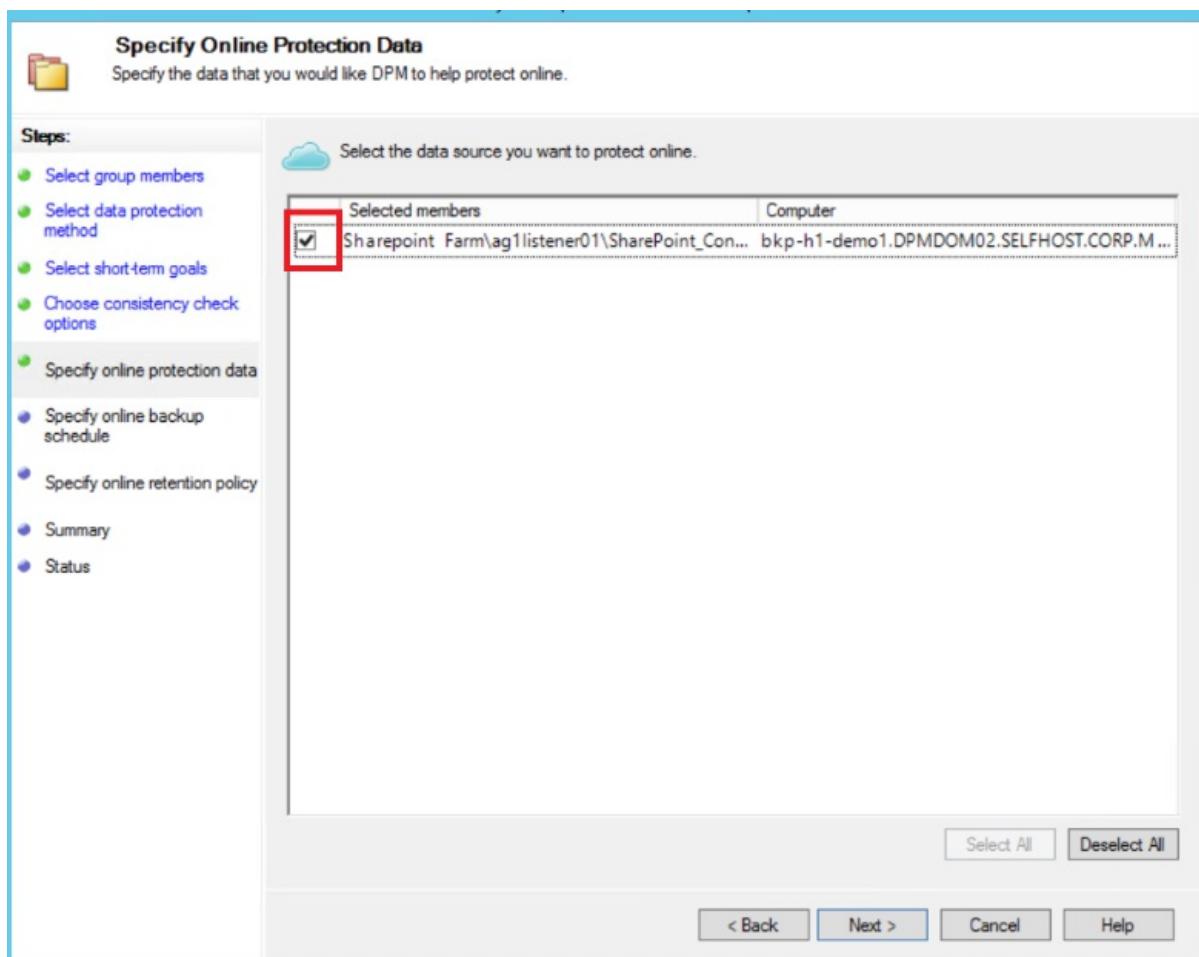
#### NOTE

To make sure that network traffic is not effected, select a time outside production hours.

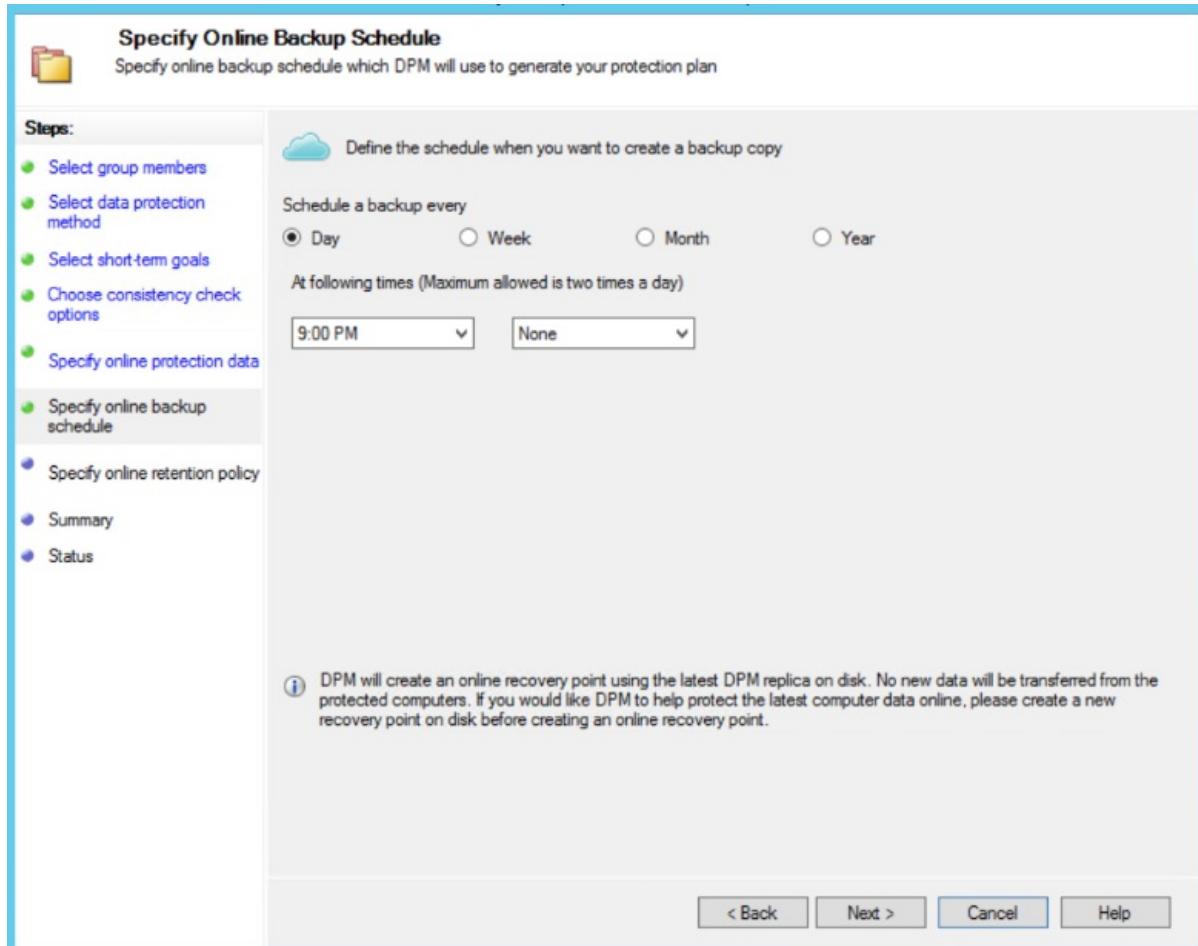
8. MABS ensures data integrity by performing consistency checks on the replica. There are two available options. You can define a schedule to run consistency checks, or DPM can run consistency checks automatically on the replica whenever it becomes inconsistent. Select your preferred option, and then click **Next**.



9. On the **Specify Online Protection Data** page, select the SharePoint farm that you want to protect, and then click **Next**.



10. On the **Specify Online Backup Schedule** page, select your preferred schedule, and then click **Next**.



**NOTE**

MABS provides a maximum of two daily backups to Azure from the then available latest disk backup point. Azure Backup can also control the amount of WAN bandwidth that can be used for backups in peak and off-peak hours by using [Azure Backup Network Throttling](#).

11. Depending on the backup schedule that you selected, on the **Specify Online Retention Policy** page, select the retention policy for daily, weekly, monthly, and yearly backup points.

**Specify Online Retention Policy**

Specify online backup schedule which DPM will use to generate your protection plan

**Steps:**

- Select group members
- Select data protection method
- Select short-term goals
- Choose consistency check options
- Specify online protection data
- **Specify online backup schedule**
- Specify online retention policy
- Summary
- Status

**Specify the retention policy which DPM will use to generate your protection plan**

Daily Retention policy  
Retain backup copies taken on At 9:00 PM for 180 Days

Weekly Retention Policy  
Retain backup copies taken on Sat At  9:00 PM for 104 Weeks

Monthly Retention Policy  
Retain backup copies taken on Last Sat At  9:00 PM for 60 Months

Day(s) 1 At  9:00 PM for 10 Years

Yearly Retention Policy  
Retain backup copies taken on Last Sat of Mar At  9:00 PM for 10 Years

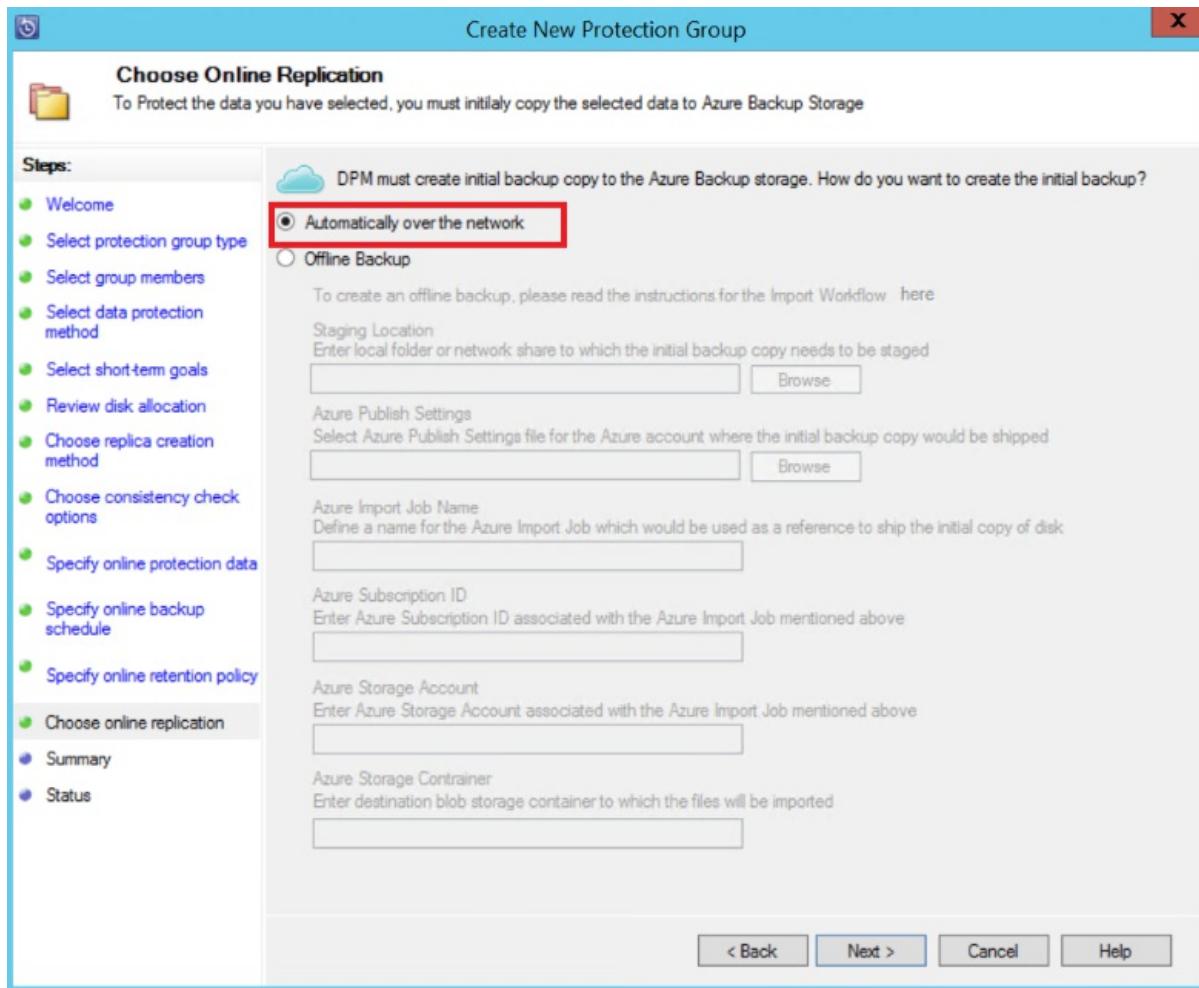
Day(s) 1 of Mar At  9:00 PM for 10 Years

**< Back** **Next >** **Cancel** **Help**

#### NOTE

MABS uses a grandfather-father-son retention scheme in which a different retention policy can be chosen for different backup points.

12. Similar to disk, an initial reference point replica needs to be created in Azure. Select your preferred option to create an initial backup copy to Azure, and then click **Next**.



13. Review your selected settings on the **Summary** page, and then click **Create Group**. You will see a success message after the protection group has been created.

**Create New Protection Group**

**Summary**  
DPM is ready to create the SharePoint Protection protection group.

**Steps:**

- Welcome
- Select protection group type
- Select group members
- Select data protection method
- Select short-term goals
- Review disk allocation
- Choose replica creation method
- Choose consistency check options
- Specify online protection data
- Specify online backup schedule
- Specify online retention policy
- Choose online replication
- Summary
- Status

**Protection group members:**  
Sharepoint Farm\ag1\listener01\SharePoint\_Config

**Protection group settings:**

| Setting                 | Details                              |
|-------------------------|--------------------------------------|
| Online backup frequency | Daily                                |
| Online backup schedule  | 9:00 PM Everyday                     |
| Online retention range  | 180 day(s)(9:00 PM Everyday)         |
|                         | 104 week(s)(9:00 PM Sat)             |
|                         | 60 month(s)(Last Sat, 9:00 PM)       |
|                         | 10 year(s)(Last Sat of Mar, 9:00 PM) |
| Online Replica Creation | Network                              |

**Note:** You can [optimize performance](#) of this protection group now or you can do it later from the actions pane.

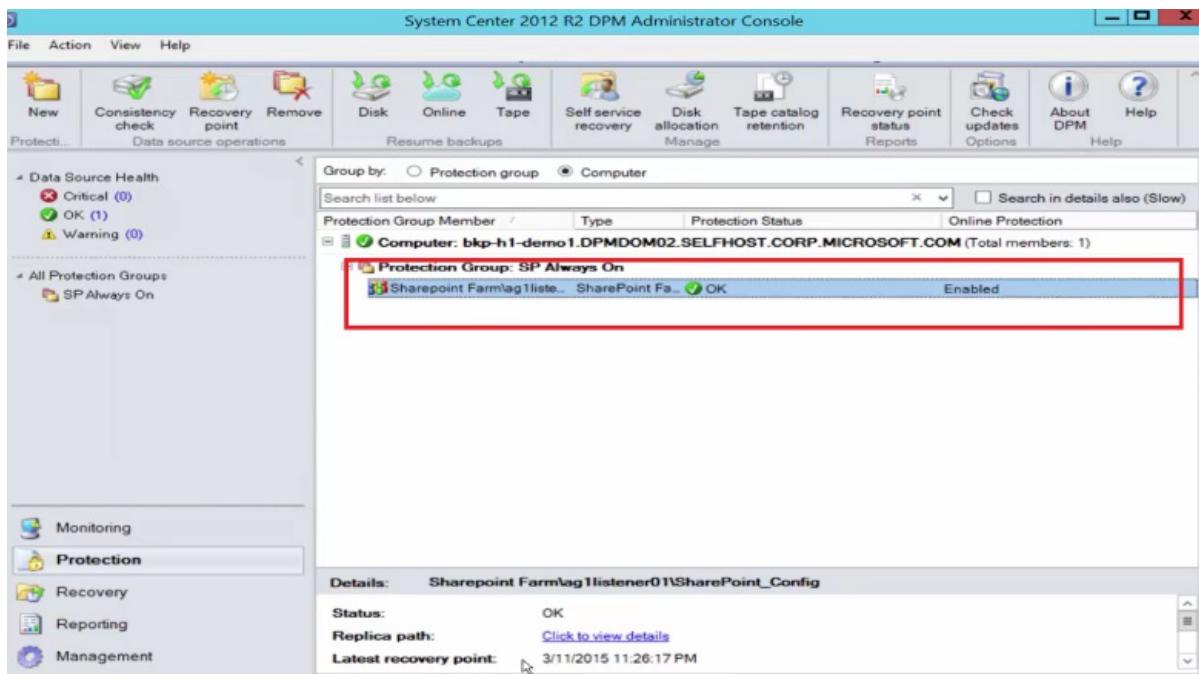
[Back](#) [Create Group](#) [Cancel](#) [Help](#)

## Restore a SharePoint item from disk by using MABS

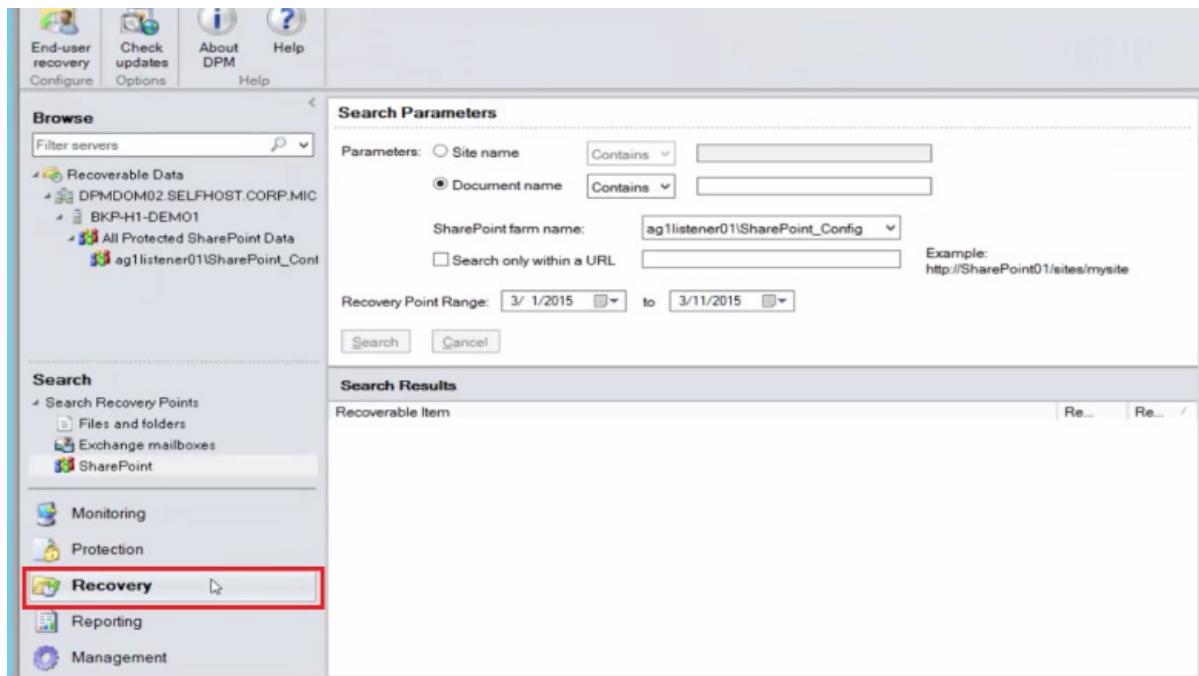
In the following example, the *Recovering SharePoint item* has been accidentally deleted and needs to be recovered.

The screenshot shows a SharePoint site collection home page. The URL in the address bar is [http://bkp-h1-demo1:8080/sites/\\_vti\\_bin/Top-Level Site Successfully Created.aspx](http://bkp-h1-demo1:8080/sites/_vti_bin/Top-Level Site Successfully Created.aspx). The page title is "site1 - Home". The left navigation bar shows "site1" with a red box around it, indicating it's selected. Below the navigation, there are several cards: "Share your site.", "Working on a deadline?", "Add lists, libraries, and other apps.", "What's your style?", and "Your site. Your brand.". In the bottom left corner, there's a "Documents" section with a "new document or drag files here" input field. A file named "Recovering SharePoint item" is listed in this section, also with a red box around it, indicating it's the item being recovered.

1. Open the **DPM Administrator Console**. All SharePoint farms that are protected by DPM are shown in the **Protection** tab.



2. To begin to recover the item, select the **Recovery** tab.



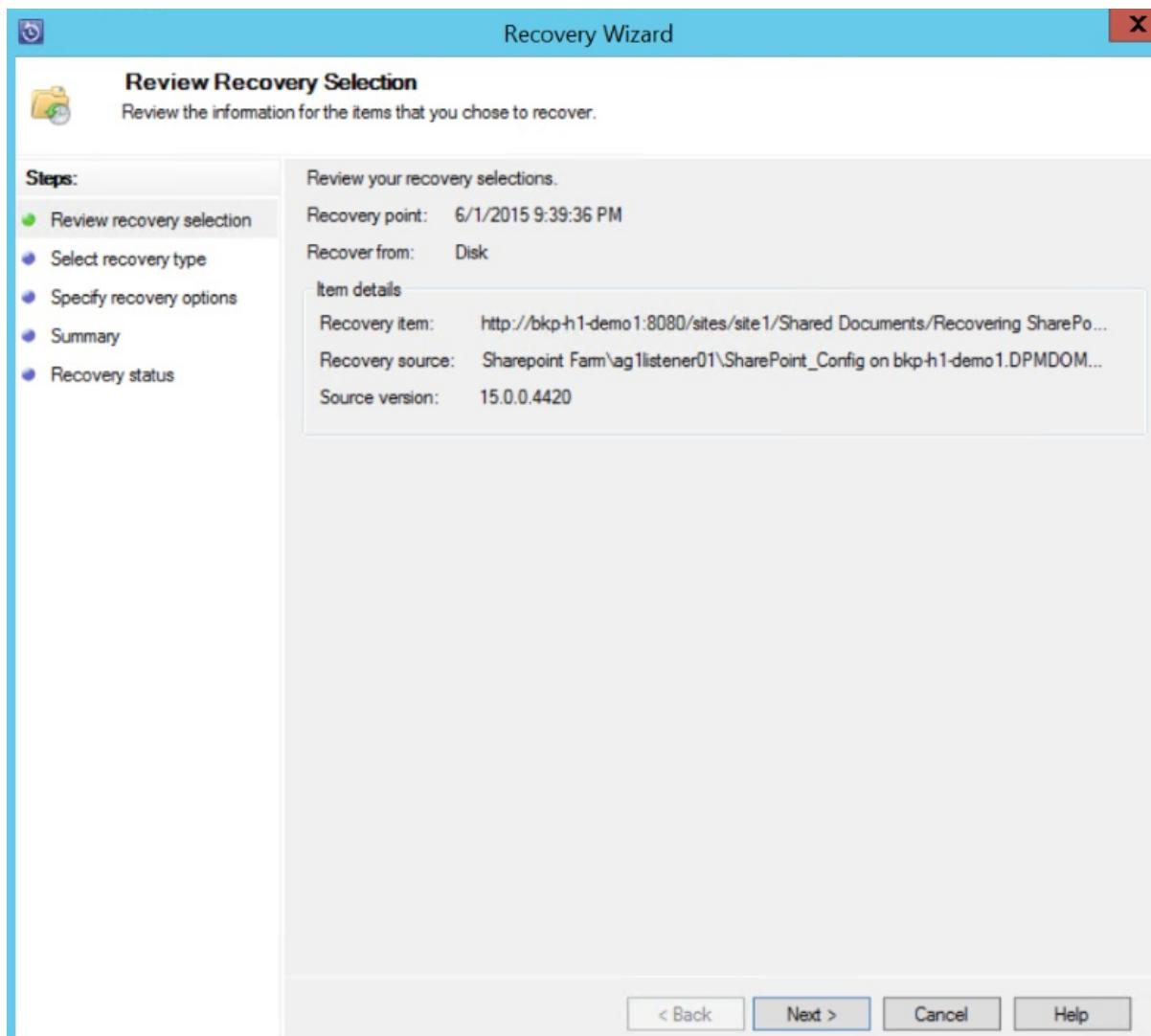
3. You can search SharePoint for *Recovering SharePoint item* by using a wildcard-based search within a recovery point range.

The screenshot shows the DPM Recovery interface. In the 'Search Parameters' section, the 'Document name' field is set to 'Contains' and contains 'Recovering\*'. The 'SharePoint farm name' dropdown is set to 'ag1listener01\SharePoint\_Config'. The 'Recovery Point Range' is set from '3/1/2015' to '3/11/2015'. The 'Search' button is highlighted with a red box. The 'Search Results' section shows a list of recovery points for the SharePoint farm. One item in the list, 'http://bkp-h1-demo1:8080/sites/site1/Shared Documents/Recovering SharePoint item.bdt', has a 'Recover...' action button next to it, which is also highlighted with a red box.

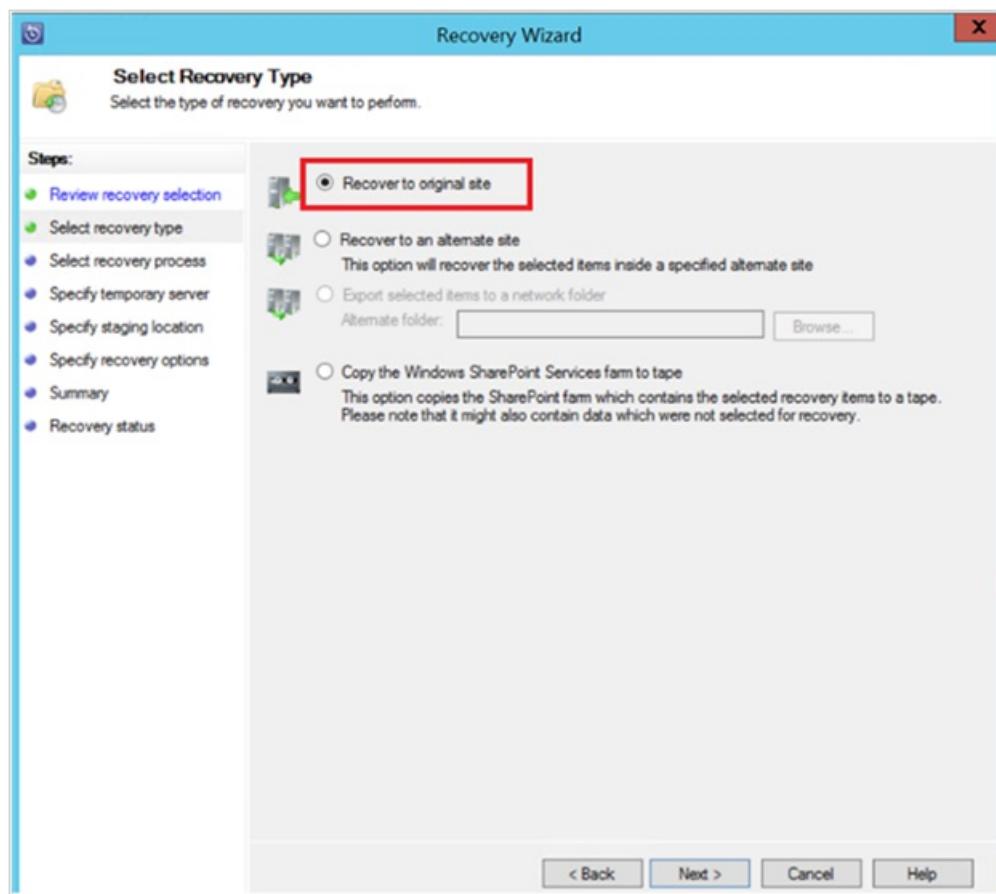
4. Select the appropriate recovery point from the search results, right-click the item, and then select **Recover**.
5. You can also browse through various recovery points and select a database or item to recover. Select **Date > Recovery time**, and then select the correct **Database > SharePoint farm > Recovery point > Item**.

The screenshot shows the DPM Recovery interface. The 'Recovery points for: ag1listener01\SharePoint\_Config' section displays a calendar for February 2015. The date 'February 09 2015' is selected. The 'Recovery time' is set to '8:00 PM (U)'. The 'Recover from' option is set to 'Disk'. The 'Path: All Protected SharePoint Data' section shows a tree view with 'SharePoint\_AdminContent\_17d8dd99-b505-4b89-a4f3-0c31bd427966' and 'WSS\_Content1' selected, both highlighted with red boxes.

6. Right-click the item, and then select **Recover** to open the **Recovery Wizard**. Click **Next**.



7. Select the type of recovery that you want to perform, and then click **Next**.

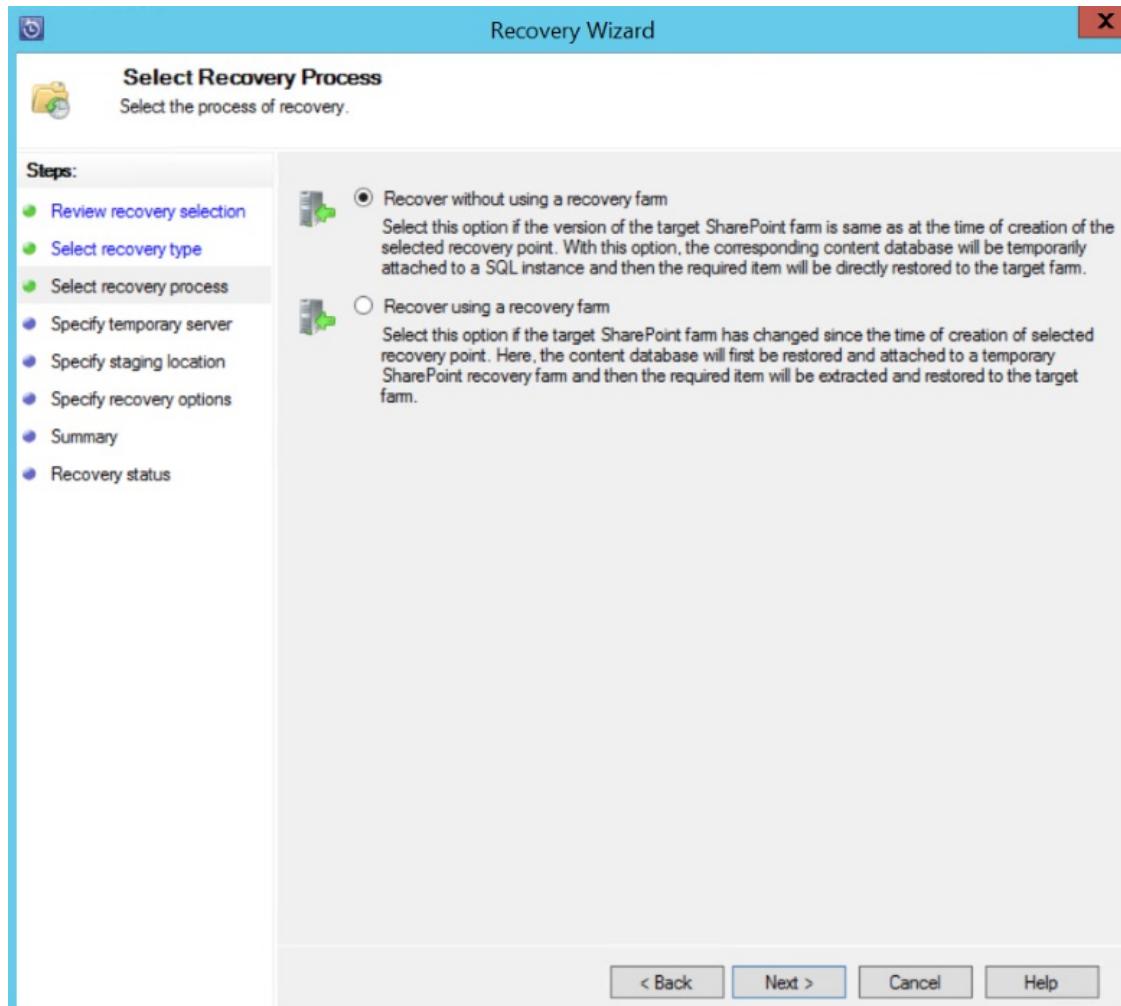


**NOTE**

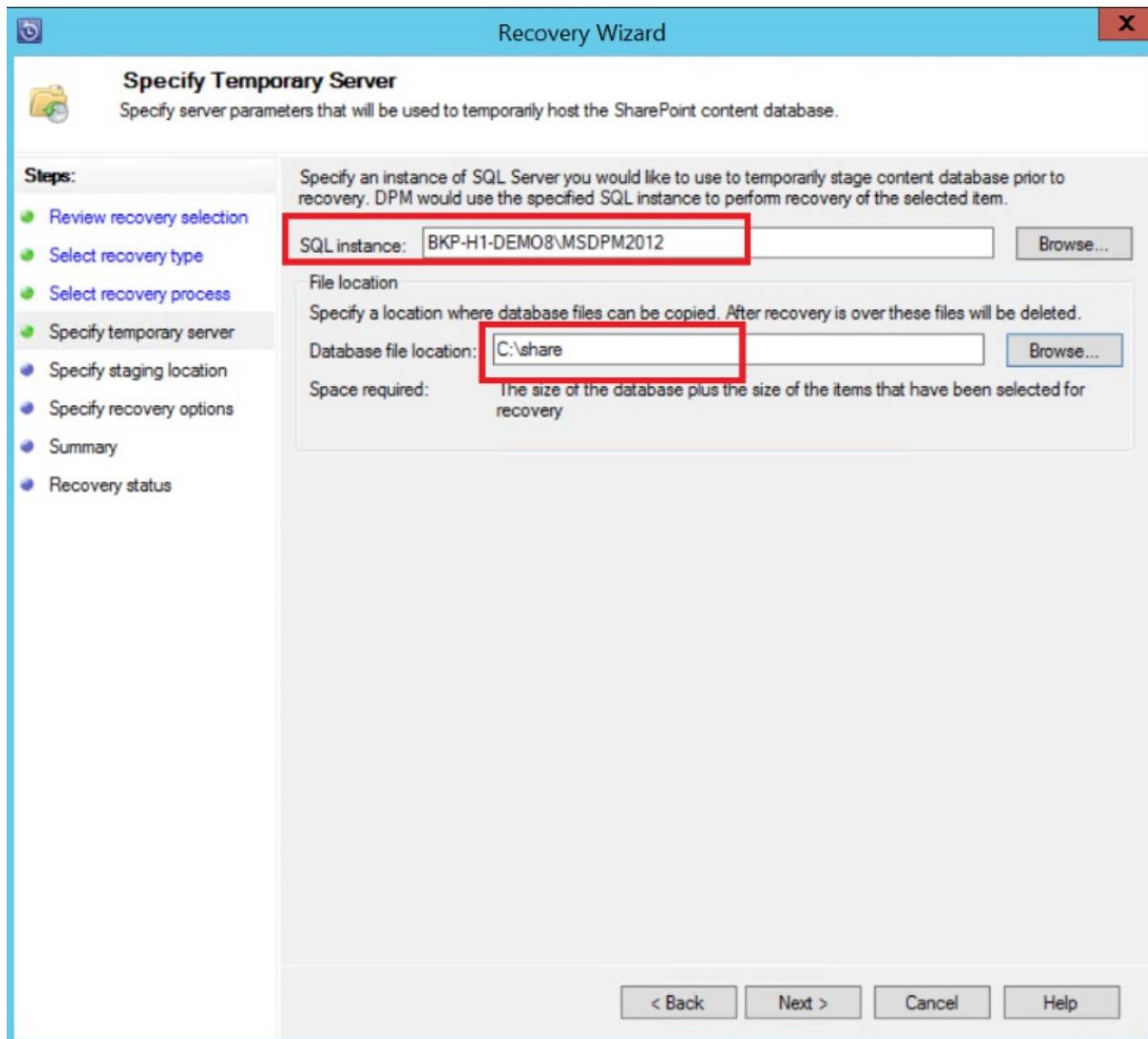
The selection of **Recover to original** in the example recovers the item to the original SharePoint site.

8. Select the **Recovery Process** that you want to use.

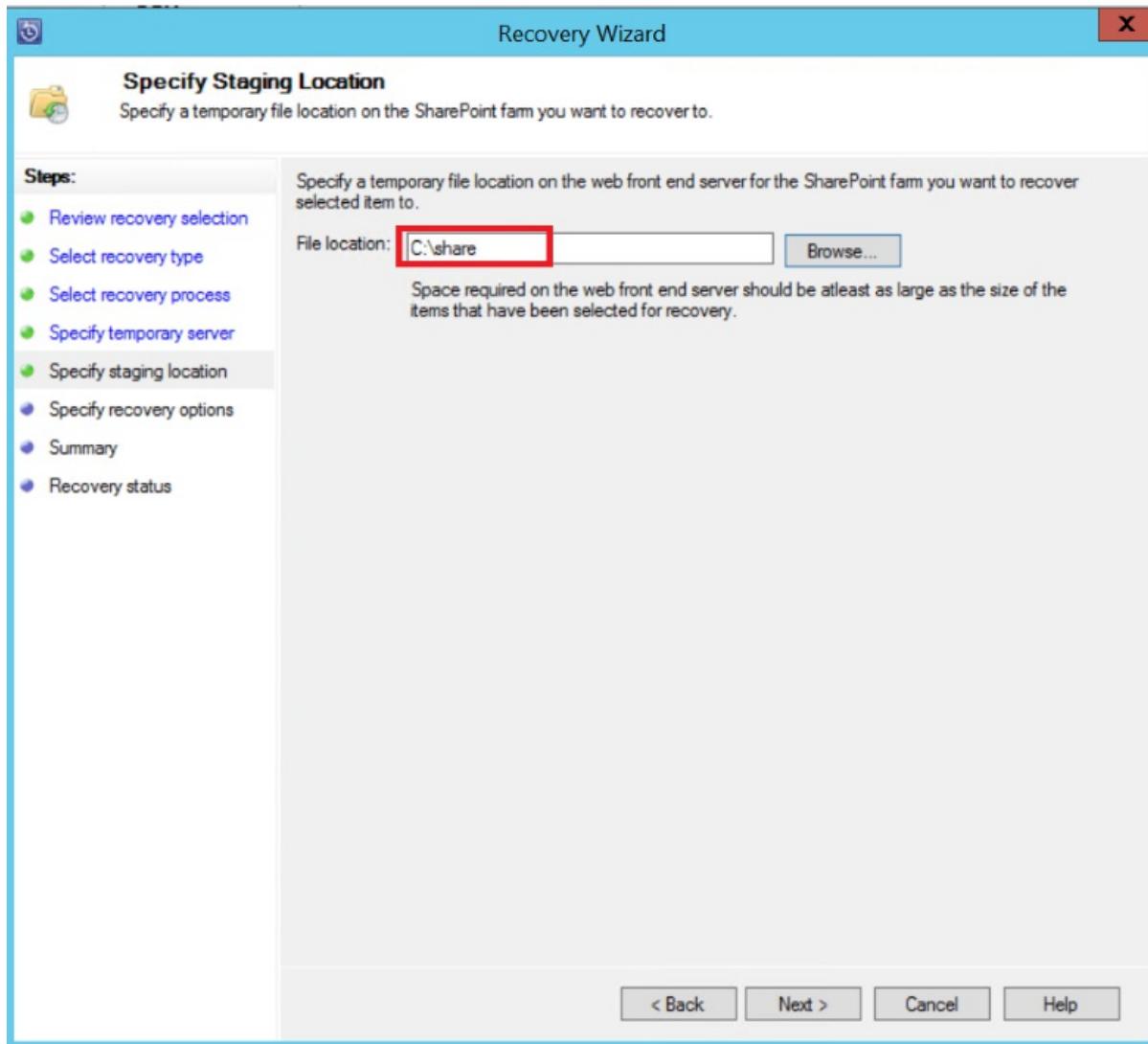
- Select **Recover without using a recovery farm** if the SharePoint farm has not changed and is the same as the recovery point that is being restored.
- Select **Recover using a recovery farm** if the SharePoint farm has changed since the recovery point was created.



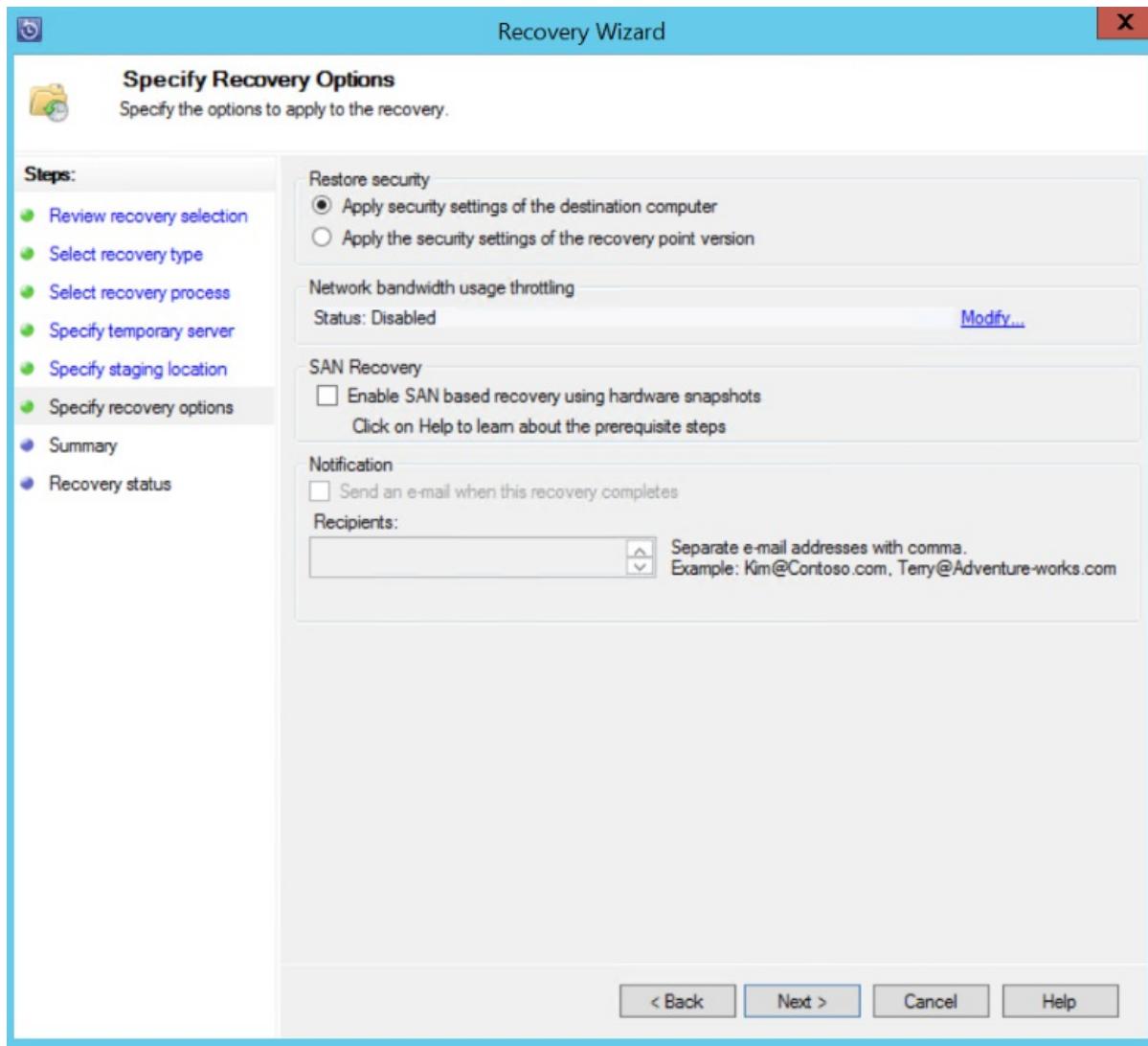
9. Provide a staging SQL Server instance location to recover the database temporarily, and provide a staging file share on MABS and the server that's running SharePoint to recover the item.



MABS attaches the content database that is hosting the SharePoint item to the temporary SQL Server instance. From the content database, it recovers the item and puts it on the staging file location on MABS. The recovered item that's on the staging location now needs to be exported to the staging location on the SharePoint farm.



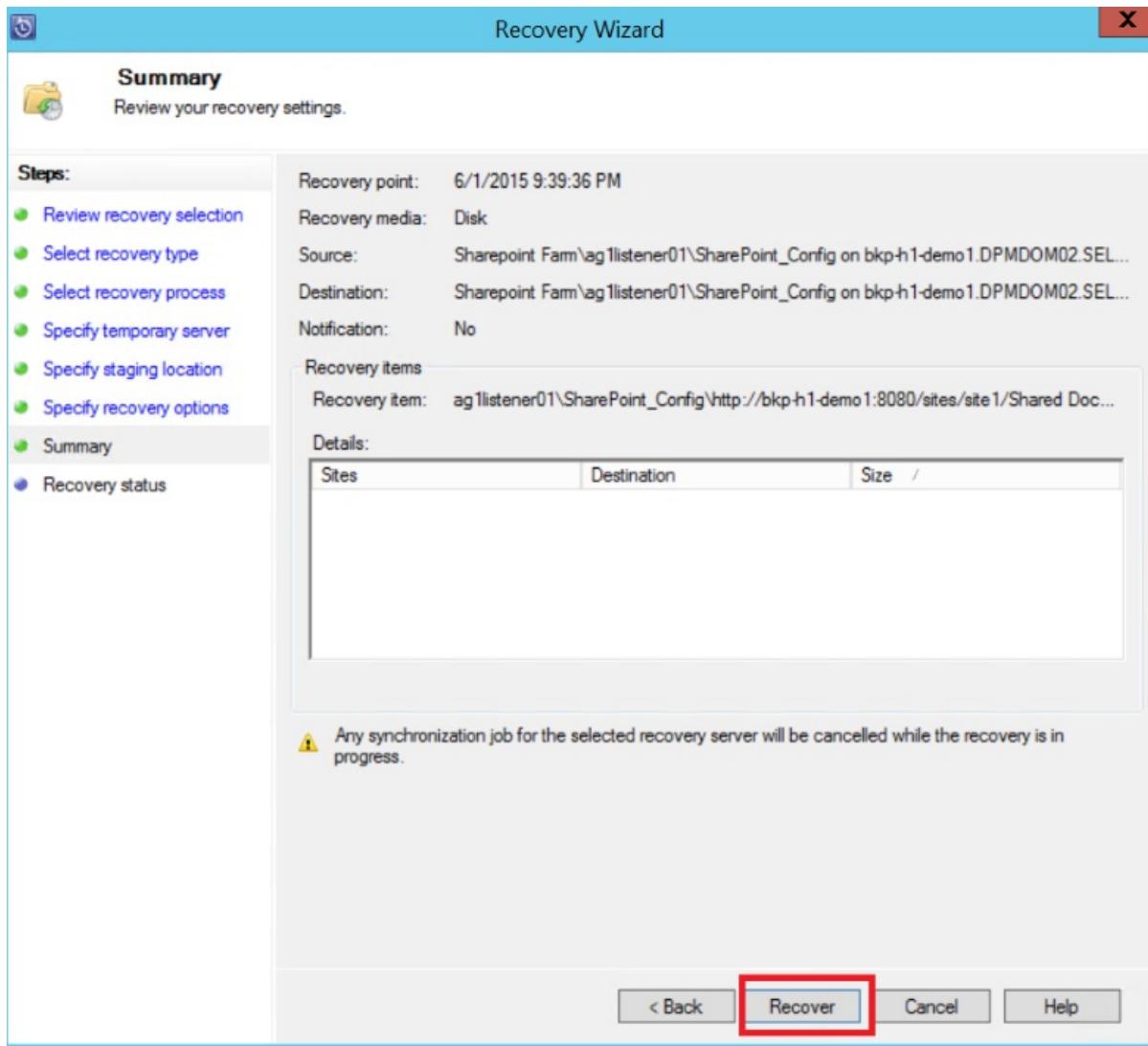
10. Select **Specify recovery options**, and apply security settings to the SharePoint farm or apply the security settings of the recovery point. Click **Next**.



#### NOTE

You can choose to throttle the network bandwidth usage. This minimizes impact to the production server during production hours.

11. Review the summary information, and then click **Recover** to begin recovery of the file.



12. Now select the **Monitoring** tab in the **MABS Administrator Console** to view the **Status** of the recovery.

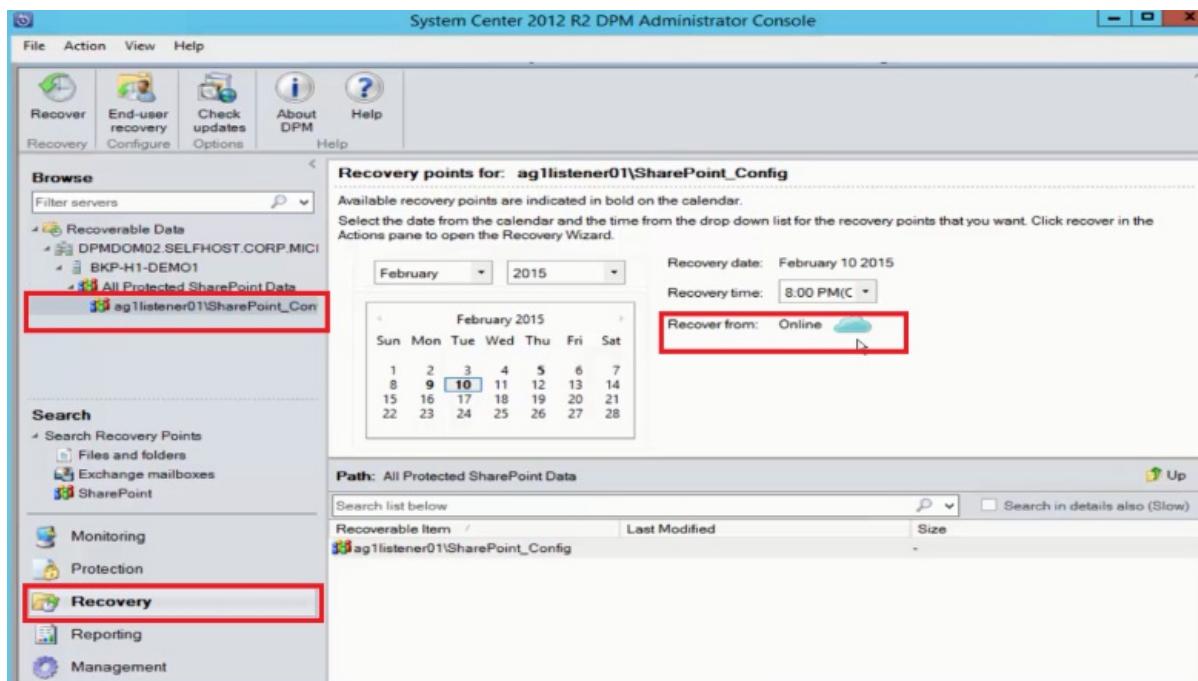
| Source                            | Computer           | Protection Gr...   | Type                              | Start Time            | End Time             | Size      |
|-----------------------------------|--------------------|--------------------|-----------------------------------|-----------------------|----------------------|-----------|
| bkp-h1-demo1.dp...                | -                  | -                  | SharePoint export and import task | 1/23/2015 12:00:00 AM | -                    | 0 MB      |
| <b>Completed (Total jobs: 82)</b> |                    |                    |                                   |                       |                      |           |
| -                                 | bkp-h1-demo8.dp... | -                  | SharePoint export and import task | 2/9/2015 11:24:45 PM  | 2/9/2015 11:24:45 PM | 0 MB      |
| -                                 | bkp-h1-demo1.dp... | -                  | SharePoint export and import task | 2/9/2015 11:24:42 PM  | 2/9/2015 11:24:45 PM | 195.81 MB |
| -                                 | ag1WSS...          | bkp-h1-demo8.dp... | Disk recovery                     | 2/9/2015 11:24:42 PM  | 2/9/2015 11:24:45 PM | 0 MB      |
| -                                 | bkp-h1-demo8.dp... | -                  | SharePoint export and import task | 2/9/2015 10:00:00 AM  | 2/9/2015 10:00:03 AM | 0 MB      |
| -                                 | bkp-h1-demo1.dp... | -                  | SharePoint export and import task | 2/9/2015 10:00:00 AM  | 2/9/2015 10:00:24 AM | 0 MB      |
| -                                 | ag1WSS...          | bkp-h1-demo8.dp... | Disk recovery                     | 2/9/2015 10:00:00 AM  | 2/9/2015 10:00:05 AM | 195.81 MB |
| -                                 | bkp-h1-demo8.dp... | -                  | SharePoint export and import task | 2/9/2015 10:00:00 AM  | 2/9/2015 10:00:03 AM | 0 MB      |
| -                                 | bkp-h1-demo8.dp... | -                  | SharePoint export and import task | 2/9/2015 9:38:00 AM   | 2/9/2015 9:38:03 AM  | 0 MB      |

#### NOTE

The file is now restored. You can refresh the SharePoint site to check the restored file.

# Restore a SharePoint database from Azure by using DPM

1. To recover a SharePoint content database, browse through various recovery points (as shown previously), and select the recovery point that you want to restore.

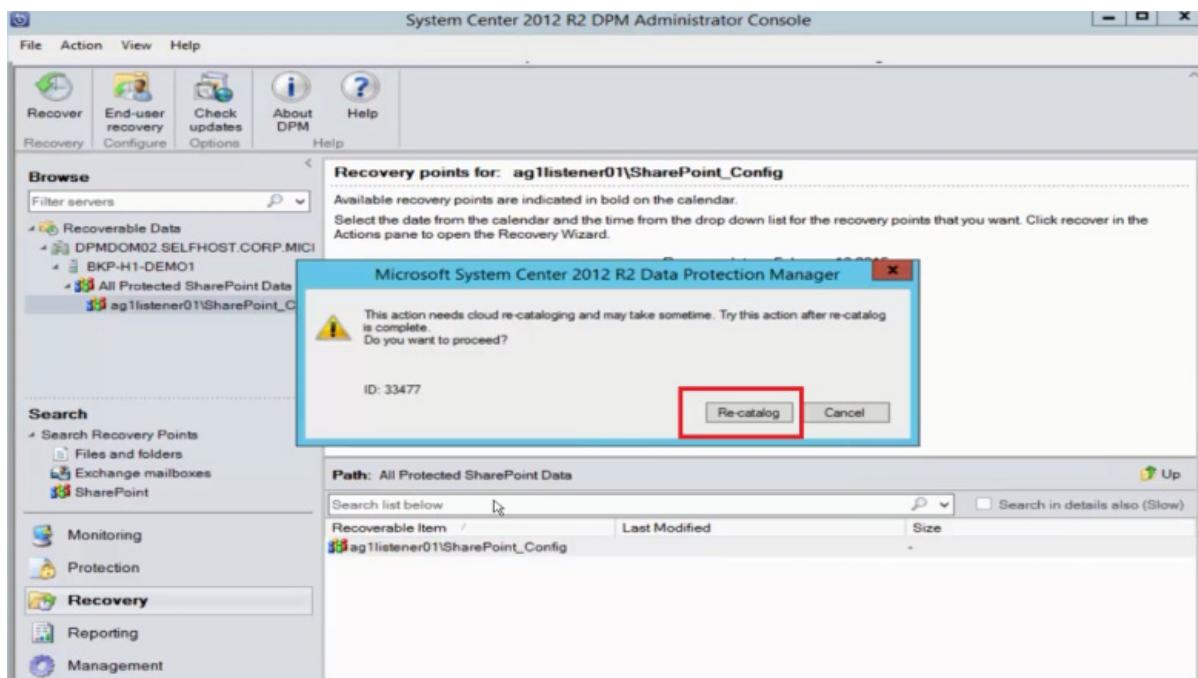


2. Double-click the SharePoint recovery point to show the available SharePoint catalog information.

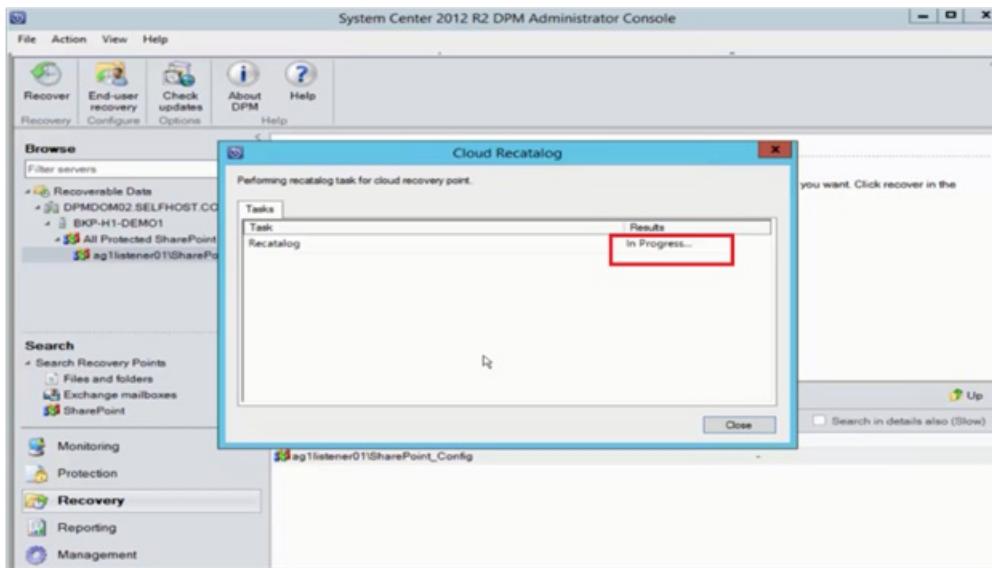
## NOTE

Because the SharePoint farm is protected for long-term retention in Azure, no catalog information (metadata) is available on MABS. As a result, whenever a point-in-time SharePoint content database needs to be recovered, you need to catalog the SharePoint farm again.

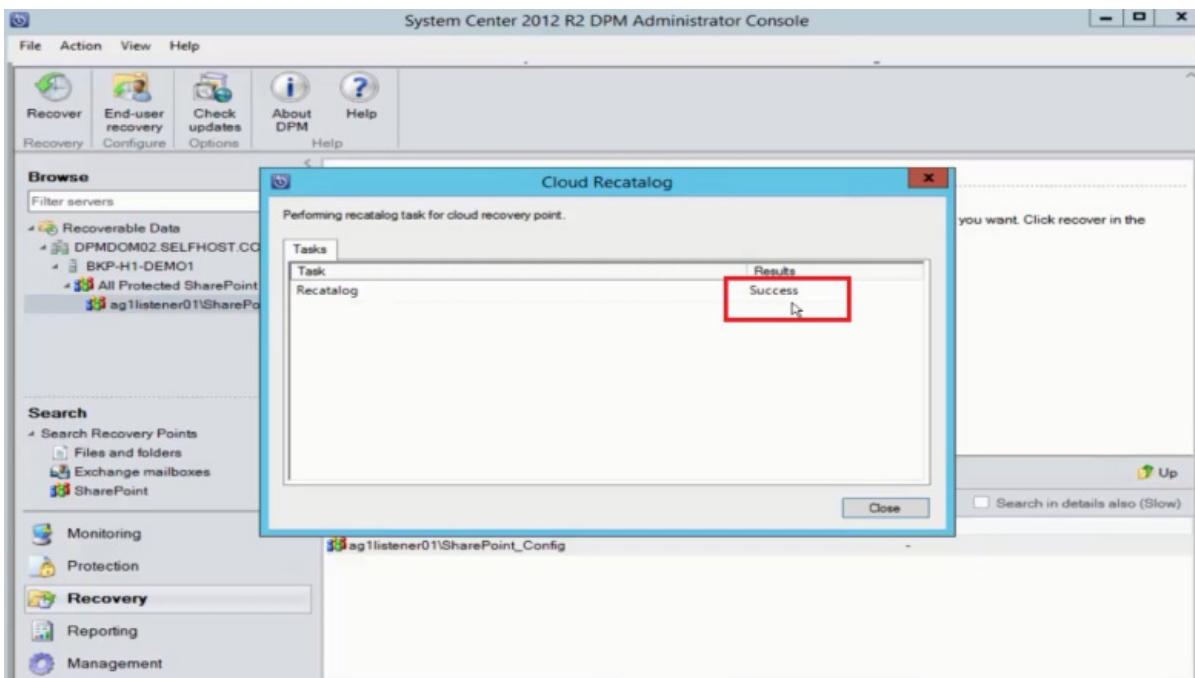
3. Click **Re-catalog**.



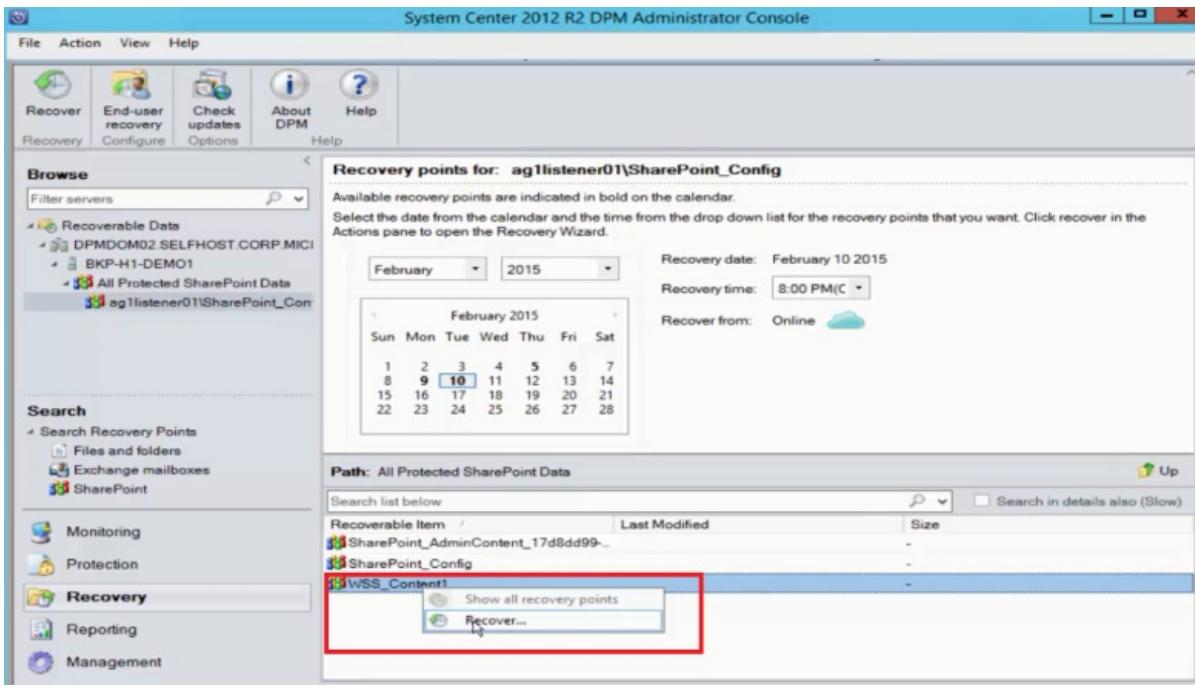
The **Cloud Recatalog** status window opens.



After cataloging is finished, the status changes to *Success*. Click **Close**.



4. Click the SharePoint object shown in the MABS **Recovery** tab to get the content database structure. Right-click the item, and then click **Recover**.



- At this point, follow the recovery steps earlier in this article to recover a SharePoint content database from disk.

## FAQs

**Q:** Can I recover a SharePoint item to the original location if SharePoint is configured by using SQL AlwaysOn (with protection on disk)?

**A:** Yes, the item can be recovered to the original SharePoint site.

**Q:** Can I recover a SharePoint database to the original location if SharePoint is configured by using SQL AlwaysOn?

**A:** Because SharePoint databases are configured in SQL AlwaysOn, they cannot be modified unless the availability group is removed. As a result, MABS cannot restore a database to the original location. You can recover a SQL Server database to another SQL Server instance.

## Next steps

See the [Backup files and application](#) article. See the [Backup SQL Server on Azure Stack](#) article.

# Back up SQL Server on Azure Stack

11/18/2019 • 5 minutes to read • [Edit Online](#)

Use this article to configure Microsoft Azure Backup Server (MABS) to protect SQL Server databases on Azure Stack.

The management of SQL Server database backup to Azure and recovery from Azure involves three steps:

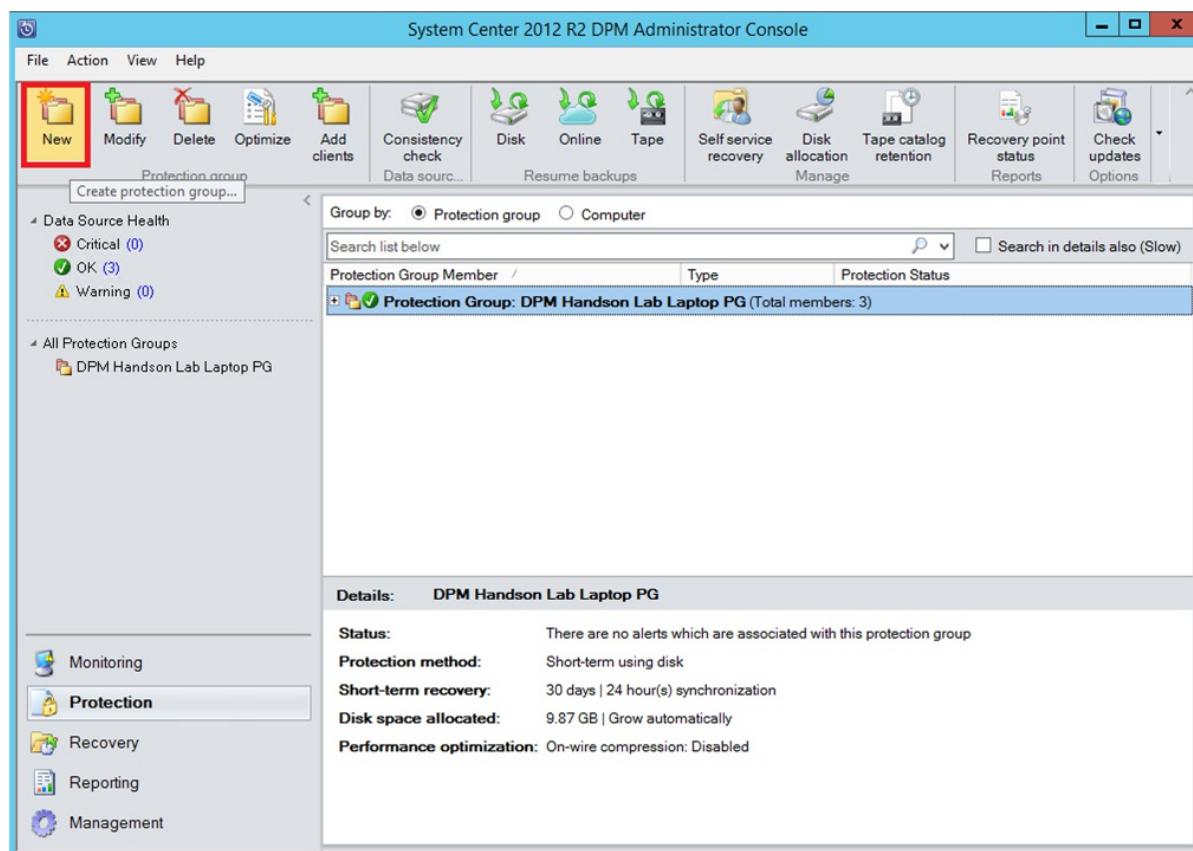
1. Create a backup policy to protect SQL Server databases
2. Create on-demand backup copies
3. Recover the database from Disks, and from Azure

## Before you start

[Install and prepare Azure Backup Server.](#)

## Create a backup policy to protect SQL Server databases to Azure

1. On the Azure Backup Server UI, click the **Protection** workspace.
2. On the tool ribbon, click **New** to create a new protection group.

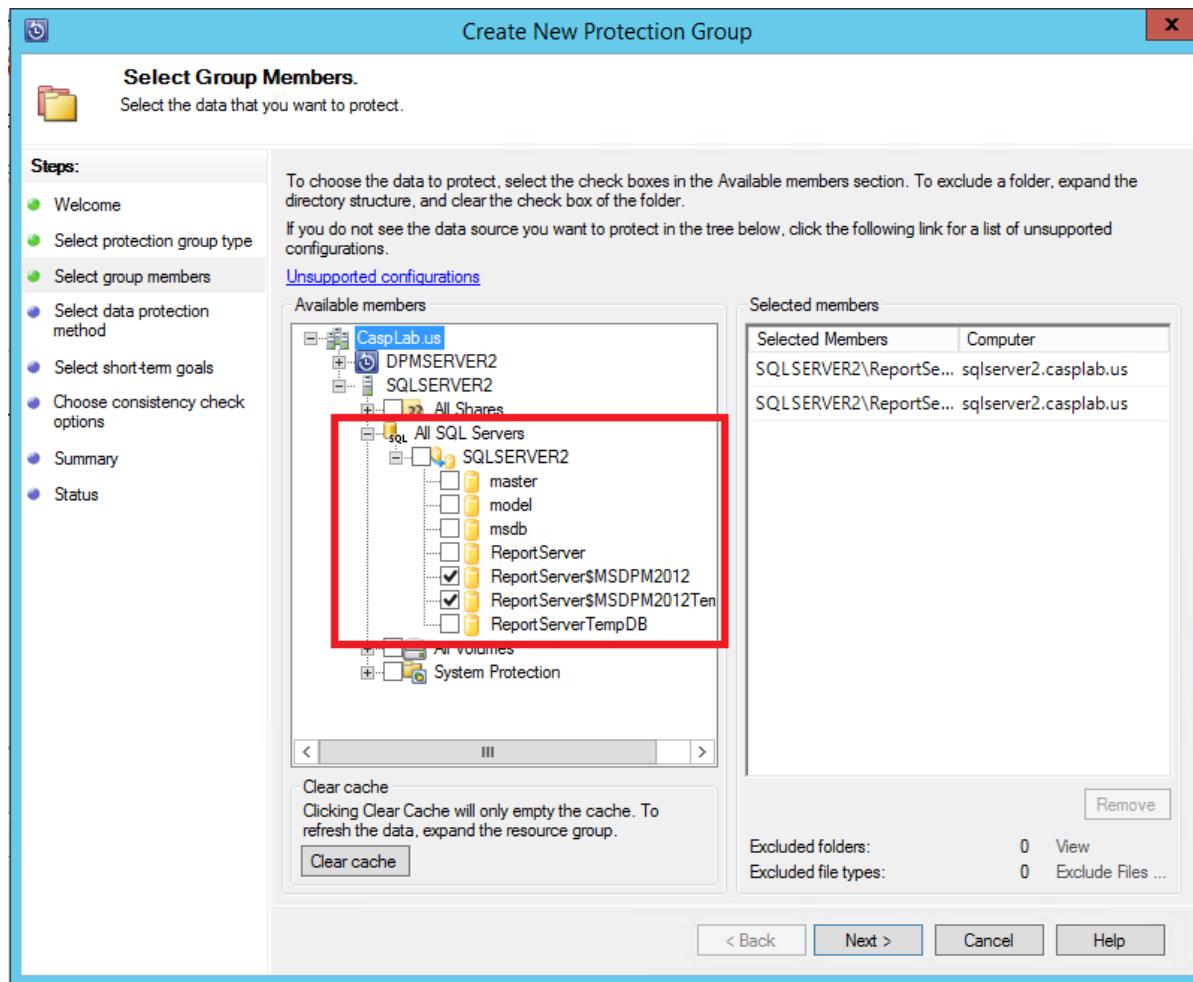


Azure Backup Server starts the Protection Group wizard, which leads you through creating a **Protection Group**. Click **Next**.

3. In the **Select Protection Group Type** screen, select **Servers**.

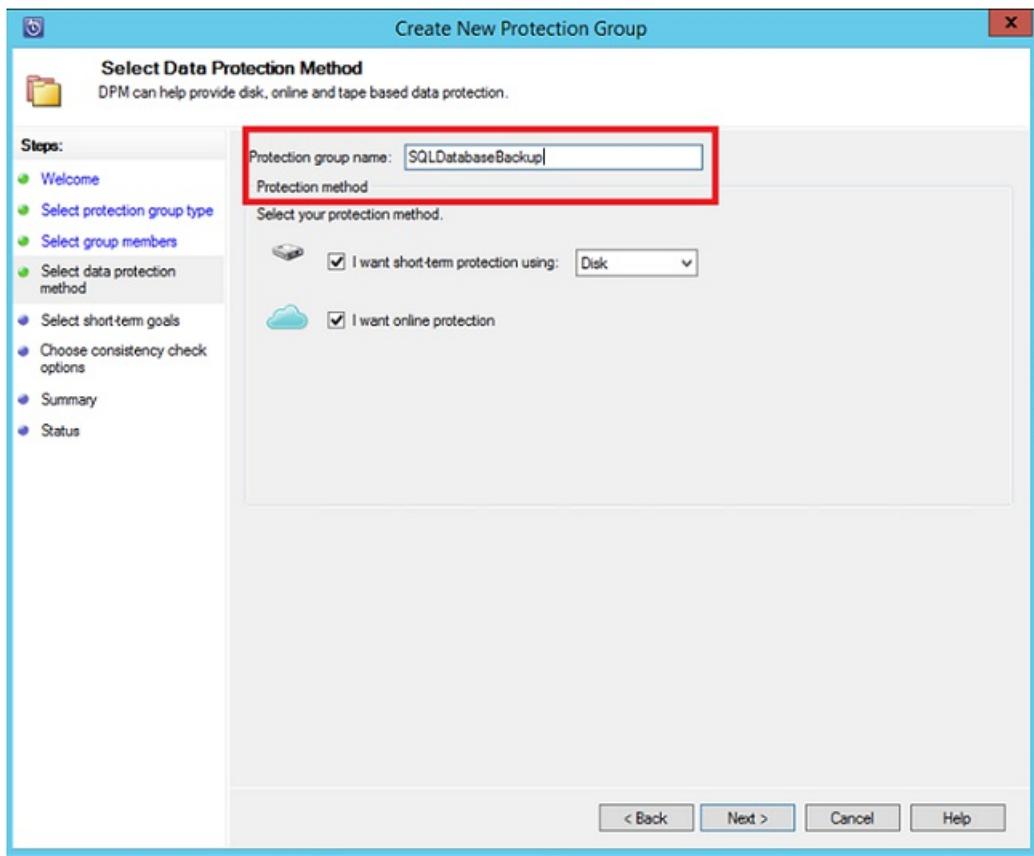


4. In the **Select Group Members** screen, the Available members list displays the various data sources. Click + to expand a folder and reveal the subfolders. Click the checkbox to select an item.



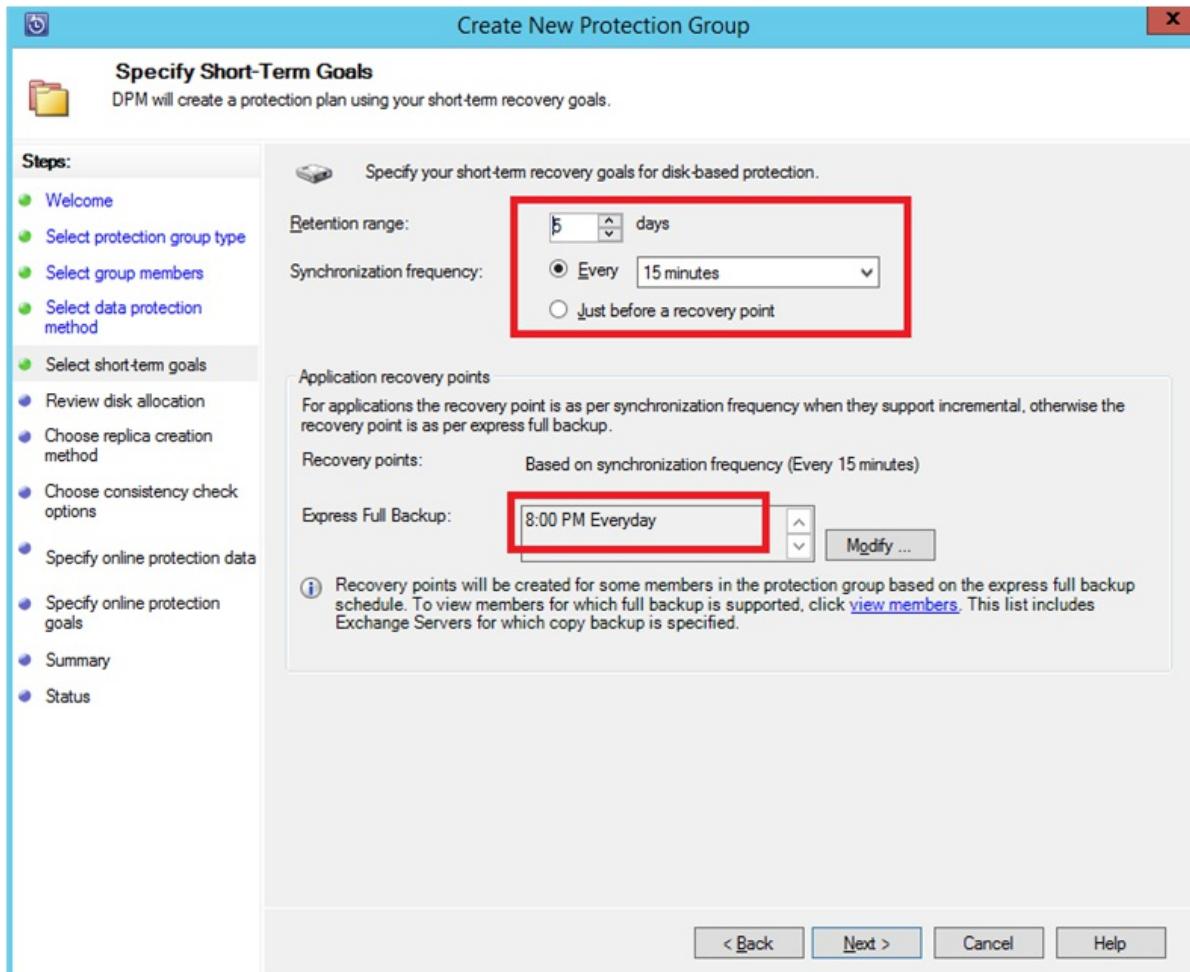
All selected items appear in the Selected members list. After selecting the servers or databases you want to protect, click **Next**.

5. In the **Select Data Protection Method** screen, provide a name for the protection group and select the **I want online Protection** checkbox.



6. In the **Specify Short-Term Goals** screen, include the necessary inputs to create backup points to disk, and click **Next**.

In the example, **Retention range** is **5 days**, **Synchronization frequency** is once every **15 minutes**, which is the backup frequency. **Express Full Backup** is set to **8:00 P.M.**



#### NOTE

In the example shown, at 8:00 PM every day a backup point is created by transferring the modified data from the previous day's 8:00 PM backup point. This process is called **Express Full Backup**. Transaction logs are synchronized every 15 minutes. If you need to recover the database at 9:00 PM, the point is created from the logs from the last express full backup point (8PM in this case).

7. On the **Review disk allocation** screen, verify the overall storage space available, and the potential disk space. Click **Next**.
8. In the **Choose Replica Creation Method**, choose how to create your first recovery point. You can transfer the initial backup manually (off network) to avoid bandwidth congestion or over the network. If you choose to wait to transfer the first backup, you can specify the time for the initial transfer. Click **Next**.

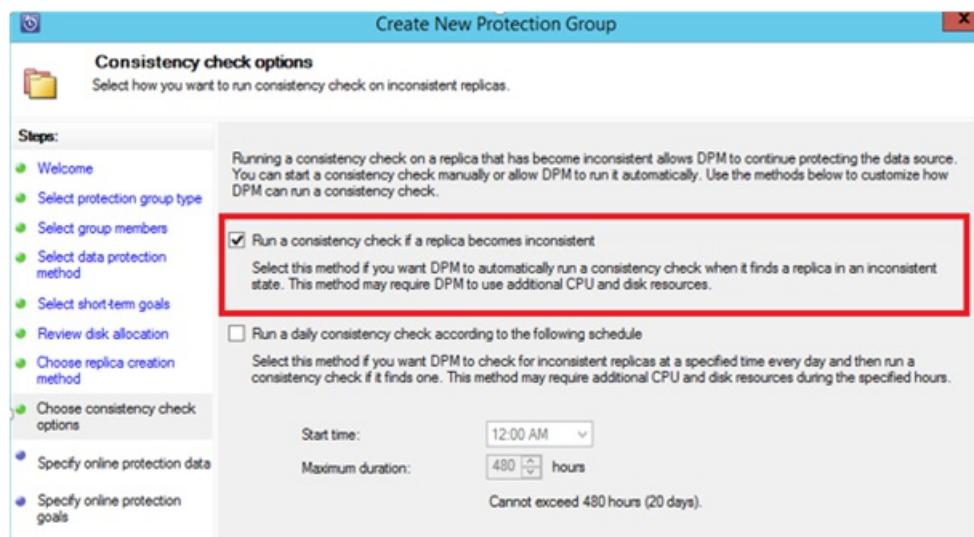


The initial backup copy requires transferring the entire data source (SQL Server database) from production server (SQL Server machine) to Azure Backup Server. This data might be large, and transferring the data over the network could exceed bandwidth. For this reason, you can choose to transfer the initial backup:

**Manually** (using removable media) to avoid bandwidth congestion, or **Automatically over the network** (at a specified time).

Once the initial backup is complete, the rest of the backups are incremental backups on the initial backup copy. Incremental backups tend to be small and are easily transferred across the network.

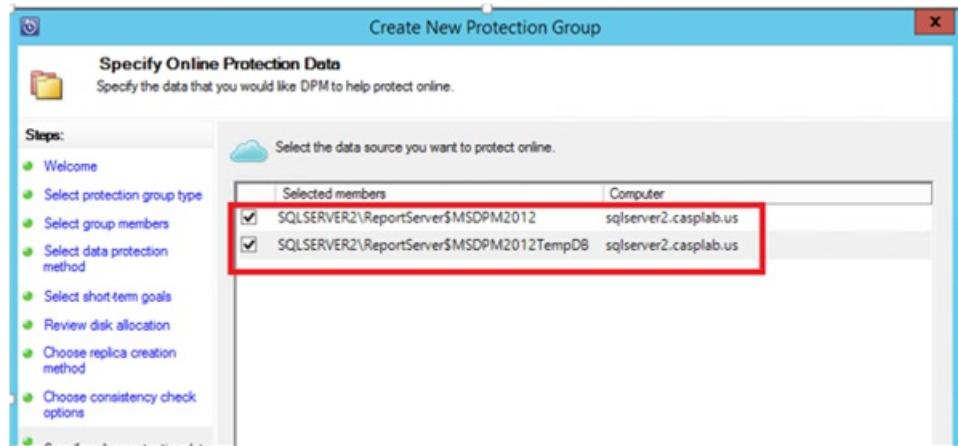
9. Choose when you want the consistency check to run and click **Next**.



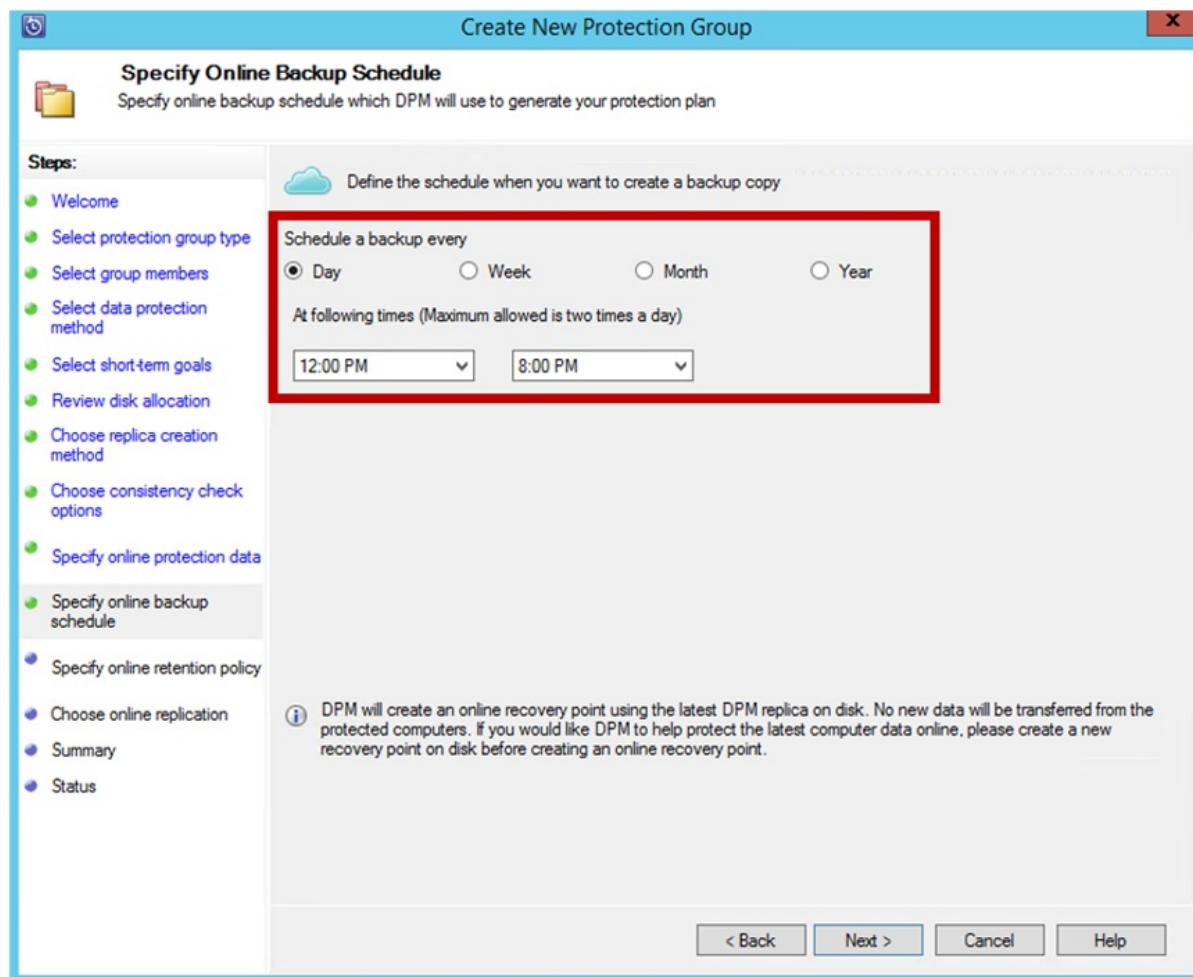
Azure Backup Server performs a consistency check on the integrity of the backup point. Azure Backup Server calculates the checksum of the backup file on the production server (SQL Server machine in this scenario) and the backed-up data for that file. If there is a conflict, it's assumed the backed-up file on Azure

Backup Server is corrupt. Azure Backup Server rectifies the backed-up data by sending the blocks corresponding to the checksum mismatch. Because consistency checks are performance-intensive, you can schedule the consistency check or run it automatically.

- To specify online protection of the datasources, select the databases to be protected to Azure and click **Next**.



- Choose backup schedules and retention policies that suit the organization policies.



In this example, backups are taken once a day at 12:00 PM and 8 PM (bottom part of the screen)

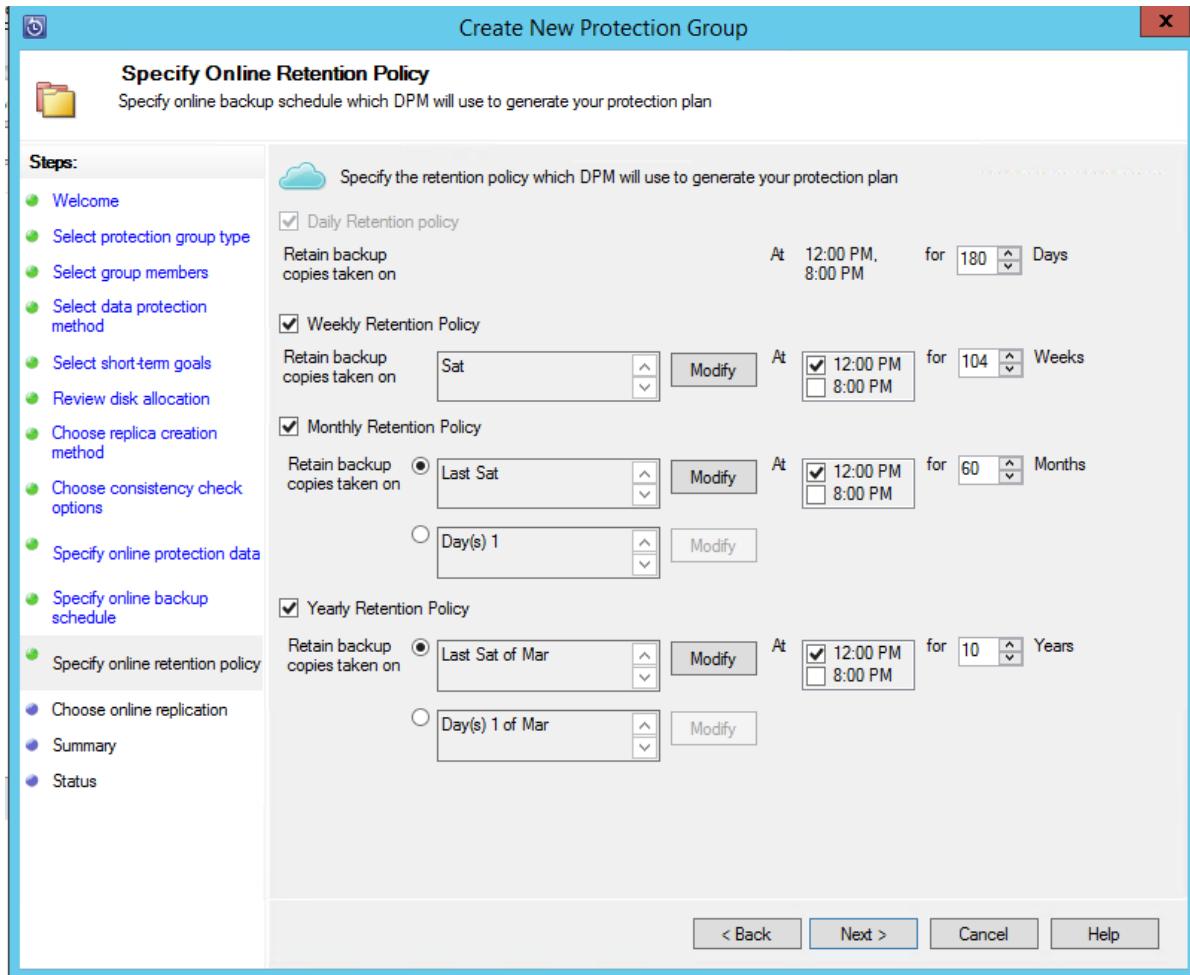
#### NOTE

It's a good practice to have a few short-term recovery points on disk, for quick recovery. These recovery points are used for operational recovery. Azure serves as a good offsite location with higher SLAs and guaranteed availability.

**Best Practice:** If you schedule backups to Azure to start after the local disk backups complete, the latest

disk backups are always copied to Azure.

12. Choose the retention policy schedule. The details on how the retention policy works are provided at [Use Azure Backup to replace your tape infrastructure article](#).

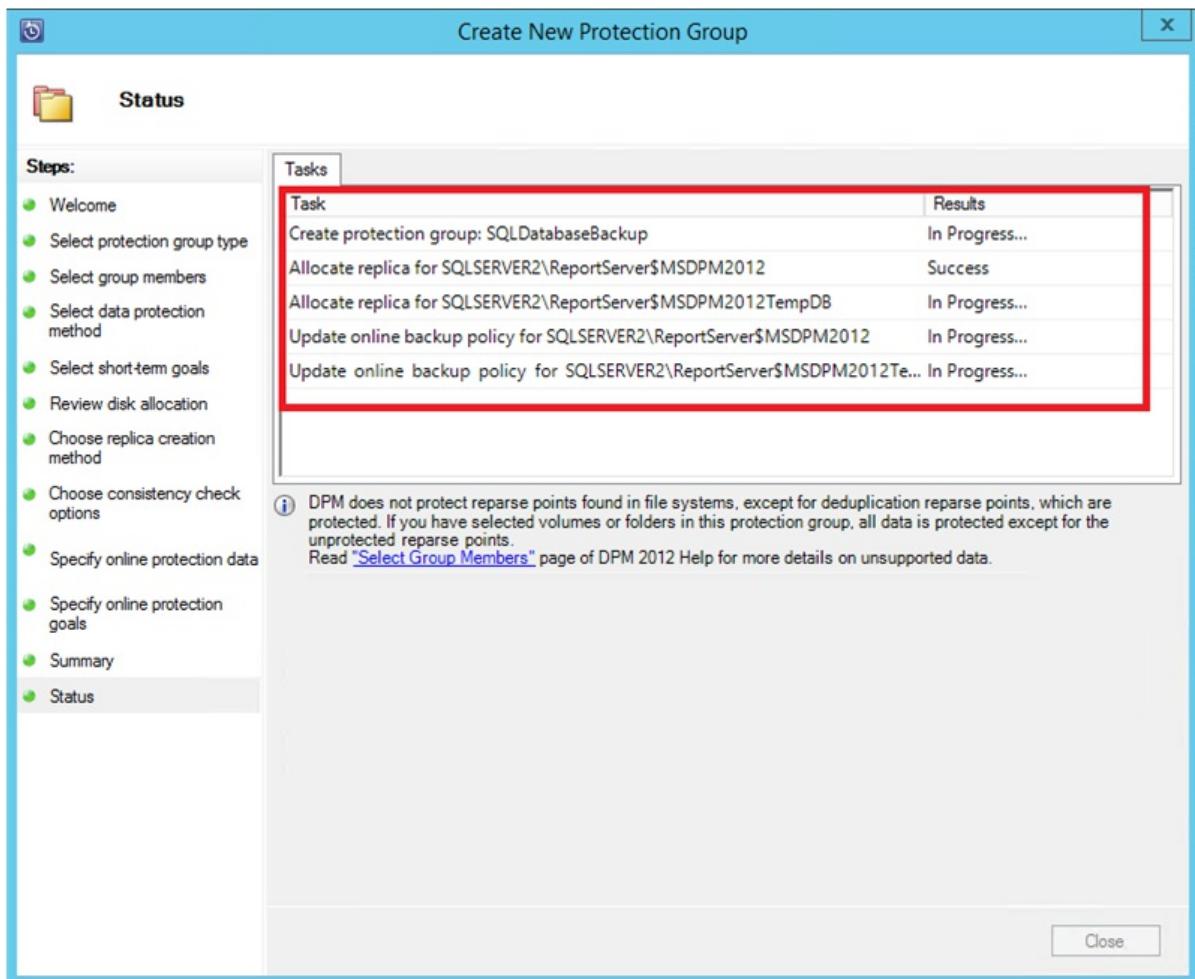


In this example:

- Backups are taken once a day at 12:00 PM and 8 PM (bottom part of the screen) and are retained for 180 days.
- The backup on Saturday at 12:00 P.M. is retained for 104 weeks
- The backup on Last Saturday at 12:00 P.M. is retained for 60 months
- The backup on Last Saturday of March at 12:00 P.M. is retained for 10 years

13. Click **Next** and select the appropriate option for transferring the initial backup copy to Azure. You can choose **Automatically over the network**

14. Once you review the policy details in the **Summary** screen, click **Create group** to complete the workflow. You can click **Close** and monitor the job progress in Monitoring workspace.



## On-demand backup of a SQL Server database

While the previous steps created a backup policy, a “recovery point” is created only when the first backup occurs. Rather than waiting for the scheduler to kick in, the steps below trigger the creation of a recovery point manually.

1. Wait until the protection group status shows **OK** for the database before creating the recovery point.

| Protection Group: SQLDatabaseBackup (Total members: 2) |    |         |
|--------------------------------------------------------|----|---------|
| Computer: sqlserver2.casplab.us                        | OK | Enabled |
| SQLSERVER2\ReportSer...                                | OK | Enabled |
| SQLSERVER2\ReportSer...                                | OK | Enabled |

**Details:** SQLSERVER2\ReportServer\$MSDPM2012

**Status:** OK

**Replica path:** [Click to view details](#)

**Latest recovery point:** 12/5/2014 4:21:54 AM

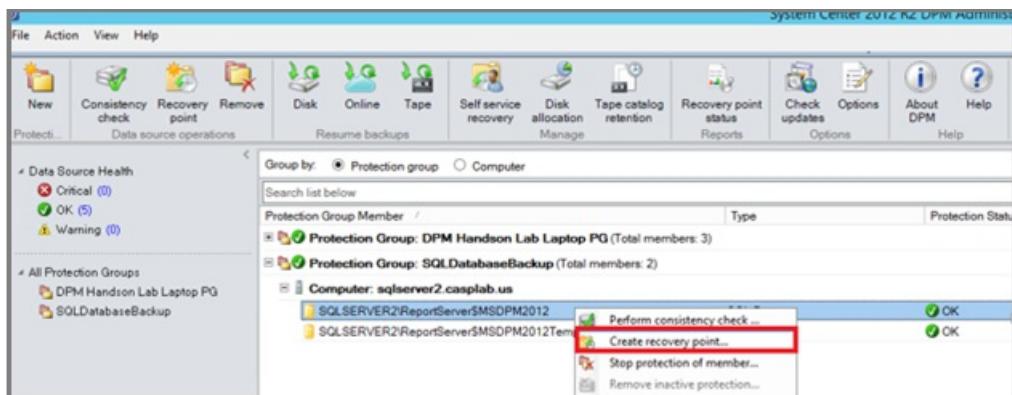
**Oldest recovery point:** 12/5/2014 4:21:54 AM

**Total recovery points:** 1

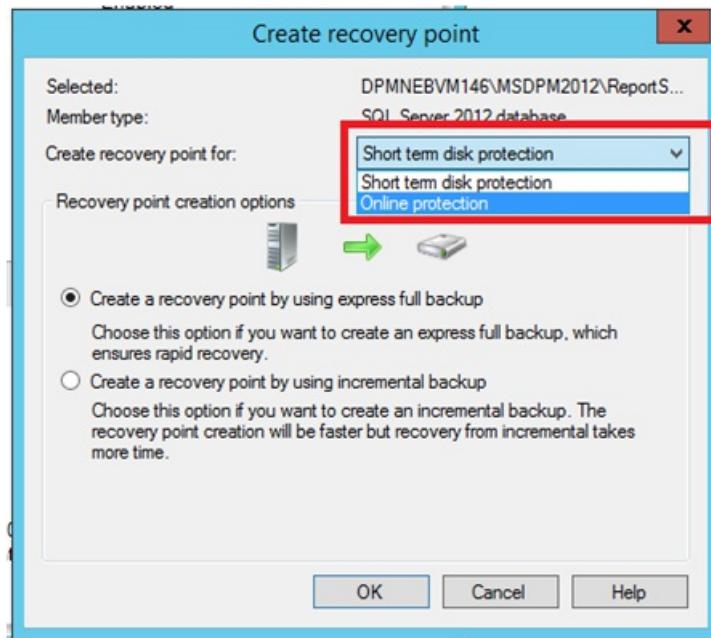
**Disk allocation:** Replica volume (co-located): 10.00 GB allocated, 93.29 MB used  
Recovery point volume (co-located): 4.57 GB allocated, 60.27 MB used

**Parent instance:** SQLSERVER2

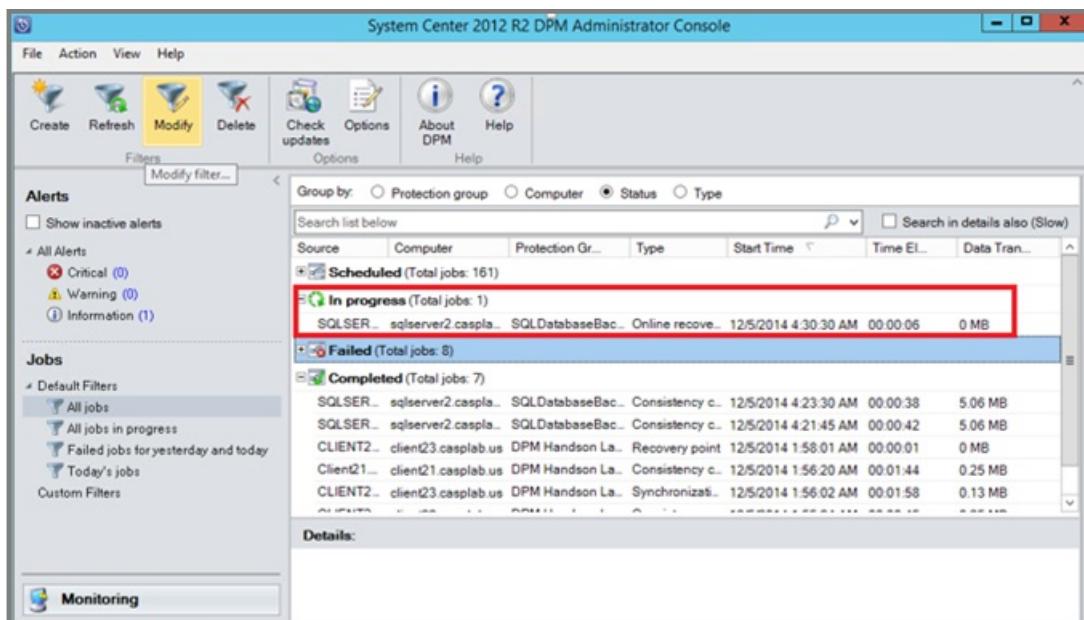
2. Right-click on the database and select **Create Recovery Point**.



3. Choose **Online Protection** in the drop-down menu and click **OK** to start creation of a recovery point in Azure.



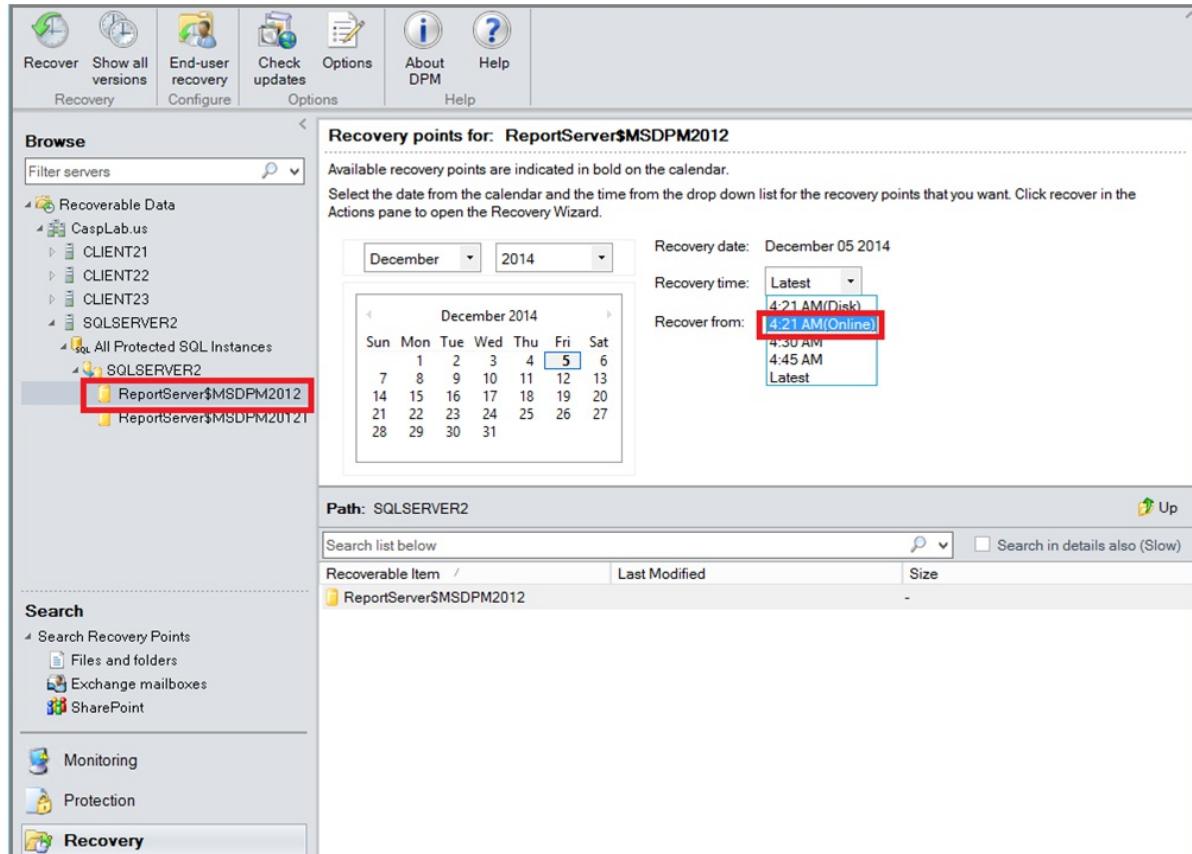
4. View the job progress in the **Monitoring** workspace.



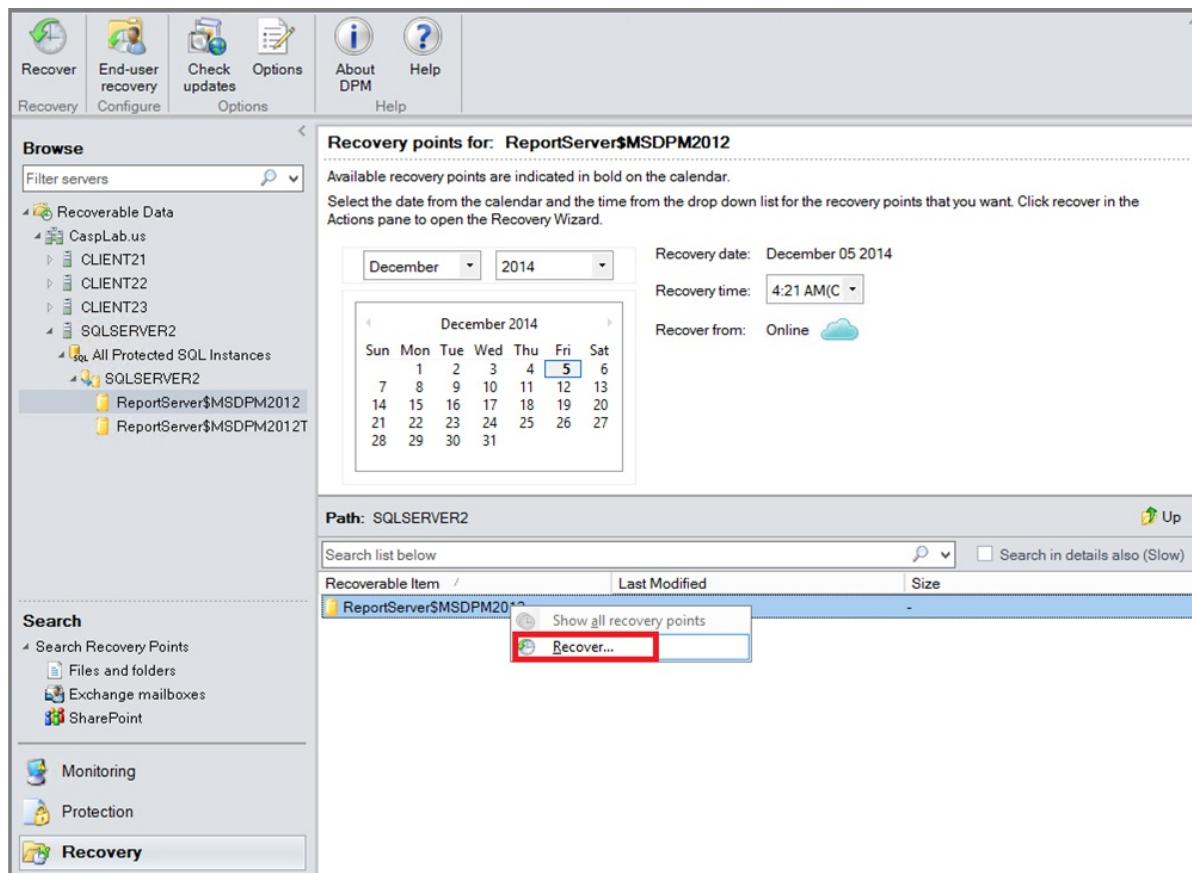
## Recover a SQL Server database from Azure

The following steps are required to recover a protected entity (SQL Server database) from Azure.

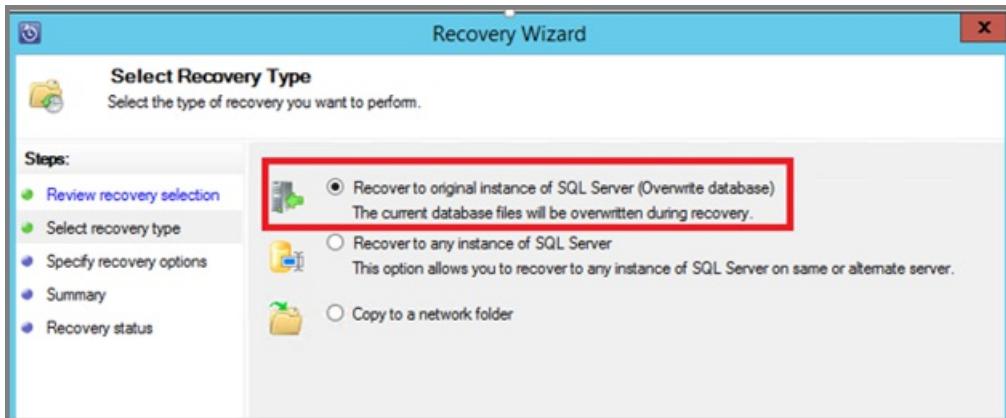
1. Open the Azure Backup Server Management Console. Navigate to **Recovery** workspace where you can see the protected servers. Browse the required database (in this case ReportServer\$MSDPM2012). Select a **Recovery from** time that is specified as an **Online** point.



2. Right-click the database name and click **Recover**.



3. MABS shows the details of the recovery point. Click **Next**. To overwrite the database, select the recovery type **Recover to original instance of SQL Server**. Click **Next**.



In this example, MABS recovers the database to another SQL Server instance, or to a standalone network folder.

4. In the **Specify Recovery options** screen, you can select the recovery options like Network bandwidth usage throttling to throttle the bandwidth used by recovery. Click **Next**.
5. In the **Summary** screen, you see all the recovery configurations provided so far. Click **Recover**.

The Recovery status shows the database being recovered. You can click **Close** to close the wizard and view the progress in the **Monitoring** workspace.



Once the recovery is completed, the restored database is application consistent.

## Next steps

See the [Backup files and application](#) article. See the [Backup SharePoint on Azure Stack](#) article.

# Prepare to back up workloads to Azure with System Center DPM

1/8/2020 • 10 minutes to read • [Edit Online](#)

This article explains how to prepare for System Center Data Protection Manager (DPM) backups to Azure, using the Azure Backup service.

The article provides:

- An overview of deploying DPM with Azure Backup.
- Prerequisites and limitations for using Azure Backup with DPM.
- Steps for preparing Azure, including setting up a Recovery Services Backup vault, and optionally modifying the type of Azure storage for the vault.
- Steps for preparing the DPM server, including downloading vault credentials, installing the Azure Backup agent, and registering the DPM server in the vault.
- Troubleshooting tips for common errors.

## Why back up DPM to Azure?

[System Center DPM](#) backs up file and application data. DPM interacts with Azure Backup as follows:

- **DPM running on a physical server or on-premises VM** — You can back up data to a Backup vault in Azure, in addition to disk and tape backup.
- **DPM running on an Azure VM** — From System Center 2012 R2 with Update 3 or later, you can deploy DPM on an Azure VM. You can back up data to Azure disks attached to the VM, or use Azure Backup to back up the data to a Backup vault.

The business benefits of backing up DPM servers to Azure include:

- For on-premises DPM, Azure Backup provides an alternative to long-term deployment to tape.
- For DPM running on an Azure VM, Azure Backup allows you to offload storage from the Azure disk. Storing older data in a Backup vault allows you to scale up your business by storing new data to disk.

## Prerequisites and limitations

| SETTING                  | REQUIREMENT                                                                     |
|--------------------------|---------------------------------------------------------------------------------|
| DPM on an Azure VM       | System Center 2012 R2 with DPM 2012 R2 Update Rollup 3 or later.                |
| DPM on a physical server | System Center 2012 SP1 or later; System Center 2012 R2.                         |
| DPM on a Hyper-V VM      | System Center 2012 SP1 or later; System Center 2012 R2.                         |
| DPM on a VMware VM       | System Center 2012 R2 with Update Rollup 5 or later.                            |
| Components               | The DPM server should have Windows PowerShell and .NET Framework 4.5 installed. |

| SETTING                | REQUIREMENT                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Supported apps         | <a href="#">Learn</a> what DPM can back up.                                                                                                                                                                                                                                                                                                                                                            |
| Supported file types   | These file types can be backed up with Azure Backup: Encrypted (full backups only); Compressed (incremental backups supported); Sparse (incremental backups supported); Compressed and sparse (treated as sparse).                                                                                                                                                                                     |
| Unsupported file types | Servers on case-sensitive file systems; hard links (skipped); reparse points (skipped); encrypted and compressed (skipped); encrypted and sparse (skipped); Compressed stream; parse stream.                                                                                                                                                                                                           |
| Local storage          | Each machine you want to back up must have local free storage that's at least 5% of the size of the data that is being backed up. For example, backing up 100 GB of data requires a minimum of 5 GB of free space in the scratch location.                                                                                                                                                             |
| Vault storage          | There's no limit to the amount of data you can back up to an Azure Backup vault, but the size of a data source (for example a virtual machine or database) shouldn't exceed 54,400 GB.                                                                                                                                                                                                                 |
| Azure ExpressRoute     | If Azure ExpressRoute is configured with Private or Microsoft peering, it cannot be used to back up the data to Azure.<br><br>If Azure ExpressRoute is configured with Public Peering, it can be used to back up the data to Azure.<br><br><b>Note:</b> Public Peering is deprecated for new circuits.                                                                                                 |
| Azure Backup agent     | If DPM is running on System Center 2012 SP1, install Rollup 2 or later for DPM SP1. This is required for agent installation.<br><br>This article describes how to deploy the latest version of the Azure Backup agent, also known as the Microsoft Azure Recovery Service (MARS) agent. If you have an earlier version deployed, update to the latest version to ensure that backup works as expected. |

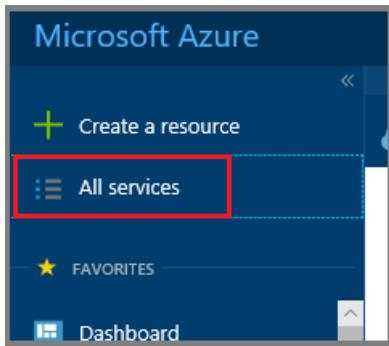
Before you start, you need an Azure account with the Azure Backup feature enabled. If you don't have an account, you can create a free trial account in just a couple of minutes. Read about [Azure Backup pricing](#).

## Create a Recovery Services vault

A Recovery Services vault is an entity that stores backups and recovery points created over time. The Recovery Services vault also contains the backup policies that are associated with the protected virtual machines.

To create a Recovery Services vault, follow these steps.

1. Sign in to your subscription in the [Azure portal](#).
2. On the left menu, select **All services**.



3. In the **All services** dialog box, enter *Recovery Services*. The list of resources filters according to your input. In the list of resources, select **Recovery Services vaults**.

The list of Recovery Services vaults in the subscription appears.

4. On the **Recovery Services vaults** dashboard, select **Add**.

The **Recovery Services vault** dialog box opens. Provide values for the **Name**, **Subscription**, **Resource group**, and **Location**.

- **Name:** Enter a friendly name to identify the vault. The name must be unique to the Azure subscription. Specify a name that has at least 2 but not more than 50 characters. The name must start with a letter and consist only of letters, numbers, and hyphens.
- **Subscription:** Choose the subscription to use. If you're a member of only one subscription, you'll see that name. If you're not sure which subscription to use, use the default (suggested) subscription.

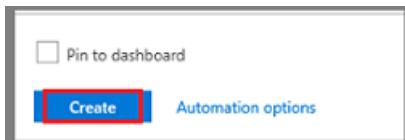
There are multiple choices only if your work or school account is associated with more than one Azure subscription.

- **Resource group:** Use an existing resource group or create a new one. To see the list of available resource groups in your subscription, select **Use existing**, and then select a resource from the drop-down list. To create a new resource group, select **Create new** and enter the name. For more information about resource groups, see [Azure Resource Manager overview](#).
- **Location:** Select the geographic region for the vault. To create a vault to protect virtual machines, the vault *must* be in the same region as the virtual machines.

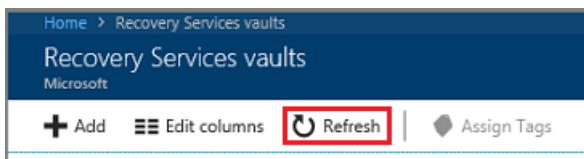
#### IMPORTANT

If you're not sure of the location of your VM, close the dialog box. Go to the list of virtual machines in the portal. If you have virtual machines in several regions, create a Recovery Services vault in each region. Create the vault in the first location, before you create the vault for another location. There's no need to specify storage accounts to store the backup data. The Recovery Services vault and Azure Backup handle that automatically.

5. When you're ready to create the Recovery Services vault, select **Create**.



It can take a while to create the Recovery Services vault. Monitor the status notifications in the **Notifications** area at the upper-right corner of the portal. After your vault is created, it's visible in the list of Recovery Services vaults. If you don't see your vault, select **Refresh**.



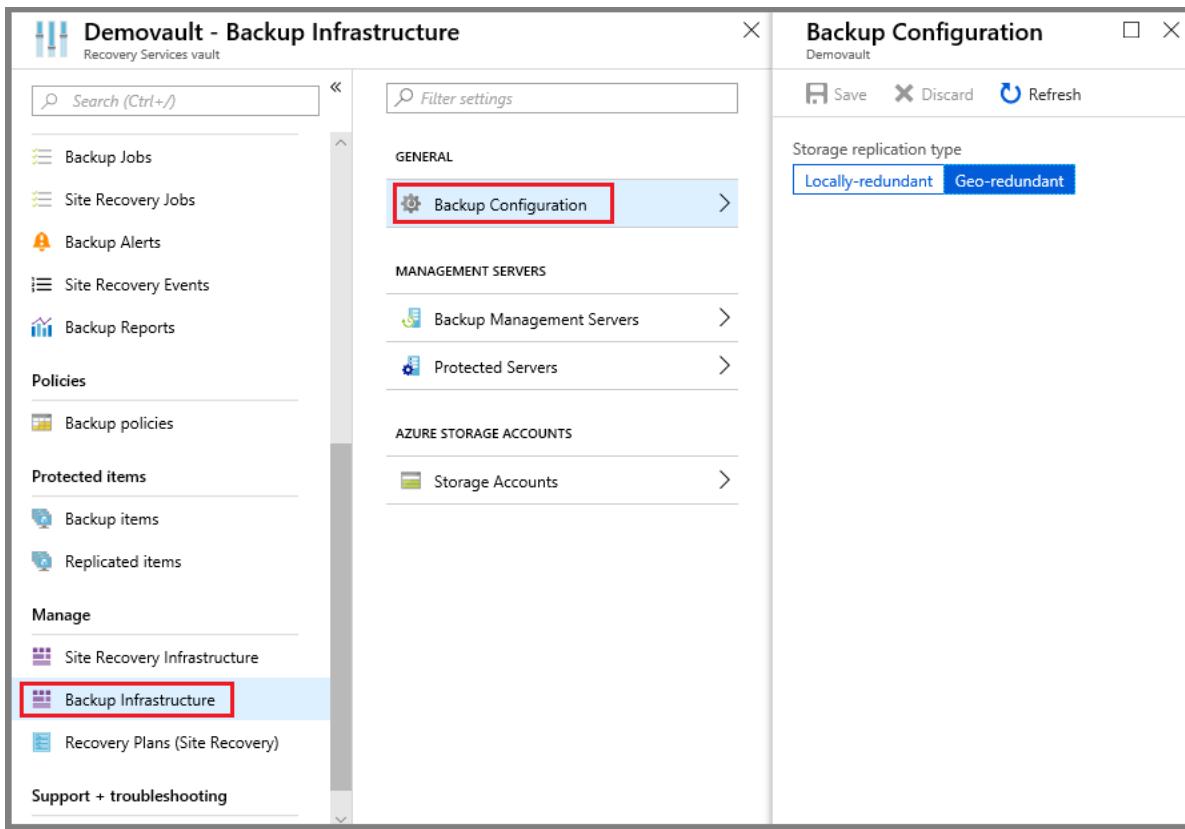
## Modify storage settings

You can choose between geo-redundant storage and locally redundant storage.

- By default, your vault has geo-redundant storage.
- If the vault is your primary backup, leave the option set to geo-redundant storage. If you want a cheaper option that isn't quite as durable, use the following procedure to configure locally redundant storage.
- Learn about [Azure storage](#), and the **geo-redundant** and **locally redundant** storage options.
- Modify storage settings before the initial backup. If you've already backed up an item, stop backing it up in the vault before you modify storage settings.

To edit the storage replication setting:

1. Open the vault dashboard.
2. In **Manage**, click **Backup Infrastructure**.
3. In **Backup Configuration** menu, select a storage option for the vault.



## Download vault credentials

You use vault credentials when you register the DPM server in the vault.

- 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).
- During the machine registration workflow, the certificate's private key is made available to the user, which authenticates the machine.
- Based on the authentication, the Azure Backup service sends data to the identified vault.

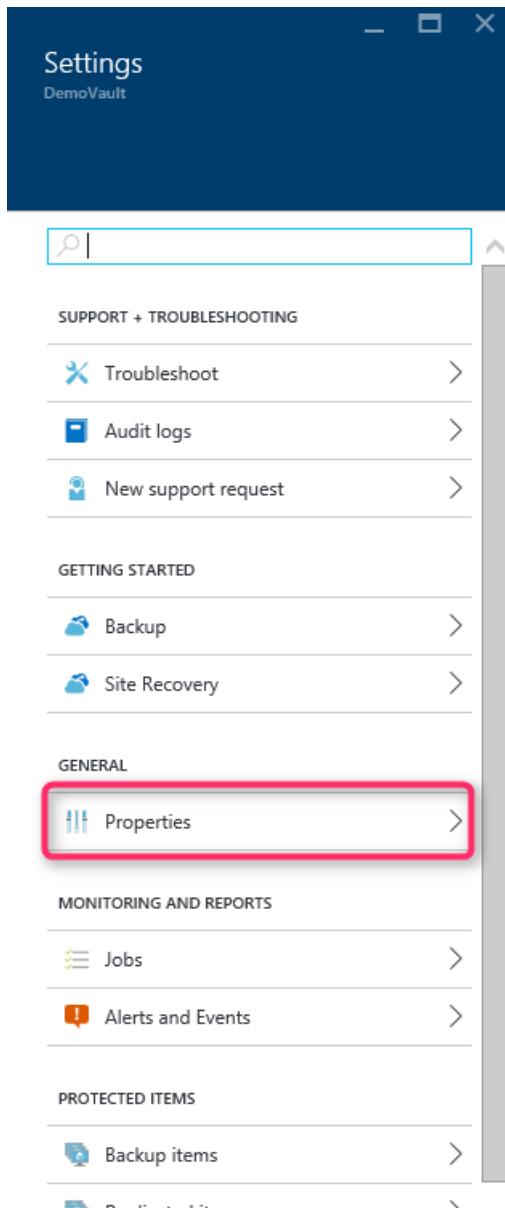
### Best practices for vault credentials

To obtain the credentials, download the vault credential file through a secure channel from the Azure portal:

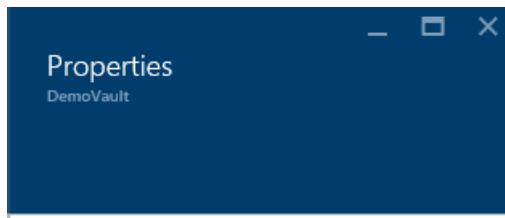
- The vault credentials are used only during the registration workflow.
- It's your responsibility to ensure that the vault credentials file is safe, and not compromised.
  - If control of the credentials is lost, the vault credentials can be used to register other machines to vault.
  - However, backup data is encrypted using a passphrase that belongs to the customer, so existing backup data can't be compromised.
- Ensure that file is saved in a location that can be accessed from the DPM server. If it is stored in a file share/SMB, check for the access permissions.
- Vault credentials expire after 48 hrs. You can download new vault credentials as many times as needed. However, only the latest vault credential file can be used during the registration workflow.
- The Azure Backup service isn't aware of the certificate's private key, and the private key isn't available in the portal or the service.

Download the vault credentials file to a local machine as follows:

1. Sign in to the [Azure portal](#).
2. Open the vault in which you want to register the DPM server.
3. In **Settings**, click **Properties**.



4. In **Properties > Backup Credentials**, click **Download**. The portal generates the vault credential file using a combination of the vault name and current date, and makes it available for download.



STATUS

Active

LOCATION

West US

SUBSCRIPTION NAME

[MAB Canary Subscription 2](#)

SUBSCRIPTION ID

da364f0f-307b-41c9-9d47-b7413ec4553



RESOURCE GROUP

[trinadhkRG](#)

---

BACKUP

Azure Backup Agent

[Download](#)

[Backup Credentials](#)

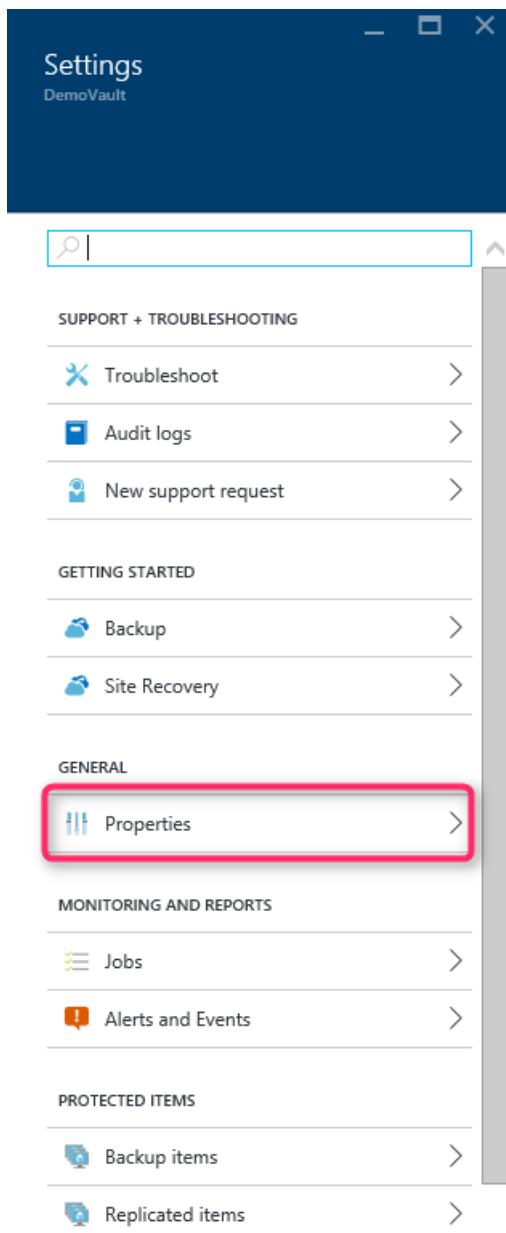
[Download](#)

5. Click **Save** to download the vault credentials to folder, or **Save As** and specify a location. It will take up to a minute for the file to be generated.

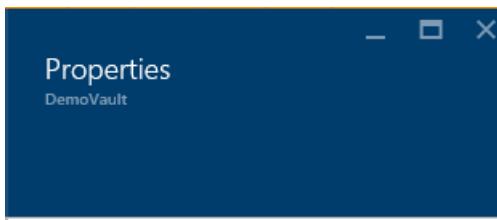
## Install the Backup Agent

Every machine that's backed up by Azure Backup must have the Backup agent (also known as the Microsoft Azure Recovery Service (MARS) agent) installed on it. Install the agent on the DPM server as follows:

1. Open the vault to which you want to register the DPM server.
2. In **Settings**, click **Properties**.



3. On the **Properties** page, download the Azure Backup Agent.



STATUS

Active

LOCATION

West US

SUBSCRIPTION NAME

[MAB Canary Subscription 2](#)

SUBSCRIPTION ID

da364f0f-307b-41c9-9d47-b7413ec45535



RESOURCE GROUP

[trinadhkRG](#)

---

BACKUP

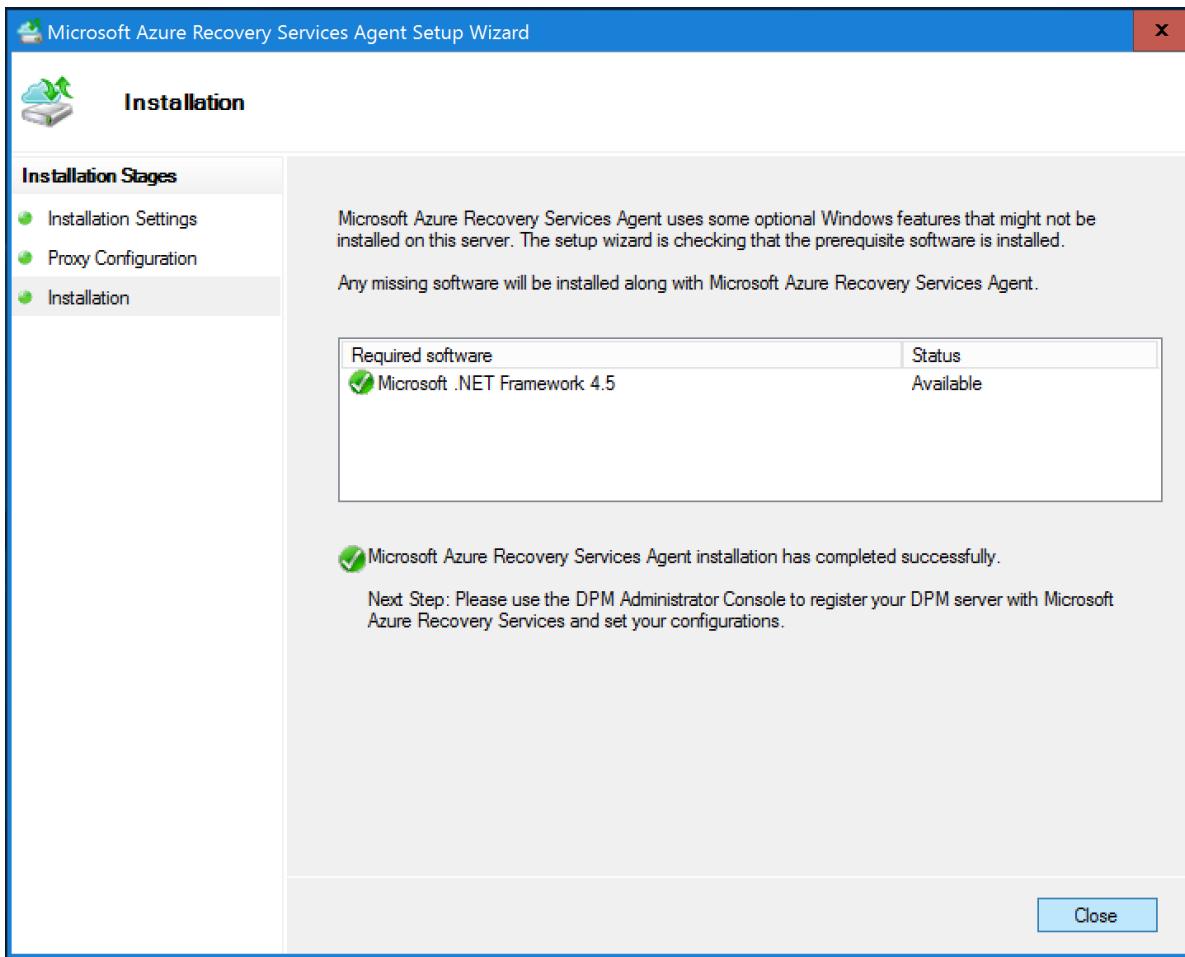
[Azure Backup Agent](#)

[Download](#)

Backup Credentials

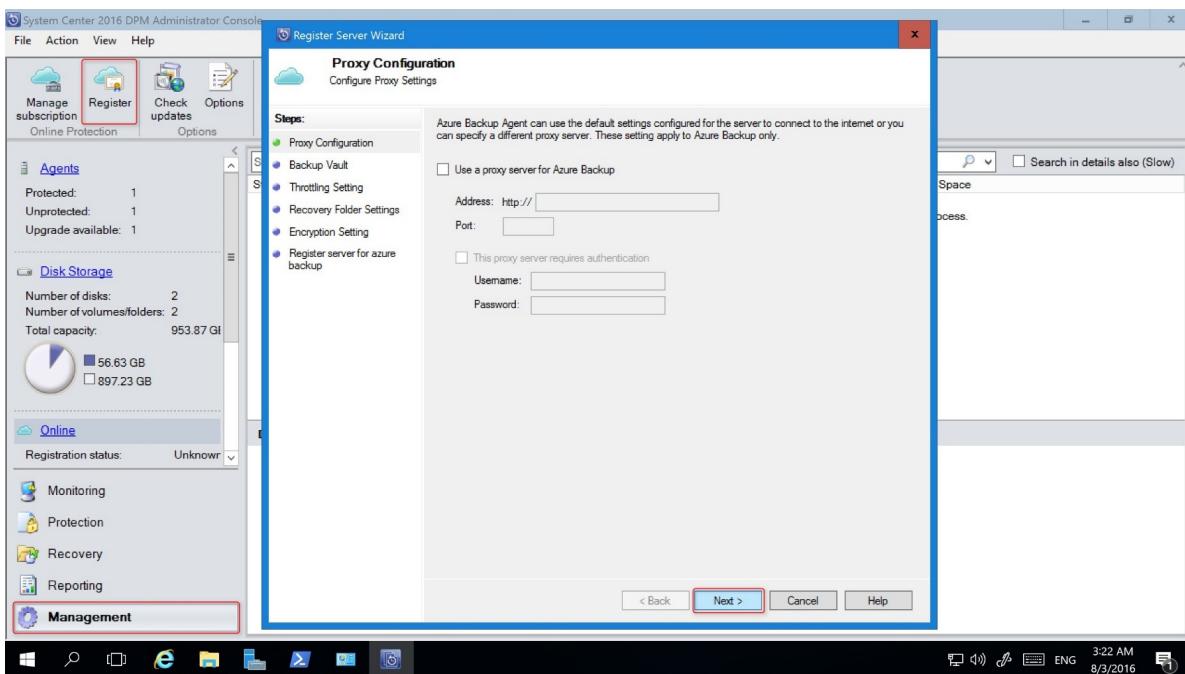
[Download](#)

4. After downloading, run MARSAgentInstaller.exe. to install the agent on the DPM machine.
5. Select an installation folder and cache folder for the agent. The cache location free space must be at least 5% of the backup data.
6. If you use a proxy server to connect to the internet, in the **Proxy configuration** screen, enter the proxy server details. If you use an authenticated proxy, enter the user name and password details in this screen.
7. The Azure Backup agent installs .NET Framework 4.5 and Windows PowerShell (if they're not installed) to complete the installation.
8. After the agent is installed, **Close** the window.

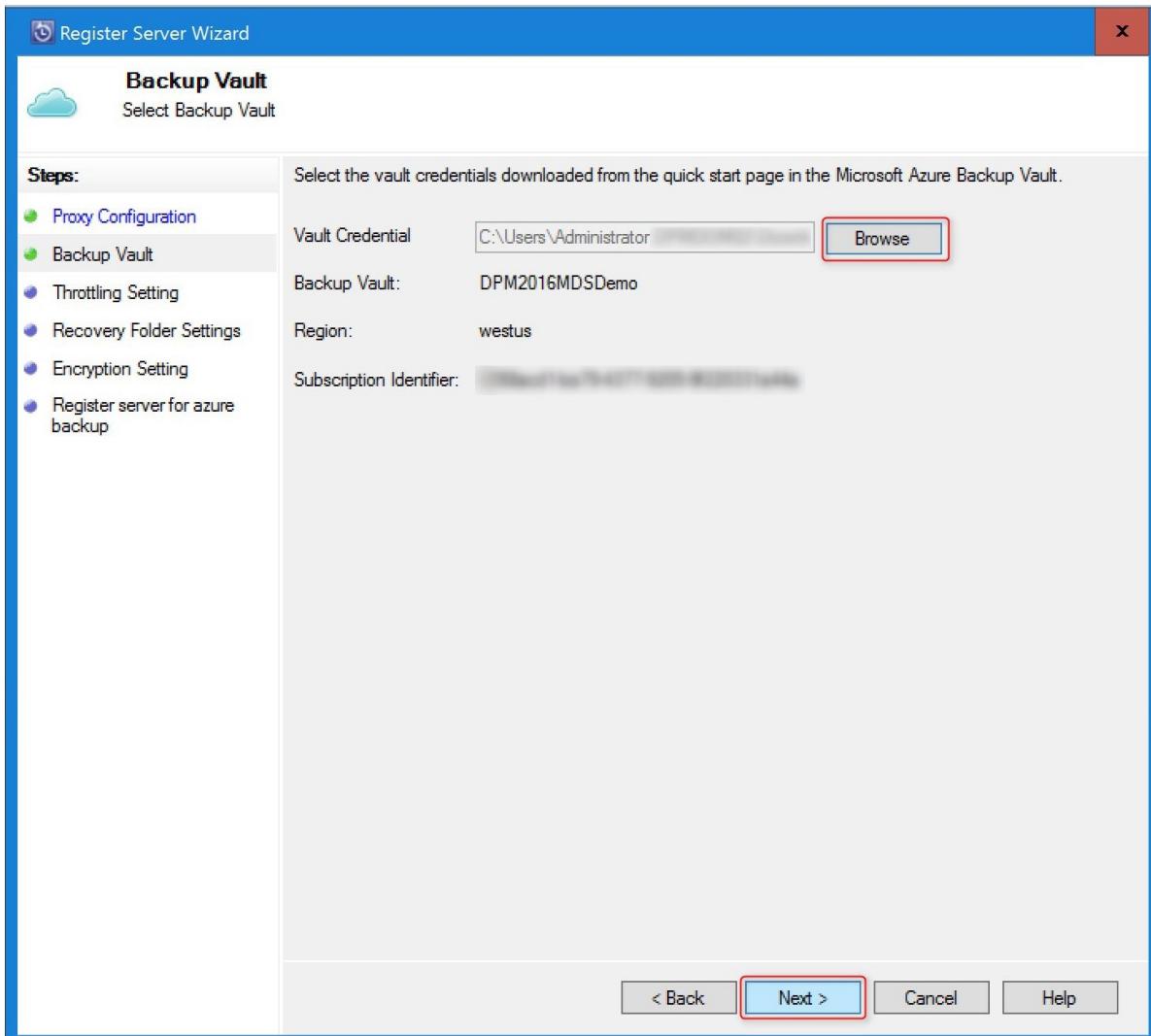


## Register the DPM server in the vault

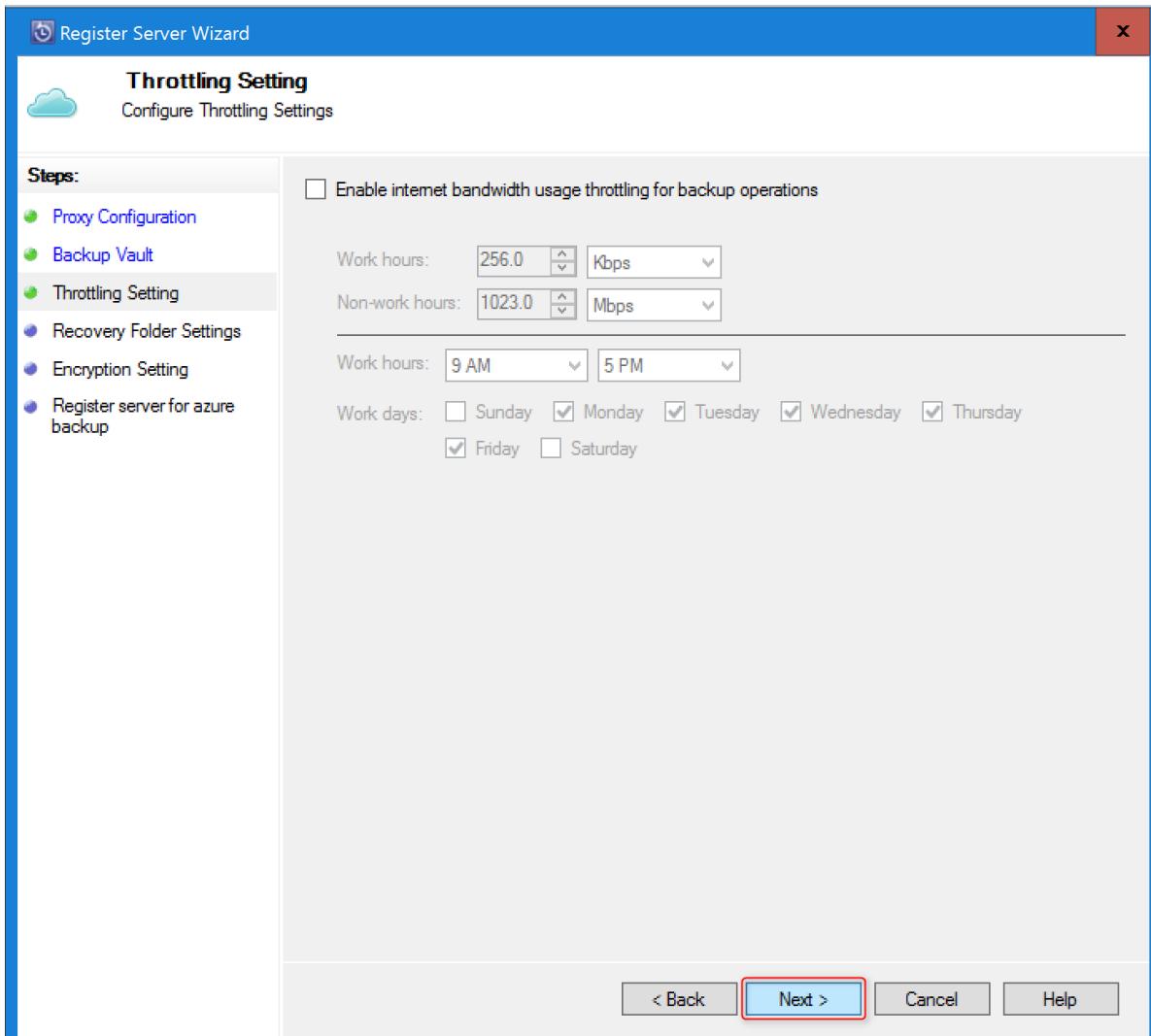
1. In the DPM Administrator console > **Management**, click **Online**. Select **Register**. It will open the Register Server Wizard.
2. In **Proxy Configuration**, specify the proxy settings as required.



3. In **Backup Vault**, browse to and select the vault credentials file that you downloaded.

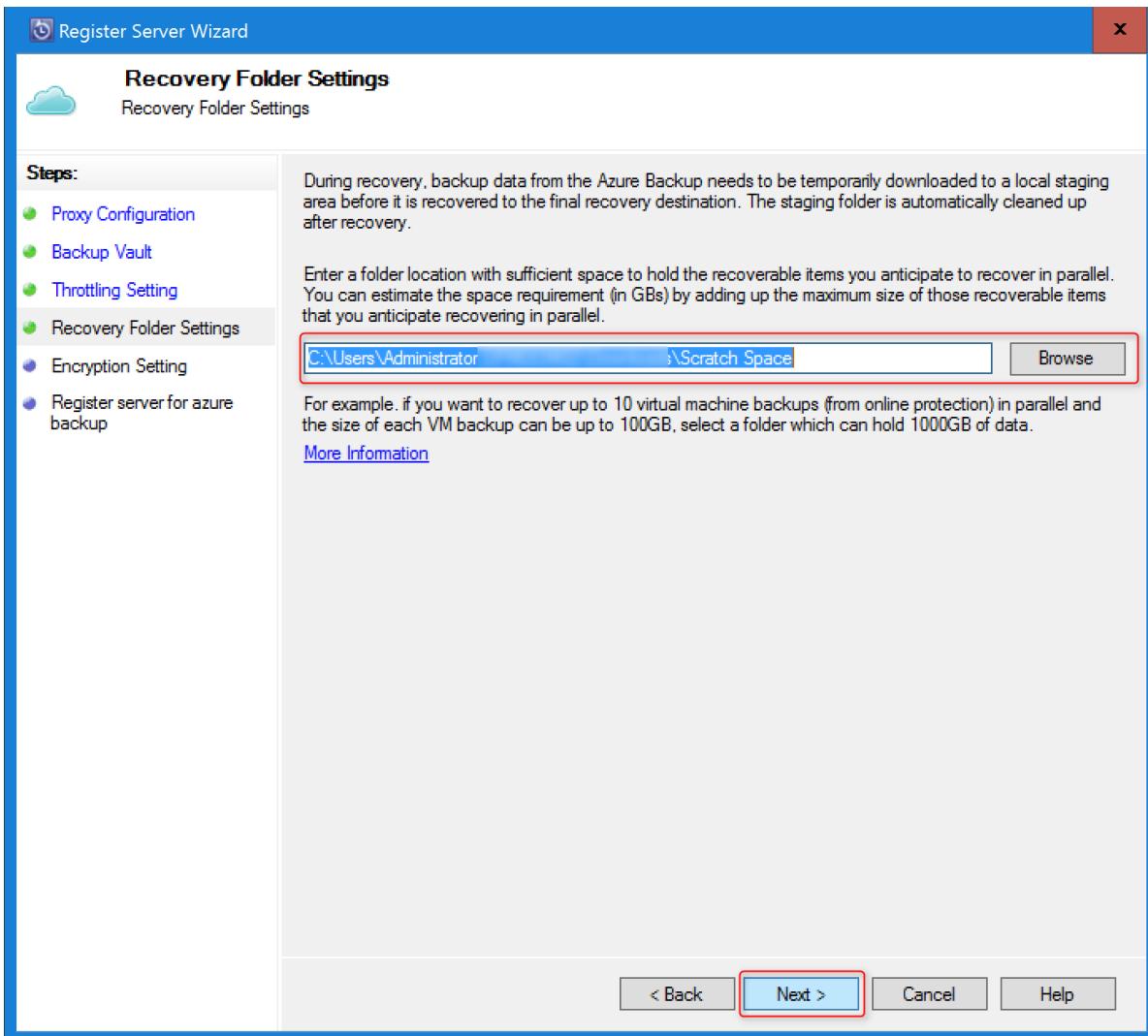


4. In **Throttling Setting**, you can optionally enable bandwidth throttling for backups. You can set the speed limits for specify work hours and days.



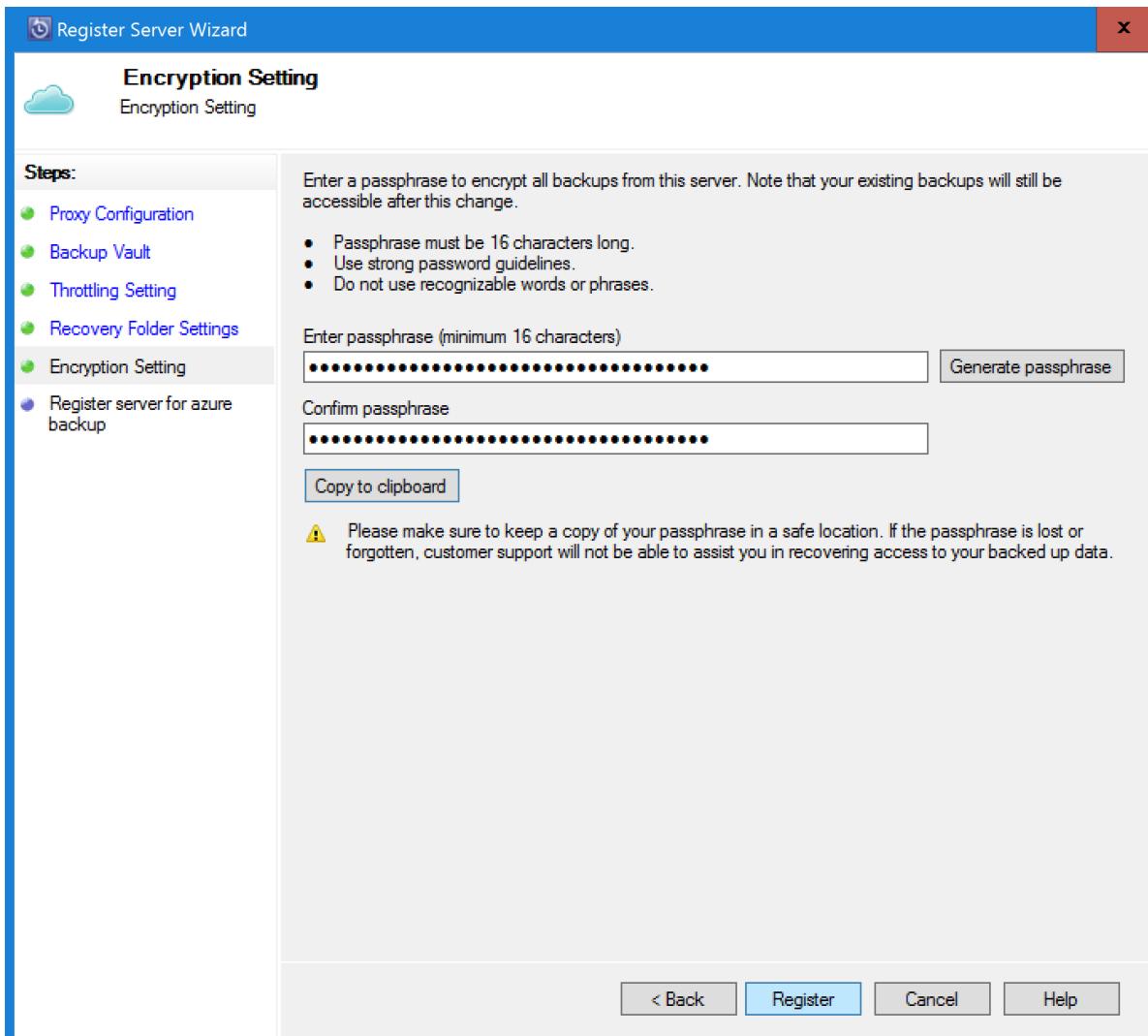
5. In **Recovery Folder Setting**, specify a location that can be used during data recovery.

- Azure Backup uses this location as a temporary holding area for recovered data.
- After finishing data recovery, Azure Backup will clean up the data in this area.
- The location must have enough space to hold items that you anticipate recovering in parallel.



6. In **Encryption setting**, generate or provide a passphrase.

- The passphrase is used to encrypt the backups to cloud.
- Specify a minimum of 16 characters.
- Save the file in a secure location, it's needed for recovery.



#### WARNING

You own the encryption passphrase and Microsoft does not have visibility into it. If the passphrase is lost or forgotten; Microsoft cannot help in recovering the backup data.

7. Click **Register** to register the DPM server to the vault.

After the server is registered successfully to the vault and you are now ready to start backing up to Microsoft Azure. You'll need to configure the protection group in the DPM console to backup workloads to Azure. [Learn how to deploy protection groups.](#)

## Troubleshoot vault credentials

### Expiration error

The vault credentials file is valid only for 48 hrs (after it's downloaded from the portal). If you encounter any error in this screen (for example, "Vault credentials file provided has expired"), login to the Azure portal and download the vault credentials file again.

### Access error

Ensure that the vault credentials file is available in a location that can be accessed by the setup application. If you encounter access related errors, copy the vault credentials file to a temporary location in this machine and retry the operation.

### Invalid credentials error

If you encounter an invalid vault credential error (for example, "Invalid vault credentials provided") the file is either

corrupted or does not have the latest credentials associated with the recovery service.

- Retry the operation after downloading a new vault credential file from the portal.
- This error is typically seen when you click on the **Download vault credential** option in the Azure portal, twice in quick succession. In this case, only the second vault credential file is valid.

# Back up an Exchange server to Azure Backup with System Center 2012 R2 DPM

2/25/2020 • 3 minutes to read • [Edit Online](#)

This article describes how to configure a System Center 2012 R2 Data Protection Manager (DPM) server to back up a Microsoft Exchange server to Azure Backup.

## Updates

To successfully register the DPM server with Azure Backup, you must install the latest update rollup for System Center 2012 R2 DPM and the latest version of the Azure Backup Agent. Get the latest update rollup from the [Microsoft Catalog](#).

### NOTE

For the examples in this article, version 2.0.8719.0 of the Azure Backup Agent is installed, and Update Rollup 6 is installed on System Center 2012 R2 DPM.

## Prerequisites

Before you continue, make sure that all the [prerequisites](#) for using Microsoft Azure Backup to protect workloads have been met. These prerequisites include the following:

- A backup vault on the Azure site has been created.
- Agent and vault credentials have been downloaded to the DPM server.
- The agent is installed on the DPM server.
- The vault credentials were used to register the DPM server.
- If you are protecting Exchange 2016, please upgrade to DPM 2012 R2 UR9 or later

## DPM protection agent

To install the DPM protection agent on the Exchange server, follow these steps:

1. Make sure that the firewalls are correctly configured. See [Configure firewall exceptions for the agent](#).
2. Install the agent on the Exchange server by clicking **Management > Agents > Install** in DPM Administrator Console. See [Install the DPM protection agent](#) for detailed steps.

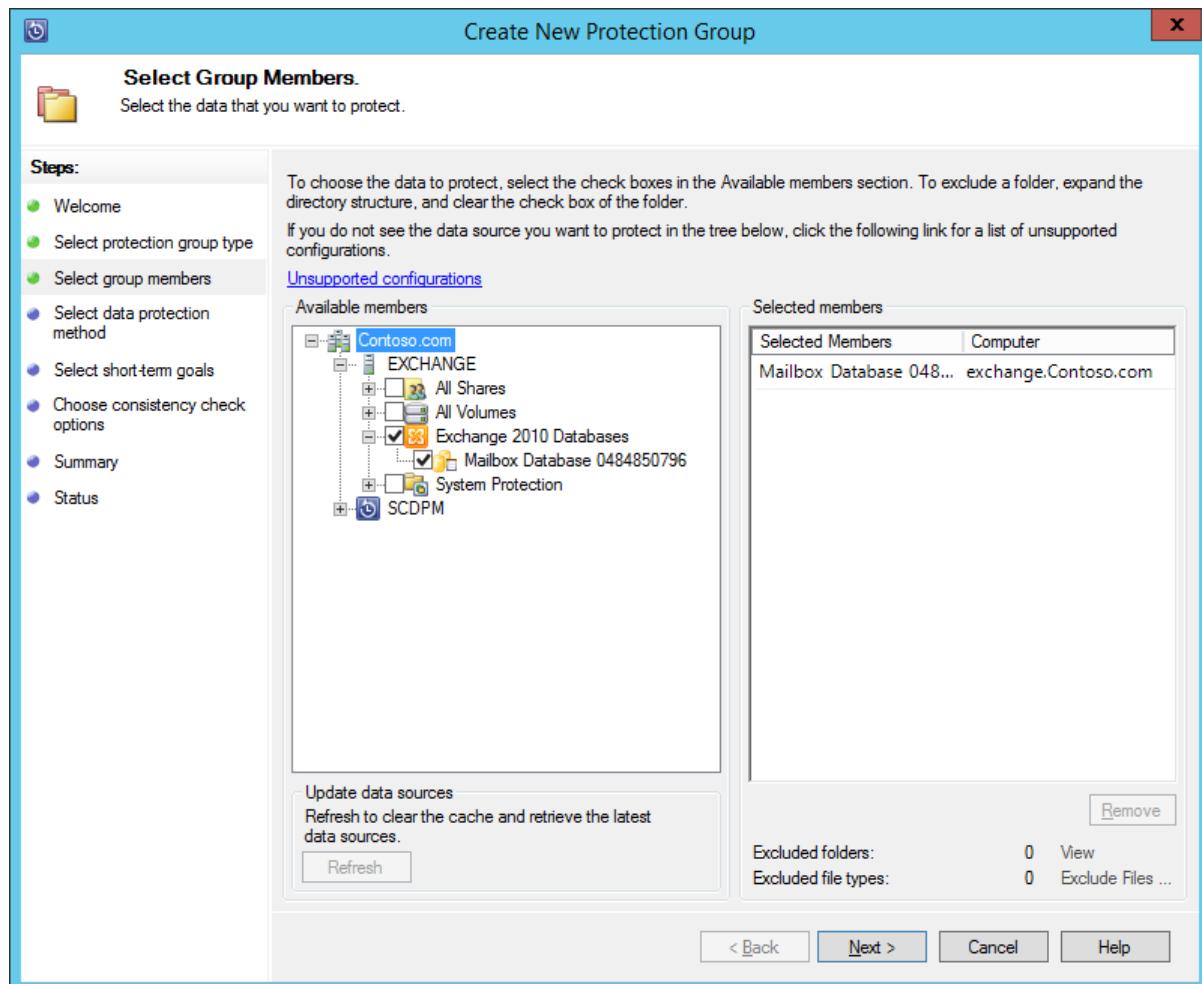
## Create a protection group for the Exchange server

1. In the DPM Administrator Console, click **Protection**, and then click **New** on the tool ribbon to open the **Create New Protection Group** wizard.
2. On the **Welcome** screen of the wizard, click **Next**.
3. On the **Select protection group type** screen, select **Servers** and click **Next**.
4. Select the Exchange server database that you want to protect and click **Next**.

#### NOTE

If you are protecting Exchange 2013, check the [Exchange 2013 prerequisites](#).

In the following example, the Exchange 2010 database is selected.



5. Select the data protection method.

Name the protection group, and then select both of the following options:

- I want short-term protection using Disk.
- I want online protection.

6. Click **Next**.

7. Select the **Run Eseutil to check data integrity** option if you want to check the integrity of the Exchange Server databases.

After you select this option, backup consistency checking will be run on the DPM server to avoid the I/O traffic that's generated by running the **eseutil** command on the Exchange server.

#### NOTE

To use this option, you must copy the Ese.dll and Eseutil.exe files to the C:\Program Files\Microsoft System Center 2012 R2\DPM\bin directory on the DPM server. Otherwise, the following error is triggered:



8. Click **Next**.

9. Select the database for **Copy Backup**, and then click **Next**.

#### NOTE

If you do not select "Full backup" for at least one DAG copy of a database, logs will not be truncated.

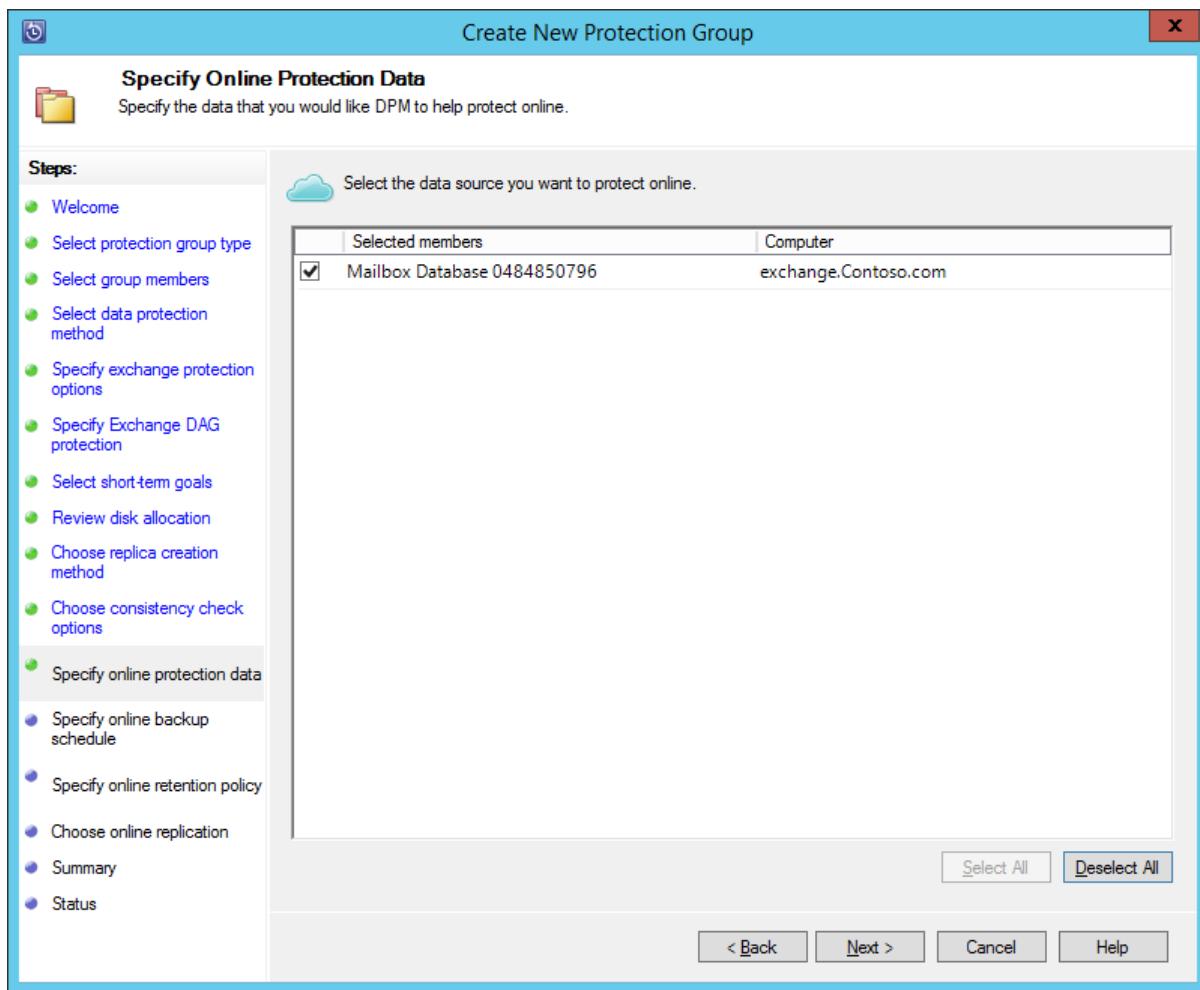
10. Configure the goals for **Short-Term backup**, and then click **Next**.

11. Review the available disk space, and then click **Next**.

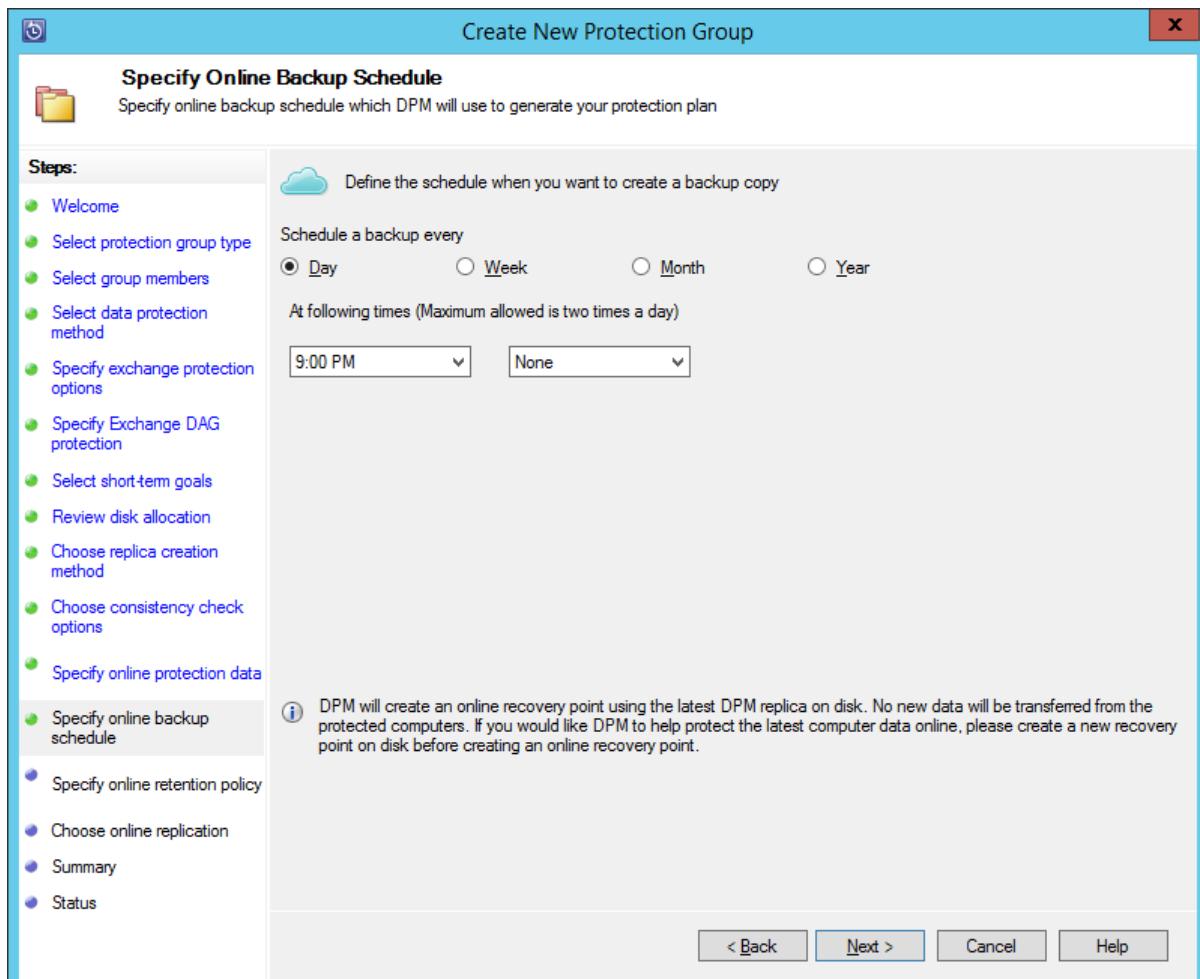
12. Select the time at which the DPM server will create the initial replication, and then click **Next**.

13. Select the consistency check options, and then click **Next**.

14. Choose the database that you want to back up to Azure, and then click **Next**. For example:



15. Define the schedule for **Azure Backup**, and then click **Next**. For example:



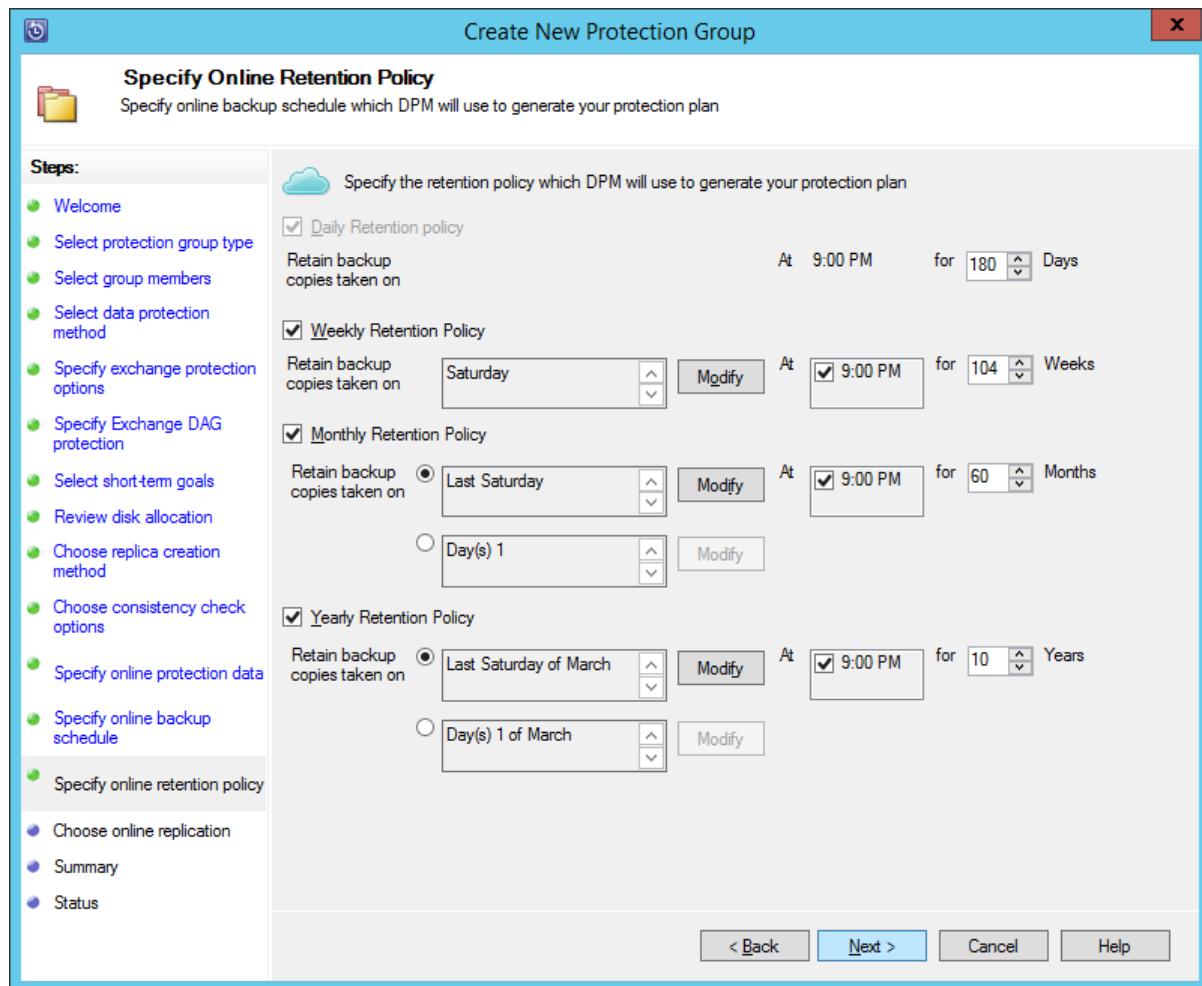
#### NOTE

Note Online recovery points are based on express full recovery points. Therefore, you must schedule the online recovery point after the time that's specified for the express full recovery point.

16. Configure the retention policy for **Azure Backup**, and then click **Next**.

17. Choose an online replication option and click **Next**.

If you have a large database, it could take a long time for the initial backup to be created over the network. To avoid this issue, you can create an offline backup.



18. Confirm the settings, and then click **Create Group**.

19. Click **Close**.

## Recover the Exchange database

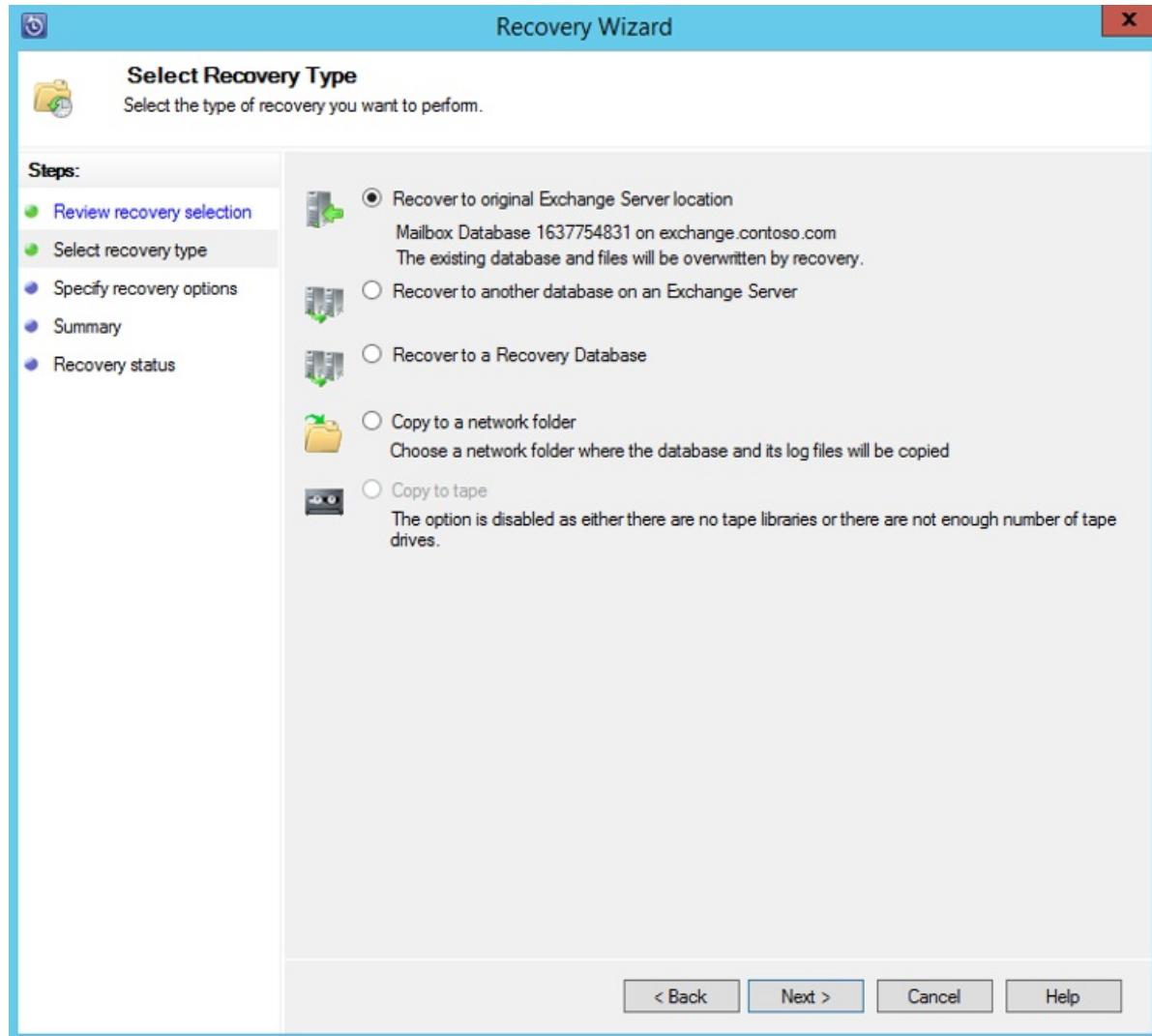
1. To recover an Exchange database, click **Recovery** in the DPM Administrator Console.
2. Locate the Exchange database that you want to recover.
3. Select an online recovery point from the *recovery time* drop-down list.
4. Click **Recover** to start the **Recovery Wizard**.

For online recovery points, there are five recovery types:

- **Recover to original Exchange Server location:** The data will be recovered to the original Exchange server.
- **Recover to another database on an Exchange Server:** The data will be recovered to another database

on another Exchange server.

- **Recover to a Recovery Database:** The data will be recovered to an Exchange Recovery Database (RDB).
- **Copy to a network folder:** The data will be recovered to a network folder.
- **Copy to tape:** If you have a tape library or a stand-alone tape drive attached and configured on the DPM server, the recovery point will be copied to a free tape.



## Next steps

- [Azure Backup FAQ](#)

# Recover data from Azure Backup Server

11/18/2019 • 4 minutes to read • [Edit Online](#)

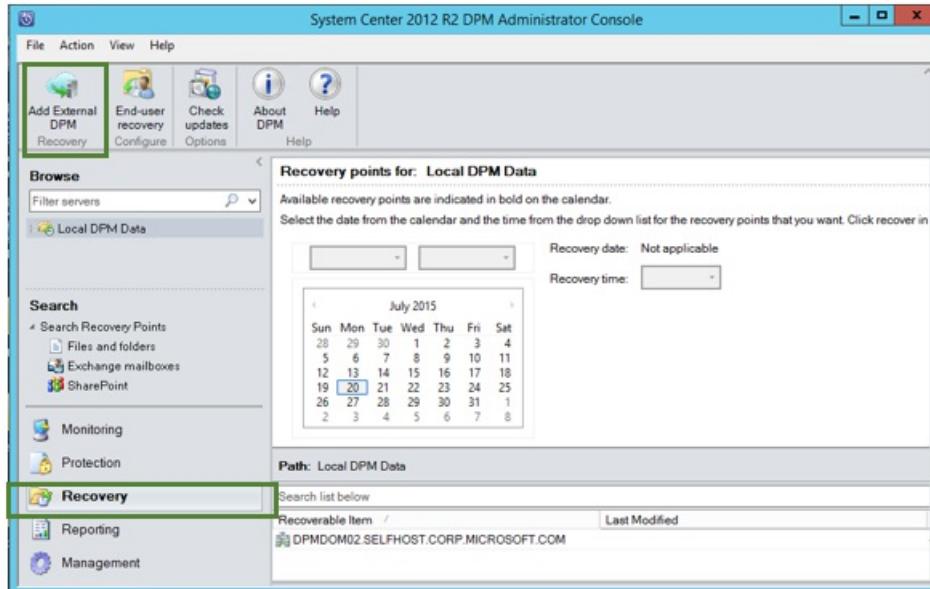
You can use Azure Backup Server to recover the data you've backed up to a Recovery Services vault. The process for doing so is integrated into the Azure Backup Server management console, and is similar to the recovery workflow for other Azure Backup components.

## NOTE

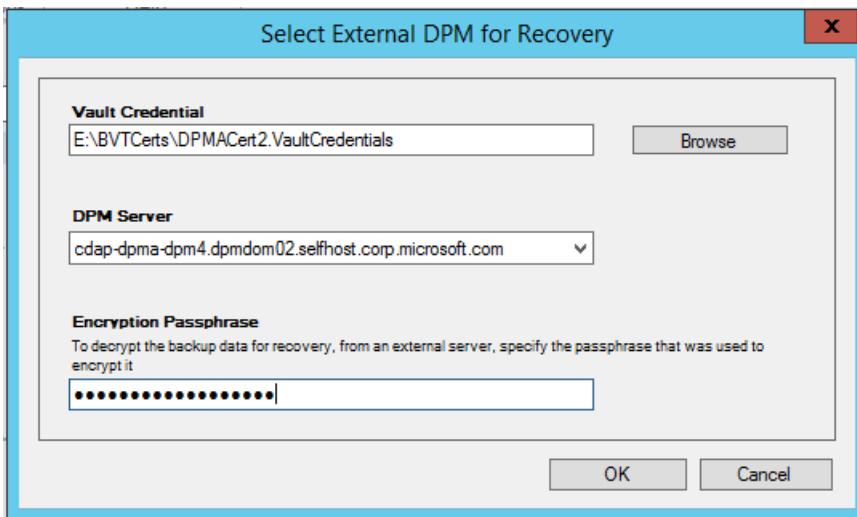
This article is applicable for [System Center Data Protection Manager 2012 R2 with UR7 or later](#), combined with the [latest Azure Backup agent](#).

To recover data from an Azure Backup Server:

- From the **Recovery** tab of the Azure Backup Server management console, click '**Add External DPM**' (at the top left of the screen).



- Download new **vault credentials** from the vault associated with the **Azure Backup Server** where the data is being recovered, choose the Azure Backup Server from the list of Azure Backup Servers registered with the Recovery Services vault, and provide the **encryption passphrase** associated with the server whose data is being recovered.

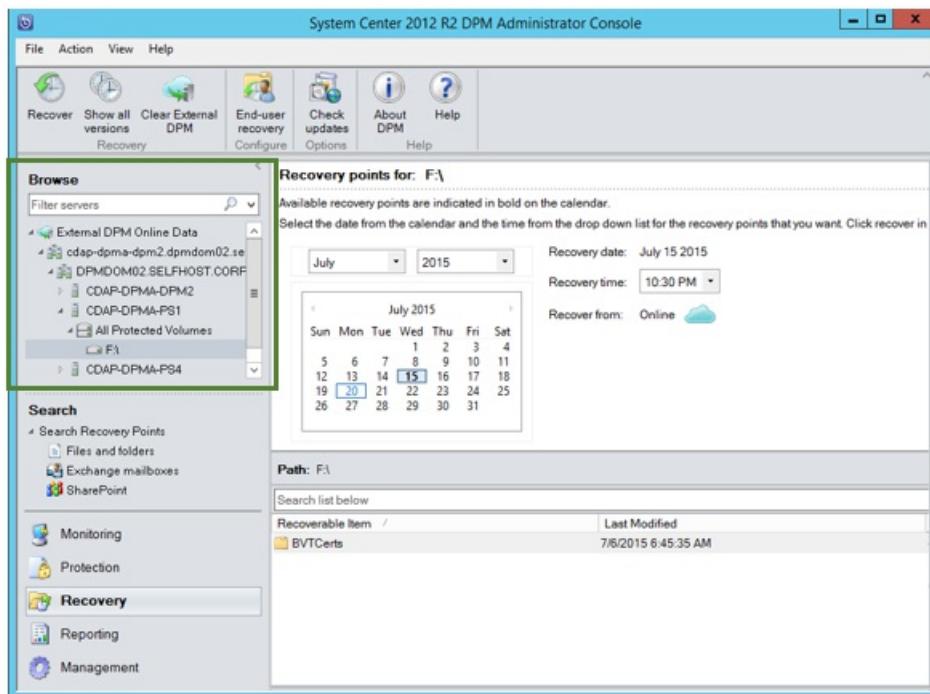


#### NOTE

Only Azure Backup Servers associated with the same registration vault can recover each other's data.

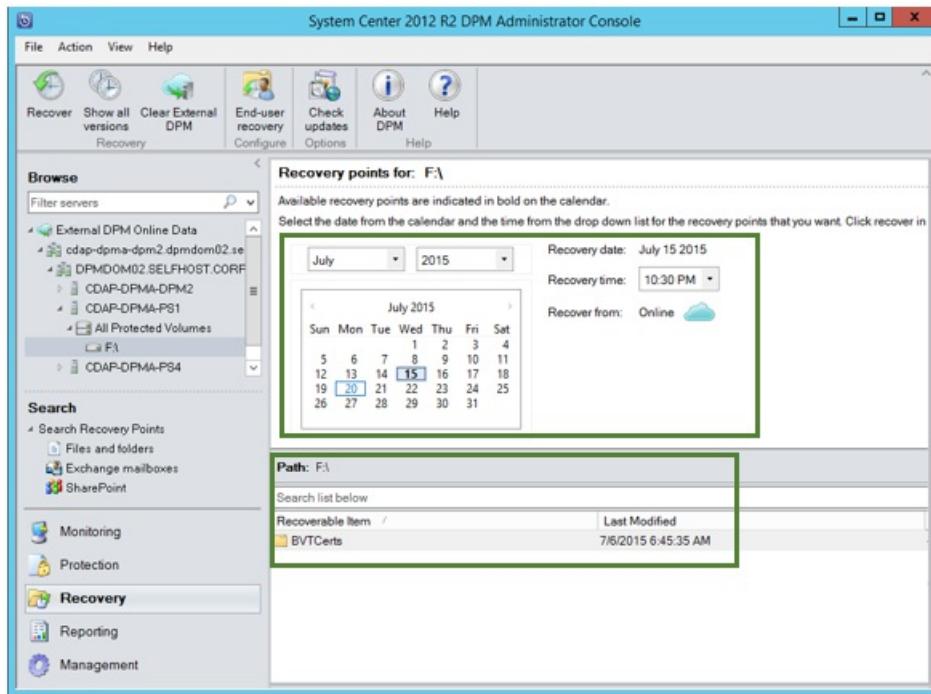
Once the External Azure Backup Server is successfully added, you can browse the data of the external server and the local Azure Backup Server from the **Recovery** tab.

3. Browse the available list of production servers protected by the external Azure Backup Server and select the appropriate data source.

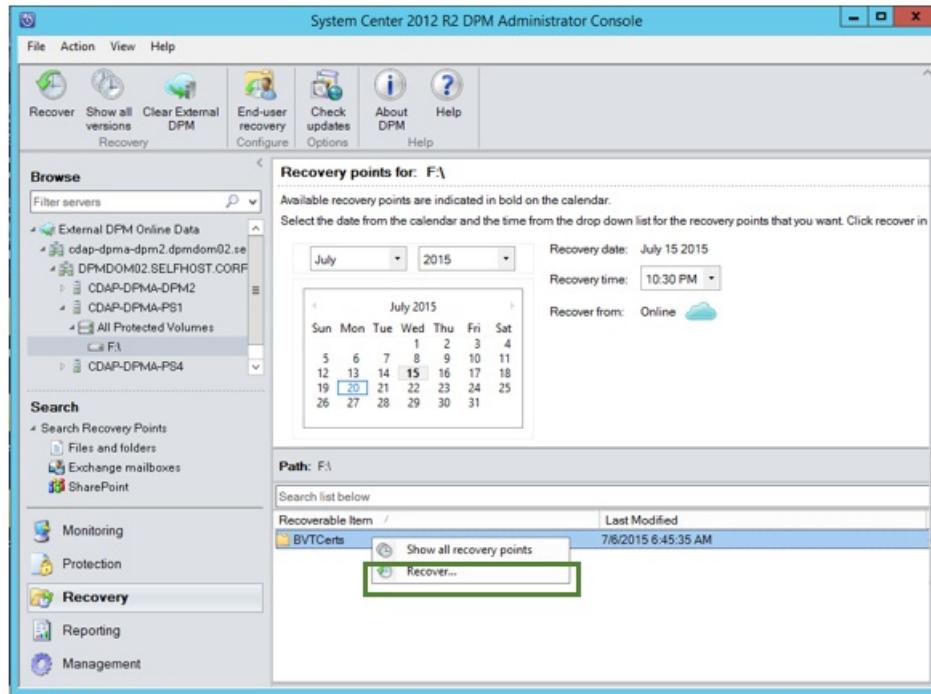


4. Select **the month and year** from the **Recovery points** drop down, select the required **Recovery date** for when the recovery point was created, and select the **Recovery time**.

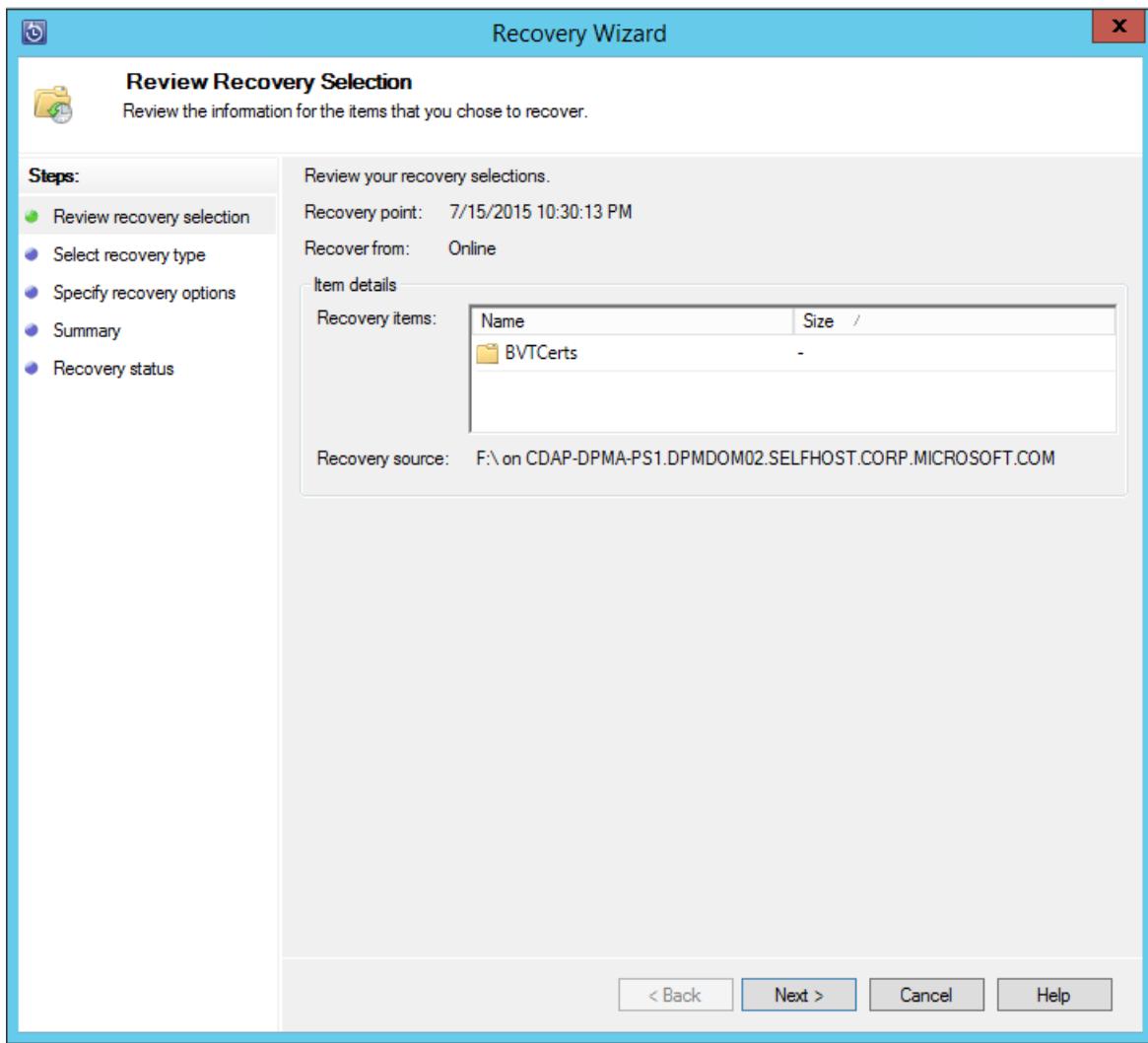
A list of files and folders appears in the bottom pane, which can be browsed and recovered to any location.



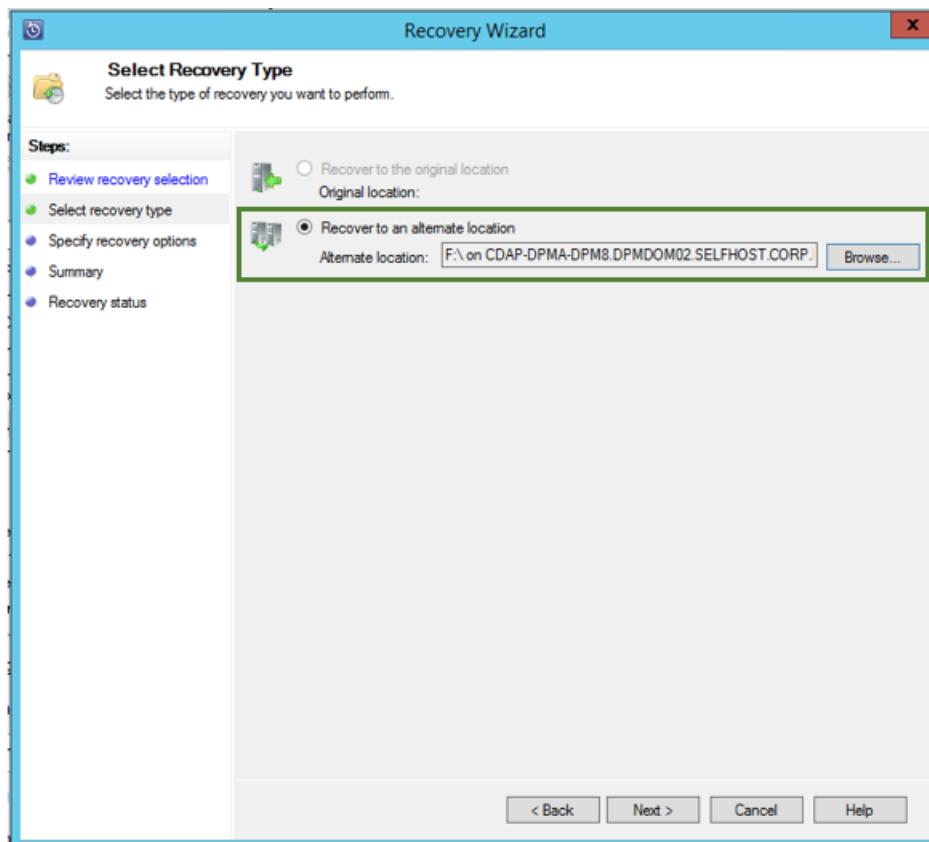
5. Right-click the appropriate item and click **Recover**.



6. Review the **Recover Selection**. Verify the data and time of the backup copy being recovered, as well as the source from which the backup copy was created. If the selection is incorrect, click **Cancel** to navigate back to recovery tab to select appropriate recovery point. If the selection is correct, click **Next**.



7. Select **Recover to an alternate location**. **Browse** to the correct location for the recovery.

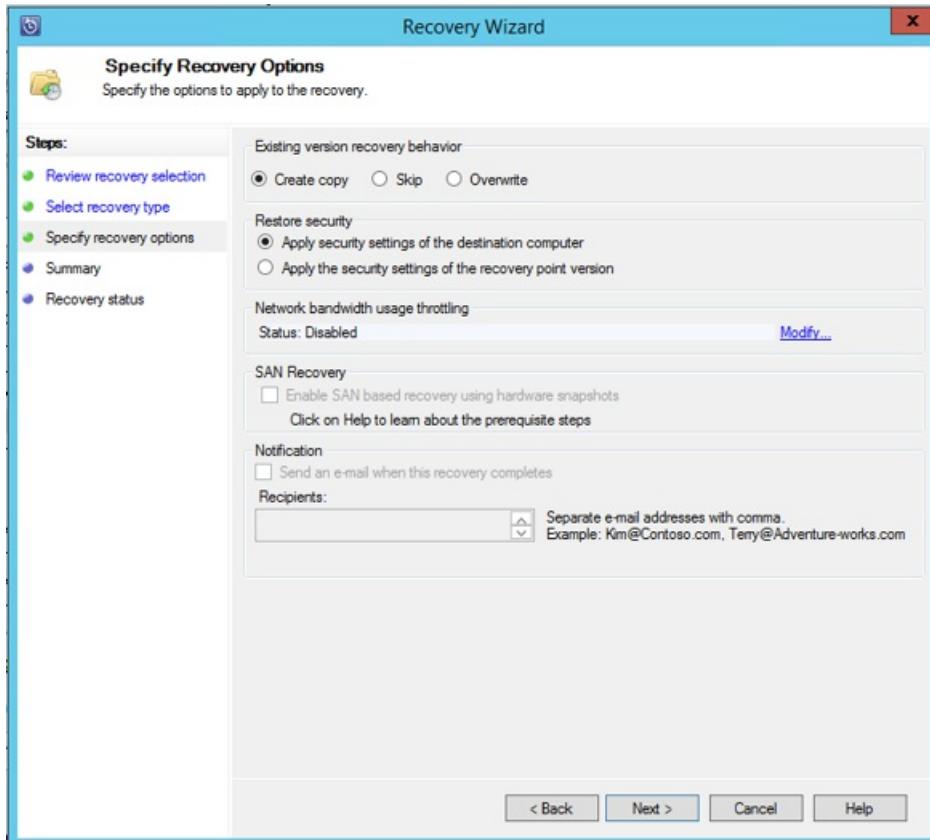


8. Choose the option related to **create copy**, **Skip**, or **Overwrite**.

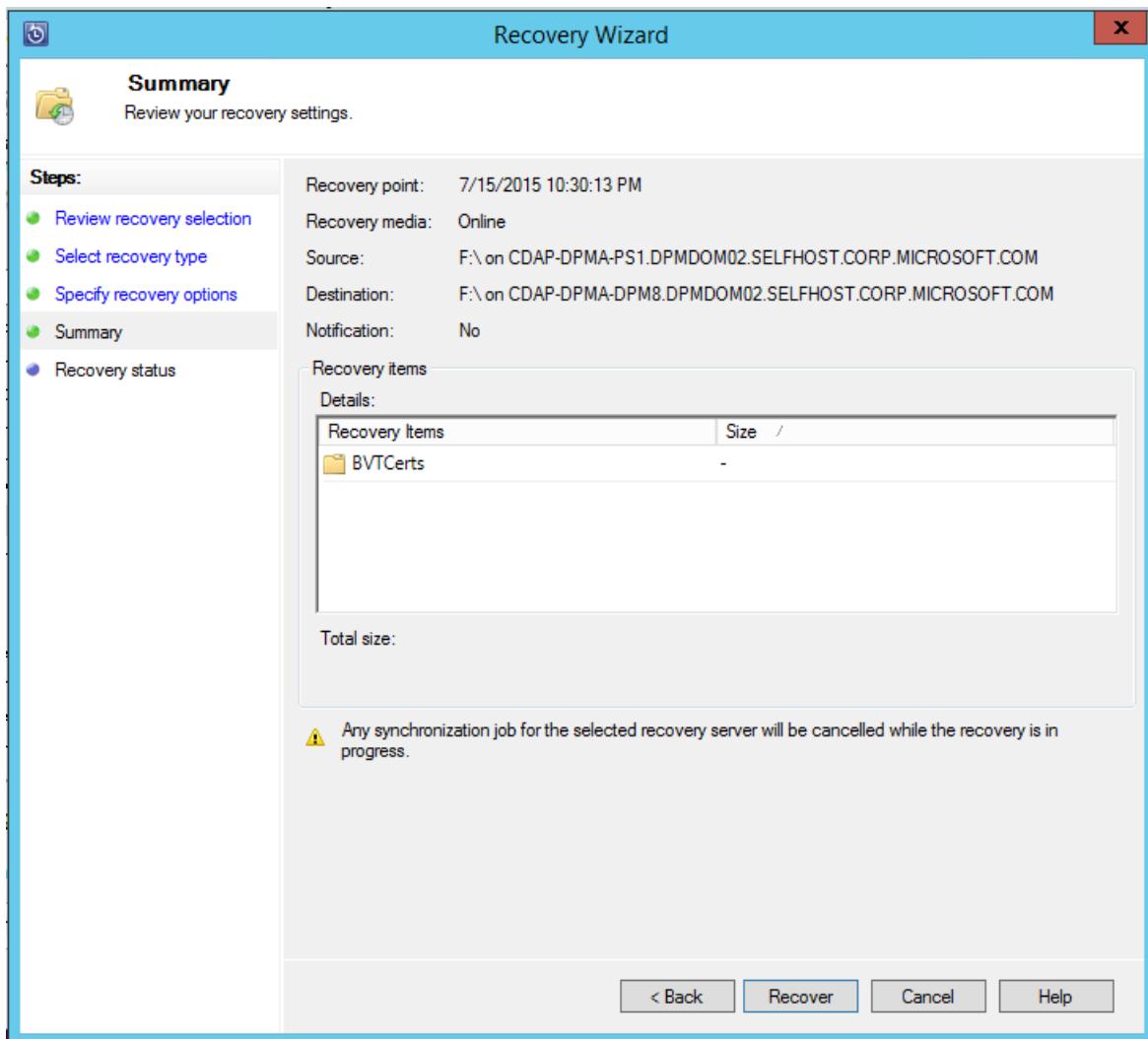
- **Create copy** - creates a copy of the file if there is a name collision.
- **Skip** - if there is a name collision, does not recover the file, which leaves the original file.
- **Overwrite** - if there is a name collision, overwrites the existing copy of the file.

Choose the appropriate option to **Restore security**. You can apply the security settings of the destination computer where the data is being recovered or the security settings that were applicable to product at the time the recovery point was created.

Identify whether a **Notification** is sent, once the recovery successfully completes.

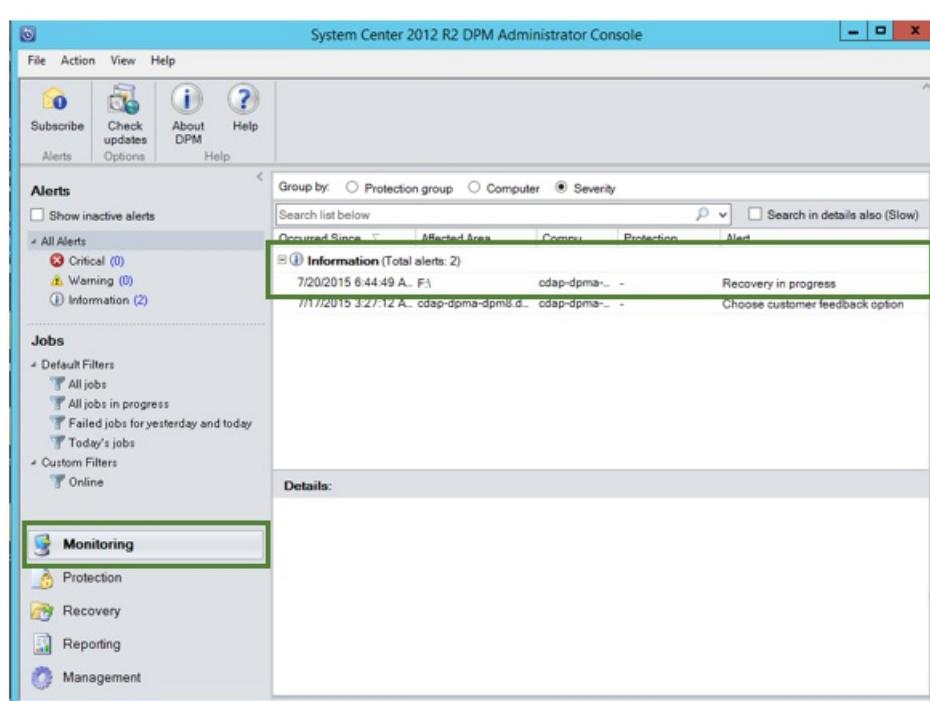


9. The **Summary** screen lists the options chosen so far. Once you click '**Recover**', the data is recovered to the appropriate on-premises location.

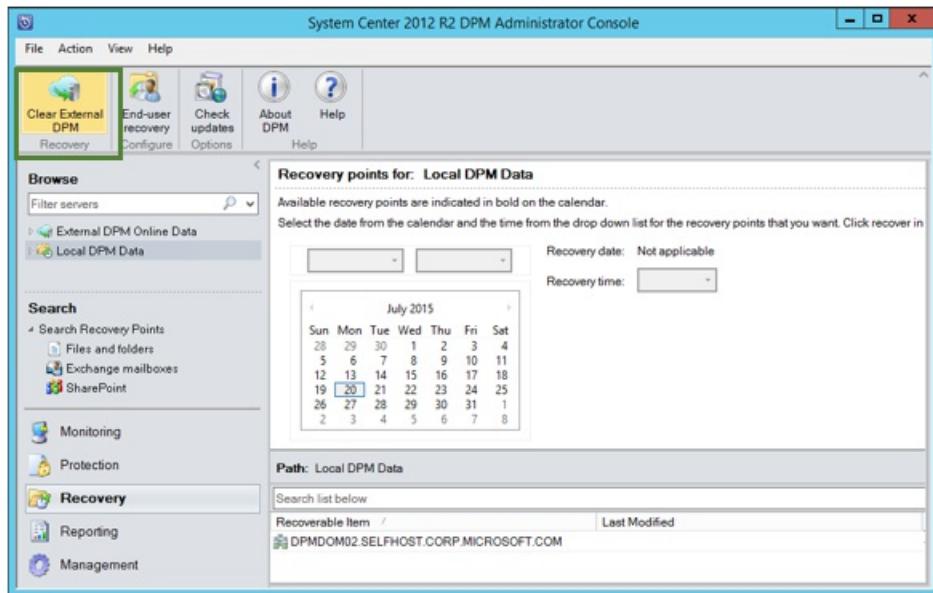


#### NOTE

The recovery job can be monitored in the **Monitoring** tab of the Azure Backup Server.



10. You can click **Clear External DPM** on the **Recovery** tab of the DPM server to remove the view of the external DPM server.



## Troubleshooting error messages

| NO. | ERROR MESSAGE                                                                            | TROUBLESHOOTING STEPS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.  | This server is not registered to the vault specified by the vault credential.            | <p><b>Cause:</b> This error appears when the vault credential file selected does not belong to the Recovery Services vault associated with Azure Backup Server on which the recovery is attempted.</p> <p><b>Resolution:</b> Download the vault credential file from the Recovery Services vault to which the Azure Backup Server is registered.</p>                                                                                                                                                                                                                                                                                                                                                         |
| 2.  | Either the recoverable data is not available or the selected server is not a DPM server. | <p><b>Cause:</b> There are no other Azure Backup Servers registered to the Recovery Services vault, or the servers have not yet uploaded the metadata, or the selected server is not an Azure Backup Server (using Windows Server or Windows Client).</p> <p><b>Resolution:</b> If there are other Azure Backup Servers registered to the Recovery Services vault, ensure that the latest Azure Backup agent is installed. If there are other Azure Backup Servers registered to the Recovery Services vault, wait for a day after installation to start the recovery process. The nightly job will upload the metadata for all the protected backups to cloud. The data will be available for recovery.</p> |

| NO. | ERROR MESSAGE                                                                                                                         | TROUBLESHOOTING STEPS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3.  | No other DPM server is registered to this vault.                                                                                      | <p><b>Cause:</b> There are no other Azure Backup Servers that are registered to the vault from which the recovery is being attempted.</p> <p><b>Resolution:</b> If there are other Azure Backup Servers registered to the Recovery Services vault, ensure that the latest Azure Backup agent is installed. If there are other Azure Backup Servers registered to the Recovery Services vault, wait for a day after installation to start the recovery process. The nightly job uploads the metadata for all protected backups to cloud. The data will be available for recovery.</p> |
| 4.  | The encryption passphrase provided does not match with passphrase associated with the following server:<br><b>&lt;server name&gt;</b> | <p><b>Cause:</b> The encryption passphrase used in the process of encrypting the data from the Azure Backup Server's data that is being recovered does not match the encryption passphrase provided. The agent is unable to decrypt the data. Hence the recovery fails.</p> <p><b>Resolution:</b> Please provide the exact same encryption passphrase associated with the Azure Backup Server whose data is being recovered.</p>                                                                                                                                                     |

## Next steps

Read the other FAQs:

- [Common questions](#) about Azure VM backups
- [Common questions](#) about the Azure Backup agent

# Back up SQL Server to Azure as a DPM workload

2/20/2020 • 6 minutes to read • [Edit Online](#)

This article leads you through the configuration steps to back up SQL Server databases by using Azure Backup.

To back up SQL Server databases to Azure, you need an Azure account. If you don't have one, you can create a free account in just a few minutes. For more information, see [Create your Azure free account](#).

To back up a SQL Server database to Azure and to recover it from Azure:

1. Create a backup policy to protect SQL Server databases in Azure.
2. Create on-demand backup copies in Azure.
3. Recover the database from Azure.

## Before you start

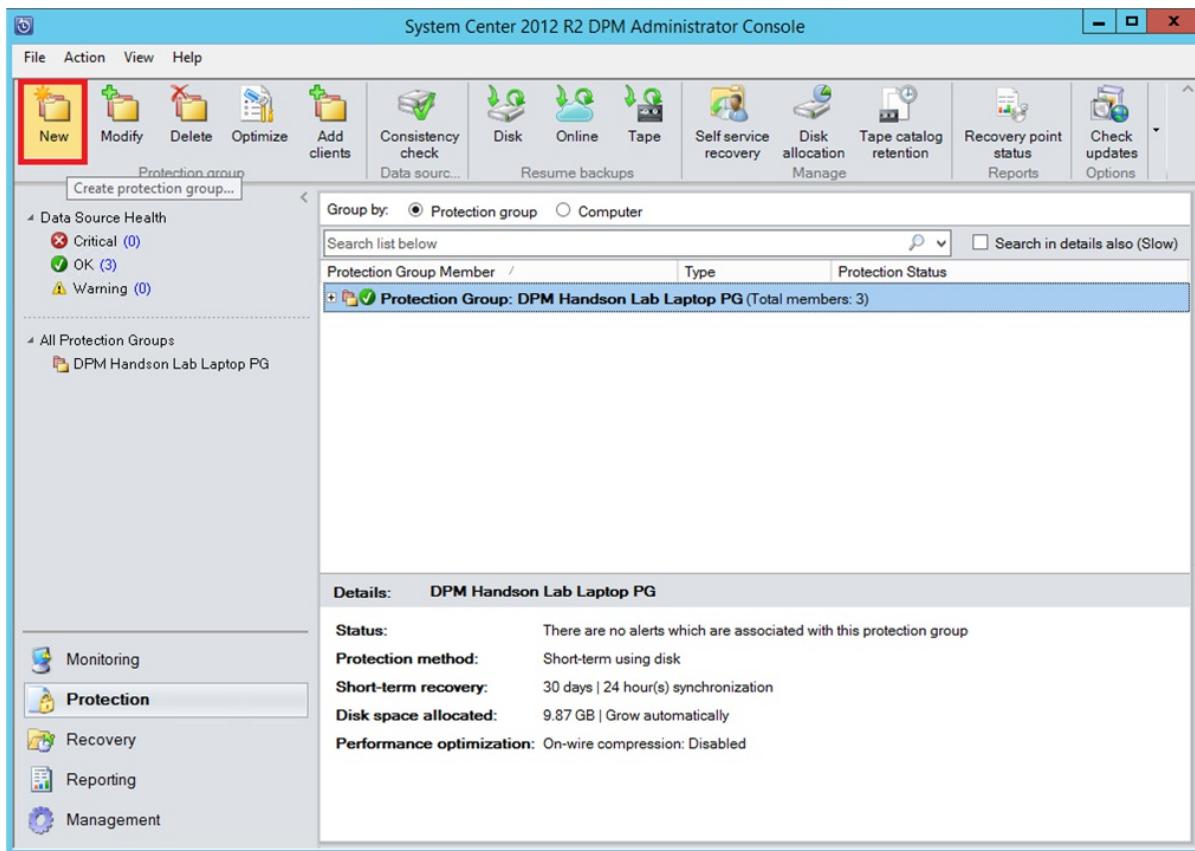
Before you begin, ensure you've met the [prerequisites](#) for using Azure Backup to protect workloads. Here are some of the prerequisite tasks:

- Create a backup vault.
- Download vault credentials.
- Install the Azure Backup agent.
- Register the server with the vault.

## Create a backup policy

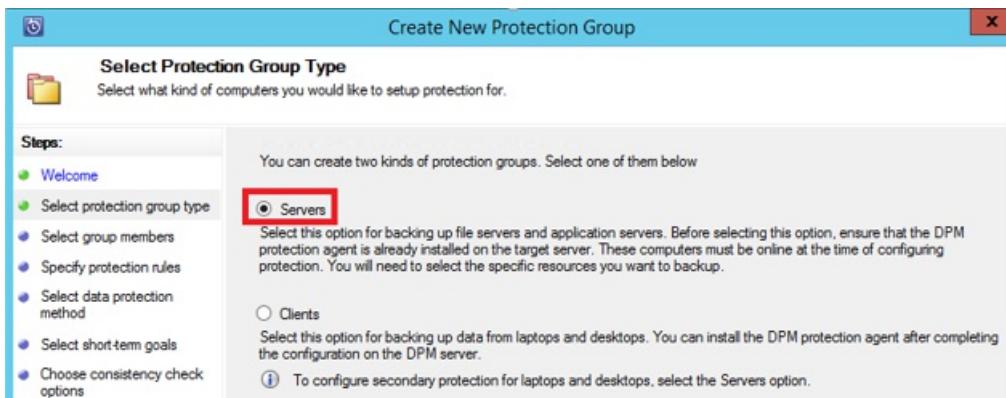
To protect SQL Server databases in Azure, first create a backup policy:

1. On the Data Protection Manager (DPM) server, select the **Protection** workspace.
2. Select **New** to create a protection group.

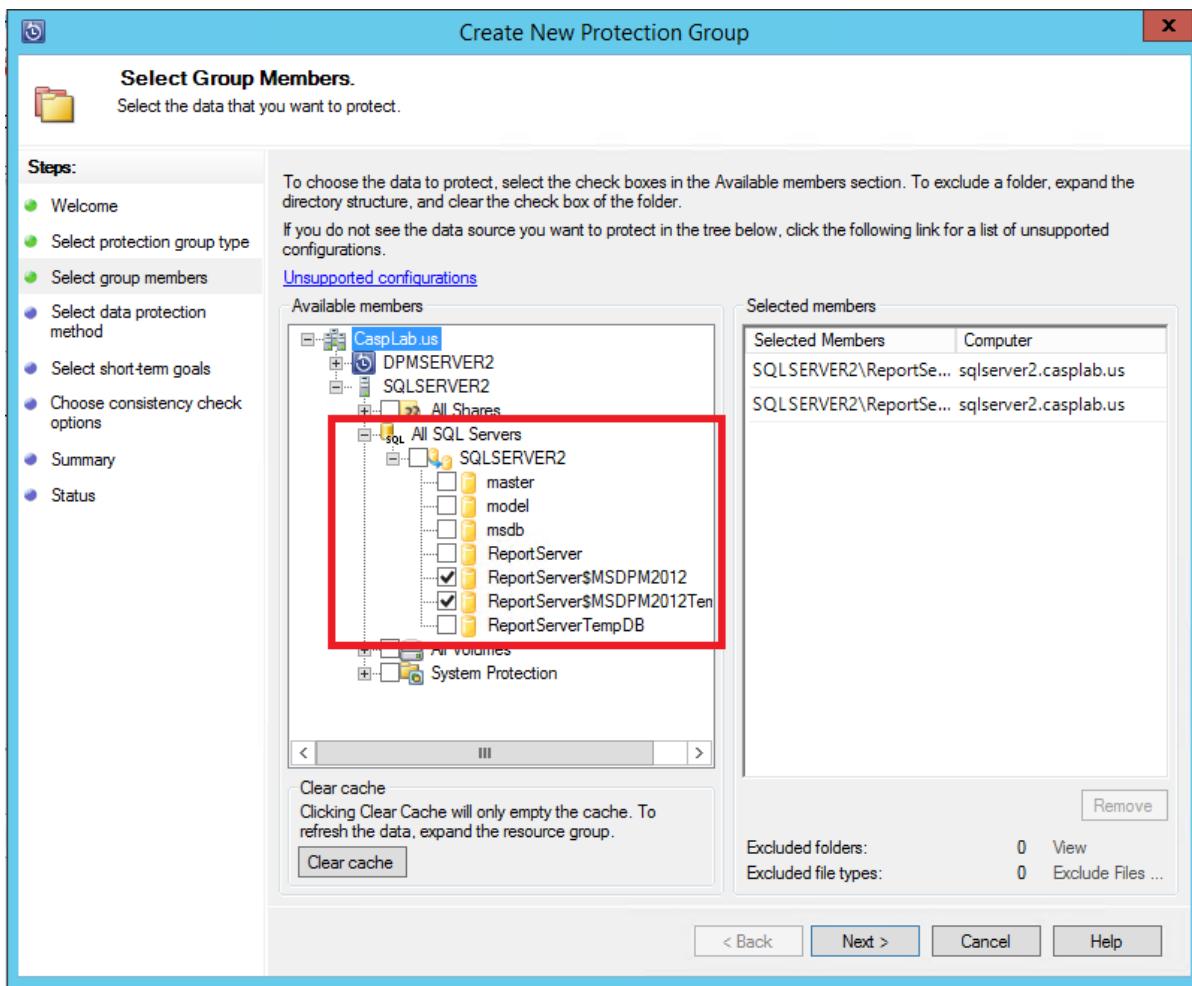


3. On the start page, review the guidance about creating a protection group. Then select **Next**.

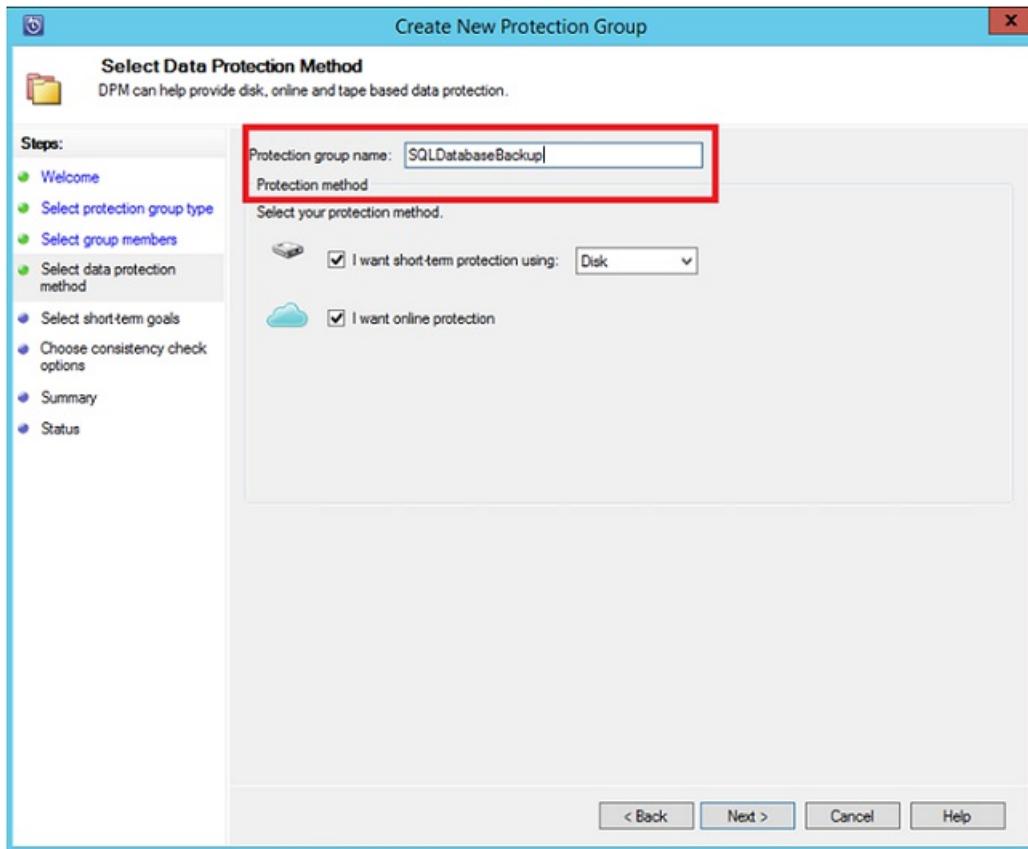
4. Select **Servers**.



5. Expand the SQL Server machine where the databases that you want to back up are located. You see the data sources that can be backed up from that server. Expand **All SQL Shares** and then select the databases that you want to back up. In this example, we select ReportServer\$MSDPM2012 and ReportServer\$MSDPM2012TempDB. Then select **Next**.



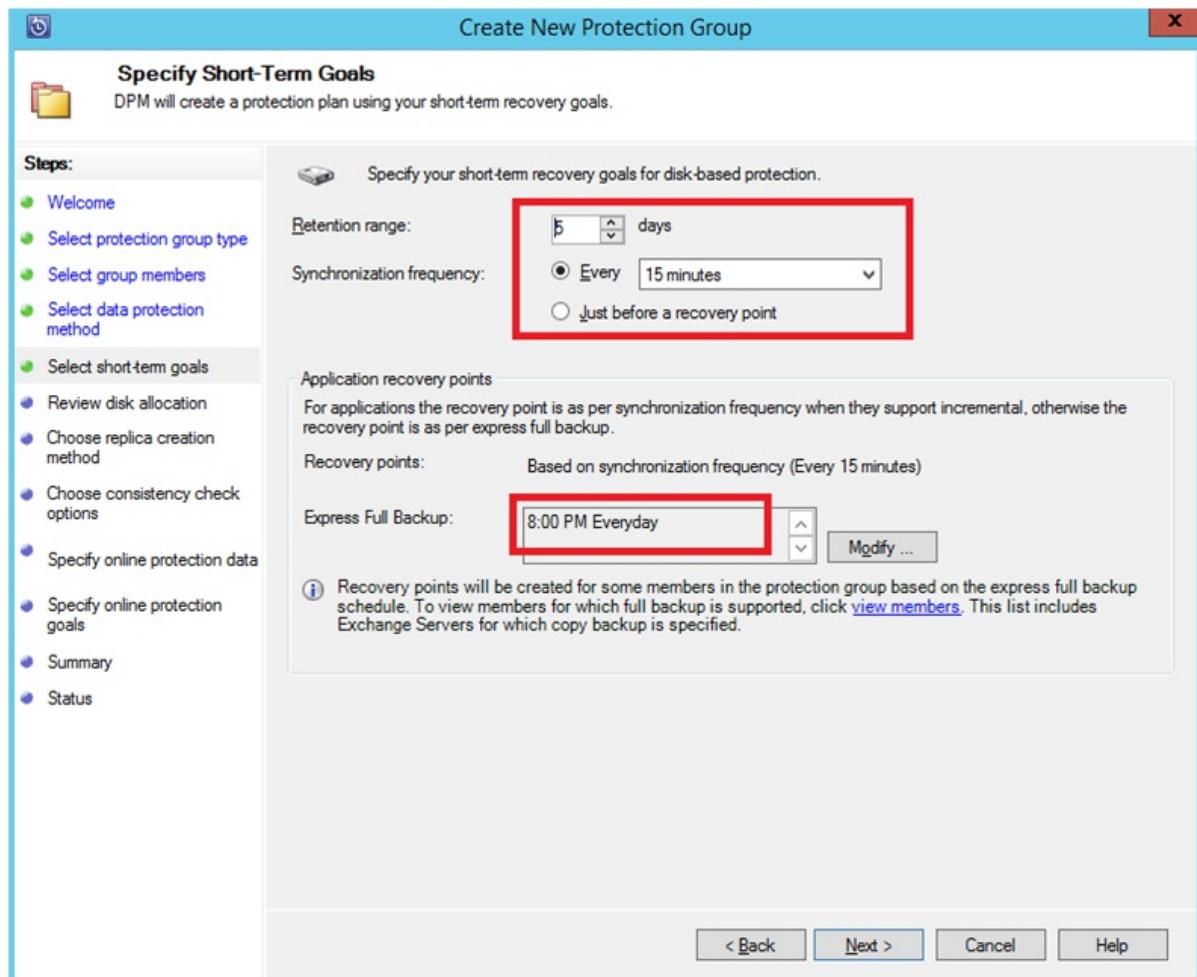
6. Name the protection group and then select **I want online protection**.



7. On the **Specify Short-Term Goals** page, include the necessary inputs to create backup points to the disk.

In this example, **Retention range** is set to **5 days**. The backup **Synchronization frequency** is set to once

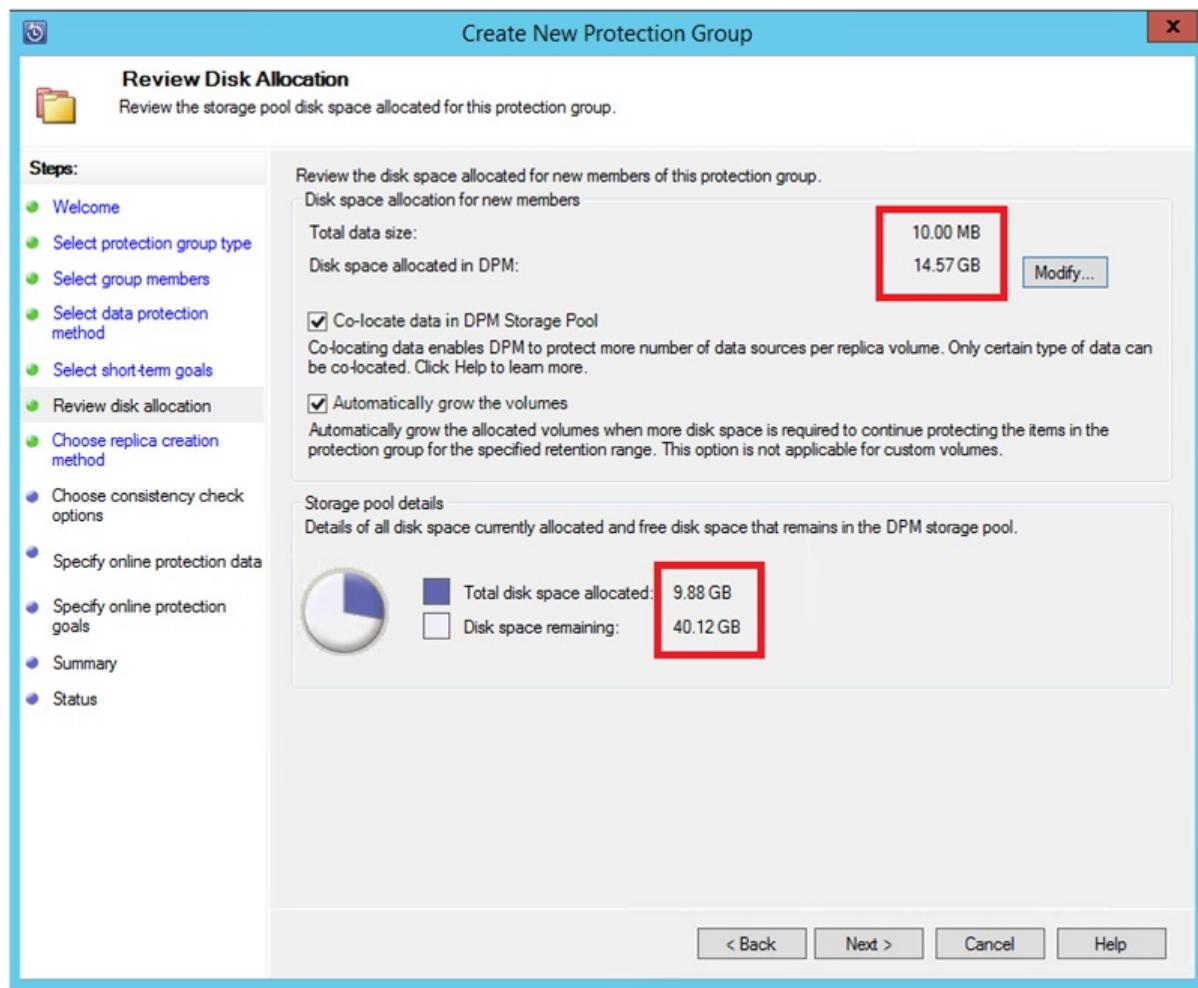
every 15 minutes. **Express Full Backup** is set to 8:00 PM.



#### NOTE

In this example, a backup point is created at 8:00 PM every day. The data that has been modified since the previous day's 8:00 PM backup point is transferred. This process is called **Express Full Backup**. Although the transaction logs are synchronized every 15 minutes, if we need to recover the database at 9:00 PM, then the point is created by replaying the logs from the last express full backup point, which is 8:00 PM in this example.

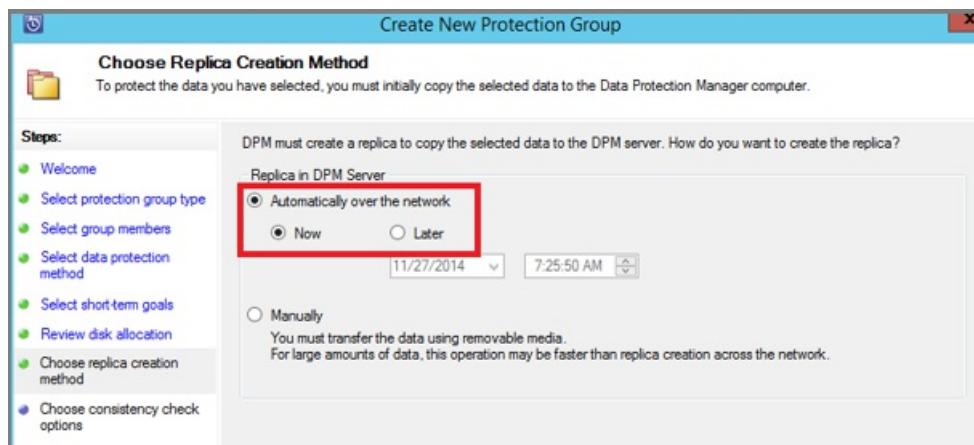
8. Select **Next**. DPM shows the overall storage space available. It also shows the potential disk space utilization.



By default, DPM creates one volume per data source (SQL Server database). The volume is used for the initial backup copy. In this configuration, Logical Disk Manager (LDM) limits DPM protection to 300 data sources (SQL Server databases). To work around this limitation, select **Co-locate data in DPM Storage Pool**. If you use this option, DPM uses a single volume for multiple data sources. This setup allows DPM to protect up to 2,000 SQL Server databases.

If you select **Automatically grow the volumes**, then DPM can account for the increased backup volume as the production data grows. If you don't select **Automatically grow the volumes**, then DPM limits the backup storage to the data sources in the protection group.

9. If you're an administrator, you can choose to transfer this initial backup **Automatically over the network** and choose the time of transfer. Or choose to **Manually** transfer the backup. Then select **Next**.

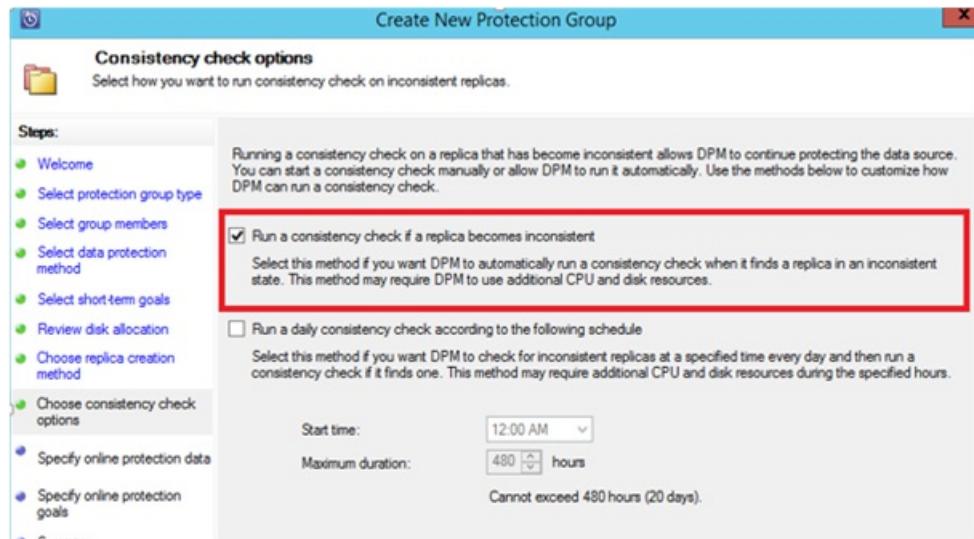


The initial backup copy requires the transfer of the entire data source (SQL Server database). The backup data moves from the production server (SQL Server machine) to the DPM server. If this backup is large, then transferring the data over the network could cause bandwidth congestion. For this reason,

administrators can choose to use removable media to transfer the initial backup **Manually**. Or they can transfer the data **Automatically over the network** at a specified time.

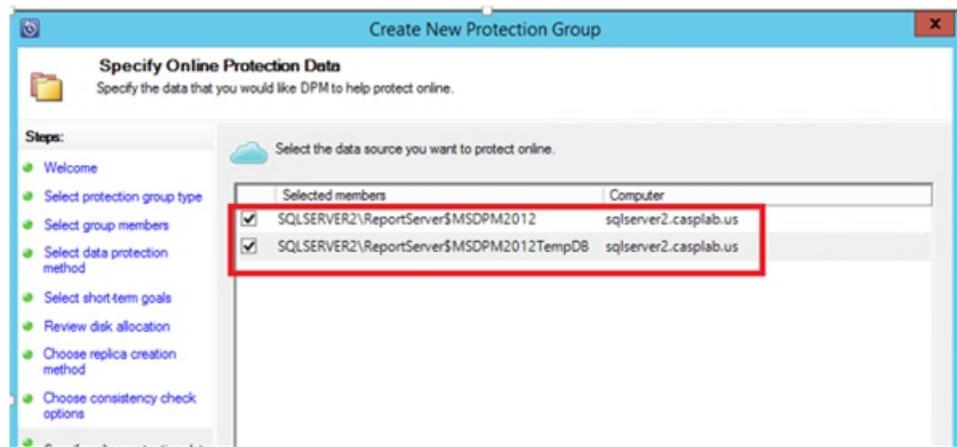
After the initial backup finishes, backups continue incrementally on the initial backup copy. Incremental backups tend to be small and are easily transferred across the network.

10. Choose when to run a consistency check. Then select **Next**.

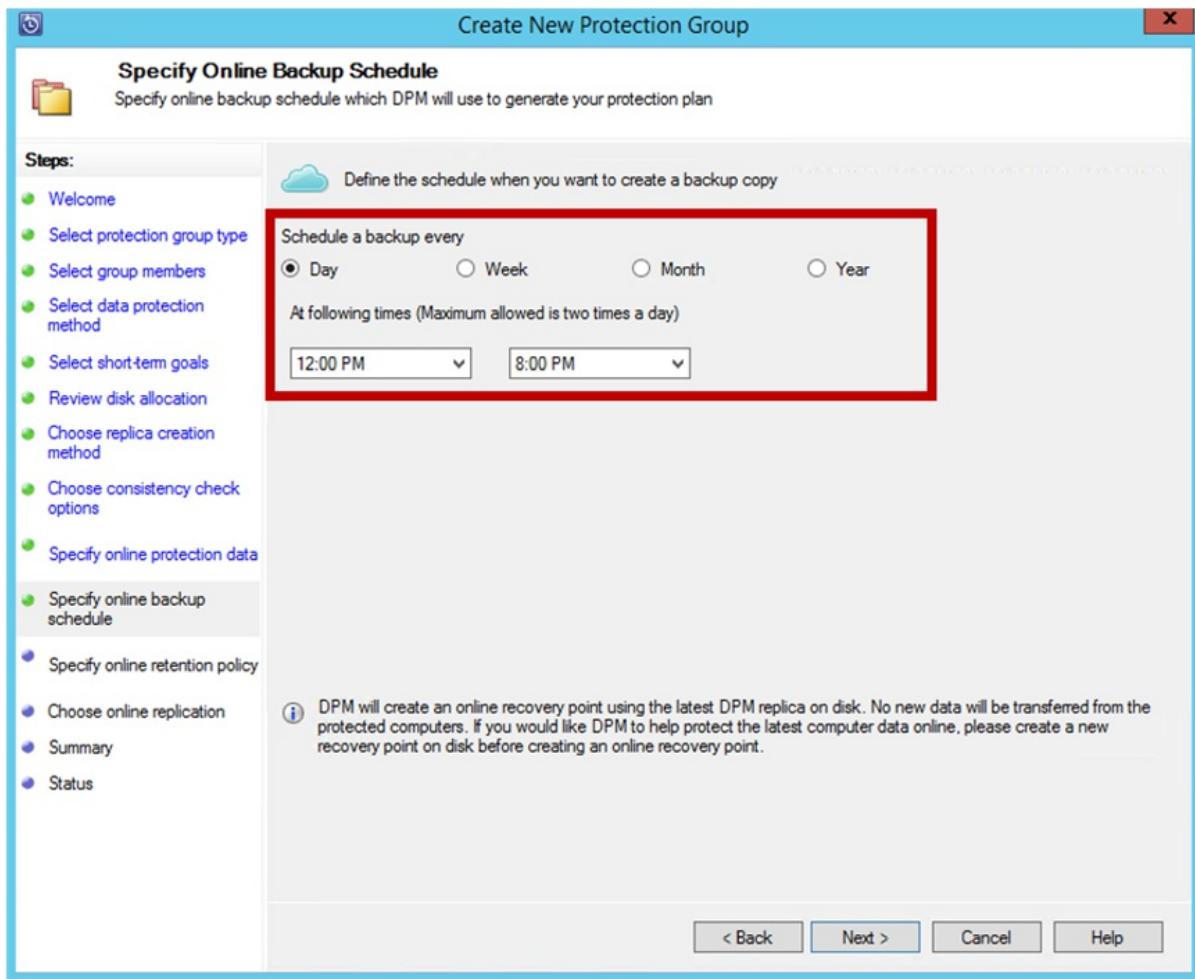


DPM can run a consistency check on the integrity of the backup point. It calculates the checksum of the backup file on the production server (the SQL Server machine in this example) and the backed-up data for that file in DPM. If the check finds a conflict, then the backed-up file in DPM is assumed to be corrupt. DPM fixes the backed-up data by sending the blocks that correspond to the checksum mismatch. Because the consistency check is a performance-intensive operation, administrators can choose to schedule the consistency check or run it automatically.

11. Select the data sources to protect in Azure. Then select **Next**.



12. If you're an administrator, you can choose backup schedules and retention policies that suit your organization's policies.



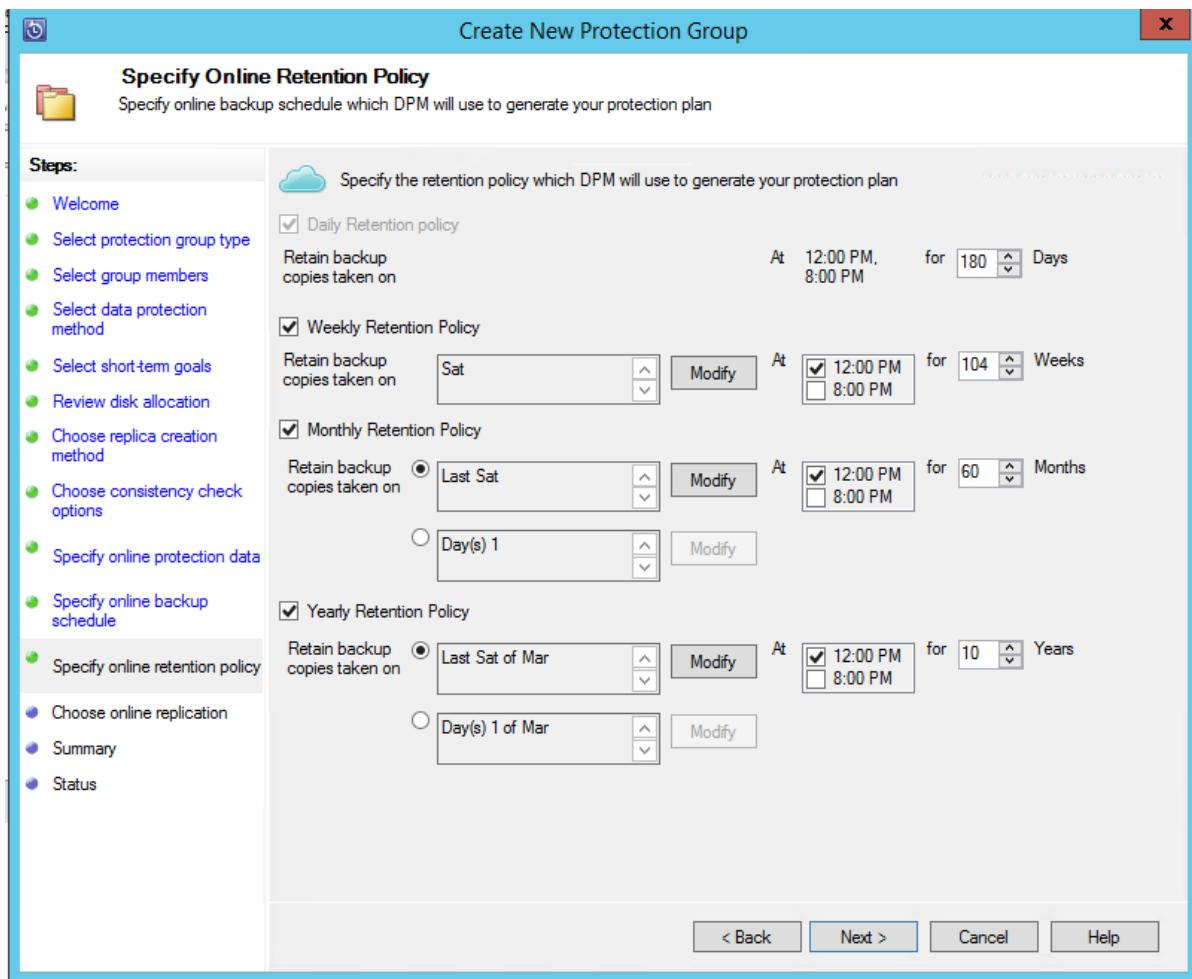
In this example, backups are taken daily at 12:00 PM and 8:00 PM.

**TIP**

For quick recovery, keep a few short-term recovery points on your disk. These recovery points are used for operational recovery. Azure serves as a good offsite location, providing higher SLAs and guaranteed availability.

Use DPM to schedule Azure Backups after the local disk backups finish. When you follow this practice, the latest disk backup is copied to Azure.

13. Choose the retention policy schedule. For more information about how the retention policy works, see [Use Azure Backup to replace your tape infrastructure](#).



In this example:

- Backups are taken daily at 12:00 PM and 8:00 PM. They're kept for 180 days.
- The backup on Saturday at 12:00 PM is kept for 104 weeks.
- The backup from the last Saturday of the month at 12:00 PM is kept for 60 months.
- The backup from the last Saturday of March at 12:00 PM is kept for 10 years.

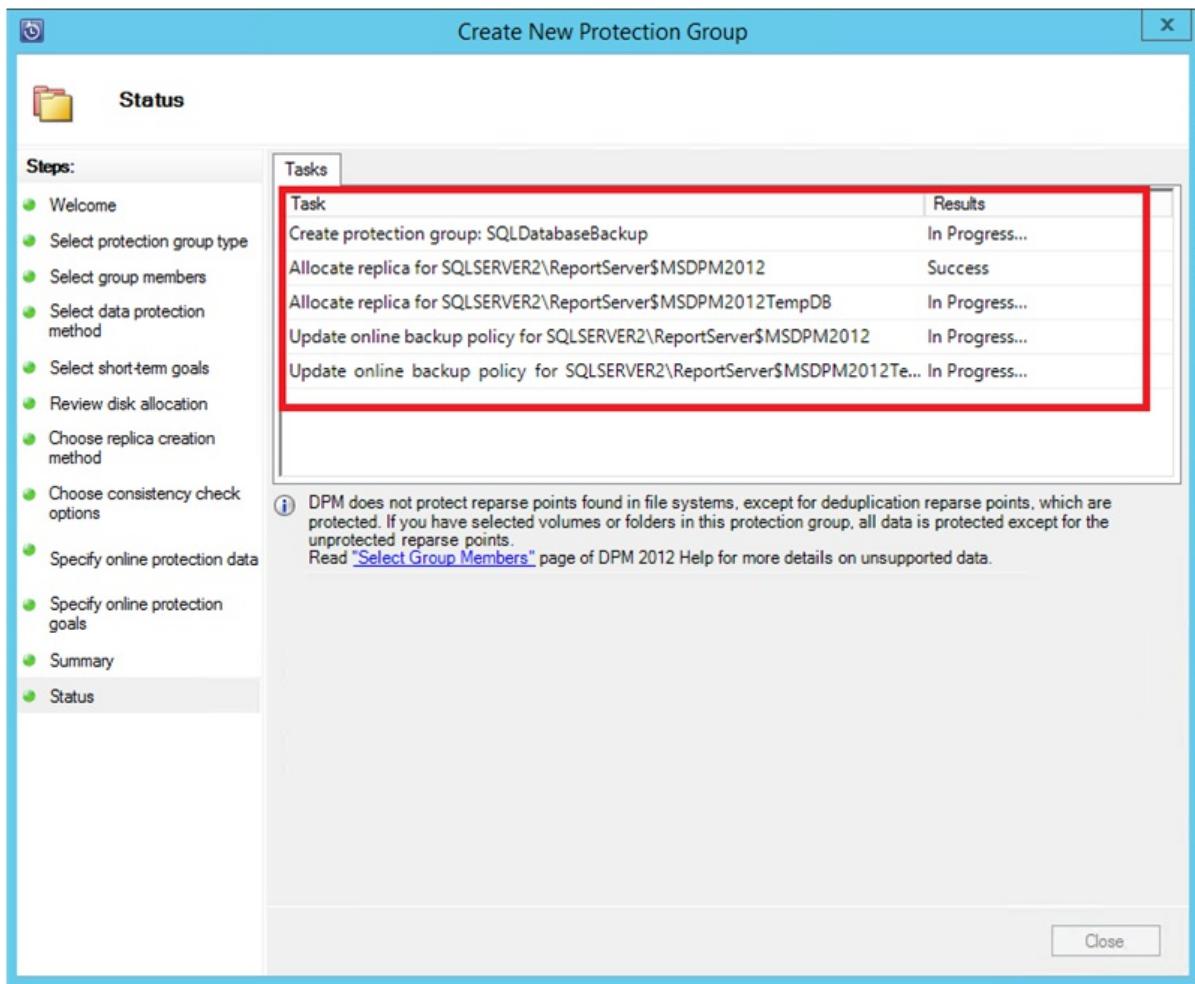
After you choose a retention policy, select **Next**.

14. Choose how to transfer the initial backup copy to Azure.

- The **Automatically over the network** option follows your backup schedule to transfer the data to Azure.
- For more information about **Offline Backup**, see [Overview of Offline Backup](#).

After you choose a transfer mechanism, select **Next**.

15. On the **Summary** page, review the policy details. Then select **Create group**. You can select **Close** and watch the job progress in the **Monitoring** workspace.



## Create on-demand backup copies of a SQL Server database

A recovery point is created when the first backup occurs. Rather than waiting for the schedule to run, you can manually trigger the creation of a recovery point:

1. In the protection group, make sure the database status is **OK**.

| Protection Group: SQLDatabaseBackup (Total members: 2) |          |    |
|--------------------------------------------------------|----------|----|
| Computer: sqlserver2.casplab.us                        | SQL Data | OK |
|                                                        | SQL Data | OK |

**Details:** SQLSERVER2\ReportServer\$MSDPM2012

**Status:** OK

**Replica path:** [Click to view details](#)

**Latest recovery point:** 12/5/2014 4:21:54 AM

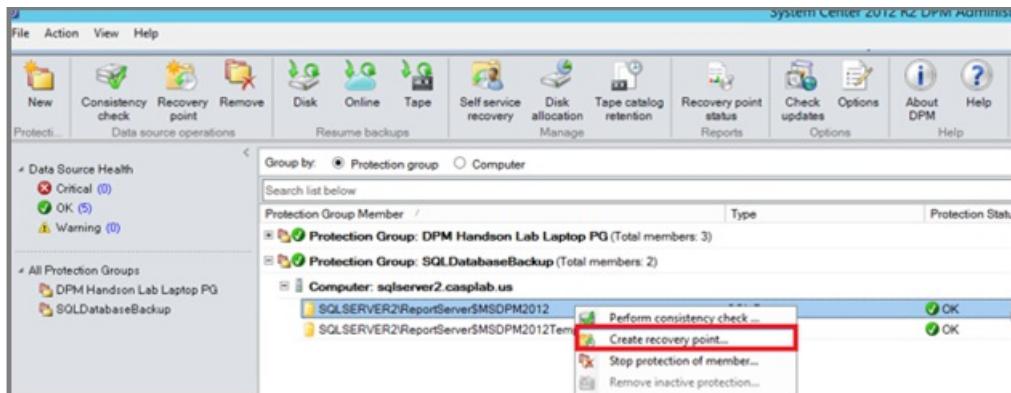
**Oldest recovery point:** 12/5/2014 4:21:54 AM

**Total recovery points:** 1

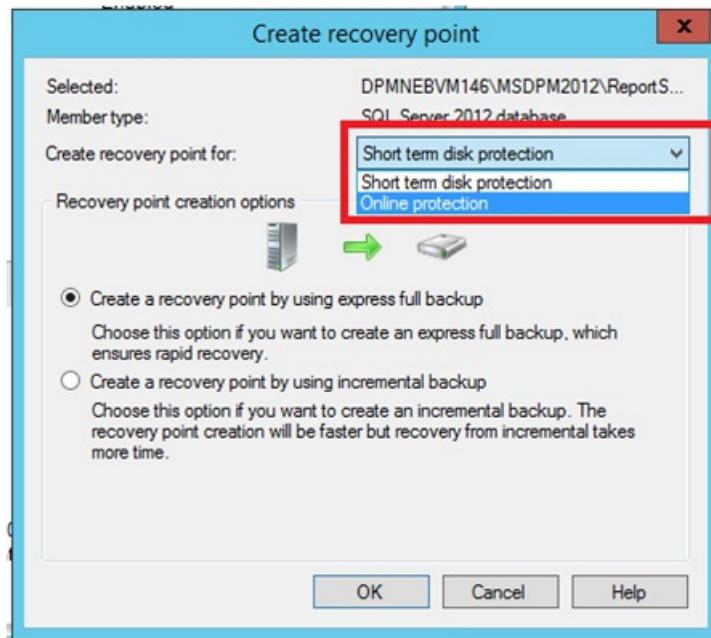
**Disk allocation:** Replica volume (co-located): 10.00 GB allocated, 93.29 MB used  
Recovery point volume (co-located): 4.57 GB allocated, 60.27 MB used

**Parent instance:** SQLSERVER2

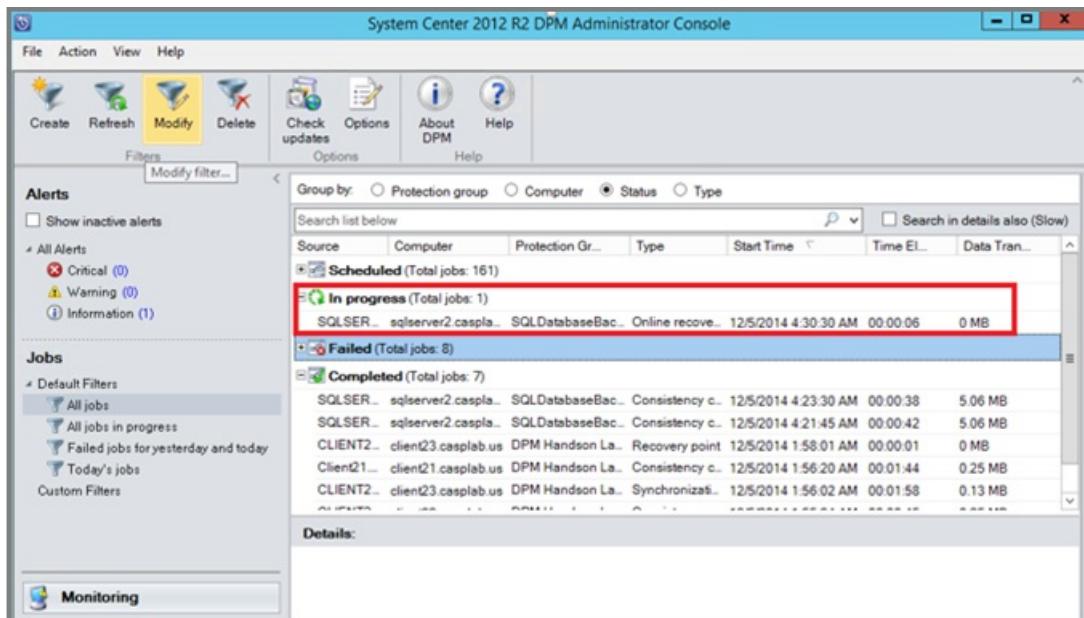
2. Right-click the database and then select **Create recovery point**.



3. In the drop-down menu, select **Online protection**. Then select **OK** to start the creation of a recovery point in Azure.



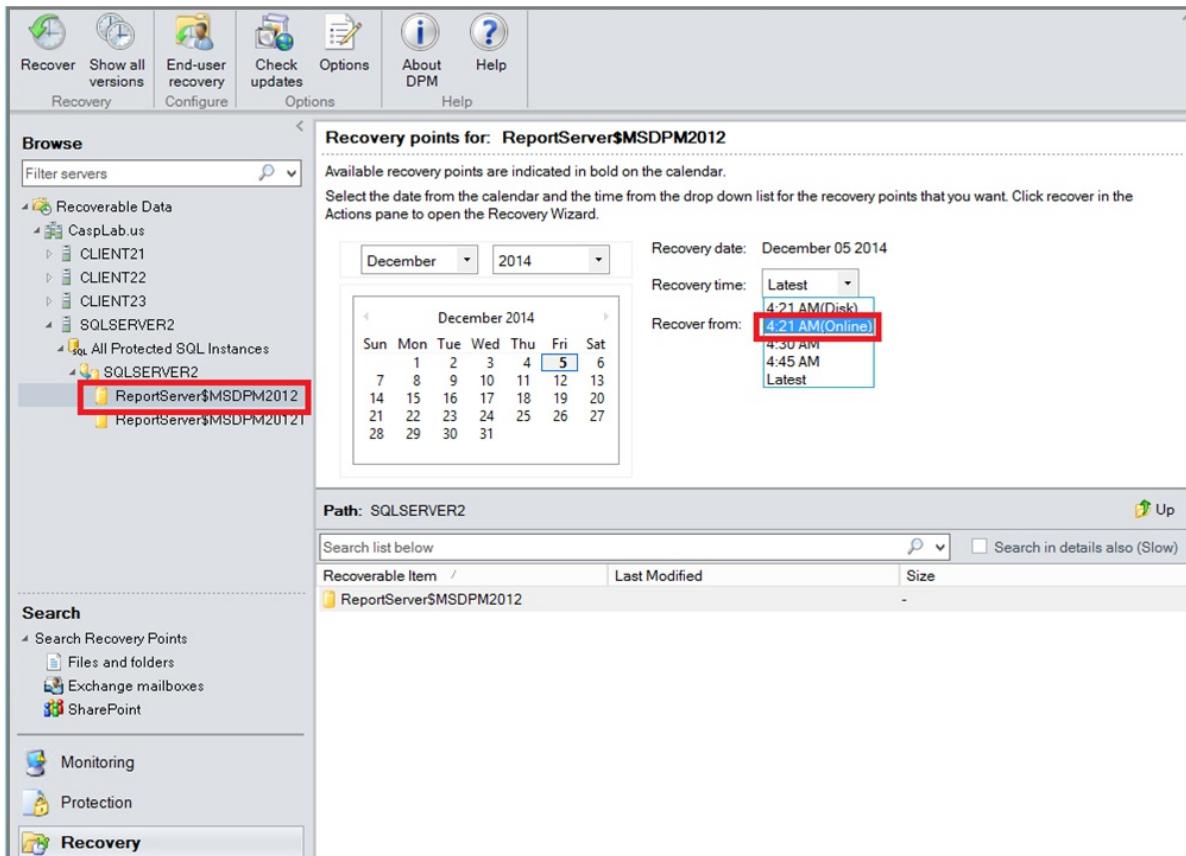
4. You can view the job progress in the **Monitoring** workspace.



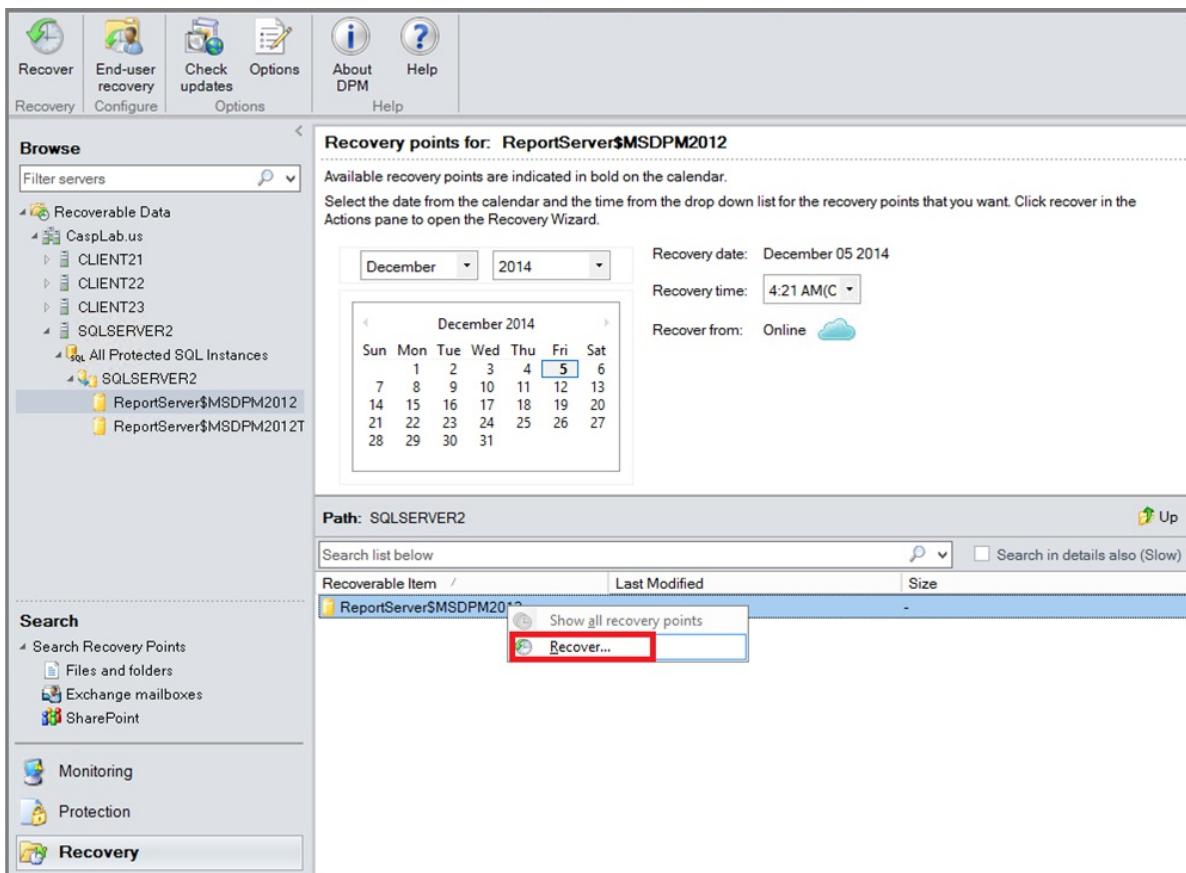
## Recover a SQL Server database from Azure

To recover a protected entity, such as a SQL Server database, from Azure:

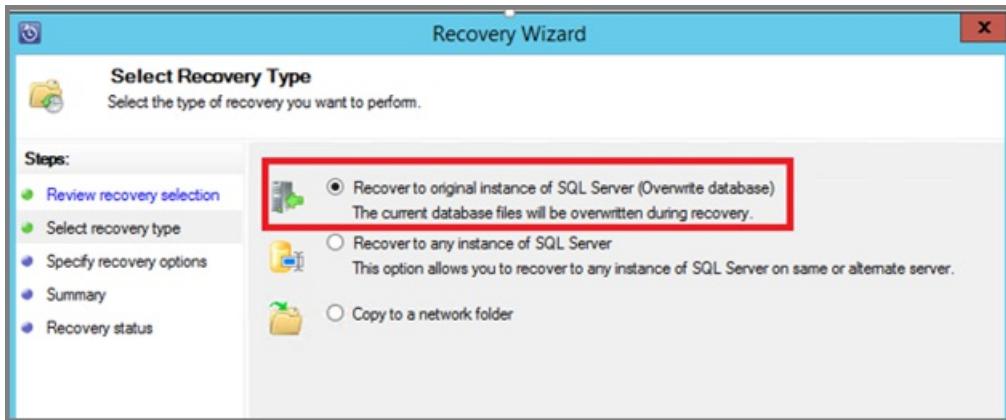
1. Open the DPM server management console. Go to the **Recovery** workspace to see the servers that DPM backs up. Select the database (in this example, ReportServer\$MSDPM2012). Select a **Recovery time** that ends with **Online**.



2. Right-click the database name and select **Recover**.



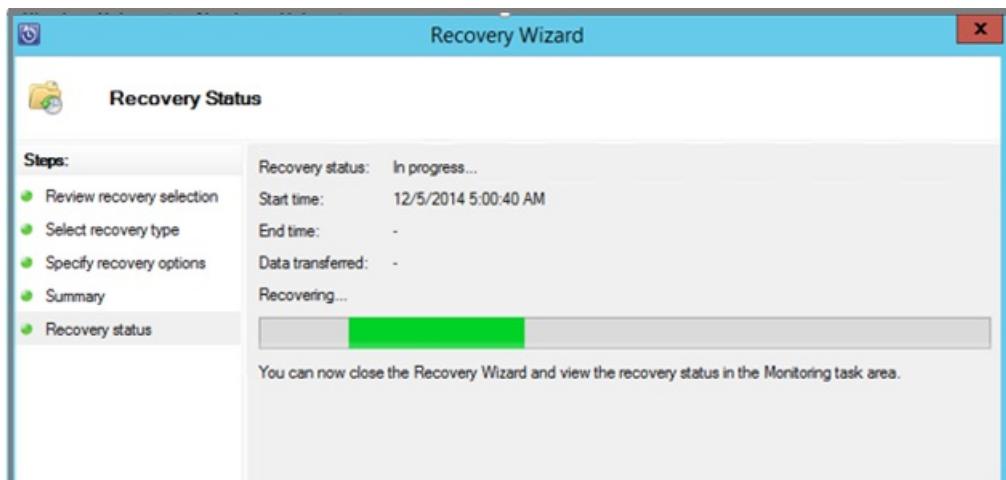
3. DPM shows the details of the recovery point. Select **Next**. To overwrite the database, select the recovery type **Recover to original instance of SQL Server**. Then select **Next**.



In this example, DPM allows the database to be recovered to another SQL Server instance or to a standalone network folder.

4. On the **Specify Recovery Options** page, you can select the recovery options. For example, you can choose **Network bandwidth usage throttling** to throttle the bandwidth that recovery uses. Then select **Next**.
5. On the **Summary** page, you see the current recovery configuration. Select **Recover**.

The recovery status shows the database being recovered. You can select **Close** to close the wizard and view the progress in the **Monitoring** workspace.



When the recovery is complete, the restored database is consistent with the application.

## Next steps

For more information, see [Azure Backup FAQ](#).

# Back up a SharePoint farm to Azure with DPM

2/24/2020 • 9 minutes to read • [Edit Online](#)

You back up a SharePoint farm to Microsoft Azure by using System Center Data Protection Manager (DPM) in much the same way that you back up other data sources. Azure Backup provides flexibility in the backup schedule to create daily, weekly, monthly, or yearly backup points and gives you retention policy options for various backup points. DPM provides the capability to store local disk copies for quick recovery-time objectives (RTO) and to store copies to Azure for economical, long-term retention.

## SharePoint supported versions and related protection scenarios

Azure Backup for DPM supports the following scenarios:

| WORKLOAD   | VERSION                                                                    | SHAREPOINT DEPLOYMENT                                                                               | DPM DEPLOYMENT TYPE                                    | DPM - SYSTEM CENTER 2012 R2                   | PROTECTION AND RECOVERY                                                                                                                                                    |
|------------|----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|--------------------------------------------------------|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SharePoint | SharePoint 2013,<br>SharePoint 2010,<br>SharePoint 2007,<br>SharePoint 3.0 | SharePoint deployed as a physical server or Hyper-V/VMware virtual machine<br>-----<br>SQL AlwaysOn | Physical server or on-premises Hyper-V virtual machine | Supports backup to Azure from Update Rollup 5 | Protect SharePoint Farm recovery options: Recovery farm, database, and file or list item from disk recovery points. Farm and database recovery from Azure recovery points. |

## Before you start

There are a few things you need to confirm before you back up a SharePoint farm to Azure.

### Prerequisites

Before you proceed, make sure that you have met all the [prerequisites for using Microsoft Azure Backup](#) to protect workloads. Some tasks for prerequisites include: create a backup vault, download vault credentials, install Azure Backup Agent, and register DPM/Azure Backup Server with the vault.

### DPM agent

The DPM agent must be installed on the server that's running SharePoint, the servers that are running SQL Server, and all other servers that are part of the SharePoint farm. For more information about how to set up the protection agent, see [Setup Protection Agent](#). The one exception is that you install the agent only on a single web front end (WFE) server. DPM needs the agent on one WFE server only to serve as the entry point for protection.

### SharePoint farm

For every 10 million items in the farm, there must be at least 2 GB of space on the volume where the DPM folder is located. This space is required for catalog generation. For DPM to recover specific items (site collections, sites, lists, document libraries, folders, individual documents, and list items), catalog generation creates a list of the URLs that are contained within each content database. You can view the list of URLs in the recoverable item pane in the **Recovery** task area of DPM Administrator Console.

### SQL Server

DPM runs as a LocalSystem account. To back up SQL Server databases, DPM needs sysadmin privileges on that account for the server that's running SQL Server. Set NT AUTHORITY\SYSTEM to *sysadmin* on the server that's running SQL Server before you back it up.

If the SharePoint farm has SQL Server databases that are configured with SQL Server aliases, install the SQL Server client components on the front-end Web server that DPM will protect.

## SharePoint Server

While performance depends on many factors such as size of SharePoint farm, as general guidance one DPM server can protect a 25-TB SharePoint farm.

## DPM Update Rollup 5

To begin protection of a SharePoint farm to Azure, you need to install DPM Update Rollup 5 or later. Update Rollup 5 provides the ability to protect a SharePoint farm to Azure if the farm is configured by using SQL AlwaysOn. For more information, see the blog post that introduces [DPM Update Rollup 5](#)

## What's not supported

- DPM that protects a SharePoint farm does not protect search indexes or application service databases. You will need to configure the protection of these databases separately.
- DPM does not provide backup of SharePoint SQL Server databases that are hosted on scale-out file server (SOFS) shares.

## Configure SharePoint protection

Before you can use DPM to protect SharePoint, you must configure the SharePoint VSS Writer service (WSS Writer service) by using **ConfigureSharePoint.exe**.

You can find **ConfigureSharePoint.exe** in the [DPM Installation Path]\bin folder on the front-end web server. This tool provides the protection agent with the credentials for the SharePoint farm. You run it on a single WFE server. If you have multiple WFE servers, select just one when you configure a protection group.

### To configure the SharePoint VSS Writer service

1. On the WFE server, at a command prompt, go to [DPM installation location]\bin\
2. Enter ConfigureSharePoint -EnableSharePointProtection.
3. Enter the farm administrator credentials. This account should be a member of the local Administrator group on the WFE server. If the farm administrator isn't a local admin grant the following permissions on the WFE server:
  - Grant the WSS\_Admin\_WPG group full control to the DPM folder (%Program Files%\Microsoft Data Protection Manager\DPM).
  - Grant the WSS\_Admin\_WPG group read access to the DPM Registry key (HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager).

#### NOTE

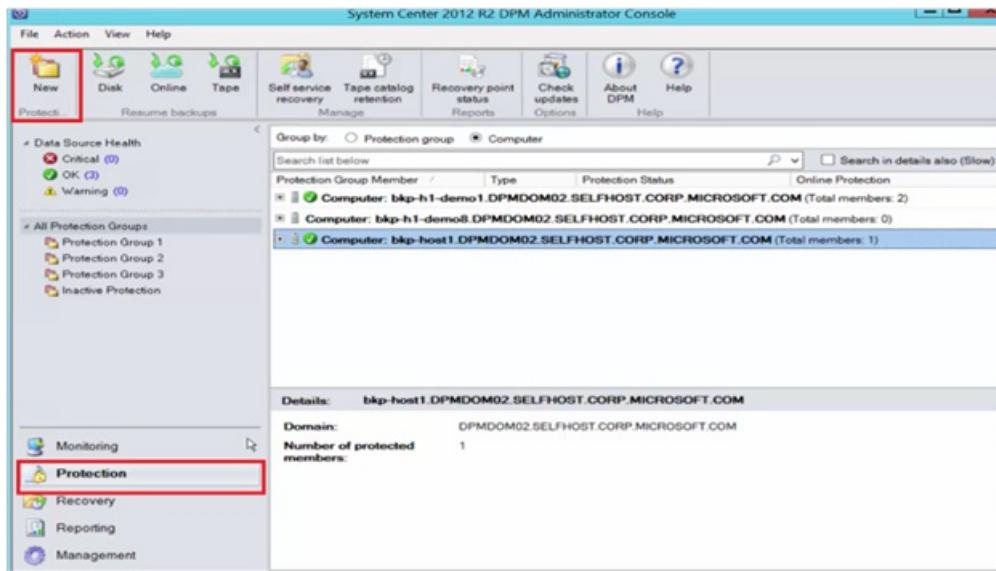
You'll need to rerun ConfigureSharePoint.exe whenever there's a change in the SharePoint farm administrator credentials.

## Back up a SharePoint farm by using DPM

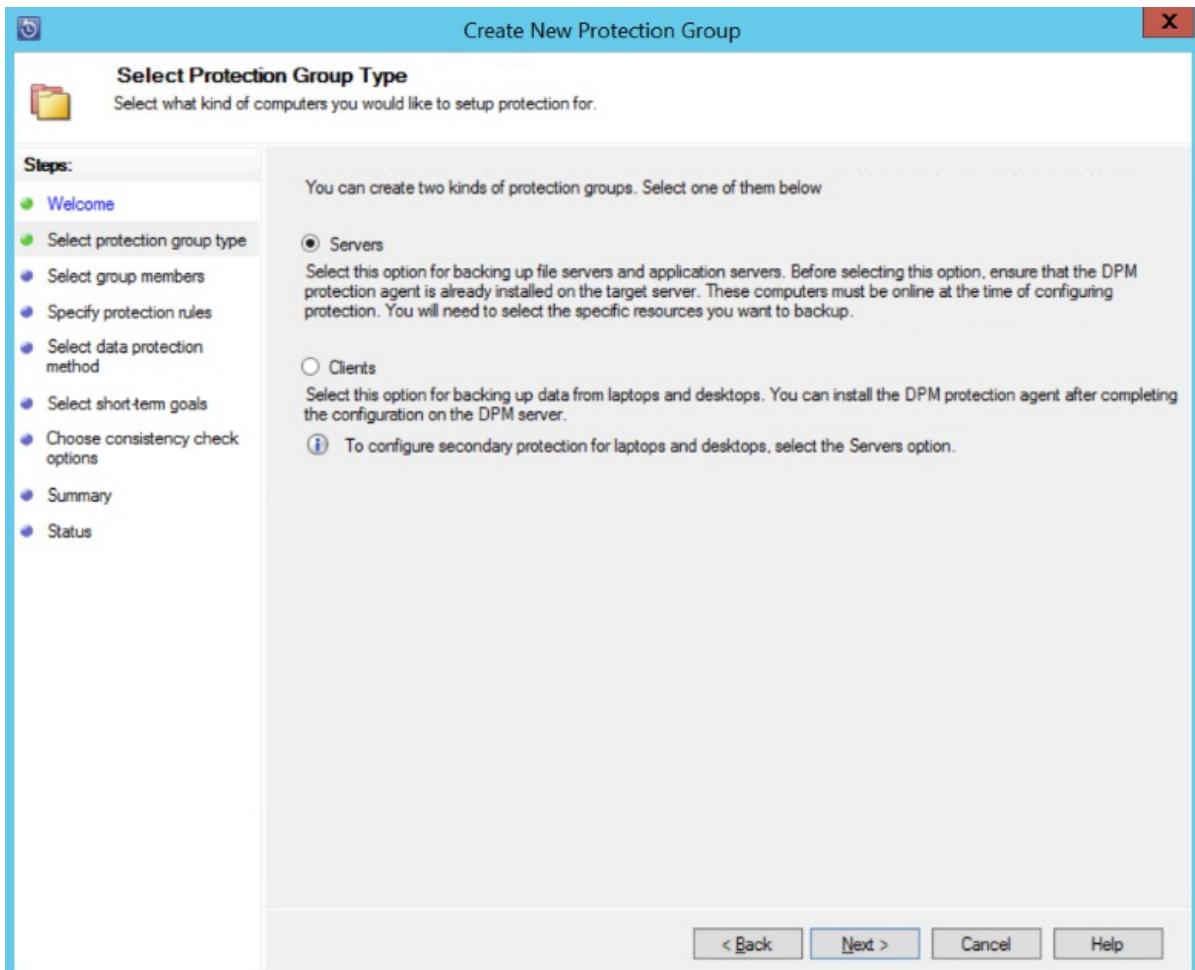
After you have configured DPM and the SharePoint farm as explained previously, SharePoint can be protected by DPM.

### To protect a SharePoint farm

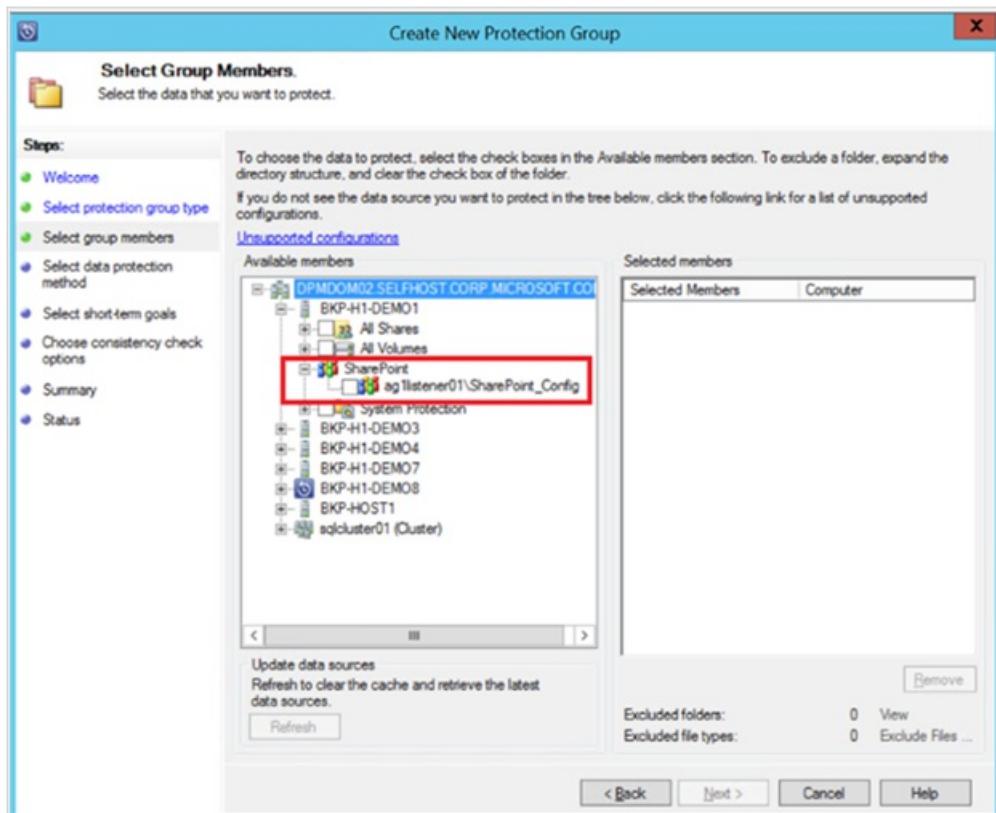
1. From the **Protection** tab of the DPM Administrator Console, click **New**.



2. On the **Select Protection Group Type** page of the **Create New Protection Group** wizard, select **Servers**, and then click **Next**.



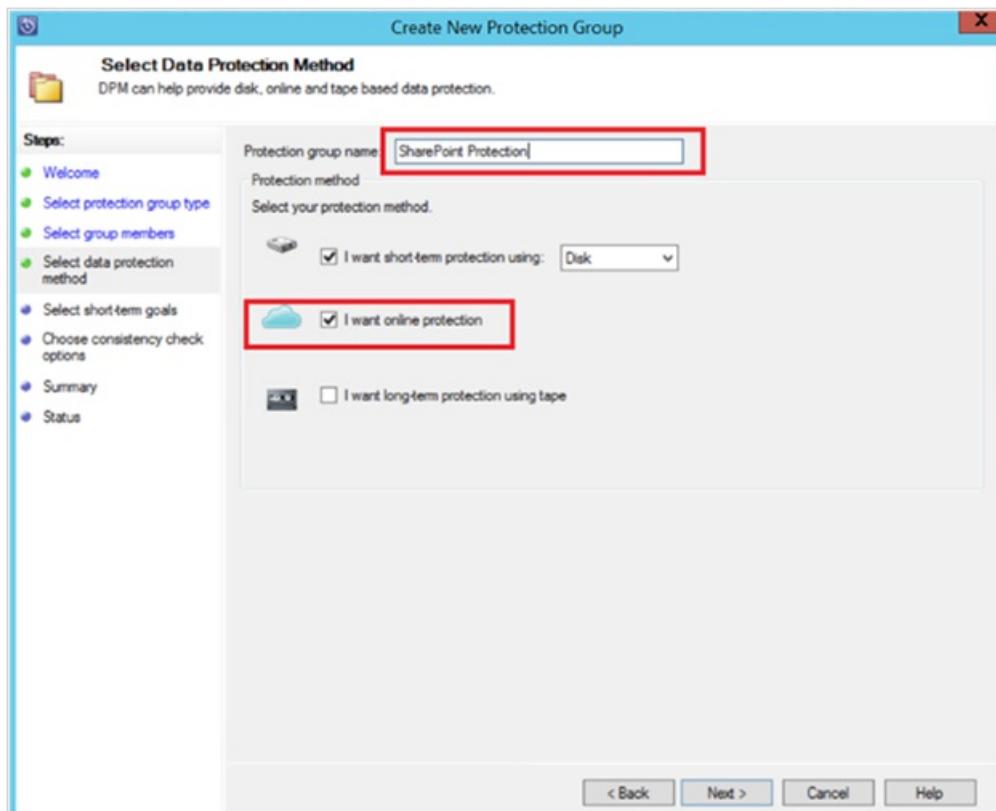
3. On the **Select Group Members** screen, select the check box for the SharePoint server you want to protect and click **Next**.



#### NOTE

With the DPM agent installed, you can see the server in the wizard. DPM also shows its structure. Because you ran ConfigureSharePoint.exe, DPM communicates with the SharePoint VSS Writer service and its corresponding SQL Server databases and recognizes the SharePoint farm structure, the associated content databases, and any corresponding items.

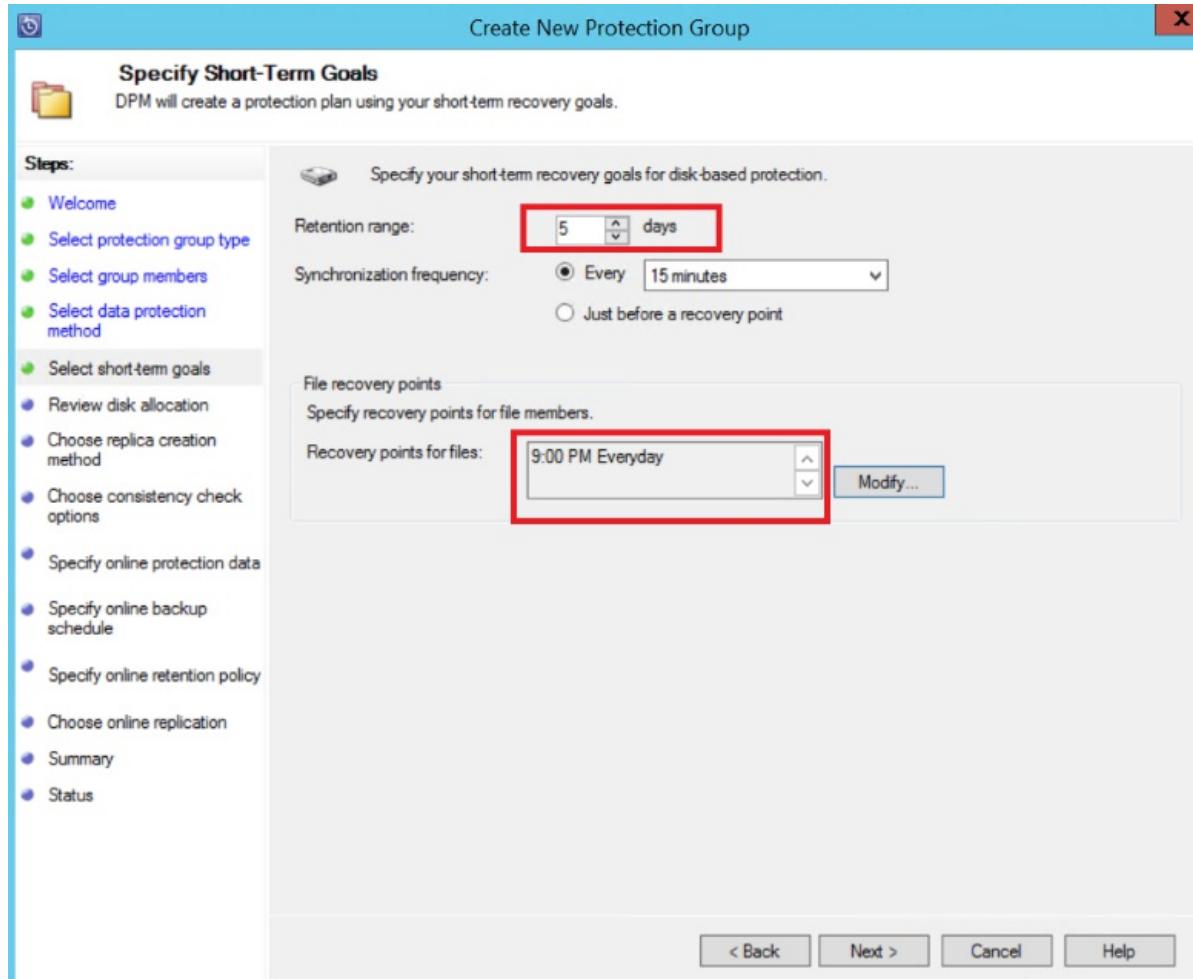
4. On the **Select Data Protection Method** page, enter the name of the **Protection Group**, and select your preferred *protection methods*. Click **Next**.



#### NOTE

The disk protection method helps to meet short recovery-time objectives. Azure is an economical, long-term protection target compared to tapes. For more information, see [Use Azure Backup to replace your tape infrastructure](#)

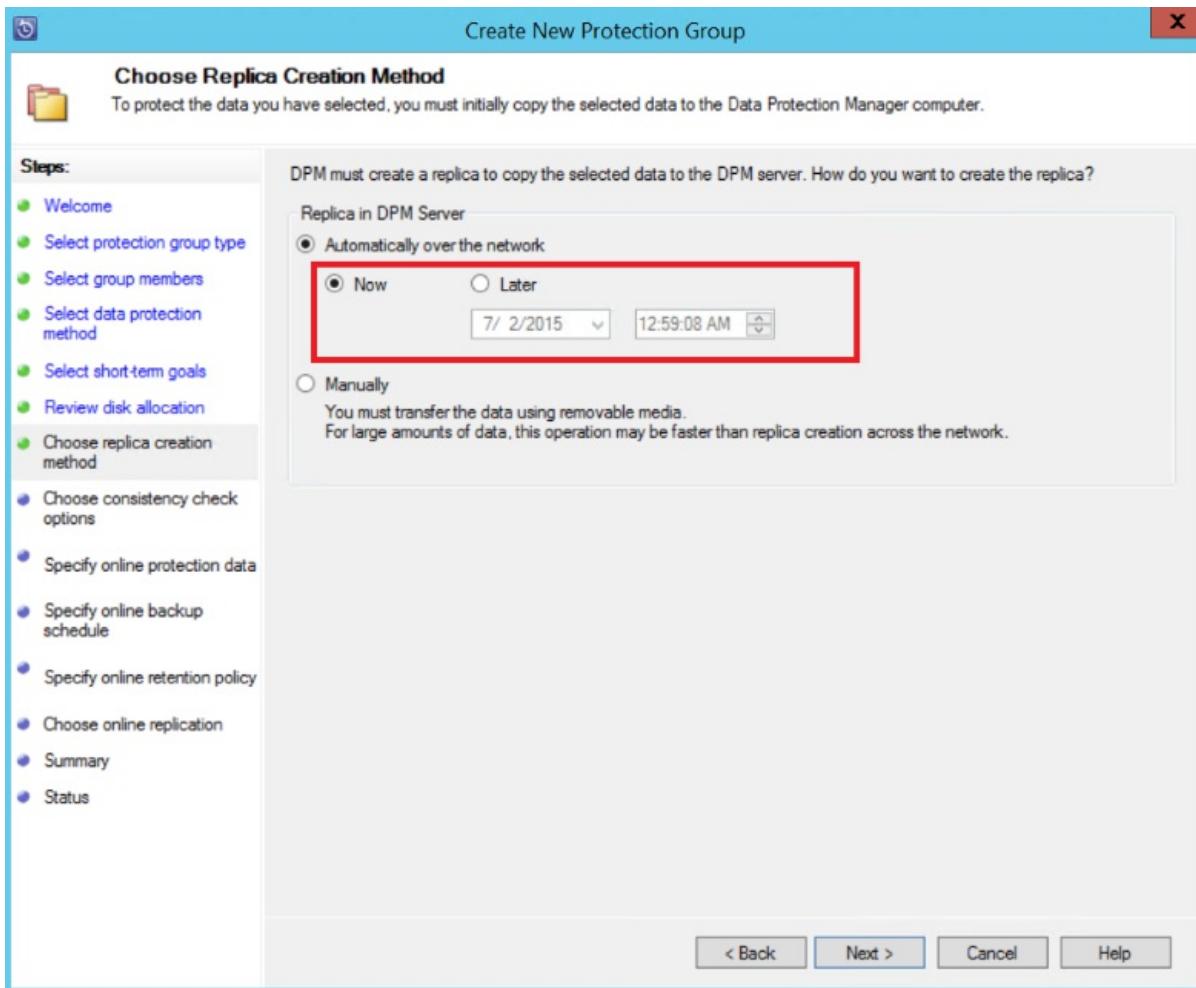
5. On the **Specify Short-Term Goals** page, select your preferred **Retention range** and identify when you want backups to occur.



#### NOTE

Because recovery is most often required for data that's less than five days old, we selected a retention range of five days on disk and ensured that the backup happens during non-production hours, for this example.

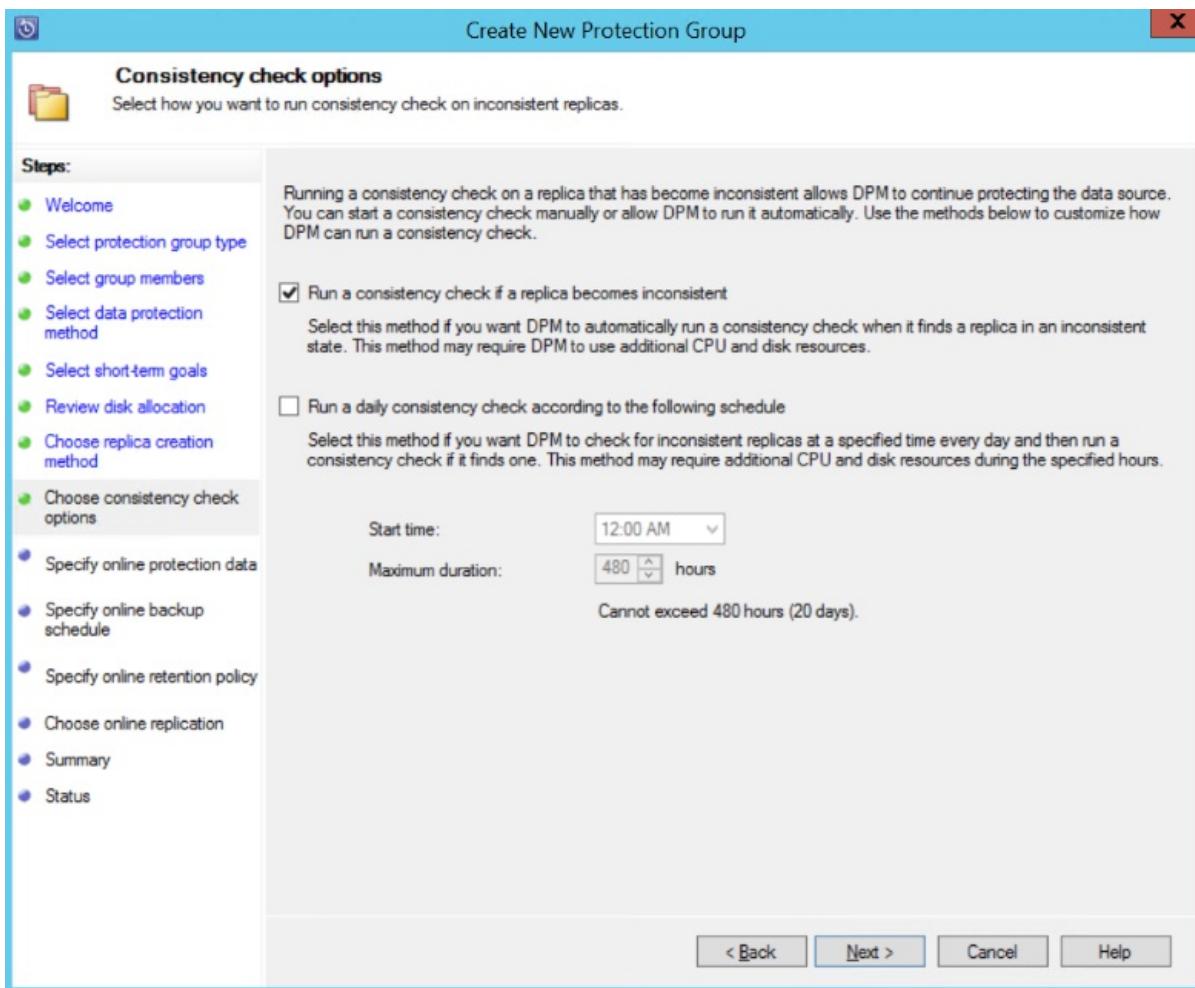
6. Review the storage pool disk space allocated for the protection group, and click then **Next**.
7. For every protection group, DPM allocates disk space to store and manage replicas. At this point, DPM must create a copy of the selected data. Select how and when you want the replica created, and then click **Next**.



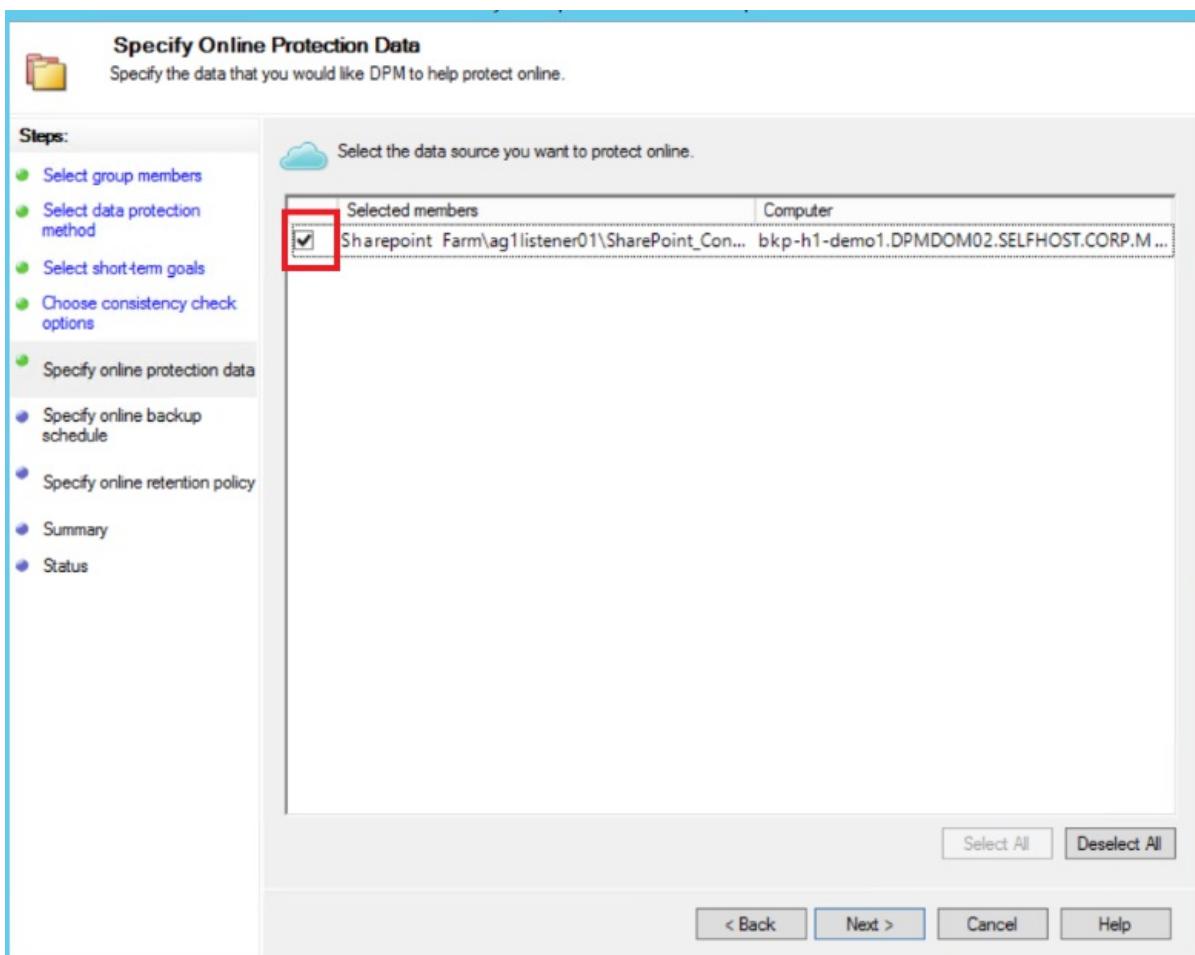
#### NOTE

To make sure that network traffic is not effected, select a time outside production hours.

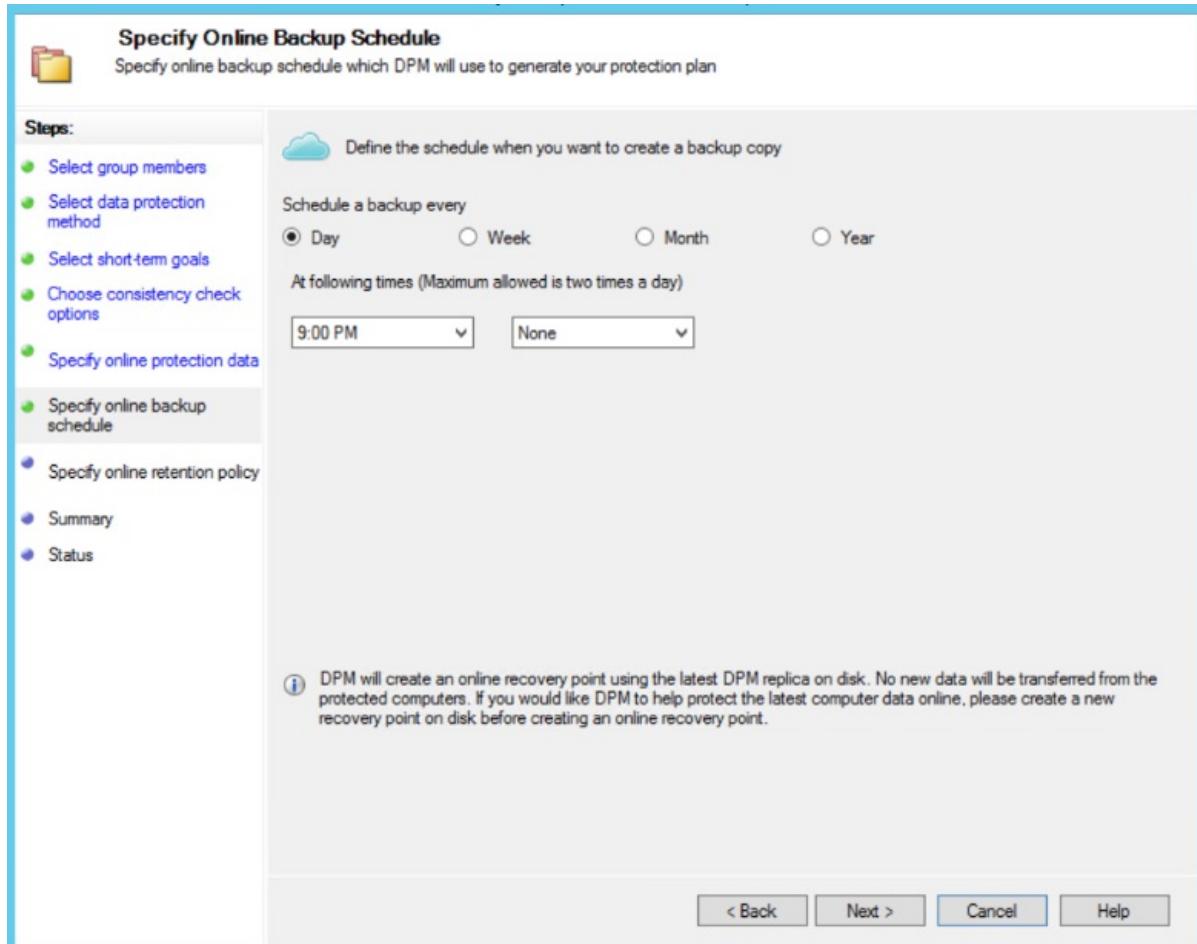
8. DPM ensures data integrity by performing consistency checks on the replica. There are two available options. You can define a schedule to run consistency checks, or DPM can run consistency checks automatically on the replica whenever it becomes inconsistent. Select your preferred option, and then click **Next**.



9. On the **Specify Online Protection Data** page, select the SharePoint farm that you want to protect, and then click **Next**.



10. On the **Specify Online Backup Schedule** page, select your preferred schedule, and then click **Next**.



#### NOTE

DPM provides a maximum of two daily backups to Azure at different times. Azure Backup can also control the amount of WAN bandwidth that can be used for backups in peak and off-peak hours by using [Azure Backup Network Throttling](#).

11. Depending on the backup schedule that you selected, on the **Specify Online Retention Policy** page, select the retention policy for daily, weekly, monthly, and yearly backup points.

**Specify Online Retention Policy**

Specify online backup schedule which DPM will use to generate your protection plan

**Steps:**

- Select group members
- Select data protection method
- Select short-term goals
- Choose consistency check options
- Specify online protection data
- Specify online backup schedule
- **Specify online retention policy**
- Summary
- Status

**Specify the retention policy which DPM will use to generate your protection plan**

Daily Retention policy  
Retain backup copies taken on At 9:00 PM for 180 Days

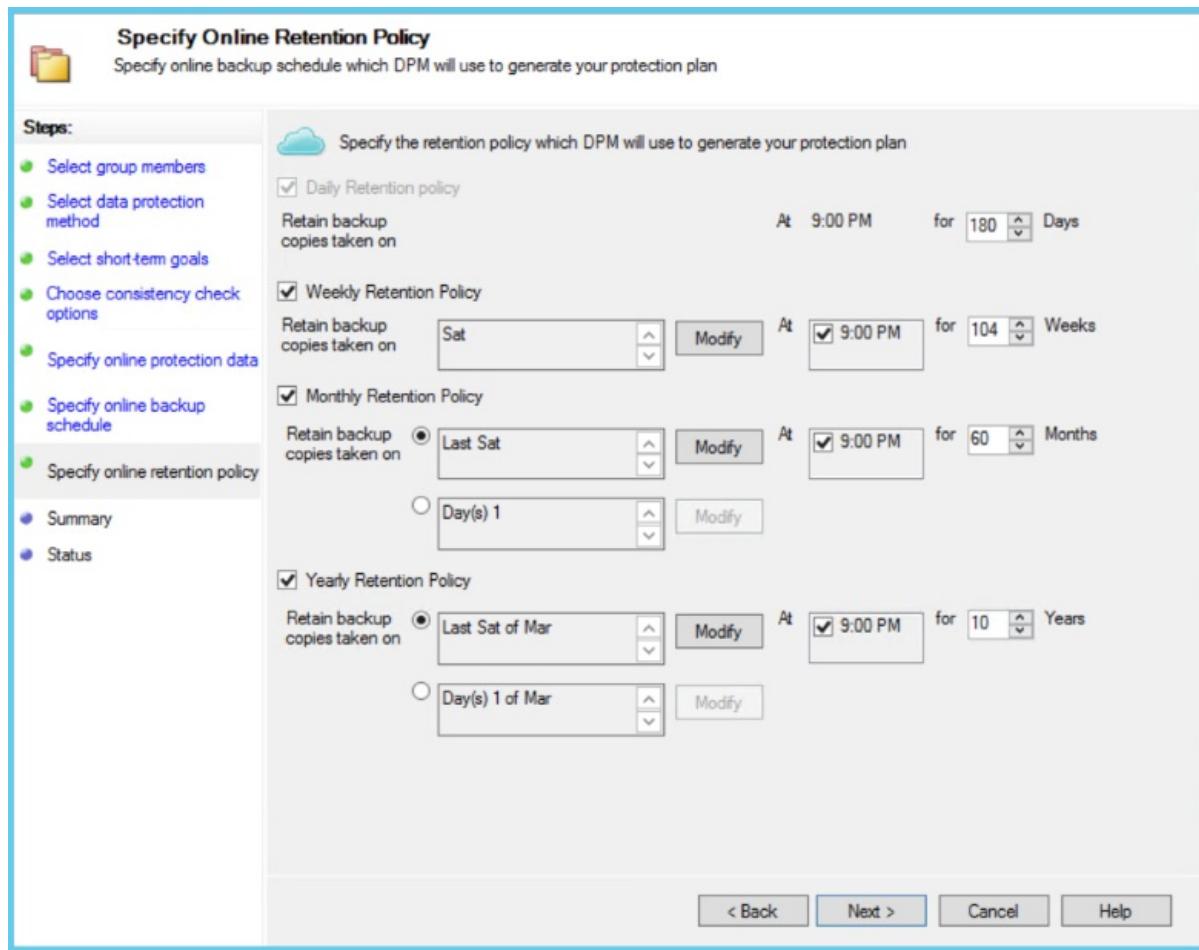
Weekly Retention Policy  
Retain backup copies taken on Sat At  9:00 PM for 104 Weeks

Monthly Retention Policy  
Retain backup copies taken on Last Sat At  9:00 PM for 60 Months

Day(s) 1 At

Yearly Retention Policy  
Retain backup copies taken on Last Sat of Mar At  9:00 PM for 10 Years

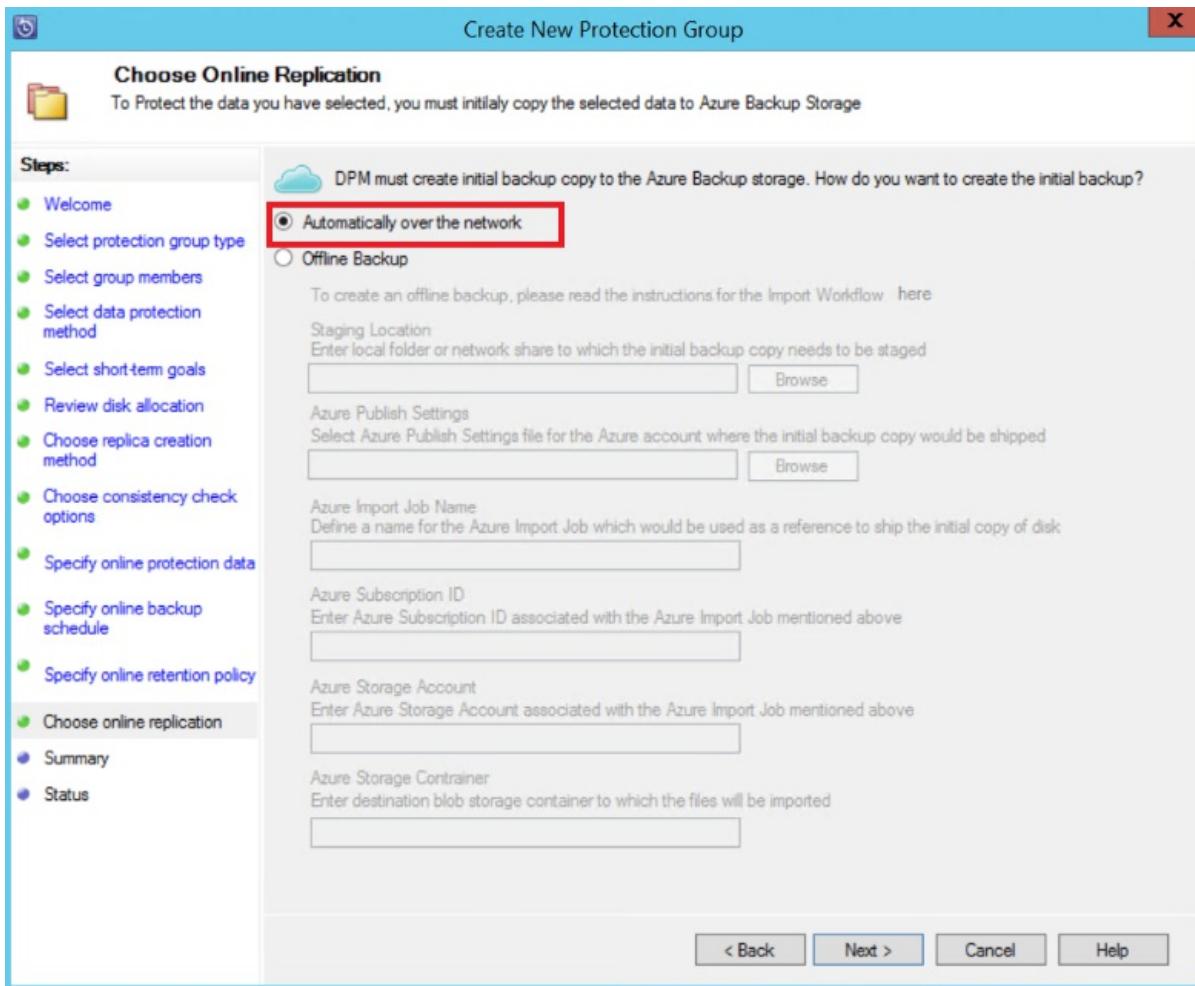
Day(s) 1 of Mar At



#### NOTE

DPM uses a grandfather-father-son retention scheme in which a different retention policy can be chosen for different backup points.

12. Similar to disk, an initial reference point replica needs to be created in Azure. Select your preferred option to create an initial backup copy to Azure, and then click **Next**.



13. Review your selected settings on the **Summary** page, and then click **Create Group**. You will see a success message after the protection group has been created.

**Create New Protection Group**

**Summary**  
DPM is ready to create the SharePoint Protection protection group.

**Steps:**

- Welcome
- Select protection group type
- Select group members
- Select data protection method
- Select short-term goals
- Review disk allocation
- Choose replica creation method
- Choose consistency check options
- Specify online protection data
- Specify online backup schedule
- Specify online retention policy
- Choose online replication
- Summary
- Status

Review the settings, and then click Create Group to create the SharePoint Protection protection group.

**Protection group members:**  
Sharepoint Farm\ag1listener01\SharePoint\_Config

**Protection group settings:**

| Setting                 | Details                              |
|-------------------------|--------------------------------------|
| Online backup frequency | Daily                                |
| Online backup schedule  | 9:00 PM Everyday                     |
| Online retention range  | 180 day(s)(9:00 PM Everyday)         |
|                         | 104 week(s)(9:00 PM Sat)             |
|                         | 60 month(s)(Last Sat, 9:00 PM)       |
|                         | 10 year(s)(Last Sat of Mar, 9:00 PM) |
| Online Replica Creation | Network                              |

(i) You can [optimize performance](#) of this protection group now or you can do it later from the actions pane.

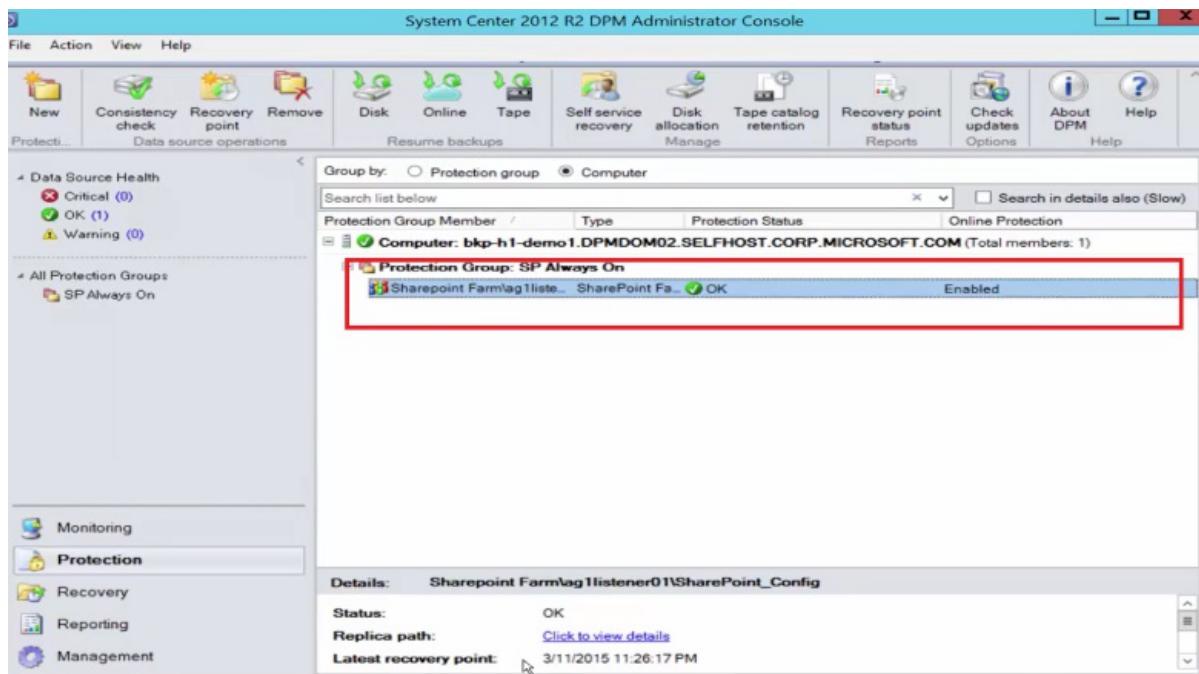
< Back      Create Group      Cancel      Help

## Restore a SharePoint item from disk by using DPM

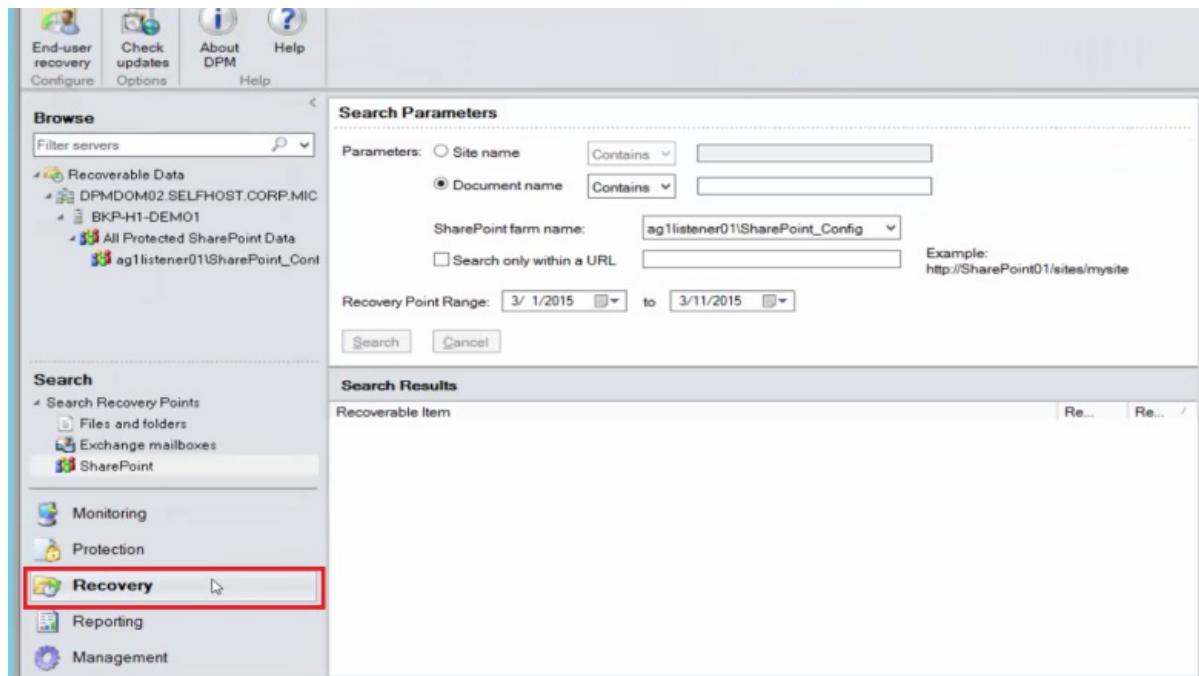
In the following example, the *Recovering SharePoint item* has been accidentally deleted and needs to be recovered.

The screenshot shows a SharePoint site collection home page titled 'site1 - Home'. The URL in the address bar is [http://bkp-h1-demo1:8080/sites/\\_vti\\_bin/Top-Level Site Successfully Created.aspx](http://bkp-h1-demo1:8080/sites/_vti_bin/Top-Level Site Successfully Created.aspx). The page features a large red box highlighting the title 'site1'. Below the title, there are several cards: 'Share your site.', 'Working on a deadline?', 'Add lists, libraries, and other apps.', 'What's your style?', and 'Your site. Your brand.'. A sidebar on the left shows navigation links like 'Home', 'Documents', 'Site Contents', and 'EDIT LINKS'. At the bottom, there is a section for 'Documents' with a red box around the item 'Recovering SharePoint item'. This item has a small red icon next to its name and a red box around the entire row.

1. Open the **DPM Administrator Console**. All SharePoint farms that are protected by DPM are shown in the **Protection** tab.



2. To begin to recover the item, select the **Recovery** tab.



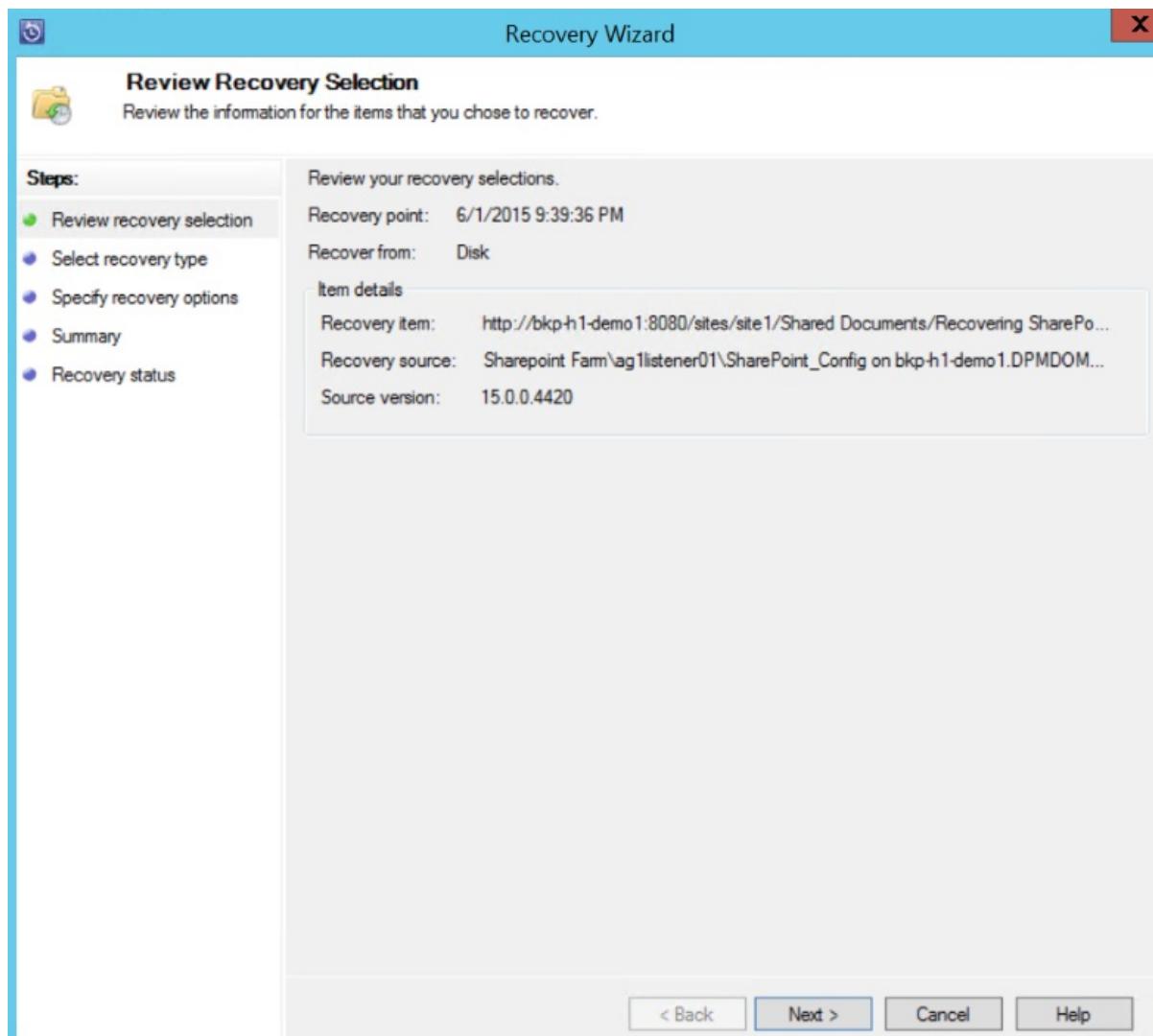
3. You can search SharePoint for *Recovering SharePoint item* by using a wildcard-based search within a recovery point range.

The screenshot shows the DPM Recovery interface. In the 'Search Parameters' section, the 'Document name' field is set to 'Contains' and contains 'Recovering\*'. The 'Recovery Point Range' is set from '3/1/2015' to '3/11/2015'. The 'Search' button is highlighted with a red box. The 'Search Results' section shows a list of recovery points for 'SharePoint' items, with one item selected and its details shown in the preview pane.

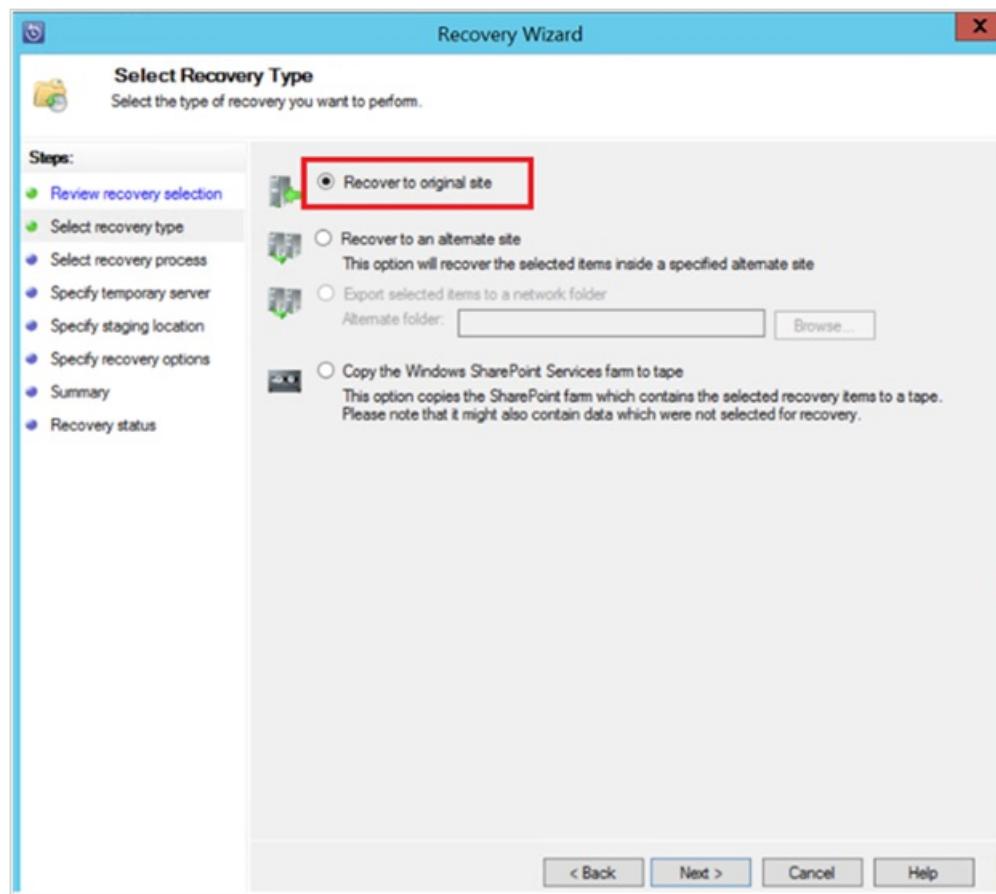
4. Select the appropriate recovery point from the search results, right-click the item, and then select **Recover**.
5. You can also browse through various recovery points and select a database or item to recover. Select **Date > Recovery time**, and then select the correct **Database > SharePoint farm > Recovery point > Item**.

The screenshot shows the DPM Recovery interface. The 'Recovery points for: ag1listener01\SharePoint\_Config' section displays recovery points for February 2015. The date 'February 09 2015' and time '8:00 PM(ET)' are selected. The 'Path: All Protected SharePoint Data' section shows the hierarchy: Recoverable Item / SharePoint\_AdminContent\_17d8dd99-b505-4b89-a4f3-0c31bd427966 / SharePoint\_Config / WSS\_Content. The 'WSS\_Content' item is highlighted with a red box.

6. Right-click the item, and then select **Recover** to open the **Recovery Wizard**. Click **Next**.



7. Select the type of recovery that you want to perform, and then click **Next**.

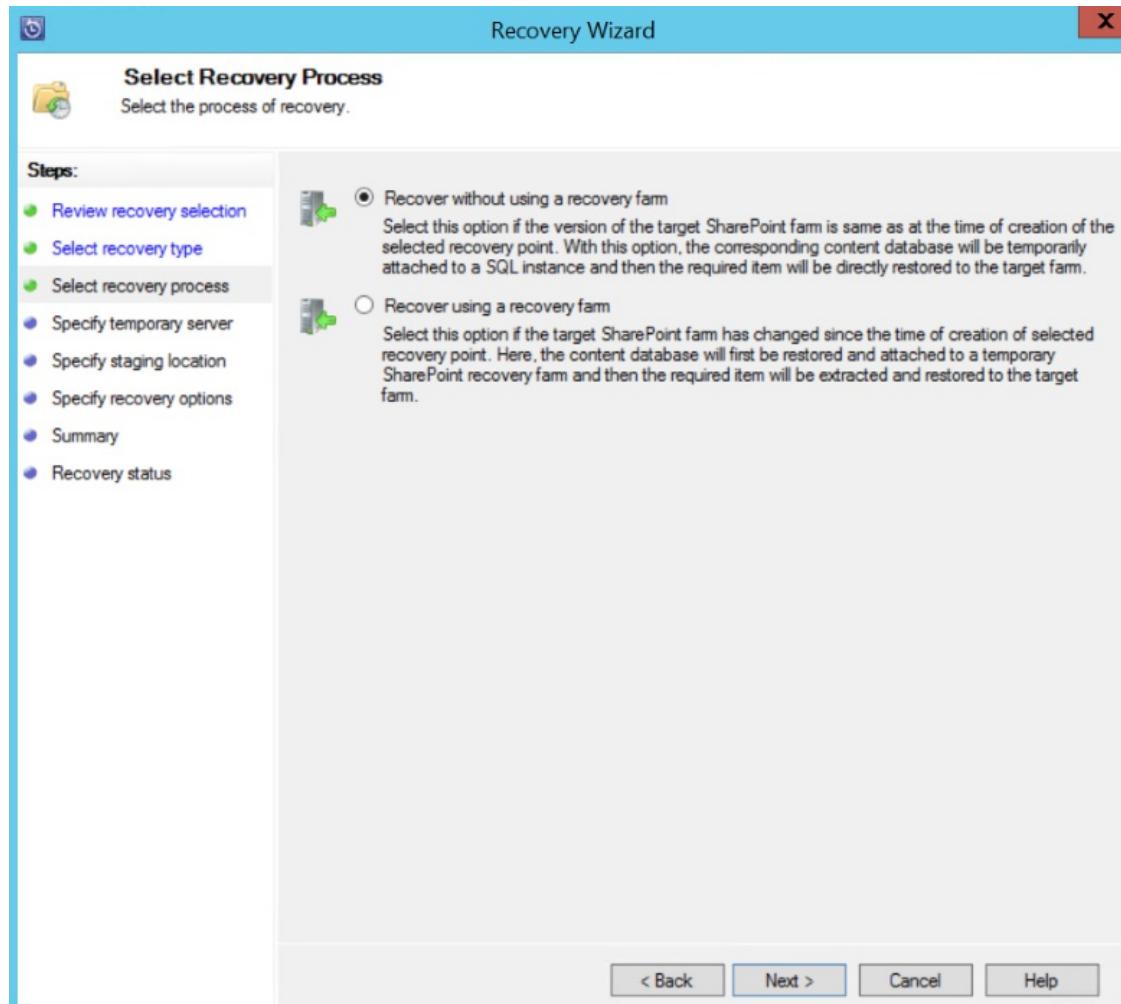


**NOTE**

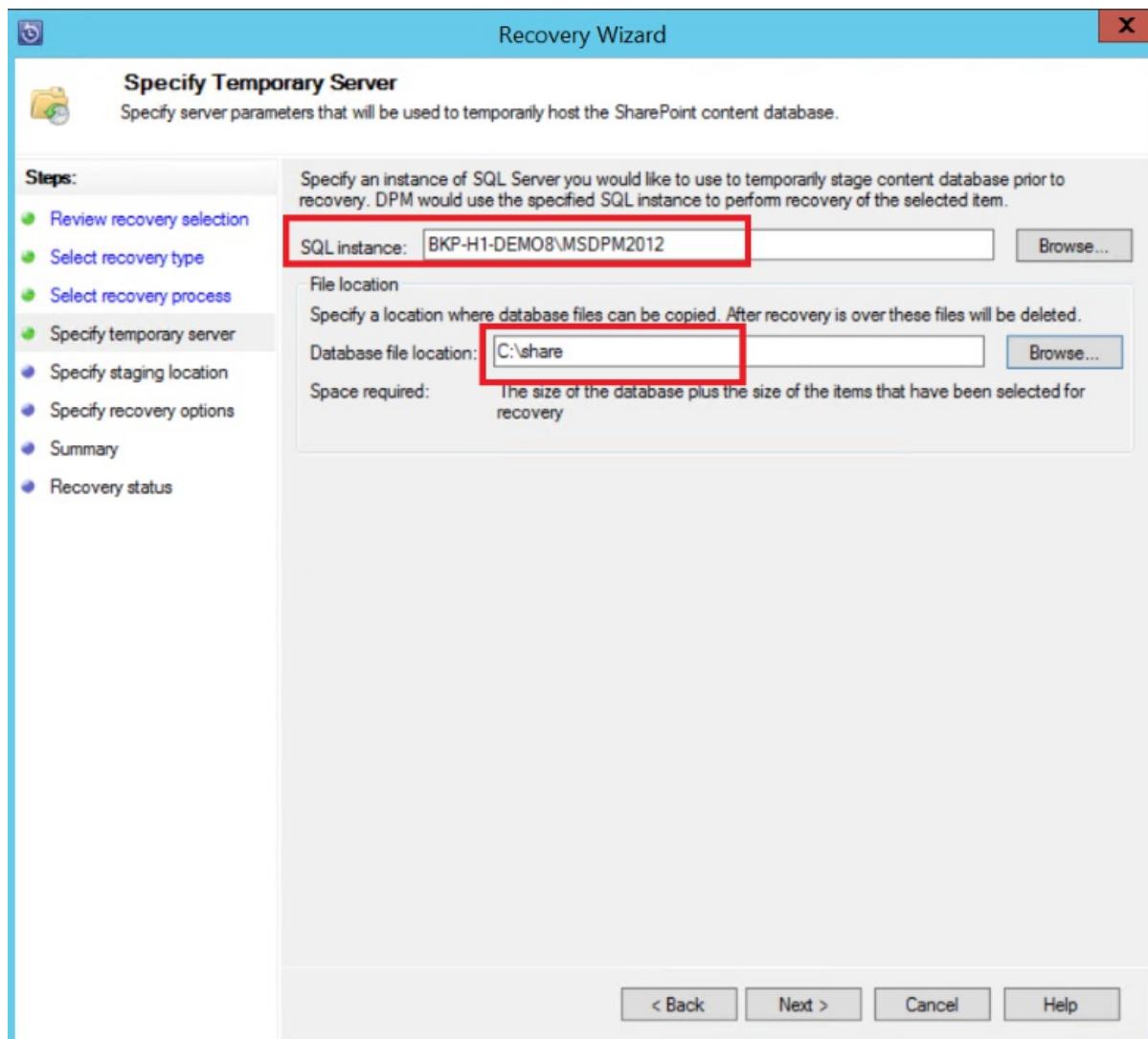
The selection of **Recover to original** in the example recovers the item to the original SharePoint site.

8. Select the **Recovery Process** that you want to use.

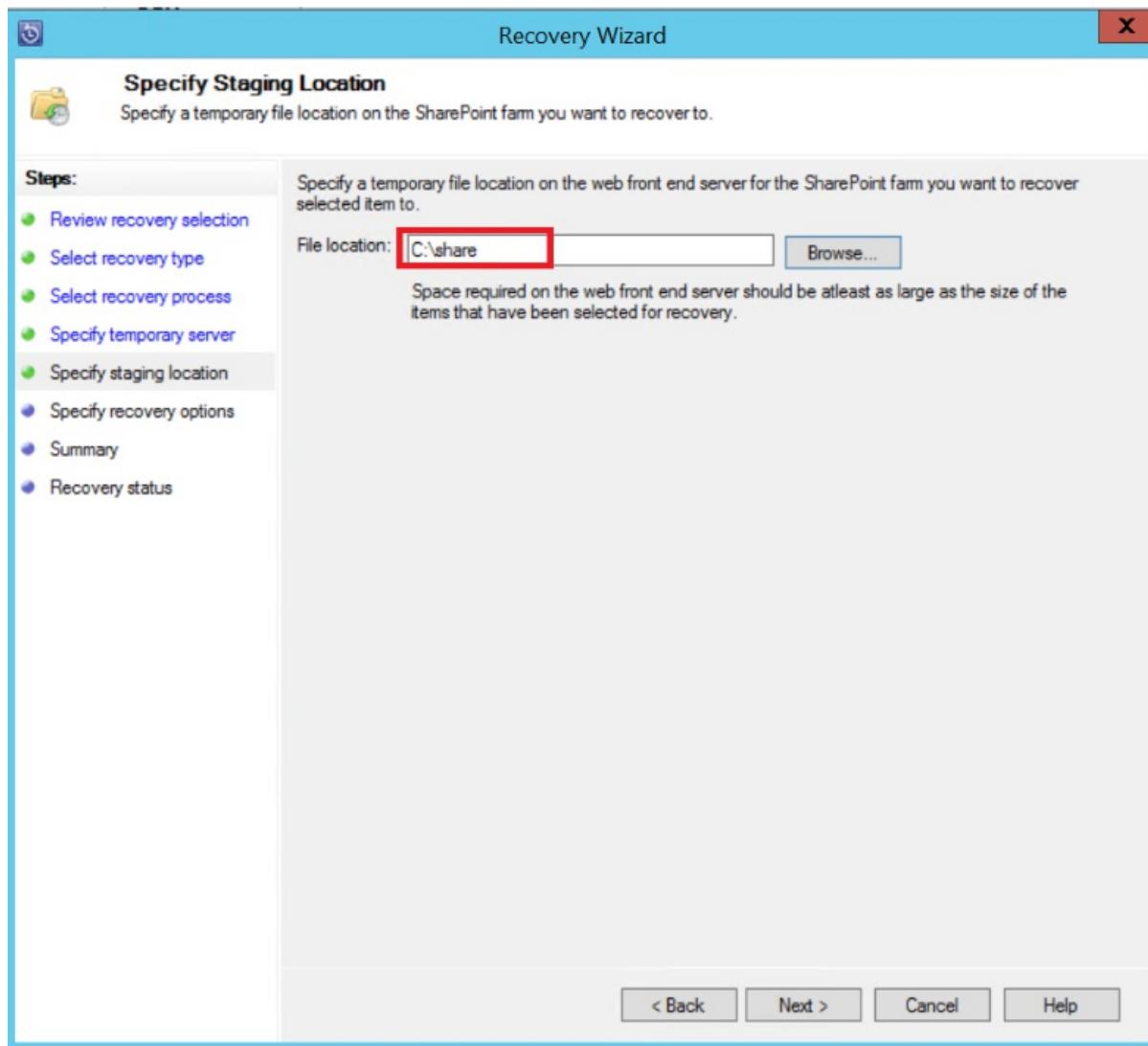
- Select **Recover without using a recovery farm** if the SharePoint farm has not changed and is the same as the recovery point that is being restored.
- Select **Recover using a recovery farm** if the SharePoint farm has changed since the recovery point was created.



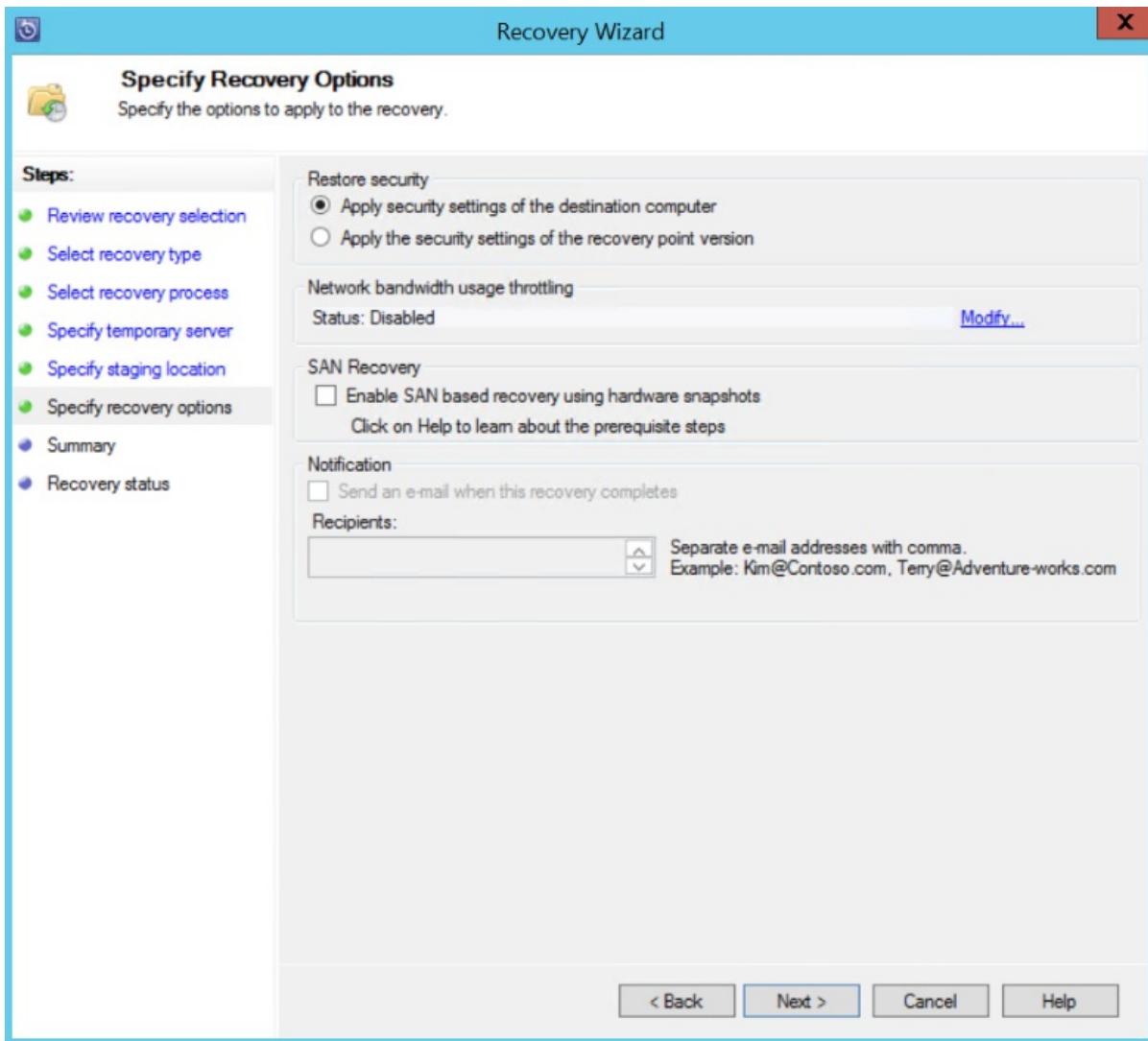
9. Provide a staging SQL Server instance location to recover the database temporarily, and provide a staging file share on the DPM server and the server that's running SharePoint to recover the item.



DPM attaches the content database that is hosting the SharePoint item to the temporary SQL Server instance. From the content database, the DPM server recovers the item and puts it on the staging file location on the DPM server. The recovered item that's on the staging location of the DPM server now needs to be exported to the staging location on the SharePoint farm.



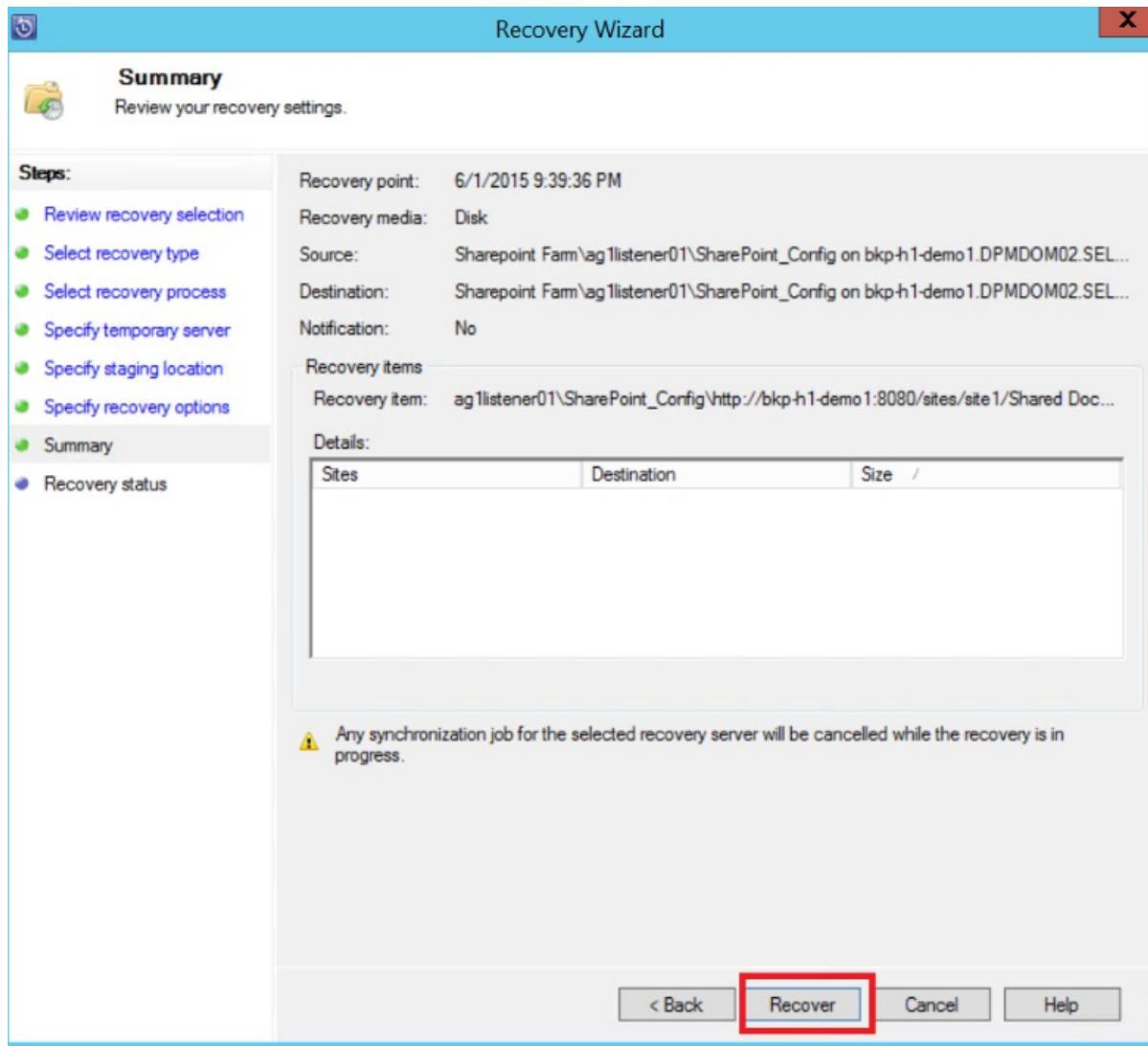
10. Select **Specify recovery options**, and apply security settings to the SharePoint farm or apply the security settings of the recovery point. Click **Next**.



#### NOTE

You can choose to throttle the network bandwidth usage. This minimizes impact to the production server during production hours.

11. Review the summary information, and then click **Recover** to begin recovery of the file.



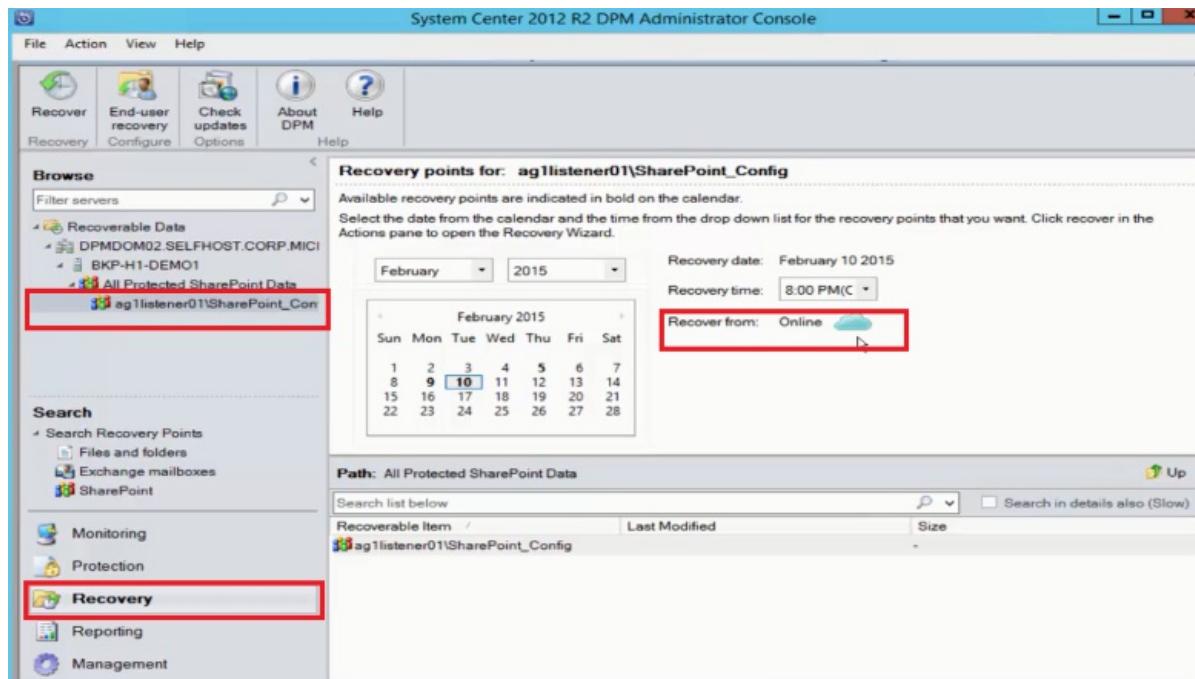
12. Now select the **Monitoring** tab in the **DPM Administrator Console** to view the **Status** of the recovery.

#### NOTE

The file is now restored. You can refresh the SharePoint site to check the restored file.

# Restore a SharePoint database from Azure by using DPM

1. To recover a SharePoint content database, browse through various recovery points (as shown previously), and select the recovery point that you want to restore.

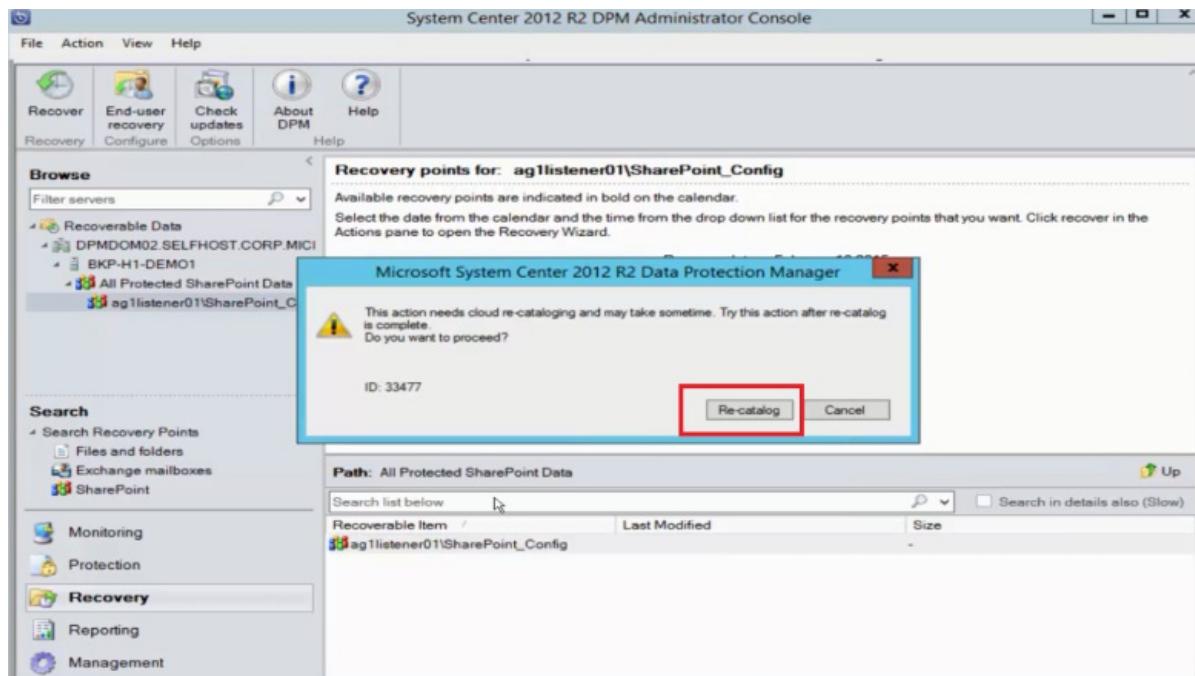


2. Double-click the SharePoint recovery point to show the available SharePoint catalog information.

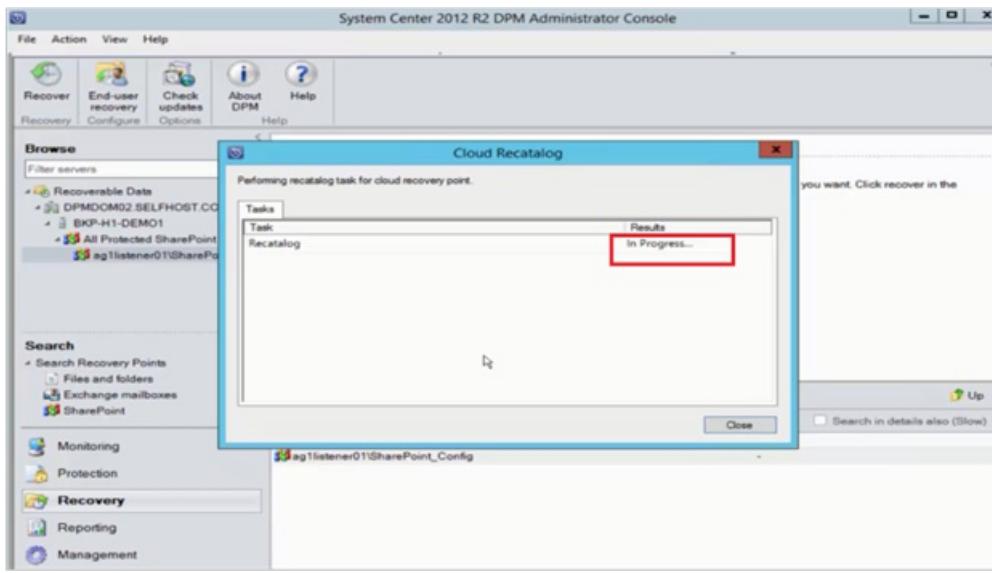
## NOTE

Because the SharePoint farm is protected for long-term retention in Azure, no catalog information (metadata) is available on the DPM server. As a result, whenever a point-in-time SharePoint content database needs to be recovered, you need to catalog the SharePoint farm again.

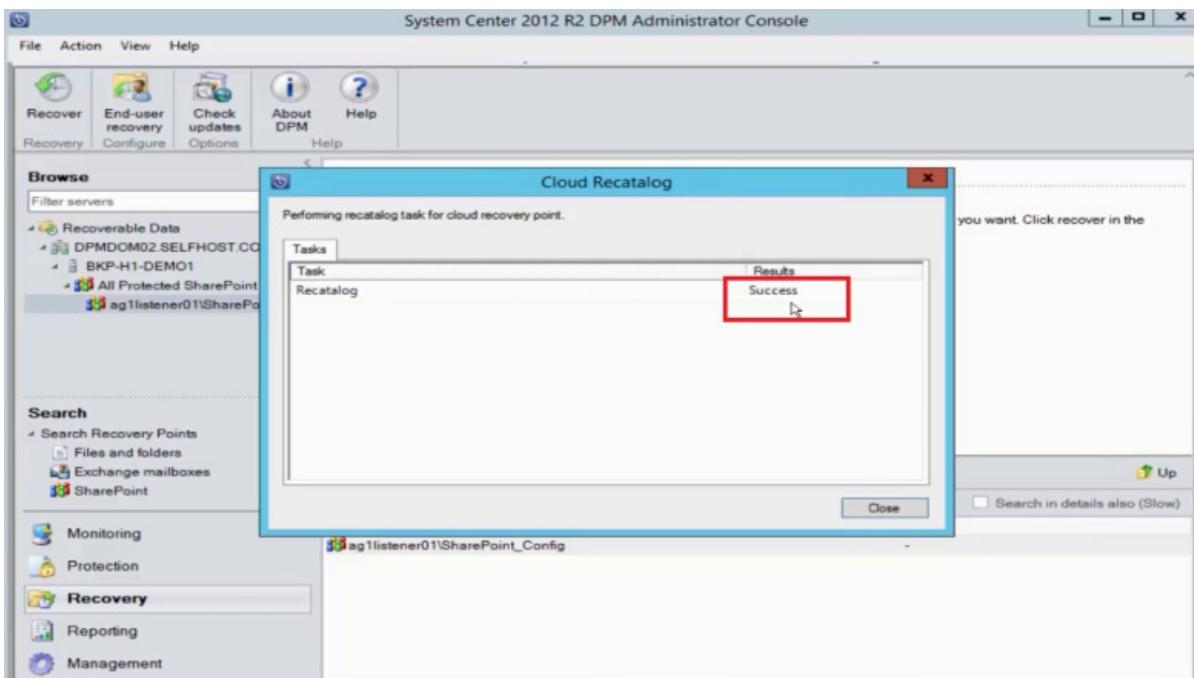
3. Click **Re-catalog**.



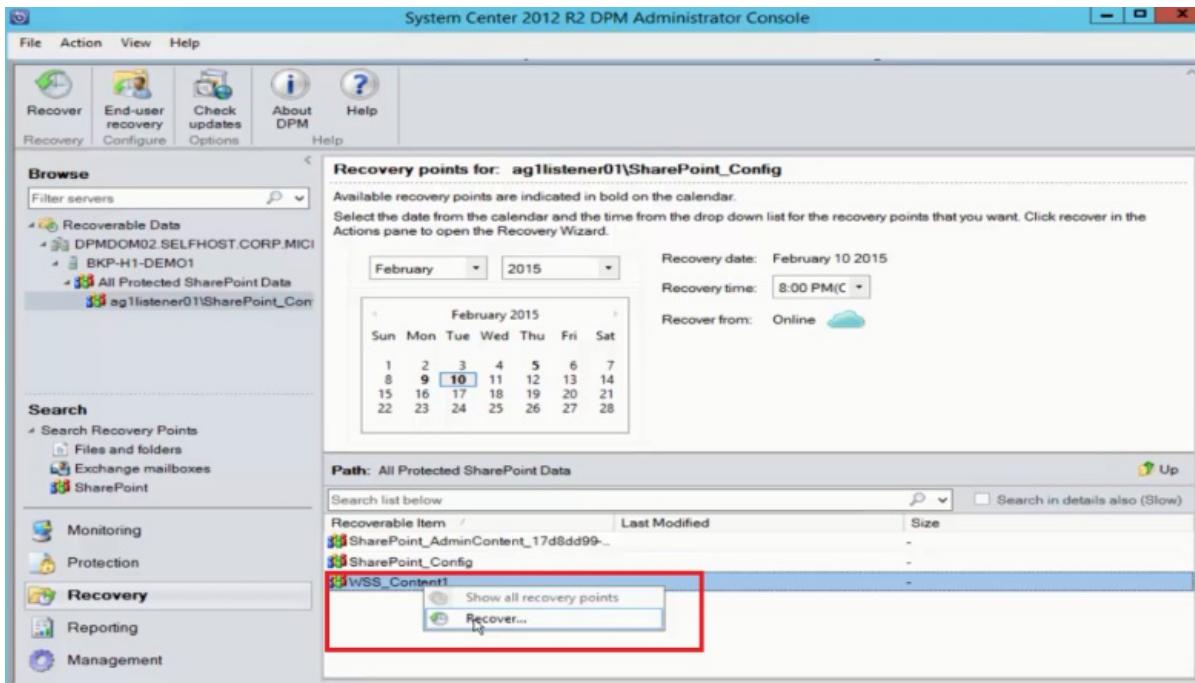
The **Cloud Recatalog** status window opens.



After cataloging is finished, the status changes to *Success*. Click **Close**.



4. Click the SharePoint object shown in the DPM **Recovery** tab to get the content database structure. Right-click the item, and then click **Recover**.



5. At this point, follow the recovery steps earlier in this article to recover a SharePoint content database from disk.

## Next steps

- Learn more about DPM Protection of SharePoint - see [Video Series - DPM Protection of SharePoint](#)
- Review [Release Notes for System Center 2012 - Data Protection Manager](#)
- Review [Release Notes for Data Protection Manager in System Center 2012 SP1](#)

# Move your long-term storage from tape to the Azure cloud

2/17/2020 • 2 minutes to read • [Edit Online](#)

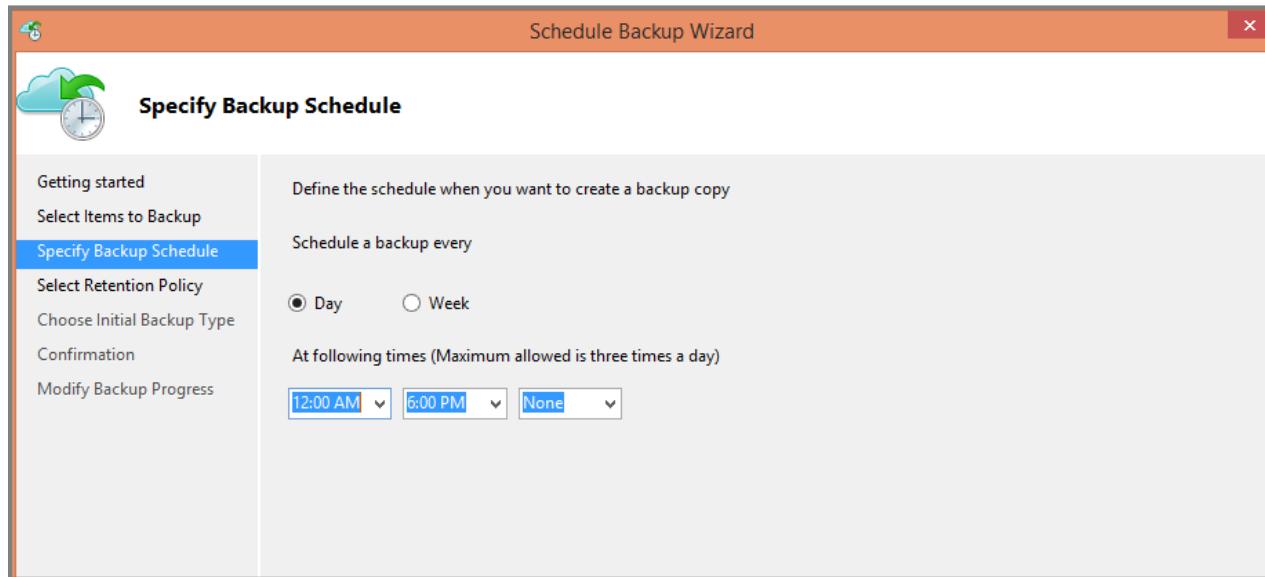
Azure Backup and System Center Data Protection Manager customers can:

- Back up data in schedules which best suit the organizational needs.
- Retain the backup data for longer periods.
- Make Azure a part of their long-term retention needs (instead of tape).

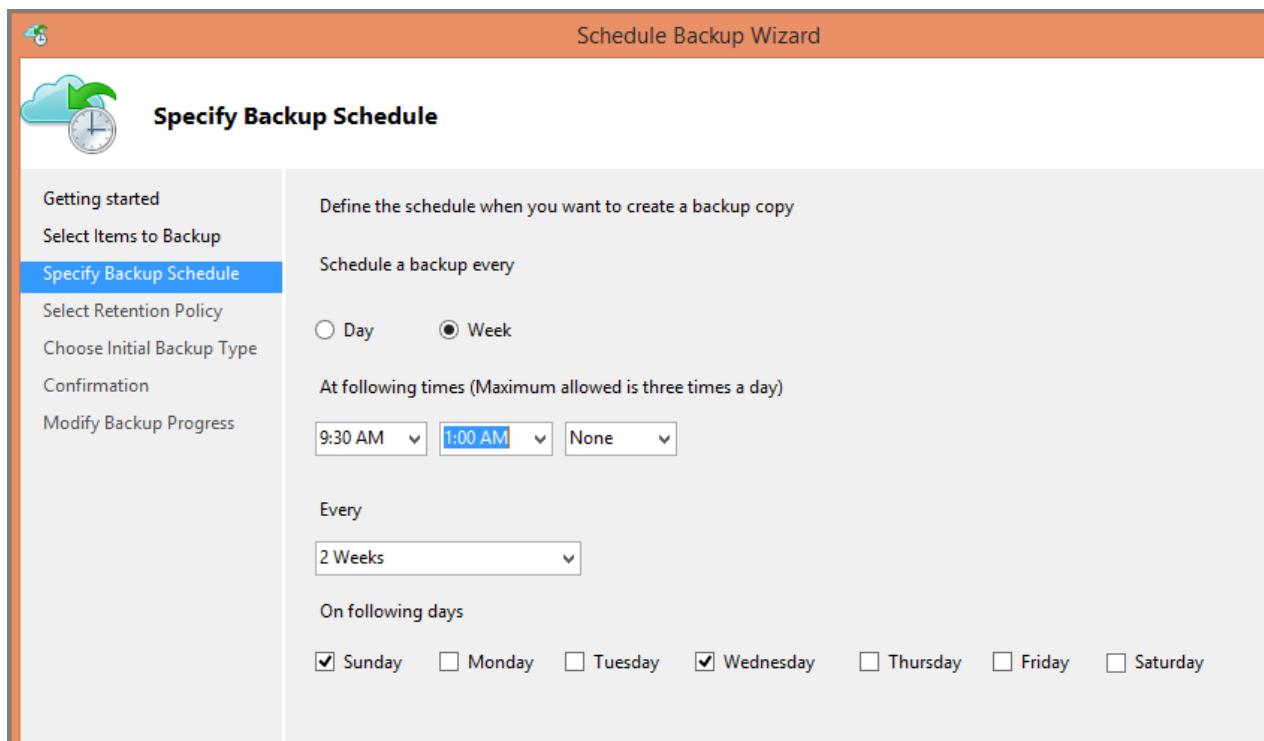
This article explains how customers can enable backup and retention policies. Customers who use tapes to address their long-term-retention needs now have a powerful and viable alternative with the availability of this feature. The feature is enabled in the latest release of the Azure Backup (which is available [here](#)). System Center DPM customers must update to, at least, DPM 2012 R2 UR5 before using DPM with the Azure Backup service.

## What is the Backup Schedule?

The backup schedule indicates the frequency of the backup operation. For example, the settings in the following screen indicate that backups are taken daily at 6pm and at midnight.

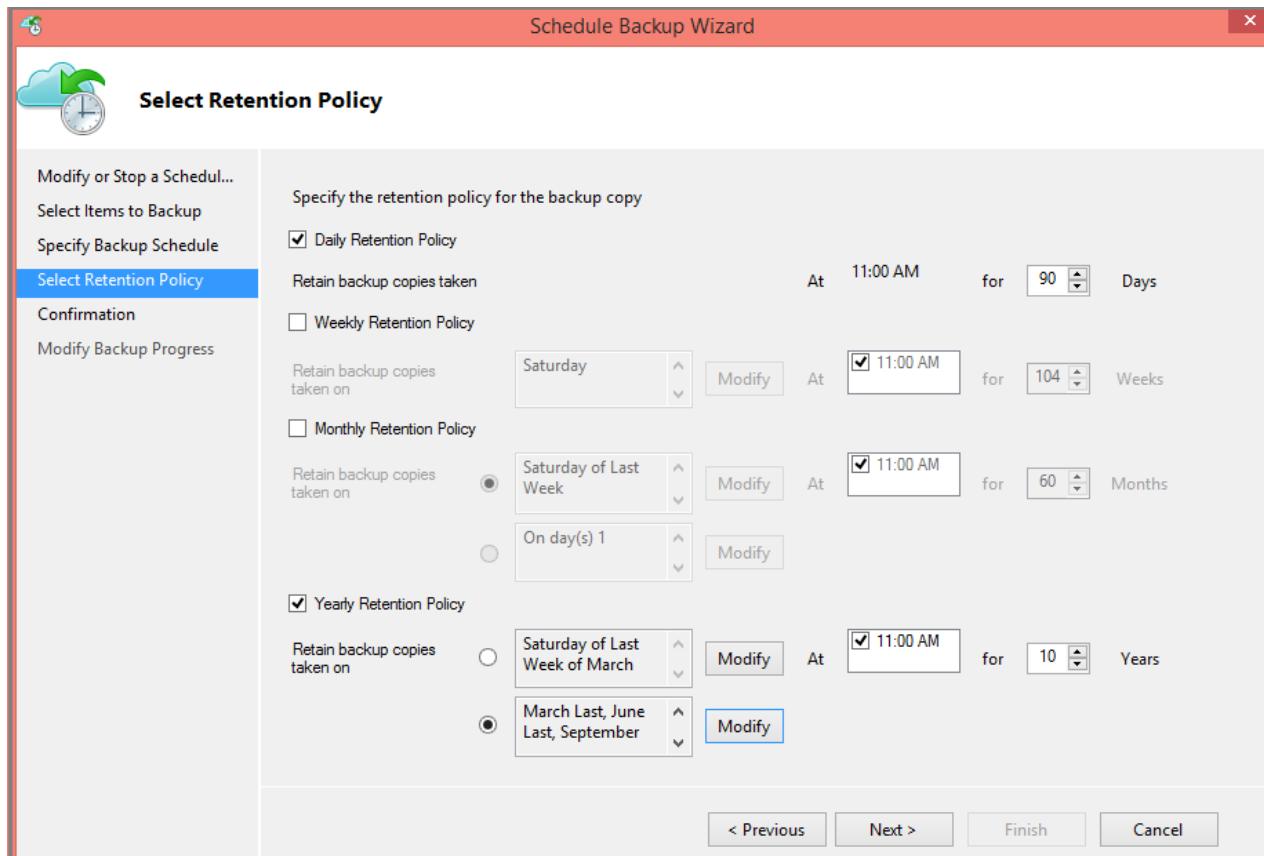


Customers can also schedule a weekly backup. For example, the settings in the following screen indicate that backups are taken every alternate Sunday & Wednesday at 9:30AM and 1:00AM.



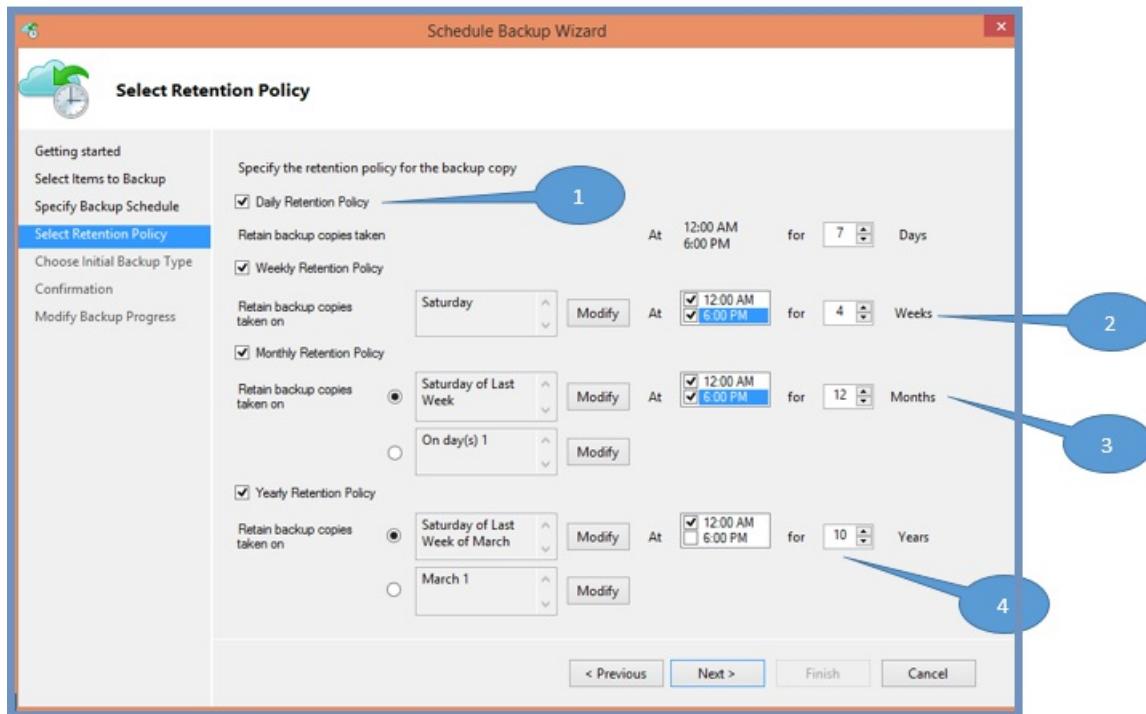
## What is the Retention Policy?

The retention policy specifies the duration for which the backup must be stored. Rather than just specifying a "flat policy" for all backup points, customers can specify different retention policies based on when the backup is taken. For example, the backup point taken daily, which serves as an operational recovery point, is preserved for 90 days. The backup point taken at the end of each quarter for audit purposes is preserved for a longer duration.



The total number of "retention points" specified in this policy is 90 (daily points) + 40 (one each quarter for 10 years) = 130.

## Example – Putting both together



- Daily retention policy:** Backups taken daily are stored for seven days.
- Weekly retention policy:** Backups taken at midnight and 6 PM Saturday are preserved for four weeks.
- Monthly retention policy:** Backups taken at midnight and 6 PM on the last Saturday of each month are preserved for 12 months.
- Yearly retention policy:** Backups taken at midnight on the last Saturday of every March are preserved for 10 years.

The total number of "retention points" (points from which a customer can restore data) in the preceding diagram is computed as follows:

- two points per day for seven days = 14 recovery points
- two points per week for four weeks = 8 recovery points
- two points per month for 12 months = 24 recovery points
- one point per year per 10 years = 10 recovery points

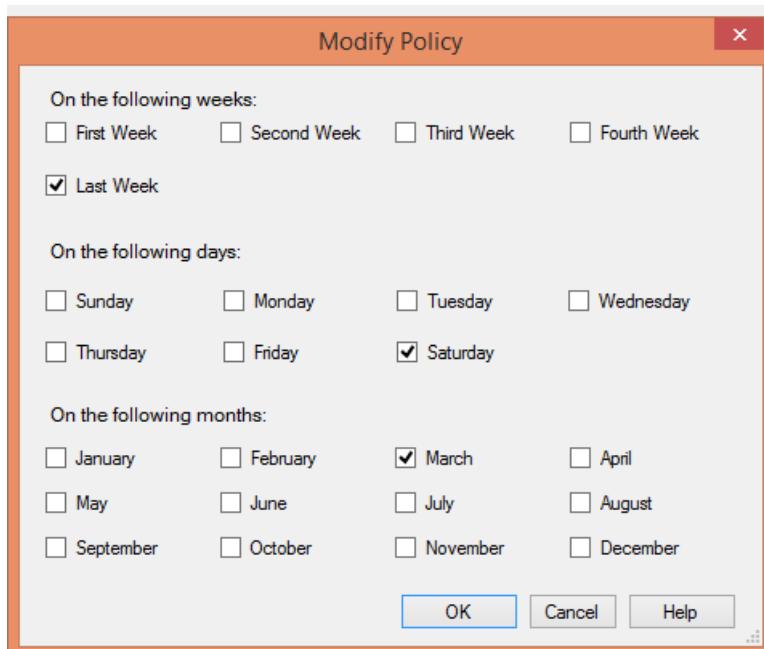
The total number of recovery points is 56.

### NOTE

Using Azure Backup you can create up to 9999 recovery points per protected instance. A protected instance is a computer, server (physical or virtual), or workload that backs up to Azure.

## Advanced configuration

By clicking **Modify** in the preceding screen, customers have further flexibility in specifying retention schedules.



## Next steps

For more information about Azure Backup, see:

- [Introduction to Azure Backup](#)
- [Try Azure Backup](#)

# Overview of Offline Backup

2/4/2020 • 3 minutes to read • [Edit Online](#)

This article gives an overview of Offline Backup.

Initial full backups to Azure typically transfer large amounts of data online and require more network bandwidth when compared to subsequent backups that transfer only incremental changes. Remote offices or datacenters in certain geographies don't always have sufficient network bandwidth. Therefore, these initial backups take several days and during this time continuously use the same network that was provisioned for applications running in the on-premises datacenter.

Azure Backup supports "Offline Backup", which allows transferring initial backup data offline, without the use of network bandwidth. It provides a mechanism to copy backup data onto physical storage-devices that are then shipped to a nearby Azure Datacenter and uploaded onto a Recovery Services Vault. This process ensures robust transfer of backup data without using any network bandwidth.

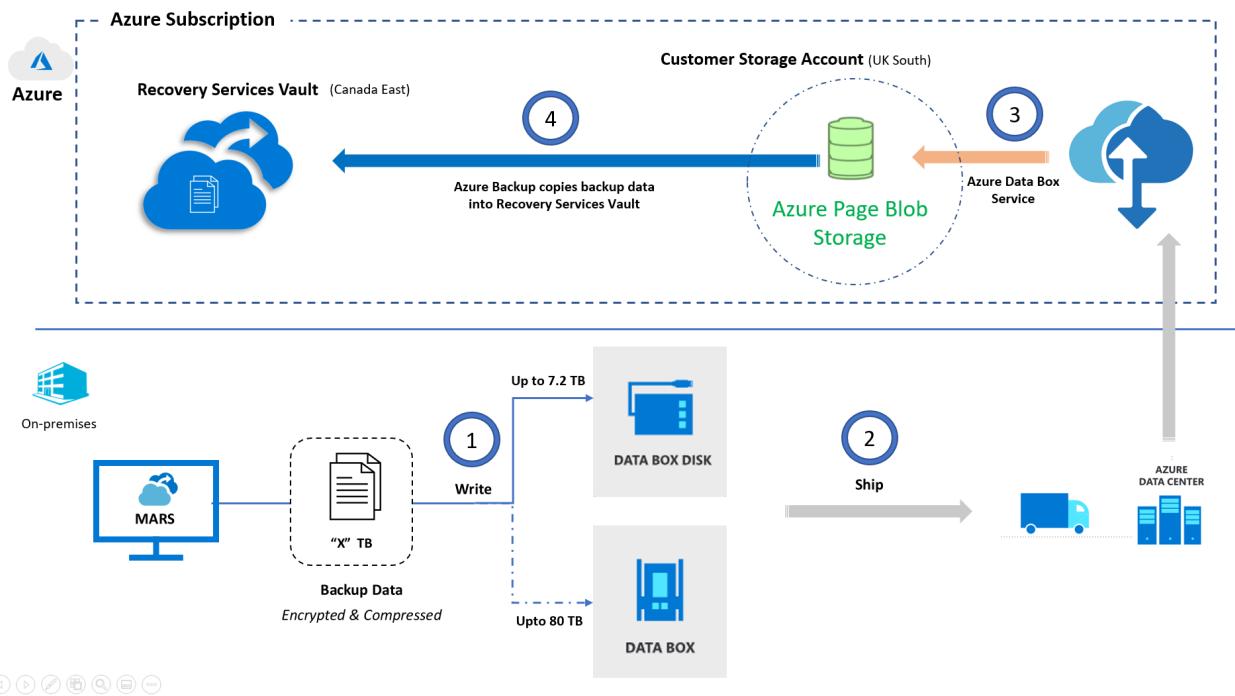
## Offline Backup options

Offline-Backup is offered in two modes based on the ownership of the storage devices.

1. Azure Data Box based Offline Backup (preview)
2. Azure Import/Export based Offline Backup

## Azure Data Box based Offline Backup (Preview)

This mode is currently supported with the MARS Agent, in preview. This option takes advantage of the [Azure Data Box service](#) to ship Microsoft-proprietary, secure, and tamper-resistant transfer appliances with USB connectors, to your datacenter or remote office and backup data is directly written onto these devices. **This option saves the effort required to procure your own Azure compatible disks and connectors or provisioning temporary storage as a staging location.** In addition, Microsoft handles the end-to-end transfer logistics, which you can track through the Azure portal. An architecture describing the movement of backup data with this option is shown below.



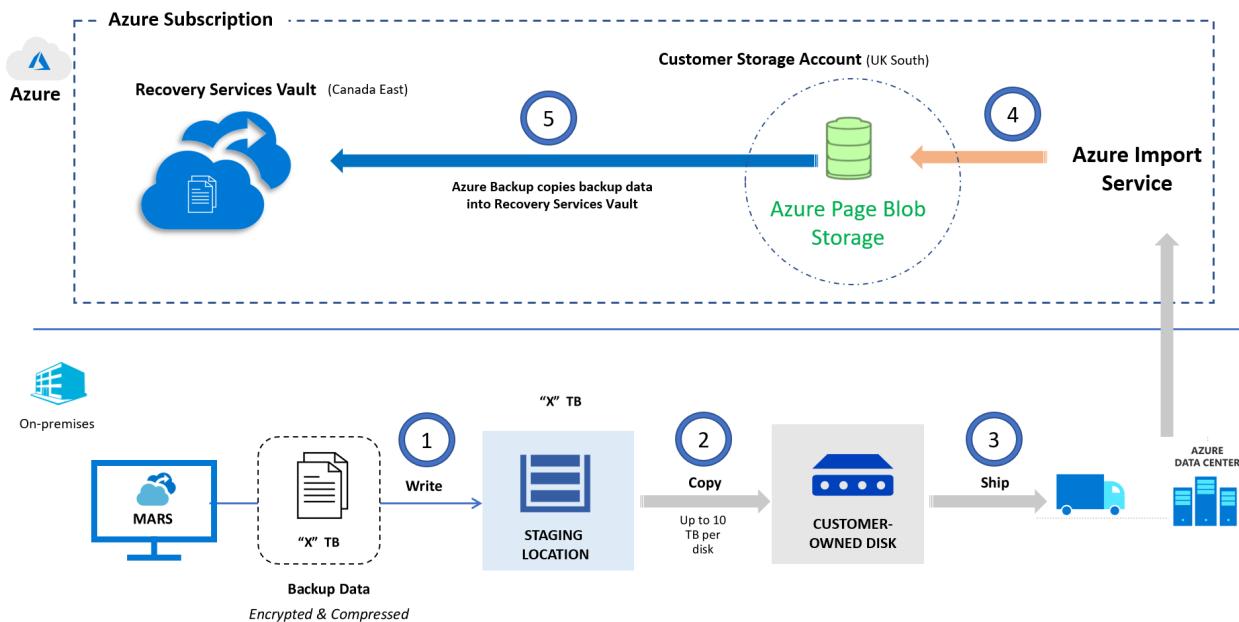
Here is a summary of the architecture:

1. Azure Backup directly copies backup data to these pre-configured devices.
2. You can then ship these devices back to an Azure Datacenter.
3. The Azure Data Box service copies the data onto a customer-owned storage account.
4. Azure Backup automatically copies backup data from the storage account to the designated Recovery Services Vault and incremental online backups are scheduled.

To use Azure Data Box based Offline Backup, refer to [this article](#).

## Azure Import/Export based Offline Backup

This option is supported by Azure Backup Server (MABS) / DPM-A / MARS Agent. It leverages the [Azure Import/Export service](#) that enables you to transfer initial backup data to Azure by using your own Azure-compatible disks and connectors. This approach requires provisioning a temporary storage known as the **Staging Location** and usage of pre-built utilities to format and copy the backup data onto customer-owned disks. An architecture describing the movement of backup data with this option is shown below:



Here is a summary of the architecture:

1. Instead of sending the backup data over the network, Azure Backup writes the backup data to a staging location.
2. The data in the staging location is written to one or more SATA disks using a custom utility.
3. As part of the preparatory work, the utility creates an Azure Import job. The SATA drives are shipped to the nearest Azure datacenter, and reference the import job to connect the activities.
4. At the Azure datacenter, the data on the disks is copied to an Azure storage account.
5. Azure Backup copies the backup data from the storage account to the Recovery Services vault, and incremental backups are scheduled.

To use Azure Import/Export based Offline Backup with the MARS Agent, refer to [this article](#).

To use the same along with MABS/DPM-A, refer to [this article](#).

## Offline Backup Support Summary

The table below compares the two available options so you can make the appropriate choices based on your scenario.

| CONSIDERATION                                                               | AZURE DATA BOX BASED OFFLINE BACKUP                                                                                                                         | AZURE IMPORT/EXPORT BASED OFFLINE BACKUP      |
|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| Azure Backup Deployment models                                              | MARS agent (Preview)                                                                                                                                        | MARS Agent, Azure Backup Server (MABS), DPM-A |
| Maximum Backup data per server (MARS) or per Protection Group (MABS, DPM-A) | Azure Data Box Disk - 7.2 TB<br>Azure Data Box - 80 TB                                                                                                      | 80 TB (up to 10 disks of 8 TB each)           |
| Security (data, device & service)                                           | Data - AES-256 Bit Encrypted<br>Device - Rugged case, proprietary credential-based interface to copy data<br>Service - Protected by Azure Security features | Data - BitLocker Encrypted                    |

| CONSIDERATION                                     | AZURE DATA BOX BASED OFFLINE BACKUP                                                                          | AZURE IMPORT/EXPORT BASED OFFLINE BACKUP             |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| Temporary Staging Location provisioning           | Not required                                                                                                 | More than or equal to the estimated backup data size |
| Supported Regions                                 | Azure Data Box Disk regions<br>Azure Data Box regions                                                        | Azure Import/Export Regions                          |
| Cross-country shipping*                           | <b>Not supported</b><br><i>Source address &amp; Destination Azure Datacenter must be in the same country</i> | Supported                                            |
| Transfer Logistics (delivery, transport, pick-up) | Fully Microsoft managed                                                                                      | Customer managed                                     |
| Pricing                                           | Azure Data Box Pricing<br>Azure Data Box Disk Pricing                                                        | Azure Import/Export Pricing                          |

- If your country doesn't have an Azure Datacenter, then you need to ship your disks to an Azure Datacenter in another country.

## Next steps

- [Azure Data Box Based Offline Backup for MARS Agent](#)
- [Azure Import/Export based Offline Backup for MARS Agent](#)
- [Azure Import/Export based Offline Backup for MABS/DPM-A](#)

# Azure Backup offline-backup using Azure Data Box

2/4/2020 • 12 minutes to read • [Edit Online](#)

You can use the [Azure Data Box](#) service to seed your large initial MARS backups offline (without using network) to an Azure Recovery Services vault. This saves both time and network bandwidth, that would otherwise be consumed moving large amounts of backup data online over a high-latency network. This enhancement is currently in preview. Azure Data Box based Offline Backup provides two distinct advantages over the [Azure Import/Export Service-based offline backup](#).

1. No need to procure your own Azure-compatible disks and connectors. Azure Data Box service ships the disks associated with the selected [Data Box SKU](#)
2. Azure Backup (MARS Agent) can directly write backup data onto the supported SKUs of Azure Data Box. This eliminates the need for provisioning a staging location for your initial backup data and the need for utilities to format and copy that data onto the disks.

## Azure Data Box with MARS Agent

This article explains how you can use Azure Data Box to seed large initial backup data offline from the MARS Agent to an Azure Recovery Services Vault. The article is divided into the following parts:

- Supported Platforms
- Supported Data Box SKUs
- Pre-requisites
- Setup MARS Agent
- Setup Azure Data Box
- Backup data transfer to Azure Data Box
- Post-Backup steps

## Supported Platforms

The process to seed data from the MARS Agent using Azure Data Box is supported on the following Windows SKUs:

| os                 | SKU                                                                   |
|--------------------|-----------------------------------------------------------------------|
| <b>Workstation</b> |                                                                       |
| Windows 10 64 bit  | Enterprise, Pro, Home                                                 |
| Windows 8.1 64 bit | Enterprise, Pro                                                       |
| Windows 8 64 bit   | Enterprise, Pro                                                       |
| Windows 7 64 bit   | Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter |
| <b>Server</b>      |                                                                       |

| OS                                    | SKU                                          |
|---------------------------------------|----------------------------------------------|
| Windows Server 2019 64 bit            | Standard, Datacenter, Essentials             |
| Windows Server 2016 64 bit            | Standard, Datacenter, Essentials             |
| Windows Server 2012 R2 64 bit         | Standard, Datacenter, Foundation             |
| Windows Server 2012 64 bit            | Datacenter, Foundation, Standard             |
| Windows Storage Server 2016 64 bit    | Standard, Workgroup                          |
| Windows Storage Server 2012 R2 64 bit | Standard, Workgroup, Essential               |
| Windows Storage Server 2012 64 bit    | Standard, Workgroup                          |
| Windows Server 2008 R2 SP1 64 bit     | Standard, Enterprise, Datacenter, Foundation |
| Windows Server 2008 SP2 64 bit        | Standard, Enterprise, Datacenter             |

## Backup Data Size and supported Data Box SKUs

| BACKUP DATA SIZE (POST COMPRESSION BY MARS)* PER SERVER | SUPPORTED AZURE DATA BOX SKU |
|---------------------------------------------------------|------------------------------|
| <= 7.2 TB                                               | Azure Data Box Disk          |
| > 7.2 TB and <= 80 TB**                                 | Azure Data Box (100 TB)      |

\*Typical compression rates vary between 10-20%

\*\* Reach out to [AskAzureBackupTeam@microsoft.com](mailto:AskAzureBackupTeam@microsoft.com) if you expect to have more than 80 TB of initial backup data for a single MARS server.

### IMPORTANT

Initial backup data from a single server must be contained within a single Azure Data Box or Azure Data Box Disk and cannot be shared between multiple devices of the same or different SKUs. However, an Azure Data Box device may contain initial backups from multiple servers.

## Pre-requisites

### Azure Subscription and required permissions

- The process requires an Azure Subscription
- The process requires that the user designated to perform the offline backup policy is an “Owner” of the Azure Subscription
- The Data Box job and the Recovery Services Vault (to which the data needs to be seeded) are required to be in the same subscriptions.
- It is recommended that the target storage account associated with the Azure Data Box job and the Recovery Services Vault be in the same region. However, this is not necessary.

### Get Azure PowerShell 3.7.0

This is the most important pre-requisite for the process. Before installing Azure PowerShell (ver. 3.7.0),

perform the following checks\*\*

#### Step 1: Check PowerShell version

- Open Windows PowerShell and run the following command:

```
Get-Module -ListAvailable AzureRM*
```

- If the output displays a version higher than **3.7.0**, perform step 2 below. Otherwise, skip to step 3.

#### Step 2: Uninstall the PowerShell version

Uninstall the current version of PowerShell by doing the following actions:

- Remove the dependent modules by running the following command in PowerShell:

```
foreach ($module in (Get-Module -ListAvailable AzureRM*).Name |Get-Unique) { write-host "Removing Module $module" Uninstall-module $module }
```

- Run the following command to ensure the successful deletion of all the dependent modules:

```
Get-Module -ListAvailable AzureRM*
```

#### Step 3: Install PowerShell version 3.7.0

Once you have verified that no AzureRM modules are present, then install version 3.7.0 using one of the following methods:

- From GitHub, [link](#)

OR

- Run the following command in the PowerShell window:

```
Install-Module -Name AzureRM -RequiredVersion 3.7.0
```

Azure PowerShell could have also been installed using an msi file. To remove it, uninstall it using the Uninstall programs option in Control Panel.

#### Order and receive the Data Box device

The Offline backup process using MARS and Azure Data Box requires that the required Data Box devices are in "Delivered" state before triggering Offline Backup using the MARS Agent. Refer to the [Backup Data Size and supported Data Box SKUs](#) to order the most suitable SKU for your requirement. Follow the steps in [this article](#) to order and receive your Data Box devices.

#### IMPORTANT

Do not select BlobStorage for the Account kind. The MARS agent requires an account that supports Page Blobs which is not supported when BlobStorage is selected. We strongly advise selecting *Storage V2 (general purpose v2)* as the Account kind when creating the target storage account for your Azure Data Box job.

**Instance details**

The default deployment model is Resource Manager, which supports the latest Azure features. You may choose to deploy using the classic deployment model instead. [Choose classic deployment model](#)

|                        |                                                                         |
|------------------------|-------------------------------------------------------------------------|
| Storage account name * | <input type="text"/>                                                    |
| Location *             | (US) East US                                                            |
| Performance            | <input checked="" type="radio"/> Standard <input type="radio"/> Premium |
| Account kind           | StorageV2 (general purpose v2)                                          |
| Replication            | Locally-redundant storage (LRS)                                         |
| Access tier (default)  | <input type="radio"/> Cool <input checked="" type="radio"/> Hot         |

## Install and Setup the MARS Agent

- Make sure you uninstall any previous installations of the MARS Agent.
- Download the latest MARS Agent from [here](#).
- Run *MARSAgentInstaller.exe* and perform \***only** the steps to [Install and Register the Agent](#) to the Recovery Services Vault to which you want your backups to be stored.

**NOTE**

The Recovery Services Vault must be in the same subscription as the Azure Data Box job.

- Once the agent is registered to the Recovery Services Vault, follow the steps in the sections below.

## Setup Azure Data Box device(s)

Depending on the Azure Data Box SKU you have ordered, perform the steps covered in the appropriate sections below to set up and prepare the Data Box device(s) for the MARS Agent to identify and transfer the initial backup data.

### Setup Azure Data Box Disk

If you ordered one or more Azure Data Box Disks (up to 8 TB each), follow the steps mentioned here to [Unpack, connect, and unlock your Data Box Disk](#).

**NOTE**

It is possible that the server with the MARS Agent does not have a USB port. In that situation you can connect your Azure Data Box Disk to another server/client and expose the root of the device as a network share.

### Setup Azure Data Box

If you ordered an Azure Data Box (up to 100 TB), follow the steps mentioned here [to setup your Data Box](#).

#### Mount your Azure Data Box as Local System

The MARS Agent operates in the Local System context and therefore requires the same level of privilege to be provided to the mount path where the Azure Data Box is connected. Follow the steps below to ensure you can mount your Data Box device as Local System using the NFS Protocol:

- Enable the Client for NFS feature on the Windows Server (that has MARS agent installed).  
Specify alternate source: *WIM:D:\Sources\Install.wim:4*

- Download PSExec from <https://download.sysinternals.com/files/PS%20Tools.zip> to the server with MARS Agent installed.
- Open an elevated command prompt and execute the following command with the directory containing PSEExec.exe as the current directory:

```
psexec.exe -s -i cmd.exe
```

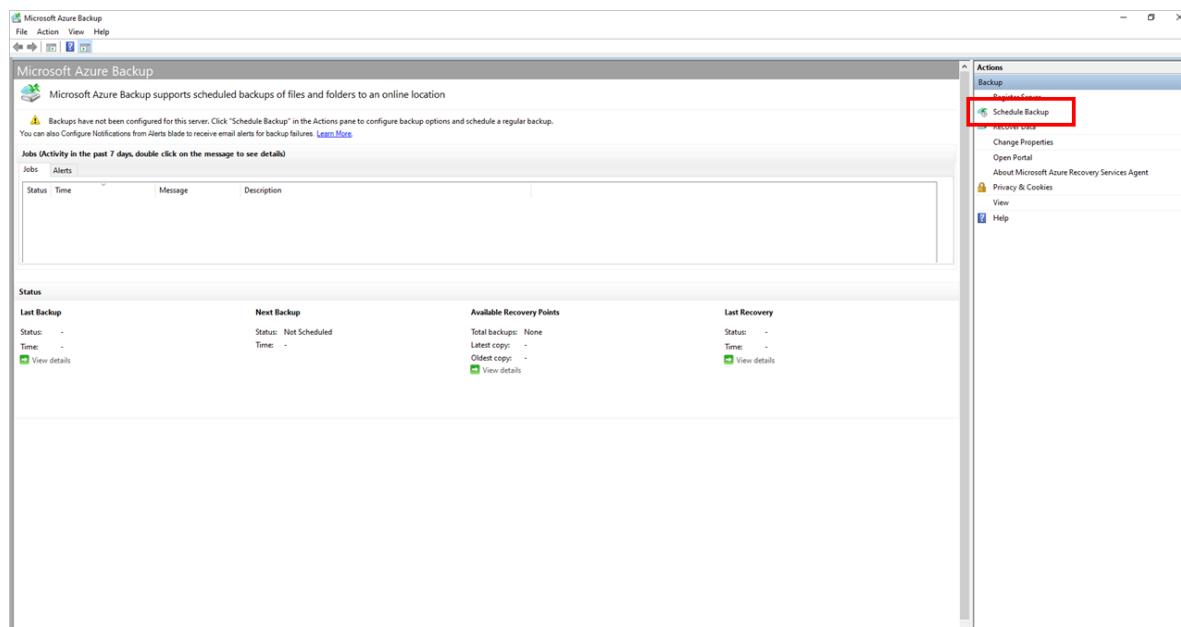
- The command window that opens as a result of the above command is in the Local System context. Use this command window to execute the steps to mount the Azure Page Blob Share as a network drive on your Windows Server.
- Follow the steps [here](#) to connect your server with the MARS Agent to the Data Box device via NFS and execute the following command on the Local System command prompt to mount the Azure Page Blobs share:

```
mount -o noblock \\<DeviceIPAddress>\<StorageAccountName_PageBlob X:
```

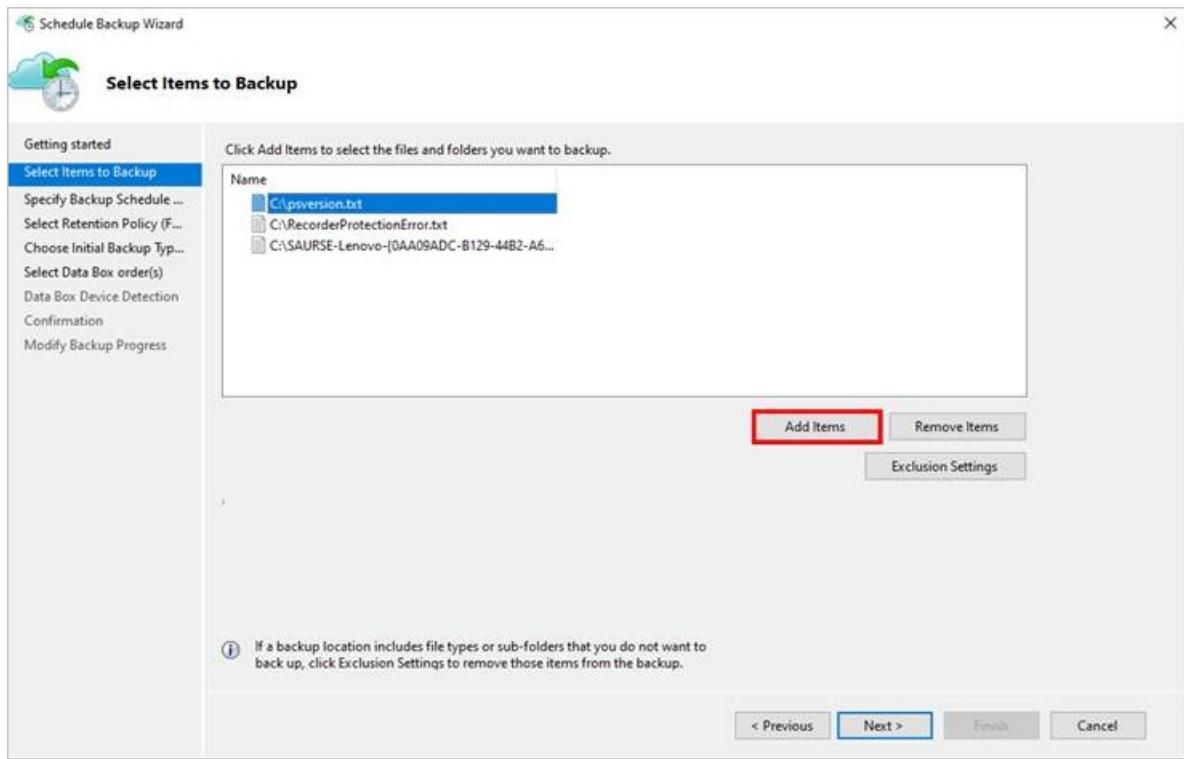
- Once mounted, check if you can access X: from your server. If yes, continue with the next section of this article.

## Transfer Initial Backup data to Azure Data Box device(s)

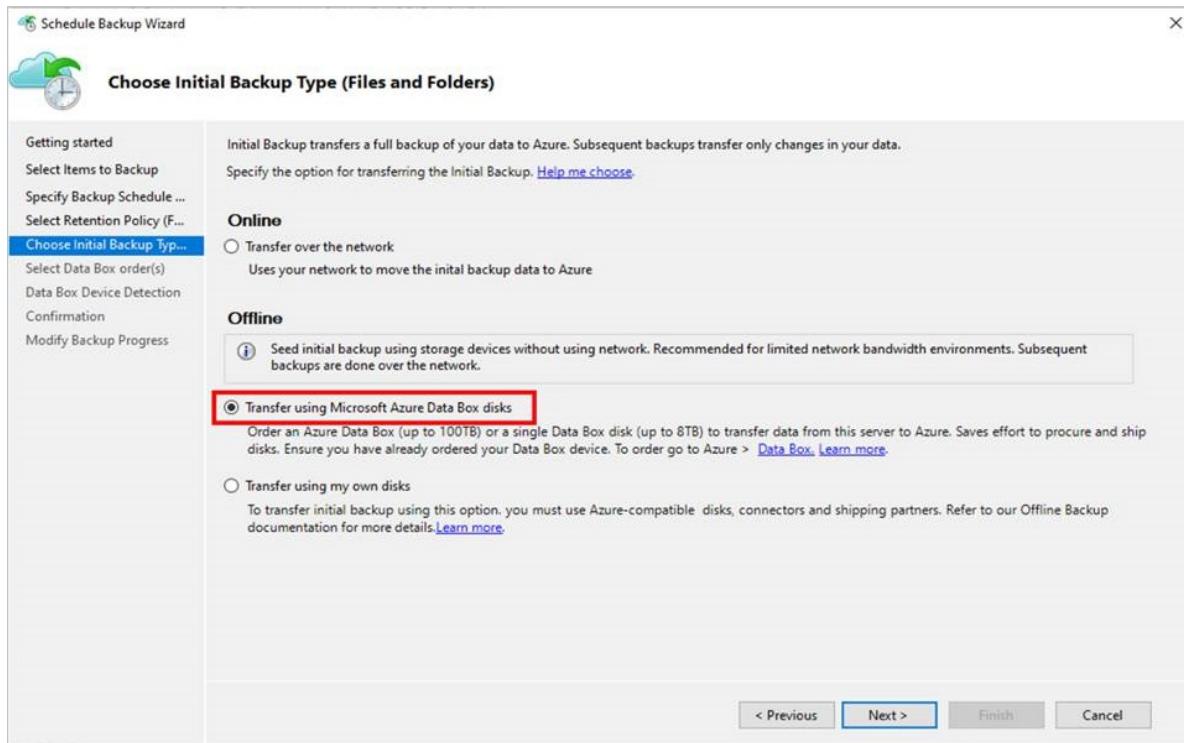
- Open the **Microsoft Azure Backup** application on your server.
- Click on **Schedule Backup** in the **Actions** pane.



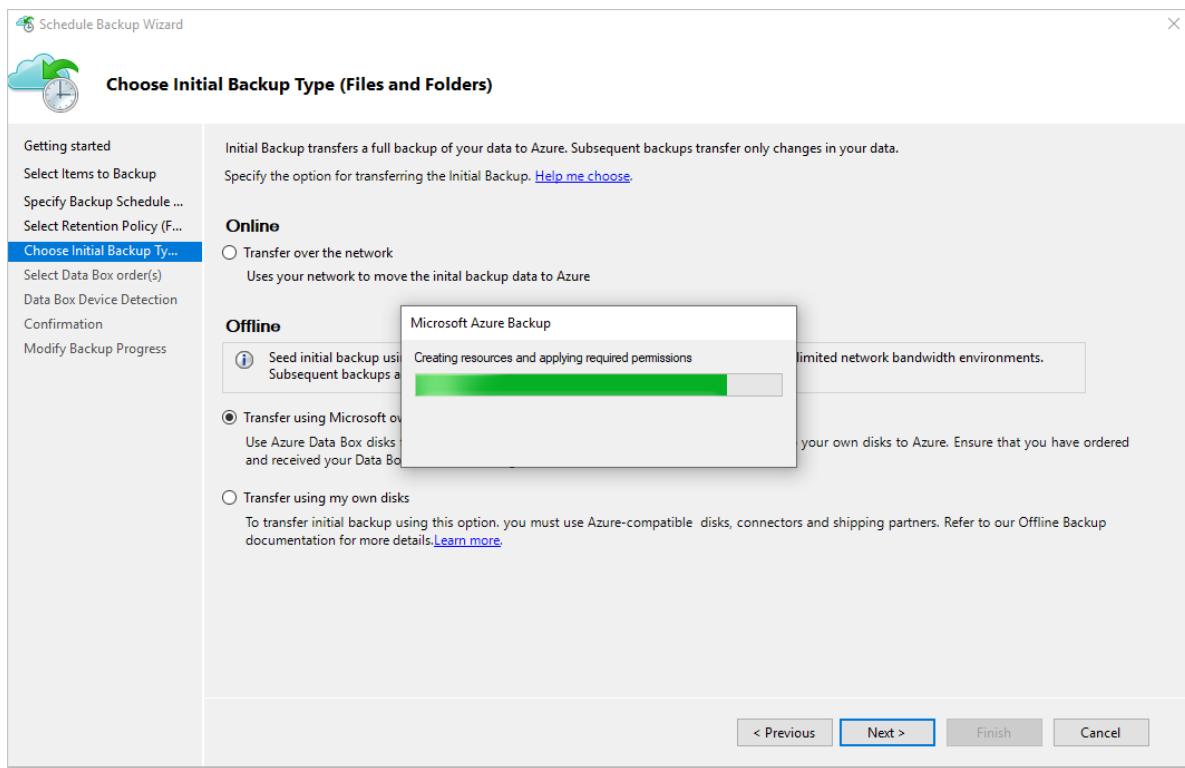
- Follow the steps in the **Schedule Backup Wizard**
- **Add Items** such that the total size of the items is within [size limits supported by the Azure Data Box SKU](#) you ordered and received.



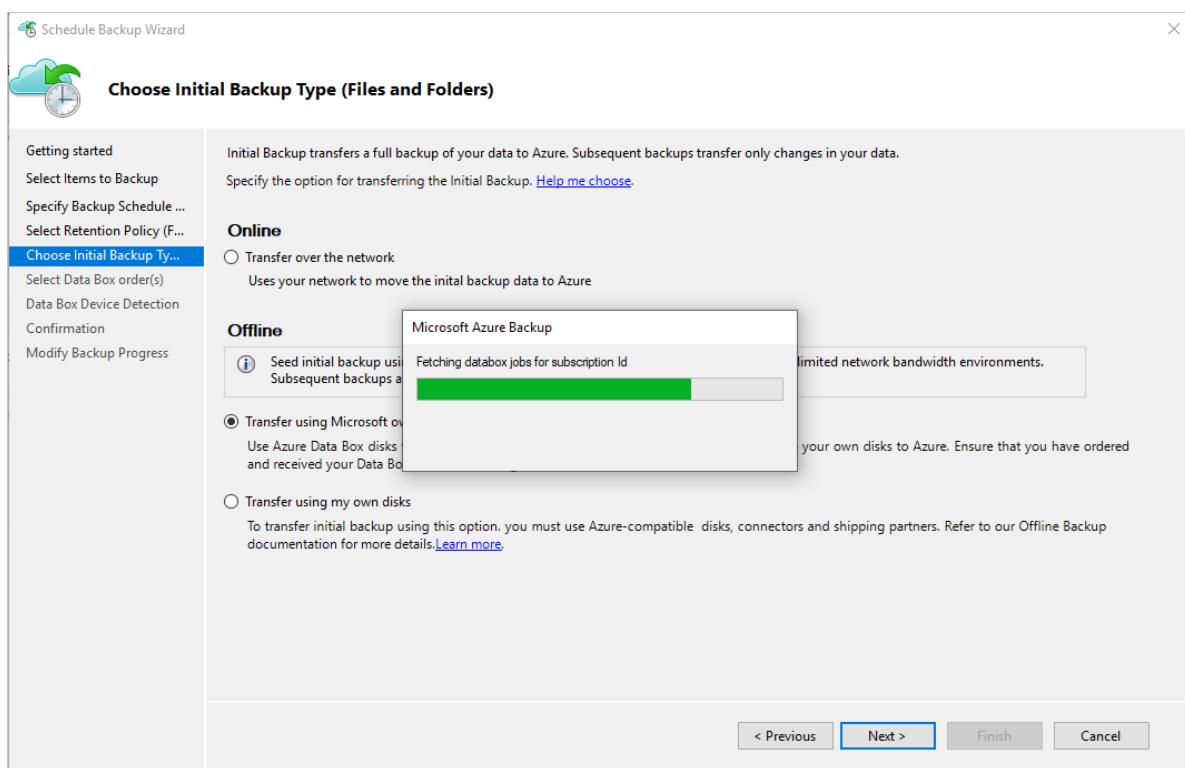
- Select the appropriate backup schedule and retention policy for Files and Folders and System State (system state is applicable only for Windows Servers and not for Windows Clients)
- On the **Choose Initial Backup Type (Files and Folders)** screen of the wizard, choose the option **Transfer using Microsoft Azure Data Box disks** and click **Next**



- Sign in to Azure when prompted using the user credentials that have owner access on the Azure Subscription. After you succeed in doing so, you should see a screen that resembles the one below:



- The MARS Agent will then fetch the Data Box jobs in the subscription that are in "Delivered" state.



- Select the correct Data box order for which you have unpacked, connected, and unlocked your Data Box disk. Click **Next**.

Schedule Backup Wizard

### Select Data Box order(s)

Getting started  
Select Items to Backup  
Specify Backup Schedule ...  
Select Retention Policy (F...  
Choose Initial Backup Ty...  
**Select Data Box order(s)**  
Data Box Device Detection  
Confirmation  
Modify Backup Progress

Choose one or more Azure Data Box order(s) from the table below.  
Only Orders in the same subscription as the Recovery Services Vault and in Delivered state are displayed  
To order Azure Data Box go to Azure > [Data Box](#). [Learn more](#).

Refresh      Last Refreshed on: 2/18/2019 6:46:05 PM

| Order Name       | Model       | Usable Capacity | Address                                       |
|------------------|-------------|-----------------|-----------------------------------------------|
| Sauseinitialseed | DataBoxDisk | 0TB             | Orlando Convention Center, Orlando, 32819, US |

Total Usable Capacity of selected orders : 0TB      [Why can't I see my order here?](#)

< Previous    Next >    Finish    Cancel

- Click on **Detect Device** on the **Data Box Device Detection** screen. This makes the MARS Agent scan for locally attached Azure Data Box disks and detect them as shown below:

Schedule Backup Wizard

### Data Box Device Detection

Getting started  
Select Items to Backup  
Specify Backup Schedule ...  
Select Retention Policy (F...  
Choose Initial Backup Ty...  
**Select Data Box order(s)**  
**Data Box Device Detection**  
Confirmation  
Modify Backup Progress

① Connect your received Data Box disks locally for automatic detection. Enter the network-connected Data Box devices when prompted, after clicking "Detect Devices". Ensure to unlock your Data Box device before clicking "Detect Device".

**Device detect status:** Success

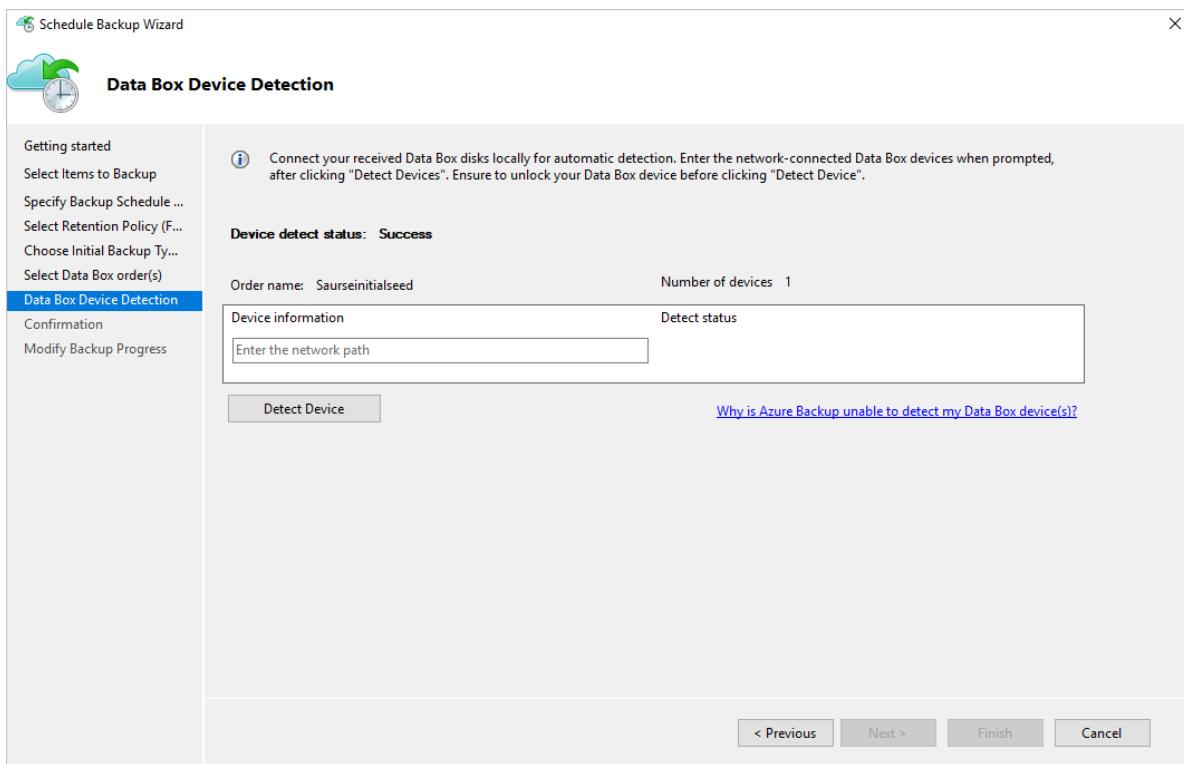
Order name: Sauseinitialseed      Number of devices 1

| Device information                                | Detect status |
|---------------------------------------------------|---------------|
| \?\Volume\{e4498839-0000-0000-0000-100000000000}\ |               |

**Detect Device**      [Why is Azure Backup unable to detect my Data Box device\(s\)?](#)

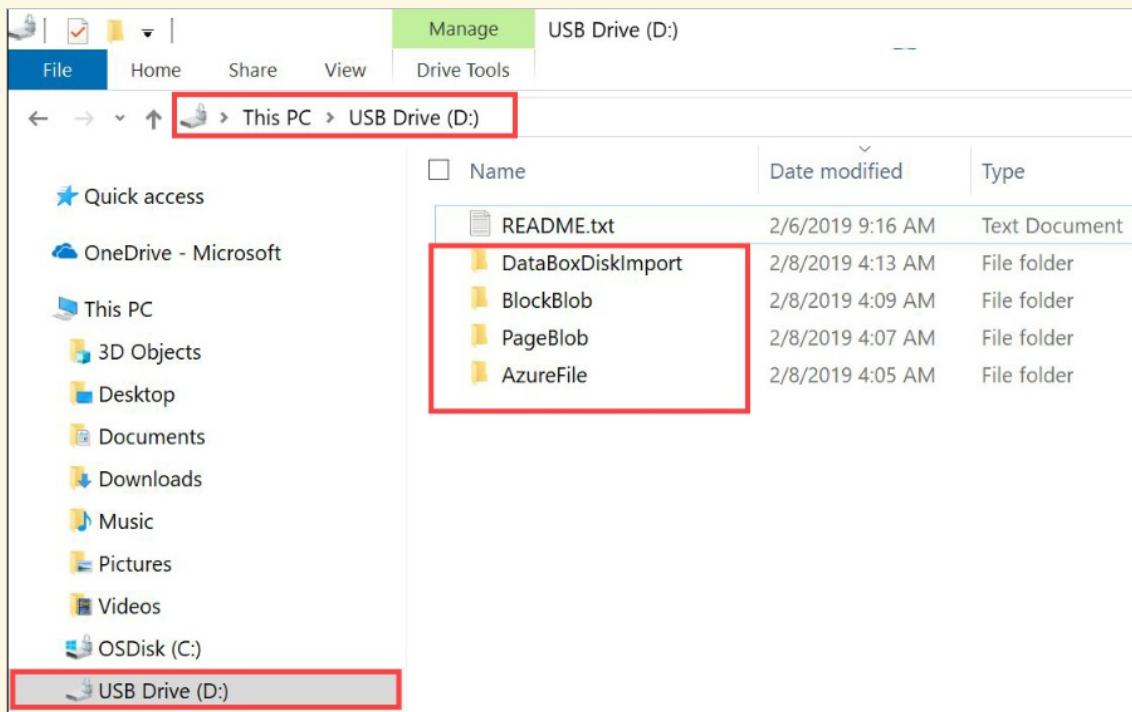
< Previous    Next >    Finish    Cancel

If you have connected the Azure Data Box as a Network Share (because of unavailability of USB ports or because you ordered and mounted the 100 TB Data Box device), detection will fail at first but will give you the option to enter the network path to the Data Box device as shown below:



### IMPORTANT

Provide the network path to the root directory of the Azure Data Box disk. This directory must contain a directory by the name *PageBlob* as shown below:

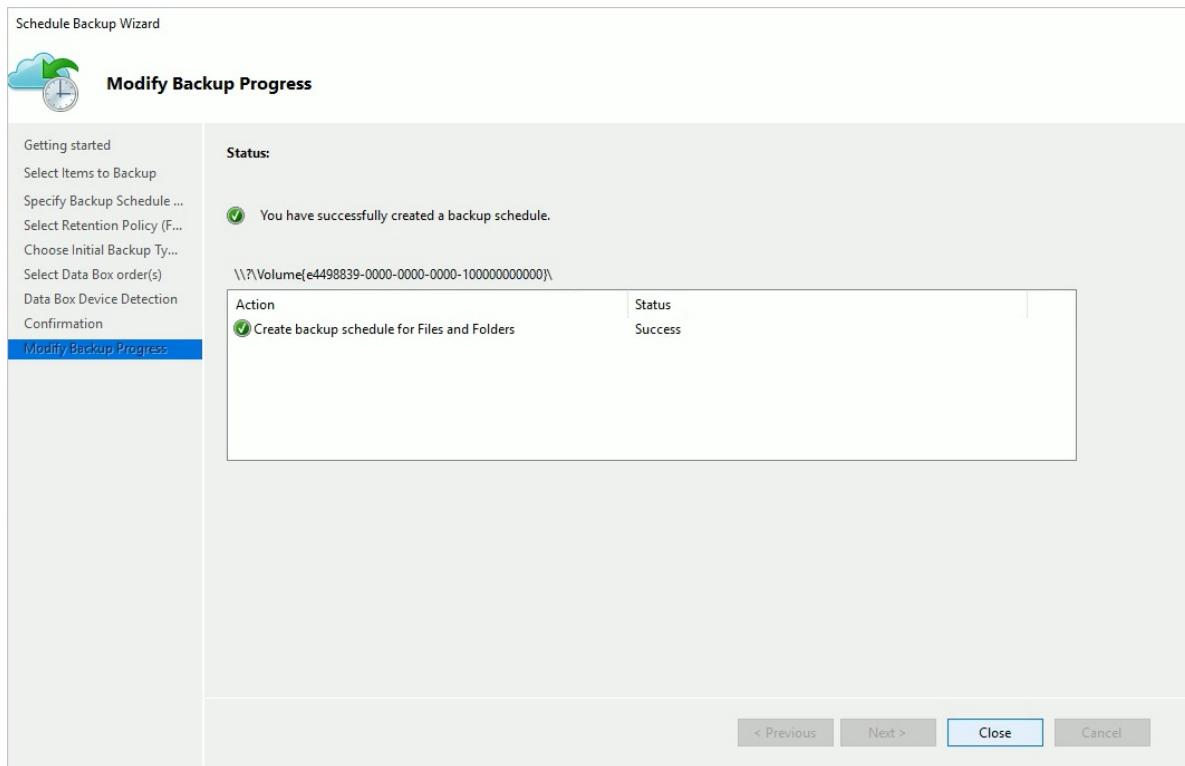


For example if the path of the disk is `\mydomain\myserver\disk1\` and *disk1* contains a directory called *PageBlob*, the path to be provided on the MARS Agent wizard is `\mydomain\myserver\disk1\`

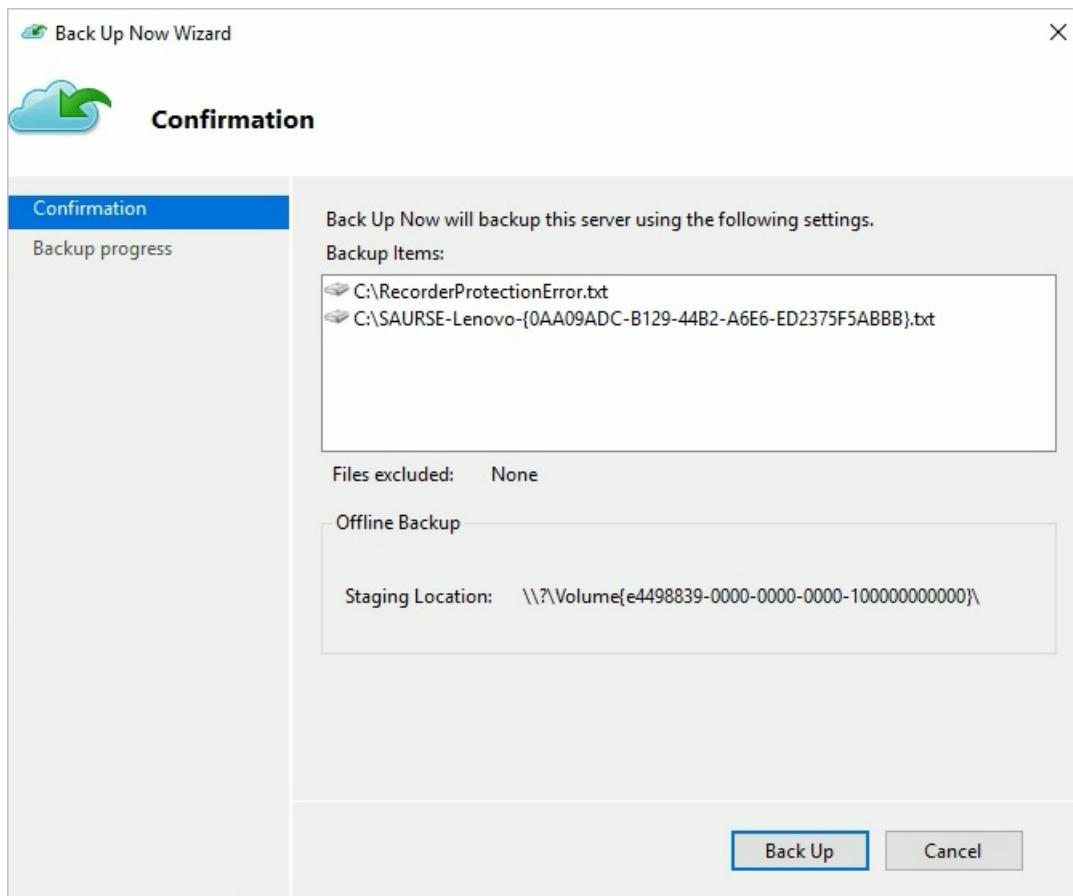
If you [setup an Azure Data Box 100 TB device](#), provide the following as the network path to the device

`\DeviceIPAddress\StorageAccountName_PageBlob`

- Click **Next** and click **Finish** on the next screen to save the Backup and Retention policy with the configuration of offline backup using Azure Data Box.
- The following screen confirms that the policy is saved successfully:

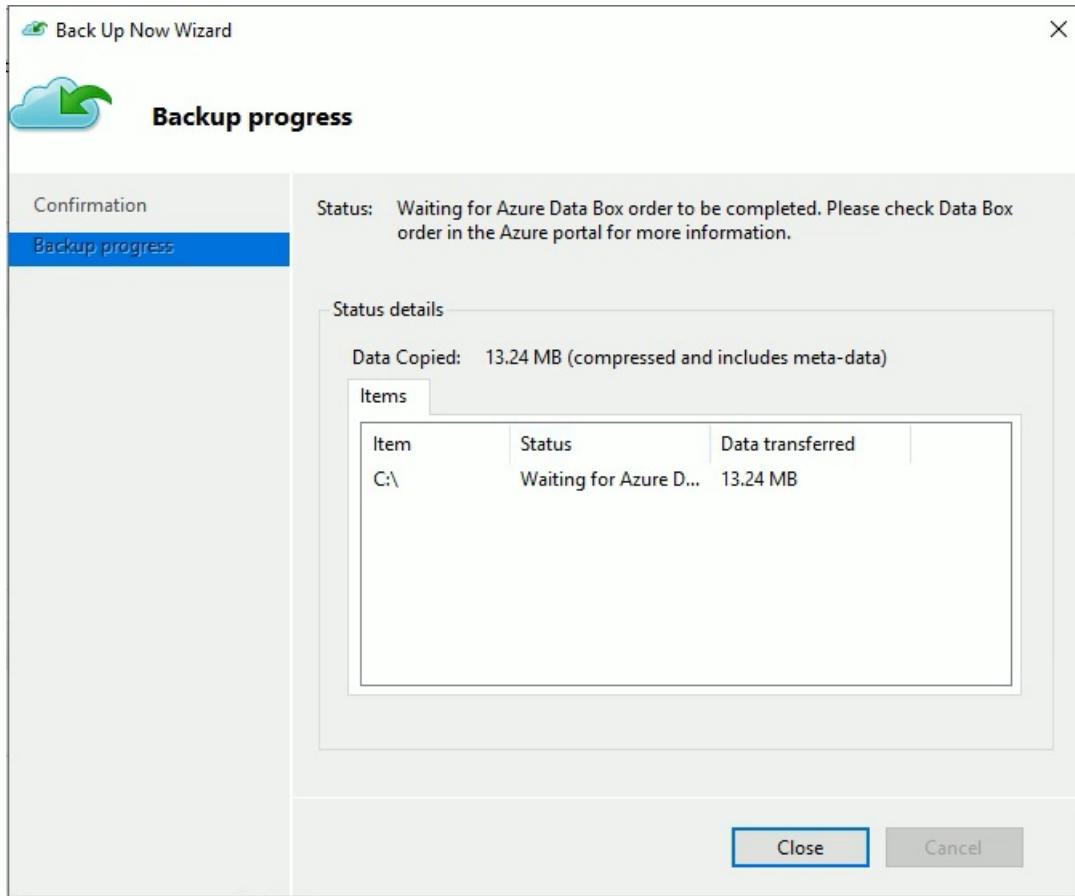


- Click **Close** on the screen above.
- Click on \***Back Up Now** in the **Actions** Pane of the MARS Agent console and click on **Back Up** in the wizard screen as shown below:



- The MARS Agent will start backing up the data you selected to the Azure Data Box device. This might take from several hours to a few days depending on the number of files and connection speed between the server with the MARS Agent and the Azure Data Box Disk.
- Once the backup of the data is complete, you will see a screen on the MARS Agent that resembles the one

below:



## Post-Backup steps

This section explains the steps to take once the backup of the data to the Azure Data Box Disk is successful.

- Follow the steps in this article to [ship the Azure Data Box disk to Azure](#). If you used an Azure Data Box 100-TB device, follow these steps to [ship the Azure Data Box to Azure](#).
- [Monitor the Data Box job](#) in the Azure portal. Once the Azure Data Box job is “Complete”, the MARS Agent will automatically move the data from the Storage Account to the Recovery Services Vault at the time of the next scheduled backup. It will then mark the backup job as “Job Completed” if a recovery point is successfully created.

### NOTE

The MARS Agent will trigger backups at the times scheduled during policy creation. However these jobs will flag “Waiting for Azure Data Box job to be completed” until the time the job is complete.

- After the MARS Agent successfully creates a recovery point corresponding to the initial backup, you may delete the Storage Account (or specific contents) associated with the Azure Data Box job.

## Troubleshooting

The Microsoft Azure Backup (MAB) agent creates an Azure AD application for you in your tenant. This application requires a certificate for authentication that is created and uploaded when configuring offline seeding policy. We use Azure PowerShell for creating and uploading the certificate to the Azure AD Application.

### Issue

At the time of configuring offline backup you may face an issue, where due to a bug in the Azure PowerShell

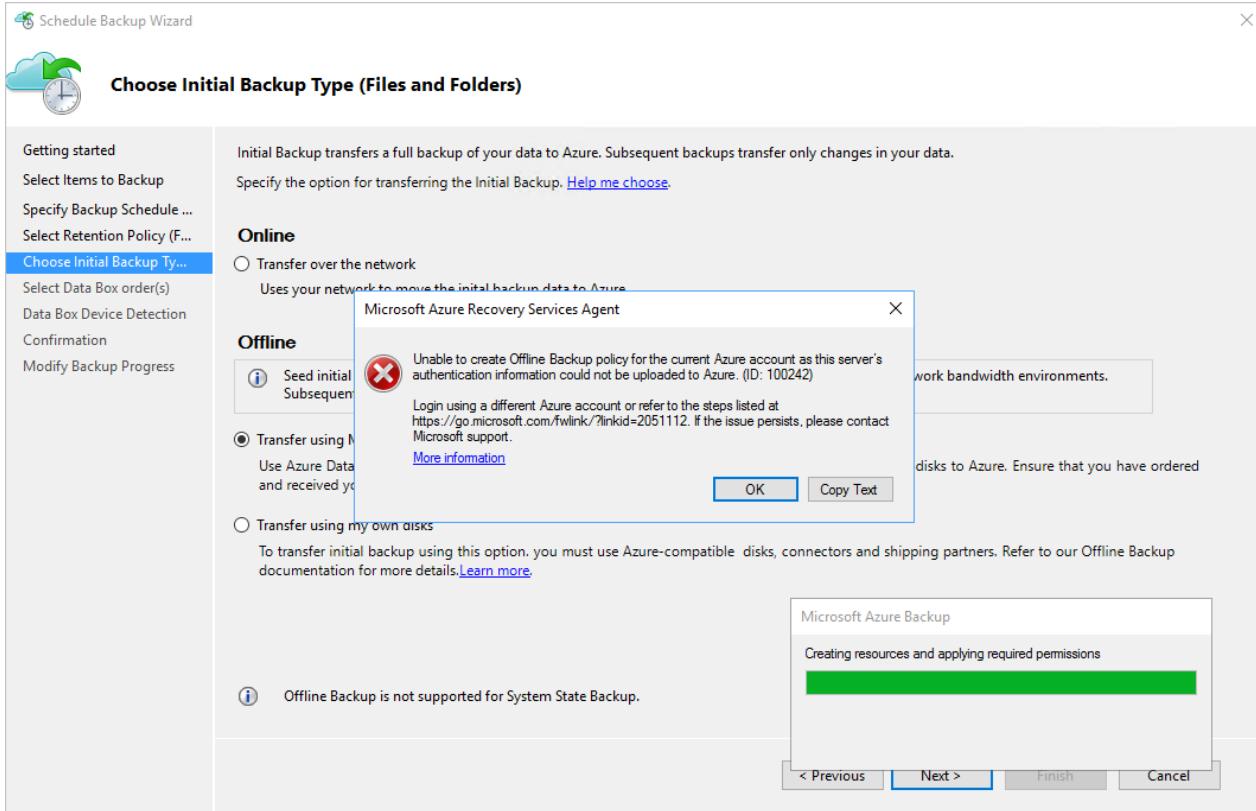
cmdlet you are unable to add multiple certificates to the same Azure AD Application created by the MAB agent. This will impact you if you have configured offline seeding policy for the same or a different server.

## How to verify if the issue is caused by this specific root cause

To ensure that the failure is due to the issue above, perform one of the following steps:

### Step 1

Check if you see the following error message in the MAB console at the time of configuring offline backup:



### Step 2

- Open the **Temp** folder in the installation path (default temp folder path is `C:\Program Files\Microsoft Azure Recovery Services Agent\Temp`). Look for the **CBUICurr** file and open the file.
- In the **CBUICurr** file, scroll to the last line and check if the failure is due to

```
Unable to create an Azure AD application credential in customer's account. Exception: Update to existing credential with KeyId <some guid> is not allowed
```

## Workaround

As a work-around to resolve this issue, perform the following steps and retry the policy configuration.

### First step

Sign in to PowerShell that appears on the MAB UI using a different account with admin access on the subscription that will have the import export job created.

### Second step

If no other server has offline seeding configured and no other server is dependent on the `AzureOfflineBackup_<Azure User Id>` application, then delete this application from **Azure portal** > **Azure Active Directory** > **App registrations**.

## NOTE

Check if the application `AzureOfflineBackup_<Azure User Id>` does not have any other offline seeding configured and also no other server is dependent on this application. Go to **Settings > Keys** under the **Public Keys** section it should not have any other public keys added. See the following screenshot for reference:

| DESCRIPTION     | EXPIRES   | VALUE  |
|-----------------|-----------|--------|
| Key description | 7/27/2019 | Hidden |

| THUMBPRINT                                | START DATE | EXPIRES    |
|-------------------------------------------|------------|------------|
| 5B0E4906014C08580F1294192B000348871EBF54  | 3/7/2018   | 4/13/2019  |
| 0FF92406E29A31D1651E52DCAE1A1F808888929   | 11/16/2018 | 12/21/2019 |
| BCACE640DF3FCA2FA6F132A9DDE5C6D6EB4C229C5 | 9/16/2018  | 10/21/2019 |
| 728748A50711B25ABAC28CDAB821DD6D217856C2  | 9/20/2018  | 10/26/2019 |
| BCACE640DF3FCA2FA6F132A9DDE5C6D6EB4C229C5 | 9/16/2018  | 10/21/2019 |

## Third step

From the server you are trying to configure offline backup, perform the following actions:

1. Open the **Manage computer certificate application** > **Personal** tab and look for the certificate with the name `CB_AzureADCertforOfflineSeeding_<ResourceId>`
2. Select the above certificate, right-click **All Tasks** and **Export** without private key, in the .cer format.
3. Go to the Azure Offline Backup application mentioned in **point 2**. In the **Settings > Keys > Upload Public Key**, upload the certificate exported in the step above.

Settings

GENERAL

- Properties
- Reply URLs
- Owners

API ACCESS

- Required permissions
- Keys

Keys

Upload a certificate (public key) with one of the following file types: .cer, .pem, .crt

Select a file...

Cancel

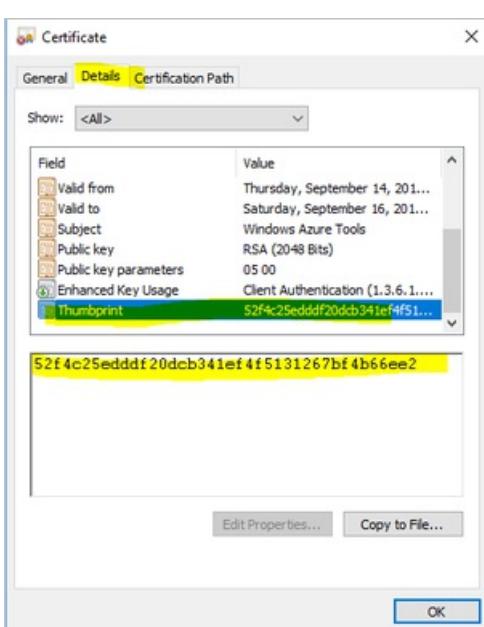
4. In the server, open the registry by typing **regedit** in the run window.
5. Go to the registry `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Azure Backup\Config\CloudBackupProvider`. Right-click on **CloudBackupProvider** and add a new string value with name `AzureADAppCertThumbprint_<Azure User Id>`

#### NOTE

To get the Azure User Id perform one of the following actions:

1. From the Azure connected PowerShell run the  
`Get-AzureRmADUser -UserPrincipalName "Account Holder's email as defined in the portal"` command.
2. Navigate to the registry path: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Azure Backup\DbgSettings\OnlineBackup`; Name: `CurrentUserld`

6. Right-click on the string added in the step above and select **Modify**. In the value, provide the thumbprint of the certificate you exported in **point 2** and click **OK**.
7. To get the value of thumbprint, double-click on the certificate, then select the **Details** tab and scroll down until you see the thumbprint field. Click on **Thumbprint** and copy the value.



## Questions

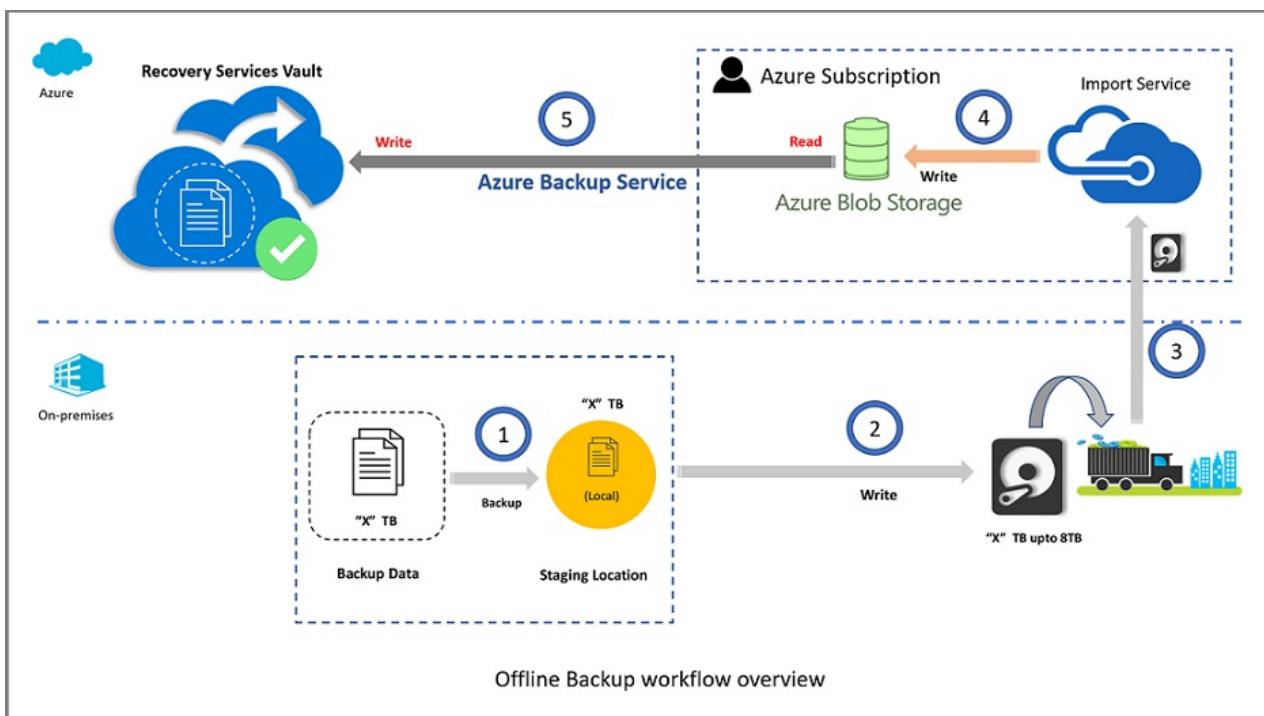
For any questions or clarifications, regarding any issues faced, reach out to [AskAzureBackupTeam@microsoft.com](mailto:AskAzureBackupTeam@microsoft.com)

# Offline-backup workflow in Azure Backup

2/4/2020 • 11 minutes to read • [Edit Online](#)

Azure Backup has several built-in efficiencies that save network and storage costs during the initial full backups of data to Azure. Initial full backups typically transfer large amounts of data and require more network bandwidth when compared to subsequent backups that transfer only the deltas/incrementals. Through the process of offline seeding, Azure Backup can use disks to upload the offline backup data to Azure.

The Azure Backup offline-seeding process is tightly integrated with the [Azure Import/Export service](#) that enables you to transfer initial backup data to Azure by using disks. If you have terabytes (TBs) of initial backup data that needs to be transferred over a high-latency and low-bandwidth network, you can use the offline-seeding workflow to ship the initial backup copy, on one or more hard drives, to an Azure datacenter. The following image provides an overview of the steps in the workflow.



The offline backup process involves the following steps:

1. Instead of sending the backup data over the network, write the backup data to a staging location.
2. Use the AzureOfflineBackupDiskPrep utility to write the data in the staging location to one or more SATA disks.
3. As part of the preparatory work, the AzureOfflineBackupDiskPrep utility creates an Azure Import job. Send the SATA drives to the nearest Azure datacenter, and reference the import job to connect the activities.
4. At the Azure datacenter, the data on the disks is copied to an Azure storage account.
5. Azure Backup copies the backup data from the storage account to the Recovery Services vault, and incremental backups are scheduled.

## Supported configurations

The following Azure Backup features or workloads support use of Offline Backup.

- Backup of files and folders with the Microsoft Azure Recovery Services (MARS) agent, also referred to as the Azure Backup agent.
- Backup of all workloads and files with System Center Data Protection Manager (SC DPM)

- Backup of all workloads and files with Microsoft Azure Backup Server

**NOTE**

Offline Backup is not supported for System State backups done using the Azure Backup agent.

## Upgrade the MARS agent

Versions of the Microsoft Azure Recovery Service (MARS) agent below 2.0.9083.0 have a dependency on the Azure Access Control service (ACS). The MARS agent is also referred to as the Azure Backup agent. In 2018, Azure [deprecated the Azure Access Control service \(ACS\)](#). Beginning March 19, 2018, all versions of the MARS agent below 2.0.9083.0 will experience backup failures. To avoid or resolve backup failures, [upgrade your MARS agent to the latest version](#). To identify servers that require a MARS agent upgrade, follow the steps in the [Backup blog for upgrading MARS agents](#). The MARS agent is used to back up files and folders, and system state data to Azure. System Center DPM and Azure Backup Server use the MARS agent to back up data to Azure.

## Prerequisites

**NOTE**

The following prerequisites and workflow apply only to Offline backup of files and folders using the [latest MARS agent](#). To perform Offline backups for workloads using System Center DPM or Azure Backup Server, refer to [this article](#).

Before initiating the Offline Backup workflow, complete the following prerequisites:

- Create a [Recovery Services vault](#). To create a vault, refer to the steps in [this article](#)
- Make sure that only the [latest version of the Azure Backup agent](#) has been installed on the Windows Server/Windows client, as applicable and the computer is registered with the Recovery Services Vault.
- Azure PowerShell 3.7.0 is required on the computer running Azure Backup agent. It is recommended that you download and [install the 3.7.0 version of Azure PowerShell](#).
- On the computer running Azure Backup agent, make sure Microsoft Edge or Internet Explorer 11 is installed, and JavaScript is enabled.
- Create an Azure Storage account in the same subscription as the Recovery Services vault.
- Make sure you have the [necessary permissions](#) to create the Azure Active Directory application. The Offline Backup workflow creates an Azure Active Directory application in the subscription associated with the Azure Storage account. The goal of the application is to provide Azure Backup with secure and scoped access to the Azure Import Service, required for the Offline Backup workflow.
- Register the Microsoft.ImportExport resource provider with the subscription containing the Azure Storage account. To register the resource provider:
  1. In the main menu, Click **Subscriptions**.
  2. If you are subscribed to multiple subscriptions, select the subscription you're using for the offline backup. If you use only one subscription, then your subscription appears.
  3. In the subscription menu, click **Resource Providers** to view the list of providers.
  4. In the list of providers scroll down to Microsoft.ImportExport. If the Status is NotRegistered, click **Register**.

| PROVIDER                      | STATUS     | Re-register | Unregister |
|-------------------------------|------------|-------------|------------|
| Microsoft.ClassicCompute      | Registered |             |            |
| Microsoft.ClassicNetwork      | Registered |             |            |
| Microsoft.ClassicStorage      | Registered |             |            |
| Microsoft.Commerce            | Registered |             |            |
| Microsoft.Compute             | Registered |             |            |
| Microsoft.ContainerService    | Registered |             |            |
| Microsoft.DataFactory         | Registered |             |            |
| Microsoft.DevTestLab          | Registered |             |            |
| Microsoft.DocumentDB          | Registered |             |            |
| Microsoft.HDInsight           | Registered |             |            |
| <b>Microsoft.ImportExport</b> | Registered | Re-register | Unregister |
| microsoft.insights            | Registered | Re-register | Unregister |
| Microsoft.KeyVault            | Registered | Re-register | Unregister |
| Microsoft.MachineLearning     | Registered | Re-register | Unregister |
| Microsoft.ManagedIdentity     | Registered | Re-register | Unregister |
| Microsoft.MobileEngagement    | Registered | Re-register | Unregister |
| Microsoft.Network             | Registered | Re-register | Unregister |
| Microsoft.OperationalInsights | Registered | Re-register | Unregister |

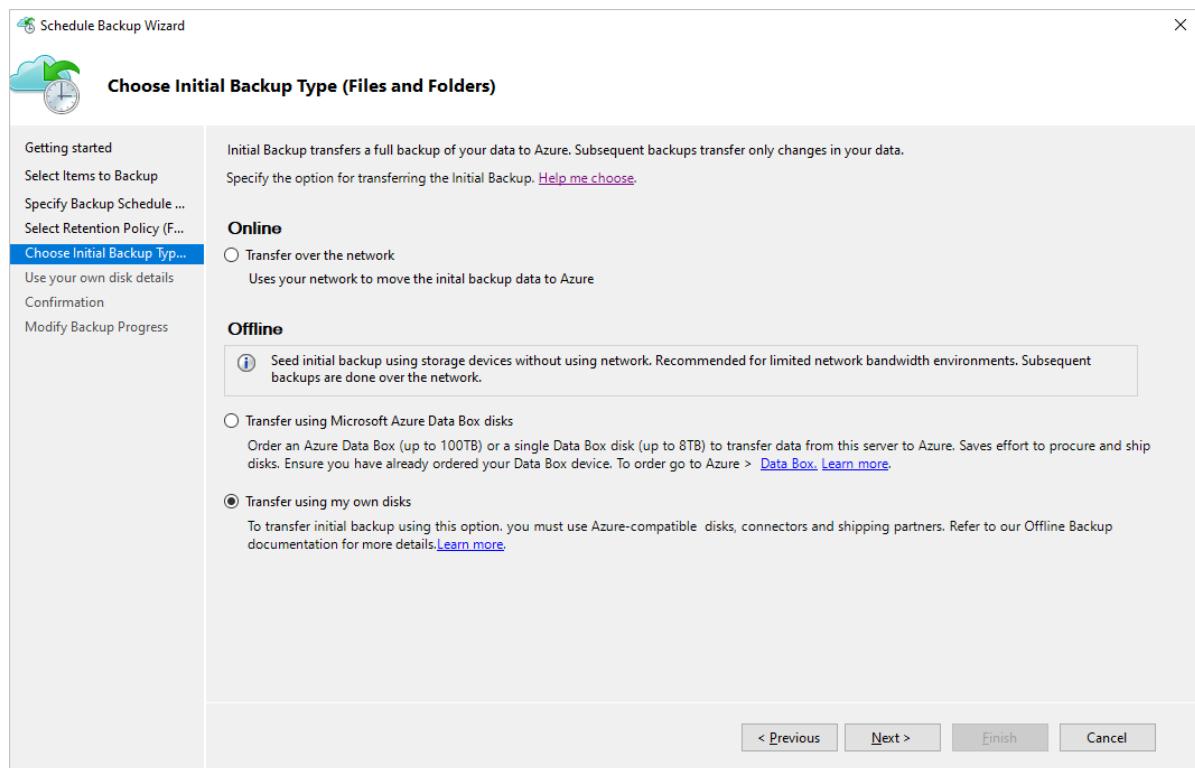
- A staging location, which might be a network share or any additional drive on the computer, internal or external, with enough disk space to hold your initial copy, is created. For example, if you are trying to back up a 500-GB file server, ensure that the staging area is at least 500 GB. (A smaller amount is used due to compression.)
- When sending disks to Azure, use only 2.5 inch SSD, or 2.5-inch or 3.5-inch SATA II/III internal hard drives. You can use hard drives up to 10 TB. Check the [Azure Import/Export service documentation](#) for the latest set of drives that the service supports.
- The SATA drives must be connected to a computer (referred to as a *copy computer*) from where the copy of backup data from the *staging location* to the SATA drives is done. Ensure that BitLocker is enabled on the *copy computer*.

## Workflow

This section describes the offline-backup workflow so that your data can be delivered to an Azure datacenter and uploaded to Azure Storage. If you have questions about the Import service or any aspect of the process, see the [Import service overview documentation](#).

### Initiate offline backup

1. When you schedule a backup on the MARS Agent, you see the following screen.

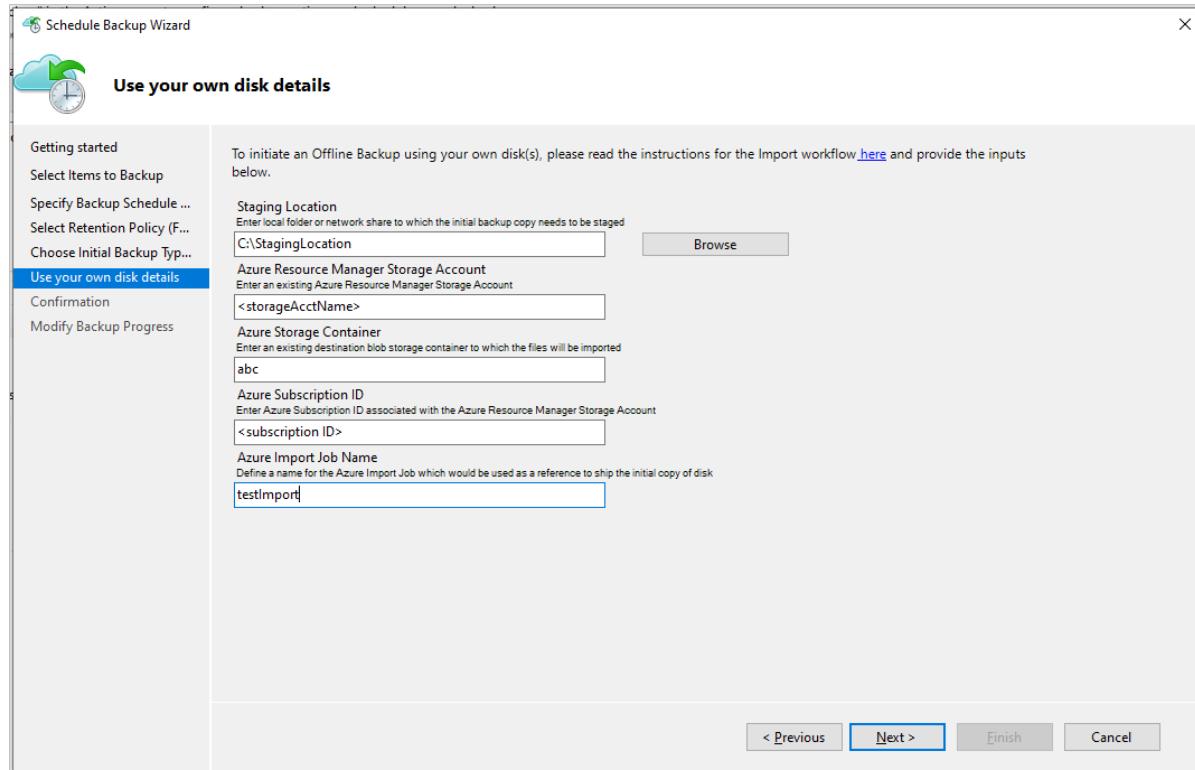


## 2. Select the option **Transfer using my own disks**.

### NOTE

We recommend using the Azure Data Box option to transfer initial backup data offline. This option saves the effort required to procure your own Azure-compatible disks by delivering Microsoft-proprietary, secure and tamper-proof Azure Data box devices to which backup data can be directly written to by the MARS Agent.

## 3. Click **Next** and fill in the inputs carefully:



The description of the inputs is as follows:

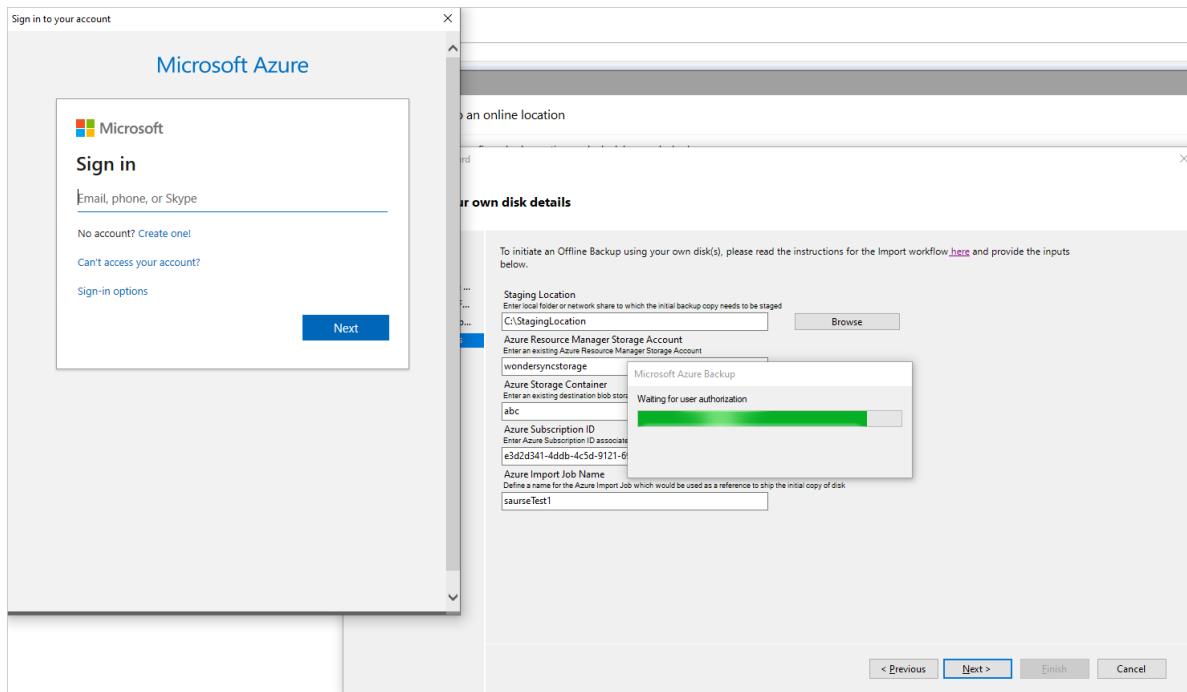
- **Staging Location:** The temporary storage location to which the initial backup copy is written. Staging

location might be on a network share or a local computer. If the copy computer and source computer are different, we recommend that you specify the full network path of the staging location.

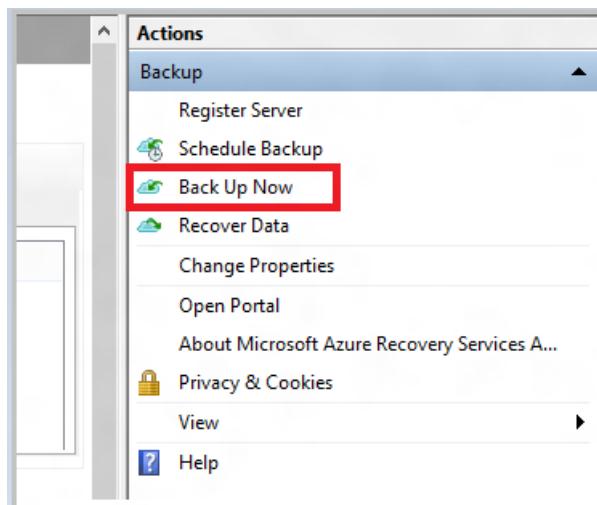
- **Azure Resource Manager Storage Account:** The name of the Resource Manager type storage account (general purpose v1 or general purpose v2) in any Azure subscription.
- **Azure Storage Container:** The name of the destination storage blob in the Azure Storage account where the backup data is imported before being copied to the Recovery Services vault.
- **Azure Subscription ID:** The ID for the Azure subscription where the Azure Storage account is created.
- **Azure Import Job Name:** The unique name by which Azure Import service and Azure Backup track the transfer of data sent on disks to Azure.

Provide the inputs on the screen and click **Next**. Save the provided *Staging location* and the *Azure Import Job Name*, as this information is required to prepare the disks.

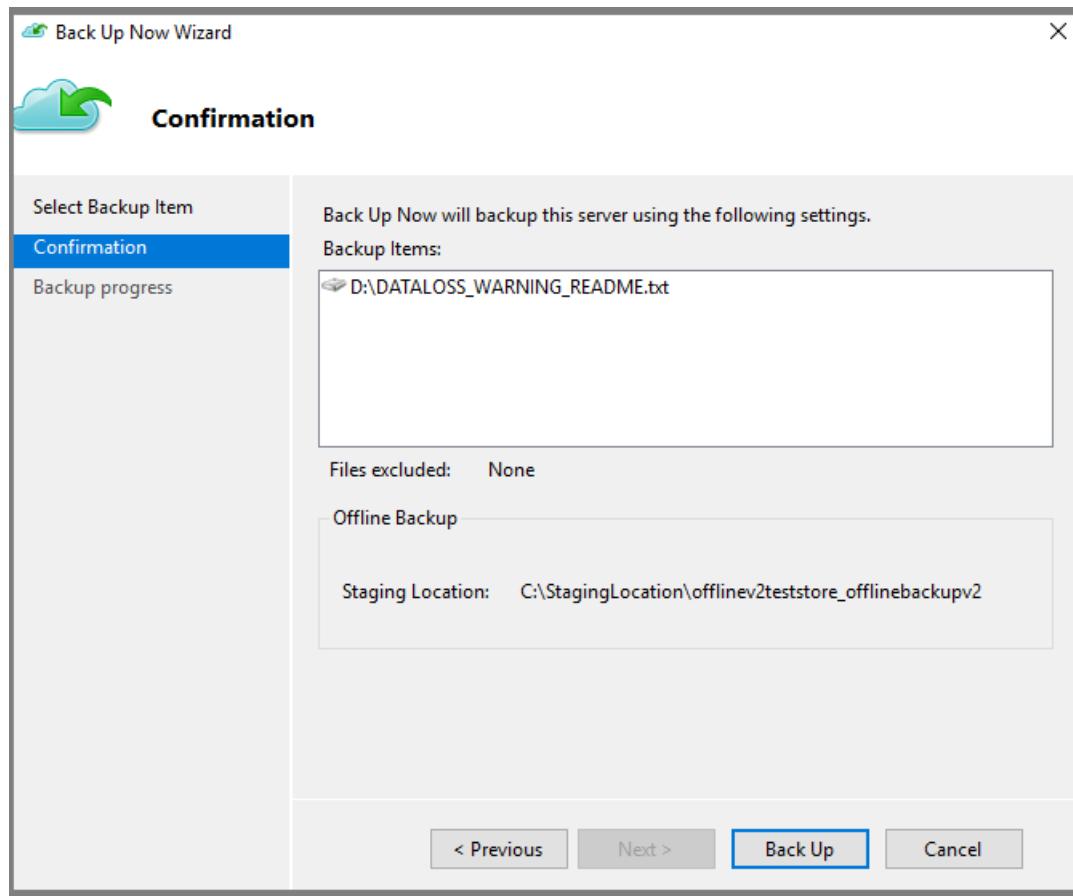
4. When prompted, sign into your Azure subscription. You must sign in so that Azure Backup can create the Azure Active Directory application, and provide the required permissions to access the Azure Import Service.



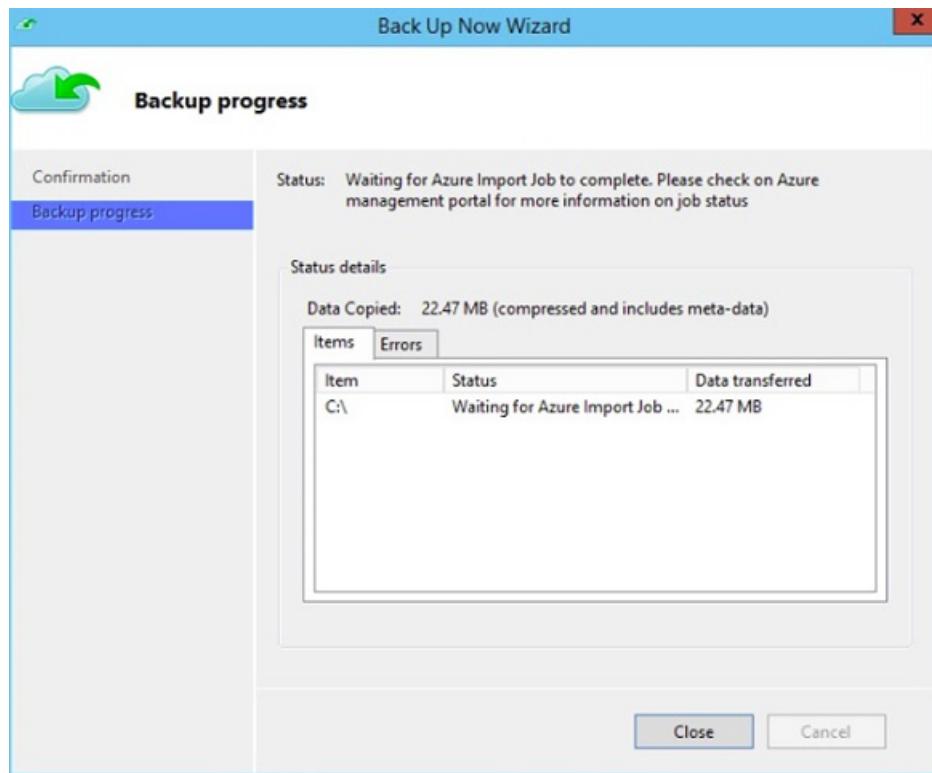
5. Complete the workflow, and in the Azure Backup agent console click **Back Up Now**.



6. In the Confirmation page of the wizard, click **Back Up**. The initial backup is written to the staging area as part of the setup.



After the operation finishes, the staging location is ready to be used for disk preparation.



## Prepare SATA drives and ship to Azure

The *AzureOfflineBackupDiskPrep* utility prepares the SATA drives that are sent to the nearest Azure datacenter. This utility is available in the Azure Backup agent installation directory (in the following path):

```
\Microsoft Azure Recovery Services Agent\Utils
```

1. Go to the directory and copy the **AzureOfflineBackupDiskPrep** directory to another computer where the SATA drives are connected. On the computer with the connected SATA drives, ensure:

- The copy computer can access the staging location for the offline-seeding workflow by using the same network path that was provided in the **Initiate offline backup** workflow.
- BitLocker is enabled on the copy computer.
- Azure PowerShell 3.7.0 is installed.
- The latest compatible browsers (Microsoft Edge or Internet Explorer 11) are installed and JavaScript is enabled.
- The copy computer can access the Azure portal. If necessary, the copy computer can be the same as the source computer.

**IMPORTANT**

If the source computer is a virtual machine, then the copy computer must be a different physical server or client machine from the source computer.

2. Open an elevated command prompt on the copy computer with the *AzureOfflineBackupDiskPrep* utility directory as the current directory, and run the following command:

```
.\AzureOfflineBackupDiskPrep.exe s:<Staging Location Path>
```

| PARAMETER                       | DESCRIPTION                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| s:<Staging Location Path>       | Mandatory input used to provide the path to the staging location that you entered in the <b>Initiate offline backup</b> workflow.                         |
| p:<Path to PublishSettingsFile> | Optional input that's used to provide the path to the <b>Azure Publish Settings</b> file that you entered in the <b>Initiate offline backup</b> workflow. |

When you run the command, the utility requests the selection of the Azure Import job that corresponds to the drives that need to be prepared. If only a single import job is associated with the provided staging location, you see a screen like the one that follows.

```
C:\Administrator: Command Prompt
C:\Program Files\Microsoft Azure Recovery Services Agent\Utils\AzureOfflineBackupDiskPrep>AzureOfflineBackupDiskPrep.exe s:C:\StagingLocation
Parsed input parameters successfully.
Session Started
Current Directory : C:\Program Files\Microsoft Azure Recovery Services Agent\Utils\AzureOfflineBackupDiskPrep
Tool Directory : C:\Program Files\Microsoft Azure Recovery Services Agent\Utils\AzureOfflineBackupDiskPrep\
Journal file name : Journalf2b9cc55-fa03-434c-bebe-09e11edd69c0.jrn

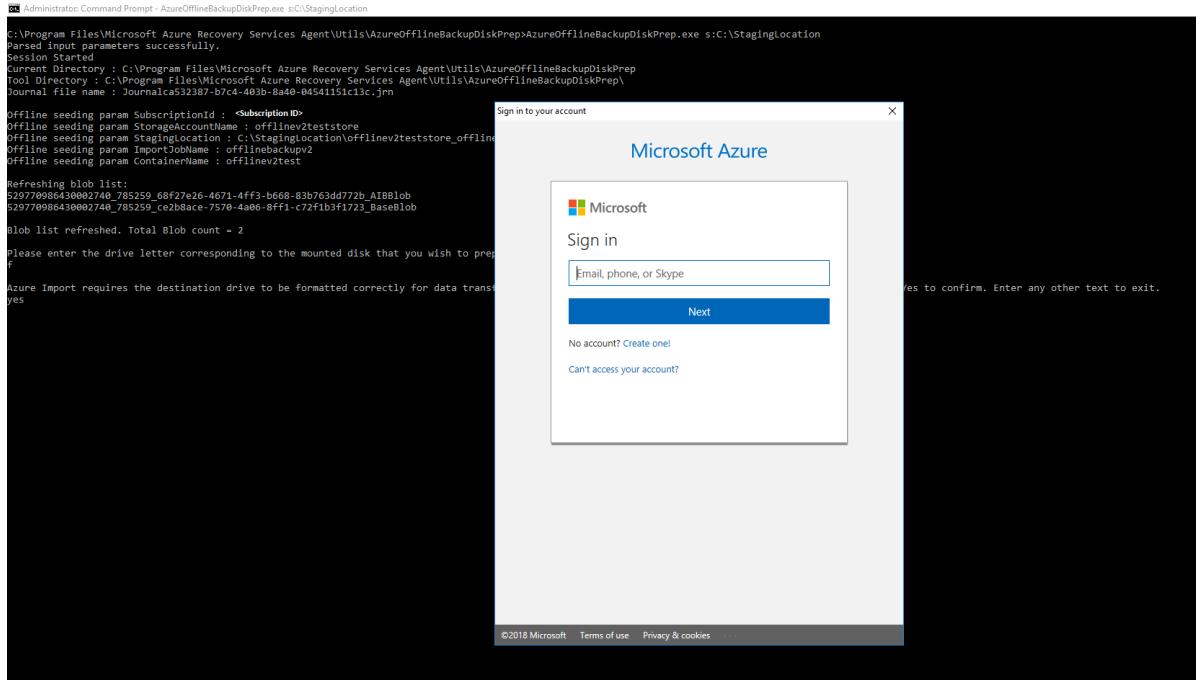
Offline seeding param SubscriptionId : <Subscription ID>
Offline seeding param StorageAccountName : offlinev2teststore
Offline seeding param StagingLocation : C:\StagingLocation\offlinev2teststore_offlinebackupv2
Offline seeding param ImportJobName : offlinebackupv2
Offline seeding param ContainerName : offlinev2test

Refreshing blob list:
529770986430002740_785259_68f27e26-4671-4ff3-b668-83b763dd772b_AIBBlob
529770986430002740_785259_ce2b8ace-7570-4a06-8ff1-c72f1b3f1723_BaseBlob

Blob list refreshed. Total Blob count = 2

Please enter the drive letter corresponding to the mounted disk that you wish to prepare.
F
```

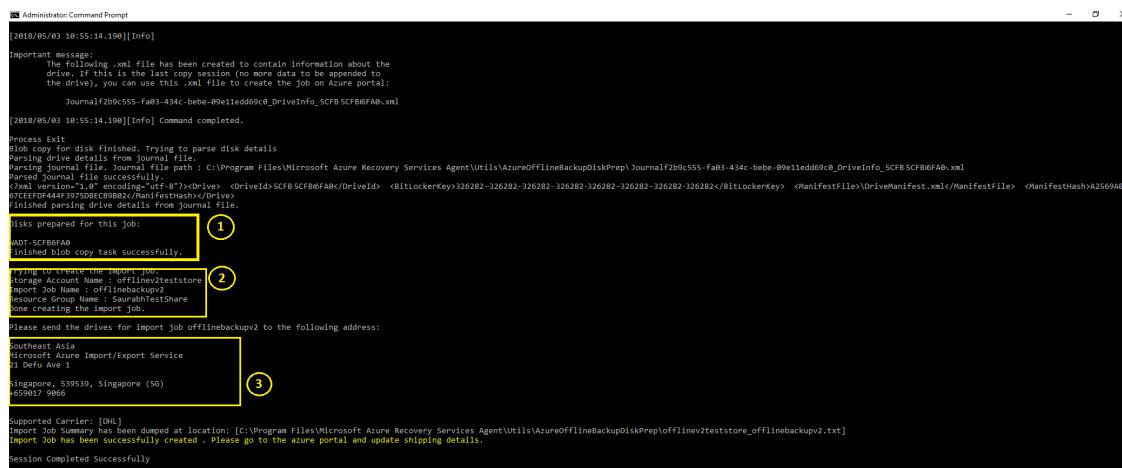
3. Enter the drive letter without the trailing colon for the mounted disk that you want to prepare for transfer to Azure.
4. Provide confirmation for the formatting of the drive when prompted.
5. You are prompted to sign into your Azure subscription. Provide your credentials.



The tool then begins to prepare the disk and copying the backup data. You may need to attach additional disks when prompted by the tool in case the provided disk does not have sufficient space for the backup data.

At the end of successful execution of the tool, the command prompt provides three pieces of information:

- a. One or more disks you provided are prepared for shipping to Azure.
- b. You receive confirmation that your import job has been created. The import job uses the name you provided.
- c. The tool displays the shipping address for the Azure datacenter.



6. At the end of the command execution, you can update the shipping information.
7. Ship the disks to the address that the tool provided and keep the tracking number for future reference.

## IMPORTANT

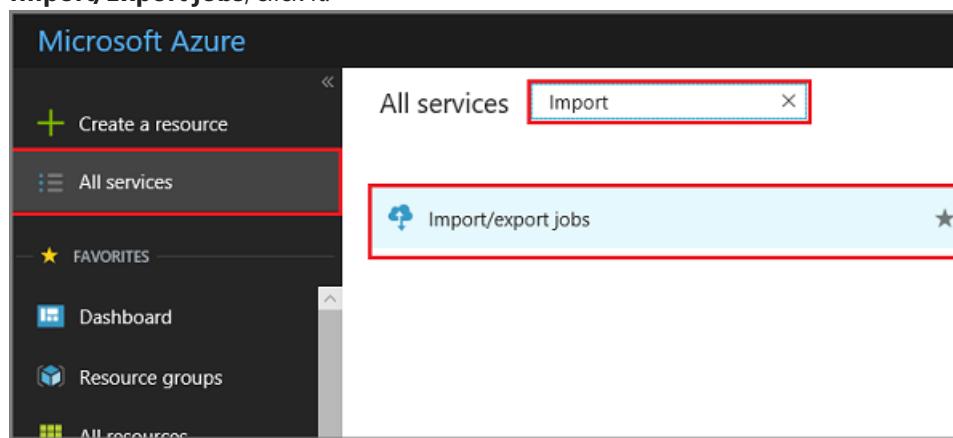
No two Azure Import Jobs can have the same tracking number. Ensure that drives prepared by the utility under a single Azure Import job are shipped together in a single package and that there is a single unique tracking number for the package. Do not combine drives prepared as part of separate Azure Import jobs in a single package.

## Update shipping details on the Azure Import job

The following procedure updates the Azure Import job shipping details. This information includes details about:

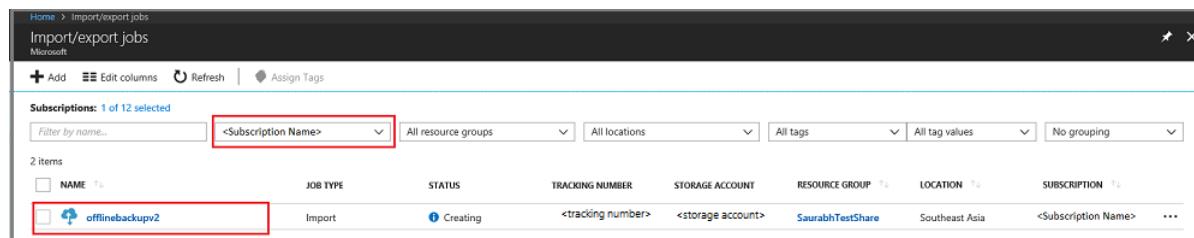
- the name of the carrier who delivers the disks to Azure
- return shipping details for your disks

1. Sign in to your Azure subscription.
2. In the main menu, click **All services** and in the All services dialog, type Import. When you see **Import/Export jobs**, click it.



The list of **Import/export jobs** menu opens, and the list of all Import/export jobs in the selected subscription appears.

3. If you have multiple subscriptions, be sure to select the subscription used to import the backup data. Then select the newly created Import job to open its details.



4. On the Settings menu for the Import job, click **Manage Shipping Info** and enter the return shipping details.

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu includes options like 'Create a resource', 'All services', 'FAVORITES' (Dashboard, Resource groups, All resources, Recent, App Services, Virtual machines (classic), Virtual machines, SQL databases, Cloud services (classic), Subscriptions, Azure Active Directory, Monitor, Security Center, Cost Management + B..., and Help + support). The main content area is titled 'offlinebackupv2 - Manage shipping info' under 'Import/export jobs'. A banner at the top says 'Return carrier' with fields for 'Carrier name' (DHL) and 'Carrier account number' (34134832). Below this is the 'Return address' section with fields for 'Contact name' (Administrator), 'Phone' (2431313312), 'Email' (admin@contoso.com), and 'Street address 1' (Contoso One, Building Zero, Park Street). There are also fields for 'Street address 2 (optional)', 'City' (Hyderabad), 'Zip code' (500072), 'State/Province' (Telangana), and 'Country/Region' (India). A sidebar on the left lists 'SETTINGS' (Manage shipping info, BitLocker keys, Properties, Locks, Automation script), 'MONITORING' (Diagnostics), and 'SUPPORT + TROUBLESHOOTING' (New support request).

5. When you have the tracking number from your shipping carrier, click the banner in the Azure Import job overview page and enter the following details:

#### IMPORTANT

Ensure that the carrier information and tracking number are updated within two weeks of Azure import job creation. Failure to verify this information within two weeks can result in the job being deleted, and drives not being processed.

The screenshot shows the Microsoft Azure portal interface. The navigation menu is identical to the previous screenshot. The main content area is titled 'offlinebackupv2' under 'Import/export job'. At the top, there is a banner with a warning icon: 'For job to progress, provide the tracking information. The job will be deleted if tracking information is not updated within 2 weeks of job creation'. Below this is the 'Essentials' section, which includes fields for 'Resource group' (changed to SaurabhTestShare), 'Status' (Creating), 'Location' (Southeast Asia), 'Subscription name' (changed to <Subscription>), 'Subscription ID' (WADT-5CFB6FA0), and 'Delivery tracking number' (Specified). To the right of these fields are 'Overall percent completed' (~), 'Storage account' (offlinev2teststore), 'Type' (Import), and 'Return tracking number' (~). Below the essentials section is a table titled '1 drive' with columns 'DRIVE ID', 'DRIVE STATE', and 'PERCENT COMPLETE'. The single row shows 'WADT-5CFB6FA0' in the DRIVE ID column, 'Specified' in the DRIVE STATE column, and a blank value in the PERCENT COMPLETE column.

## Time to process the drives

The amount of time it takes to process an Azure import job varies depending on different factors such as shipping time, job type, type and size of the data being copied, and the size of the disks provided. The Azure Import/Export service does not have an SLA but after the disks are received the service strives to complete the backup data copy to your Azure storage account in 7 to 10 days.

## Monitoring Azure Import Job status

You can monitor the status of your Import job from the Azure portal by navigating to the **Import/Export jobs** page and selecting your job. For more information on the status of the Import jobs, see the [Storage Import Export service](#) article.

## Complete the workflow

After the import job successfully completes, initial backup data is available in your storage account. At the time of the next scheduled backup, Azure Backup copies the contents of the data from the storage account to the Recovery Services vault as shown below:

At the time of the next scheduled backup, Azure Backup performs an incremental backup.

## Cleaning up resources

Once the initial backup is complete, you can safely delete the data imported to the Azure Storage Container and the backup data in the Staging Location.

## Next steps

- For any questions on the Azure Import/Export workflow, refer to [Use the Microsoft Azure Import/Export service to transfer data to Blob storage](#).

# Offline-backup workflow for DPM and Azure Backup Server

2/4/2020 • 14 minutes to read • [Edit Online](#)

Azure Backup has several built-in efficiencies that save network and storage costs during the initial full backups of data to Azure. Initial full backups typically transfer large amounts of data and require more network bandwidth when compared to subsequent backups that transfer only the deltas/incrementals. Azure Backup compresses the initial backups. Through the process of offline seeding, Azure Backup can use disks to upload the compressed initial backup data offline to Azure.

The offline-seeding process of Azure Backup is tightly integrated with the [Azure Import/Export service](#) that enables you to transfer data to Azure by using disks. If you have terabytes (TBs) of initial backup data that needs to be transferred over a high-latency and low-bandwidth network, you can use the offline-seeding workflow to ship the initial backup copy on one or more hard drives to an Azure datacenter. This article provides an overview and further details steps that complete this workflow for System Center DPM and Azure Backup Server.

## NOTE

The process of Offline backup for the Microsoft Azure Recovery Services (MARS) agent is distinct from System Center DPM and Azure Backup Server. For information on using Offline backup with MARS agent, see [this article](#). Offline Backup is not supported for System State backups done using the Azure Backup agent.

## Overview

With the offline-seeding capability of Azure Backup and Azure Import/Export, it is simple to upload the data offline to Azure by using disks. The Offline Backup process involves the following steps:

- The backup data, instead of being sent over the network, is written to a *staging location*
- The data on the *staging location* is then written to one or more SATA disks using the *AzureOfflineBackupDiskPrep* utility
- An Azure Import job is automatically created by the utility
- The SATA drives are then sent to the nearest Azure datacenter
- After the upload of the backup data to Azure is finished, Azure Backup copies the backup data to the backup vault and the incremental backups are scheduled.

## Supported configurations

Offline Backup is supported for all deployment models of Azure Backup that offsite backup data from on-premises to the Microsoft Cloud. This includes

- Backup of files and folders with the Microsoft Azure Recovery Services (MARS) Agent or the Azure Backup agent.
- Backup of all workloads and files with System Center Data Protection Manager (SC DPM)
- Backup of all workloads and files with Microsoft Azure Backup Server

## Prerequisites

Ensure that the following prerequisites are met before initiating the Offline Backup workflow

- A [Recovery Services vault](#) has been created. To create one, refer to the steps in [this article](#)
- Azure Backup agent or Azure Backup Server or SC DPM has been installed on either Windows Server/Windows client, as applicable and the computer is registered with the Recovery Services Vault. Ensure that only the [latest version of Azure Backup](#) is used.
- [Download the Azure Publish settings file](#) on the computer from which you plan to back up your data. The subscription from which you download the publish settings file can be different from the subscription that contains the Recovery Services Vault. If your subscription is on sovereign Azure Clouds, then use the following links as appropriate to download the Azure Publish settings file.

| SOVEREIGN CLOUD REGION | AZURE PUBLISH SETTINGS FILE LINK |
|------------------------|----------------------------------|
| United States          | <a href="#">Link</a>             |
| China                  | <a href="#">Link</a>             |

- An Azure Storage account with *Resource Manager* deployment model has been created in the subscription from which you downloaded the publish settings file as shown below:

The screenshot shows the 'Instance details' section of the Azure Storage account creation interface. It includes fields for Storage account name, Location, Performance (Standard selected), Account kind (StorageV2 selected), Replication (Locally-redundant storage selected), and Access tier (Hot selected). A note at the top states: 'The default deployment model is Resource Manager, which supports the latest Azure features. You may choose to deploy using the classic deployment model instead. [Choose classic deployment model](#)'.

- A staging location, which might be a network share or any additional drive on the computer, internal or external, with enough disk space to hold your initial copy, is created. For example, if you are trying to back up a 500-GB file server, ensure that the staging area is at least 500 GB. (A smaller amount is used due to compression.)
- With regards to disks that will be sent to Azure, ensure that only 2.5 inch SSD, or 2.5-inch or 3.5-inch SATA II/III internal hard drives are used. You can use hard drives up to 10 TB. Check the [Azure Import/Export service documentation](#) for the latest set of drives that the service supports.
- The SATA drives have to be connected to a computer (referred to as a *copy computer*) from where the copy of backup data from the *staging location* to the SATA drives is done. Ensure that BitLocker is enabled on the *copy computer*.

## Prepare the Server for the Offline Backup process

### NOTE

If you cannot find the listed utilities such as *AzureOfflineBackupCertGen.exe* in your installation of the MARS agent, write to [AskAzureBackupTeam@microsoft.com](mailto:AskAzureBackupTeam@microsoft.com) to get access to them.

- Open an elevated command prompt on the server and run the following command:

```
AzureOfflineBackupCertGen.exe CreateNewApplication SubscriptionId:<Subscription ID>
```

The tool will create an Azure Offline Backup AD Application if one does not exist.

If an Application already exists, this executable will ask you to manually upload the certificate to the application in the tenant. Follow the steps below in [this section](#) to upload the certificate manually to the application.

- The AzureOfflineBackup.exe tool will generate an OfflineApplicationParams.xml file. Copy this file to the server with MABS or DPM.
- Install the [latest MARS agent](#) on the DPM/Azure Backup (MABS) server.
- Register the server to Azure.
- Run the following command:

```
AzureOfflineBackupCertGen.exe AddRegistryEntries SubscriptionId:<subscriptionid> xmlfilepath:<path of the OfflineApplicationParams.xml file> storageaccountname:<storageaccountname configured with Azure Data Box>
```

- The command above will create the file

```
C:\Program Files\Microsoft Azure Recovery Services Agent\Scratch\MicrosoftBackupProvider\OfflineApplicationParams_<Storageaccountname>.xml
```

## Manually upload Offline Backup Certificate

Follow the steps below to manually upload the Offline Backup certificate to a previously created Azure Active Directory application meant for Offline Backup.

1. Sign in to the Azure portal.
2. Go to **Azure Active Directory > App registrations**
3. Navigate to the **Owned Applications** tab and locate an application with the display name format

AzureOfflineBackup \_<Azure User Id> as shown below:

The screenshot shows the Azure Active Directory - App registrations interface. The left sidebar has 'Manage' selected, with 'App registrations' highlighted. The main area shows the 'Owned applications' tab is selected. A table lists an application with the following details:

| Display name                                      | Application (client) ID        | Created On | Certificates & secrets |
|---------------------------------------------------|--------------------------------|------------|------------------------|
| AzureOfflineBackup_5f6ae501-c125-4242-aac4-fab555 | 13b8e47a-4fee-47a0-9a48-991cf7 | 3/13/2019  | -                      |

4. Click on the application. Under the **Manage** tab on the left pane, go to **Certificates & secrets**.
5. Check for pre-existing certificates or public keys. If there are none, you can safely delete the application by clicking on the **Delete** button on the application's **Overview** page. Following this, you can retry the steps to [Prepare the Server for the Offline Backup](#) process and skip the steps below. Otherwise, execute the following steps from the DPM / Azure Backup Server (MABS) server where you wish to configure Offline Backup.
6. Open the **Manage computer certificate application > Personal** tab and look for the certificate with the

name CB\_AzureADCertforOfflineSeeding\_<ResourceId>

7. Select the certificate above, right-click on **All Tasks** and then **Export**, without private key, in the .cer format.
8. Go to the Azure Offline Backup application in the Azure portal.
9. Click on **Manage > Certificates & secrets > Upload certificate**, and upload the certificate exported in the previous step.

The screenshot shows the 'Certificates & secrets' section of the Azure Offline Backup application. On the left, there's a sidebar with 'Manage' selected, showing options like Branding, Authentication, Certificates & secrets (which is highlighted), Token configuration (preview), API permissions, Expose an API, Owners, Roles and administrators (Preview), Manifest, Support + Troubleshooting, Troubleshooting, and New support request. The main area has a heading 'AzureOfflineBackup\_5f6ae501-c125-4242-aac4-fab5554f6879 - Certificates & secrets'. It contains sections for 'Certificates' (with an 'Upload certificate' button) and 'Client secrets' (with a '+ New client secret' button). A note at the top says: 'Credentials enable applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.'

10. On the server, open the registry by typing **regedit** in the run window.
11. Go to the registry entry *Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows Azure Backup\Config\CloudBackupProvider*.
12. Right-click on **CloudBackupProvider** and add a new string value with the name

AzureADAppCertThumbprint\_<Azure User Id>

#### NOTE

Note: To find the Azure User Id, perform one of the following steps:

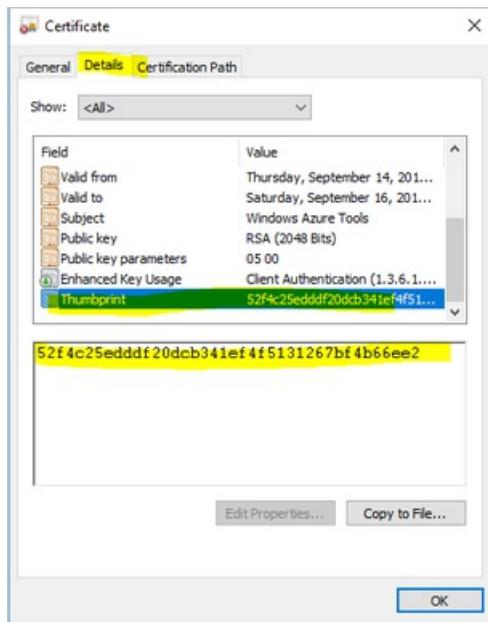
1. From the Azure connected PowerShell run the

```
Get-AzureRmADUser -UserPrincipalName "Account Holder's email as appears in the portal" command.
```

2. Navigate to the registry path:

```
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Azure Backup\DbgSettings\OnlineBackup;
Name: CurrentUserId;
```

13. Right-click on the string added in the previous step and select **Modify**. In the value, provide the thumbprint of the certificate you exported in step 7 and click **OK**.
14. To get the value of the thumbprint, double-click on the certificate, then select the **Details** tab and scroll down until you see the thumbprint field. Click on **Thumbprint** and copy the value.



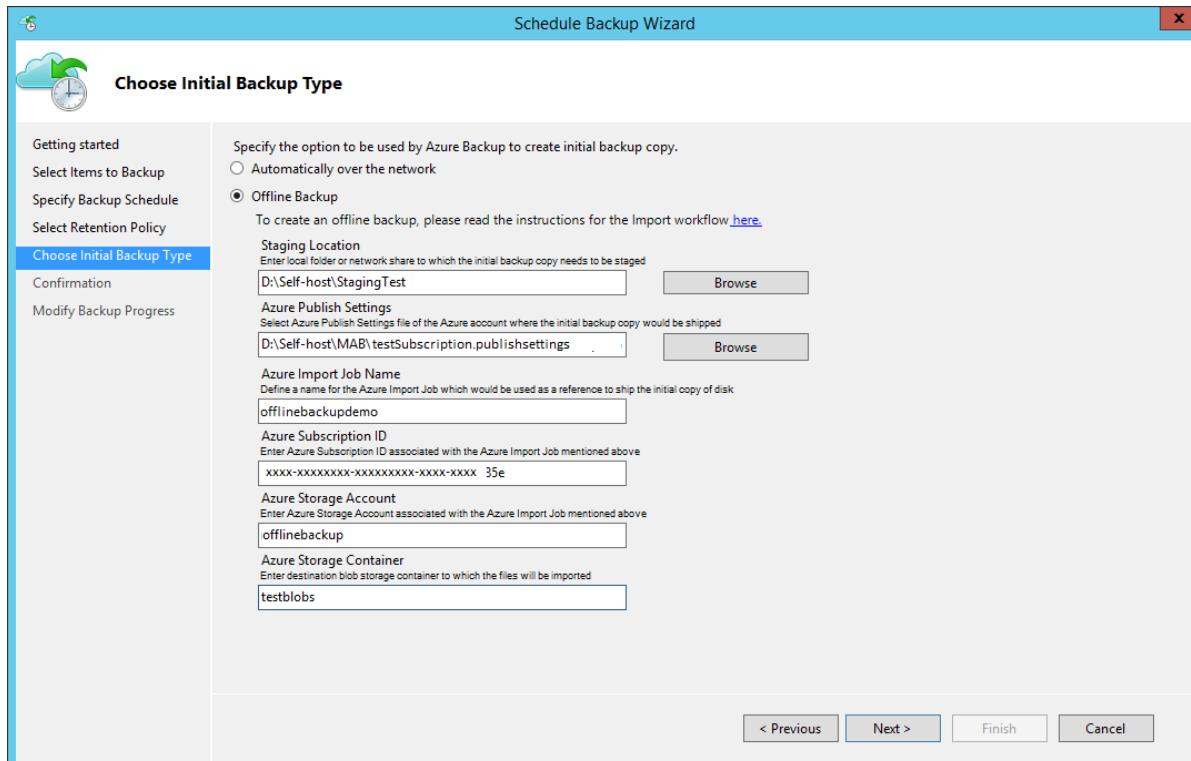
15. Continue to the [Workflow](#) section to proceed with the Offline Backup process.

## Workflow

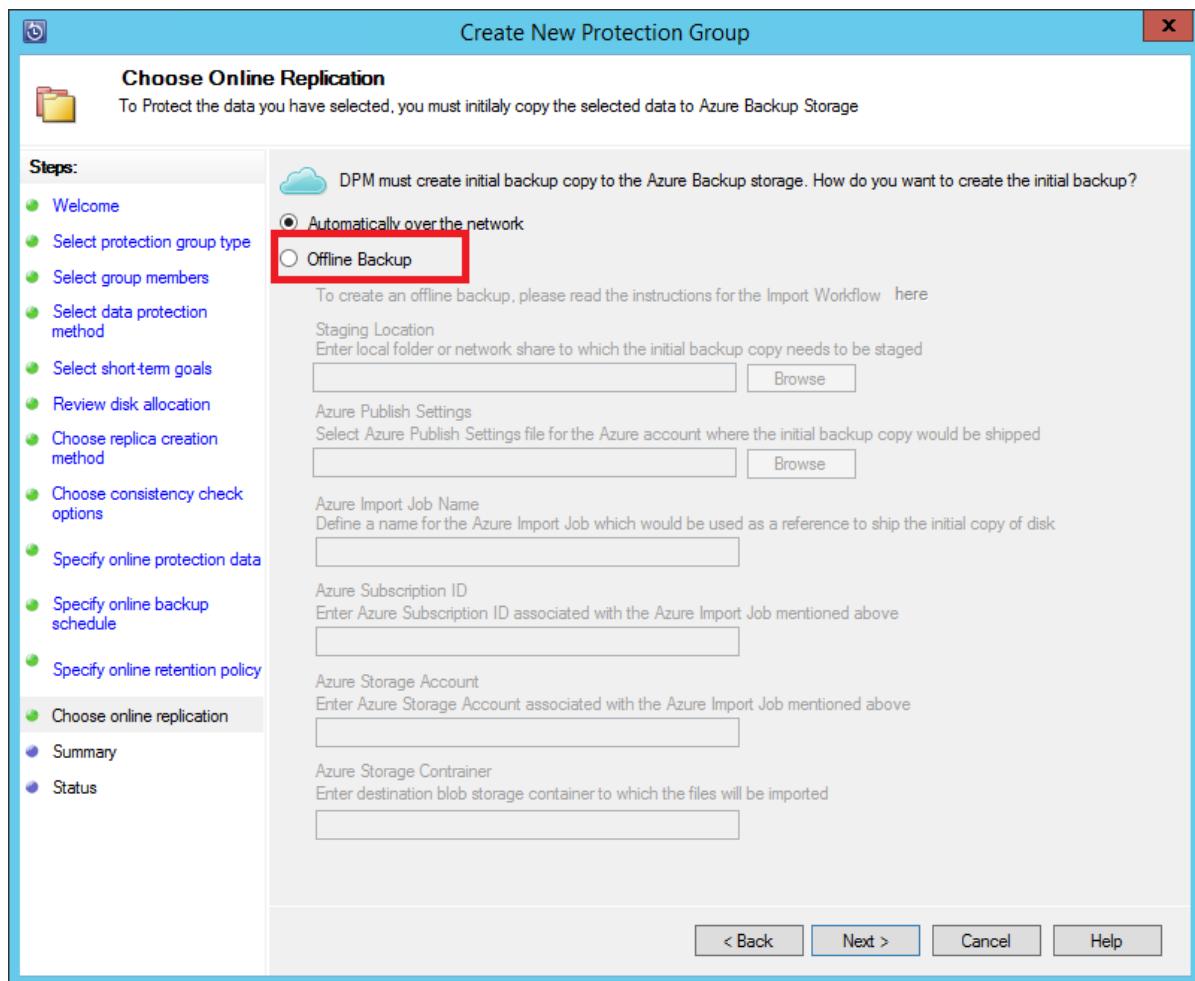
The information in this section helps you complete the offline-backup workflow so that your data can be delivered to an Azure datacenter and uploaded to Azure Storage. If you have questions about the Import service or any aspect of the process, see the [Import service overview](#) documentation referenced earlier.

### Initiate offline backup

1. When you schedule a backup, you see the following screen (in Windows Server, Windows client, or System Center Data Protection Manager).



Here's the corresponding screen in System Center Data Protection Manager:

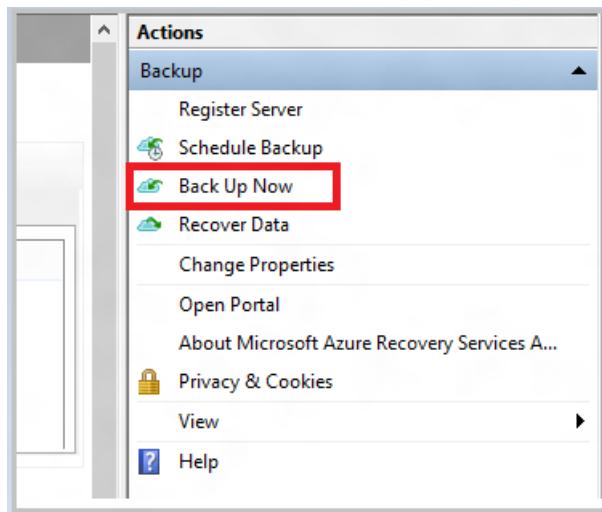


The description of the inputs is as follows:

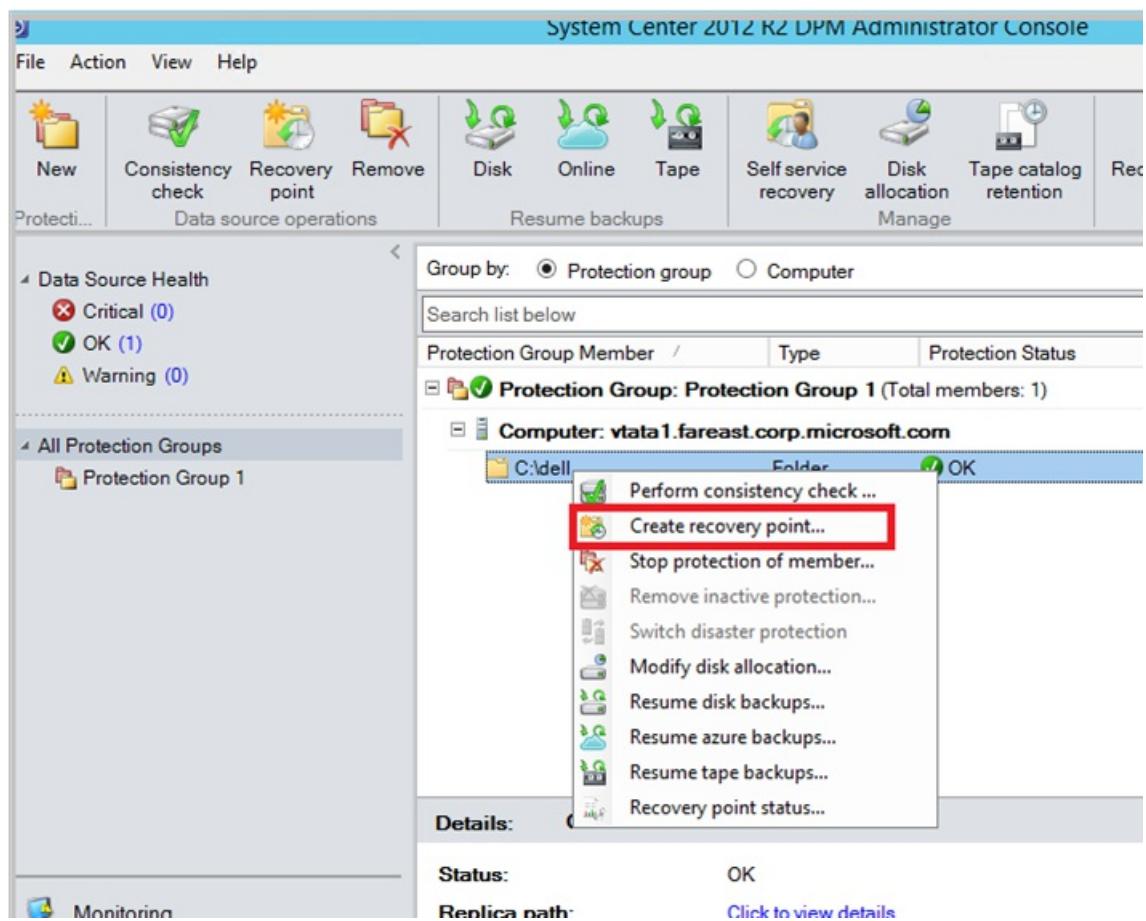
- **Staging Location:** The temporary storage location to which the initial backup copy is written. Staging location might be on a network share or a local computer. If the copy computer and source computer are different, we recommend that you specify the full network path of the staging location.
- **Azure Import Job Name:** The unique name by which Azure Import service and Azure Backup track the transfer of data sent on disks to Azure.
- **Azure Publish Settings:** Provide the local path to the publish settings file.
- **Azure Subscription ID:** The Azure subscription ID for the subscription from where you downloaded the Azure Publish settings file.
- **Azure Storage Account:** The name of the storage account in the Azure subscription associated with the Azure Publish settings file.
- **Azure Storage Container:** The name of the destination storage blob in the Azure storage account where the backup data is imported.

Save the *staging location* and the *Azure Import Job Name* you provided as it is required to prepare the disks.

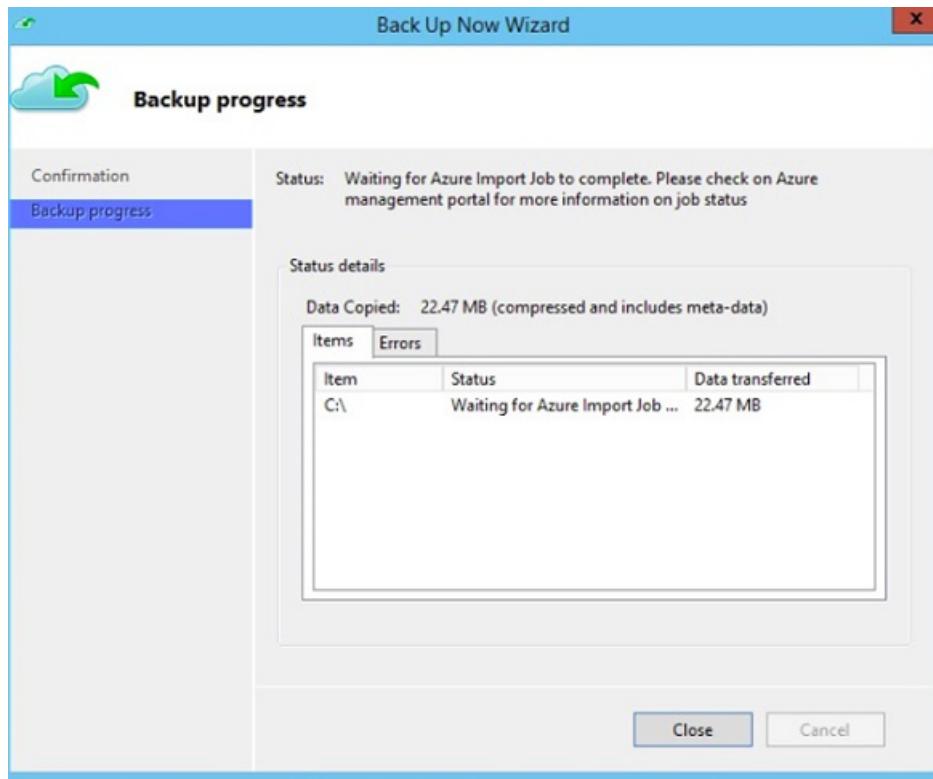
2. Complete the workflow, and to initiate the offline-backup copy, click **Back Up Now** in the Azure Backup agent management console. The initial backup is written to the staging area as part of this step.



To complete the corresponding workflow in System Center Data Protection Manager or Azure Backup server, right-click the **Protection Group**, and then choose the **Create recovery point** option. You then choose the **Online Protection** option.



After the operation finishes, the staging location is ready to be used for disk preparation.



## Prepare SATA drives and ship to Azure

The *AzureOfflineBackupDiskPrep* utility is used to prepare the SATA drives that are sent to the nearest Azure Datacenter. This utility is available in installation directory of the Recovery Services agent in the following path:

```
\\Microsoft Azure Recovery Services Agent\Utils
```

1. Go to the directory, and copy the **AzureOfflineBackupDiskPrep** directory to a copy computer on which the SATA drives to be prepared are connected. Ensure the following with regards to the copy computer:
  - The copy computer can access the staging location for the offline-seeding workflow by using the same network path that was provided in the **Initiate offline backup** workflow.
  - BitLocker is enabled on the copy computer.
  - The copy computer can access the Azure portal.

If necessary, the copy computer can be the same as the source computer.

### IMPORTANT

If the source computer is a virtual machine, then it is mandatory to use a different physical server or client machine as the copy computer.

2. Open an elevated command prompt on the copy computer with the *AzureOfflineBackupDiskPrep* utility directory as the current directory, and run the following command:

```
.\AzureOfflineBackupDiskPrep.exe s:<*Staging Location Path*> [p:<*Path to AzurePublishSettingsFile*>]
```

| PARAMETER                          | DESCRIPTION                                                                                                                              |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| s:< <i>Staging Location Path</i> > | Mandatory input that's used to provide the path to the staging location that you entered in the <b>Initiate offline backup</b> workflow. |

| PARAMETER                       | DESCRIPTION                                                                                                                                               |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| p:<Path to PublishSettingsFile> | Optional input that's used to provide the path to the <b>Azure Publish Settings</b> file that you entered in the <b>Initiate offline backup</b> workflow. |

#### NOTE

The <Path to AzurePublishSettingFile> value is mandatory when the copy computer and source computer are different.

When you run the command, the utility requests the selection of the Azure Import job that corresponds to the drives that need to be prepared. If only a single import job is associated with the provided staging location, you see a screen like the one that follows.

```

Administrator: Command Prompt - AzureOfflineBackupDiskPrep.exe s:D:\Self-host\StagingTest
C:\Program Files\Microsoft Azure Recovery Services Agent\Utils\AzureOfflineBackupDiskPrep>AzureOfflineBackupDiskPrep.exe s:D:\Self-host\StagingTest
Session Started
Current Directory : C:\Program Files\Microsoft Azure Recovery Services Agent\Utils\AzureOfflineBackupDiskPrep
Tool Directory : C:\Program Files\Microsoft Azure Recovery Services Agent\Utils\AzureOfflineBackupDiskPrep\
Journal file name : Journal15510014b-d287-46c1-9cf5-5153083695ba.jrn
Offline seeding param SubscriptionId : XXXX-XXXXXX-XXXXXX-XXXX-XXXXXX e719485e
Offline seeding param StorageAccountName : offlinebackup
Offline seeding param StagingLocation : D:\Self-host\StagingTest\sakgargofflinebackup_offlinebackupdemo
Offline seeding param ImportJobName : offlinebackupdemo
Offline seeding param ContainerName : testblobs

Refreshing blob list:
4254395142362963202_108321_6c802c45-cf4f-4428-a49a-923c6631549f_A1BBlob
4254395142362963202_108321_6c802c45-cf4f-4428-a49a-923c6631549f_BaseBlob

Blob list refreshed. Total Blob count = 2
Please enter the drive letter corresponding to the mounted disk that you wish to prepare.
-
```

- Enter the drive letter without the trailing colon for the mounted disk that you want to prepare for transfer to Azure. Provide confirmation for the formatting of the drive when prompted.

The tool then begins to prepare the disk and copying the backup data. You may need to attach additional disks when prompted by the tool in case the provided disk does not have sufficient space for the backup data.

At the end of successful execution of the tool, one or more disks that you provided are prepared for shipping to Azure. In addition, an import job with the name you provided during the **Initiate offline backup** workflow is created in Azure. Finally, the tool displays the shipping address to the Azure datacenter where the disks need to be shipped.

```

Administrator: Command Prompt

Important message:
The following .xml file has been created to contain information about the
drive. If this is the last copy session (no more data to be appended to
the drive), you can use this .xml file to create the job on Azure portal:
Journal197bd1378-b22a-43e9-acbf-fdaac12c295a_DriveInfo_WMDT-7EF80474.xml
[2016/08/18 14:21:59.736][Info] Command completed.

Process Exit
Blob copy for disk finished. Trying to parse disk details
Parse journal file. Journal file path : C:\Program Files\Microsoft Azure Recovery Services Agent\Utils\AzureOfflineBackupDiskPrep\Journal197bd1378-b22a-43e9-acbf-fdaac12c295a_DriveInfo_
Parsed journal file successfully.
<?xml version="1.0" encoding="utf-8"?><Drive> <DriveId>WMDT-7EF80474</DriveId> <BitLockerKey>i53021-i53021-i53021-i53021-i53021-i53021-i53021</BitLockerKey> <ManifestFile><Drive
Disks prepared for this job:
WMDT-7EF80474
Finished blob copy task successfully.

Trying to create the import job...
Import Job Name : offlinebackupdemo
Supported Drive Destination : (Central India)
Ship the drive(s) to the following location:
Windows Azure Import Export Service
HDS Infra Infra Pvt. Ltd. c/o Tata Communications Ltd., IDC Building, 2nd floor, Alandi Road
Dighi, Pune, Mahar, 411015
India, Phone: +91-7276022257
Supported Carrier: [DHL]
Import job with name 'offlinebackupdemo' is not found.
Done creating the import job.
Go to the following link on classic azure portal and update shipping details:
https://manage.windowsazure.com/#/workspaces/storageextension/StorageAccount/offlinebackupsaure/ImportExport
Note that the link works only in classic Azure Portal. If the portal is deprecated or removed, this link might not work.
Import Job Summary has been dumped at location: [C:\Program Files\Microsoft Azure Recovery Services Agent\Utils\AzureOfflineBackupDiskPrep\sakgargoflinebackup_offlinebackupdemo.txt]
Session Completed Successfully

```

- At the end of the command execution you also see the option to update Shipping information as shown below:

```

Import job with name 'offlinebackuptest1' is not found
Done creating the import job.
Go to the following link on classic azure portal and update shipping details:
https://manage.windowsazure.com/#/workspaces/storageextension/StorageAccount/offlinebackupsaure/ImportExport
In case you cannot locate your newly created import job at the provided link, you can update Shipping details of your import job using this utility. Execute 'AzureOfflineBackupDiskPrep.exe help' for more info
Import Job Summary has been dumped at location: [C:\Program Files\Microsoft Azure Recovery Services Agent\Utils\AzureOfflineBackupDiskPrep\offlinebackupsaure_offlinebackuptest1.txt]

Import Job has been created. Do you want to update the shipping details now ? Enter 'yes' to confirm. Enter any other key to exit.

```

- You can enter the details right away. The tool guides you through the process involving a series of inputs. However if you do not have information like tracking number or other details related to Shipping, you can end the session. The steps to update shipping details later are provided in this article.
- Ship the disks to the address that the tool provided and keep the tracking number for future reference.

#### IMPORTANT

No two Azure Import Jobs can have the same tracking number. Ensure that drives prepared by the utility under a single Azure Import Job are shipped together in a single package and that there is a single unique tracking number for the package. Do not combine drives prepared as part of **different** Azure Import Jobs in a single package.

- When you have the tracking number information, go to the source computer, which is awaiting Import Job completion and run the following command in an elevated command prompt with *AzureOfflineBackupDiskPrep* utility directory as the current directory:

```
.\AzureOfflineBackupDiskPrep.exe u:
```

You can optionally run the following command from a different computer such as the *copy computer*, with *AzureOfflineBackupDiskPrep* utility directory as the current directory:

```
.\AzureOfflineBackupDiskPrep.exe u: s:<*Staging Location Path*> p:<*Path to AzurePublishSettingsFile*>
```

| PARAMETER                          | DESCRIPTION                                                                                                                                                                           |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| u:                                 | Mandatory input used to update shipping details for an Azure Import job                                                                                                               |
| s:< <i>Staging Location Path</i> > | Mandatory input when the command is not run on the source computer. Used to provide the path to the staging location that you entered in the <b>Initiate offline backup</b> workflow. |

| PARAMETER                       | DESCRIPTION                                                                                                                                                                                             |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| p:<Path to PublishSettingsFile> | Mandatory input when the command is not run on the source computer. Used to provide the path to the <b>Azure Publish Settings</b> file that you entered in the <b>Initiate offline backup</b> workflow. |

The utility automatically detects the Import job that the source computer is waiting on or the import jobs associated with the staging location when the command is run on a different computer. It then provides the option to update shipping information through a series of inputs as shown below:

```
C:\Program Files\Microsoft Azure Recovery Services Agent\Utils\AzureOfflineBackupDiskPrep>AzureOfflineBackupDiskPrep.exe s:C:\StagingLocation u:
Parsed input parameters successfully.
Session Started
Current Directory : C:\Program Files\Microsoft Azure Recovery Services Agent\Utils\AzureOfflineBackupDiskPrep
Tool Directory : C:\Program Files\Microsoft Azure Recovery Services Agent\Utils\AzureOfflineBackupDiskPrep\
Journal file name : Journal1aa4702d5-2f3b-4933-a318-33d16d13f016.jrn

Offline seeding param SubscriptionId : <Subscription ID>
Offline seeding param StorageAccountName : offlinebackupsaurse
Offline seeding param StagingLocation : C:\StagingLocation\offlinebackupsaurse_offlinebackuptest1
Offline seeding param ImportJobName : offlinebackuptest1
Offline seeding param ContainerName : offlinebackupnew
Import Job already created.

Trying to update the import job shipping details.
Storage Account Name : offlinebackupsaurse
Import Job Name : offlinebackuptest1

The current import job status is : Creating

Import job has been created. Updating the shipping details for importjob : offlinebackuptest1
Supported Drive Destination : [Australia Southeast]
Ship the drive(s) to the following location:

Microsoft Azure Import/Export Service
Microsoft, c/o NEXTDC Ltd, Delivery code TAU130676, 826-830 Lorimer St, Port
Melbourne, Melbourne, 3207
Australia, Phone: 61 3 9646 5539

Supported Carrier: [DHL]

Enter the delivery package shipping details:
Enter the shipping carrier Name:
FedEx
Enter the tracking number for the package:
23456
Retrieved the number of drives for the import job: 1
```

- Once all the inputs are provided, review the details carefully and commit the shipping info you provided by typing **yes**.

```

***** SHIPPING INFORMATION
***** *****

Delivery package details:
Shipping carrier name :DHL
Shipping tracking number :42346235

Return shipping details:
Shipping carrier name :DHL
Shipping tracking number :124376

Return address details:
Name ::<Contact Name>
Address :Flat 30X, Imagine Residency, Greater Park, Hyderabad, T.S-500084, India
Contact number : <contact number>
Email id : <contact email id>

Review shipping info entered carefully,you will not be able to re-enter shipping info once updated using this utility.
Enter 'yes' to update shipping info. Enter 'cancel' to modify shipping info. Enter anything else to exit.
```

- On updating the Shipping info successfully, the utility provides a local location where the shipping details entered by you are stored as shown below

```
Review shipping info entered carefully,you will not be able to re-enter shipping info once updated using this utility.
Enter 'yes' to update shipping info. Enter 'cancel' to modify shipping info. Enter anything else to exit.
yes
Session job updated
Shipping details summary has been dumped at location: [C:\Program Files\Microsoft Azure Recovery Services Agent\Utils\AzureOfflineBackupDiskPrep\offlinebackupsaurse_offlinebackuptest1_shippinginfo.txt]
Session Completed Successfully
```

### IMPORTANT

Ensure that the drives reach the Azure Datacenter within two weeks of providing the Shipping information using the *AzureOfflineBackupDiskPrep* utility. Failure to do so can result in the drives not being processed.

Once you complete the steps above, the Azure Datacenter is ready to receive the drives and further process them to transfer the backup data from the drives to the classic-type Azure storage account you created.

### Time to process the drives

The amount of time it takes to process an Azure import job varies depending on different factors such as shipping time, job type, type and size of the data being copied, and the size of the disks provided. The Azure Import/Export service does not have an SLA but after the disks are received the service strives to complete the backup data copy to your Azure storage account in 7 to 10 days. The next section details how you can monitor the status of the Azure import job.

### Monitoring Azure Import Job status

While your drives are in transit or at the Azure datacenter to be copied to the storage account, the Azure Backup agent or SC DPM or the Azure Backup server console on the source computer shows the following job status for your scheduled backups.

Waiting for Azure Import Job to complete. Please check on Azure Management portal for more information on job status

Follow the steps below, to check the Import Job status.

1. Open an elevated command prompt on the source computer and run the following command:

```
AzureOfflineBackupDiskPrep.exe u:
```

2. The output shows the current status of the Import Job as shown below:

```
C:\Program Files\Microsoft Azure Recovery Services Agent\Utils\AzureOfflineBackupDiskPrep>AzureOfflineBackupDiskPrep.exe u:
Parsed input parameters successfully.
Session Started
Current Directory : C:\Program Files\Microsoft Azure Recovery Services Agent\Utils\AzureOfflineBackupDiskPrep
Tool Directory : C:\Program Files\Microsoft Azure Recovery Services Agent\Utils\AzureOfflineBackupDiskPrep\
Journal file name : Journaleb64edc0-b141-46d5-90cd-31a68e3b39f7.jrn

Offline seeding param SubscriptionId : <subscriptionid>
Offline seeding param StorageAccountName : offlinebackupsaurse
Offline seeding param ImportJobName : offlinebackuptest1
Offline seeding param ContainerName : offlinebackupnew

Trying to update the import job shipping details.
Storage Account Name : offlinebackupsaurse
Import Job Name : offlinebackuptest1

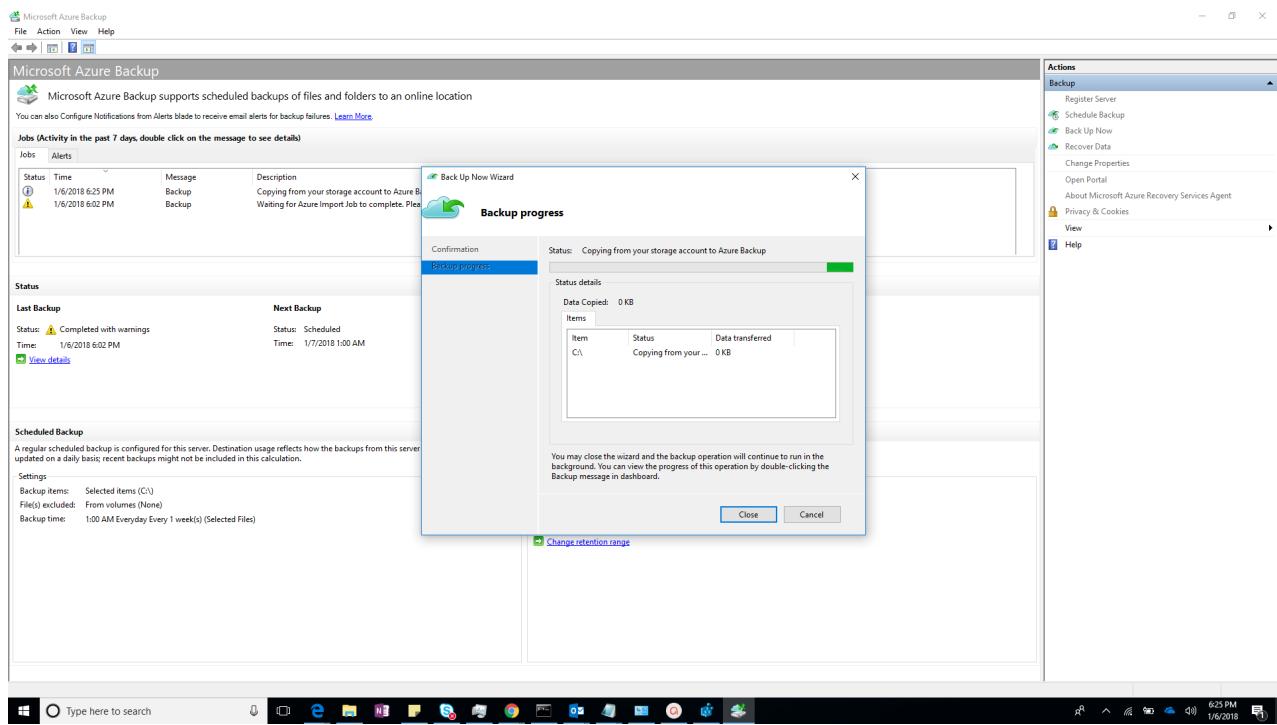
The current import job status is : Shipping

Import job shipping details have been updated for the importjob : offlinebackuptest1
Session Completed Successfully
```

For more information on the various states of the Azure import job, see [this article](#)

### Complete the workflow

After the import job finishes, initial backup data is available in your storage account. At the time of the next scheduled backup, Azure backup copies the contents of the data from the storage account to the Recovery Services vault as shown below:



At the time of the next scheduled backup, Azure Backup performs incremental backup over the initial backup copy.

## Next steps

- For any questions on the Azure Import/Export workflow, refer to [Use the Microsoft Azure Import/Export service to transfer data to Blob storage](#).

# Monitor your backups with Backup Explorer

2/11/2020 • 4 minutes to read • [Edit Online](#)

As organizations back up more and more machines to the cloud, it becomes increasingly important to monitor these backups efficiently. The best way to begin is to use a central location for viewing operational information across a large estate.

Backup Explorer is a built-in Azure Monitor workbook that gives Azure Backup customers this single, central location. Backup Explorer helps you monitor operational activities across the entire Backup estate on Azure, spanning tenants, locations, subscriptions, resource groups, and vaults. Broadly, Backup Explorer provides the following capabilities:

- **At-scale perspective:** Get an aggregated view of the backup items, jobs, alerts, policies, and resources that aren't yet configured for backup across the entire estate.
- **Drill-down analysis:** Display detailed information about each of your jobs, alerts, policies, and backup items, all in one place.
- **Actionable interfaces:** After you identify an issue, you can resolve it by going seamlessly to the relevant backup item or Azure resource.

These capabilities are provided out-of-box by native integration with Azure Resource Graph and Azure Monitor workbooks.

## NOTE

- Backup Explorer is currently available only for Azure virtual machines (VMs) data.
- Backup Explorer is meant to be an operational dashboard for viewing information about your backups over the last 7 days (maximum).
- Currently, customizing the Backup Explorer template is not supported.
- We do not recommend writing custom automations on Azure Resource Graph data.

## Get started

You can access Backup Explorer by going to any of your Recovery Services vaults and selecting the **Backup Explorer** link in the **Overview** pane.

**contoso-vault**  
Recovery Services vault

Search (Ctrl+ /)

+ Backup + Replicate Delete Refresh

Protect on-premises VMs by directly replicating to managed disks in Azure →  
Protection of Azure VMs using Storage Spaces Direct is now available →  
Disaster recovery for VMs deployed in Availability Zones to another region →

**Overview**

**Activity log**

**Access control (IAM)**

**Tags**

**Diagnose and solve problems**

**Settings**

Properties

Locks

Export template

**Getting started**

Backup

Site Recovery

**Protected items**

**Backup**

Getting started

Backup dashboard

Backup items

Backup policies

Backup Reports

**Backup Explorer**

Learn more ↗

**Site Recovery**

Getting started

Site Recovery dashboard

Replicated items

Manage Recovery Plans

Learn more ↗

Selecting the link opens Backup Explorer, which provides an aggregated view across all the vaults and subscriptions that you have access to. If you're using an Azure Lighthouse account, you can view data across all the tenants that you have access to. For more information, see the "Cross-tenant views" section at the end of this article.

Summary Backup Items Jobs Alerts Policies Backup Not Enabled

Backup Explorer (Virtual Machines) - Summary How to use backup explorer?

Subscriptions (All) Vault Location (All) Vault (All) Time Range (Last 24 hours)

Click on any of the tiles to see more details

|                                     |                                    |                                     |                                                      |
|-------------------------------------|------------------------------------|-------------------------------------|------------------------------------------------------|
| Backup Items<br>Total<br><b>359</b> | Backup Jobs<br>Total<br><b>423</b> | Backup Alerts<br>Total<br><b>26</b> | Backup Not Enabled<br>Virtual Machines<br><b>413</b> |
|-------------------------------------|------------------------------------|-------------------------------------|------------------------------------------------------|

## Backup Explorer use cases

Backup Explorer displays multiple tabs, each providing detailed information about a specific backup artifact (for example, a backup item, job, or policy). This section provides a brief overview of each of the tabs. The videos provide sample use cases for each backup artifact, along with descriptions of the available controls.

### The Summary tab

The **Summary** tab provides a quick glance at the overall condition of your backup estate. For example, you can view the number of items being protected, the number of items for which protection hasn't been enabled, or how many jobs were successful in the last 24 hours.

### The Backup Items tab

You can filter and view each of your backup items by subscription, vault, and other characteristics. By selecting the name of a backup item, you can open the Azure pane for that item. For example, from the table, you might observe that the last backup failed for item X. By selecting X, you can open the item's **Backup** pane, where you can trigger an on-demand backup operation.

## The Jobs tab

Select the **Jobs** tab to view the details of all the jobs that were triggered over the last 7 days. Here, you can filter by *Job Operation*, *Job Status*, and *Error Code* (for failed jobs).

## The Alerts tab

Select the **Alerts** tab to view details of all alerts that were generated on your vaults over the last 7 days. You can filter alerts by type (*Backup Failure* or *Restore Failure*), current status (*Active* or *Resolved*), and severity (*Critical*, *Warning*, or *Information*). You can also select a link to go the Azure VM and take any necessary action.

## The Policies tab

You can select the **Policies** tab to view key information about all the backup policies that have been created across your backup estate. You can view the number of items associated with each policy, along with the retention range and backup frequency specified by the policy.

## The Backup Not Enabled tab

Backup should be enabled for all machines that require protection. With Backup Explorer, backup administrators can quickly identify which machines in an organization are not yet protected by backup. To view this information, select the **Backup Not Enabled** tab.

The **Backup Not Enabled** pane displays a table with a list of unprotected machines. Your organization might assign different tags to production machines and test machines, or to machines that serve a variety of functions. Because each class of machines needs a separate backup policy, filtering by tags helps you view information that's specific to each. Selecting the name of any machine redirects you to that machine's **Configure Backup** pane, where you can choose to apply an appropriate backup policy.

## Export to Excel

You can export the contents of any table or chart as an Excel spreadsheet. The contents are exported as is, with your existing filters applied. To export additional table rows, you can increase the number of rows to be displayed on the page by using the **Rows Per Page** drop-down list at the top of each tab.

## Pin to the dashboard

You can select the "pin" icon at the top of each table or chart to pin it to your Azure portal dashboard. Pinning this information helps you create a customized dashboard that's tailored to display the information that's most important to you.

## Cross-tenant views

If you're an Azure Lighthouse user with delegated access to subscriptions across multiple tenant environments, you can use the default subscription filter. You display the subscriptions that you want to see data for by selecting the

"filter" icon at the top right of the Azure portal. When you use this feature, Backup Explorer aggregates information about all the vaults across your selected subscriptions. To learn more, see [What is Azure Lighthouse?](#).

## Next steps

[Learn how to use Azure Monitor for getting insights on your backup data](#)

# Monitoring Azure Backup workloads

11/18/2019 • 3 minutes to read • [Edit Online](#)

Azure Backup provides multiple backup solutions based on the backup requirement and infrastructure topology (On-premises vs Azure). Any backup user or admin should see what is going on across all solutions and expected to be notified in important scenarios. This article details the monitoring and notification capabilities provided by Azure Backup service.

## Backup Jobs in Recovery Services vault

Azure Backup provides in-built monitoring and alerting capabilities for workloads being protected by Azure Backup. In the Recovery Services vault settings, the **Monitoring** section provides in-built jobs and alerts.



Jobs are generated when operations such as configuring backup, backup, restore, delete backup, and so on, are performed.

Jobs from the following Azure Backup solutions are shown here:

- Azure VM backup
- Azure File backup
- Azure workload backup such as SQL
- Azure Backup agent (MAB)

Jobs from System Center Data Protection Manager (SC-DPM), Microsoft Azure Backup Server (MABS) are NOT displayed.

#### **NOTE**

Azure workloads such as SQL backups within Azure VMs have huge number of backup jobs. For example, log backups can run for every 15 minutes. Hence, for such DB workloads, only user triggered operations are displayed. Scheduled backup operations are NOT displayed.

## Backup Alerts in Recovery Services vault

Alerts are primarily scenarios where users are notified so that they can take relevant action. The **Backup Alerts** section shows alerts generated by Azure Backup service. These alerts are defined by the service and user cannot custom create any alerts.

### **Alert scenarios**

The following scenarios are defined by service as alertable scenarios.

- Backup/Restore failures
- Backup succeeded with warnings for Azure Backup Agent (MAB)
- Stop protection with retain data/Stop protection with delete data

### **Exceptions when an alert is not raised**

There are few exceptions when an alert is not raised on a failure, they are:

- User explicitly canceled the running job
- The job fails because another backup job is in progress (nothing to act on here since we just have to wait for the previous job to finish)
- The VM backup job fails because the backed-up Azure VM no longer exists

The above exceptions are designed from the understanding that the result of these operations (primarily user triggered) shows up immediately on portal/PS/CLI clients. Hence, the user is immediately aware and doesn't need a notification.

### **Alerts from the following Azure Backup solutions are shown here**

- Azure VM backups
- Azure File backups
- Azure workload backups such as SQL
- Azure Backup agent (MAB)

#### **NOTE**

Alerts from System Center Data Protection Manager (SC-DPM), Microsoft Azure Backup Server (MABS) are NOT displayed here.

### **Alert types**

Based on alert severity, alerts can be defined in three types:

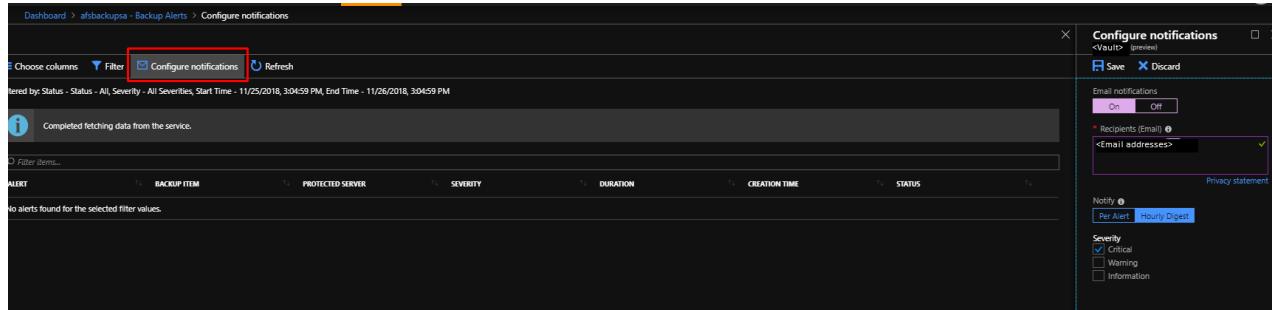
- **Critical:** In principle, any backup or recovery failure (scheduled or user triggered) would lead to generation of an alert and would be shown as a Critical alert and also destructive operations such as delete backup.
- **Warning:** If the backup operation succeeds but with few warnings, they are listed as Warning alerts.
- **Informational:** As of today, no informational alert is generated by Azure Backup service.

## Notification for Backup Alerts

## NOTE

Configuration of notification can be done only through Azure Portal. PS/CLI/REST API/Azure Resource Manager Template support is not supported.

Once an alert is raised, users are notified. Azure Backup provides an inbuilt notification mechanism via e-mail. One can specify individual email addresses or distribution lists to be notified when an alert is generated. You can also choose whether to get notified for each individual alert or to group them in an hourly digest and then get notified.



The screenshot shows the 'Configure notifications' dialog box in the Azure Backup Alerts section. The 'Email notifications' switch is set to 'On'. Below it, there's a field for 'Recipients (Email)' with a placeholder '<Email addresses>'. At the bottom, there are 'Notify' options: 'Per Alert' (selected) and 'Hourly Digest'. Under 'Severity', 'Critical' is checked, while 'Warning' and 'Information' are unchecked. The main pane shows a table with columns: ALERT, BACKUP ITEM, PROTECTED SERVER, SEVERITY, DURATION, CREATION TIME, and STATUS. A filter bar at the top indicates 'Status - All, Severity - All Severities, Start Time - 11/25/2018, 3:04:59 PM, End Time - 11/26/2018, 3:04:59 PM'. A message says 'Completed fetching data from the service.'

## NOTE

The alerts for SQL backups will be consolidated and the email is sent only for the first occurrence. But if the alert is inactivated by the user, the next occurrence will trigger another email.

When notification is configured, you will receive a welcome or introductory email. This confirms that Azure Backup can send emails to these addresses when an alert is raised.

If the frequency was set to an hourly digest and an alert was raised and resolved within an hour, it will not be a part of the upcoming hourly digest.

## NOTE

- If a destructive operation such as **stop protection with delete data** is performed, an alert is raised and an email is sent to subscription owners, admins, and co-admins even if notifications are NOT configured for the Recover Service vault.
- To configure notification for successful jobs use [Log Analytics](#).

## Inactivating alerts

To inactivate/resolve an active alert, you can click on the list item corresponding to the alert you wish to inactivate. This opens up a screen that displays detailed information about the alert, with an 'Inactivate' button on the top. Clicking this button would change the status of the alert to 'Inactive'. You may also inactivate an alert by right-clicking on the list item corresponding to that alert and selecting 'Inactivate'.

Home > [Redacted] > Details

Inactivate

|                        |                                                                                                                |
|------------------------|----------------------------------------------------------------------------------------------------------------|
| Alert                  | Backup failure                                                                                                 |
| Status                 | Active                                                                                                         |
| Alert type             | Backup                                                                                                         |
| Severity               | Critical                                                                                                       |
| Backup item            | fs1                                                                                                            |
| Backup item type       | [Redacted]                                                                                                     |
| Protected server       | [Redacted]                                                                                                     |
| Creation time          | 5/28/2019, 1:30:53 PM                                                                                          |
| Latest occurrence time | 5/28/2019, 1:30:53 PM                                                                                          |
| Occurrence count       | 1                                                                                                              |
| Description            | Operation failed as the specified storage account does not exist anymore.                                      |
| Recommended action     | Retry the operation after some time. If the problem persists, please contact Microsoft support for assistance. |
| Alert raised on        | BackupItem                                                                                                     |

## Next steps

[Monitor Azure backup workloads using Azure Monitor](#)

# Monitor at scale by using Azure Monitor

2/24/2020 • 6 minutes to read • [Edit Online](#)

Azure Backup provides [built-in monitoring and alerting capabilities](#) in a Recovery Services vault. These capabilities are available without any additional management infrastructure. But this built-in service is limited in the following scenarios:

- If you monitor data from multiple Recovery Services vaults across subscriptions
- If the preferred notification channel is *not* email
- If users want alerts for more scenarios
- If you want to view information from an on-premises component such as System Center Data Protection Manager in Azure, which the portal doesn't show in [Backup Jobs](#) or [Backup Alerts](#)

## Using Log Analytics workspace

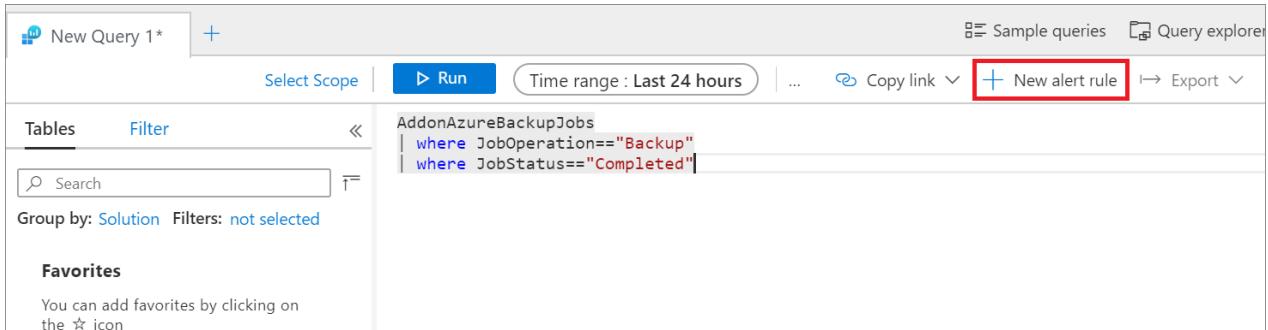
### Create alerts by using Log Analytics

In Azure Monitor, you can create your own alerts in a Log Analytics workspace. In the workspace, you use *Azure action groups* to select your preferred notification mechanism.

#### IMPORTANT

For information on the cost of creating this query, see [Azure Monitor pricing](#).

Open the **Logs** section of the Log Analytics workspace and write a query your own Logs. When you select **New Alert Rule**, the Azure Monitor alert-creation page opens, as shown in the following image.



The screenshot shows the Azure Log Analytics workspace interface. At the top, there's a header with 'New Query 1\*' and a '+' button. Below it are buttons for 'Select Scope', 'Run', 'Time range: Last 24 hours', 'Copy link', and a red-bordered 'New alert rule' button. The main area contains a query editor with the following code:

```
AddonAzureBackupJobs
| where JobOperation=="Backup"
| where JobStatus=="Completed"
```

On the left, there are sections for 'Tables' (selected), 'Filter', 'Search', 'Group by: Solution', 'Filters: not selected', and 'Favorites'. A note at the bottom says 'You can add favorites by clicking on the star icon'.

Here the resource is already marked as the Log Analytics workspace, and action group integration is provided.

## Create rule

Rules management

|  <p><b>* RESOURCE</b></p> <p>&lt;LA workspace name&gt;</p> <p><b>Select</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <p><b>HIERARCHY</b></p> <p>&lt;Subscription Name&gt; &gt; &lt;LA workspace name&gt;</p> |                   |                   |                          |  |                        |                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|-------------------|-------------------|--------------------------|--|------------------------|-------------------|
| <p><b>* CONDITION</b></p> <p>Whenever the Custom log search is &lt;logic undefined&gt;</p> <p>Monthly cost in USD (Estimated) ⓘ</p> <p>\$ &lt;Est. price&gt;</p> <p>Total \$ &lt;Total price&gt;</p> <p>Add condition</p> <p><b>i</b> We currently support configuring only two metrics signals or one log search signal or one activity log signal per alert rule. An alert will be triggered when the conditions for all the above configured criteria are met</p>                                                                                                                                                                     |                                                                                         |                   |                   |                          |  |                        |                   |
| <p><b>* ACTION GROUPS</b></p> <p>Notify your team via email and text messages or automate actions using webhooks, runbooks, functions, logic apps or integrating with external ITSM solutions. Learn more here</p> <table border="1"> <thead> <tr> <th>ACTION GROUP NAME</th> <th>ACTION GROUP TYPE</th> </tr> </thead> <tbody> <tr> <td>No action group selected</td> <td></td> </tr> <tr> <td><b>Select existing</b></td> <td><b>Create New</b></td> </tr> </tbody> </table> <p><b>Customize Actions</b></p> <p><input type="checkbox"/> Email subject ⓘ</p> <p><input type="checkbox"/> Include custom Json payload for webhook ⓘ</p> |                                                                                         | ACTION GROUP NAME | ACTION GROUP TYPE | No action group selected |  | <b>Select existing</b> | <b>Create New</b> |
| ACTION GROUP NAME                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | ACTION GROUP TYPE                                                                       |                   |                   |                          |  |                        |                   |
| No action group selected                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                         |                   |                   |                          |  |                        |                   |
| <b>Select existing</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <b>Create New</b>                                                                       |                   |                   |                          |  |                        |                   |
| <p><b>ALERT DETAILS</b></p> <p><b>* Alert rule name</b> ⓘ</p> <p>Specify alert rule name. Sample: 'Percentage CPU greater than 70'</p> <p><b>* Description</b></p> <p>Specify alert description here...</p>                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                         |                   |                   |                          |  |                        |                   |

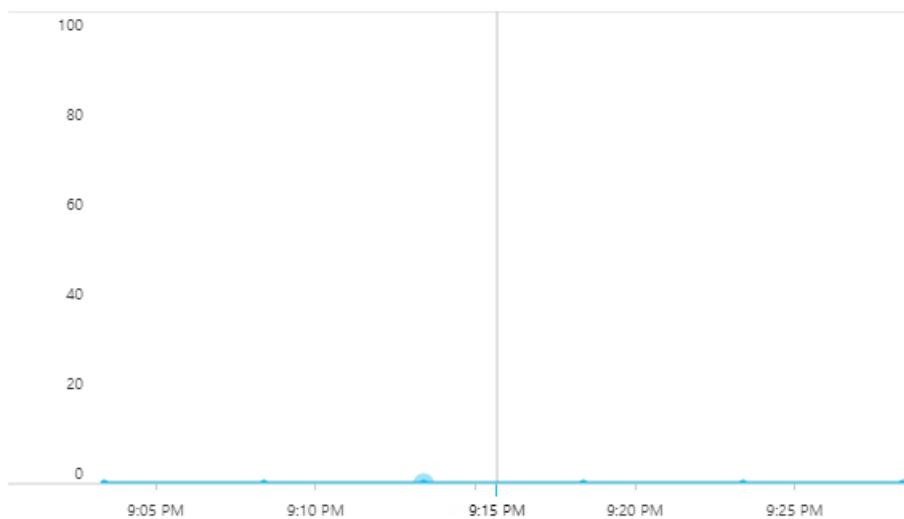
### Alert condition

The defining characteristic of an alert is its triggering condition. Select **Condition** to automatically load the Kusto query on the **Logs** page as shown in the following image. Here you can edit the condition to suit your needs. For more information, see [Sample Kusto queries](#).

## Configure signal logic

[-> Back to signal selection](#)

### Custom log search



#### \* Search query [?](#)

```
AzureDiagnostics
| where Category == "AzureBackupReport"
| where OperationName == "Job" and JobOperation_s == "Backup"
```

[View result of query in Azure Monitor - Logs](#)

Query to be executed : AzureDiagnostics | where Category == "AzureBackupReport" | where OperationName == "Job" and JobOperation\_s == "Backup" | where JobStatus\_s == "Failed" | count  
For time window : 2/19/2019, 9:23:23 PM - 2/19/2019, 9:28:23 PM

### Alert logic

|                            |                             |                               |
|----------------------------|-----------------------------|-------------------------------|
| Based on <a href="#">?</a> | Condition <a href="#">?</a> | * Threshold <a href="#">?</a> |
| Number of results          | Greater than                | <input type="text"/>          |

### Condition preview

Whenever the custom log search is greater than <undefined> count

### Evaluated based on

|                                         |                                            |
|-----------------------------------------|--------------------------------------------|
| * Period (in minutes) <a href="#">?</a> | * Frequency (in minutes) <a href="#">?</a> |
| <input type="text" value="5"/>          | <input type="text" value="5"/>             |

**Done**

If necessary, you can edit the Kusto query. Choose a threshold, period, and frequency. The threshold determines when the alert will be raised. The period is the window of time in which the query is run. For example, if the threshold is greater than 0, the period is 5 minutes, and the frequency is 5 minutes, then the rule runs the query every 5 minutes, reviewing the previous 5 minutes. If the number of results is greater than 0, you're notified through the selected action group.

### Alert action groups

Use an action group to specify a notification channel. To see the available notification mechanisms, under **Action groups**, select **Create New**.

Add action group

\* Action group name

\* Short name

\* Subscription  <Subscription Name>

\* Resource group  Default-ActivityLogAlerts (to be created)

**Actions**

| ACTION NAME                                     | ACTION TYPE                                                                                                                                                                                                                                                            | STATUS | DETAILS | ACTIONS |
|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---------|---------|
| <input type="text"/> Unique name for the act... | <input type="button" value="Email/SMS/Push/Voice"/> <input type="button" value="Azure Function"/> <input type="button" value="LogicApp"/> <input type="button" value="Webhook"/> <input type="button" value="ITSM"/> <input type="button" value="Automation Runbook"/> |        |         |         |
| Privacy Statement                               | Email/SMS/Push/Voice                                                                                                                                                                                                                                                   |        |         |         |
| Pricing                                         | Azure Function                                                                                                                                                                                                                                                         |        |         |         |
|                                                 | LogicApp                                                                                                                                                                                                                                                               |        |         |         |
|                                                 | Webhook                                                                                                                                                                                                                                                                |        |         |         |
|                                                 | ITSM                                                                                                                                                                                                                                                                   |        |         |         |
|                                                 | Automation Runbook                                                                                                                                                                                                                                                     |        |         |         |

**OK**

You can satisfy all alerting and monitoring requirements from Log Analytics alone, or you can use Log Analytics to supplement built-in notifications.

For more information, see [Create, view, and manage log alerts by using Azure Monitor](#) and [Create and manage action groups in the Azure portal](#).

### Sample Kusto queries

The default graphs give you Kusto queries for basic scenarios on which you can build alerts. You can also modify the queries to get the data you want to be alerted on. Paste the following sample Kusto queries in the **Logs** page and then create alerts on the queries:

- All successful backup jobs

```
AddonAzureBackupJobs
| where JobOperation=="Backup"
| where JobStatus=="Completed"
```

- All failed backup jobs

```
AddonAzureBackupJobs
| where JobOperation=="Backup"
| where JobStatus=="Failed"
```

- All successful Azure VM backup jobs

```

AddonAzureBackupJobs
| where JobOperation=="Backup"
| where JobStatus=="Completed"
| join kind=inner
(
 CoreAzureBackup
 | where OperationName == "BackupItem"
 | where BackupItemType=="VM" and BackupManagementType=="IaaSVM"
 | distinct BackupItemUniqueId, BackupItemFriendlyName
)
on BackupItemUniqueId

```

- All successful SQL log backup jobs

```

AddonAzureBackupJobs
| where JobOperation=="Backup" and JobOperationSubType=="Log"
| where JobStatus=="Completed"
| join kind=inner
(
 CoreAzureBackup
 | where OperationName == "BackupItem"
 | where BackupItemType=="SQLDataBase" and BackupManagementType=="AzureWorkload"
 | distinct BackupItemUniqueId, BackupItemFriendlyName
)
on BackupItemUniqueId

```

- All successful Azure Backup agent jobs

```

AddonAzureBackupJobs
| where JobOperation=="Backup"
| where JobStatus=="Completed"
| join kind=inner
(
 CoreAzureBackup
 | where OperationName == "BackupItem"
 | where BackupItemType=="FileFolder" and BackupManagementType=="MAB"
 | distinct BackupItemUniqueId, BackupItemFriendlyName
)
on BackupItemUniqueId

```

- Backup Storage Consumed per Backup Item

```

CoreAzureBackup
//Get all Backup Items
| where OperationName == "BackupItem"
//Get distinct Backup Items
| distinct BackupItemUniqueId, BackupItemFriendlyName
| join kind=leftouter
(AddonAzureBackupStorage
| where OperationName == "StorageAssociation"
//Get latest record for each Backup Item
| summarize arg_max(TimeGenerated, *) by BackupItemUniqueId
| project BackupItemUniqueId , StorageConsumedInMBs)
on BackupItemUniqueId
| project BackupItemUniqueId , BackupItemFriendlyName , StorageConsumedInMBs
| sort by StorageConsumedInMBs desc

```

## Diagnostic data update frequency

The diagnostic data from the vault is pumped to the Log Analytics workspace with some lag. Every event arrives at the Log Analytics workspace *20 to 30 minutes* after it's pushed from the Recovery Services vault. Here are

further details about the lag:

- Across all solutions, the backup service's built-in alerts are pushed as soon as they're created. So they usually appear in the Log Analytics workspace after 20 to 30 minutes.
- Across all solutions, on-demand backup jobs and restore jobs are pushed as soon as they *finish*.
- For all solutions except SQL backup, scheduled backup jobs are pushed as soon as they *finish*.
- For SQL backup, because log backups can occur every 15 minutes, information for all the completed scheduled backup jobs, including logs, is batched and pushed every 6 hours.
- Across all solutions, other information such as the backup item, policy, recovery points, storage, and so on, is pushed at least *once per day*.
- A change in the backup configuration (such as changing policy or editing policy) triggers a push of all related backup information.

## Using the Recovery Services vault's activity logs

### Caution

The following steps apply only to *Azure VM backups*. You can't use these steps for solutions such as the Azure Backup agent, SQL backups within Azure, or Azure Files.

You can also use activity logs to get notification for events such as backup success. To begin, follow these steps:

1. Sign in into the Azure portal.
2. Open the relevant Recovery Services vault.
3. In the vault's properties, open the **Activity log** section.

To identify the appropriate log and create an alert:

1. Verify that you're receiving activity logs for successful backups by applying the filters shown in the following image. Change the **Timespan** value as necessary to view records.

| OPERATION NAME        | STATUS    | TIME     | TIME STAMP      | SUBSCRIPTION        | EVENT INITIATED BY         |
|-----------------------|-----------|----------|-----------------|---------------------|----------------------------|
| Backup Protected Item | Failed    | 16 h ago | Sun Feb 24 ...  | <Subscription Name> | Microsoft.RecoveryServices |
| Backup Protected Item | Succeeded | 16 h ago | Sun Feb 24 2... | <Subscription Name> | Microsoft.RecoveryServices |

2. Select the operation name to see the relevant details.
3. Select **New alert rule** to open the **Create rule** page.
4. Create an alert by following the steps in [Create, view, and manage activity log alerts by using Azure Monitor](#).

## Refresh container

Tue May 21 2019 16:15:25 GMT+0530 (India Standard Time)

[+ New alert rule](#)

[Summary](#) [JSON](#) [Change history \(Preview\)](#)

Operation name Refresh container

Time stamp Tue May 21 2019 16:15:25 GMT+0530 (India Standard Time)

Event initiated by

Here the resource is the Recovery Services vault itself. Repeat the same steps for all of the vaults in which you want to be notified through activity logs. The condition won't have a threshold, period, or frequency because this alert is based on events. As soon as the relevant activity log is generated, the alert is raised.

## Using Log Analytics to monitor at scale

You can view all alerts created from activity logs and Log Analytics workspaces in Azure Monitor. Just open the **Alerts** pane on the left.

Although you can get notifications through activity logs, we highly recommend using Log Analytics rather than activity logs for monitoring at scale. Here's why:

- **Limited scenarios:** Notifications through activity logs apply only to Azure VM backups. The notifications must be set up for every Recovery Services vault.
- **Definition fit:** The scheduled backup activity doesn't fit with the latest definition of activity logs. Instead, it aligns with [resource logs](#). This alignment causes unexpected effects when the data that flows through the activity log channel changes.
- **Problems with the activity log channel:** In Recovery Services vaults, activity logs that are pumped from Azure Backup follow a new model. Unfortunately, this change affects the generation of activity logs in Azure Government, Azure Germany, and Azure China 21Vianet. If users of these cloud services create or configure any alerts from activity logs in Azure Monitor, the alerts aren't triggered. Also, in all Azure public regions, if a user [collects Recovery Services activity logs into a Log Analytics workspace](#), these logs don't appear.

Use a Log Analytics workspace for monitoring and alerting at scale for all your workloads that are protected by Azure Backup.

## Next steps

To create custom queries, see [Log Analytics data model](#).

# Configure Azure Backup reports

2/24/2020 • 7 minutes to read • [Edit Online](#)

A common requirement for backup admins is to obtain insights on backups, based on data spanning a long period of time. There could be multiple use cases for such a solution - allocating and forecasting of cloud storage consumed, auditing of backups and restores, and identifying key trends at different levels of granularity.

Today, Azure Backup provides a reporting solution that leverages [Azure Monitor Logs](#) and [Azure Workbooks](#), helping you get rich insights on your backups across your entire backup estate. This article explains how to configure and view Backup Reports.

## Supported scenarios

- Backup Reports are supported for Azure VMs, SQL in Azure VMs, SAP HANA/ASE in Azure VMs, Azure Backup Agent (MARS), Azure Backup Server (MABS) and System Center DPM.
- For DPM workloads, Backup Reports are supported for DPM Version 5.1.363.0 and above, and Agent Version 2.0.9127.0 and above.
- For MABS workloads, Backup Reports are supported for MABS Version 13.0.415.0 and above, and Agent Version 2.0.9170.0 and above.
- Backup Reports can be viewed across all backup items, vaults, subscriptions and regions as long as their data is being sent to a Log Analytics (LA) Workspace that the user has access to.
- If you are an [Azure Lighthouse](#) user with delegated access to your customers' subscriptions, you can use these reports with Azure Lighthouse to view reports across all your tenants.
- Data for log backup jobs is currently not displayed in the reports.

## Getting started

To get started with using the reports, follow the three steps detailed below:

### 1. **Create a Log Analytics (LA) workspace (or use an existing one):**

You need to set up one or more LA Workspaces to store your backup reporting data. The location and subscription where this LA workspace can be created is independent of the location and subscription where your vaults exist.

Refer to the following article: [Create a Log Analytics Workspace in the Azure portal](#) to set up an LA Workspace.

By default, the data in an LA Workspace is retained for 30 days. To see data for a longer time horizon, change the retention period of the LA Workspace. To change the retention period, refer to the following article: [Manage usage and costs with Azure Monitor Logs](#).

### 2. **Configure diagnostics settings for your vaults:**

Azure Resource Manager resources, such as Recovery Services vaults, record information about scheduled operations and user-triggered operations as diagnostics data.

In the monitoring section of your Recovery Services vault, select **Diagnostic settings** and specify the target for the Recovery Services vault's diagnostic data. [Learn more about using diagnostic events](#).

## Diagnostics settings

Save Discard Delete

Name \*

test



Archive to a storage account

Stream to an event hub

Send to Log Analytics

Subscription

contososub



Log Analytics Workspace

contosoworkspace ( eastus )



Destination table ⓘ

Azure diagnostics  Resource specific

**i** You need to create separate diagnostics settings for Azure Backup and Azure Site Recovery events to prevent potential data loss. For Azure Backup events, if you choose the 'Resource specific' mode, you must select the following events only - CoreAzureBackup, AddonAzureBackupJobs, AddonAzureBackupAlerts, AddonAzureBackupPolicy, AddonAzureBackupStorage, AddonAzureBackupProtectedInstance. The AzureBackupReport event works only in 'Azure diagnostics' mode. [Learn more](#)

log

AzureBackupReport

CoreAzureBackup

AddonAzureBackupJobs

AddonAzureBackupAlerts

AddonAzureBackupPolicy

AddonAzureBackupStorage

AddonAzureBackupProtectedInstance

AzureSiteRecoveryJobs

AzureSiteRecoveryEvents

AzureSiteRecoveryReplicatedItems

AzureSiteRecoveryReplicationStats

AzureSiteRecoveryRecoveryPoints

Azure Backup also provides a built-in Azure Policy, which automates the configuration of diagnostic settings for all vaults in a given scope. Refer to the following article to learn how to use this policy: [Configure Vault Diagnostics](#)

## Settings at scale

### 3. View reports on the Azure portal:

Once you have configured your vaults to send data to LA, view your backup reports by navigating to any vault's blade and clicking on the **Backup Reports** menu item.

The screenshot shows the Azure portal interface for a 'Recovery Services vault' named 'contoso-vault'. On the left, there's a navigation sidebar with links like 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Properties', 'Locks', and 'Export template'. Below these are sections for 'Getting started' (with 'Backup' and 'Site Recovery' options) and 'Protected items'. On the right, under the 'Backup' heading, there are several links: 'Getting started', 'Backup dashboard', 'Backup items', 'Backup policies', 'Backup Reports' (which is highlighted with a red box), 'Backup Explorer', and 'Learn more'. A large blue cloud icon with a circular arrow is centered between the sidebar and the main content area.

Clicking this link opens up the Backup Report Workbook.

#### NOTE

Currently, the initial load of the report may take up to 1 minute.

Below is a description of the various tabs that the report contains:

- **Summary** - The Summary tab provides a high-level overview of your backup estate. Under the Summary tab, you can get a quick glance of the total number of backup items, total cloud storage consumed, the number of protected instances and the job success rate per workload type. For more detailed information around a specific backup artifact type, navigate to the respective tabs.

[Overview](#) [Summary](#) [Backup Items](#) [Usage](#) [Jobs](#) [Policies](#)

### Report Filters

Filters are applied left to right and top to bottom on each page. [Learn More](#)

Time Range ⓘ  Backup Management Type ⓘ Subscription Name ⓘ Vault Location ⓘ Vault Name ⓘ

All datetimes are in UTC. Data for the current partial day is not shown in the reports. [Learn More](#)

|                           |                                    |                                     |                           |
|---------------------------|------------------------------------|-------------------------------------|---------------------------|
| Backup Items<br><b>42</b> | Protected Instances<br><b>15.5</b> | Cloud Storage (GB)<br><b>570.98</b> | Jobs Created<br><b>33</b> |
|---------------------------|------------------------------------|-------------------------------------|---------------------------|

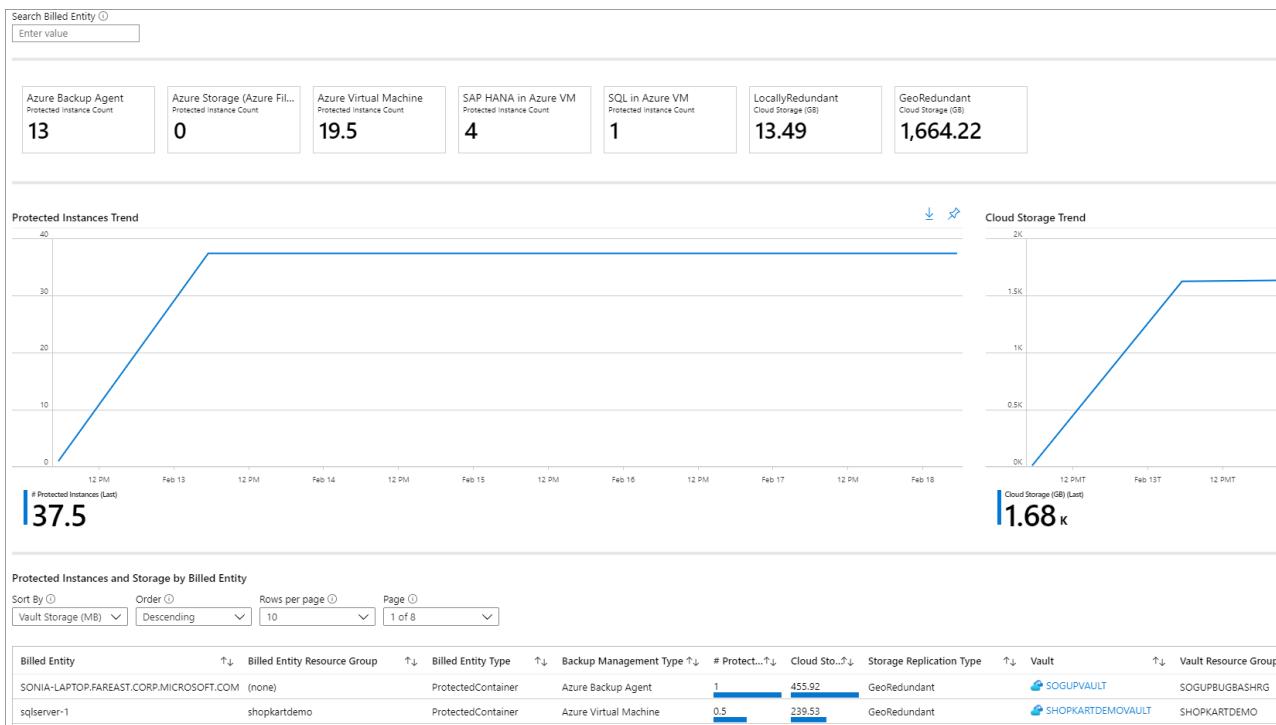
#### Key Parameters by Backup Item Type

| Backup Management Type      | Backup Item Type | # Backup... | Job Succ... | Cloud Sto... |
|-----------------------------|------------------|-------------|-------------|--------------|
| Azure Backup Agent          | Files and Folder | 7           | -           | 190.60       |
| Azure Storage (Azure Files) | Azure File Share | 1           | 100.0 %     | 0.00         |

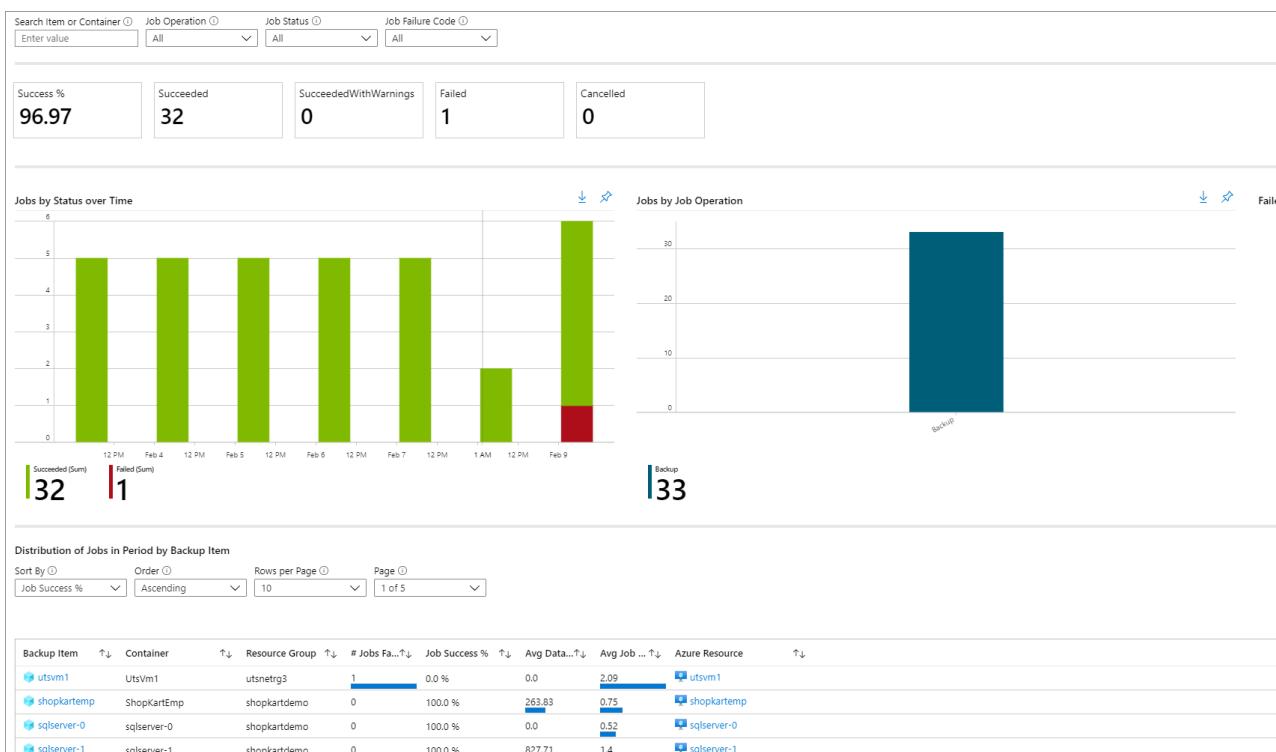
- Backup Items** - The Backup Items tab allows you to see information and trends on cloud storage consumed at a Backup Item level. For example, if you are using SQL in Azure VM backup, you can see the cloud storage consumed for each SQL database being backed up. You can also choose to see data for backup items of a particular protection status. For example, clicking on the **Protection Stopped** tile at the top of the tab, filters all the below widgets to show data only for Backup Items in Protection Stopped state.

| Search item or Container ⓘ<br>Enter value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                               |                                  |                                            |                |                  |                          |                |                          |                |    |                                         |        |                                            |        |            |              |  |             |             |              |             |        |                  |              |             |          |              |         |                     |        |              |              |              |    |              |         |                     |        |              |              |              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|----------------------------------|--------------------------------------------|----------------|------------------|--------------------------|----------------|--------------------------|----------------|----|-----------------------------------------|--------|--------------------------------------------|--------|------------|--------------|--|-------------|-------------|--------------|-------------|--------|------------------|--------------|-------------|----------|--------------|---------|---------------------|--------|--------------|--------------|--------------|----|--------------|---------|---------------------|--------|--------------|--------------|--------------|
| Protected<br><b>82</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | ProtectionStopped<br><b>7</b>                                                 | InitialBackupPending<br><b>2</b> |                                            |                |                  |                          |                |                          |                |    |                                         |        |                                            |        |            |              |  |             |             |              |             |        |                  |              |             |          |              |         |                     |        |              |              |              |    |              |         |                     |        |              |              |              |
| <p>Backup Items Trend</p> <p># Backup Items (Last)<br/><b>91</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <p>Cloud Storage Trend</p> <p>Cloud Storage (GB) (Last)<br/><b>1.68 k</b></p> |                                  |                                            |                |                  |                          |                |                          |                |    |                                         |        |                                            |        |            |              |  |             |             |              |             |        |                  |              |             |          |              |         |                     |        |              |              |              |    |              |         |                     |        |              |              |              |
| <p>Storage by BackupItem</p> <p>Search Policy Name ⓘ Sort By ⓘ Order ⓘ Rows Per Page ⓘ Page ⓘ</p> <table border="1"> <thead> <tr> <th>Backup Item</th> <th>Container</th> <th>Resource Group</th> <th>Policy</th> <th>Cloud Sto...</th> <th>Vault</th> <th>Storage Replication Type</th> <th>Azure Resource</th> </tr> </thead> <tbody> <tr> <td>C1</td> <td>SONIA-LAPTOP.FAREAST.CORP.MICROSOFT.COM</td> <td>(none)</td> <td>MABPol01b8affd-9f34-4de1-bc8c-5b02197b486f</td> <td>455.92</td> <td>SOGUPVAULT</td> <td>GeoRedundant</td> <td></td> </tr> <tr> <td>sqlserver-1</td> <td>sqlserver-1</td> <td>shopkartdemo</td> <td>FinanceTest</td> <td>239.53</td> <td>SHOPARTDEMOVAULT</td> <td>GeoRedundant</td> <td>sqlserver-1</td> </tr> <tr> <td>systemdb</td> <td>hanamachine2</td> <td>SAPHANA</td> <td>SAPHANABackupPolicy</td> <td>117.06</td> <td>SAPHANAVULT2</td> <td>GeoRedundant</td> <td>hanamachine2</td> </tr> <tr> <td>hx</td> <td>hanamachine2</td> <td>SAPHANA</td> <td>SAPHANABackupPolicy</td> <td>116.13</td> <td>SAPHANAVULT2</td> <td>GeoRedundant</td> <td>hanamachine2</td> </tr> </tbody> </table> |                                                                               | Backup Item                      | Container                                  | Resource Group | Policy           | Cloud Sto...             | Vault          | Storage Replication Type | Azure Resource | C1 | SONIA-LAPTOP.FAREAST.CORP.MICROSOFT.COM | (none) | MABPol01b8affd-9f34-4de1-bc8c-5b02197b486f | 455.92 | SOGUPVAULT | GeoRedundant |  | sqlserver-1 | sqlserver-1 | shopkartdemo | FinanceTest | 239.53 | SHOPARTDEMOVAULT | GeoRedundant | sqlserver-1 | systemdb | hanamachine2 | SAPHANA | SAPHANABackupPolicy | 117.06 | SAPHANAVULT2 | GeoRedundant | hanamachine2 | hx | hanamachine2 | SAPHANA | SAPHANABackupPolicy | 116.13 | SAPHANAVULT2 | GeoRedundant | hanamachine2 |
| Backup Item                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Container                                                                     | Resource Group                   | Policy                                     | Cloud Sto...   | Vault            | Storage Replication Type | Azure Resource |                          |                |    |                                         |        |                                            |        |            |              |  |             |             |              |             |        |                  |              |             |          |              |         |                     |        |              |              |              |    |              |         |                     |        |              |              |              |
| C1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | SONIA-LAPTOP.FAREAST.CORP.MICROSOFT.COM                                       | (none)                           | MABPol01b8affd-9f34-4de1-bc8c-5b02197b486f | 455.92         | SOGUPVAULT       | GeoRedundant             |                |                          |                |    |                                         |        |                                            |        |            |              |  |             |             |              |             |        |                  |              |             |          |              |         |                     |        |              |              |              |    |              |         |                     |        |              |              |              |
| sqlserver-1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | sqlserver-1                                                                   | shopkartdemo                     | FinanceTest                                | 239.53         | SHOPARTDEMOVAULT | GeoRedundant             | sqlserver-1    |                          |                |    |                                         |        |                                            |        |            |              |  |             |             |              |             |        |                  |              |             |          |              |         |                     |        |              |              |              |    |              |         |                     |        |              |              |              |
| systemdb                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | hanamachine2                                                                  | SAPHANA                          | SAPHANABackupPolicy                        | 117.06         | SAPHANAVULT2     | GeoRedundant             | hanamachine2   |                          |                |    |                                         |        |                                            |        |            |              |  |             |             |              |             |        |                  |              |             |          |              |         |                     |        |              |              |              |    |              |         |                     |        |              |              |              |
| hx                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | hanamachine2                                                                  | SAPHANA                          | SAPHANABackupPolicy                        | 116.13         | SAPHANAVULT2     | GeoRedundant             | hanamachine2   |                          |                |    |                                         |        |                                            |        |            |              |  |             |             |              |             |        |                  |              |             |          |              |         |                     |        |              |              |              |    |              |         |                     |        |              |              |              |

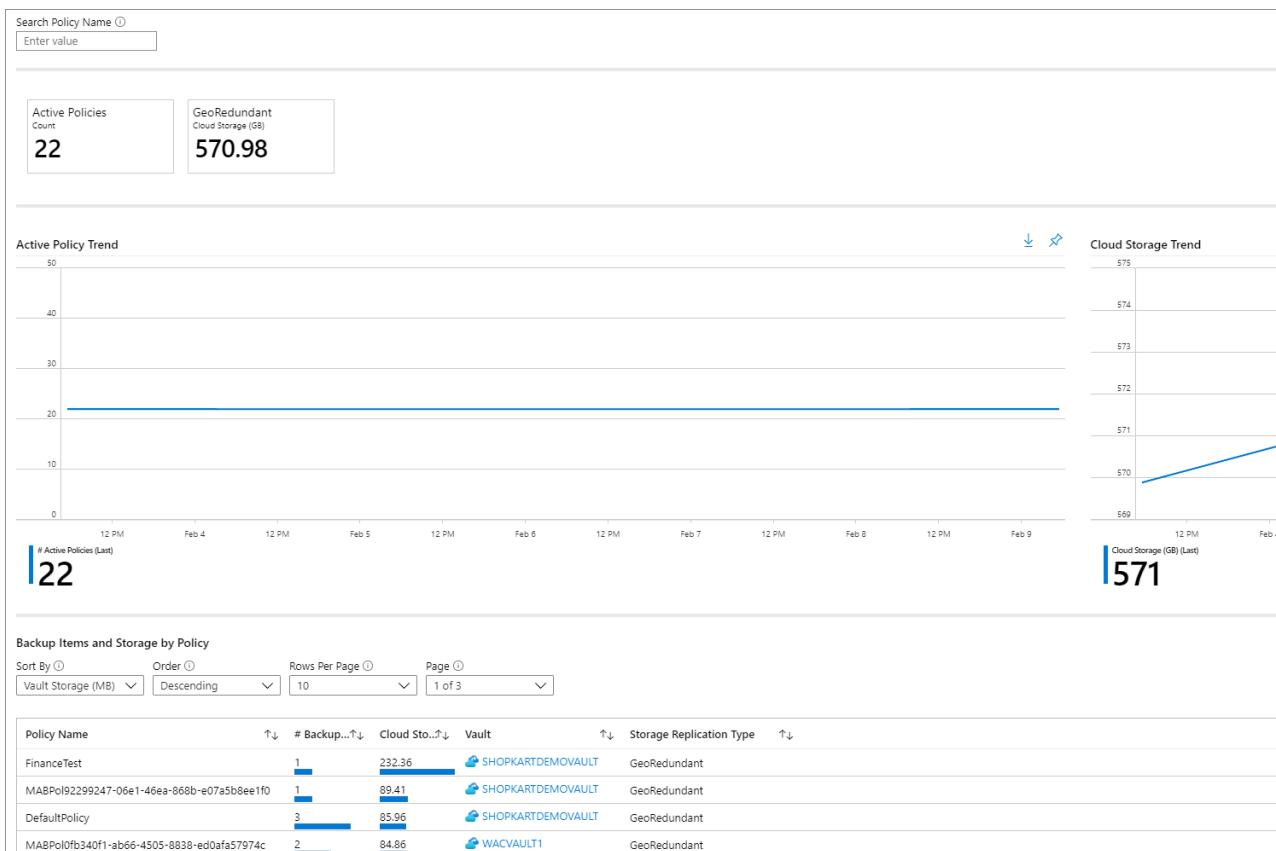
- Usage** - The Usage tab helps you view key billing parameters for your backups. The information shown in this tab is at a billing entity (protected container) level. For example, in the case of a DPM server being backed up to Azure, you can view the trend of protected instances and cloud storage consumed for the DPM server. Similarly, if you are using SQL in Azure Backup or SAP HANA in Azure Backup, this tab gives you usage-related information at the level of the virtual machine that these databases are contained in.



- Jobs** - The Jobs tab lets you view long running trends on jobs, such as the number of failed jobs per day and the top causes of job failure. You can view this information at both an aggregate level and at a backup item level. Clicking on a particular backup item in a grid lets you view detailed information on each job that was triggered on that backup item in the selected time range.



- Policies** - The Policies tab lets you view information on all of your active policies, such as the number of associated items, and the total cloud storage consumed by items backed up under a given policy. Clicking on a particular policy lets you view information on each of its associated backup items.



## Exporting to Excel

Clicking on the down arrow button at the top right of any widget (table/chart) exports the contents of that widget as an Excel sheet, as-is with existing filters applied. To export more rows of a table to Excel, you can increase the number of rows displayed on the page by using the **Rows Per Page** dropdown at the top of each grid.

## Pinning to Dashboard

Click the Pin Icon at the top of each widget to pin the widget to your Azure portal dashboard. This helps you create customized dashboards tailored to display the most important information that you need.

## Cross-tenant Reports

If you are an [Azure Lighthouse](#) user with delegated access to subscriptions across multiple tenant environments, you can use the default subscription filter (by clicking on the filter icon in the top right of the Azure portal) to choose all the subscriptions you wish to see data for. Doing so will let you select LA Workspaces across your tenants to view multi-tenanted reports.

## Conventions used in Backup Reports

- Filters work from left to right and top to bottom on each tab, that is, any filter only applies to all those widgets that are positioned either to the right of that filter or below that filter.
- Clicking on a colored tile filters the widgets below the tile for records pertaining to the value of that tile. For example, clicking on the *Protection Stopped* tile in the Backup Items tab filters the grids and charts below to show data for backup items in 'Protection Stopped' state.
- Tiles that are not colored are not clickable.
- Data for the current partial day is not shown in the reports. Thus, when the selected value of **Time Range** is, **Last 7 days**, the report shows records for the last 7 completed days (which does not include the current day).
- The report shows details of Jobs (apart from log jobs) that were **triggered** in the selected time range.
- The values shown for Cloud Storage and Protected Instances, are at the **end** of the selected time range.

- The Backup Items displayed in the reports are those items that exist at the **end** of the selected time range. Backup Items which were deleted in the middle of the selected time range are not displayed. The same convention applies for Backup Policies as well.

## Query load times

The widgets in the Backup Report are powered by Kusto queries, which run on the user's LA Workspaces. As these queries typically involve the processing of large amounts of data, with multiple joins to enable richer insights, the widgets may not load instantaneously when the user is viewing reports across a large backup estate. The table below provides a rough estimate of the time that different widgets can take to load, based on the number of backup items and the time range for which the report is being viewed:

| # DATASOURCES | TIME HORIZON | LOAD TIMES (APPROX.)                                                                             |
|---------------|--------------|--------------------------------------------------------------------------------------------------|
| ~5 K          | 1 month      | Tiles: 5-10 secs<br>Grids: 5-10 secs<br>Charts: 5-10 secs<br>Report-level filters: 5-10 secs     |
| ~5 K          | 3 months     | Tiles: 5-10 secs<br>Grids: 5-10 secs<br>Charts: 5-10 secs<br>Report-level filters: 5-10 secs     |
| ~10 K         | 3 months     | Tiles: 15-20 secs<br>Grids: 15-20 secs<br>Charts: 1-2 mins<br>Report-level filters: 25-30 secs   |
| ~15 K         | 1 month      | Tiles: 15-20 secs<br>Grids: 15-20 secs<br>Charts: 50-60 secs<br>Report-level filters: 20-25 secs |
| ~15 K         | 3 months     | Tiles: 20-30 secs<br>Grids: 20-30 secs<br>Charts: 2-3 mins<br>Report-level filters: 50-60 secs   |

## What happened to the Power BI Reports?

- Our earlier Power BI template app for reporting (which sourced data from an Azure Storage Account) is on a deprecation path. It is recommended to start sending vault diagnostic data to Log Analytics as described above, to view reports.
- In addition, the V1 schema of sending diagnostics data to a storage account or an LA Workspace is also on a deprecation path. This means that if you have written any custom queries or automations based on the V1 schema, you are advised to update these queries to use the currently supported V2 schema.

## Next steps

[Learn more about monitoring and reporting with Azure Backup](#)

# Using Diagnostics Settings for Recovery Services Vaults

2/24/2020 • 4 minutes to read • [Edit Online](#)

Azure Backup sends diagnostics events that can be collected and used for the purposes of analysis, alerting and reporting.

You can configure diagnostics settings for a Recovery Services Vault via the Azure portal, by navigating to the vault and clicking the **Diagnostic Settings** menu item. Clicking on **+ Add Diagnostic Setting** lets you send one or more diagnostics events to a Storage Account, Event Hub, or a Log Analytics (LA) Workspace.

Home > contosovault - Diagnostic settings > Diagnostics settings

## Diagnostics settings

Save Discard Delete

Name \*

Archive to a storage account  
 Stream to an event hub  
 Send to Log Analytics

log

AzureBackupReport  
 CoreAzureBackup  
 AddonAzureBackupJobs  
 AddonAzureBackupAlerts  
 AddonAzureBackupPolicy  
 AddonAzureBackupStorage  
 AddonAzureBackupProtectedInstance  
 AzureSiteRecoveryJobs  
 AzureSiteRecoveryEvents  
 AzureSiteRecoveryReplicatedItems  
 AzureSiteRecoveryReplicationStats  
 AzureSiteRecoveryRecoveryPoints  
 AzureSiteRecoveryReplicationDataUploadRate  
 AzureSiteRecoveryProtectedDiskDataChurn

## Diagnostics Events Available for Azure Backup Users

Azure Backup provides the following diagnostic events, each of which provides detailed data on a specific set of backup-related artifacts:

- CoreAzureBackup
- AddonAzureBackupAlerts
- AddonAzureBackupProtectedInstance
- AddonAzureBackupJobs
- AddonAzureBackupPolicy

- AddonAzureBackupStorage

#### Data Model for Azure Backup Diagnostics Events

Data for these events can be sent to either a storage account, LA workspace, or an Event Hub. If you are sending this data to an LA Workspace, you need to select the **Resource Specific** toggle in the **Diagnostics Setting** screen (see more information in the sections below).

## Using Diagnostics Settings with Log Analytics (LA)

Aligning with the Azure Log Analytics roadmap, Azure Backup now allows you to send vault diagnostics data to dedicated LA tables for Backup. These are referred to as [Resource Specific tables](#).

To send your vault diagnostics data to LA:

1. Navigate to your vault and click on **Diagnostic Settings**. Click + **Add Diagnostic Setting**.
2. Give a name to the Diagnostics setting.
3. Check the box **Send to Log Analytics** and select a Log Analytics Workspace.
4. Select **Resource Specific** in the toggle and check the following six events - **CoreAzureBackup**, **AddonAzureBackupAlerts**, **AddonAzureBackupProtectedInstance**, **AddonAzureBackupJobs**, **AddonAzureBackupPolicy**, and **AddonAzureBackupStorage**.
5. Click on **Save**.

## Diagnostics settings

Save Discard Delete

Name \*

test



Archive to a storage account

Stream to an event hub

Send to Log Analytics

Subscription

contososub



Log Analytics Workspace

contosoworkspace ( eastus )



Destination table ⓘ

Azure diagnostics  Resource specific



You need to create separate diagnostics settings for Azure Backup and Azure Site Recovery events to prevent potential data loss. For Azure Backup events, if you choose the 'Resource specific' mode, you must select the following events only - CoreAzureBackup, AddonAzureBackupJobs, AddonAzureBackupAlerts, AddonAzureBackupPolicy, AddonAzureBackupStorage, AddonAzureBackupProtectedInstance. The AzureBackupReport event works only in 'Azure diagnostics' mode. [Learn more](#)

log

AzureBackupReport

CoreAzureBackup

AddonAzureBackupJobs

AddonAzureBackupAlerts

AddonAzureBackupPolicy

AddonAzureBackupStorage

AddonAzureBackupProtectedInstance

AzureSiteRecoveryJobs

AzureSiteRecoveryEvents

AzureSiteRecoveryReplicatedItems

AzureSiteRecoveryReplicationStats

AzureSiteRecoveryRecoveryPoints

Once data flows into the LA Workspace, dedicated tables for each of these events are created in your workspace. You can query any of these tables directly and also perform joins or unions between these tables if necessary.

## IMPORTANT

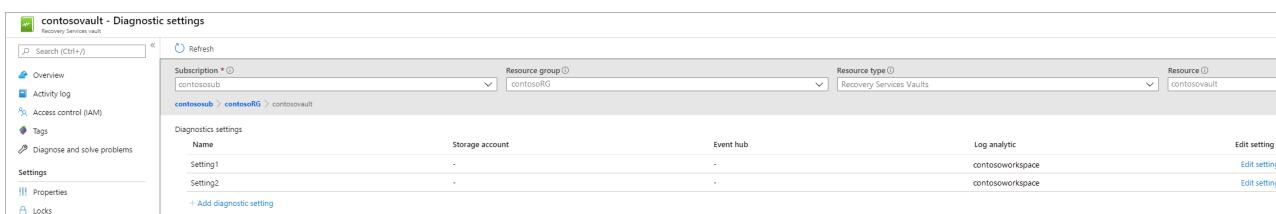
The above six events, namely, CoreAzureBackup, AddonAzureBackupAlerts, AddonAzureBackupProtectedInstance, AddonAzureBackupJobs, AddonAzureBackupPolicy, and AddonAzureBackupStorage, are supported **only** in Resource Specific Mode. Please note that if you try to send data for these six events in Azure Diagnostics Mode, no data will flow to the LA Workspace.

## Legacy Event

Traditionally, all backup-related diagnostics data for a vault has been contained in a single event called 'AzureBackupReport'. The six events described above are, in essence, a decomposition of all the data contained in AzureBackupReport.

Currently, we continue to support the AzureBackupReport event for backward-compatibility, in cases where users have existing custom queries on this event, for example, custom log alerts, custom visualizations etc. However, we recommend choosing the new events for all new diagnostics settings on the vault since this makes the data much easier to work with in log queries, provides better discoverability of schemas and their structure, improves performance across both ingestion latency and query times. Support for using the Azure Diagnostics mode will eventually be phased out and hence choosing the new events may help you to avoid complex migrations at a later date.

You may choose to create separate diagnostics settings for AzureBackupReport and the six new events, until you have migrated all of your custom queries to use data from the new tables. The below image shows an example of a vault having two diagnostic settings. The first setting, named **Setting1** sends data of AzureBackupReport event to an LA Workspace in AzureDiagnostics mode. The second setting, named **Setting2** sends data of the six new Azure Backup events to an LA Workspace in Resource Specific mode.



## IMPORTANT

The AzureBackupReport event is supported **only** in Azure Diagnostics Mode. Please note that if you try to send data for this event in Resource Specific Mode, no data will flow to the LA Workspace.

## NOTE

The toggle for Azure Diagnostics / Resource Specific appears only if the user checks **Send to Log Analytics**. To send data to a Storage Account or an Event Hub, a user can simply select the required destination and check any of the desired events, without any additional inputs. Again, it is recommended not to choose the legacy event AzureBackupReport, going forward.

## Users sending Azure Site Recovery Events to Log Analytics (LA)

Azure Backup and Azure Site Recovery Events are sent from the same Recovery Services Vault. As Azure Site Recovery is currently not onboarded onto Resource Specific tables, users wanting to send Azure Site Recovery Events to LA are directed to use Azure Diagnostics Mode **only** (see image below). **Choosing Resource Specific Mode for the Azure Site Recovery Events will prevent the required data from being sent to the LA Workspace.**

## Diagnostics settings

Save Discard Delete

Name \*

Setting3



Archive to a storage account

Stream to an event hub

Send to Log Analytics

Subscription

contososub



Log Analytics Workspace

contosoworkspace ( eastus )



Destination table ⓘ

Azure diagnostics Resource specific

You need to create separate diagnostics settings for Azure Backup and Azure Site Recovery events to prevent potential data loss. For Azure Backup events, if you choose the 'Resource specific' mode, you must select the following events only - CoreAzureBackup, AddonAzureBackupJobs, AddonAzureBackupAlerts, AddonAzureBackupPolicy, AddonAzureBackupStorage, AddonAzureBackupProtectedInstance. The AzureBackupReport event works only in 'Azure diagnostics' mode. [Learn more](#)

log

AzureBackupReport

CoreAzureBackup

AddonAzureBackupJobs

AddonAzureBackupAlerts

AddonAzureBackupPolicy

AddonAzureBackupStorage

AddonAzureBackupProtectedInstance

AzureSiteRecoveryJobs

AzureSiteRecoveryEvents

AzureSiteRecoveryReplicatedItems

AzureSiteRecoveryReplicationStats

AzureSiteRecoveryRecoveryPoints

AzureSiteRecoveryReplicationDataUploadRate

AzureSiteRecoveryProtectedDiskDataChurn

To summarize the above nuances:

- If you already have LA diagnostics set up with Azure Diagnostics and have written custom queries on top of it, keep that setting **intact**, until you migrate your queries to use data from the new events.
- If you also want to onboard onto new tables (as recommended), create a **new** diagnostics setting, choose **Resource Specific** and select the six new events as specified above.
- If you are currently sending Azure Site Recovery Events to LA, **do not** choose Resource Specific mode for these events, otherwise data for these events will not flow into your LA Workspace. Instead, create an **additional diagnostic setting**, select **Azure Diagnostics**, and choose the relevant Azure Site Recovery events.

The below image shows an example of a user having three diagnostic settings for a vault. The first setting, named **Setting1** sends data from AzureBackupReport event to an LA Workspace in AzureDiagnostics mode. The second setting, named **Setting2** sends data from the six new Azure Backup events to an LA Workspace in Resource Specific mode. The third setting, named **Setting3**, sends data from the Azure Site Recovery events to an LA Workspace in Azure Diagnostics Mode.

The screenshot shows the Azure portal interface for managing diagnostic settings. The left sidebar lists vault-related options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Properties, Locks, and Export template. The main area is titled "Diagnostic settings" for a vault named "contosovault". It includes filters for Subscription ("contosousub"), Resource group ("contosolog"), Resource type ("Recovery Services Vaults"), and Resource ("contosovault"). A table lists three diagnostic settings:

| Name     | Storage account | Event hub | Log analytic     | Edit setting |
|----------|-----------------|-----------|------------------|--------------|
| Setting1 | -               | -         | contosoworkspace | Edit setting |
| Setting2 | -               | -         | contosoworkspace | Edit setting |
| Setting3 | -               | -         | contosoworkspace | Edit setting |

An "Add diagnostic setting" link is visible at the bottom of the table.

## Next steps

[Learn the Log Analytics Data Model for the Diagnostics Events](#)

# Data Model for Azure Backup Diagnostics Events

2/24/2020 • 10 minutes to read • [Edit Online](#)

## CoreAzureBackup

This table provides information about core backup entities, such as vaults and backup items.

| FIELD                          | DATA TYPE | DESCRIPTION                                                                                                         |
|--------------------------------|-----------|---------------------------------------------------------------------------------------------------------------------|
| ResourceId                     | Text      | Resource identifier for data being collected. For example, Recovery Services vault resource ID.                     |
| OperationName                  | Text      | This field represents the name of the current operation - BackupItem, BackupItemAssociation, or ProtectedContainer. |
| Category                       | Text      | This field represents the category of diagnostics data pushed to Azure Monitor logs. For example, CoreAzureBackup.  |
| AgentVersion                   | Text      | Version number of Agent Backup or the Protection Agent (in case of SC DPM and MABS)                                 |
| AzureBackupAgentVersion        | Text      | Version of the Azure Backup Agent on the Backup Management Server                                                   |
| AzureDataCenter                | Text      | Data center where the vault is located                                                                              |
| BackupItemAppVersion           | Text      | Application version of the backup item                                                                              |
| BackupItemFriendlyName         | Text      | Friendly name of the backup item                                                                                    |
| BackupItemName                 | Text      | Name of the backup item                                                                                             |
| BackupItemProtectionState      | Text      | Protection State of the Backup Item                                                                                 |
| BackupItemFrontEndSize         | Text      | Front-end size of the backup item                                                                                   |
| BackupItemType                 | Text      | Type of backup item. For example: VM, FileFolder                                                                    |
| BackupItemUniqueId             | Text      | Unique identifier of the backup item                                                                                |
| BackupManagementServerType     | Text      | Type of the Backup Management Server, as in MABS, SC DPM                                                            |
| BackupManagementServerUniqueId | Text      | Field to uniquely identify the Backup Management Server                                                             |

| FIELD                             | DATA TYPE | DESCRIPTION                                                                                            |
|-----------------------------------|-----------|--------------------------------------------------------------------------------------------------------|
| BackupManagementType              | Text      | Provider type for server doing backup job. For example, IaaSVM, FileFolder                             |
| BackupManagementServerName        | Text      | Name of the Backup Management Server                                                                   |
| BackupManagementServerOSVersion   | Text      | OS version of the Backup Management Server                                                             |
| BackupManagementServerVersion     | Text      | Version of the Backup Management Server                                                                |
| LatestRecoveryPointLocation       | Text      | Location of the latest recovery point for the backup item                                              |
| LatestRecoveryPointTime           | DateTime  | Date time of the latest recovery point for the backup item                                             |
| OldestRecoveryPointLocation       | Text      | Location of the oldest recovery point for the backup item                                              |
| OldestRecoveryPointTime           | DateTime  | Date time of the latest recovery point for the backup item                                             |
| PolicyUniqueId                    | Text      | Unique ID to identify the policy                                                                       |
| ProtectedContainerFriendlyName    | Text      | Friendly name of the protected server                                                                  |
| ProtectedContainerLocation        | Text      | Whether the Protected Container is located On-premises or in Azure                                     |
| ProtectedContainerName            | Text      | Name of the Protected Container                                                                        |
| ProtectedContainerOSType          | Text      | OS Type of the Protected Container                                                                     |
| ProtectedContainerOSVersion       | Text      | OS Version of the Protected Container                                                                  |
| ProtectedContainerProtectionState | Text      | Protection State of the Protected Container                                                            |
| ProtectedContainerType            | Text      | Whether the Protected Container is a server, or a container                                            |
| ProtectedContainerUniqueId        | Text      | Unique ID used to identify the protected container for everything except VMs backed up using DPM, MABS |
| ProtectedContainerWorkloadType    | Text      | Type of the Protected Container backed up. For example, IaaSVMContainer                                |

| FIELD                          | DATA TYPE | DESCRIPTION                                                                                                |
|--------------------------------|-----------|------------------------------------------------------------------------------------------------------------|
| ProtectionGroupName            | Text      | Name of the Protection Group the Backup Item is protected in, for SC DPM, and MABS, if applicable          |
| ResourceGroupName              | Text      | Resource group of the resource (for example, Recovery Services vault) for data being collected             |
| SchemaVersion                  | Text      | This field denotes the current version of the schema, it is <b>V2</b>                                      |
| SecondaryBackupProtectionState | Text      | Whether secondary protection is enabled for the backup item                                                |
| State                          | Text      | State of the backup item object. For example, Active, Deleted                                              |
| StorageReplicationType         | Text      | Type of storage replication for the vault. For example, GeoRedundant                                       |
| SubscriptionId                 | Text      | Subscription identifier of the resource (for example, Recovery Services vault) for which data is collected |
| VaultName                      | Text      | Name of the vault                                                                                          |
| VaultTags                      | Text      | Tags associated with the vault resource                                                                    |
| VaultUniqueId                  | Text      | Unique Identifier of the vault                                                                             |
| SourceSystem                   | Text      | Source system of the current data - Azure                                                                  |

## AddonAzureBackupAlerts

This table provides details about alert related fields.

| FIELD         | DATA TYPE | DESCRIPTION                                                                                                          |
|---------------|-----------|----------------------------------------------------------------------------------------------------------------------|
| ResourceId    | Text      | Unique identifier for the resource about which data is collected. For example, a Recovery Services vault resource ID |
| OperationName | Text      | Name of the current operation. For example, Alert                                                                    |
| Category      | Text      | Category of diagnostics data pushed to Azure Monitor logs - AddonAzureBackupAlerts                                   |
| AlertCode     | Text      | Code to uniquely identify an alert type                                                                              |

| FIELD                          | DATA TYPE | DESCRIPTION                                                                                                 |
|--------------------------------|-----------|-------------------------------------------------------------------------------------------------------------|
| AlertConsolidationStatus       | Text      | Identify if the alert is a consolidated alert or not                                                        |
| AlertOccurrenceDateTime        | DateTime  | Date and time when the alert was created                                                                    |
| AlertRaisedOn                  | Text      | Type of entity the alert is raised on                                                                       |
| AlertSeverity                  | Text      | Severity of the alert. For example, Critical                                                                |
| AlertStatus                    | Text      | Status of the alert. For example, Active                                                                    |
| AlertTimeToResolveInMinutes    | Number    | Time taken to resolve an alert. Blank for active alerts.                                                    |
| AlertType                      | Text      | Type of alert. For example, Backup                                                                          |
| AlertUniqueld                  | Text      | Unique identifier of the generated alert                                                                    |
| BackupItemUniqueld             | Text      | Unique identifier of the backup item associated with the alert                                              |
| BackupManagementServerUniqueld | Text      | Field to uniquely identify the Backup Management Server the Backup Item is protected through, if applicable |
| BackupManagementType           | Text      | Provider type for server doing backup job, for example, IaaSVM, FileFolder                                  |
| CountOfAlertsConsolidated      | Number    | Number of alerts consolidated if it is a consolidated alert                                                 |
| ProtectedContainerUniqueld     | Text      | Unique identifier of the protected server associated with the alert                                         |
| RecommendedAction              | Text      | Action recommended to resolve the alert                                                                     |
| SchemaVersion                  | Text      | Current version of the schema, for example <b>V2</b>                                                        |
| State                          | Text      | Current state of the alert object, for example, Active, Deleted                                             |
| StorageUniqueld                | Text      | Unique ID used to identify the storage entity                                                               |
| VaultUniqueld                  | Text      | Unique ID used to identify the vault related to the alert                                                   |
| SourceSystem                   | Text      | Source system of the current data - Azure                                                                   |

## AddonAzureBackupProtectedInstance

This table provides basic protected instances-related fields.

| FIELD                          | DATA TYPE | DESCRIPTION                                                                                                          |
|--------------------------------|-----------|----------------------------------------------------------------------------------------------------------------------|
| ResourceId                     | Text      | Unique identifier for the resource about which data is collected. For example, a Recovery Services vault resource ID |
| OperationName                  | Text      | Name of the operation, for example ProtectedInstance                                                                 |
| Category                       | Text      | Category of diagnostics data pushed to Azure Monitor logs - AddonAzureBackupProtectedInstance                        |
| BackupItemUniqueId             | Text      | Unique ID of the backup item                                                                                         |
| BackupManagementServerUniqueId | Text      | Field to uniquely identify the Backup Management Server the Backup Item is protected through, if applicable          |
| BackupManagementType           | Text      | Provider type for server doing backup job, for example, IaaSVM, FileFolder                                           |
| ProtectedContainerUniqueId     | Text      | Unique ID to identify the protected container the job is run on                                                      |
| ProtectedInstanceCount         | Text      | Count of Protected Instances for the associated backup item or protected container on that date-time                 |
| SchemaVersion                  | Text      | Current version of the schema, for example <b>V2</b>                                                                 |
| State                          | Text      | State of the backup item object, for example, Active, Deleted                                                        |
| VaultUniqueId                  | Text      | Unique identifier of the protected vault associated with the protected instance                                      |
| SourceSystem                   | Text      | Source system of the current data - Azure                                                                            |

## AddonAzureBackupJobs

This table provides details about job-related fields.

| FIELD      | DATA TYPE | DESCRIPTION                                                                                    |
|------------|-----------|------------------------------------------------------------------------------------------------|
| ResourceId | Text      | Resource identifier for data being collected. For example, Recovery Services vault resource ID |

| FIELD                          | DATA TYPE | DESCRIPTION                                                                                            |
|--------------------------------|-----------|--------------------------------------------------------------------------------------------------------|
| OperationName                  | Text      | This field represents name of the current operation - Job                                              |
| Category                       | Text      | This field represents category of diagnostics data pushed to Azure Monitor logs - AddonAzureBackupJobs |
| AdhocOrScheduledJob            | Text      | Field to specify if the job is Ad Hoc or Scheduled                                                     |
| BackupItemUniqueId             | Text      | Unique ID used to identify the backup item related to the storage entity                               |
| BackupManagementServerUniqueId | Text      | Unique ID used to identify the backup management server related to the storage entity                  |
| BackupManagementType           | Text      | Provider type for performing backup, for example, IaaSVM, FileFolder to which this alert belongs to    |
| DataTransferredInMB            | Number    | Data transferred in MB for this job                                                                    |
| JobDurationInSecs              | Number    | Total job duration in seconds                                                                          |
| JobFailureCode                 | Text      | Failure Code string because of which job failure happened                                              |
| JobOperation                   | Text      | Operation for which job is run for example, Backup, Restore, Configure Backup                          |
| JobOperationSubType            | Text      | Sub Type of the Job Operation. For example, 'Log', in the case of Log Backup Job                       |
| JobStartTime                   | DateTime  | Date and time when job started running                                                                 |
| JobStatus                      | Text      | Status of the finished job, for example, Completed, Failed                                             |
| JobUniqueId                    | Text      | Unique ID to identify the job                                                                          |
| ProtectedContainerUniqueId     | Text      | Unique identifier of the protected server associated with the alert                                    |
| RecoveryJobDestination         | Text      | Destination of a recovery job, where the data is recovered                                             |
| RecoveryJobRPDateTime          | DateTime  | The date, time when the recovery point that is being recovered was created                             |

| FIELD                | DATA TYPE | DESCRIPTION                                                              |
|----------------------|-----------|--------------------------------------------------------------------------|
| RecoveryJobLocation  | Text      | The location where the recovery point that is being recovered was stored |
| RecoveryLocationType | Text      | Type of the Recovery Location                                            |
| SchemaVersion        | Text      | Current version of the schema, for example <b>V2</b>                     |
| State                | Text      | Current state of the alert object, for example, Active, Deleted          |
| VaultUniqueld        | Text      | Unique identifier of the protected vault associated with the alert       |
| SourceSystem         | Text      | Source system of the current data - Azure                                |

## AddonAzureBackupPolicy

This table provides details about policy-related fields.

| FIELD                          | DATA TYPE    | DESCRIPTION                                                                                                          |
|--------------------------------|--------------|----------------------------------------------------------------------------------------------------------------------|
| Resourceld                     | Text         | Unique identifier for the resource about which data is collected. For example, a Recovery Services vault resource ID |
| OperationName                  | Text         | Name of the operation, for example, Policy or PolicyAssociation                                                      |
| Category                       | Text         | Category of diagnostics data pushed to Azure Monitor logs - AddonAzureBackupPolicy                                   |
| BackupDaysOfTheWeek            | Text         | Days of the week when backups have been scheduled                                                                    |
| BackupFrequency                | Text         | Frequency with which backups are run. For example, daily, weekly                                                     |
| BackupManagementType           | Text         | Provider type for server doing backup job. For example, IaaSVM, FileFolder                                           |
| BackupManagementServerUniqueld | Text         | Field to uniquely identify the Backup Management Server the Backup Item is protected through, if applicable          |
| BackupTimes                    | Text         | Date and time when backups are scheduled                                                                             |
| DailyRetentionDuration         | Whole Number | Total retention duration in days for configured backups                                                              |

| FIELD                           | DATA TYPE      | DESCRIPTION                                                                                          |
|---------------------------------|----------------|------------------------------------------------------------------------------------------------------|
| DailyRetentionTimes             | Text           | Date and time when daily retention was configured                                                    |
| DiffBackupDaysOfTheWeek         | Text           | Days of the week for Differential backups for SQL in Azure VM Backup                                 |
| DiffBackupFormat                | Text           | Format for Differential backups for SQL in Azure VM backup                                           |
| DiffBackupRetentionDuration     | Decimal Number | Retention duration for Differential backups for SQL in Azure VM Backup                               |
| DiffBackupTime                  | Time           | Time for Differential backups for SQL in Azure VM Backup                                             |
| LogBackupFrequency              | Decimal Number | Frequency for Log backups for SQL                                                                    |
| LogBackupRetentionDuration      | Decimal Number | Retention duration for Log backups for SQL in Azure VM Backup                                        |
| MonthlyRetentionDaysOfTheMonth  | Text           | Weeks of the month when monthly retention is configured. For example, First, Last, etc.              |
| MonthlyRetentionDaysOfTheWeek   | Text           | Days of the week selected for monthly retention                                                      |
| MonthlyRetentionDuration        | Text           | Total retention duration in months for configured backups                                            |
| MonthlyRetentionFormat          | Text           | Type of configuration for monthly retention. For example, daily for day based, weekly for week based |
| MonthlyRetentionTimes           | Text           | Date and time when monthly retention is configured                                                   |
| MonthlyRetentionWeeksOfTheMonth | Text           | Weeks of the month when monthly retention is configured. For example, First, Last, etc.              |
| PolicyName                      | Text           | Name of the policy defined                                                                           |
| PolicyUniqueId                  | Text           | Unique ID to identify the policy                                                                     |
| PolicyTimeZone                  | Text           | Timezone in which the Policy Time Fields are specified in the logs                                   |
| RetentionDuration               | Text           | Retention duration for configured backups                                                            |
| RetentionType                   | Text           | Type of retention                                                                                    |

| FIELD                          | DATA TYPE      | DESCRIPTION                                                                                         |
|--------------------------------|----------------|-----------------------------------------------------------------------------------------------------|
| SchemaVersion                  | Text           | This field denotes current version of the schema, it is <b>V2</b>                                   |
| State                          | Text           | Current state of the policy object. For example, Active, Deleted                                    |
| SynchronisationFrequencyPerDay | Whole Number   | Number of times in a day a file backup is synchronized for SC DPM and MABS                          |
| VaultUniqueld                  | Text           | Unique ID of the vault that this policy belongs to                                                  |
| WeeklyRetentionDaysOfTheWeek   | Text           | Days of the week selected for weekly retention                                                      |
| WeeklyRetentionDuration        | Decimal Number | Total weekly retention duration in weeks for configured backups                                     |
| WeeklyRetentionTimes           | Text           | Date and time when weekly retention is configured                                                   |
| YearlyRetentionDaysOfTheMonth  | Text           | Dates of the month selected for yearly retention                                                    |
| YearlyRetentionDaysOfTheWeek   | Text           | Days of the week selected for yearly retention                                                      |
| YearlyRetentionDuration        | Decimal Number | Total retention duration in years for configured backups                                            |
| YearlyRetentionFormat          | Text           | Type of configuration for yearly retention, for example, daily for day based, weekly for week based |
| YearlyRetentionMonthsOfTheYear | Text           | Months of the year selected for yearly retention                                                    |
| YearlyRetentionTimes           | Text           | Date and time when yearly retention is configured                                                   |
| YearlyRetentionWeeksOfTheMonth | Text           | Weeks of the month selected for yearly retention                                                    |
| SourceSystem                   | Text           | Source system of the current data - Azure                                                           |

## AddonAzureBackupStorage

This table provides details about storage-related fields.

| FIELD | DATA TYPE | DESCRIPTION |
|-------|-----------|-------------|
|-------|-----------|-------------|

| FIELD                          | DATA TYPE | DESCRIPTION                                                                                                 |
|--------------------------------|-----------|-------------------------------------------------------------------------------------------------------------|
| ResourceId                     | Text      | Resource identifier for data being collected. For example, Recovery Services vault resource ID              |
| OperationName                  | Text      | This field represents name of the current operation - Storage or StorageAssociation                         |
| Category                       | Text      | This field represents category of diagnostics data pushed to Azure Monitor logs - AddonAzureBackupStorage   |
| BackupItemUniqueId             | Text      | Unique ID used to identify the backup item for VMs backed up using DPM, MABS                                |
| BackupManagementServerUniqueId | Text      | Field to uniquely identify the Backup Management Server the Backup Item is protected through, if applicable |
| BackupManagementType           | Text      | Provider type for server doing backup job. For example, IaaSVM, FileFolder                                  |
| PreferredWorkloadOnVolume      | Text      | Workload for which this volume is the preferred storage                                                     |
| ProtectedContainerUniqueId     | Text      | Unique identifier of the protected server associated with the alert                                         |
| SchemaVersion                  | Text      | Version of the schema. For example, V2                                                                      |
| State                          | Text      | State of the backup item object. For example, Active, Deleted                                               |
| StorageAllocatedInMBs          | Number    | Size of storage allocated by the corresponding backup item in the corresponding storage of type Disk        |
| StorageConsumedInMBs           | Number    | Size of storage consumed by the corresponding backup item in the corresponding storage                      |
| StorageName                    | Text      | Name of storage entity. For example, E:\                                                                    |
| StorageTotalSizeInGBs          | Text      | Total size of storage, in GB, consumed by storage entity                                                    |
| StorageType                    | Text      | Type of Storage, for example Cloud, Volume, Disk                                                            |
| StorageUniqueId                | Text      | Unique ID used to identify the storage entity                                                               |

| FIELD              | DATA TYPE | DESCRIPTION                                                        |
|--------------------|-----------|--------------------------------------------------------------------|
| VaultUniqueId      | Text      | Unique ID used to identify the vault related to the storage entity |
| VolumeFriendlyName | Text      | Friendly name of the storage volume                                |
| SourceSystem       | Text      | Source system of the current data - Azure                          |

## Next steps

- [Learn how to send diagnostics data to Log Analytics](#)
- [Learn how to write queries on Resource specific tables](#)

# Log Analytics data model for Azure Backup data

2/24/2020 • 18 minutes to read • [Edit Online](#)

Use the Log Analytics data model to create custom alerts from Log Analytics.

## NOTE

This article was recently updated to use the term Azure Monitor logs instead of Log Analytics. Log data is still stored in a Log Analytics workspace and is still collected and analyzed by the same Log Analytics service. We are updating the terminology to better reflect the role of [logs in Azure Monitor](#). See [Azure Monitor terminology changes](#) for details.

## NOTE

This data model is in reference to the Azure Diagnostics Mode of sending diagnostic events to Log Analytics (LA). To learn the data model for the new Resource Specific Mode, you can refer to the following article: [Data Model for Azure Backup Diagnostic Events](#)

## Using Azure Backup data model

You can use the following fields provided as part of the data model to create visuals, custom queries, and dashboard as per your requirements.

### Alert

This table provides details about alert related fields.

| FIELD                         | DATA TYPE | DESCRIPTION                                                 |
|-------------------------------|-----------|-------------------------------------------------------------|
| AlertUniqueId_s               | Text      | Unique identifier of the generated alert                    |
| AlertType_s                   | Text      | Type of alert, for example, Backup                          |
| AlertStatus_s                 | Text      | Status of the alert, for example, Active                    |
| AlertOccurrenceDateTime_s     | Date/Time | Date and time when alert was created                        |
| AlertSeverity_s               | Text      | Severity of the alert, for example, Critical                |
| AlertTimeToResolveInMinutes_s | Number    | Time taken to resolve an alert. Blank for active alerts.    |
| AlertConsolidationStatus_s    | Text      | Identify if the alert is a consolidated alert or not        |
| CountOfAlertsConsolidated_s   | Number    | Number of alerts consolidated if it is a consolidated alert |
| AlertRaisedOn_s               | Text      | Type of entity the alert is raised on                       |
| AlertCode_s                   | Text      | Code to uniquely identify an alert type                     |

| FIELD                        | DATA TYPE | DESCRIPTION                                                                                                          |
|------------------------------|-----------|----------------------------------------------------------------------------------------------------------------------|
| RecommendedAction_s          | Text      | Action recommended to resolve the alert                                                                              |
| EventName_s                  | Text      | Name of the event. Always AzureBackupCentralReport                                                                   |
| BackupItemUniqueId_s         | Text      | Unique identifier of the backup item associated with the alert                                                       |
| SchemaVersion_s              | Text      | Current version of the schema, for example <b>V2</b>                                                                 |
| State_s                      | Text      | Current state of the alert object, for example, Active, Deleted                                                      |
| BackupManagementType_s       | Text      | Provider type for performing backup, for example, IaaSVM, FileFolder to which this alert belongs to                  |
| OperationName                | Text      | Name of the current operation, for example, Alert                                                                    |
| Category                     | Text      | Category of diagnostics data pushed to Azure Monitor logs. Always AzureBackupReport                                  |
| Resource                     | Text      | This is the resource for which data is being collected, it shows Recovery Services vault name                        |
| ProtectedContainerUniqueId_s | Text      | Unique identifier of the protected server associated with the alert (Was ProtectedServerUniqueId_s in V1)            |
| VaultUniqueId_s              | Text      | Unique identifier of the protected vault associated with the alert                                                   |
| SourceSystem                 | Text      | Source system of the current data - Azure                                                                            |
| ResourceId                   | Text      | Unique identifier for the resource about which data is collected. For example, a Recovery Services vault resource ID |
| SubscriptionId               | Text      | Subscription identifier of the resource (ex. Recovery Services vault) for which data is collected                    |
| ResourceGroup                | Text      | Resource group of the resource (ex. Recovery Services vault) for which data is collected                             |
| ResourceProvider             | Text      | Resource provider for which data is collected. For example, Microsoft.RecoveryServices                               |

| FIELD        | DATA TYPE | DESCRIPTION                                                    |
|--------------|-----------|----------------------------------------------------------------|
| ResourceType | Text      | Resource type for which data is collected. For example, Vaults |

## BackupItem

This table provides details about backup item-related fields.

| FIELD                            | DATA TYPE | DESCRIPTION                                                                                               |
|----------------------------------|-----------|-----------------------------------------------------------------------------------------------------------|
| EventName_s                      | Text      | Name of the event. Always AzureBackupCentralReport                                                        |
| BackupItemUniqueId_s             | Text      | Unique identifier of the backup item                                                                      |
| BackupItemId_s                   | Text      | Identifier of backup item (This field is only for v1 schema)                                              |
| BackupItemName_s                 | Text      | Name of backup item                                                                                       |
| BackupItemFriendlyName_s         | Text      | Friendly name of backup item                                                                              |
| BackupItemType_s                 | Text      | Type of backup item, for example, VM, FileFolder                                                          |
| BackupItemProtectionState_s      | Text      | Protection State of the Backup Item                                                                       |
| BackupItemAppVersion_s           | Text      | Application version of the backup item                                                                    |
| ProtectionState_s                | Text      | Current protection state of the backup item, for example, Protected, ProtectionStopped                    |
| ProtectionGroupName_s            | Text      | Name of the Protection Group the Backup Item is protected in, for SC DPM, and MABS, if applicable         |
| SecondaryBackupProtectionState_s | Text      | Whether secondary protection is enabled for the backup item                                               |
| SchemaVersion_s                  | Text      | Version of the schema, for example, <b>V2</b>                                                             |
| State_s                          | Text      | State of the backup item object, for example, Active, Deleted                                             |
| BackupManagementType_s           | Text      | Provider type for performing backup, for example, IaaSVM, FileFolder to which this backup item belongs to |
| OperationName                    | Text      | Name of the operation, for example, BackupItem                                                            |

| FIELD            | DATA TYPE | DESCRIPTION                                                                                        |
|------------------|-----------|----------------------------------------------------------------------------------------------------|
| Category         | Text      | Category of diagnostics data pushed to Azure Monitor logs. Always AzureBackupReport                |
| Resource         | Text      | Resource for which data is collected, for example, Recovery Services vault name                    |
| SourceSystem     | Text      | Source system of the current data - Azure                                                          |
| ResourceId       | Text      | Resource ID for data being collected, for example, Recovery Services vault resource ID             |
| SubscriptionId   | Text      | Subscription identifier of the resource (for ex. Recovery Services vault) for data being collected |
| ResourceGroup    | Text      | Resource group of the resource (for ex. Recovery Services vault) for data being collected          |
| ResourceProvider | Text      | Resource provider for data being collected, for example, Microsoft.RecoveryServices                |
| ResourceType     | Text      | Type of the resource for data being collected, for example, Vaults                                 |

## BackupItemAssociation

This table provides details about backup item associations with various entities.

| FIELD                            | DATA TYPE | DESCRIPTION                                                                                                 |
|----------------------------------|-----------|-------------------------------------------------------------------------------------------------------------|
| EventName_s                      | Text      | This field represents name of this event, it is always AzureBackupCentralReport                             |
| BackupItemUniqueld_s             | Text      | Unique ID of the backup item                                                                                |
| SchemaVersion_s                  | Text      | This field denotes current version of the schema, it is <b>V2</b>                                           |
| State_s                          | Text      | Current state of the backup item association object, for example, Active, Deleted                           |
| BackupManagementType_s           | Text      | Provider type for server doing backup job, for example, IaaSVM, FileFolder                                  |
| BackupItemSourceSize_s           | Text      | Front-end size of the backup item                                                                           |
| BackupManagementServerUniqueld_s | Text      | Field to uniquely identify the Backup Management Server the Backup Item is protected through, if applicable |

| FIELD                        | DATA TYPE | DESCRIPTION                                                                                                     |
|------------------------------|-----------|-----------------------------------------------------------------------------------------------------------------|
| Category                     | Text      | This field represents category of diagnostics data pushed to Log Analytics, it is AzureBackupReport             |
| OperationName                | Text      | This field represents name of the current operation - BackupItemAssociation                                     |
| Resource                     | Text      | This is the resource for which data is being collected, it shows Recovery Services vault name                   |
| ProtectedContainerUniqueId_s | Text      | Unique identifier of the protected server associated with the backup item (Was ProtectedServerUniqueId_s in V1) |
| VaultUniqueId_s              | Text      | Unique identifier of the vault containing the backup item                                                       |
| SourceSystem                 | Text      | Source system of the current data - Azure                                                                       |
| ResourceId                   | Text      | Resource identifier for data being collected. For example, Recovery Services vault resource ID                  |
| SubscriptionId               | Text      | Subscription identifier of the resource (for ex. Recovery Services vault) for which data is being collected     |
| ResourceGroup                | Text      | Resource group of the resource (for ex. Recovery Services vault) for which data is being collected              |
| ResourceProvider             | Text      | Resource provider for data being collected, for example, Microsoft.RecoveryServices                             |
| ResourceType                 | Text      | Type of the resource for data is being collected, for example, Vaults                                           |

## BackupManagementServer

This table provides details about backup item associations with various entities.

| FIELD                           | DATA TYPE | DESCRIPTION                                                       |
|---------------------------------|-----------|-------------------------------------------------------------------|
| BackupManagementServerName_s    | Text      | Name of the Backup Management Server                              |
| AzureBackupAgentVersion_s       | Text      | Version of the Azure Backup Agent on the Backup Management Server |
| BackupManagementServerVersion_s | Text      | Version of the Backup Management Server                           |

| FIELD                             | DATA TYPE | DESCRIPTION                                                                                                 |
|-----------------------------------|-----------|-------------------------------------------------------------------------------------------------------------|
| BackupManagementServerOSVersion_s | Text      | OS version of the Backup Management Server                                                                  |
| BackupManagementServerType_s      | Text      | Type of the Backup Management Server, as MABS, SC DPM                                                       |
| BackupManagementServerUniqueId_s  | Text      | Field to uniquely identify the Backup Management Server                                                     |
| SourceSystem                      | Text      | Source system of the current data - Azure                                                                   |
| ResourceId                        | Text      | Resource identifier for data being collected. For example, Recovery Services vault resource ID              |
| SubscriptionId                    | Text      | Subscription identifier of the resource (for ex. Recovery Services vault) for which data is being collected |
| ResourceGroup                     | Text      | Resource group of the resource (for ex. Recovery Services vault) for which data is being collected          |
| ResourceProvider                  | Text      | Resource provider for data being collected, for example, Microsoft.RecoveryServices                         |
| ResourceType                      | Text      | Type of the resource for data is being collected, for example, Vaults                                       |

## Job

This table provides details about job-related fields.

| FIELD                  | DATA TYPE | DESCRIPTION                                                                |
|------------------------|-----------|----------------------------------------------------------------------------|
| EventName_s            | Text      | Name of the event. Always AzureBackupCentralReport                         |
| BackupItemUniqueId_s   | Text      | Unique identifier of the backup item                                       |
| SchemaVersion_s        | Text      | Version of the schema, for example, V2                                     |
| State_s                | Text      | Current state of the job object, for example, Active, Deleted              |
| BackupManagementType_s | Text      | Provider type for server doing backup job, for example, IaaSVM, FileFolder |
| OperationName          | Text      | This field represents name of the current operation - Job                  |

| FIELD                        | DATA TYPE | DESCRIPTION                                                                                              |
|------------------------------|-----------|----------------------------------------------------------------------------------------------------------|
| Category                     | Text      | This field represents category of diagnostics data pushed to Azure Monitor logs, it is AzureBackupReport |
| Resource                     | Text      | This is the resource for which data is being collected, it shows Recovery Services vault name            |
| ProtectedServerUniqueld_s    | Text      | Unique identifier of the protected server associated the job                                             |
| ProtectedContainerUniqueld_s | Text      | Unique ID to identify the protected container the job is run on                                          |
| VaultUniqueld_s              | Text      | Unique identifier of the protected vault                                                                 |
| JobOperation_s               | Text      | Operation for which job is run for example, Backup, Restore, Configure Backup                            |
| JobStatus_s                  | Text      | Status of the finished job, for example, Completed, Failed                                               |
| JobFailureCode_s             | Text      | Failure Code string because of which job failure happened                                                |
| JobStartTimeDateTime_s       | Date/Time | Date and time when job started running                                                                   |
| BackupStorageDestination_s   | Text      | Destination of backup storage, for example, Cloud, Disk                                                  |
| AdHocOrScheduledJob_s        | Text      | Field to specify if the job is Ad Hoc or Scheduled                                                       |
| JobDurationInSecs_s          | Number    | Total job duration in seconds                                                                            |
| DataTransferredInMB_s        | Number    | Data transferred in MB for this job                                                                      |
| JobUniqueld_g                | Text      | Unique ID to identify the job                                                                            |
| RecoveryJobDestination_s     | Text      | Destination of a recovery job, where the data is recovered                                               |
| RecoveryJobRPDateTime_s      | DateTime  | The date, Time when the recovery point that is being recovered was created                               |
| RecoveryJobRPLocation_s      | Text      | The location where the recovery point that is being recovered was stored                                 |
| SourceSystem                 | Text      | Source system of the current data - Azure                                                                |

| FIELD            | DATA TYPE | DESCRIPTION                                                                                       |
|------------------|-----------|---------------------------------------------------------------------------------------------------|
| ResourceId       | Text      | Resource identifier for data being collected. For example, Recovery Services vault resource ID    |
| SubscriptionId   | Text      | Subscription identifier of the resource (ex. Recovery Services vault) for which data is collected |
| ResourceGroup    | Text      | Resource group of the resource (ex. Recovery Services vault) for which data is collected          |
| ResourceProvider | Text      | Resource provider for which data is collected. For example, Microsoft.RecoveryServices            |
| ResourceType     | Text      | Resource type for which data is collected. For example, Vaults                                    |

## Policy

This table provides details about policy-related fields.

| FIELD                  | DATA TYPE | VERSIONS APPLICABLE | DESCRIPTION                                                                                              |
|------------------------|-----------|---------------------|----------------------------------------------------------------------------------------------------------|
| EventName_s            | Text      |                     | This field represents name of this event, it is always AzureBackupCentralReport                          |
| SchemaVersion_s        | Text      |                     | This field denotes current version of the schema, it is <b>V2</b>                                        |
| State_s                | Text      |                     | Current state of the policy object, for example, Active, Deleted                                         |
| BackupManagementType_s | Text      |                     | Provider type for server doing backup job, for example, IaaSVM, FileFolder                               |
| OperationName          | Text      |                     | This field represents name of the current operation - Policy                                             |
| Category               | Text      |                     | This field represents category of diagnostics data pushed to Azure Monitor logs, it is AzureBackupReport |

| FIELD                          | DATA TYPE      | VERSIONS APPLICABLE | DESCRIPTION                                                                                   |
|--------------------------------|----------------|---------------------|-----------------------------------------------------------------------------------------------|
| Resource                       | Text           |                     | This is the resource for which data is being collected, it shows Recovery Services vault name |
| PolicyUniqueld_g               | Text           |                     | Unique ID to identify the policy                                                              |
| PolicyName_s                   | Text           |                     | Name of the policy defined                                                                    |
| BackupFrequency_s              | Text           |                     | Frequency with which backups are run, for example, daily, weekly                              |
| BackupTimes_s                  | Text           |                     | Date and time when backups are scheduled                                                      |
| BackupDaysOfTheWeek_s          | Text           |                     | Days of the week when backups have been scheduled                                             |
| RetentionDuration_s            | Whole Number   |                     | Retention duration for configured backups                                                     |
| DailyRetentionDuration_s       | Whole Number   |                     | Total retention duration in days for configured backups                                       |
| DailyRetentionTimes_s          | Text           |                     | Date and time when daily retention was configured                                             |
| WeeklyRetentionDuration_s      | Decimal Number |                     | Total weekly retention duration in weeks for configured backups                               |
| WeeklyRetentionTime_s_s        | Text           |                     | Date and time when weekly retention is configured                                             |
| WeeklyRetentionDaysOfTheWeek_s | Text           |                     | Days of the week selected for weekly retention                                                |
| MonthlyRetentionDuration_s     | Decimal Number |                     | Total retention duration in months for configured backups                                     |
| MonthlyRetentionTimes_s        | Text           |                     | Date and time when monthly retention is configured                                            |

| FIELD                             | DATA TYPE      | VERSIONS APPLICABLE | DESCRIPTION                                                                                          |
|-----------------------------------|----------------|---------------------|------------------------------------------------------------------------------------------------------|
| MonthlyRetentionFormat_s          | Text           |                     | Type of configuration for monthly retention, for example, daily for day based, weekly for week based |
| MonthlyRetentionDaysOfTheWeek_s   | Text           |                     | Days of the week selected for monthly retention                                                      |
| MonthlyRetentionWeeksOfTheMonth_s | Text           |                     | Weeks of the month when monthly retention is configured, for example, First, Last etc.               |
| YearlyRetentionDuration_s         | Decimal Number |                     | Total retention duration in years for configured backups                                             |
| YearlyRetentionTimes_s            | Text           |                     | Date and time when yearly retention is configured                                                    |
| YearlyRetentionMonthsOfTheYear_s  | Text           |                     | Months of the year selected for yearly retention                                                     |
| YearlyRetentionFormat_s           | Text           |                     | Type of configuration for yearly retention, for example, daily for day based, weekly for week based  |
| YearlyRetentionDaysOfTheMonth_s   | Text           |                     | Dates of the month selected for yearly retention                                                     |
| SynchronisationFrequencyPerDay_s  | Whole Number   | v2                  | Number of times in a day a file backup is synchronized for SC DPM and MABS                           |
| DiffBackupFormat_s                | Text           | v2                  | Format for Differential backups for SQL in Azure VM backup                                           |
| DiffBackupTime_s                  | Time           | v2                  | Time for Differential backups for SQL in Azure VM Backup                                             |
| DiffBackupRetentionDuration_s     | Decimal Number | v2                  | Retention duration for Differential backups for SQL in Azure VM Backup                               |

| FIELD                        | DATA TYPE      | VERSIONS APPLICABLE | DESCRIPTION                                                                                       |
|------------------------------|----------------|---------------------|---------------------------------------------------------------------------------------------------|
| LogBackupFrequency_s         | Decimal Number | v2                  | Frequency for Log backups for SQL                                                                 |
| LogBackupRetentionDuration_s | Decimal Number | v2                  | Retention duration for Log backups for SQL in Azure VM Backup                                     |
| DiffBackupDaysofTheWeek_s    | Text           | v2                  | Days of the week for Differential backups for SQL in Azure VM Backup                              |
| SourceSystem                 | Text           |                     | Source system of the current data - Azure                                                         |
| ResourceId                   | Text           |                     | Resource identifier for data being collected. For example, Recovery Services vault resource ID    |
| SubscriptionId               | Text           |                     | Subscription identifier of the resource (ex. Recovery Services vault) for which data is collected |
| ResourceGroup                | Text           |                     | Resource group of the resource (ex. Recovery Services vault) for which data is collected          |
| ResourceProvider             | Text           |                     | Resource provider for which data is collected. For example, Microsoft.RecoveryServices            |
| ResourceType                 | Text           |                     | Resource type for which data is collected. For example, Vaults                                    |

### PolicyAssociation

This table provides details about policy associations with various entities.

| FIELD           | DATA TYPE | VERSIONS APPLICABLE | DESCRIPTION                                                                     |
|-----------------|-----------|---------------------|---------------------------------------------------------------------------------|
| EventName_s     | Text      |                     | This field represents name of this event, it is always AzureBackupCentralReport |
| SchemaVersion_s | Text      |                     | This field denotes current version of the schema, it is V2                      |

| FIELD                                | DATA TYPE | VERSIONS APPLICABLE | DESCRIPTION                                                                                                 |
|--------------------------------------|-----------|---------------------|-------------------------------------------------------------------------------------------------------------|
| State_s                              | Text      |                     | Current state of the policy object, for example, Active, Deleted                                            |
| BackupManagementType_s               | Text      |                     | Provider type for server doing backup job, for example, IaaSVM, FileFolder                                  |
| OperationName                        | Text      |                     | This field represents name of the current operation - PolicyAssociation                                     |
| Category                             | Text      |                     | This field represents category of diagnostics data pushed to Azure Monitor logs, it is AzureBackupReport    |
| Resource                             | Text      |                     | This is the resource for which data is being collected, it shows Recovery Services vault name               |
| PolicyUniqueId_g                     | Text      |                     | Unique ID to identify the policy                                                                            |
| VaultUniqueId_s                      | Text      |                     | Unique ID of the vault to which this policy belongs to                                                      |
| BackupManagementServerU<br>niqueId_s | Text      | v2                  | Field to uniquely identify the Backup Management Server the Backup Item is protected through, if applicable |
| SourceSystem                         | Text      |                     | Source system of the current data - Azure                                                                   |
| ResourceId                           | Text      |                     | Resource identifier for data being collected. For example, Recovery Services vault resource ID              |
| SubscriptionId                       | Text      |                     | Subscription identifier of the resource (ex. Recovery Services vault) for which data is collected           |
| ResourceGroup                        | Text      |                     | Resource group of the resource (ex. Recovery Services vault) for which data is collected                    |
| ResourceProvider                     | Text      |                     | Resource provider for which data is collected. For example, Microsoft.RecoveryServices                      |

| FIELD        | DATA TYPE | VERSIONS APPLICABLE | DESCRIPTION                                                    |
|--------------|-----------|---------------------|----------------------------------------------------------------|
| ResourceType | Text      |                     | Resource type for which data is collected. For example, Vaults |

## Protected Container

This table provides basic fields about Protected Containers. (Was ProtectedServer in v1)

| FIELD                                | DATA TYPE | DESCRIPTION                                                                         |
|--------------------------------------|-----------|-------------------------------------------------------------------------------------|
| ProtectedContainerUniqueId_s         | Text      | Field to uniquely identify a Protected Container                                    |
| ProtectedContainerOSType_s           | Text      | OS Type of the Protected Container                                                  |
| ProtectedContainerOSVersion_s        | Text      | OS Version of the Protected Container                                               |
| AgentVersion_s                       | Text      | Version number of Agent Backup or the Protection Agent (In case of SC DPM and MABS) |
| BackupManagementType_s               | Text      | Provider type for performing backup. For example, IaaSVM, FileFolder                |
| EntityState_s                        | Text      | Current state of the protected server object. For example, Active, Deleted          |
| ProtectedContainerFriendlyName_s     | Text      | Friendly name of protected server                                                   |
| ProtectedContainerName_s             | Text      | Name of the Protected Container                                                     |
| ProtectedContainerWorkloadType_s     | Text      | Type of the Protected Container backed up. For example, IaaSVMContainer             |
| ProtectedContainerLocation_s         | Text      | Whether the Protected Container is located On-premises or in Azure                  |
| ProtectedContainerType_s             | Text      | Whether the Protected Container is a server, or a container                         |
| ProtectedContainerProtectionState_s' | Text      | Protection State of the Protected Container                                         |

## Storage

This table provides details about storage-related fields.

| FIELD                 | DATA TYPE      | DESCRIPTION                                                                                               |
|-----------------------|----------------|-----------------------------------------------------------------------------------------------------------|
| CloudStorageInBytes_s | Decimal Number | Cloud backup storage used by backups, calculated based on latest value (This field is only for v1 schema) |

| FIELD                     | DATA TYPE      | DESCRIPTION                                                                                                      |
|---------------------------|----------------|------------------------------------------------------------------------------------------------------------------|
| ProtectedInstances_s      | Decimal Number | Number of protected instances used for calculating frontend storage in billing, calculated based on latest value |
| EventName_s               | Text           | This field represents name of this event, it is always AzureBackupCentralReport                                  |
| SchemaVersion_s           | Text           | This field denotes current version of the schema, it is <b>V2</b>                                                |
| State_s                   | Text           | Current state of the storage object, for example, Active, Deleted                                                |
| BackupManagementType_s    | Text           | Provider type for server doing backup job, for example, IaaSVM, FileFolder                                       |
| OperationName             | Text           | This field represents name of the current operation - Storage                                                    |
| Category                  | Text           | This field represents category of diagnostics data pushed to Azure Monitor logs, it is AzureBackupReport         |
| Resource                  | Text           | This is the resource for which data is being collected, it shows Recovery Services vault name                    |
| ProtectedServerUniqueId_s | Text           | Unique ID of the protected server for which storage is calculated                                                |
| VaultUniqueId_s           | Text           | Unique ID of the vault for storage is calculated                                                                 |
| SourceSystem              | Text           | Source system of the current data - Azure                                                                        |
| ResourceId                | Text           | Resource identifier for data being collected. For example, Recovery Services vault resource ID                   |
| SubscriptionId            | Text           | Subscription identifier of the resource (ex. Recovery Services vault) for which data is collected                |
| ResourceGroup             | Text           | Resource group of the resource (ex. Recovery Services vault) for which data is collected                         |
| ResourceProvider          | Text           | Resource provider for which data is collected. For example, Microsoft.RecoveryServices                           |
| ResourceType              | Text           | Resource type for which data is collected. For example, Vaults                                                   |

| FIELD                   | DATA TYPE | DESCRIPTION                                              |
|-------------------------|-----------|----------------------------------------------------------|
| StorageUniqueId_s       | Text      | Unique ID used to identify the storage entity            |
| StorageType_s           | Text      | Type of Storage, for example Cloud, Volume, Disk         |
| StorageName_s           | Text      | Name of storage entity, for example E:\                  |
| StorageTotalSizeInGBs_s | Text      | Total size of storage, in GB, consumed by storage entity |

## StorageAssociation

This table provides basic storage-related fields connecting storage to other entities.

| FIELD                            | DATA TYPE | DESCRIPTION                                                                                          |
|----------------------------------|-----------|------------------------------------------------------------------------------------------------------|
| StorageUniqueId_s                | Text      | Unique ID used to identify the storage entity                                                        |
| SchemaVersion_s                  | Text      | This field denotes current version of the schema, it is <b>V2</b>                                    |
| BackupItemUniqueId_s             | Text      | Unique ID used to identify the backup item related to the storage entity                             |
| BackupManagementServerUniqueId_s | Text      | Unique ID used to identify the backup management server related to the storage entity                |
| VaultUniqueId_s                  | Text      | Unique ID used to identify the vault related to the storage entity                                   |
| StorageConsumedInMBs_s           | Number    | Size of storage consumed by the corresponding backup item in the corresponding storage               |
| StorageAllocatedInMBs_s          | Number    | Size of storage allocated by the corresponding backup item in the corresponding storage of type Disk |

## Vault

This table provides details about vault-related fields.

| FIELD           | DATA TYPE | DESCRIPTION                                                                     |
|-----------------|-----------|---------------------------------------------------------------------------------|
| EventName_s     | Text      | This field represents name of this event, it is always AzureBackupCentralReport |
| SchemaVersion_s | Text      | This field denotes current version of the schema, it is <b>V2</b>               |
| State_s         | Text      | Current state of the vault object, for example, Active, Deleted                 |

| FIELD                    | DATA TYPE | DESCRIPTION                                                                                              |
|--------------------------|-----------|----------------------------------------------------------------------------------------------------------|
| OperationName            | Text      | This field represents name of the current operation - Vault                                              |
| Category                 | Text      | This field represents category of diagnostics data pushed to Azure Monitor logs, it is AzureBackupReport |
| Resource                 | Text      | This is the resource for which data is being collected, it shows Recovery Services vault name            |
| VaultUniqueld_s          | Text      | Unique ID of the vault                                                                                   |
| VaultName_s              | Text      | Name of the vault                                                                                        |
| AzureDataCenter_s        | Text      | Data center where vault is located                                                                       |
| StorageReplicationType_s | Text      | Type of storage replication for the vault, for example, GeoRedundant                                     |
| SourceSystem             | Text      | Source system of the current data - Azure                                                                |
| Resourceld               | Text      | Resource identifier for data being collected. For example, Recovery Services vault resource ID           |
| SubscriptionId           | Text      | Subscription identifier of the resource (ex. Recovery Services vault) for which data is collected        |
| ResourceGroup            | Text      | Resource group of the resource (ex. Recovery Services vault) for which data is collected                 |
| ResourceProvider         | Text      | Resource provider for which data is collected. For example, Microsoft.RecoveryServices                   |
| ResourceType             | Text      | Resource type for which data is collected. For example, Vaults                                           |

## Backup Management Server

This table provides basic fields about Backup Management Servers.

| FIELD                        | DATA TYPE | DESCRIPTION                                                       |
|------------------------------|-----------|-------------------------------------------------------------------|
| BackupManagementServerName_s | Text      | Name of the Backup Management Server                              |
| AzureBackupAgentVersion_s    | Text      | Version of the Azure Backup Agent on the Backup Management Server |

| FIELD                             | DATA TYPE | DESCRIPTION                                             |
|-----------------------------------|-----------|---------------------------------------------------------|
| BackupManagementServerVersion_s   | Text      | Version of the Backup Management Server                 |
| BackupManagementServerOSVersion_s | Text      | OS version of the Backup Management Server              |
| BackupManagementServerType_s      | Text      | Type of the Backup Management Server, as MABS, SC DPM   |
| BackupManagementServerUniqueId_s  | Text      | Field to uniquely identify the Backup Management Server |

### PreferredWorkloadOnVolume

This table specifies the workload(s) a Volume is associated with.

| FIELD             | DATA TYPE | DESCRIPTION                                                  |
|-------------------|-----------|--------------------------------------------------------------|
| StorageUniqueId_s | Text      | Unique ID used to identify the storage entity                |
| BackupItemType_s  | Text      | The workloads for which this volume is the preferred storage |

### ProtectedInstance

This table provides basic protected instances-related fields.

| FIELD                        | DATA TYPE | VERSIONS APPLICABLE | DESCRIPTION                                                                                            |
|------------------------------|-----------|---------------------|--------------------------------------------------------------------------------------------------------|
| BackupItemUniqueId_s         | Text      | v2                  | Unique ID used to identify the backup item for VMs backed up using DPM, MABS                           |
| ProtectedContainerUniqueId_s | Text      | v2                  | Unique ID used to identify the protected container for everything except VMs backed up using DPM, MABS |
| ProtectedInstanceCount_s     | Text      | v2                  | Count of Protected Instances for the associated backup item or protected container on that date-time   |

### RecoveryPoint

This table provides basic recovery point related fields.

| FIELD                | DATA TYPE | DESCRIPTION                                                                  |
|----------------------|-----------|------------------------------------------------------------------------------|
| BackupItemUniqueId_s | Text      | Unique ID used to identify the backup item for VMs backed up using DPM, MABS |

| FIELD                         | DATA TYPE | DESCRIPTION                                                |
|-------------------------------|-----------|------------------------------------------------------------|
| OldestRecoveryPointTime_s     | Text      | Date time of the oldest recovery point for the backup item |
| OldestRecoveryPointLocation_s | Text      | Location of the oldest recovery point for the backup item  |
| LatestRecoveryPointTime_s     | Text      | Date time of the latest recovery point for the backup item |
| LatestRecoveryPointLocation_s | Text      | Location of the latest recovery point for the backup item  |

## Sample Kusto Queries

Below are a few samples to help you write queries on Azure Backup data that resides in the Azure Diagnostics table:

- All successful backup jobs

```
AzureDiagnostics
| where Category == "AzureBackupReport"
| where SchemaVersion_s == "V2"
| where OperationName == "Job" and JobOperation_s == "Backup"
| where JobStatus_s == "Completed"
```

- All failed backup jobs

```
AzureDiagnostics
| where Category == "AzureBackupReport"
| where SchemaVersion_s == "V2"
| where OperationName == "Job" and JobOperation_s == "Backup"
| where JobStatus_s == "Failed"
```

- All successful Azure VM backup jobs

```
AzureDiagnostics
| where Category == "AzureBackupReport"
| where SchemaVersion_s == "V2"
| extend JobOperationSubType_s = columnifexists("JobOperationSubType_s", "")
| where OperationName == "Job" and JobOperation_s == "Backup" and JobStatus_s == "Completed" and
JobOperationSubType_s != "Log" and JobOperationSubType_s != "Recovery point_Log"
| join kind=inner
(
 AzureDiagnostics
 | where Category == "AzureBackupReport"
 | where OperationName == "BackupItem"
 | where SchemaVersion_s == "V2"
 | where BackupItemType_s == "VM" and BackupManagementType_s == "IaaSVM"
 | distinct BackupItemUniqueId_s, BackupItemFriendlyName_s
 | project BackupItemUniqueId_s , BackupItemFriendlyName_s
)
on BackupItemUniqueId_s
| extend Vault= Resource
| project-away Resource
```

- All successful SQL log backup jobs

```

AzureDiagnostics
| where Category == "AzureBackupReport"
| where SchemaVersion_s == "V2"
| extend JobOperationSubType_s = columnifexists("JobOperationSubType_s", "")
| where OperationName == "Job" and JobOperation_s == "Backup" and JobStatus_s == "Completed" and
JobOperationSubType_s == "Log"
| join kind=inner
(
 AzureDiagnostics
 | where Category == "AzureBackupReport"
 | where OperationName == "BackupItem"
 | where SchemaVersion_s == "V2"
 | where BackupItemType_s == "SQLDataBase" and BackupManagementType_s == "AzureWorkload"
 | distinct BackupItemUniqueId_s, BackupItemFriendlyName_s
 | project BackupItemUniqueId_s , BackupItemFriendlyName_s
)
on BackupItemUniqueId_s
| extend Vault= Resource
| project-away Resource

```

- All successful Azure Backup agent jobs

```

AzureDiagnostics
| where Category == "AzureBackupReport"
| where SchemaVersion_s == "V2"
| extend JobOperationSubType_s = columnifexists("JobOperationSubType_s", "")
| where OperationName == "Job" and JobOperation_s == "Backup" and JobStatus_s == "Completed" and
JobOperationSubType_s != "Log" and JobOperationSubType_s != "Recovery point_Log"
| join kind=inner
(
 AzureDiagnostics
 | where Category == "AzureBackupReport"
 | where OperationName == "BackupItem"
 | where SchemaVersion_s == "V2"
 | where BackupItemType_s == "FileFolder" and BackupManagementType_s == "MAB"
 | distinct BackupItemUniqueId_s, BackupItemFriendlyName_s
 | project BackupItemUniqueId_s , BackupItemFriendlyName_s
)
on BackupItemUniqueId_s
| extend Vault= Resource
| project-away Resource

```

## Next steps

Once you review the data model, you can start [creating custom queries](#) in Azure Monitor logs to build your own dashboard.

# Auto-Enable Backup on VM Creation using Azure Policy

2/24/2020 • 2 minutes to read • [Edit Online](#)

One of the key responsibilities of a Backup or Compliance Admin in an organization is to ensure that all business-critical machines are backed up with the appropriate retention.

Today, Azure Backup provides a built-in policy (using Azure Policy) that can be assigned to **all Azure VMs in a specified location within a subscription or resource group**. When this policy is assigned to a given scope, all new VMs created in that scope are automatically configured for backup to an **existing vault in the same location and subscription**. The user can specify the vault and the retention policy to which the backed up VMs should be associated.

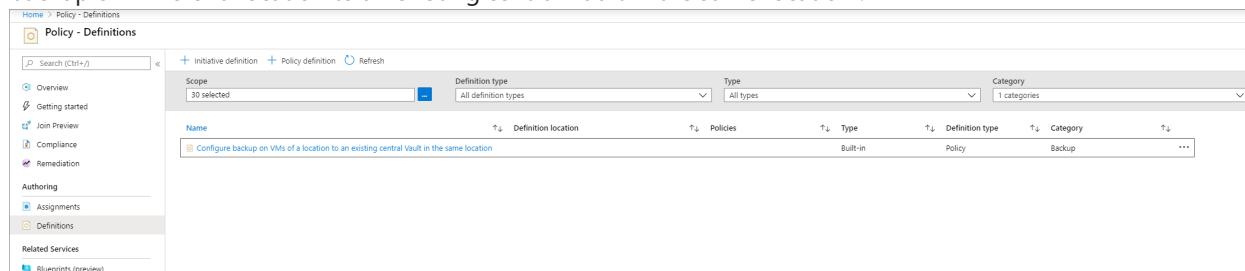
## Supported Scenarios

- The built-in policy is currently supported only for Azure VMs. Users must take care to ensure that the retention policy specified during assignment is a VM retention policy. Refer to [this document](#) to see all the VM SKUs supported by this policy.
- The policy can be assigned to a single location and subscription at a time. To enable backup for VMs across locations and subscriptions, multiple instances of the policy assignment need to be created, one for each combination of location and subscription.
- The specified vault and the VMs configured for backup can be under different resource groups.
- Management Group scope is currently unsupported.
- The built-in policy is currently not available in national clouds.

## Using the built-in policy

To assign the policy to the required scope, please follow the below steps:

1. Sign in to the Azure Portal and navigate to the **Policy** Dashboard.
2. Select **Definitions** in the left menu to get a list of all built-in policies across Azure Resources.
3. Filter the list for **Category=Backup**. You will see the list filtered down to a single policy named 'Configure backup on VMs of a location to an existing central Vault in the same location'.



The screenshot shows the Azure Policy Definitions blade. The left sidebar has 'Definitions' selected. The main area shows a table with one row. The row contains a link titled 'Configure backup on VMs of a location to an existing central Vault in the same location'. The table columns are: Name, Definition location, Policies, Type, Definition type, Category, and ... (ellipsis). The 'Category' column shows 'Backup'.

4. Click on the name of the policy. You will be redirected to the detailed definition for this policy.

Home > Policy > Definitions > Configure backup on VMs of a location to an existing central Vault in the same location

Policy definition

Name : Configure backup on VMs of a location to an existing central Vault in the same location

Description : This policy configures Azure Backup protection on VMs in a given location to an existing central vault in the same location. It applies to only those VMs that are not already configured for back...

Available Effects : `deployIfNotExists`, `authIfNotExists`, `enabled`

Category : Backup

Definition location : `providers/Microsoft.Authorization/policyDefinitions/09eae6bc-1220-4151-8104-e9f51c936913`

Definition ID : `09eae6bc-1220-4151-8104-e9f51c936913`

Type : Built-in

Mode : Indeed

A

Definition Assignments (1) Parameters

```
1 {
2 "properties": {
3 "displayName": "Configure backup on VMs of a location to an existing central Vault in the same location",
4 "policyType": "BuiltIn",
5 "mode": "Indeed",
6 "description": "This policy configures Azure Backup protection on VMs in a given location to an existing central vault in the same location. It applies to only those VMs that are not already configured for backup. It is recommended that this policy is assigned to not more than 200 VMs.",
7 "metadata": {
8 "category": "Backup"
9 },
10 "parameters": {
11 "vaultLocation": {
12 "type": "String",
13 "metadata": {
14 "displayName": "location (Specify the location of the VMs that you want to protect)",
15 "description": "Specify the location of the VMs that you want to protect. VMs should be backed up to a vault in the same location.\nFor example - southeastasia",
16 "strength": "Microsoft.RecoveryServicesVaults/backupPolicySet",
17 },
18 },
19 "backupPolicyId": {
20 "type": "String",
21 "metadata": {
22 "displayName": "Backup Policy (of type Azure VM from a vault in the location chosen above)",
23 "description": "Specify the id of the Azure backup policy to configure backup of the virtual machines. The selected Azure backup policy should be of type Azure virtual machine. This policy needs to be in a vault that is present in the location chosen above.\nFor example - /subscriptions/{SubscriptionId}/re
24 "strength": "Microsoft.RecoveryServicesVaults/backupPolicySet",
25 },
26 },
27 },
28 "effect": {
29 "type": "String",
30 "metadata": {
31 "displayName": "Effect",
32 "description": "Enable or disable the execution of the policy",
33 },
34 "allowedValues": [
35 "deployIfNotExists",
36 "authIfNotExists",
37 "disabled"
38],
39 "defaultValue": "deployIfNotExists"
40 }
41 }
42}
```

5. Click on the **Assign** button at the top of the blade. This redirects you to the **Assign Policy** blade.
  6. Under **Basics**, click on the three dots next to the **Scope** field. This opens up a right context blade where you can select the subscription for the policy to be applied on. You can also optionally select a resource group, so that the policy is applied only for VMs in a particular resource group.

Home > Policy - Definitions > Configure backup on VMs of a location to an existing central Vault in the same location > Configure backup on VMs of a location to an existing central Vault in the same location

Assign policy

Configure backup on VMs of a location to an existing central Vault in the same location

Basics Parameters Remediation Review + create

**Scope**

Scope (Learn more about setting the scope) \*

**Exclusions**

Optionally select resources to exempt from the policy assignment

**Basics**

Policy definition

Configure backup on VMs of a location to an existing central Vault in the same location

Assignment name \* ⓘ

Configure backup on VMs of a location to an existing central Vault in the same location

Description

7. In the **Parameters** tab, choose a location from the drop-down, and select the vault and backup policy to which the VMs in the scope must be associated.

Home > Policy - Definitions > Configure backup on VMs of a location to an existing central Vault in the same location > Configure backup on VMs of a location to an existing central Vault in the same location

## Configure backup on VMs of a location to an existing central Vault in the same location

Assign policy

---

[Basics](#) [Parameters](#) [Remediation](#) [Review + create](#)

Specify parameters for this policy assignment.

Location (Specify the location of the VMs that you want to protect) \* ⓘ

Backup Policy (of type Azure VM from a vault in the location chosen above) \* ⓘ

Effect \* ⓘ

deployIfNotExists

8. Ensure that **Effect** is set to `deployIfNotExists`.
  9. Navigate to **Review+create** and click **Create**.

## NOTE

Azure Policy can also be used on existing VMs, using [remediation](#).

**NOTE**

It is recommended that this policy is not assigned to more than 200 VMs at a time. If the policy is assigned to more than 200 VMs, it can result in the backup getting triggered a few hours later than that specified by the schedule.

## Next Steps

[Learn more about Azure Policy](#)

# Configure Vault Diagnostics settings at scale

2/24/2020 • 4 minutes to read • [Edit Online](#)

The reporting solution provided by Azure Backup leverages Log Analytics (LA). For the data of any given vault to be sent to LA, a [diagnostics setting](#) needs to be created for that vault.

Often, adding a diagnostics setting manually per vault can be a cumbersome task. In addition, any new vault created also needs to have diagnostics settings enabled in order to be able to view reports for this vault.

To simplify the creation of diagnostics settings at scale (with LA as the destination), Azure Backup provides a built-in [Azure Policy](#). This policy adds an LA diagnostics setting to all vaults in a given subscription or resource group. The following sections provide instructions on how to use this policy.

## Supported Scenarios

- The policy can be applied at one time to all Recovery Services vaults in a particular subscription (or to a resource group within the subscription). The user assigning the policy needs to have 'Owner' access to the subscription to which the policy is assigned.
- The LA Workspace as specified by the user (to which diagnostics data will be sent to) can be in a different subscription from the vaults to which the policy is assigned. The user needs to have 'Reader', 'Contributor' or 'Owner' access to the subscription in which the specified LA Workspace exists.
- Management Group scope is currently unsupported.
- The built-in policy is currently not available in national clouds.

## Assigning the built-in policy to a scope

To assign the policy for vaults in the required scope, follow the steps below:

1. Sign in to the Azure portal and navigate to the **Policy** Dashboard.
2. Select **Definitions** in the left menu to get a list of all built-in policies across Azure Resources.
3. Filter the list for **Category=Monitoring**. Locate the policy named **[Preview]: Deploy Diagnostic Settings for Recovery Services Vault to Log Analytics workspace for resource specific categories**.

The screenshot shows the Azure Policy - Definitions dashboard. On the left, there's a navigation menu with links like Overview, Getting started, Join Preview, Compliance, Remediation, Authoring (Assignments and Definitions), and Definitions (which is selected). The main area has a search bar and filter buttons for Initiative definition, Policy definition, and Refresh. Below that are four filter dropdowns: Scope (29 selected), Definition type (All definition types), Type (All types), and Category (1 categories). A table lists policies, with the third row being the target policy: "[Preview]: Deploy Diagnostic Settings for Recovery Services Vault to Log Analytics workspace for resource specific categories".

4. Click on the name of the policy. You will be redirected to the detailed definition for this policy.

[Preview]: Deploy Diagnostic Settings for Recovery Services Vault to Log Analytics workspace for resource specific categories.

Policy definition

| Actions |                      |
|---------|----------------------|
|         | Assign               |
|         | Edit definition      |
|         | Duplicate definition |
|         | Delete definition    |

Name : [Preview]: Deploy Diagnostic Settings for Recovery Services Vault to Log Analytics workspace for resource specific categories.

Description : Deploy Diagnostic Settings for Recovery Services Vault to stream to Log Analytics workspace for resource specific categories.

Available Effects : DeployIfNotExists

Category : Monitoring

Definition location : --

Definition ID : /providers/Microsoft.Authorization/policyDefinitions/12345678-1234-1234-1234-1234567890ab

Type : Built-in

Mode : Indexed

Definition

Assignments (3)

Parameters

```

1 {
2 "properties": {
3 "displayName": "[Preview]: Deploy Diagnostic Settings for Recovery Services Vault to Log Analytics workspace for resource specific categories",
4 "policyType": "BuiltIn",
5 "mode": "Indexed",
6 "description": "Deploy Diagnostic Settings for Recovery Services Vault to stream to Log Analytics workspace for Resource Specific Categories",
7 "metadata": {
8 "version": "1.0.0-preview",
9 "preview": true,
10 "category": "Monitoring"
11 }
12 }
13}

```

- Click on the **Assign** button at the top of the blade. This redirects you to the **Assign Policy** blade.
- Under **Basics**, click on the three dots next to the **Scope** field. This opens up a right context blade where you can select the subscription for the policy to be applied on. You can also optionally select a resource group, so that the policy is applied only for vaults in a particular resource group.

[Preview]: Deploy Diagnostic Settings for Recovery Services Vault to Log Analytics workspace for resource specific categories.

Assign policy

| Basics                                                                                                                         | Parameters | Remediation | Review + create |
|--------------------------------------------------------------------------------------------------------------------------------|------------|-------------|-----------------|
| <b>Scope</b>                                                                                                                   |            |             |                 |
| Scope <a href="#">Learn more about setting the scope *</a>                                                                     |            |             |                 |
|                                                                                                                                |            |             |                 |
| <b>Exclusions</b>                                                                                                              |            |             |                 |
| Optionally select resources to exempt from the policy assignment                                                               |            |             |                 |
| <b>Basics</b>                                                                                                                  |            |             |                 |
| <b>Policy definition</b>                                                                                                       |            |             |                 |
| [Preview]: Deploy Diagnostic Settings for Recovery Services Vault to Log Analytics workspace for resource specific categories. |            |             |                 |
| <b>Assignment name *</b>                                                                                                       |            |             |                 |
| [Preview]: Deploy Diagnostic Settings for Recovery Services Vault to Log Analytics workspace for resource specific categories. |            |             |                 |
| <b>Description</b>                                                                                                             |            |             |                 |

- Under **Parameters**, enter the following information:
  - Profile Name** - The name that will be assigned to the diagnostics settings created by the policy.
  - Log Analytics Workspace** - The Log Analytics Workspace to which the diagnostics setting should be associated. Diagnostics data of all vaults in the scope of the Policy assignment will be pushed to the specified LA Workspace.
  - Exclusion Tag Name (optional) and Exclusion Tag Value (optional)** - You can choose to exclude vaults containing a certain tag name and value from the policy assignment. For example, if you do **not** want a diagnostics setting to be added to those vaults which have a tag 'isTest' set to the value 'yes', you must enter 'isTest' in the **Exclusion Tag Name** field and 'yes' in the **Exclusion Tag Value** field. If any (or both) of

these two fields are left empty, the policy will be applied to all relevant vaults irrespective of the tags they contain.

[Preview]: Deploy Diagnostic Settings for Recovery Services Vault to Log Analytics workspace

Assign policy

Basics Parameters Remediation Review + create

Specify parameters for this policy assignment.

Profile name \* ⓘ  
setbypolicy\_logAnalytics

Log Analytics workspace \* ⓘ  
▼

Exclusion Tag Name ⓘ  
▼

Exclusion Tag Value ⓘ  
▼

8. **Create a remediation task** - Once the policy is assigned to a scope, any new vaults created in that scope automatically get LA diagnostics settings configured (within 30 minutes from the time of creation of the vault). To add a diagnostics setting to existing vaults in the scope, you can trigger a remediation task at policy assignment time. To trigger a remediation task, select the checkbox **Create a Remediation task**.

[Preview]: Deploy Diagnostic Settings for Recovery Services Vault to Log Analytics workspace

Assign policy

Basics Parameters Remediation Review + create

By default, this assignment will only take effect on newly created resources. Existing resources can be updated via a remediation task after the policy is assigned. For deployIfNotExists policies, the remediation task will deploy the specified template. For modify policies, the remediation task will edit tags on the existing resources.

Create a remediation task ⓘ

Policy to remediate  
[Preview]: Deploy Diagnostic Settings for Recovery Services Vault to Log Analytics workspace for r... ▼

Managed Identity

Policies with the deployIfNotExists and modify effect types need the ability to deploy resources and edit tags on existing resources respectively. To do this, a managed identity will be created for you.  
[Learn more about Managed Identity.](#)

Create a Managed Identity

9. Navigate to the **Review+Create** tab and click **Create**.

## Under what conditions will the remediation task apply to a vault?

The remediation task is applied to vaults that are non-compliant according to the definition of the policy. A vault is non-compliant if it satisfies either of the following conditions:

- No diagnostics setting is present for the vault.
- Diagnostic settings are present for the vault but neither of the settings has **all of** the Resource specific events enabled with LA as destination, and **Resource specific** selected in the toggle.

So even if a user has a vault with the AzureBackupReport event enabled in AzureDiagnostics mode (which is supported by Backup Reports), the remediation task will still apply to this vault, since the Resource specific mode is the recommended way of creating diagnostics settings, [going forward](#).

Further, if a user has a vault with only a subset of the six Resource specific events enabled, the remediation task will apply for this vault, since Backup Reports will work as expected only if all of the six Resource specific events are enabled.

#### NOTE

If a vault has an existing diagnostics setting with a **subset of Resource specific** categories enabled, configured to send data to a particular LA Workspace, say 'Workspace X', then the remediation task will fail (for that vault alone) if the destination LA Workspace provided in the Policy assignment is the **same** 'Workspace X'.

This is because, if the events enabled by two different diagnostics settings on the same resource **overlap** in some form, then the settings cannot have the same LA Workspace as the destination. You will have to manually resolve this failure, by navigating to the relevant vault and configuring a diagnostics setting with a different LA Workspace as the destination.

Note that the remediation task will **not** fail if the existing diagnostics setting as only AzureBackupReport enabled with Workspace X as the destination, since in this case, there will be no overlap between the events enabled by the existing setting and the events enabled by the setting created by the remediation task.

## Next Steps

- [Learn how to use Backup Reports](#)
- [Learn more about Azure Policy](#)
- [Use Azure Policy to auto-enable backup for all VMs in a give scope](#)

# Back up and restore Azure VMs with PowerShell

12/27/2019 • 26 minutes to read • [Edit Online](#)

This article explains how to back up and restore an Azure VM in an [Azure Backup](#) Recovery Services vault using PowerShell cmdlets.

In this article you learn how to:

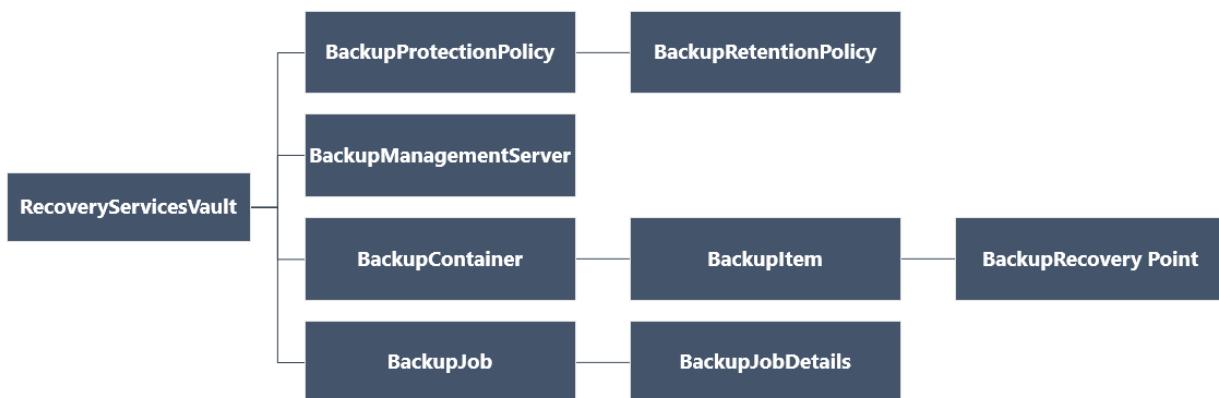
- Create a Recovery Services vault and set the vault context.
- Define a backup policy
- Apply the backup policy to protect multiple virtual machines
- Trigger an on-demand backup job for the protected virtual machines Before you can back up (or protect) a virtual machine, you must complete the [prerequisites](#) to prepare your environment for protecting your VMs.

## Before you start

- [Learn more](#) about Recovery Services vaults.
- [Review](#) the architecture for Azure VM backup, [learn about](#) the backup process, and [review](#) support, limitations, and prerequisites.
- Review the PowerShell object hierarchy for Recovery Services.

## Recovery Services object hierarchy

The object hierarchy is summarized in the following diagram.



Review the [Az.RecoveryServices](#) cmdlet reference reference in the Azure library.

## Set up and register

### NOTE

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

To begin:

1. Download the latest version of PowerShell

2. Find the Azure Backup PowerShell cmdlets available by typing the following command:

```
Get-Command *azrecoveryservices*
```

The aliases and cmdlets for Azure Backup, Azure Site Recovery, and the Recovery Services vault appear.

The following image is an example of what you'll see. It is not the complete list of cmdlets.

| CommandType | Name                                               | Version | Source              |
|-------------|----------------------------------------------------|---------|---------------------|
| Alias       | Get-AzRecoveryServicesAsrNotificationSetting       | 1.0.1   | Az.RecoveryServices |
| Alias       | Get-AzRecoveryServicesAsrVaultSettings             | 1.0.1   | Az.RecoveryServices |
| Alias       | Get-AzRecoveryServicesBackupProperties             | 1.0.1   | Az.RecoveryServices |
| Alias       | Set-AzRecoveryServicesAsrNotificationSetting       | 1.0.1   | Az.RecoveryServices |
| Alias       | Set-AzRecoveryServicesAsrVaultSettings             | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Backup-AzRecoveryServicesBackupItem                | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Disable-AzRecoveryServicesBackupAutoProtection     | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Disable-AzRecoveryServicesBackupProtection         | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Disable-AzRecoveryServicesBackupRPMountScript      | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Edit-AzRecoveryServicesAsrRecoveryPlan             | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Enable-AzRecoveryServicesBackupAutoProtection      | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Enable-AzRecoveryServicesBackupProtection          | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrAlertSetting              | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrEvent                     | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrFabric                    | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrJob                       | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrNetwork                   | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrNetworkMapping            | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrPolicy                    | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrProtectableItem           | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrProtectionContainer       | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrProtectionContainerMap... | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrRecoveryPlan              | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrRecoveryPoint             | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrReplicationProtectedItem  | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrServicesProvider          | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrStorageClassification     | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrStorageClassificationM... | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrVaultContext              | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrvCenter                   | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupContainer              | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupItem                   | 1.0.1   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupJob                    | 1.0.1   | Az.RecoveryServices |

3. Sign in to your Azure account using **Connect-AzAccount**. This cmdlet brings up a web page prompts you for your account credentials:

- Alternately, you can include your account credentials as a parameter in the **Connect-AzAccount** cmdlet, using the **-Credential** parameter.
- If you are CSP partner working on behalf of a tenant, specify the customer as a tenant, by using their tenantID or tenant primary domain name. For example: **Connect-AzAccount -Tenant "fabrikam.com"**

4. Associate the subscription you want to use with the account, since an account can have several subscriptions:

```
Select-AzSubscription -SubscriptionName $SubscriptionName
```

5. If you are using Azure Backup for the first time, you must use the **Register-AzResourceProvider** cmdlet to register the Azure Recovery Service provider with your subscription.

```
Register-AzResourceProvider -ProviderNamespace "Microsoft.RecoveryServices"
```

6. You can verify that the Providers registered successfully, using the following commands:

```
Get-AzResourceProvider -ProviderNamespace "Microsoft.RecoveryServices"
```

In the command output, the **RegistrationState** should change to **Registered**. If not, just run the [Register-AzResourceProvider](#) cmdlet again.

## Create a Recovery Services vault

The following steps lead you through creating a Recovery Services vault. A Recovery Services vault is different than a Backup vault.

1. The Recovery Services vault is a Resource Manager resource, so you need to place it within a resource group. You can use an existing resource group, or create a resource group with the [New-AzResourceGroup](#) cmdlet. When creating a resource group, specify the name and location for the resource group.

```
New-AzResourceGroup -Name "test-rg" -Location "West US"
```

2. Use the [New-AzRecoveryServicesVault](#) cmdlet to create the Recovery Services vault. Be sure to specify the same location for the vault as was used for the resource group.

```
New-AzRecoveryServicesVault -Name "testvault" -ResourceGroupName "test-rg" -Location "West US"
```

3. Specify the type of storage redundancy to use; you can use [Locally Redundant Storage \(LRS\)](#) or [Geo Redundant Storage \(GRS\)](#). The following example shows the `-BackupStorageRedundancy` option for `testvault` is set to `GeoRedundant`.

```
$vault1 = Get-AzRecoveryServicesVault -Name "testvault"
Set-AzRecoveryServicesBackupProperty -Vault $vault1 -BackupStorageRedundancy GeoRedundant
```

### TIP

Many Azure Backup cmdlets require the Recovery Services vault object as an input. For this reason, it is convenient to store the Backup Recovery Services vault object in a variable.

## View the vaults in a subscription

To view all vaults in the subscription, use [Get-AzRecoveryServicesVault](#):

```
Get-AzRecoveryServicesVault
```

The output is similar to the following example, notice the associated `ResourceGroupName` and `Location` are provided.

|                   |   |                                                              |
|-------------------|---|--------------------------------------------------------------|
| Name              | : | Contoso-vault                                                |
| ID                | : | /subscriptions/1234                                          |
| Type              | : | Microsoft.RecoveryServices/vaults                            |
| Location          | : | WestUS                                                       |
| ResourceGroupName | : | Contoso-docs-rg                                              |
| SubscriptionId    | : | 1234-567f-8910-abc                                           |
| Properties        | : | Microsoft.Azure.Commands.RecoveryServices.ARSVaultProperties |

# Back up Azure VMs

Use a Recovery Services vault to protect your virtual machines. Before you apply the protection, set the vault context (the type of data protected in the vault), and verify the protection policy. The protection policy is the schedule when the backup jobs run, and how long each backup snapshot is retained.

## Set vault context

Before enabling protection on a VM, use [Set-AzRecoveryServicesVaultContext](#) to set the vault context. Once the vault context is set, it applies to all subsequent cmdlets. The following example sets the vault context for the vault, *testvault*.

```
Get-AzRecoveryServicesVault -Name "testvault" -ResourceGroupName "Contoso-docs-rg" | Set-AzRecoveryServicesVaultContext
```

## Fetch the vault ID

We plan on deprecating the vault context setting in accordance with Azure PowerShell guidelines. Instead, you can store or fetch the vault ID, and pass it to relevant commands. So, if you haven't set the vault context or want to specify the command to run for a certain vault, pass the vault ID as "-vaultID" to all relevant command, as follows:

```
$targetVault = Get-AzRecoveryServicesVault -ResourceGroupName "Contoso-docs-rg" -Name "testvault"
$targetVault.ID
```

Or

```
$targetVaultID = Get-AzRecoveryServicesVault -ResourceGroupName "Contoso-docs-rg" -Name "testvault" | select -ExpandProperty ID
```

## Modifying storage replication settings

Use [Set-AzRecoveryServicesBackupProperty](#) command to set the Storage replication configuration of the vault to LRS/GRS

```
Set-AzRecoveryServicesBackupProperty -Vault $targetVault -BackupStorageRedundancy GeoRedundant/LocallyRedundant
```

### NOTE

Storage Redundancy can be modified only if there are no backup items protected to the vault.

## Create a protection policy

When you create a Recovery Services vault, it comes with default protection and retention policies. The default protection policy triggers a backup job each day at a specified time. The default retention policy retains the daily recovery point for 30 days. You can use the default policy to quickly protect your VM and edit the policy later with different details.

Use [Get-AzRecoveryServicesBackupProtectionPolicy](#) to view the protection policies available in the vault.

You can use this cmdlet to get a specific policy, or to view the policies associated with a workload type. The following example gets policies for workload type, AzureVM.

```
Get-AzRecoveryServicesBackupProtectionPolicy -WorkloadType "AzureVM" -VaultId $targetVault.ID
```

The output is similar to the following example:

| Name          | WorkloadType | BackupManagementType | BackupTime           | DaysOfWeek |
|---------------|--------------|----------------------|----------------------|------------|
| DefaultPolicy | AzureVM      | AzureVM              | 4/14/2016 5:00:00 PM |            |

#### NOTE

The timezone of the BackupTime field in PowerShell is UTC. However, when the backup time is shown in the Azure portal, the time is adjusted to your local timezone.

A backup protection policy is associated with at least one retention policy. A retention policy defines how long a recovery point is kept before it is deleted.

- Use [Get-AzRecoveryServicesBackupRetentionPolicyObject](#) to view the default retention policy.
- Similarly you can use [Get-AzRecoveryServicesBackupSchedulePolicyObject](#) to obtain the default schedule policy.
- The [New-AzRecoveryServicesBackupProtectionPolicy](#) cmdlet creates a PowerShell object that holds backup policy information.
- The schedule and retention policy objects are used as inputs to the [New-AzRecoveryServicesBackupProtectionPolicy](#) cmdlet.

By default, a start time is defined in the Schedule Policy Object. Use the following example to change the start time to the desired start time. The desired start time should be in UTC as well. The below example assumes the desired start time is 01:00 AM UTC for daily backups.

```
$schPol = Get-AzRecoveryServicesBackupSchedulePolicyObject -WorkloadType "AzureVM" -VaultId $targetVault.ID
$UtcTime = Get-Date -Date "2019-03-20 01:00:00Z"
$UtcTime = $UtcTime.ToUniversalTime()
$schPol.ScheduleRunTimes[0] = $UtcTime
```

#### IMPORTANT

You need to provide the start time in 30 minute multiples only. In the above example, it can be only "01:00:00" or "02:30:00". The start time cannot be "01:15:00"

The following example stores the schedule policy and the retention policy in variables. The example uses those variables to define the parameters when creating a protection policy, *NewPolicy*.

```
$retPol = Get-AzRecoveryServicesBackupRetentionPolicyObject -WorkloadType "AzureVM" -VaultId $targetVault.ID
New-AzRecoveryServicesBackupProtectionPolicy -Name "NewPolicy" -WorkloadType "AzureVM" -RetentionPolicy
$retPol -SchedulePolicy $schPol -VaultId $targetVault.ID
```

The output is similar to the following example:

| Name      | WorkloadType | BackupManagementType | BackupTime           | DaysOfWeek |
|-----------|--------------|----------------------|----------------------|------------|
| NewPolicy | AzureVM      | AzureVM              | 4/24/2016 1:30:00 AM |            |

#### Enable protection

Once you've defined the protection policy, you still must enable the policy for an item. Use [Enable-AzRecoveryServicesBackupProtection](#) to enable protection. Enabling protection requires two objects - the item

and the policy. Once the policy has been associated with the vault, the backup workflow is triggered at the time defined in the policy schedule.

#### IMPORTANT

While using PS to enable backup for multiple VMs at once, ensure that a single policy doesn't have more than 100 VMs associated with it. This is a [recommended best practice](#). Currently, the PS client doesn't explicitly block if there are more than 100 VMs but the check is planned to be added in the future.

The following examples enable protection for the item, V2VM, using the policy, NewPolicy. The examples differ based on whether the VM is encrypted, and what type of encryption.

To enable the protection on **non-encrypted Resource Manager VMs**:

```
$pol = Get-AzRecoveryServicesBackupProtectionPolicy -Name "NewPolicy" -VaultId $targetVault.ID
Enable-AzRecoveryServicesBackupProtection -Policy $pol -Name "V2VM" -ResourceGroupName "RGName1" -VaultId
$targetVault.ID
```

To enable the protection on encrypted VMs (encrypted using BEK and KEK), you must give the Azure Backup service permission to read keys and secrets from the key vault.

```
Set-AzKeyVaultAccessPolicy -VaultName "KeyVaultName" -ResourceGroupName "RGNameOfKeyVault" -PermissionsToKeys
backup,get,list -PermissionsToSecrets get,list -ServicePrincipalName 262044b1-e2ce-469f-a196-69ab7ada62d3
$pol = Get-AzRecoveryServicesBackupProtectionPolicy -Name "NewPolicy" -VaultId $targetVault.ID
Enable-AzRecoveryServicesBackupProtection -Policy $pol -Name "V2VM" -ResourceGroupName "RGName1" -VaultId
$targetVault.ID
```

To enable the protection on **encrypted VMs (encrypted using BEK only)**, you must give the Azure Backup service permission to read secrets from the key vault.

```
Set-AzKeyVaultAccessPolicy -VaultName "KeyVaultName" -ResourceGroupName "RGNameOfKeyVault" -
PermissionsToSecrets backup,get,list -ServicePrincipalName 262044b1-e2ce-469f-a196-69ab7ada62d3
$pol = Get-AzRecoveryServicesBackupProtectionPolicy -Name "NewPolicy" -VaultId $targetVault.ID
Enable-AzRecoveryServicesBackupProtection -Policy $pol -Name "V2VM" -ResourceGroupName "RGName1" -VaultId
$targetVault.ID
```

#### NOTE

If you are using the Azure Government cloud, then use the value ff281ffe-705c-4f53-9f37-a40e6f2c68f3 for the parameter ServicePrincipalName in [Set-AzKeyVaultAccessPolicy](#) cmdlet.

## Monitoring a backup job

You can monitor long-running operations, such as backup jobs, without using the Azure portal. To get the status of an in-progress job, use the [Get-AzRecoveryServicesBackupJob](#) cmdlet. This cmdlet gets the backup jobs for a specific vault, and that vault is specified in the vault context. The following example gets the status of an in-progress job as an array, and stores the status in the \$joblist variable.

```
$joblist = Get-AzRecoveryServicesBackupJob -Status "InProgress" -VaultId $targetVault.ID
$joblist[0]
```

The output is similar to the following example:

| WorkloadName                         | Operation | Status     | StartTime | EndTime    |
|--------------------------------------|-----------|------------|-----------|------------|
| JobID                                | -----     | -----      | -----     | -----      |
| V2VM                                 | Backup    | InProgress | 4/23/2016 | 5:00:30 PM |
| cf4b3ef5-2fac-4c8e-a215-d2eba4124f27 |           |            |           |            |

Instead of polling these jobs for completion - which is unnecessary additional code - use the [Wait-AzRecoveryServicesBackupJob](#) cmdlet. This cmdlet pauses the execution until either the job completes or the specified timeout value is reached.

```
Wait-AzRecoveryServicesBackupJob -Job $joblist[0] -Timeout 43200 -VaultId $targetVault.ID
```

## Manage Azure VM backups

### Modify a protection policy

To modify the protection policy, use [Set-AzRecoveryServicesBackupProtectionPolicy](#) to modify the SchedulePolicy or RetentionPolicy objects.

#### Modifying scheduled time

When you create a protection policy, it is assigned a start-time by default. The following examples show how to modify the start time of a protection policy.

```
$SchPol = Get-AzRecoveryServicesBackupSchedulePolicyObject -WorkloadType "AzureVM"
$UtcTime = Get-Date -Date "2019-03-20 01:00:00Z" (This is the time that the customer wants to start the backup)
$UtcTime = $UtcTime.ToUniversalTime()
$SchPol.ScheduleRunTimes[0] = $UtcTime
$pol = Get-AzRecoveryServicesBackupProtectionPolicy -Name "NewPolicy" -VaultId $targetVault.ID
Set-AzRecoveryServicesBackupProtectionPolicy -Policy $pol -SchedulePolicy $SchPol -VaultId $targetVault.ID
```

#### Modifying retention

The following example changes the recovery point retention to 365 days.

```
$retPol = Get-AzRecoveryServicesBackupRetentionPolicyObject -WorkloadType "AzureVM"
$retPol.DailySchedule.DurationCountInDays = 365
$pol = Get-AzRecoveryServicesBackupProtectionPolicy -Name "NewPolicy" -VaultId $targetVault.ID
Set-AzRecoveryServicesBackupProtectionPolicy -Policy $pol -RetentionPolicy $RetPol -VaultId $targetVault.ID
```

#### Configuring Instant restore snapshot retention

##### NOTE

From Az PS version 1.6.0 onwards, one can update the instant restore snapshot retention period in policy using Powershell

```
$bkpPol = Get-AzRecoveryServicesBackupProtectionPolicy -WorkloadType "AzureVM" -VaultId $targetVault.ID
$bkpPol.SnapshotRetentionInDays=7
Set-AzRecoveryServicesBackupProtectionPolicy -policy $bkpPol -VaultId $targetVault.ID
```

The default value will be 2, user can set the value with a min of 1 and max of 5. For weekly backup policies, the period is set to 5 and cannot be changed.

### Trigger a backup

Use [Backup-AzRecoveryServicesBackupItem](#) to trigger a backup job. If it's the initial backup, it is a full backup.

Subsequent backups take an incremental copy. The following example takes a VM backup to be retained for 60 days.

```
$namedContainer = Get-AzRecoveryServicesBackupContainer -ContainerType "AzureVM" -Status "Registered" -FriendlyName "V2VM" -VaultId $targetVault.ID
$item = Get-AzRecoveryServicesBackupItem -Container $namedContainer -WorkloadType "AzureVM" -VaultId $targetVault.ID
$endDate = (Get-Date).AddDays(60).ToUniversalTime()
$job = Backup-AzRecoveryServicesBackupItem -Item $item -VaultId $targetVault.ID -ExpiryDateTimeUTC $endDate
```

The output is similar to the following example:

| WorkloadName                         | Operation | Status     | StartTime | EndTime    |
|--------------------------------------|-----------|------------|-----------|------------|
| JobID                                | -----     | -----      | -----     | -----      |
| V2VM                                 | Backup    | InProgress | 4/23/2016 | 5:00:30 PM |
| cf4b3ef5-2fac-4c8e-a215-d2eba4124f27 |           |            |           |            |

#### NOTE

The timezone of the StartTime and EndTime fields in PowerShell is UTC. However, when the time is shown in the Azure portal, the time is adjusted to your local timezone.

### Change policy for backup items

User can either modify existing policy or change the policy of the backed-up item from Policy1 to Policy2. To switch policies for a backed-up item, fetch the relevant policy and back up item and use the [Enable-AzRecoveryServices](#) command with backup item as the parameter.

```
$TargetPol1 = Get-AzRecoveryServicesBackupProtectionPolicy -Name <PolicyName> -VaultId $targetVault.ID
$anotherBkpItem = Get-AzRecoveryServicesBackupItem -WorkloadType AzureVM -BackupManagementType AzureVM -Name "<BackupItemName>" -VaultId $targetVault.ID
Enable-AzRecoveryServicesBackupProtection -Item $anotherBkpItem -Policy $TargetPol1 -VaultId $targetVault.ID
```

The command waits until the configure backup is completed and returns the following output.

| WorkloadName                         | Operation       | Status    | StartTime            | EndTime              |
|--------------------------------------|-----------------|-----------|----------------------|----------------------|
| JobID                                | -----           | -----     | -----                | -----                |
| TestVM                               | ConfigureBackup | Completed | 3/18/2019 8:00:21 PM | 3/18/2019 8:02:16 PM |
| 654e8aa2-4096-402b-b5a9-e5e71a496c4e |                 |           |                      |                      |

### Stop protection

#### Retain data

If user wishes to stop protection, they can use the [Disable-AzRecoveryServicesBackupProtection](#) PS cmdlet. This will stop the scheduled backups but the data backed up until now is retained forever.

```
$bkpItem = Get-AzRecoveryServicesBackupItem -BackupManagementType AzureVM -WorkloadType AzureVM -Name "<backup item name>" -VaultId $targetVault.ID
Disable-AzRecoveryServicesBackupProtection -Item $bkpItem -VaultId $targetVault.ID
```

#### Delete backup data

In order to completely remove the stored backup data in the vault, just add '-RemoveRecoveryPoints' flag/switch

to the 'disable' protection command.

```
Disable-AzRecoveryServicesBackupProtection -Item $bkpItem -VaultId $targetVault.ID -RemoveRecoveryPoints
```

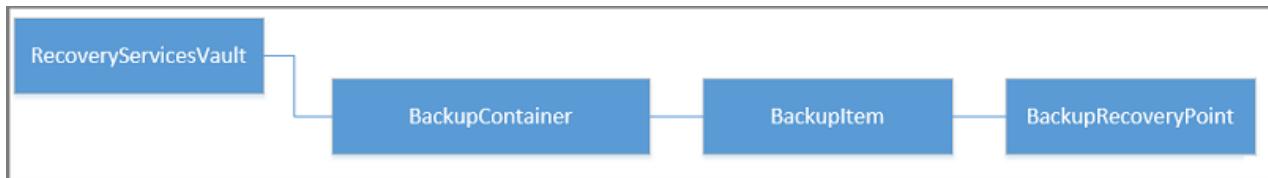
## Restore an Azure VM

There is an important difference between the restoring a VM using the Azure portal and restoring a VM using PowerShell. With PowerShell, the restore operation is complete once the disks and configuration information from the recovery point are created. The restore operation doesn't create the virtual machine. To create a virtual machine from disk, see the section, [Create the VM from restored disks](#). If you don't want to restore the entire VM, but want to restore or recover a few files from an Azure VM backup, refer to the [file recovery section](#).

### TIP

The restore operation does not create the virtual machine.

The following graphic shows the object hierarchy from the RecoveryServicesVault down to the BackupRecoveryPoint.



To restore backup data, identify the backed-up item and the recovery point that holds the point-in-time data. Use [Restore-AzRecoveryServicesBackupItem](#) to restore data from the vault to your account.

The basic steps to restore an Azure VM are:

- Select the VM.
- Choose a recovery point.
- Restore the disks.
- Create the VM from stored disks.

### Select the VM

To get the PowerShell object that identifies the right backup item, start from the container in the vault, and work your way down the object hierarchy. To select the container that represents the VM, use the [Get-AzRecoveryServicesBackupContainer](#) cmdlet and pipe that to the [Get-AzRecoveryServicesBackupItem](#) cmdlet.

```
$namedContainer = Get-AzRecoveryServicesBackupContainer -ContainerType "AzureVM" -Status "Registered" -FriendlyName "V2VM" -VaultId $targetVault.ID
$backupitem = Get-AzRecoveryServicesBackupItem -Container $namedContainer -WorkloadType "AzureVM" -VaultId $targetVault.ID
```

### Choose a recovery point

Use the [Get-AzRecoveryServicesBackupRecoveryPoint](#) cmdlet to list all recovery points for the backup item. Then choose the recovery point to restore. If you are unsure which recovery point to use, it is a good practice to choose the most recent RecoveryPointType = AppConsistent point in the list.

In the following script, the variable, `$rp`, is an array of recovery points for the selected backup item, from the past seven days. The array is sorted in reverse order of time with the latest recovery point at index 0. Use standard PowerShell array indexing to pick the recovery point. In the example, `$rp[0]` selects the latest recovery point.

```
$startDate = (Get-Date).AddDays(-7)
$endDate = Get-Date
$rp = Get-AzRecoveryServicesBackupRecoveryPoint -Item $backupitem -StartDate $startdate.ToUniversalTime() -
EndDate $enddate.ToUniversalTime() -VaultId $targetVault.ID
$rp[0]
```

The output is similar to the following example:

```
RecoveryPointAdditionalInfo :
SourceVMStorageType : NormalStorage
Name : 15260861925810
ItemName : VM;iaasvmcontainer;RGName1;V2VM
RecoveryPointId : /subscriptions/XX/resourceGroups/
RGName1/providers/Microsoft.RecoveryServices/vaults/testvault/backupFabrics/Azure/protectionContainers/IaasVMContainer;iaasvmcontainer;RGName1;V2VM/protectedItems/VM;iaasvmcontainer;RGName1;V2VM/recoveryPoints/15260861925810
RecoveryPointType : AppConsistent
RecoveryPointTime : 4/23/2016 5:02:04 PM
WorkloadType : AzureVM
ContainerName : IaasVMContainer;iaasvmcontainer; RGName1;V2VM
ContainerType : AzureVM
BackupManagementType : AzureVM
```

## Restore the disks

Use the [Restore-AzRecoveryServicesBackupItem](#) cmdlet to restore a backup item's data and configuration to a recovery point. Once you identify a recovery point, use it as the value for the **-RecoveryPoint** parameter. In the above sample, **\$rp[0]** was the recovery point to use. In the following sample code, **\$rp[0]** is the recovery point to use for restoring the disk.

To restore the disks and configuration information:

```
$restorejob = Restore-AzRecoveryServicesBackupItem -RecoveryPoint $rp[0] -StorageAccountName "DestAccount" -
StorageAccountResourceGroupName "DestRG" -VaultId $targetVault.ID
$restorejob
```

## Restore managed disks

### NOTE

If the backed VM has managed disks and you want to restore them as managed disks, we have introduced the capability from Azure PowerShell RM module v 6.7.0. onwards

Provide an additional parameter **TargetResourceGroupName** to specify the RG to which managed disks will be restored.

### NOTE

It is strongly recommended to use the **TargetResourceGroupName** parameter for restoring managed disks since it results in significant performance improvements. Also, from Azure Powershell Az module 1.0 onwards, this parameter is mandatory in case of a restore with managed disks

```
$restorejob = Restore-AzRecoveryServicesBackupItem -RecoveryPoint $rp[0] -StorageAccountName "DestAccount" -
StorageAccountResourceGroupName "DestRG" -TargetResourceGroupName "DestRGforManagedDisks" -VaultId
$targetVault.ID
```

The **VMConfig.JSON** file will be restored to the storage account and the managed disks will be restored to the specified target RG.

The output is similar to the following example:

| WorkloadName | Operation | Status     | StartTime            | EndTime | JobID     |
|--------------|-----------|------------|----------------------|---------|-----------|
| V2VM         | Restore   | InProgress | 4/23/2016 5:00:30 PM |         | cf4b3ef5- |

Use the [Wait-AzRecoveryServicesBackupJob](#) cmdlet to wait for the Restore job to complete.

```
Wait-AzRecoveryServicesBackupJob -Job $restorejob -Timeout 43200
```

Once the Restore job has completed, use the [Get-AzRecoveryServicesBackupJobDetails](#) cmdlet to get the details of the restore operation. The JobDetails property has the information needed to rebuild the VM.

```
$restorejob = Get-AzRecoveryServicesBackupJob -Job $restorejob -VaultId $targetVault.ID
$details = Get-AzRecoveryServicesBackupJobDetails -Job $restorejob -VaultId $targetVault.ID
```

Once you restore the disks, go to the next section to create the VM.

## Replace disks in Azure VM

To replace the disks and configuration information, perform the below steps:

- Step 1: [Restore the disks](#)
- Step 2: [Detach data disk using PowerShell](#)
- Step 3: [Attach data disk to Windows VM with PowerShell](#)

## Create a VM from restored disks

After you restore the disks, use the following steps to create and configure the virtual machine from disk.

### NOTE

1. AzureAz module 3.0.0 or higher is required.
2. To create encrypted VMs from restored disks, your Azure role must have permission to perform the action, **Microsoft.KeyVault/vaults/deploy/action**. If your role does not have this permission, create a custom role with this action. For more information, see [Custom Roles in Azure RBAC](#).
3. After restoring disks, you can now get a deployment template which you can directly use to create a new VM. No more different PS cmdlets to create managed/unmanaged VMs which are encrypted/unencrypted.

## Create a VM using the deployment template

The resultant job details give the template URI that can be queried and deployed.

```
$properties = $details.properties
$storageAccountName = $properties["Target Storage Account Name"]
$containerName = $properties["Config Blob Container Name"]
$templateBlobURI = $properties["Template Blob Uri"]
```

The template is not directly accessible since it is under a customer's storage account and the given container. We

need the complete URL (along with a temporary SAS token) to access this template.

1. First extract the template name from the templateBlobURI. The format is mentioned below. You can use the split operation in Powershell to extract the final template name from this URL.

```
https://<storageAccountName.blob.core.windows.net>/<containerName>/<templateName>
```

2. Then the full URL can be generated as explained [here](#).

```
Set-AzCurrentStorageAccount -Name $storageAccountName -ResourceGroupName <StorageAccount RG name>
$templateBlobFullURI = New-AzStorageBlobSASToken -Container $containerName -Blob <templateName> -Permission r
-FullUri
```

3. Deploy the template to create a new VM as explained [here](#).

```
New-AzResourceGroupDeployment -Name ExampleDeployment ResourceGroupName ExampleResourceGroup -TemplateUri
$templateBlobFullURI -storageAccountType Standard_GRS
```

## Create a VM using the config file

The following section lists steps necessary to create a VM using "VMConfig" file.

### NOTE

It is highly recommended to use the deployment template detailed above to create a VM. This section (Points 1-6) will be deprecated soon.

1. Query the restored disk properties for the job details.

```
$properties = $details.properties
$storageAccountName = $properties["Target Storage Account Name"]
$containerName = $properties["Config Blob Container Name"]
$configBlobName = $properties["Config Blob Name"]
```

2. Set the Azure storage context and restore the JSON configuration file.

```
Set-AzCurrentStorageAccount -Name $storageaccountname -ResourceGroupName "testvault"
$destination_path = "C:\vmconfig.json"
Get-AzStorageBlobContent -Container $containerName -Blob $configBlobName -Destination $destination_path
$obj = ((Get-Content -Path $destination_path -Raw -Encoding Unicode)).TrimEnd([char]0x00) |
ConvertFrom-Json
```

3. Use the JSON configuration file to create the VM configuration.

```
$vm = New-AzVMConfig -VMSize $obj.'properties.hardwareProfile'.vmSize -VMName "testrestore"
```

4. Attach the OS disk and data disks. This step provides examples for various managed and encrypted VM configurations. Use the example that suits your VM configuration.

- **Non-managed and non-encrypted VMs** - Use the following sample for non-managed, non-encrypted VMs.

```

Set-AzVMOSDisk -VM $vm -Name "osdisk" -VhdUri $obj.'properties.StorageProfile'.osDisk.vhd.Uri -
CreateOption "Attach"
$vm.StorageProfile.OsDisk.OsType = $obj.'properties.StorageProfile'.OsDisk.OsType
foreach($dd in $obj.'properties.StorageProfile'.DataDisks)
{
 $vm = Add-AzVMDataDisk -VM $vm -Name "datadisk1" -VhdUri $dd.vhd.Uri -DiskSizeInGB 127 -Lun $dd.Lun -
CreateOption "Attach"
}

```

- **Non-managed and encrypted VMs with Azure AD (BEK only)** - For non-managed, encrypted VMs with Azure AD (encrypted using BEK only), you need to restore the secret to the key vault before you can attach disks. For more information, see the [Restore an encrypted virtual machine from an Azure Backup recovery point](#). The following sample shows how to attach OS and data disks for encrypted VMs. When setting the OS disk, make sure to mention the relevant OS type.

```

$dekuUrl =
"https://ContosoKeyVault.vault.azure.net:443/secrets/ContosoSecret007/xx000000xx0849999f3xx30000003163"
$dekuUrl = "/subscriptions/abcdedf007-4xyz-1a2b-0000-
12a2b345675c/resourceGroups/ContosoRG108/providers/Microsoft.KeyVault/vaults/ContosoKeyVault"
Set-AzVMOSDisk -VM $vm -Name "osdisk" -VhdUri $obj.'properties.storageProfile'.osDisk.vhd.uri -
DiskEncryptionKeyUrl $dekuUrl -DiskEncryptionKeyVaultId $keyVaultId -CreateOption "Attach" -Windows/Linux
$vm.StorageProfile.OsDisk.OsType = $obj.'properties.storageProfile'.osDisk.osType
foreach($dd in $obj.'properties.storageProfile'.dataDisks)
{
 $vm = Add-AzVMDataDisk -VM $vm -Name "datadisk1" -VhdUri $dd.vhd.Uri -DiskSizeInGB 127 -Lun $dd.Lun -
CreateOption "Attach"
}

```

- **Non-managed and encrypted VMs with Azure AD (BEK and KEK)** - For non-managed, encrypted VMs with Azure AD (encrypted using BEK and KEK), restore the key and secret to the key vault before attaching the disks. For more information, see [Restore an encrypted virtual machine from an Azure Backup recovery point](#). The following sample shows how to attach OS and data disks for encrypted VMs.

```

$dekuUrl =
"https://ContosoKeyVault.vault.azure.net:443/secrets/ContosoSecret007/xx000000xx0849999f3xx30000003163"
$kekUrl =
"https://ContosoKeyVault.vault.azure.net:443/keys/ContosoKey007/x9xxx00000x0000x9b9949999xx0x006"
$keyVaultId = "/subscriptions/abcdedf007-4xyz-1a2b-0000-
12a2b345675c/resourceGroups/ContosoRG108/providers/Microsoft.KeyVault/vaults/ContosoKeyVault"
Set-AzVMOSDisk -VM $vm -Name "osdisk" -VhdUri $obj.'properties.storageProfile'.osDisk.vhd.uri -
DiskEncryptionKeyUrl $dekuUrl -DiskEncryptionKeyVaultId $keyVaultId -KeyEncryptionKeyUrl $kekUrl -
KeyEncryptionKeyVaultId $keyVaultId -CreateOption "Attach" -Windows
$vm.StorageProfile.OsDisk.OsType = $obj.'properties.storageProfile'.osDisk.osType
foreach($dd in $obj.'properties.storageProfile'.dataDisks)
{
 $vm = Add-AzVMDataDisk -VM $vm -Name "datadisk1" -VhdUri $dd.vhd.Uri -DiskSizeInGB 127 -Lun $dd.Lun -
CreateOption "Attach"
}

```

- **Non-managed and encrypted VMs without Azure AD (BEK only)** - For non-managed, encrypted VMs without Azure AD (encrypted using BEK only), if source **keyVault/secret are not available** restore the secrets to key vault using the procedure in [Restore an non-encrypted virtual machine from an Azure Backup recovery point](#). Then execute the following scripts to set encryption details on the restored OS blob (this step is not required for data blob). The \$dekuurl can be fetched from the restored keyVault.

The below script needs to be executed only when the source keyVault/secret is not available.

```

$dekUrl =
"https://ContosoKeyVault.vault.azure.net/secrets/ContosoSecret007/xx000000xx0849999f3xx30000003163"
$keyVaultId = "/subscriptions/abcdedf007-4xyz-1a2b-0000-
12a2b345675c/resourceGroups/ContosoRG108/providers/Microsoft.KeyVault/vaults/ContosoKeyVault"
$encSetting = "{\"encryptionEnabled\":true,\"encryptionSettings\":[{\"diskEncryptionKey\":
\"sourceVault\":{\"id\":\"$keyVaultId\"},\"secretUrl\":\"$dekUrl\"}]}"
$osBlobName = $obj.'properties.StorageProfile'.osDisk.name + ".vhdx"
$osBlob = Get-AzStorageBlob -Container $containerName -Blob $osBlobName
$osBlob.ICloudBlob.Metadata["DiskEncryptionSettings"] = $encSetting
$osBlob.ICloudBlob.SetMetadata()

```

After the **secrets are available** and the encryption details are also set on the OS Blob, attach the disks using the script given below.

If the source keyVault/secrets are available already, then the above script need not be executed.

```

Set-AzVMOSDisk -VM $vm -Name "osdisk" -VhdUri $obj.'properties.StorageProfile'.osDisk.vhd.Uri -
CreateOption "Attach"
$vvm.StorageProfile.OsDisk.OsType = $obj.'properties.StorageProfile'.OsDisk.OsType
foreach($dd in $obj.'properties.StorageProfile'.DataDisks)
{
 $vm = Add-AzVMDataDisk -VM $vm -Name "datadisk1" -VhdUri $dd.vhd.Uri -DiskSizeInGB 127 -Lun $dd.Lun -
CreateOption "Attach"
}

```

- **Non-managed and encrypted VMs without Azure AD (BEK and KEK)** - For non-managed, encrypted VMs without Azure AD (encrypted using BEK & KEK), if source **keyVault/key/secret are not available** restore the key and secrets to key vault using the procedure in [Restore an non-encrypted virtual machine from an Azure Backup recovery point](#). Then execute the following scripts to set encryption details on the restored OS blob (this step is not required for data blob). The \$dekurl and \$kekurl can be fetched from the restored keyVault.

The below script needs to be executed only when the source keyVault/key/secret is not available.

```

$dekUrl =
"https://ContosoKeyVault.vault.azure.net/secrets/ContosoSecret007/xx000000xx0849999f3xx30000003163"
$kekUrl = "https://ContosoKeyVault.vault.azure.net/keys/ContosoKey007/x9xxx00000x0000x9b9949999xx0x006"
$keyVaultId = "/subscriptions/abcdedf007-4xyz-1a2b-0000-
12a2b345675c/resourceGroups/ContosoRG108/providers/Microsoft.KeyVault/vaults/ContosoKeyVault"
$encSetting = "{\"encryptionEnabled\":true,\"encryptionSettings\":[{\"diskEncryptionKey\":
\"sourceVault\":{\"id\":\"$keyVaultId\"},\"keyUrl\":\"$kekUrl\"},\"keyEncryptionKey\":{\"sourceVault\":
{\"id\":\"$keyVaultId\"},\"keyUrl\":\"$kekUrl\"}]}"
$osBlobName = $obj.'properties.StorageProfile'.osDisk.name + ".vhdx"
$osBlob = Get-AzStorageBlob -Container $containerName -Blob $osBlobName
$osBlob.ICloudBlob.Metadata["DiskEncryptionSettings"] = $encSetting
$osBlob.ICloudBlob.SetMetadata()

```

After the **key/secrets are available** and the encryption details are set on the OS Blob, attach the disks using the script given below.

If the source keyVault/key/secrets are available, then the above script need not be executed.

```

Set-AzVMOSDisk -VM $vm -Name "osdisk" -VhdUri $obj.'properties.StorageProfile'.osDisk.vhd.Uri -
CreateOption "Attach"
$vm.StorageProfile.OsDisk.OsType = $obj.'properties.StorageProfile'.OsDisk.OsType
foreach($dd in $obj.'properties.StorageProfile'.DataDisks)
{
 $vm = Add-AzVMDataDisk -VM $vm -Name "datadisk1" -VhdUri $dd.vhd.Uri -DiskSizeInGB 127 -Lun $dd.Lun -
CreateOption "Attach"
}

```

- **Managed and non-encrypted VMs** - For managed non-encrypted VMs, attach the restored managed disks. For in-depth information, see [Attach a data disk to a Windows VM using PowerShell](#).
- **Managed and encrypted VMs with Azure AD (BEK only)** - For managed encrypted VMs with Azure AD (encrypted using BEK only), attach the restored managed disks. For in-depth information, see [Attach a data disk to a Windows VM using PowerShell](#).
- **Managed and encrypted VMs with Azure AD (BEK and KEK)** - For managed encrypted VMs with Azure AD (encrypted using BEK and KEK), attach the restored managed disks. For in-depth information, see [Attach a data disk to a Windows VM using PowerShell](#).
- **Managed and encrypted VMs without Azure AD (BEK only)** - For managed, encrypted VMs without Azure AD (encrypted using BEK only), if source **keyVault/secret are not available** restore the secrets to key vault using the procedure in [Restore an non-encrypted virtual machine from an Azure Backup recovery point](#). Then execute the following scripts to set encryption details on the restored OS disk (this step is not required for data disk). The \$dekurl can be fetched from the restored keyVault.

The below script needs to be executed only when the source keyVault/secret is not available.

```

$dekUrl = "https://ContosoKeyVault.vault.azure.net/secrets/ContosoSecret007/xx00000xx0849999f3xx30000003163"
$keyVaultId = "/subscriptions/abcdef007-4xyz-1a2b-0000-
12a2b345675c/resourceGroups/ContosoRG108/providers/Microsoft.KeyVault/vaults/ContosoKeyVault"
$diskupdateconfig = New-AzDiskUpdateConfig -EncryptionSettingsEnabled $true
$encryptionSettingsElement = New-Object Microsoft.Azure.Management.Compute.Models.EncryptionSettingsElement
$encryptionSettingsElement.DiskEncryptionKey = New-Object
Microsoft.Azure.Management.Compute.Models.KeyVaultAndSecretReference
$encryptionSettingsElement.DiskEncryptionKey.SourceVault = New-Object
Microsoft.Azure.Management.Compute.Models.SourceVault
$encryptionSettingsElement.DiskEncryptionKey.SourceVault.Id = $keyVaultId
$encryptionSettingsElement.DiskEncryptionKey.SecretUrl = $dekUrl
$diskupdateconfig.EncryptionSettingsCollection.EncryptionSettings = New-Object
System.Collections.Generic.List[Microsoft.Azure.Management.Compute.Models.EncryptionSettingsElement]
$diskupdateconfig.EncryptionSettingsCollection.EncryptionSettings.Add($encryptionSettingsElement)
$diskupdateconfig.EncryptionSettingsCollection.EncryptionSettingsVersion = "1.1"
Update-AzDisk -ResourceGroupName "testvault" -DiskName $obj.'properties.StorageProfile'.osDisk.name -
DiskUpdate $diskupdateconfig

```

After the secrets are available and the encryption details are set on the OS disk, to attach the restored managed disks, see [Attach a data disk to a Windows VM using PowerShell](#).

- **Managed and encrypted VMs without Azure AD (BEK and KEK)** - For managed, encrypted VMs without Azure AD (encrypted using BEK & KEK), if source **keyVault/secret are not available** restore the key and secrets to key vault using the procedure in [Restore an non-encrypted virtual machine from an Azure Backup recovery point](#). Then execute the following scripts to set encryption details on the restored OS disk (this step is not required for data disks). The \$dekurl and \$kekurl can be fetched from the restored keyVault.

The below script needs to be executed only when the source keyVault/secret is not available.

```

$dekUrl = "https://ContosoKeyVault.vault.azure.net/secrets/ContosoSecret007/xx000000xx0849999f3xx30000003163"
$kekUrl = "https://ContosoKeyVault.vault.azure.net/keys/ContosoKey007/x9xxx0000x0000x9b9949999xx0x006"
$keyVaultId = "/subscriptions/abcdedf007-4xyz-1a2b-0000-
12a2b345675c/resourceGroups/ContosoRG108/providers/Microsoft.KeyVault/vaults/ContosoKeyVault"
$diskupdateconfig = New-AzDiskUpdateConfig -EncryptionSettingsEnabled $true
$encryptionSettingsElement = New-Object Microsoft.Azure.Management.Compute.Models.EncryptionSettingsElement
$encryptionSettingsElement.DiskEncryptionKey = New-Object
Microsoft.Azure.Management.Compute.Models.KeyVaultAndSecretReference
$encryptionSettingsElement.DiskEncryptionKey.SourceVault = New-Object
Microsoft.Azure.Management.Compute.Models.SourceVault
$encryptionSettingsElement.DiskEncryptionKey.SourceVault.Id = $keyVaultId
$encryptionSettingsElement.DiskEncryptionKey.SecretUrl = $dekUrl
$encryptionSettingsElement.KeyEncryptionKey = New-Object
Microsoft.Azure.Management.Compute.Models.KeyVaultAndKeyReference
$encryptionSettingsElement.KeyEncryptionKey.SourceVault = New-Object
Microsoft.Azure.Management.Compute.Models.SourceVault
$encryptionSettingsElement.KeyEncryptionKey.SourceVault.Id = $keyVaultId
$encryptionSettingsElement.KeyEncryptionKey.KeyUrl = $kekUrl
$diskupdateconfig.EncryptionSettingsCollection.EncryptionSettings = New-Object
System.Collections.Generic.List[Microsoft.Azure.Management.Compute.Models.EncryptionSettingsElement]
$diskupdateconfig.EncryptionSettingsCollection.EncryptionSettings.Add($encryptionSettingsElement)
$diskupdateconfig.EncryptionSettingsCollection.EncryptionSettingsVersion = "1.1"
Update-AzDisk -ResourceGroupName "testvault" -DiskName $obj.'properties.StorageProfile'.osDisk.name -
DiskUpdate $diskupdateconfig

```

After the key/secrets are available and the encryption details are set on the OS disk, to attach the restored managed disks, see [Attach a data disk to a Windows VM using PowerShell](#).

#### 5. Set the Network settings.

```

$nicName="p1234"
$pip = New-AzPublicIpAddress -Name $nicName -ResourceGroupName "test" -Location "WestUS" -
AllocationMethod Dynamic
$virtualNetwork = New-AzVirtualNetwork -ResourceGroupName "test" -Location "WestUS" -Name "testvNET" -
AddressPrefix 10.0.0.0/16
$virtualNetwork | Set-AzVirtualNetwork
$vnet = Get-AzVirtualNetwork -Name "testvNET" -ResourceGroupName "test"
$subnetindex=0
$nic = New-AzNetworkInterface -Name $nicName -ResourceGroupName "test" -Location "WestUS" -SubnetId
$vnet.Subnets[$subnetindex].Id -PublicIpAddressId $pip.Id
$vm=Add-AzVMNetworkInterface -VM $vm -Id $nic.Id

```

#### 6. Create the virtual machine.

```
New-AzVM -ResourceGroupName "test" -Location "WestUS" -VM $vm
```

#### 7. Push ADE extension. If the ADE extensions are not pushed, then the data disks will be marked as unencrypted, so it is mandatory for the steps below to be executed:

- **For VM with Azure AD** - Use the following command to manually enable encryption for the data disks

#### **BEK only**

```

Set-AzVMDiskEncryptionExtension -ResourceGroupName $RG -VMName $vm.Name -AadClientID
$aadClientID -AadClientSecret $aadClientSecret -DiskEncryptionKeyVaultUrl $dekUrl -
DiskEncryptionKeyVaultId $keyVaultId -VolumeType Data

```

#### **BEK and KEK**

```
Set-AzVMDiskEncryptionExtension -ResourceGroupName $RG -VMName $vm.Name -AadClientID
$aadClientID -AadClientSecret $aadClientSecret -DiskEncryptionKeyVaultUrl $dekUrl -
DiskEncryptionKeyVaultId $keyVaultId -KeyEncryptionKeyUrl $kekUrl -KeyEncryptionKeyVaultId
$keyVaultId -VolumeType Data
```

- **For VM without Azure AD** - Use the following command to manually enable encryption for the data disks.

If during the command execution it asks for AADClientID, then you need to update your Azure PowerShell.

### BEK only

```
Set-AzVMDiskEncryptionExtension -ResourceGroupName $RG -VMName $vm.Name -
DiskEncryptionKeyVaultUrl $dekUrl -DiskEncryptionKeyVaultId $keyVaultId -SkipVmBackup -
VolumeType "All"
```

### BEK and KEK

```
Set-AzVMDiskEncryptionExtension -ResourceGroupName $RG -VMName $vm.Name -
DiskEncryptionKeyVaultUrl $dekUrl -DiskEncryptionKeyVaultId $keyVaultId -KeyEncryptionKeyUrl
$kekUrl -KeyEncryptionKeyVaultId $keyVaultId -SkipVmBackup -VolumeType "All"
```

#### NOTE

Ensure to manually delete the JASON files created as part of encrypted VM restore disk process.

## Restore files from an Azure VM backup

In addition to restoring disks, you can also restore individual files from an Azure VM backup. The restore files functionality provides access to all files in a recovery point. Manage the files via File Explorer as you would for normal files.

The basic steps to restore a file from an Azure VM backup are:

- Select the VM
- Choose a recovery point
- Mount the disks of recovery point
- Copy the required files
- Unmount the disk

### Select the VM

To get the PowerShell object that identifies the right backup item, start from the container in the vault, and work your way down the object hierarchy. To select the container that represents the VM, use the [Get-AzRecoveryServicesBackupContainer](#) cmdlet and pipe that to the [Get-AzRecoveryServicesBackupItem](#) cmdlet.

```
$namedContainer = Get-AzRecoveryServicesBackupContainer -ContainerType "AzureVM" -Status "Registered" -
FriendlyName "V2VM" -VaultId $targetVault.ID
$backupitem = Get-AzRecoveryServicesBackupItem -Container $namedContainer -WorkloadType "AzureVM" -VaultId
$targetVault.ID
```

### Choose a recovery point

Use the [Get-AzRecoveryServicesBackupRecoveryPoint](#) cmdlet to list all recovery points for the backup item. Then

choose the recovery point to restore. If you are unsure which recovery point to use, it is a good practice to choose the most recent RecoveryPointType = AppConsistent point in the list.

In the following script, the variable, \$rp, is an array of recovery points for the selected backup item, from the past seven days. The array is sorted in reverse order of time with the latest recovery point at index 0. Use standard PowerShell array indexing to pick the recovery point. In the example, \$rp[0] selects the latest recovery point.

```
$startDate = (Get-Date).AddDays(-7)
$endDate = Get-Date
$rp = Get-AzRecoveryServicesBackupRecoveryPoint -Item $backupitem -StartDate $startdate.ToUniversalTime() -
EndDate $enddate.ToUniversalTime() -VaultId $targetVault.ID
$rp[0]
```

The output is similar to the following example:

```
RecoveryPointAdditionalInfo :
SourceVMStorageType : NormalStorage
Name : 15260861925810
ItemName : VM;iaasvmcontainer;RGName1;V2VM
RecoveryPointId : /subscriptions/XX/resourceGroups/
RGName1/providers/Microsoft.RecoveryServices/vaults/testvault/backupFabrics/Azure/protectionContainers/IaaSVMC
ontainer;iaasvmcontainer;RGName1;V2VM/protectedItems/VM;iaasvmcontainer;
RGName1;V2VM/recoveryPoints/15260861925810
RecoveryPointType : AppConsistent
RecoveryPointTime : 4/23/2016 5:02:04 PM
WorkloadType : AzureVM
ContainerName : IaaSVMContainer;iaasvmcontainer; RGName1;V2VM
ContainerType : AzureVM
BackupManagementType : AzureVM
```

## Mount the disks of recovery point

Use the [Get-AzRecoveryServicesBackupRPMountScript](#) cmdlet to get the script to mount all the disks of the recovery point.

### NOTE

The disks are mounted as iSCSI attached disks to the machine where the script is run. Mounting occurs immediately, and you don't incur any charges.

```
Get-AzRecoveryServicesBackupRPMountScript -RecoveryPoint $rp[0] -VaultId $targetVault.ID
```

The output is similar to the following example:

| OsType  | Password        | Filename                                                                                      |
|---------|-----------------|-----------------------------------------------------------------------------------------------|
| Windows | e3632984e51f496 | V2VM_wus2_8287309959960546283_451516692429_cbd6061f7fc543c489f1974d33659fed07a6e0c2e08740.exe |

Run the script on the machine where you want to recover the files. To execute the script, you must enter the password provided. After the disks are attached, use Windows File Explorer to browse the new volumes and files. For more information, see the Backup article, [Recover files from Azure virtual machine backup](#).

## Unmount the disks

After the required files are copied, use [Disable-AzRecoveryServicesBackupRPMountScript](#) to unmount the disks. Be sure to unmount the disks so access to the files of the recovery point is removed.

```
Disable-AzRecoveryServicesBackupRPMountScript -RecoveryPoint $rp[0] -VaultId $targetVault.ID
```

## Next steps

If you prefer to use PowerShell to engage with your Azure resources, see the PowerShell article, [Deploy and Manage Backup for Windows Server](#). If you manage DPM backups, see the article, [Deploy and Manage Backup for DPM](#).

# Deploy and manage backup to Azure for Data Protection Manager (DPM) servers using PowerShell

2/25/2020 • 13 minutes to read • [Edit Online](#)

This article shows you how to use PowerShell to setup Azure Backup on a DPM server, and to manage backup and recovery.

## Setting up the PowerShell environment

Before you can use PowerShell to manage backups from Data Protection Manager to Azure, you need to have the right environment in PowerShell. At the start of the PowerShell session, ensure that you run the following command to import the right modules and allow you to correctly reference the DPM cmdlets:

```
& "C:\Program Files\Microsoft System Center 2012 R2\DPM\DPM\bin\DpmCliInitScript.ps1"
```

```
Welcome to the DPM Management Shell!
```

```
Full list of cmdlets: Get-Command
Only DPM cmdlets: Get-DPMCommand
Get general help: help
Get help for a cmdlet: help <cmdlet-name> or <cmdlet-name> -?
Get definition of a cmdlet: Get-Command <cmdlet-name> -Syntax
Sample DPM scripts: Get-DPMSampleScript
```

## Setup and Registration

### NOTE

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

To begin, [download the latest Azure PowerShell](#).

The following setup and registration tasks can be automated with PowerShell:

- Create a Recovery Services vault
- Installing the Azure Backup agent
- Registering with the Azure Backup service
- Networking settings
- Encryption settings

## Create a recovery services vault

The following steps lead you through creating a Recovery Services vault. A Recovery Services vault is different than a Backup vault.

1. If you are using Azure Backup for the first time, you must use the **Register-AzResourceProvider** cmdlet to

register the Azure Recovery Service provider with your subscription.

```
Register-AzResourceProvider -ProviderNamespace "Microsoft.RecoveryServices"
```

2. The Recovery Services vault is an ARM resource, so you need to place it within a Resource Group. You can use an existing resource group, or create a new one. When creating a new resource group, specify the name and location for the resource group.

```
New-AzResourceGroup -Name "test-rg" -Location "West US"
```

3. Use the **New-AzRecoveryServicesVault** cmdlet to create a new vault. Be sure to specify the same location for the vault as was used for the resource group.

```
New-AzRecoveryServicesVault -Name "testvault" -ResourceGroupName "test-rg" -Location "West US"
```

4. Specify the type of storage redundancy to use; you can use [Locally Redundant Storage \(LRS\)](#) or [Geo Redundant Storage \(GRS\)](#). The following example shows the -BackupStorageRedundancy option for testVault is set to GeoRedundant.

**TIP**

Many Azure Backup cmdlets require the Recovery Services vault object as an input. For this reason, it is convenient to store the Backup Recovery Services vault object in a variable.

```
$vault1 = Get-AzRecoveryServicesVault -Name "testVault"
Set-AzRecoveryServicesBackupProperties -vault $vault1 -BackupStorageRedundancy GeoRedundant
```

## View the vaults in a subscription

Use **Get-AzRecoveryServicesVault** to view the list of all vaults in the current subscription. You can use this command to check that a new vault was created, or to see what vaults are available in the subscription.

Run the command, Get-AzRecoveryServicesVault, and all vaults in the subscription are listed.

```
Get-AzRecoveryServicesVault
```

|                   |   |                                                              |
|-------------------|---|--------------------------------------------------------------|
| Name              | : | Contoso-vault                                                |
| ID                | : | /subscriptions/1234                                          |
| Type              | : | Microsoft.RecoveryServices/vaults                            |
| Location          | : | WestUS                                                       |
| ResourceGroupName | : | Contoso-docs-rg                                              |
| SubscriptionId    | : | 1234-567f-8910-abc                                           |
| Properties        | : | Microsoft.Azure.Commands.RecoveryServices.ARSVaultProperties |

## Installing the Azure Backup agent on a DPM Server

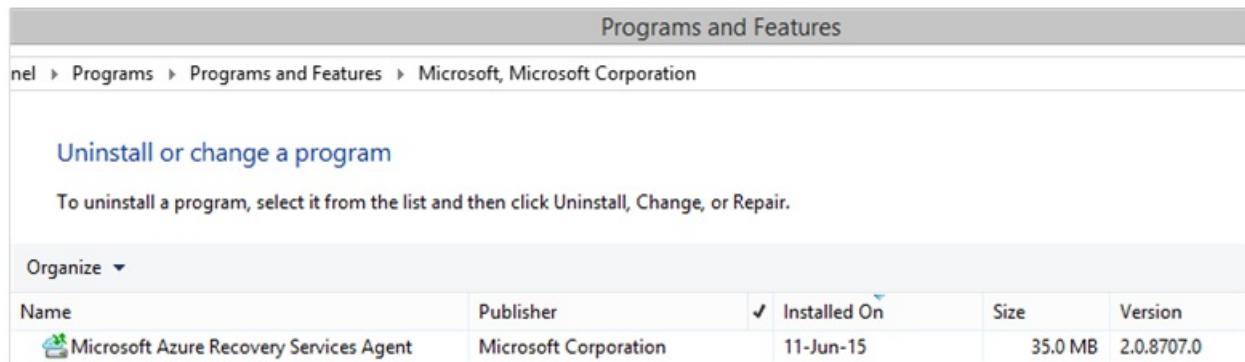
Before you install the Azure Backup agent, you need to have the installer downloaded and present on the Windows Server. You can get the latest version of the installer from the [Microsoft Download Center](#) or from the Recovery Services vault's Dashboard page. Save the installer to an easily accessible location like \*C:\Downloads\*.

To install the agent, run the following command in an elevated PowerShell console **on the DPM server**:

```
MARSAgentInstaller.exe /q
```

This installs the agent with all the default options. The installation takes a few minutes in the background. If you do not specify the */nu* option the **Windows Update** window opens at the end of the installation to check for any updates.

The agent shows up in the list of installed programs. To see the list of installed programs, go to **Control Panel > Programs > Programs and Features**.



## Installation options

To see all the options available via the command line, use the following command:

```
MARSAgentInstaller.exe /?
```

The available options include:

| OPTION        | DETAILS                                                     | DEFAULT                                                          |
|---------------|-------------------------------------------------------------|------------------------------------------------------------------|
| /q            | Quiet installation                                          | -                                                                |
| /p:"location" | Path to the installation folder for the Azure Backup agent. | C:\Program Files\Microsoft Azure Recovery Services Agent         |
| /s:"location" | Path to the cache folder for the Azure Backup agent.        | C:\Program Files\Microsoft Azure Recovery Services Agent\Scratch |
| /m            | Opt-in to Microsoft Update                                  | -                                                                |
| /nu           | Do not Check for updates after installation is complete     | -                                                                |
| /d            | Uninstalls Microsoft Azure Recovery Services Agent          | -                                                                |
| /ph           | Proxy Host Address                                          | -                                                                |
| /po           | Proxy Host Port Number                                      | -                                                                |
| /pu           | Proxy Host UserName                                         | -                                                                |
| /pw           | Proxy Password                                              | -                                                                |

# Registering DPM to a Recovery Services Vault

After you created the Recovery Services vault, download the latest agent and the vault credentials and store it in a convenient location like C:\Downloads.

```
$credspath = "C:\downloads"
$credsfilename = Get-AzRecoveryServicesVaultSettingsFile -Backup -Vault $vault1 -Path $credspath
$credsfilename
```

```
C:\downloads\testvault_Sun Apr 10 2016.VaultCredentials
```

On the DPM server, run the [Start-OBRegistration](#) cmdlet to register the machine with the vault.

```
$cred = $credspath + $credsfilename
Start-OBRegistration-VaultCredentials $cred -Confirm:$false
```

```
CertThumbprint : 7a2ef2caa2e74b6ed1222a5e89288ddad438df2
SubscriptionID : ef4ab577-c2c0-43e4-af80-af49f485f3d1
ServiceResourceName: testvault
Region : West US
Machine registration succeeded.
```

## Initial configuration settings

Once the DPM Server is registered with the Recovery Services vault, it starts with default subscription settings. These subscription settings include Networking, Encryption and the Staging area. To change subscription settings you need to first get a handle on the existing (default) settings using the [Get-DPMCloudSubscriptionSetting](#) cmdlet:

```
$setting = Get-DPMCloudSubscriptionSetting -DPMServerName "TestingServer"
```

All modifications are made to this local PowerShell object `$setting` and then the full object is committed to DPM and Azure Backup to save them using the [Set-DPMCloudSubscriptionSetting](#) cmdlet. You need to use the `-Commit` flag to ensure that the changes are persisted. The settings will not be applied and used by Azure Backup unless committed.

```
Set-DPMCloudSubscriptionSetting -DPMServerName "TestingServer" -SubscriptionSetting $setting -Commit
```

## Networking

If the connectivity of the DPM machine to the Azure Backup service on the internet is through a proxy server, then the proxy server settings should be provided for successful backups. This is done by using the `-ProxyServer` and `-ProxyPort`, `-ProxyUsername` and the `ProxyPassword` parameters with the [Set-DPMCloudSubscriptionSetting](#) cmdlet. In this example, there is no proxy server so we are explicitly clearing any proxy-related information.

```
Set-DPMCloudSubscriptionSetting -DPMServerName "TestingServer" -SubscriptionSetting $setting -NoProxy
```

Bandwidth usage can also be controlled with options of `-WorkHourBandwidth` and `-NonWorkHourBandwidth` for a given set of days of the week. In this example, we are not setting any throttling.

```
Set-DPMCloudSubscriptionSetting -DPMServerName "TestingServer" -SubscriptionSetting $setting -NoThrottle
```

## Configuring the staging Area

The Azure Backup agent running on the DPM server needs temporary storage for data restored from the cloud (local staging area). Configure the staging area using the [Set-DPMCloudSubscriptionSetting](#) cmdlet and the `-StagingAreaPath` parameter.

```
Set-DPMCloudSubscriptionSetting -DPMServerName "TestingServer" -SubscriptionSetting $setting -StagingAreaPath "C:\StagingArea"
```

In the example above, the staging area will be set to `C:\StagingArea` in the PowerShell object `$setting`. Ensure that the specified folder already exists, or else the final commit of the subscription settings will fail.

### Encryption settings

The backup data sent to Azure Backup is encrypted to protect the confidentiality of the data. The encryption passphrase is the "password" to decrypt the data at the time of restore. It is important to keep this information safe and secure once it is set.

In the example below, the first command converts the string `passphrase123456789` to a secure string and assigns the secure string to the variable named `$Passphrase`. The second command sets the secure string in `$Passphrase` as the password for encrypting backups.

```
$Passphrase = ConvertTo-SecureString -string "passphrase123456789" -AsPlainText -Force
Set-DPMCloudSubscriptionSetting -DPMServerName "TestingServer" -SubscriptionSetting $setting -EncryptionPassphrase $Passphrase
```

#### IMPORTANT

Keep the passphrase information safe and secure once it is set. You will not be able to restore data from Azure without this passphrase.

At this point, you should have made all the required changes to the `$setting` object. Remember to commit the changes.

```
Set-DPMCloudSubscriptionSetting -DPMServerName "TestingServer" -SubscriptionSetting $setting -Commit
```

## Protect data to Azure Backup

In this section, you will add a production server to DPM and then protect the data to local DPM storage and then to Azure Backup. In the examples, we will demonstrate how to back up files and folders. The logic can easily be extended to backup any DPM-supported data source. All your DPM backups are governed by a Protection Group (PG) with four parts:

1. **Group members** is a list of all the protectable objects (also known as *Datasources* in DPM) that you want to protect in the same protection group. For example, you may want to protect production VMs in one protection group and SQL Server databases in another protection group as they may have different backup requirements. Before you can back up any datasource on a production server you need to make sure the DPM Agent is installed on the server and is managed by DPM. Follow the steps for [installing the DPM Agent](#) and linking it to the appropriate DPM Server.

2. **Data protection method** specifies the target backup locations - tape, disk, and cloud. In our example we will protect data to the local disk and to the cloud.
3. A **backup schedule** that specifies when backups need to be taken and how often the data should be synchronized between the DPM Server and the production server.
4. A **retention schedule** that specifies how long to retain the recovery points in Azure.

### **Creating a protection group**

Start by creating a new Protection Group using the [New-DPMProtectionGroup](#) cmdlet.

```
$PG = New-DPMProtectionGroup -DPMServerName "TestingServer" -Name "ProtectGroup01"
```

The above cmdlet will create a Protection Group named *ProtectGroup01*. An existing protection group can also be modified later to add backup to the Azure cloud. However, to make any changes to the Protection Group - new or existing - we need to get a handle on a *modifiable* object using the [Get-DPMModifiableProtectionGroup](#) cmdlet.

```
$MPG = Get-ModifiableProtectionGroup $PG
```

### **Adding group members to the Protection Group**

Each DPM Agent knows the list of datasources on the server that it is installed on. To add a datasource to the Protection Group, the DPM Agent needs to first send a list of the datasources back to the DPM server. One or more datasources are then selected and added to the Protection Group. The PowerShell steps needed to achieve this are:

1. Fetch a list of all servers managed by DPM through the DPM Agent.
2. Choose a specific server.
3. Fetch a list of all datasources on the server.
4. Choose one or more datasources and add them to the Protection Group

The list of servers on which the DPM Agent is installed and is being managed by the DPM Server is acquired with the [Get-DPMProductionServer](#) cmdlet. In this example we will filter and only configure PS with name *productionserver01* for backup.

```
$server = Get-ProductionServer -DPMServerName "TestingServer" | Where-Object {($_.servername) -contains "productionserver01"}
```

Now fetch the list of datasources on `$server` using the [Get-DPMDataSource](#) cmdlet. In this example we are filtering for the volume *D:\* that we want to configure for backup. This datasource is then added to the Protection Group using the [Add-DPMChildDatasource](#) cmdlet. Remember to use the *modifiable* protection group object `$MPG` to make the additions.

```
$DS = Get-Datasource -ProductionServer $server -Inquire | Where-Object { $_.Name -contains "D:\" }

Add-DPMChildDatasource -ProtectionGroup $MPG -ChildDatasource $DS
```

Repeat this step as many times as required, until you have added all the chosen datasources to the protection group. You can also start with just one datasource, and complete the workflow for creating the Protection Group, and at a later point add more datasources to the Protection Group.

### **Selecting the data protection method**

Once the datasources have been added to the Protection Group, the next step is to specify the protection method using the [Set-DPMProtectionType](#) cmdlet. In this example, the Protection Group is setup for local disk and cloud

backup. You also need to specify the datasource that you want to protect to cloud using the [Add-DPMChildDatasource](#) cmdlet with -Online flag.

```
Set-DPMProtectionType -ProtectionGroup $MPG -ShortTerm Disk -LongTerm Online
Add-DPMChildDatasource -ProtectionGroup $MPG -ChildDatasource $DS -Online
```

## Setting the retention range

Set the retention for the backup points using the [Set-DPMPolicyObjective](#) cmdlet. While it might seem odd to set the retention before the backup schedule has been defined, using the [Set-DPMPolicyObjective](#) cmdlet automatically sets a default backup schedule that can then be modified. It is always possible to set the backup schedule first and the retention policy after.

In the example below, the cmdlet sets the retention parameters for disk backups. This will retain backups for 10 days, and sync data every 6 hours between the production server and the DPM server. The

[SynchronizationFrequencyMinutes](#) doesn't define how often a backup point is created, but how often data is copied to the DPM server. This setting prevents backups from becoming too large.

```
Set-DPMPolicyObjective -ProtectionGroup $MPG -RetentionRangeInDays 10 -SynchronizationFrequencyMinutes 360
```

For backups going to Azure (DPM refers to them as Online backups) the retention ranges can be configured for [long term retention using a Grandfather-Father-Son scheme \(GFS\)](#). That is, you can define a combined retention policy involving daily, weekly, monthly and yearly retention policies. In this example, we create an array representing the complex retention scheme that we want, and then configure the retention range using the [Set-DPMPolicyObjective](#) cmdlet.

```
$RRList = @()
$RRList += (New-Object -TypeName Microsoft.Internal.EnterpriseStorage.Dls.UI.ObjectModel.OMCommon.RetentionRange -ArgumentList 180, Days)
$RRList += (New-Object -TypeName Microsoft.Internal.EnterpriseStorage.Dls.UI.ObjectModel.OMCommon.RetentionRange -ArgumentList 104, Weeks)
$RRList += (New-Object -TypeName Microsoft.Internal.EnterpriseStorage.Dls.UI.ObjectModel.OMCommon.RetentionRange -ArgumentList 60, Month)
$RRList += (New-Object -TypeName Microsoft.Internal.EnterpriseStorage.Dls.UI.ObjectModel.OMCommon.RetentionRange -ArgumentList 10, Years)
Set-DPMPolicyObjective -ProtectionGroup $MPG -OnlineRetentionRangeList $RRList
```

## Set the backup schedule

DPM sets a default backup schedule automatically if you specify the protection objective using the [Set-DPMPolicyObjective](#) cmdlet. To change the default schedules, use the [Get-DPMPolicySchedule](#) cmdlet followed by the [Set-DPMPolicySchedule](#) cmdlet.

```
$onlineSch = Get-DPMPolicySchedule -ProtectionGroup $mpg -LongTerm Online
Set-DPMPolicySchedule -ProtectionGroup $MPG -Schedule $onlineSch[0] -TimesOfDay 02:00
Set-DPMPolicySchedule -ProtectionGroup $MPG -Schedule $onlineSch[1] -TimesOfDay 02:00 -DaysOfWeek Sa,Su -
Interval 1
Set-DPMPolicySchedule -ProtectionGroup $MPG -Schedule $onlineSch[2] -TimesOfDay 02:00 -RelativeIntervals
First,Third -DaysOfWeek Sa
Set-DPMPolicySchedule -ProtectionGroup $MPG -Schedule $onlineSch[3] -TimesOfDay 02:00 -DaysOfMonth 2,5,8,9 -
Months Jan,Jul
Set-DPMProtectionGroup -ProtectionGroup $MPG
```

In the above example, [\\$onlineSch](#) is an array with four elements that contains the existing online protection schedule for the Protection Group in the GFS scheme:

1. [\\$onlineSch\[0\]](#) contains the daily schedule

2. `$onlineSch[1]` contains the weekly schedule
3. `$onlineSch[2]` contains the monthly schedule
4. `$onlineSch[3]` contains the yearly schedule

So if you need to modify the weekly schedule, you need to refer to the `$onlineSch[1]`.

### Initial backup

When backing up a datasource for the first time, DPM needs creates initial replica that creates a full copy of the datasource to be protected on DPM replica volume. This activity can either be scheduled for a specific time, or can be triggered manually, using the [Set-DPMReplicaCreationMethod](#) cmdlet with the parameter `-NOW`.

```
Set-DPMReplicaCreationMethod -ProtectionGroup $MPG -NOW
```

### Changing the size of DPM Replica & recovery point volume

You can also change the size of DPM Replica volume and Shadow Copy volume using [Set-DPMDatasourceDiskAllocation](#) cmdlet as in the following example: `Get-DatasourceDiskAllocation -Datasource $DS Set-DatasourceDiskAllocation -Datasource $DS -ProtectionGroup $MPG -manual -ReplicaArea (2gb) -ShadowCopyArea (2gb)`

### Committing the changes to the Protection Group

Finally, the changes need to be committed before DPM can take the backup per the new Protection Group configuration. This can be achieved using the [Set-DPMProtectionGroup](#) cmdlet.

```
Set-DPMProtectionGroup -ProtectionGroup $MPG
```

## View the backup points

You can use the [Get-DPMRecoveryPoint](#) cmdlet to get a list of all recovery points for a datasource. In this example, we will:

- fetch all the PGs on the DPM server and stored in an array `$PG`
- get the datasources corresponding to the `$PG[0]`
- get all the recovery points for a datasource.

```
$PG = Get-DPMProtectionGroup -DPMServerName "TestingServer"
$DS = Get-DPMDatasource -ProtectionGroup $PG[0]
$RecoveryPoints = Get-DPMRecoverypoint -Datasource $DS[0] -Online
```

## Restore data protected on Azure

Restoring data is a combination of a `RecoverableItem` object and a `RecoveryOption` object. In the previous section, we got a list of the backup points for a datasource.

In the example below, we demonstrate how to restore a Hyper-V virtual machine from Azure Backup by combining backup points with the target for recovery. This example includes:

- Creating a recovery option using the [New-DPMRecoveryOption](#) cmdlet.
- Fetching the array of backup points using the [Get-DPMRecoveryPoint](#) cmdlet.
- Choosing a backup point to restore from.

```
$RecoveryOption = New-DPMRecoveryOption -HyperVDataSource -TargetServer "HVDCenter02" -RecoveryLocation
AlternateHyperVServer -RecoveryType Recover -TargetLocation "C:\VMRecovery"

$PG = Get-DPMProtectionGroup -DPMServerName "TestingServer"
$DS = Get-DPMDatasource -ProtectionGroup $PG[0]
$RecoveryPoints = Get-DPMRecoverypoint -Datasource $DS[0] -Online

Restore-DPMRecoverableItem -RecoverableItem $RecoveryPoints[0] -RecoveryOption $RecoveryOption
```

The commands can easily be extended for any datasource type.

## Next steps

- For more information about DPM to Azure Backup see [Introduction to DPM Backup](#)

# Deploy and manage backup to Azure for Windows Server/Windows Client using PowerShell

2/26/2020 • 16 minutes to read • [Edit Online](#)

This article shows you how to use PowerShell for setting up Azure Backup on Windows Server or a Windows client, and managing backup and recovery.

## Install Azure PowerShell

### NOTE

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

To get started, [install the latest PowerShell release](#).

## Create a recovery services vault

The following steps lead you through creating a Recovery Services vault. A Recovery Services vault is different than a Backup vault.

1. If you are using Azure Backup for the first time, you must use the **Register-AzResourceProvider** cmdlet to register the Azure Recovery Service provider with your subscription.

```
Register-AzResourceProvider -ProviderNamespace "Microsoft.RecoveryServices"
```

2. The Recovery Services vault is an ARM resource, so you need to place it within a Resource Group. You can use an existing resource group, or create a new one. When creating a new resource group, specify the name and location for the resource group.

```
New-AzResourceGroup -Name "test-rg" -Location "WestUS"
```

3. Use the **New-AzRecoveryServicesVault** cmdlet to create the new vault. Be sure to specify the same location for the vault as was used for the resource group.

```
New-AzRecoveryServicesVault -Name "testvault" -ResourceGroupName "test-rg" -Location "WestUS"
```

4. Specify the type of storage redundancy to use; you can use [Locally Redundant Storage \(LRS\)](#) or [Geo Redundant Storage \(GRS\)](#). The following example shows the -BackupStorageRedundancy option for testVault is set to GeoRedundant.

**TIP**

Many Azure Backup cmdlets require the Recovery Services vault object as an input. For this reason, it is convenient to store the Backup Recovery Services vault object in a variable.

```
$Vault1 = Get-AzRecoveryServicesVault -Name "testVault"
Set-AzRecoveryServicesBackupProperties -Vault $Vault1 -BackupStorageRedundancy GeoRedundant
```

## View the vaults in a subscription

Use **Get-AzRecoveryServicesVault** to view the list of all vaults in the current subscription. You can use this command to check that a new vault was created, or to see what vaults are available in the subscription.

Run the command, **Get-AzRecoveryServicesVault**, and all vaults in the subscription are listed.

```
Get-AzRecoveryServicesVault
```

|                   |   |                                                              |
|-------------------|---|--------------------------------------------------------------|
| Name              | : | Contoso-vault                                                |
| ID                | : | /subscriptions/1234                                          |
| Type              | : | Microsoft.RecoveryServices/vaults                            |
| Location          | : | WestUS                                                       |
| ResourceGroupName | : | Contoso-docs-rg                                              |
| SubscriptionId    | : | 1234-567f-8910-abc                                           |
| Properties        | : | Microsoft.Azure.Commands.RecoveryServices.ARSVaultProperties |

## Upgrade the MARS agent

Versions of the Microsoft Azure Recovery Service (MARS) agent below 2.0.9083.0 have a dependency on the Azure Access Control service (ACS). The MARS agent is also referred to as the Azure Backup agent. In 2018, Azure [deprecated the Azure Access Control service \(ACS\)](#). Beginning March 19, 2018, all versions of the MARS agent below 2.0.9083.0 will experience backup failures. To avoid or resolve backup failures, [upgrade your MARS agent to the latest version](#). To identify servers that require a MARS agent upgrade, follow the steps in the [Backup blog for upgrading MARS agents](#). The MARS agent is used to back up files and folders, and system state data to Azure. System Center DPM and Azure Backup Server use the MARS agent to back up data to Azure.

## Installing the Azure Backup agent

Before you install the Azure Backup agent, you need to have the installer downloaded and present on the Windows Server. You can get the latest version of the installer from the [Microsoft Download Center](#) or from the Recovery Services vault's Dashboard page. Save the installer to an easily accessible location like \*C:\Downloads\*.

Alternatively, use PowerShell to get the downloader:

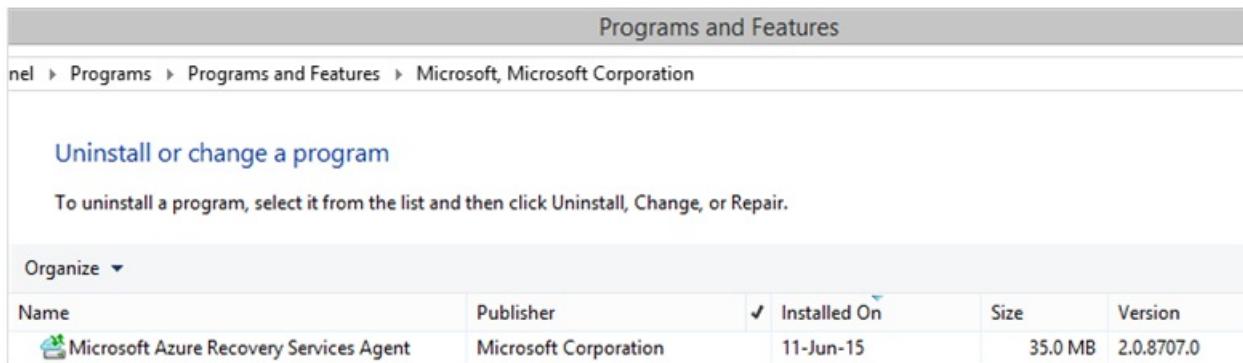
```
$MarsAURL = 'https://aka.ms/Azurebackup_Agent'
$WC = New-Object System.Net.WebClient
$WC.DownloadFile($MarsAURL, 'C:\downloads\MARSAgentInstaller.EXE')
C:\Downloads\MARSAgentInstaller.EXE /q
```

To install the agent, run the following command in an elevated PowerShell console:

```
MARSAgentInstaller.exe /q
```

This installs the agent with all the default options. The installation takes a few minutes in the background. If you do not specify the /nu option, then the **Windows Update** window will open at the end of the installation to check for any updates. Once installed, the agent will show in the list of installed programs.

To see the list of installed programs, go to **Control Panel > Programs > Programs and Features**.



The screenshot shows the Windows Control Panel's 'Programs and Features' section. At the top, it says 'Programs and Features'. Below that, the path 'Control Panel > Programs > Programs and Features > Microsoft, Microsoft Corporation' is shown. Underneath, there's a heading 'Uninstall or change a program' with the instruction 'To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.' A table lists the installed program: Microsoft Azure Recovery Services Agent by Microsoft Corporation, installed on 11-Jun-15, 35.0 MB, version 2.0.8707.0. There is an 'Organize' dropdown menu above the table.

## Installation options

To see all the options available via the command line, use the following command:

```
MARSAgentInstaller.exe /?
```

The available options include:

| OPTION        | DETAILS                                                     | DEFAULT                                                          |
|---------------|-------------------------------------------------------------|------------------------------------------------------------------|
| /q            | Quiet installation                                          | -                                                                |
| /p:"location" | Path to the installation folder for the Azure Backup agent. | C:\Program Files\Microsoft Azure Recovery Services Agent         |
| /s:"location" | Path to the cache folder for the Azure Backup agent.        | C:\Program Files\Microsoft Azure Recovery Services Agent\Scratch |
| /m            | Opt-in to Microsoft Update                                  | -                                                                |
| /nu           | Do not Check for updates after installation is complete     | -                                                                |
| /d            | Uninstalls Microsoft Azure Recovery Services Agent          | -                                                                |
| /ph           | Proxy Host Address                                          | -                                                                |
| /po           | Proxy Host Port Number                                      | -                                                                |
| /pu           | Proxy Host UserName                                         | -                                                                |
| /pw           | Proxy Password                                              | -                                                                |

## Registering Windows Server or Windows client machine to a Recovery Services Vault

After you created the Recovery Services vault, download the latest agent and the vault credentials and store it in a

convenient location like C:\Downloads.

```
$credsPath = "C:\downloads"
$credsFilename = Get-AzRecoveryServicesVaultSettingsFile -Backup -Vault $Vault1 -Path $credsPath
```

## Registering using the PS Az module

### NOTE

A bug with generation of vault certificate is fixed in Az 3.5.0 release. Use Az 3.5.0 release version or greater to download a vault certificate.

In the latest Az module of Powershell, due to underlying platform limitations, downloading the vault credentials requires a self-signed certificate. The following example shows how to provide a self-signed certificate and download the vault credentials.

```
$dt = $(Get-Date).ToString("M-d-yyyy")
$cert = New-SelfSignedCertificate -CertStoreLocation Cert:\CurrentUser\My -FriendlyName 'test-
vaultcredentials' -subject "Windows Azure Tools" -KeyExportPolicy Exportable -NotAfter $($Get-
Date).AddHours(48) -NotBefore $($Get-Date).AddHours(-24) -KeyProtection None -KeyUsage None -TextExtension
@("2.5.29.37={text}1.3.6.1.5.5.7.3.2") -Provider "Microsoft Enhanced Cryptographic Provider v1.0"
$certificate =
[convert]::ToBase64String($cert.Export([System.Security.Cryptography.X509Certificates.X509ContentType]::Pfx))
$credsFilename = Get-AzRecoveryServicesVaultSettingsFile -Backup -Vault $Vault -Path $credsPath -Certificate
$certificate
```

On the Windows Server or Windows client machine, run the [Start-OBRegistration](#) cmdlet to register the machine with the vault. This, and other cmdlets used for backup, are from the **MSONLINE** module, which the Mars AgentInstaller added as part of the installation process.

The Agent installer does not update the \$Env:PSModulePath variable. This means module auto-load fails. To resolve this, you can do the following:

```
$Env:PSModulePath += 'C:\Program Files\Microsoft Azure Recovery Services Agent\bin\Modules'
```

Alternatively, you can manually load the module in your script as follows:

```
Import-Module -Name 'C:\Program Files\Microsoft Azure Recovery Services Agent\bin\Modules\MSOnlineBackup'
```

Once you load the Online Backup cmdlets, you register the vault credentials:

```
Start-OBRegistration -VaultCredentials $credsFilename.FilePath -Confirm:$false
```

```
CertThumbprint : 7a2ef2caa2e74b6ed1222a5e89288ddad438df2
SubscriptionID : ef4ab577-c2c0-43e4-af80-af49f485f3d1
ServiceResourceName : testvault
Region : WestUS
Machine registration succeeded.
```

### IMPORTANT

Do not use relative paths to specify the vault credentials file. You must provide an absolute path as an input to the cmdlet.

## Networking settings

When the connectivity of the Windows machine to the internet is through a proxy server, the proxy settings can also be provided to the agent. In this example, there is no proxy server, so we are explicitly clearing any proxy-related information.

Bandwidth usage can also be controlled with the options of `work hour bandwidth` and `non-work hour bandwidth` for a given set of days of the week.

Setting the proxy and bandwidth details is done using the [Set-OBMachineSetting](#) cmdlet:

```
Set-OBMachineSetting -NoProxy
```

```
Server properties updated successfully.
```

```
Set-OBMachineSetting -NoThrottle
```

```
Server properties updated successfully.
```

## Encryption settings

The backup data sent to Azure Backup is encrypted to protect the confidentiality of the data. The encryption passphrase is the "password" to decrypt the data at the time of restore.

You must generate a security pin by selecting **Generate**, under **Settings > Properties > Security PIN** in the **Recovery Services vault** section of the Azure portal. Then, use this as the `<generatedPIN>` in the command:

```
$PassPhrase = ConvertTo-SecureString -String "Complex!123_STRING" -AsPlainText -Force
Set-OBMachineSetting -EncryptionPassPhrase $PassPhrase -SecurityPin "<generatedPIN>"
```

```
Server properties updated successfully
```

### IMPORTANT

Keep the passphrase information safe and secure once it is set. You can't restore data from Azure without this passphrase.

## Back up files and folders

All backups from Windows Servers and clients to Azure Backup are governed by a policy. The policy comprises three parts:

1. A **backup schedule** that specifies when backups need to be taken and synchronized with the service.
2. A **retention schedule** that specifies how long to retain the recovery points in Azure.
3. A **file inclusion/exclusion specification** that dictates what should be backed up.

In this document, since we're automating backup, we'll assume nothing has been configured. We begin by creating a new backup policy using the [New-OBPolicy](#) cmdlet.

```
$NewPolicy = New-OBPolicy
```

At this time the policy is empty and other cmdlets are needed to define what items will be included or excluded, when backups will run, and where the backups will be stored.

### Configuring the backup schedule

The first of the three parts of a policy is the backup schedule, which is created using the [New-OBSchedule](#) cmdlet. The backup schedule defines when backups need to be taken. When creating a schedule, you need to specify two input parameters:

- **Days of the week** that the backup should run. You can run the backup job on just one day, or every day of the week, or any combination in between.
- **Times of the day** when the backup should run. You can define up to three different times of the day when the backup will be triggered.

For instance, you could configure a backup policy that runs at 4PM every Saturday and Sunday.

```
$Schedule = New-OBSchedule -DaysOfWeek Saturday, Sunday -TimesOfDay 16:00
```

The backup schedule needs to be associated with a policy, and this can be achieved by using the [Set-OBSchedule](#) cmdlet.

```
Set-OBSchedule -Policy $NewPolicy -Schedule $Schedule
```

```
BackupSchedule : 4:00 PM Saturday, Sunday, Every 1 week(s) DsList : PolicyName : RetentionPolicy : State : New
PolicyState : Valid
```

### Configuring a retention policy

The retention policy defines how long recovery points created from backup jobs are retained. When creating a new retention policy using the [New-OBRetentionPolicy](#) cmdlet, you can specify the number of days that the backup recovery points need to be retained with Azure Backup. The example below sets a retention policy of seven days.

```
$RetentionPolicy = New-OBRetentionPolicy -RetentionDays 7
```

The retention policy must be associated with the main policy using the cmdlet [Set-OBRetentionPolicy](#):

```
Set-OBRetentionPolicy -Policy $NewPolicy -RetentionPolicy $RetentionPolicy
```

```

BackupSchedule : 4:00 PM
 Saturday, Sunday,
 Every 1 week(s)
DsList :
PolicyName :
RetentionPolicy : Retention Days : 7

 WeeklyLTRSchedule :
 Weekly schedule is not set

 MonthlyLTRSchedule :
 Monthly schedule is not set

 YearlyLTRSchedule :
 Yearly schedule is not set

State : New
PolicyState : Valid

```

### Including and excluding files to be backed up

An `OBFileSpec` object defines the files to be included and excluded in a backup. This is a set of rules that scope out the protected files and folders on a machine. You can have as many file inclusion or exclusion rules as required, and associate them with a policy. When creating a new `OBFileSpec` object, you can:

- Specify the files and folders to be included
- Specify the files and folders to be excluded
- Specify recursive backup of data in a folder (or) whether only the top-level files in the specified folder should be backed up.

The latter is achieved by using the `-NonRecursive` flag in the `New-OBFileSpec` command.

In the example below, we'll back up volume C: and D: and exclude the OS binaries in the Windows folder and any temporary folders. To do so, we'll create two file specifications using the `New-OBFileSpec` cmdlet - one for inclusion and one for exclusion. Once the file specifications have been created, they're associated with the policy using the `Add-OBFileSpec` cmdlet.

```

$Inclusions = New-OBFileSpec -FileSpec @("C:\", "D:\")
$Exclusions = New-OBFileSpec -FileSpec @("C:\windows", "C:\temp") -Exclude
Add-OBFileSpec -Policy $NewPolicy -FileSpec $Inclusions

```

```
BackupSchedule : 4:00 PM
 Saturday, Sunday,
 Every 1 week(s)
DsList : {DataSource
 DataSourceId:0
 Name:C:\FileSpec:FileSpec
 FileSpec:C:\FileSpec:FileSpec
 IsExclude:False
 IsRecursive:True

 , DataSource
 DataSourceId:0
 Name:D:\FileSpec:FileSpec
 FileSpec:D:\FileSpec:FileSpec
 IsExclude:False
 IsRecursive:True

}
PolicyName :
RetentionPolicy : Retention Days : 7

WeeklyLTRSchedule :
Weekly schedule is not set

MonthlyLTRSchedule :
Monthly schedule is not set

YearlyLTRSchedule :
Yearly schedule is not set

State : New
PolicyState : Valid
```

```
Add-OBFileSpec -Policy $NewPolicy -FileSpec $Exclusions
```

```

BackupSchedule : 4:00 PM
 Saturday, Sunday,
 Every 1 week(s)
DsList : {DataSource
 DataSourceId:0
 Name:C:\FileSpec:FileSpec
 FileSpec:C:\FileSpec
 IsExclude:False
 IsRecursive:True
 ,FileSpec
 FileSpec:C:\windows
 IsExclude:True
 IsRecursive:True
 ,FileSpec
 FileSpec:C:\temp
 IsExclude:True
 IsRecursive:True

 , DataSource
 DataSourceId:0
 Name:D:\FileSpec:FileSpec
 FileSpec:D:\FileSpec
 IsExclude:False
 IsRecursive:True

}
PolicyName :
RetentionPolicy : Retention Days : 7

WeeklyLTRSchedule :
Weekly schedule is not set

MonthlyLTRSchedule :
Monthly schedule is not set

YearlyLTRSchedule :
Yearly schedule is not set

State : New
PolicyState : Valid

```

## Applying the policy

Now the policy object is complete and has an associated backup schedule, retention policy, and an inclusion/exclusion list of files. This policy can now be committed for Azure Backup to use. Before you apply the newly created policy, ensure that there are no existing backup policies associated with the server by using the [Remove-OBPolicy](#) cmdlet. Removing the policy will prompt for confirmation. To skip the confirmation, use the `-Confirm:$false` flag with the cmdlet.

```
Get-OBPolicy | Remove-OBPolicy
```

```
Microsoft Azure Backup Are you sure you want to remove this backup policy? This will delete all the backed up data. [Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"):
```

Committing the policy object is done using the [Set-OBPolicy](#) cmdlet. This will also ask for confirmation. To skip the confirmation, use the `-Confirm:$false` flag with the cmdlet.

```
Set-OBPolicy -Policy $NewPolicy
```

```

Microsoft Azure Backup Do you want to save this backup policy ? [Y] Yes [A] Yes to All [N] No [L] No to All
[S] Suspend [?] Help (default is "Y"):
BackupSchedule : 4:00 PM Saturday, Sunday, Every 1 week(s)
DsList : {DataSource
 DatasourceId:4508156004108672185
 Name:C:\FileSpec:FileSpec
 FileSpec:C:\IsExclude:False
 IsRecursive:True,
 FileSpec
 FileSpec:C:\windows
 IsExclude:True
 IsRecursive:True,
 FileSpec
 FileSpec:C:\temp
 IsExclude:True
 IsRecursive:True,
 DataSource
 DatasourceId:4508156005178868542
 Name:D:\FileSpec:FileSpec
 FileSpec:D:\IsExclude:False
 IsRecursive:True
 }
PolicyName : c2eb6568-8a06-49f4-a20e-3019ae411bac
RetentionPolicy : Retention Days : 7
 WeeklyLTRSchedule :
 Weekly schedule is not set

 MonthlyLTRSchedule :
 Monthly schedule is not set

 YearlyLTRSchedule :
 Yearly schedule is not set
State : Existing PolicyState : Valid

```

You can view the details of the existing backup policy using the [Get-OBPolicy](#) cmdlet. You can drill down further using the [Get-OBSchedule](#) cmdlet for the backup schedule and the [Get-OBRetentionPolicy](#) cmdlet for the retention policies

```
Get-OBPolicy | Get-OBSchedule
```

```

SchedulePolicyName : 71944081-9950-4f7e-841d-32f0a0a1359a
ScheduleRunDays : {Saturday, Sunday}
ScheduleRunTimes : {16:00:00}
State : Existing

```

```
Get-OBPolicy | Get-OBRetentionPolicy
```

```

RetentionDays : 7
RetentionPolicyName : ca3574ec-8331-46fd-a605-c01743a5265e
State : Existing

```

```
Get-OBPolicy | Get-OBFileSpec
```

```
FileName : *
FilePath : \?\Volume{b835d359-a1dd-11e2-be72-2016d8d89f0f}\
FileSpec : D:\\
IsExclude : False
IsRecursive : True

FileName : *
FilePath : \?\Volume{cdd41007-a22f-11e2-be6c-806e6f6e6963}\\
FileSpec : C:\\
IsExclude : False
IsRecursive : True

FileName : *
FilePath : \?\Volume{cdd41007-a22f-11e2-be6c-806e6f6e6963}\\windows
FileSpec : C:\\windows
IsExclude : True
IsRecursive : True

FileName : *
FilePath : \?\Volume{cdd41007-a22f-11e2-be6c-806e6f6e6963}\\temp
FileSpec : C:\\temp
IsExclude : True
IsRecursive : True
```

## Performing an on-demand backup

Once a backup policy has been set, the backups will occur per the schedule. Triggering an on-demand backup is also possible using the [Start-OBBackup](#) cmdlet:

```
Get-OBPolicy | Start-OBBackup
```

```
Initializing
Taking snapshot of volumes...
Preparing storage...
Generating backup metadata information and preparing the metadata VHD...
Data transfer is in progress. It might take longer since it is the first backup and all data needs to be transferred...
Data transfer completed and all backed up data is in the cloud. Verifying data integrity...
Data transfer completed
In progress...
Job completed.
The backup operation completed successfully.
```

## Back up Windows Server System State in MABS agent

This section covers the PowerShell command to set up System State in MABS agent

### Schedule

```
$sched = New-OBSchedule -DaysOfWeek Sunday,Monday,Tuesday,Wednesday,Thursday,Friday,Saturday -TimesOfDay 2:00
```

### Retention

```
$rtn = New-OBRetentionPolicy -RetentionDays 32 -RetentionWeeklyPolicy -RetentionWeeks 13 -WeekDaysOfWeek Sunday -WeekTimesOfDay 2:00 -RetentionMonthlyPolicy -RetentionMonths 13 -MonthDaysOfMonth 1 -MonthTimesOfDay 2:00
```

## Configuring schedule and retention

```
New-OBPolicy | Add-OBSchedule | Set-OBRetentionPolicy -RetentionPolicy $rtn | Set-OBSchedule -Schedule $sched | Set-OBSchedulePolicy
```

## Verifying the policy

```
Get-OBSchedulePolicy
```

# Restore data from Azure Backup

This section will guide you through the steps for automating recovery of data from Azure Backup. Doing so involves the following steps:

1. Pick the source volume
2. Choose a backup point to restore
3. Specify an item to restore
4. Trigger the restore process

## Picking the source volume

In order to restore an item from Azure Backup, you first need to identify the source of the item. Since we're executing the commands in the context of a Windows Server or a Windows client, the machine is already identified. The next step in identifying the source is to identify the volume containing it. A list of volumes or sources being backed up from this machine can be retrieved by executing the [Get-OBRecoverableSource](#) cmdlet. This command returns an array of all the sources backed up from this server/client.

```
$Source = Get-OBRecoverableSource
$Source
```

```
FriendlyName : C:\
RecoverySourceName : C:\
ServerName : myserver.microsoft.com

FriendlyName : D:\
RecoverySourceName : D:\
ServerName : myserver.microsoft.com
```

## Choosing a backup point from which to restore

You retrieve a list of backup points by executing the [Get-OBRecoverableItem](#) cmdlet with appropriate parameters. In our example, we'll choose the latest backup point for the source volume C: and use it to recover a specific file.

```
$Rps = Get-OBRecoverableItem $Source[0]
$Rps
```

```

IsDir : False
ItemNameFriendly : C:\Volume{297cbf7a-0000-0000-0000-401f00000000}\myserver.microsoft.com
ItemNameGuid : \\?\Volume{297cbf7a-0000-0000-0000-401f00000000}\myserver.microsoft.com
LocalMountPoint : C:\Volume{297cbf7a-0000-0000-0000-401f00000000}\myserver.microsoft.com
MountPointName : C:\Volume{297cbf7a-0000-0000-0000-401f00000000}\myserver.microsoft.com
Name : C:\Volume{297cbf7a-0000-0000-0000-401f00000000}\myserver.microsoft.com
PointInTime : 10/17/2019 7:52:13 PM
ServerName : myserver.microsoft.com
ItemSize :
ItemLastModifiedTime :

IsDir : False
ItemNameFriendly : C:\Volume{297cbf7a-0000-0000-0000-401f00000000}\myserver.microsoft.com
ItemNameGuid : \\?\Volume{297cbf7a-0000-0000-0000-401f00000000}\myserver.microsoft.com
LocalMountPoint : C:\Volume{297cbf7a-0000-0000-0000-401f00000000}\myserver.microsoft.com
MountPointName : C:\Volume{297cbf7a-0000-0000-0000-401f00000000}\myserver.microsoft.com
Name : C:\Volume{297cbf7a-0000-0000-0000-401f00000000}\myserver.microsoft.com
PointInTime : 10/16/2019 7:00:19 PM
ServerName : myserver.microsoft.com
ItemSize :
ItemLastModifiedTime :

```

The object `$Rps` is an array of backup points. The first element is the latest point and the Nth element is the oldest point. To choose the latest point, we will use `$Rps[0]`.

### Specifying an item to restore

To restore a specific file, specify the file name relative to the root volume. For example, to retrieve C:\Test\Cat.jpg, execute the following command.

```

$item = New-OBRecoverableItem $Rps[0] "Test\cat.jpg" $FALSE
$item

```

```

IsDir : False
ItemNameFriendly : C:\Test\cat.jpg
ItemNameGuid :
LocalMountPoint : C:\Volume{297cbf7a-0000-0000-0000-401f00000000}\myserver.microsoft.com
MountPointName : C:\Volume{297cbf7a-0000-0000-0000-401f00000000}\myserver.microsoft.com
Name : cat.jpg
PointInTime : 10/17/2019 7:52:13 PM
ServerName : myserver.microsoft.com
ItemSize :
ItemLastModifiedTime : 21-Jun-14 6:43:02 AM

```

### Triggering the restore process

To trigger the restore process, we first need to specify the recovery options. This can be done by using the [New-OBRecoveryOption](#) cmdlet. For this example, let's assume that we want to restore the files to C:\temp. Let's also assume that we want to skip files that already exist on the destination folder C:\temp. To create such a recovery option, use the following command:

```

$RecoveryOption = New-OBRecoveryOption -DestinationPath "C:\temp" -OverwriteType Skip

```

Now trigger the restore process by using the [Start-OBRecovery](#) command on the selected `$item` from the output of the [Get-OBRecoverableItem](#) cmdlet:

```
Start-OBRecovery -RecoverableItem $Item -RecoveryOption $RecoveryOption
```

```
Estimating size of backup items...
Job completed.
The recovery operation completed successfully.
```

## Uninstalling the Azure Backup agent

Uninstalling the Azure Backup agent can be done by using the following command:

```
.\MARSInstaller.exe /d /q
```

Uninstalling the agent binaries from the machine has some consequences to consider:

- It removes the file-filter from the machine, and tracking of changes is stopped.
- All policy information is removed from the machine, but the policy information continues to be stored in the service.
- All backup schedules are removed, and no further backups are taken.

However, the data stored in Azure remains and is retained as per the retention policy setup by you. Older points are automatically aged out.

## Remote management

All the management around the Azure Backup agent, policies, and data sources can be done remotely through PowerShell. The machine that will be managed remotely needs to be prepared correctly.

By default, the WinRM service is configured for manual startup. The startup type must be set to *Automatic* and the service should be started. To verify that the WinRM service is running, the value of the Status property should be *Running*.

```
Get-Service -Name WinRM
```

| Status  | Name  | DisplayName                            |
|---------|-------|----------------------------------------|
| -----   | ----- | -----                                  |
| Running | winrm | Windows Remote Management (WS-Manag... |

PowerShell should be configured for remoting.

```
Enable-PSRemoting -Force
```

```
WinRM is already set up to receive requests on this computer.
WinRM has been updated for remote management.
WinRM firewall exception enabled.
```

```
Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Force
```

The machine can now be managed remotely - starting from the installation of the agent. For example, the following script copies the agent to the remote machine and installs it.

```
$DLoc = "\\\$REMOTE SERVER01\c$\Windows\Temp"
$Agent = "\\\$REMOTE SERVER01\c$\Windows\Temp\MARS Agent Installer.exe"
$Args = "/q"
Copy-Item "C:\Downloads\MARS Agent Installer.exe" -Destination $DLoc -Force

$Session = New-PSSession -ComputerName REMOTESERVER01
Invoke-Command -Session $Session -Script { param($D, $A) Start-Process -FilePath $D $A -Wait } -ArgumentList
$Agent, $Args
```

## Next steps

For more information about Azure Backup for Windows Server/Client:

- [Introduction to Azure Backup](#)
- [Back up Windows Servers](#)

# Back up and restore SQL databases in Azure VMs with PowerShell

11/18/2019 • 16 minutes to read • [Edit Online](#)

This article describes how to use Azure PowerShell to back up and recover a SQL DB within an Azure VM using [Azure Backup Recovery Services vault](#).

This article explains how to:

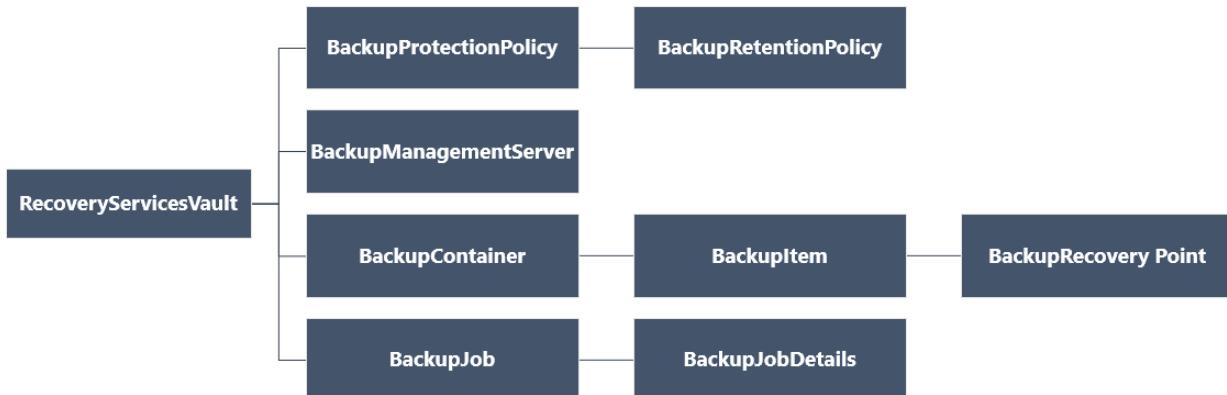
- Set up PowerShell and register the Azure Recovery Services Provider.
- Create a Recovery Services vault.
- Configure backup for SQL DB within an Azure VM.
- Run a backup job.
- Restore a backed up SQL DB.
- Monitor backup and restore jobs.

## Before you start

- [Learn more](#) about Recovery Services vaults.
- Read about the feature capabilities for [backing up SQL DBs within Azure VMs](#).
- Review the PowerShell object hierarchy for Recovery Services.

## Recovery Services object hierarchy

The object hierarchy is summarized in the following diagram.



Review the [Az.RecoveryServices cmdlet reference](#) reference in the Azure library.

## Set up and install

Set up PowerShell as follows:

1. [Download the latest version of Az PowerShell](#). The minimum version required is 1.5.0.
2. Find the Azure Backup PowerShell cmdlets with this command:

```
Get-Command *azrecoveryservices*
```

3. Review the aliases and cmdlets for Azure Backup and the Recovery Services vault. Here's an example of what you might see. It's not a complete list of cmdlets.

| CommandType | Name                                               | Version | Source              |
|-------------|----------------------------------------------------|---------|---------------------|
| Alias       | Get-AzRecoveryServicesAsrNotificationSetting       | 0.7.0   | Az.RecoveryServices |
| Alias       | Get-AzRecoveryServicesAsrVaultSettings             | 0.7.0   | Az.RecoveryServices |
| Alias       | Get-AzRecoveryServicesBackupProperties             | 0.7.0   | Az.RecoveryServices |
| Alias       | Set-AzRecoveryServicesAsrNotificationSetting       | 0.7.0   | Az.RecoveryServices |
| Alias       | Set-AzRecoveryServicesAsrVaultSettings             | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Backup-AzRecoveryServicesBackupItem                | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Disable-AzRecoveryServicesBackupProtection         | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Disable-AzRecoveryServicesBackupRPMountScript      | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Edit-AzRecoveryServicesAsrRecoveryPlan             | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Enable-AzRecoveryServicesBackupProtection          | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrAlertSetting              | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrEvent                     | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrFabric                    | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrJob                       | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrNetwork                   | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrNetworkMapping            | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrPolicy                    | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrProtectableItem           | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrProtectionContainer       | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrProtectionContainerMap... | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrRecoveryPlan              | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrRecoveryPoint             | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrReplicationProtectedItem  | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrServicesProvider          | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrStorageClassification     | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrStorageClassificationM... | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrVaultContext              | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesAsrvCenter                   | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupContainer              | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupItem                   | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupJob                    | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupJobDetails             | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupManagementServer       | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupProperty               | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupProtectionPolicy       | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupRecoveryPoint          | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupRetentionPolicyObject  | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupRPMountScript          | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupSchedulePolicyObject   | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesBackupStatus                 | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesVault                        | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Get-AzRecoveryServicesVaultSettingsFile            | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Import-AzRecoveryServicesAsrVaultSettingsFile      | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesAsrAzureToAzureDiskReplic... | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesAsrFabric                    | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesAsrNetworkMapping            | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesAsrPolicy                    | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesAsrProtectableItem           | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesAsrProtectionContainer       | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesAsrProtectionContainerMap... | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesAsrRecoveryPlan              | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesAsrReplicationProtectedItem  | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesAsrStorageClassificationM... | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesAsrvCenter                   | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesBackupProtectionPolicy       | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | New-AzRecoveryServicesVault                        | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Remove-AzRecoveryServicesAsrFabric                 | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Remove-AzRecoveryServicesAsrNetworkMapping         | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Remove-AzRecoveryServicesAsrPolicy                 | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Remove-AzRecoveryServicesAsrProtectionContainer    | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Remove-AzRecoveryServicesAsrProtectionContainer... | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Remove-AzRecoveryServicesAsrRecoveryPlan           | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Remove-AzRecoveryServicesAsrReplicationProtecte... | 0.7.0   | Az.RecoveryServices |
| Cmdlet      | Remove-AzRecoveryServicesAsrServicesProvider       | 0.7.0   | Az.RecoveryServices |

4. Sign in to your Azure account with **Connect-AzAccount**.
5. On the web page that appears, you're prompted to input your account credentials.
  - Alternately, you can include your account credentials as a parameter in the **Connect-AzAccount** cmdlet with **-Credential**.
  - If you're a CSP partner working for a tenant, specify the customer as a tenant, using their tenantID or tenant primary domain name. An example is **Connect-AzAccount -Tenant** fabrikam.com.
6. Associate the subscription you want to use with the account, because an account can have several

subscriptions.

```
Select-AzSubscription -SubscriptionName $SubscriptionName
```

7. If you're using Azure Backup for the first time, use the **Register-AzResourceProvider** cmdlet to register the Azure Recovery Services provider with your subscription.

```
Register-AzResourceProvider -ProviderNamespace "Microsoft.RecoveryServices"
```

8. Verify that the providers registered successfully:

```
Get-AzResourceProvider -ProviderNamespace "Microsoft.RecoveryServices"
```

9. In the command output, verify that **RegistrationState** changes to **Registered**. If it doesn't, run the **Register-AzResourceProvider** cmdlet again.

## Create a Recovery Services vault

Follow these steps to create a Recovery Services vault.

The Recovery Services vault is a Resource Manager resource, so you must place it within a resource group. You can use an existing resource group, or you can create a resource group with the **New-AzResourceGroup** cmdlet. When you create a resource group, specify the name and location for the resource group.

1. A vault is placed in a resource group. If you don't have an existing resource group, create a new one with the **New-AzResourceGroup**. In this example, we create a new resource group in the West US region.

```
New-AzResourceGroup -Name "test-rg" -Location "West US"
```

2. Use the **New-AzRecoveryServicesVault** cmdlet to create the vault. Specify the same location for the vault as was used for the resource group.

```
New-AzRecoveryServicesVault -Name "testvault" -ResourceGroupName "test-rg" -Location "West US"
```

3. Specify the type of redundancy to use for the vault storage.

- You can use [locally redundant storage](#) or [geo-redundant storage](#).
- The following example sets the **-BackupStorageRedundancy** option for the [Set-AzRecoveryServicesBackupProperty](#) cmd for **testvault** set to **GeoRedundant**.

```
$vault1 = Get-AzRecoveryServicesVault -Name "testvault"
Set-AzRecoveryServicesBackupProperties -Vault $vault1 -BackupStorageRedundancy GeoRedundant
```

### View the vaults in a subscription

To view all vaults in the subscription, use [Get-AzRecoveryServicesVault](#).

```
Get-AzRecoveryServicesVault
```

The output is similar to the following. The associated resource group and location are provided.

```
Name : Contoso-vault
ID : /subscriptions/1234
Type : Microsoft.RecoveryServices/vaults
Location : WestUS
ResourceGroupName : Contoso-docs-rg
SubscriptionId : 1234-567f-8910-abc
Properties : Microsoft.Azure.Commands.RecoveryServices.ARSVaultProperties
```

## Set the vault context

Store the vault object in a variable, and set the vault context.

- Many Azure Backup cmdlets require the Recovery Services vault object as an input, so it's convenient to store the vault object in a variable.
- The vault context is the type of data protected in the vault. Set it with [Set-AzRecoveryServicesVaultContext](#). After the context is set, it applies to all subsequent cmdlets.

The following example sets the vault context for **testvault**.

```
Get-AzRecoveryServicesVault -Name "testvault" | Set-AzRecoveryServicesVaultContext
```

## Fetch the vault ID

We plan on deprecating the vault context setting in accordance with Azure PowerShell guidelines. Instead, you can store or fetch the vault ID, and pass it to relevant commands, as follows:

```
$vaultID = Get-AzRecoveryServicesVault -ResourceGroupName "Contoso-docs-rg" -Name "testvault" | select -ExpandProperty ID
```

## Configure a backup policy

A backup policy specifies the schedule for backups, and how long backup recovery points should be kept:

- A backup policy is associated with at least one retention policy. A retention policy defines how long a recovery point is kept before it's deleted.
- View the default backup policy retention using [Get-AzRecoveryServicesBackupRetentionPolicyObject](#).
- View the default backup policy schedule using [Get-AzRecoveryServicesBackupSchedulePolicyObject](#).
- You use the [New-AzRecoveryServicesBackupProtectionPolicy](#) cmdlet to create a new backup policy. You input the schedule and retention policy objects.

By default, a start time is defined in the Schedule Policy Object. Use the following example to change the start time to the desired start time. The desired start time should be in UTC as well. The below example assumes the desired start time is 01:00 AM UTC for daily backups.

```
$schPol = Get-AzRecoveryServicesBackupSchedulePolicyObject -WorkloadType "MSSQL"
$UtcTime = Get-Date -Date "2019-03-20 01:30:00Z"
$UtcTime = $UtcTime.ToUniversalTime()
$schpol.ScheduleRunTimes[0] = $UtcTime
```

### IMPORTANT

You need to provide the start time in 30 minute multiples only. In the above example, it can be only "01:00:00" or "02:30:00". The start time cannot be "01:15:00"

The following example stores the schedule policy and the retention policy in variables. It then uses those variables as parameters for a new policy (**NewSQLPolicy**). **NewSQLPolicy** takes a daily "Full" backup, retains it for 180 days and takes a log backup every 2 hours

```
$schPol = Get-AzRecoveryServicesBackupSchedulePolicyObject -WorkloadType "MSSQL"
$retPol = Get-AzRecoveryServicesBackupRetentionPolicyObject -WorkloadType "MSSQL"
$NewSQLPolicy = New-AzRecoveryServicesBackupProtectionPolicy -Name "NewSQLPolicy" -WorkloadType "MSSQL" -
 RetentionPolicy $retPol -SchedulePolicy $schPol
```

The output is similar to the following.

| Name                 | WorkloadType       | BackupManagementType | BackupTime            | Frequency |
|----------------------|--------------------|----------------------|-----------------------|-----------|
| IsDifferentialBackup | IsLogBackupEnabled |                      |                       |           |
| Enabled              |                    |                      |                       |           |
| ---                  | -----              | -----                | -----                 | -----     |
| ---                  | ---                | ---                  | ---                   | ---       |
| NewSQLPolicy         | MSSQL              | AzureWorkload        | 3/15/2019 01:30:00 AM | Daily     |
| False                | True               |                      |                       |           |

## Enable backup

### Registering the SQL VM

For Azure VM backups and Azure File shares, Backup service can connect to these Azure Resource Manager resources and fetch the relevant details. Since SQL is an application within an Azure VM, Backup service needs permission to access the application and fetch the necessary details. In order to do that, you need to 'register' the Azure VM that contains the SQL application with a Recovery services vault. Once you register a SQL VM with a vault, you can protect the SQL DBs to that vault only. Use [Register-AzRecoveryServicesBackupContainer](#) PS cmdlet to register the VM.

```
$myVM = Get-AzVM -ResourceGroupName <VMRG Name> -Name <VMName>
Register-AzRecoveryServicesBackupContainer -ResourceId $myVM.ID -BackupManagementType AzureWorkload -
 WorkloadType MSSQL -VaultId $targetVault.ID -Force
```

The command will return a 'backup container' of this resource and the status will be 'registered'

#### NOTE

If the force parameter is not given, user is asked to confirm with a text 'Do you want to disable protection for this container'. Please ignore this text and say "Y" to confirm. This is a known issue and we are working to remove the text and the requirement for the force parameter.

### Fetching SQL DBs

Once the registration is done, Backup service will be able to list all the available SQL components within the VM. To view all the SQL components yet to be backed up to this vault use [Get-AzRecoveryServicesBackupProtectableItem](#) PS cmdlet

```
Get-AzRecoveryServicesBackupProtectableItem -WorkloadType MSSQL -VaultId $targetVault.ID
```

The output will show all unprotected SQL components across all SQL VMs registered to this vault with Item Type and ServerName. You can further filter to a particular SQL VM by passing the '-Container' parameter or use the combination of 'Name' and 'ServerName' along with ItemType flag to arrive at a unique SQL item.

```
$SQLDB = Get-AzRecoveryServicesBackupProtectableItem -workloadType MSSQL -ItemType SQLDataBase -VaultId $targetVault.ID -Name "<Item Name>" -ServerName "<Server Name>"
```

## Configuring backup

Now that we have the required SQL DB and the policy with which it needs to be backed up, we can use the [Enable-AzRecoveryServicesBackupProtection](#) cmdlet to configure backup for this SQL DB.

```
Enable-AzRecoveryServicesBackupProtection -ProtectableItem $SQLDB -Policy $NewSQLPolicy
```

The command waits until the configure backup is completed and returns the following output.

| WorkloadName                         | Operation       | Status    | StartTime            | EndTime              |
|--------------------------------------|-----------------|-----------|----------------------|----------------------|
| JobID                                |                 |           |                      |                      |
| master                               | ConfigureBackup | Completed | 3/18/2019 6:00:21 PM | 3/18/2019 6:01:35 PM |
| 654e8aa2-4096-402b-b5a9-e5e71a496c4e |                 |           |                      |                      |

## Fetching new SQL DBs

Once the machine is registered, Backup service will fetch the details of the DBs available then. If user adds SQL DBs/SQL instances to the registered machine later, one needs to manually trigger the backup service to perform a fresh 'inquiry' to get ALL the unprotected DBs (including the newly added ones) again. Use the [Initialize-AzRecoveryServicesBackupItem](#) PS cmdlet on the SQL VM to perform a fresh inquiry. The command waits until the operation is completed. Later use the [Get-AzRecoveryServicesBackupProtectableItem](#) PS cmdlet to get the list of latest unprotected SQL components

```
$SQLContainer = Get-AzRecoveryServicesBackupContainer -ContainerType AzureVMAppContainer -FriendlyName <VM name> -VaultId $targetvault.ID
Initialize-AzRecoveryServicesBackupProtectableItem -Container $SQLContainer -WorkloadType MSSQL -VaultId $targetvault.ID
Get-AzRecoveryServicesBackupProtectableItem -workloadType MSSQL -ItemType SQLDataBase -VaultId $targetVault.ID
```

Once the relevant protectable items are fetched, enable the backups as instructed in the [above section](#). If one doesn't want to manually detect new DBs, they can opt for autoprotection as explained [below](#).

## Enable autoprotection

A user can configure backup such that all DBs added in the future are automatically protected with a certain policy. To enable autoprotection, use [Enable-AzRecoveryServicesBackupAutoProtection](#) PS cmdlet.

Since the instruction is to back up all future DBs, the operation is done at a SQLInstance level.

```
$SQLInstance = Get-AzRecoveryServicesBackupProtectableItem -workloadType MSSQL -ItemType SQLInstance -VaultId $targetVault.ID -Name "<Protectable Item name>" -ServerName "<Server Name>"
Enable-AzRecoveryServicesBackupAutoProtection -InputItem $SQLInstance -BackupManagementType AzureWorkload -WorkloadType MSSQL -Policy $NewSQLPolicy -VaultId $targetvault.ID
```

Once the autoprotection intent is given, the inquiry into the machine to fetch newly added DBs takes place as a scheduled background task every 8 hours.

## Restore SQL DBs

Azure Backup can restore SQL Server databases that are running on Azure VMs as follows:

- Restore to a specific date or time (to the second) by using transaction log backups. Azure Backup automatically determines the appropriate full differential backup and the chain of log backups that are required to restore based on the selected time.
- Restore a specific full or differential backup to restore to a specific recovery point.

Check the prerequisites mentioned [here](#) before restoring SQL DBs.

First fetch the relevant backed up SQL DB using the [Get-AzRecoveryServicesBackupItem](#) PS cmdlet.

```
$bkpItem = Get-AzRecoveryServicesBackupItem -BackupManagementType AzureWorkload -WorkloadType MSSQL -Name "<backup item name>" -VaultId $targetVault.ID
```

### Fetch the relevant restore time

As outlined above, user can restore the backed-up SQL DB to a full/differential copy **OR** to a log point-in-time.

#### Fetch distinct recovery points

Use [Get-AzRecoveryServicesBackupRecoveryPoint](#) to fetch distinct (Full/differential) recovery points for a backed-up SQL DB.

```
$startDate = (Get-Date).AddDays(-7).ToUniversalTime()
$endDate = (Get-Date).ToUniversalTime()
Get-AzRecoveryServicesBackupRecoveryPoint -Item $bkpItem -VaultId $targetVault.ID -StartDate $startdate -
EndDate $endDate
```

The output is similar to the following example

| RecoveryPointId | RecoveryPointType | RecoveryPointTime    | ItemName          | tType         |
|-----------------|-------------------|----------------------|-------------------|---------------|
| BackupManagemen |                   |                      |                   |               |
| --              | --                | --                   | --                | --            |
| 6660368097802   | Full              | 3/18/2019 8:09:35 PM | MSSQLSERVER;model | AzureWorkload |

Use the 'RecoveryPointId' filter or an array filter to fetch the relevant recovery point.

```
$FullRP = Get-AzRecoveryServicesBackupRecoveryPoint -Item $bkpItem -VaultId $targetVault.ID -RecoveryPointId
"6660368097802"
```

#### Fetch point-in-time recovery point

If the user wants to restore the DB to a certain point-in-time, use [Get-AzRecoveryServicesBackupRecoveryLogChain](#) PS cmdlet. The cmdlet returns a list of dates that represent start and end times of an unbroken, continuous log chain for that SQL backup item. The desired point-in-time should be within this range.

```
Get-AzRecoveryServicesBackupRecoveryLogChain -Item $bkpItem -Item -VaultId $targetVault.ID
```

The output will be similar to the following example.

| ItemName                       | StartTime            | EndTime               |
|--------------------------------|----------------------|-----------------------|
| SQLDataBase;MSSQLSERVER;azu... | 3/18/2019 8:09:35 PM | 3/19/2019 12:08:32 PM |

The above output means that user can restore to any point-in-time between the displayed start time and end time.

The times are in UTC. Construct any point-in-time in PS that is within the range shown above.

#### NOTE

When a log point-in-time selected for restore, user need not specify the starting point i.e., full backup from which the DB is restored. Azure Backup service will take care of the entire recovery plan i.e., which full backup to choose, what log backups to apply etc.

## Determine recovery configuration

In case of SQL DB restore, the following restore scenarios are supported.

- Overriding the backed-up SQL DB with data from another recovery point - OriginalWorkloadRestore
- Restoring the SQL DB as a new DB in the same SQL instance - AlternateWorkloadRestore
- Restoring the SQL DB as a new DB in another SQL instance in another SQL VM - AlternateWorkloadRestore

After fetching the relevant recovery point (distinct or log point-in-time), use [Get-AzRecoveryServicesBackupWorkloadRecoveryConfig](#) PS cmdlet to fetch the recovery config object as per the desired recovery plan.

### Original workload restore

To override the backed-up DB with data from the recovery point, just specify the right flag and the relevant recovery point as shown in the following example(s).

#### Original restore with distinct Recovery point

```
$OverwriteWithFullConfig = Get-AzRecoveryServicesBackupWorkloadRecoveryConfig -RecoveryPoint $FullRP -
OriginalWorkloadRestore -VaultId $targetVault.ID
```

#### Original restore with log point-in-time

```
$OverwriteWithLogConfig = Get-AzRecoveryServicesBackupWorkloadRecoveryConfig -PointInTime $PointInTime -Item
$bkpItem -OriginalWorkloadRestore -VaultId $targetVault.ID
```

### Alternate workload restore

#### IMPORTANT

A backed up SQL DB can be restored as a new DB to another SQLInstance only, in a Azure VM 'registered' to this vault.

As outlined above, if the target SQLInstance lies within another Azure VM, make sure it is [registered to this vault](#) and the relevant SQLInstance appears as a protectable item.

```
$TargetInstance = Get-AzRecoveryServicesBackupProtectableItem -WorkloadType MSSQL -ItemType SQLInstance -Name "
<SQLInstance Name>" -ServerName "<SQL VM name>" -VaultId $targetVault.ID
```

Then just pass the relevant recovery point, target SQL instance with the right flag as shown below.

#### Alternate restore with distinct Recovery point

```
$AnotherInstanceWithFullConfig = Get-AzRecoveryServicesBackupWorkloadRecoveryConfig -RecoveryPoint $FullRP -
TargetItem $TargetInstance -AlternateWorkloadRestore -VaultId $targetVault.ID
```

#### Alternate restore with log point-in-time

```
$AnotherInstanceWithLogConfig = Get-AzRecoveryServicesBackupWorkloadRecoveryConfig -PointInTime $PointInTime -
Item $bkpItem -AlternateWorkloadRestore -VaultId $targetVault.ID
```

The final recovery point configuration object obtained from [Get-AzRecoveryServicesBackupWorkloadRecoveryConfig](#) PS cmdlet has all the relevant information for restore and is as shown below.

```
TargetServer : <SQL server name>
TargetInstance : <Target Instance name>
RestoredDBName : <Target Instance name>/azurebackup1_restored_3_19_2019_1850
OverwriteWLIfpresent : No
NoRecoveryMode : Disabled
targetPhysicalPath : {azurebackup1, azurebackup1_log}
ContainerId : /Subscriptions/00000000-0000-0000-0000-
000000000000/resourceGroups/testRG/providers/Microsoft.RecoveryServices/vaults/testVault/backupFabrics/Azure/pr
otectionContainers/vmappcontainer;compute;computeRG;SQLVMName
SourceResourceId : /subscriptions/00000000-0000-0000-0000-
000000000000/resourceGroups/computeRG/VMAppContainer/SQLVMName
RestoreRequestType : Alternate WL Restore
RecoveryPoint :
Microsoft.Azure.Commands.RecoveryServices.Backup.Cmdlets.Models.AzureWorkloadRecoveryPoint
PointInTime : 1/1/0001 12:00:00 AM
```

You can edit the restored DB name, OverwriteWLIfpresent, NoRecoveryMode, and targetPhysicalPath fields. Get more details for the target file paths as shown below.

```
$AnotherInstanceWithFullConfig.targetPhysicalPath

MappingType SourceLogicalName SourcePath TargetPath
----- ----- -----
Data azurebackup1 F:\Data\azurebackup1.mdf F:\Data\azurebackup1_1553001753.mdf
Log azurebackup1_log F:\Log\azurebackup1_log.ldf F:\Log\azurebackup1_log_1553001753.ldf
```

Set the relevant PS properties as string values as shown below.

```
$AnotherInstanceWithFullConfig.OverwriteWLIfpresent = "Yes"
$AnotherInstanceWithFullConfig | fl

TargetServer : <SQL server name>
TargetInstance : <Target Instance name>
RestoredDBName : <Target Instance name>/azurebackup1_restored_3_19_2019_1850
OverwriteWLIfpresent : Yes
NoRecoveryMode : Disabled
targetPhysicalPath : {azurebackup1, azurebackup1_log}
ContainerId : /Subscriptions/00000000-0000-0000-0000-
000000000000/resourceGroups/testRG/providers/Microsoft.RecoveryServices/vaults/testVault/backupFabrics/Azure/pr
otectionContainers/vmappcontainer;compute;computeRG;SQLVMName
SourceResourceId : /subscriptions/00000000-0000-0000-0000-
000000000000/resourceGroups/computeRG/VMAppContainer/SQLVMName
RestoreRequestType : Alternate WL Restore
RecoveryPoint :
Microsoft.Azure.Commands.RecoveryServices.Backup.Cmdlets.Models.AzureWorkloadRecoveryPoint
PointInTime : 1/1/0001 12:00:00 AM
```

### IMPORTANT

Make sure that the final recovery config object has all the necessary and proper values since the restore operation will be based on the config object.

## Restore with relevant configuration

Once the relevant recovery Config object is obtained and verified, use the [Restore-AzRecoveryServicesBackupItem](#) PS cmdlet to start the restore process.

```
Restore-AzRecoveryServicesBackupItem -WLRecoveryConfig $AnotherInstanceWithLogConfig -VaultId $targetVault.ID
```

The restore operation returns a job to be tracked.

| WorkloadName                         | Operation | Status     | StartTime             | EndTime |
|--------------------------------------|-----------|------------|-----------------------|---------|
| JobID                                | -----     | -----      | -----                 | -----   |
| MSSQLSERVER/m...                     | Restore   | InProgress | 3/17/2019 10:02:45 AM |         |
| 3274xg2b-e4fg-5952-89b4-8cb566gc1748 |           |            |                       |         |

## Manage SQL backups

### On-demand backup

Once backup has been enabled for a DB, user can also trigger an on-demand backup for the DB using [Backup-AzRecoveryServicesBackupItem](#) PS cmdlet. The following example triggers a full backup on a SQL DB with compression enabled and the full backup should be retained for 60 days.

```
$bkpItem = Get-AzRecoveryServicesBackupItem -BackupManagementType AzureWorkload -WorkloadType MSSQL -Name "<backup item name>" -VaultId $targetVault.ID
$endDate = (Get-Date).AddDays(60).ToUniversalTime()
Backup-AzRecoveryServicesBackupItem -Item $bkpItem -BackupType Full -EnableCompression -VaultId $targetVault.ID
-ExpiryDateTimeUTC $endDate
```

The on-demand backup command returns a job to be tracked.

| WorkloadName                         | Operation | Status     | StartTime            | EndTime |
|--------------------------------------|-----------|------------|----------------------|---------|
| JobID                                | -----     | -----      | -----                | -----   |
| MSSQLSERVER/m...                     | Backup    | InProgress | 3/18/2019 8:41:27 PM |         |
| 2516bb1a-d3ef-4841-97a3-9ba455fb0637 |           |            |                      |         |

If the output is lost or if you want to get the relevant Job ID, [get the list of jobs](#) from Azure Backup service and then track it and its details.

### Change policy for backup items

User can either modify existing policy or change the policy of the backed-up item from Policy1 to Policy2. To switch policies for a backed-up item, fetch the relevant policy and back up item and use the [Enable-AzRecoveryServices](#) command with backup item as the parameter.

```
$TargetPol1 = Get-AzRecoveryServicesBackupProtectionPolicy -Name <PolicyName>
$anotherBkpItem = Get-AzRecoveryServicesBackupItem -WorkloadType MSSQL -BackupManagementType AzureWorkload -
Name "<BackupItemName>"
Enable-AzRecoveryServicesBackupProtection -Item $anotherBkpItem -Policy $TargetPol1
```

The command waits until the configure backup is completed and returns the following output.

| WorkloadName                         | Operation       | Status    | StartTime            | EndTime              |
|--------------------------------------|-----------------|-----------|----------------------|----------------------|
| JobID                                |                 |           |                      |                      |
| -----                                | -----           | -----     | -----                | -----                |
| -----                                |                 |           |                      |                      |
| master                               | ConfigureBackup | Completed | 3/18/2019 8:00:21 PM | 3/18/2019 8:02:16 PM |
| 654e8aa2-4096-402b-b5a9-e5e71a496c4e |                 |           |                      |                      |

## Re-register SQL VMs

### WARNING

Make sure to read this [document](#) to understand the failure symptoms and causes before attempting re-registration

To trigger re-registration of the SQL VM, fetch the relevant backup container and pass it to the register cmdlet.

```
$SQLContainer = Get-AzRecoveryServicesBackupContainer -ContainerType AzureVMAppContainer -FriendlyName <VM name> -VaultId $targetvault.ID
Register-AzRecoveryServicesBackupContainer -Container $SQLContainer -BackupManagementType AzureWorkload -WorkloadType MSSQL -VaultId $targetVault.ID
```

## Stop protection

### Retain data

If user wishes to stop protection, they can use the [Disable-AzRecoveryServicesBackupProtection](#) PS cmdlet. This will stop the scheduled backups but the data backed up until now is retained forever.

```
$bkpItem = Get-AzRecoveryServicesBackupItem -BackupManagementType AzureWorkload -WorkloadType MSSQL -Name "<backup item name>" -VaultId $targetVault.ID
Disable-AzRecoveryServicesBackupProtection -Item $bkpItem -VaultId $targetVault.ID
```

## Delete backup data

In order to completely remove the stored backup data in the vault, just add '-RemoveRecoveryPoints' flag/switch to the ['disable' protection command](#).

```
Disable-AzRecoveryServicesBackupProtection -Item $bkpItem -VaultId $targetVault.ID -RemoveRecoveryPoints
```

## Disable auto protection

If autoprotection was configured on an SQLInstance, user can disable it using the [Disable-AzRecoveryServicesBackupAutoProtection](#) PS cmdlet.

```
$SQLInstance = Get-AzRecoveryServicesBackupProtectableItem -workloadType MSSQL -ItemType SQLInstance -VaultId $targetVault.ID -Name "<Protectable Item name>" -ServerName "<Server Name>"
Disable-AzRecoveryServicesBackupAutoProtection -InputItem $SQLInstance -BackupManagementType AzureWorkload -WorkloadType MSSQL -VaultId $targetvault.ID
```

## Unregister SQL VM

If all the DBs of a SQL server [are no longer protected and no backup data exists](#), user can unregister the SQL VM from this vault. Only then user can protect DBs to another vault. Use [Unregister-AzRecoveryServicesBackupContainer](#) PS cmdlet to unregister the SQL VM.

```
$SQLContainer = Get-AzRecoveryServicesBackupContainer -ContainerType AzureVMAppContainer -FriendlyName <VM name> -VaultId $targetvault.ID
Unregister-AzRecoveryServicesBackupContainer -Container $SQLContainer -VaultId $targetvault.ID
```

## Track Azure Backup jobs

It is important to note that Azure Backup only tracks user triggered jobs in SQL backup. Scheduled backups (including log backups) are not visible in portal/powershell. However, if any scheduled jobs fail, a [backup alert](#) is generated and shown in portal. [Use Azure Monitor](#) to track all the scheduled jobs and other relevant information.

Users can track on-demand/user triggered operations with the JobID that is returned in the [output](#) of asynchronous jobs such as backup. Use [Get-AzRecoveryServicesBackupJobDetail](#) PS cmdlet to track job and its details.

```
Get-AzRecoveryServicesBackupJobDetails -JobId 2516bb1a-d3ef-4841-97a3-9ba455fb0637 -VaultId $targetVault.ID
```

To get the list of on-demand jobs and their statuses from Azure Backup service, use [Get-AzRecoveryServicesBackupJob](#) PS cmdlet. The following example returns all the in-progress SQL jobs.

```
Get-AzRecoveryServicesBackupJob -Status InProgress -BackupManagementType AzureWorkload
```

To cancel an in-progress job, use the [Stop-AzRecoveryServicesBackupJob](#) PS cmdlet.

## Managing SQL Always On Availability groups

For SQL Always On Availability Groups, make sure to [register all the nodes](#) of the Availability group (AG). Once registration is done for all nodes, a SQL availability group object is logically created under protectable items. The databases under the SQL AG will be listed as 'SQLDatabase'. The nodes will show up as standalone instances and the default SQL databases under them will be listed as SQL databases as well.

For example, let's assume a SQL AG has two nodes: 'sql-server-0' and 'sql-server-1' and 1 SQL AG DB. Once both these nodes are registered, if user [lists the protectable items](#), it lists the following components

- A SQL AG object - protectable item type as SQLAvailabilityGroup
- A SQL AG DB - protectable item type as SQLDatabase
- sql-server-0 - protectable item type as SQLInstance
- sql-server-1 - protectable item type as SQLInstance
- Any default SQL DBs (master, model, msdb) under sql-server-0 - protectable item type as SQLDatabase
- Any default SQL DBs (master, model, msdb) under sql-server-1 - protectable item type as SQLDatabase

sql-server-0, sql-server-1 will also be listed as "AzureVMAContainer" when [backup containers are listed](#).

Just fetch the relevant SQL database to [enable backup](#) and the [on-demand backup](#) and [restore](#) PS cmdlets are identical.

# Azure Backup PowerShell samples

1/28/2020 • 2 minutes to read • [Edit Online](#)

The following table links to PowerShell script samples that use Azure Backup to back up and restore data.

|                                                               |                                                                          |
|---------------------------------------------------------------|--------------------------------------------------------------------------|
| <a href="#">Back up an encrypted virtual machine to Azure</a> | Back up all data on the encrypted virtual machine.                       |
| <a href="#">Find Registered Storage Account</a>               | Find the recovery services vault where the storage account is registered |

# Create Azure Recovery Services Vault using REST API

11/18/2019 • 2 minutes to read • [Edit Online](#)

The steps to create an Azure Recovery Services Vault using REST API are outlined in [create vault REST API](#) documentation. Let us use this document as a reference to create a vault called "testVault" in "West US".

To create or update an Azure Recovery Services vault, use the following *PUT* operation.

PUT

`https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.RecoveryServices/vaults/{vaultName}?api-version=2016-06-01`

## Create a request

To create the *PUT* request, the `{subscription-id}` parameter is required. If you have multiple subscriptions, see [Working with multiple subscriptions](#). You define a `{resourceGroupName}` and `{vaultName}` for your resources, along with the `api-version` parameter. This article uses `api-version=2016-06-01`.

The following headers are required:

| REQUEST HEADER              | DESCRIPTION                                                |
|-----------------------------|------------------------------------------------------------|
| <code>Content-Type:</code>  | Required. Set to <code>application/json</code> .           |
| <code>Authorization:</code> | Required. Set to a valid <code>Bearer</code> access token. |

For more information about how to create the request, see [Components of a REST API request/response](#).

## Create the request body

The following common definitions are used to build a request body:

| NAME       | REQUIRED | TYPE            | DESCRIPTION                                                     |
|------------|----------|-----------------|-----------------------------------------------------------------|
| eTag       |          | String          | Optional eTag                                                   |
| location   | true     | String          | Resource location                                               |
| properties |          | VaultProperties | Properties of the vault                                         |
| sku        |          | Sku             | Identifies the unique system identifier for each Azure resource |
| tags       |          | Object          | Resource tags                                                   |

Note that vault name and resource group name are provided in the PUT URI. The request body defines the location.

## Example request body

The following example body is used to create a vault in "West US". Specify the location. The SKU is always "Standard".

```
{
 "properties": {},
 "sku": {
 "name": "Standard"
 },
 "location": "West US"
}
```

## Responses

There are two successful responses for the operation to create or update a Recovery Services vault:

| NAME        | TYPE  | DESCRIPTION |
|-------------|-------|-------------|
| 200 OK      | Vault | OK          |
| 201 Created | Vault | Created     |

For more information about REST API responses, see [Process the response message](#).

### Example response

A condensed *201 Created* response from the previous example request body shows an *id* has been assigned and the *provisioningState* is *Succeeded*:

```
{
 "location": "westus",
 "name": "testVault",
 "properties": {
 "provisioningState": "Succeeded"
 },
 "id": "/subscriptions/77777777-b0c6-47a2-b37c-d8e65a629c18/resourceGroups/Default-RecoveryServices-
ResourceGroup/providers/Microsoft.RecoveryServices/vaults/testVault",
 "type": "Microsoft.RecoveryServices/vaults",
 "sku": {
 "name": "Standard"
 }
}
```

## Next steps

[Create a backup policy for backing up an Azure VM in this vault.](#)

For more information on the Azure REST APIs, see the following documents:

- [Azure Recovery Services provider REST API](#)
- [Get started with Azure REST API](#)

# Update Azure Recovery Services Vault configurations using REST API

12/20/2019 • 2 minutes to read • [Edit Online](#)

This article describes how to update backup related configurations in Azure Recovery Services vault using REST API.

## Soft delete state

Deleting backups of a protected item is a significant operation that has to be monitored. To protect against accidental deletions, Azure Recovery Services vault has a soft-delete capability. This capability allows customers to restore deleted backups, if necessary, within a time period after the deletion.

But there are scenarios in which this capability is not required. An Azure Recovery Services vault cannot be deleted if there are backup items within it, even soft-deleted ones. This may pose a problem if the vault needs to be immediately deleted. For example: deployment operations often clean up the created resources in the same workflow. A deployment can create a vault, configure backups for an item, do a test restore and then proceed to delete the backup items and the vault. If the vault deletion fails, the entire deployment might fail. Disabling soft-delete is the only way to guarantee immediate deletion.

Hence, the customer needs to carefully choose whether or not to disable soft-delete for a particular vault depending on the scenario. For more information, see the [soft-delete article](#).

### Fetch soft delete state using REST API

By default, the soft-delete state will be enabled for any newly created Recovery Services vault. To fetch/update the state of soft-delete for a vault, use the backup vault's config related [REST API document](#)

To fetch the current state of soft-delete for a vault, use the following *GET* operation

```
GET
https://management.azure.com/Subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.RecoveryServices/vaults/{vaultName}/backupconfig/vaultconfig?api-version=2019-05-13
```

The GET URI has `{subscriptionId}`, `{vaultName}`, `{vaultrgroupname}` parameters. In this example, `{vaultName}` is "testVault" and `{vaultrgroupname}` is "testVaultRG". As all the required parameters are given in the URI, there is no need for a separate request body.

```
GET https://management.azure.com/Subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/testVaultRG/providers/Microsoft.RecoveryServices/vaults/testVault/backupconfig/vaultconfig?api-version=2019-05-13
```

### Responses

The successful response for the 'GET' operation is shown below:

| NAME   | TYPE                                      | DESCRIPTION |
|--------|-------------------------------------------|-------------|
| 200 OK | <a href="#">BackupResourceVaultConfig</a> | OK          |

#### Example response

Once the 'GET' request is submitted, a 200 (successful) response is returned.

```
{
 "id": "/subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/testvaultRG/providers/Microsoft.RecoveryServices/vaults/testvault/backupconfig/vaul
tconfig",
 "name": "vaultconfig",
 "type": "Microsoft.RecoveryServices/vaults/backupconfig",
 "properties": {
 "enhancedSecurityState": "Enabled",
 "softDeleteFeatureState": "Enabled"
 }
}
```

## Update soft delete state using REST API

To update the soft-delete state of the recovery services vault using REST API, use the following *PATCH* operation

```
PATCH
https://management.azure.com/Subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Micros
oft.RecoveryServices/vaults/{vaultName}/backupconfig/vaultconfig?api-version=2019-05-13
```

The PATCH URI has `{subscriptionId}` , `{vaultName}` , `{vaultresourceGroupName}` parameters. In this example, `{vaultName}` is "testVault" and `{vaultresourceGroupName}` is "testVaultRG". If we replace the URI with the values above, then the URI will look like this.

```
PATCH https://management.azure.com/Subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/testVaultRG/providers/Microsoft.RecoveryServices/vaults/testVault/backupconfig/vaul
tconfig?api-version=2019-05-13
```

### Create the request body

The following common definitions are used to create a request body

For more details, refer to [the REST API documentation](#)

| NAME       | REQUIRED | TYPE            | DESCRIPTION             |
|------------|----------|-----------------|-------------------------|
| eTag       |          | String          | Optional eTag           |
| location   | true     | String          | Resource location       |
| properties |          | VaultProperties | Properties of the vault |
| tags       |          | Object          | Resource tags           |

### Example request body

The following example is used to update the soft-delete state to 'disabled'.

```
{
 "properties": {
 "enhancedSecurityState": "Enabled",
 "softDeleteFeatureState": "Disabled"
 }
}
```

### Responses

The successful response for the 'PATCH' operation is shown below:

| NAME   | TYPE                      | DESCRIPTION |
|--------|---------------------------|-------------|
| 200 OK | BackupResourceVaultConfig | OK          |

#### Example response

Once the 'PATCH' request is submitted, a 200 (successful) response is returned.

```
{
 "id": "/subscriptions/00000000-0000-0000-0000-
000000000000/resourceGroups/testvaultRG/providers/Microsoft.RecoveryServices/vaults/testvault/backupconfig/vaul
tconfig",
 "name": "vaultconfig",
 "type": "Microsoft.RecoveryServices/vaults/backupconfig",
 "properties": {
 "enhancedSecurityState": "Enabled",
 "softDeleteFeatureState": "Disabled"
 }
}
```

## Next steps

[Create a backup policy for backing up an Azure VM in this vault.](#)

For more information on the Azure REST APIs, see the following documents:

- [Azure Recovery Services provider REST API](#)
- [Get started with Azure REST API](#)

# Create Azure Recovery Services backup policies using REST API

2/2/2020 • 3 minutes to read • [Edit Online](#)

The steps to create a backup policy for an Azure Recovery Services vault are outlined in the [policy REST API document](#). Let us use this document as a reference to create a policy for Azure VM backup.

## Create or update a policy

To create or update an Azure Backup policy, use the following *PUT* operation

```
PUT
```

```
https://management.azure.com/Subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.RecoveryServices/vaults/{vaultName}/backupPolicies/{policyName}?api-version=2019-05-13
```

The `{policyName}` and `{vaultName}` are provided in the URI. Additional information is provided in the request body.

## Create the request body

For example, to create a policy for Azure VM backup, following are the components of the request body.

| NAME       | REQUIRED | TYPE                                                          | DESCRIPTION                         |
|------------|----------|---------------------------------------------------------------|-------------------------------------|
| properties | True     | ProtectionPolicy: <a href="#">AzureIaaSVMProtectionPolicy</a> | ProtectionPolicyResource properties |
| tags       |          | Object                                                        | Resource tags                       |

For the complete list of definitions in the request body, refer to the [backup policy REST API document](#).

### Example request body

The following request body defines a backup policy for Azure VM backups.

The policy says:

- Take a weekly backup every Monday, Wednesday, Thursday at 10:00 AM Pacific Standard Time.
- Retain the backups taken on every Monday, Wednesday, Thursday for one week.
- Retain the backups taken on every first Wednesday and third Thursday of a month for two months (overrides the previous retention conditions, if any).
- Retain the backups taken on fourth Monday and fourth Thursday in February and November for four years (overrides the previous retention conditions, if any).

```
{
 "properties": {
 "backupManagementType": "AzureIaaSVM",
 "timeZone": "Pacific Standard Time",
 "schedulePolicy": {
 "schedulePolicyType": "SimpleSchedulePolicy",
 "scheduleRunFrequency": "Weekly",
 "scheduleRunTimes": [
```

```
 "2018-01-24T10:00:00Z"
],
 "scheduleRunDays": [
 "Monday",
 "Wednesday",
 "Thursday"
]
},
"retentionPolicy": {
 "retentionPolicyType": "LongTermRetentionPolicy",
 "weeklySchedule": {
 "daysOfTheWeek": [
 "Monday",
 "Wednesday",
 "Thursday"
],
 "retentionTimes": [
 "2018-01-24T10:00:00Z"
],
 "retentionDuration": {
 "count": 1,
 "durationType": "Weeks"
 }
 },
 "monthlySchedule": {
 "retentionScheduleFormatType": "Weekly",
 "retentionScheduleWeekly": {
 "daysOfTheWeek": [
 "Wednesday",
 "Thursday"
],
 "weeksOfTheMonth": [
 "First",
 "Third"
],
 "retentionTimes": [
 "2018-01-24T10:00:00Z"
],
 "retentionDuration": {
 "count": 2,
 "durationType": "Months"
 }
 },
 "yearlySchedule": {
 "retentionScheduleFormatType": "Weekly",
 "monthsOfYear": [
 "February",
 "November"
],
 "retentionScheduleWeekly": {
 "daysOfTheWeek": [
 "Monday",
 "Thursday"
],
 "weeksOfTheMonth": [
 "Fourth"
],
 "retentionTimes": [
 "2018-01-24T10:00:00Z"
],
 "retentionDuration": {
 "count": 4,
 "durationType": "Years"
 }
 }
 }
 }
}
```

```
}
```

### IMPORTANT

The time formats for schedule and retention support only DateTime. They do not support Time format alone.

## Responses

The backup policy creation/update is a [asynchronous operation](#). It means this operation creates another operation that needs to be tracked separately.

It returns two responses: 202 (Accepted) when another operation is created, and then 200 (OK) when that operation completes.

| NAME         | TYPE                                      | DESCRIPTION |
|--------------|-------------------------------------------|-------------|
| 200 OK       | <a href="#">Protection PolicyResource</a> | OK          |
| 202 Accepted |                                           | Accepted    |

### Example responses

Once you submit the *PUT* request for policy creation or updating, the initial response is 202 (Accepted) with a location header or Azure-async-header.

```
HTTP/1.1 202 Accepted
Pragma: no-cache
Retry-After: 60
Azure-AsyncOperation: https://management.azure.com/Subscriptions/00000000-0000-0000-0000-
000000000000/resourceGroups/SwaggerTestRg/providers/Microsoft.RecoveryServices/vaults/testVault/backupPolicies
/testPolicy1/operations/00000000-0000-0000-0000-000000000000?api-version=2016-06-01
X-Content-Type-Options: nosniff
x-ms-request-id: db785be0-bb20-4598-bc9f-70c9428b170b
x-ms-client-request-id: e1f94eef-9b2d-45c4-85b8-151e12b07d03; e1f94eef-9b2d-45c4-85b8-151e12b07d03
Strict-Transport-Security: max-age=31536000; includeSubDomains
x-ms-ratelimit-remaining-subscription-writes: 1199
x-ms-correlation-request-id: db785be0-bb20-4598-bc9f-70c9428b170b
x-ms-routing-request-id: SOUTHHINDIA:20180521T073907Z:db785be0-bb20-4598-bc9f-70c9428b170b
Cache-Control: no-cache
Date: Mon, 21 May 2018 07:39:06 GMT
Location: https://management.azure.com/Subscriptions/00000000-0000-0000-0000-
000000000000/resourceGroups/SwaggerTestRg/providers/Microsoft.RecoveryServices/vaults/testVault/backupPolicies
/testPolicy1/operationResults/00000000-0000-0000-0000-000000000000?api-version=2019-05-13
X-Powered-By: ASP.NET
```

Then track the resulting operation using the location header or Azure-AsyncOperation header with a simple *GET* command.

```
GET https://management.azure.com/Subscriptions/00000000-0000-0000-0000-
000000000000/resourceGroups/SwaggerTestRg/providers/Microsoft.RecoveryServices/vaults/testVault/backupPolicies
/testPolicy1/operationResults/00000000-0000-0000-0000-000000000000?api-version=2019-05-13
```

Once the operation completes, it returns 200 (OK) with the policy content in the response body.

```
{
 "id": "/Subscriptions/00000000-0000-0000-0000-
000000000000/resourceGroups/SwaggerTestRg/providers/Microsoft.RecoveryServices/vaults/testVault/backupPolicies
/testPolicy1"
```

```
/testpolicy1 ,
 "name": "testPolicy1",
 "type": "Microsoft.RecoveryServices/vaults/backupPolicies",
 "properties": {
 "backupManagementType": "AzureIaaSVM",
 "schedulePolicy": {
 "schedulePolicyType": "SimpleSchedulePolicy",
 "scheduleRunFrequency": "Weekly",
 "scheduleRunDays": [
 "Monday",
 "Wednesday",
 "Thursday"
],
 "scheduleRunTimes": [
 "2018-01-24T10:00:00Z"
],
 "scheduleWeeklyFrequency": 0
 },
 "retentionPolicy": {
 "retentionPolicyType": "LongTermRetentionPolicy",
 "weeklySchedule": {
 "daysOfTheWeek": [
 "Monday",
 "Wednesday",
 "Thursday"
],
 "retentionTimes": [
 "2018-01-24T10:00:00Z"
],
 "retentionDuration": {
 "count": 1,
 "durationType": "Weeks"
 }
 },
 "monthlySchedule": {
 "retentionScheduleFormatType": "Weekly",
 "retentionScheduleWeekly": {
 "daysOfTheWeek": [
 "Wednesday",
 "Thursday"
],
 "weeksOfTheMonth": [
 "First",
 "Third"
]
 },
 "retentionTimes": [
 "2018-01-24T10:00:00Z"
],
 "retentionDuration": {
 "count": 2,
 "durationType": "Months"
 }
 },
 "yearlySchedule": {
 "retentionScheduleFormatType": "Weekly",
 "monthsOfYear": [
 "February",
 "November"
],
 "retentionScheduleWeekly": {
 "daysOfTheWeek": [
 "Monday",
 "Thursday"
],
 "weeksOfTheMonth": [
 "Fourth"
]
 },
 "retentionDuration": {
 "count": 1,
 "durationType": "Years"
 }
 }
 }
 }
}
```

```
 "retentionTimes": [
 "2018-01-24T10:00:00Z"
],
 "retentionDuration": {
 "count": 4,
 "durationType": "Years"
 }
 },
 "timeZone": "Pacific Standard Time",
 "protectedItemCount": 0
}
}
```

If a policy is already being used to protect an item, any update in the policy will result in [modifying protection](#) for all such associated items.

## Next steps

[Enable protection for an unprotected Azure VM.](#)

For more information on the Azure Backup REST APIs, see the following documents:

- [Azure Recovery Services provider REST API](#)
- [Get started with Azure REST API](#)

# Back up an Azure VM using Azure Backup via REST API

12/20/2019 • 10 minutes to read • [Edit Online](#)

This article describes how to manage backups for an Azure VM using Azure Backup via REST API. Configure protection for the first time for a previously unprotected Azure VM, trigger an on-demand backup for a protected Azure VM and modify backup properties of a backed-up VM via REST API as explained here.

Refer to [create vault](#) and [create policy](#) REST API tutorials for creating new vaults and policies.

Let's assume you want to protect a VM "testVM" under a resource group "testRG" to a Recovery Services vault "testVault", present within the resource group "testVaultRG", with the default policy (named "DefaultPolicy").

## Configure backup for an unprotected Azure VM using REST API

### Discover unprotected Azure VMs

First, the vault should be able to identify the Azure VM. This is triggered using the [refresh operation](#). It is an asynchronous *POST* operation that makes sure the vault gets the latest list of all unprotected VM in the current subscription and 'caches' them. Once the VM is 'cached', Recovery services will be able to access the VM and protect it.

POST

```
https://management.azure.com/Subscriptions/{subscriptionId}/resourceGroups/{vaultresourceGroupName}/providers/Microsoft.RecoveryServices/vaults/{vaultName}/backupFabrics/{fabricName}/refreshContainers?api-version=2016-12-01
```

The POST URI has `{subscriptionId}`, `{vaultName}`, `{vaultresourceGroupName}`, `{fabricName}` parameters. The `{fabricName}` is "Azure". As per our example, `{vaultName}` is "testVault" and `{vaultresourceGroupName}` is "testVaultRG". As all the required parameters are given in the URI, there is no need for a separate request body.

```
POST https://management.azure.com/Subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/testVaultRG/providers/Microsoft.RecoveryServices/vaults/testVault/backupFabrics/Azure/refreshContainers?api-version=2016-12-01
```

### Responses

The 'refresh' operation is an [asynchronous operation](#). It means this operation creates another operation that needs to be tracked separately.

It returns two responses: 202 (Accepted) when another operation is created and then 200 (OK) when that operation completes.

| NAME           | TYPE | DESCRIPTION                 |
|----------------|------|-----------------------------|
| 204 No Content |      | OK with No content returned |
| 202 Accepted   |      | Accepted                    |

#### Example responses

Once the *POST* request is submitted, a 202 (Accepted) response is returned.

```

HTTP/1.1 202 Accepted
Pragma: no-cache
Retry-After: 60
X-Content-Type-Options: nosniff
x-ms-request-id: 43cf550d-e463-421c-8922-37e4766db27d
x-ms-client-request-id: 4910609f-bb9b-4c23-8527-eb6fa2d3253f; 4910609f-bb9b-4c23-8527-eb6fa2d3253f
Strict-Transport-Security: max-age=31536000; includeSubDomains
x-ms-ratelimit-remaining-subscription-writes: 1199
x-ms-correlation-request-id: 43cf550d-e463-421c-8922-37e4766db27d
x-ms-routing-request-id: SOUTHINDIA:20180521T105701Z:43cf550d-e463-421c-8922-37e4766db27d
Cache-Control: no-cache
Date: Mon, 21 May 2018 10:57:00 GMT
Location: https://management.azure.com/subscriptions//00000000-0000-0000-0000-
000000000000/resourceGroups/testVaultRG/providers/microsoft.recoveryservices/vaults/testVault/backupFabrics/Az
ure/operationResults/aad204aa-a5cf-4be2-a7db-a224819e5890?api-version=2019-05-13
X-Powered-By: ASP.NET

```

Track the resulting operation using the "Location" header with a simple *GET* command

```

GET https://management.azure.com/subscriptions/00000000-0000-0000-0000-
000000000000/resourceGroups/testVaultRG/providers/microsoft.recoveryservices/vaults/testVault/backupFabrics/Az
ure/operationResults/aad204aa-a5cf-4be2-a7db-a224819e5890?api-version=2019-05-13

```

Once all the Azure VMs are discovered, the *GET* command returns a 204 (No Content) response. The vault is now able to discover any VM within the subscription.

```

HTTP/1.1 204 NoContent
Pragma: no-cache
X-Content-Type-Options: nosniff
x-ms-request-id: cf6cd73b-9189-4942-a61d-878fcf76b1c1
x-ms-client-request-id: 25bb6345-f9fc-4406-be1a-dc6db0eefafe; 25bb6345-f9fc-4406-be1a-dc6db0eefafe
Strict-Transport-Security: max-age=31536000; includeSubDomains
x-ms-ratelimit-remaining-subscription-reads: 14997
x-ms-correlation-request-id: cf6cd73b-9189-4942-a61d-878fcf76b1c1
x-ms-routing-request-id: SOUTHINDIA:20180521T105825Z:cf6cd73b-9189-4942-a61d-878fcf76b1c1
Cache-Control: no-cache
Date: Mon, 21 May 2018 10:58:25 GMT
X-Powered-By: ASP.NET

```

## Selecting the relevant Azure VM

You can confirm that "caching" is done by [listing all protectable items](#) under the subscription and locate the desired VM in the response. [The response of this operation](#) also gives you information on how Recovery Services identifies a VM. Once you are familiar with the pattern, you can skip this step and directly proceed to [enabling protection](#).

This operation is a *GET* operation.

```

GET
https://management.azure.com/Subscriptions/{subscriptionId}/resourceGroups/{vaultResourceGroupName}/providers/
Microsoft.RecoveryServices/vaults/{vaultName}/backupProtectableItems?api-version=2016-12-
01&$filter=backupManagementType eq 'AzureIaaSVM'

```

The *GET* URI has all the required parameters. No additional request body is needed.

### Responses

| NAME   | TYPE                                                | DESCRIPTION |
|--------|-----------------------------------------------------|-------------|
| 200 OK | <a href="#">WorkloadProtectableItemResourceList</a> | OK          |

## Example responses

Once the *GET* request is submitted, a 200 (OK) response is returned.

```
HTTP/1.1 200 OK
Pragma: no-cache
X-Content-Type-Options: nosniff
x-ms-request-id: 7c2cf56a-e6be-4345-96df-c27ed849fe36
x-ms-client-request-id: 40c8601a-c217-4c68-87da-01db8dac93dd; 40c8601a-c217-4c68-87da-01db8dac93dd
Strict-Transport-Security: max-age=31536000; includeSubDomains
x-ms-ratelimit-remaining-subscription-reads: 14979
x-ms-correlation-request-id: 7c2cf56a-e6be-4345-96df-c27ed849fe36
x-ms-routing-request-id: SOUTHINDIA:20180521T071408Z:7c2cf56a-e6be-4345-96df-c27ed849fe36
Cache-Control: no-cache
Date: Mon, 21 May 2018 07:14:08 GMT
Server: Microsoft-IIS/8.0
X-Powered-By: ASP.NET

{
 "value": [
 {
 "id": "/subscriptions/00000000-0000-0000-0000-
000000000000/resourceGroups/testVaultRG/providers/microsoft.recoveryservices/vaults/testVault/backupFabrics/Azure/protectionContainers/IaaSVMContainer;iaasvmcontainerv2;testRG;testVM/protectableItems/vm;iaasvmcontainerv2;testRG;testVM",
 "name": "iaasvmcontainerv2;testRG;testVM",
 "type": "Microsoft.RecoveryServices/vaults/backupFabrics/protectionContainers/protectableItems",
 "properties": {
 "virtualMachineId": "/subscriptions/00000000-0000-0000-0000-
000000000000/resourceGroups/testRG/providers/Microsoft.Compute/virtualMachines/testVM",
 "virtualMachineVersion": "Compute",
 "resourceGroup": "testRG",
 "backupManagementType": "AzureIaaSVM",
 "protectableItemType": "Microsoft.Compute/virtualMachines",
 "friendlyName": "testVM",
 "protectionState": "NotProtected"
 }
 },

]
}
```

### TIP

The number of values in a *GET* response is limited to 200 for a 'page'. Use the 'nextLink' field to get the URL for next set of responses.

The response contains the list of all unprotected Azure VMs and each `{value}` contains all the information required by Azure Recovery Service to configure backup. To configure backup, note the `{name}` field and the `{virtualMachineId}` field in `{properties}` section. Construct two variables from these field values as mentioned below.

- `containerName = "iaasvmcontainer;" + {name}`
- `protectedItemName = "vm;" + {name}`
- `{virtualMachineId}` is used later in [the request body](#)

In the example, the above values translate to:

- `containerName = "iaasvmcontainer;iaasvmcontainerv2;testRG;testVM"`
- `protectedItemName = "vm;iaasvmcontainerv2;testRG;testVM"`

## Enabling protection for the Azure VM

After the relevant VM is "cached" and "identified", select the policy to protect. To know more about existing policies

in the vault, refer to [list Policy API](#). Then select the [relevant policy](#) by referring to the policy name. To create policies, refer to [create policy tutorial](#). "DefaultPolicy" is selected in the below example.

Enabling protection is an asynchronous *PUT* operation that creates a 'protected item'.

```
https://management.azure.com/Subscriptions/{subscriptionId}/resourceGroups/{vaultresourceGroupName}/providers/Microsoft.RecoveryServices/vaults/{vaultName}/backupFabrics/{fabricName}/protectionContainers/{containerName}/protectedItems/{protectedItemName}?api-version=2019-05-13
```

The `{containerName}` and `{protectedItemName}` are as constructed above. The `{fabricName}` is "Azure". For our example, this translates to:

```
PUT https://management.azure.com/Subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/testVaultRG/providers/Microsoft.RecoveryServices/vaults/testVault/backupFabrics/Azure/protectionContainers/iaasvmcontainer;iaasvmcontainerv2;testRG;testVM/protectedItems/vm;iaasvmcontainerv2;testRG;testVM?api-version=2019-05-13
```

#### Create the request body

To create a protected item, following are the components of the request body.

| NAME       | TYPE                     | DESCRIPTION                       |
|------------|--------------------------|-----------------------------------|
| properties | AzurelaaSVMProtectedItem | ProtectedItem Resource properties |

For the complete list of definitions of the request body and other details, refer to [create protected item REST API document](#).

#### Example request body

The following request body defines properties required to create a protected item.

```
{
 "properties": {
 "protectedItemType": "Microsoft.Compute/virtualMachines",
 "sourceResourceId": "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/testRG/providers/Microsoft.Compute/virtualMachines/testVM",
 "policyId": "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/testVaultRG/providers/microsoft.recoveryservices/vaults/testVault/backupPolicies/DefaultPolicy"
 }
}
```

The `{sourceResourceId}` is the `{virtualMachineId}` mentioned above from the [response of list protectable items](#).

#### Responses

The creation of a protected item is an [asynchronous operation](#). It means this operation creates another operation that needs to be tracked separately.

It returns two responses: 202 (Accepted) when another operation is created and then 200 (OK) when that operation completes.

| NAME         | TYPE                  | DESCRIPTION |
|--------------|-----------------------|-------------|
| 200 OK       | ProtectedItemResource | OK          |
| 202 Accepted |                       | Accepted    |

#### Example responses

Once you submit the *PUT* request for protected item creation or update, the initial response is 202 (Accepted) with a location header or Azure-async-header.

```
HTTP/1.1 202 Accepted
Pragma: no-cache
Retry-After: 60
Azure-AsyncOperation: https://management.azure.com/subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/testVaultRG/providers/microsoft.recoveryservices/vaults/testVault/backupFabrics/Az
ure/protectionContainers/iaasvmcontainer;iaasvmcontainerv2;testRG;testVM/protectedItems/vm;testRG;testVM/ope
rationsStatus/a0866047-6fc7-4ac3-ba38-fb0ae8aa550f?api-version=2019-05-13
X-Content-Type-Options: nosniff
x-ms-request-id: db785be0-bb20-4598-bc9f-70c9428b170b
x-ms-client-request-id: e1f94eef-9b2d-45c4-85b8-151e12b07d03; e1f94eef-9b2d-45c4-85b8-151e12b07d03
Strict-Transport-Security: max-age=31536000; includeSubDomains
x-ms-ratelimit-remaining-subscription-writes: 1199
x-ms-correlation-request-id: db785be0-bb20-4598-bc9f-70c9428b170b
x-ms-routing-request-id: SOUTHINDIA:20180521T073907Z:db785be0-bb20-4598-bc9f-70c9428b170b
Cache-Control: no-cache
Date: Mon, 21 May 2018 07:39:06 GMT
Location: https://management.azure.com/subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/testVaultRG/providers/microsoft.recoveryservices/vaults/testVault/backupFabrics/Az
ure/protectionContainers/iaasvmcontainer;iaasvmcontainerv2;testRG;testVM/protectedItems/vm;testRG;testVM/ope
rationsResults/a0866047-6fc7-4ac3-ba38-fb0ae8aa550f?api-version=2019-05-13
X-Powered-By: ASP.NET
```

Then track the resulting operation using the location header or Azure-AsyncOperation header with a simple *GET* command.

```
GET https://management.azure.com/subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/testVaultRG/providers/microsoft.recoveryservices/vaults/testVault/backupFabrics/Az
ure/protectionContainers/iaasvmcontainer;iaasvmcontainerv2;testRG;testVM/protectedItems/vm;testRG;testVM/ope
rationsStatus/a0866047-6fc7-4ac3-ba38-fb0ae8aa550f?api-version=2019-05-13
```

Once the operation completes, it returns 200 (OK) with the protected item content in the response body.

```
{
 "id": "/subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/testVaultRG/providers/microsoft.recoveryservices/vaults/testVault/backupFabrics/Az
ure/protectionContainers/iaasvmcontainer;iaasvmcontainerv2;testRG;testVM/protectedItems/vm;testRG;testVM",
 "name": "VM;testRG;testVM",
 "type": "Microsoft.RecoveryServices/vaults/backupFabrics/protectionContainers/protectedItems",
 "properties": {
 "friendlyName": "testVM",
 "virtualMachineId": "/subscriptions/00000000-0000-0000-
0000000000/resourceGroups/testRG/providers/Microsoft.Compute/virtualMachines/testVM",
 "protectionStatus": "Healthy",
 "protectionState": "IRPending",
 "healthStatus": "Passed",
 "lastBackupStatus": "",
 "lastBackupTime": "2001-01-01T00:00:00Z",
 "protectedItemDataId": "17592691116891",
 "extendedInfo": {
 "recoveryPointCount": 0,
 "policyInconsistent": false
 },
 "protectedItemType": "Microsoft.Compute/virtualMachines",
 "backupManagementType": "AzureIaaSVM",
 "workloadType": "VM",
 "containerName": "iaasvmcontainerv2;testRG;testVM",
 "sourceResourceId": "/subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/testRG/providers/Microsoft.Compute/virtualMachines/testVM",
 "policyId": "/subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/testVaultRG/providers/microsoft.recoveryservices/vaults/testVault/backupPolicies/D
efaultPolicy",
 "policyName": "DefaultPolicy"
 }
}
```

This confirms that protection is enabled for the VM and the first backup will be triggered as per the policy schedule.

## Trigger an on-demand backup for a protected Azure VM

Once an Azure VM is configured for backup, backups happen as per the policy schedule. You can wait for the first scheduled backup or trigger an on-demand backup anytime. Retention for on-demand backups is separate from backup policy's retention and can be specified to a particular date-time. If not specified, it's assumed to be 30 days from the day of the trigger of on-demand backup.

Triggering an on-demand backup is a *POST* operation.

```
POST
https://management.azure.com/Subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Micro
soft.RecoveryServices/vaults/{vaultName}/backupFabrics/{fabricName}/protectionContainers/{containerName}/prote
ctedItems/{protectedItemName}/backup?api-version=2016-12-01
```

The `{containerName}` and `{protectedItemName}` are as constructed [above](#). The `{fabricName}` is "Azure". For our example, this translates to:

```
POST https://management.azure.com/Subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/testVaultRG/providers/Microsoft.RecoveryServices/vaults/testVault/backupFabrics/Az
ure/protectionContainers/iaasvmcontainer;iaasvmcontainerv2;testRG;testVM/protectedItems/vm;iaasvmcontainerv2;t
estRG;testVM/backup?api-version=2016-12-01
```

## Create the request body

To trigger an on-demand backup, following are the components of the request body.

| NAME       | TYPE                | DESCRIPTION                      |
|------------|---------------------|----------------------------------|
| properties | IaaSVMBackupRequest | BackupRequestResource properties |

For the complete list of definitions of the request body and other details, refer to [trigger backups for protected items REST API document](#).

#### Example request body

The following request body defines properties required to trigger a backup for a protected item. If the retention is not specified, it will be retained for 30 days from the time of trigger of the backup job.

```
{
 "properties": {
 "objectType": "IaaSVMBackupRequest",
 "recoveryPointExpiryTimeInUTC": "2018-12-01T02:16:20.3156909Z"
 }
}
```

#### Responses

Triggering an on-demand backup is an [asynchronous operation](#). It means this operation creates another operation that needs to be tracked separately.

It returns two responses: 202 (Accepted) when another operation is created and then 200 (OK) when that operation completes.

| NAME         | TYPE | DESCRIPTION |
|--------------|------|-------------|
| 202 Accepted |      | Accepted    |

#### Example responses

Once you submit the *POST* request for an on-demand backup, the initial response is 202 (Accepted) with a location header or Azure-async-header.

```
HTTP/1.1 202 Accepted
Pragma: no-cache
Retry-After: 60
Azure-AsyncOperation: https://management.azure.com/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/testVaultRG/providers/microsoft.recoveryservices/vaults/testVault/backupFabrics/Azure/protectionContainers/iaasvmcontainer;iaasvmcontainerv2;testVaultRG;testVM/protectedItems/vm;testRG;testVM/operationsStatus/b8daecaa-f8f5-44ed-9f18-491a9e9ba01f?api-version=2019-05-13
X-Content-Type-Options: nosniff
x-ms-request-id: 7885ca75-c7c6-43fb-a38c-c0cc437d8810
x-ms-client-request-id: 7df8e874-1d66-4f81-8e91-da2fe054811d; 7df8e874-1d66-4f81-8e91-da2fe054811d
Strict-Transport-Security: max-age=31536000; includeSubDomains
x-ms-ratelimit-remaining-subscription-writes: 1199
x-ms-correlation-request-id: 7885ca75-c7c6-43fb-a38c-c0cc437d8810
x-ms-routing-request-id: SOUTHHINDIA:20180521T083541Z:7885ca75-c7c6-43fb-a38c-c0cc437d8810
Cache-Control: no-cache
Date: Mon, 21 May 2018 08:35:41 GMT
Location: https://management.azure.com/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/testVaultRG/providers/microsoft.recoveryservices/vaults/testVault/backupFabrics/Azure/protectionContainers/iaasvmcontainer;iaasvmcontainerv2;testVaultRG;testVM/protectedItems/vm;testRG;testVM/operationResults/b8daecaa-f8f5-44ed-9f18-491a9e9ba01f?api-version=2019-05-13
X-Powered-By: ASP.NET
```

Then track the resulting operation using the location header or Azure-AsyncOperation header with a simple *GET*

command.

```
GET https://management.azure.com/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/testVaultRG/providers/microsoft.recoveryservices/vaults/testVault/backupFabrics/Azure/protectionContainers/iaasvmcontainer;iaasvmcontainerv2;testRG;testVM/protectedItems/vm;testRG;testVM/operationsStatus/a0866047-6fc7-4ac3-ba38-fb0ae8aa550f?api-version=2019-05-13
```

Once the operation completes, it returns 200 (OK) with the ID of the resulting backup job in the response body.

```
HTTP/1.1 200 OK
Pragma: no-cache
X-Content-Type-Options: nosniff
x-ms-request-id: a8b13524-2c95-445f-b107-920806f385c1
x-ms-client-request-id: 5a63209d-3708-4e69-a75f-9499f4c8977c; 5a63209d-3708-4e69-a75f-9499f4c8977c
Strict-Transport-Security: max-age=31536000; includeSubDomains
x-ms-ratelimit-remaining-subscription-reads: 14995
x-ms-correlation-request-id: a8b13524-2c95-445f-b107-920806f385c1
x-ms-routing-request-id: SOUTHINDIA:20180521T083723Z:a8b13524-2c95-445f-b107-920806f385c1
Cache-Control: no-cache
Date: Mon, 21 May 2018 08:37:22 GMT
Server: Microsoft-IIS/8.0
X-Powered-By: ASP.NET

{
 "id": "00000000-0000-0000-0000-000000000000",
 "name": "00000000-0000-0000-0000-000000000000",
 "status": "Succeeded",
 "startTime": "2018-05-21T08:35:40.9488967Z",
 "endTime": "2018-05-21T08:35:40.9488967Z",
 "properties": {
 "objectType": "OperationStatusJobExtendedInfo",
 "jobId": "7ddead57-bcb9-4269-ac31-6a1b57588700"
 }
}
```

Since the backup job is a long running operation, it needs to be tracked as explained in the [monitor jobs using REST API document](#).

## Modify the backup configuration for a protected Azure VM

### Changing the policy of protection

To change the policy with which VM is protected, you can use the same format as [enabling protection](#). Just provide the new policy ID in [the request body](#) and submit the request. For example: To change the policy of testVM from 'DefaultPolicy' to 'ProdPolicy', provide the 'ProdPolicy' ID in the request body.

```
{
 "properties": {
 "protectedItemType": "Microsoft.Compute/virtualMachines",
 "sourceResourceId": "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/testRG/providers/Microsoft.Compute/virtualMachines/testVM",
 "policyId": "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/testVaultRG/providers/microsoft.recoveryservices/vaults/testVault/backupPolicies/ProdPolicy"
 }
}
```

The response will follow the same format as mentioned [for enabling protection](#)

### Stop protection but retain existing data

To remove protection on a protected VM but retain the data already backed up, remove the policy in the request

body and submit the request. Once the association with policy is removed, backups are no longer triggered and no new recovery points are created.

```
{
 "properties": {
 "protectedItemType": "Microsoft.Compute/virtualMachines",
 "sourceResourceId": "/subscriptions/00000000-0000-0000-0000-
00000000/resourceGroups/testRG/providers/Microsoft.Compute/virtualMachines/testVM",
 "policyId": ""
 }
}
```

The response will follow the same format as mentioned [for triggering an on-demand backup](#). The resultant job should be tracked as explained in the [monitor jobs using REST API document](#).

### Stop protection and delete data

To remove the protection on a protected VM and delete the backup data as well, perform a delete operation as detailed [here](#).

Stopping protection and deleting data is a *DELETE* operation.

```
DELETE
https://management.azure.com/Subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Micro
soft.RecoveryServices/vaults/{vaultName}/backupFabrics/{fabricName}/protectionContainers/{containerName}/prote
ctedItems/{protectedItemName}?api-version=2019-05-13
```

The `{containerName}` and `{protectedItemName}` are as constructed [above](#). `{fabricName}` is "Azure". For our example, this translates to:

```
DELETE https://management.azure.com//Subscriptions/00000000-0000-0000-0000-
00000000/resourceGroups/testVaultRG/providers/Microsoft.RecoveryServices/vaults/testVault/backupFabrics/Az
ure/protectionContainers/iaasvmcontainer;iaasvmcontainerv2;testRG;testVM/protectedItems/vm;iaasvmcontainerv2;t
estRG;testVM?api-version=2019-05-13
```

### Responses

*DELETE* protection is an [asynchronous operation](#). It means this operation creates another operation that needs to be tracked separately.

It returns two responses: 202 (Accepted) when another operation is created and then 204 (NoContent) when that operation completes.

| NAME          | TYPE | DESCRIPTION |
|---------------|------|-------------|
| 204 NoContent |      | NoContent   |
| 202 Accepted  |      | Accepted    |

### IMPORTANT

In order to protect against accidental delete scenarios, there is a [soft-delete feature available](#) for Recovery services vault. If the soft-delete state of the vault is set to enabled, then the delete operation will NOT immediately delete the data. It will be kept for 14 days and then permanently purged. Customer is not charged for storage for this 14 days period. To undo the deletion operation, refer to the [undo-delete section](#).

### Undo the stop protection and delete data

Undoing the accidental deletion is similar to creating the backup item. After undoing the deletion, the item is retained but no future backups are triggered.

Undo deletion is a *PUT* operation which is very similar to [changing the policy](#) and/or [enabling the protection](#). Just provide the intent to undo the deletion with the variable *isRehydrate* in [the request body](#) and submit the request. For example: To undo the deletion for testVM, the following request body should be used.

```
{
 "properties": {
 "protectedItemType": "Microsoft.Compute/virtualMachines",
 "protectionState": "ProtectionStopped",
 "sourceResourceId": "/subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/testRG/providers/Microsoft.Compute/virtualMachines/testVM",
 "isRehydrate": true
 }
}
```

The response will follow the same format as mentioned [for triggering an on-demand backup](#). The resultant job should be tracked as explained in the [monitor jobs using REST API](#) document.

## Next steps

[Restore data from an Azure Virtual machine backup](#).

For more information on the Azure Backup REST APIs, see the following documents:

- [Azure Recovery Services provider REST API](#)
- [Get started with Azure REST API](#)

# Restore Azure Virtual machines using REST API

11/18/2019 • 4 minutes to read • [Edit Online](#)

Once the backup of an Azure virtual machine using Azure Backup is completed, one can restore entire Azure Virtual machines or disks or files from the same backup copy. This article describes how to restore an Azure VM or disks using REST API.

For any restore operation, one has to identify the relevant recovery point first.

## Select Recovery point

The available recovery points of a backup item can be listed using the [list recovery point REST API](#). It is a simple *GET* operation with all the relevant values.

```
GET
https://management.azure.com/Subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.RecoveryServices/vaults/{vaultName}/backupFabrics/{fabricName}/protectionContainers/{containerName}/protectedItems/{protectedItemName}/recoveryPoints?api-version=2019-05-13
```

The `{containerName}` and `{protectedItemName}` are as constructed [here](#). `{fabricName}` is "Azure".

The *GET* URI has all the required parameters. There is no need for an additional request body

### Responses

| NAME   | TYPE                                      | DESCRIPTION |
|--------|-------------------------------------------|-------------|
| 200 OK | <a href="#">RecoveryPointResourceList</a> | OK          |

### Example response

Once the *GET* URI is submitted, a 200 (OK) response is returned.

```
HTTP/1.1 200 OK
Pragma: no-cache
X-Content-Type-Options: nosniff
x-ms-request-id: 03453538-2f8d-46de-8374-143ccdf60f40
x-ms-client-request-id: c48f4436-ce3f-42da-b537-12710d4d1a24; c48f4436-ce3f-42da-b537-12710d4d1a24
Strict-Transport-Security: max-age=31536000; includeSubDomains
x-ms-ratelimit-remaining-subscription-reads: 14998
x-ms-correlation-request-id: 03453538-2f8d-46de-8374-143ccdf60f40
x-ms-routing-request-id: SOUTHINDIA:20180604T071851Z:03453538-2f8d-46de-8374-143ccdf60f40
Cache-Control: no-cache
Date: Mon, 04 Jun 2018 07:18:51 GMT
Server: Microsoft-IIS/8.0
X-Powered-By: ASP.NET

{
 "value": [
 {
 "id": "/subscriptions/00000000-0000-0000-0000-
000000000000/resourceGroups/testVaultRG/providers/microsoft.recoveryservices/vaults/testVault/backupFabrics/Az
ure/protectionContainers/iaasvmcontainer;iaasvmcontainerv2;testRG;testVM/protectedItems/VM;testRG;testVM/recov
eryPoints/20982486783671",
 "name": "20982486783671",
 "type": "Microsoft.RecoveryServices/vaults/backupFabrics/protectionContainers/protectedItems/recoveryPoints",
 "properties": {
```

```

 "objectType": "IaaSVMRecoveryPoint",
 "recoveryPointType": "AppConsistent",
 "recoveryPointTime": "2018-06-04T06:06:00.5121087Z",
 "recoveryPointAdditionalInfo": "",
 "sourceVMStorageType": "NormalStorage",
 "isSourceVMEncrypted": false,
 "isInstantIlrSessionActive": false,
 "recoveryPointTierDetails": [
 {
 "type": 1,
 "status": 1
 },
 {
 "type": 2,
 "status": 1
 }
],
 "isManagedVirtualMachine": true,
 "virtualMachineSize": "Standard_A1_v2",
 "originalStorageAccountOption": false
},
{
 "id": "/subscriptions/00000000-0000-0000-0000-
000000000000/resourceGroups/testVaultRG/providers/microsoft.recoveryservices/vaults/testVault/backupFabrics/Az
ure/protectionContainers/iaasvmcontainer;iaasvmcontainerv2;testRG;testVM/protectedItems/VM;testRG;testVM/recov
eryPoints/23358112038108",
 "name": "23358112038108",
 "type": "Microsoft.RecoveryServices/vaults/backupFabrics/protectionContainers/protectedItems/recoveryPoints",
 "properties": {
 "objectType": "IaaSVMRecoveryPoint",
 "recoveryPointType": "CrashConsistent",
 "recoveryPointTime": "2018-06-03T06:20:56.3043878Z",
 "recoveryPointAdditionalInfo": "",
 "sourceVMStorageType": "NormalStorage",
 "isSourceVMEncrypted": false,
 "isInstantIlrSessionActive": false,
 "recoveryPointTierDetails": [
 {
 "type": 1,
 "status": 1
 },
 {
 "type": 2,
 "status": 1
 }
],
 "isManagedVirtualMachine": true,
 "virtualMachineSize": "Standard_A1_v2",
 "originalStorageAccountOption": false
 }
},
.....

```

The recovery point is identified with the `{name}` field in the above response.

## Restore disks

If there is a need to customize the creation of a VM from the backup data, one can just restore disks into a chosen storage account and create a VM from those disks as per their requirements. The storage account should be in the same region as the recovery services vault and should not be zone redundant. The disks as well as the configuration of the backed-up VM ("vmconfig.json") will be stored in the given storage account.

Triggering restore disks is a *POST* request. To know more about the Restore disks operation, refer to the "[trigger](#)

restore" REST API.

POST

<https://management.azure.com/Subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.RecoveryServices/vaults/{vaultName}/backupFabrics/{fabricName}/protectionContainers/{containerName}/protectedItems/{protectedItemName}/recoveryPoints/{recoveryPointId}/restore?api-version=2019-05-13>

The `{containerName}` and `{protectedItemName}` are as constructed [here](#). `{fabricName}` is "Azure" and the `{recoveryPointId}` is the `{name}` field of the recovery point mentioned [above](#).

### Create request body

To trigger a disk restore from an Azure VM backup, following are the components of the request body.

| NAME       | TYPE                                 | DESCRIPTION                      |
|------------|--------------------------------------|----------------------------------|
| properties | <a href="#">IaaSVMRestoreRequest</a> | RestoreRequestResourceProperties |

For the complete list of definitions of the request body and other details, refer to [trigger Restore REST API document](#).

### Example request

The following request body defines properties required to trigger a disk restore.

```
{
 "properties": {
 "objectType": "IaaSVMRestoreRequest",
 "recoveryPointId": "20982486783671",
 "recoveryType": "RestoreDisks",
 "sourceResourceId": "/subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/testRG/providers/Microsoft.Compute/virtualMachines/testVM",
 "storageAccountId": "/subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/testRG/providers/Microsoft.Storage/storageAccounts/testAccount",
 "region": "westus",
 "createNewCloudService": false,
 "originalStorageAccountOption": false,
 "encryptionDetails": {
 "encryptionEnabled": false
 }
 }
}
```

### Response

The triggering of a restore disk is an [asynchronous operation](#). It means this operation creates another operation that needs to be tracked separately.

It returns two responses: 202 (Accepted) when another operation is created and then 200 (OK) when that operation completes.

| NAME         | TYPE | DESCRIPTION |
|--------------|------|-------------|
| 202 Accepted |      | Accepted    |

### Example responses

Once you submit the *POST* URI for triggering restore disks, the initial response is 202 (Accepted) with a location header or Azure-async-header.

```

HTTP/1.1 202 Accepted
Pragma: no-cache
Retry-After: 60
Azure-AsyncOperation: https://management.azure.com/subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/testVaultRG/providers/microsoft.recoveryservices/vaults/testVault/backupFabrics/Az
ure/protectionContainers/iaasvmcontainer;iaasvmcontainerv2;testRG;testVM/protectedItems/vm;testRG;testVM/opera
tionsStatus/781a0f18-e250-4d73-b059-5e9ffed4069e?api-version=2019-05-13
X-Content-Type-Options: nosniff
x-ms-request-id: 893fe372-8d6c-4c56-b589-45a95eeef95f
x-ms-client-request-id: a15ce064-25bd-4ac6-87e5-e3bc6ec65c0b; a15ce064-25bd-4ac6-87e5-e3bc6ec65c0b
Strict-Transport-Security: max-age=31536000; includeSubDomains
x-ms-ratelimit-remaining-subscription-writes: 1198
x-ms-correlation-request-id: 893fe372-8d6c-4c56-b589-45a95eeef95f
x-ms-routing-request-id: SOUTHINDIA:20180604T130003Z:893fe372-8d6c-4c56-b589-45a95eeef95f
Cache-Control: no-cache
Date: Mon, 04 Jun 2018 13:00:03 GMT
Location: https://management.azure.com/subscriptions//subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/testVaultRG/providers/microsoft.recoveryservices/vaults/testVault/backupFabrics/Az
ure/protectionContainers/iaasvmcontainer;iaasvmcontainerv2;testRG;testVM/protectedItems/vm;testRG;testVM/opera
tionResults/781a0f18-e250-4d73-b059-5e9ffed4069e?api-version=2019-05-13
X-Powered-By: ASP.NET

```

Then track the resulting operation using the location header or Azure-AsyncOperation header with a simple *GET* command.

```

GET https://management.azure.com/subscriptions//subscriptions/00000000-0000-0000-0000-
0000000000/resourceGroups/testVaultRG/providers/microsoft.recoveryservices/vaults/testVault/backupFabrics/Az
ure/protectionContainers/iaasvmcontainer;iaasvmcontainerv2;testRG;testVM/protectedItems/vm;testRG;testVM/opera
tionResults/781a0f18-e250-4d73-b059-5e9ffed4069e?api-version=2019-05-13

```

Once the operation completes, it returns 200 (OK) with the ID of the resulting restore job in the response body.

```

HTTP/1.1 200 OK
Pragma: no-cache
X-Content-Type-Options: nosniff
x-ms-request-id: ea2a8011-eb83-4a4b-9ed2-e694070a966a
x-ms-client-request-id: a7f3a144-ed80-41ee-bffe-ae6a90c35a2f; a7f3a144-ed80-41ee-bffe-ae6a90c35a2f
Strict-Transport-Security: max-age=31536000; includeSubDomains
x-ms-ratelimit-remaining-subscription-reads: 14973
x-ms-correlation-request-id: ea2a8011-eb83-4a4b-9ed2-e694070a966a
x-ms-routing-request-id: SOUTHINDIA:20180604T130917Z:ea2a8011-eb83-4a4b-9ed2-e694070a966a
Cache-Control: no-cache
Date: Mon, 04 Jun 2018 13:09:17 GMT
Server: Microsoft-IIS/8.0
X-Powered-By: ASP.NET

{
 "id": "781a0f18-e250-4d73-b059-5e9ffed4069e",
 "name": "781a0f18-e250-4d73-b059-5e9ffed4069e",
 "status": "Succeeded",
 "startTime": "2018-06-04T13:00:03.8068176Z",
 "endTime": "2018-06-04T13:00:03.8068176Z",
 "properties": {
 "objectType": "OperationStatusJobExtendedInfo",
 "jobId": "3021262a-fb3a-4538-9b37-e3e97a386093"
 }
}

```

Since the backup job is a long running operation, it should be tracked as explained in the [monitor jobs using REST API document](#).

Once the long running job is complete, the disks and the configuration of the backed up virtual machine

("VMConfig.json") will be present in the given storage account.

## Restore as another virtual machine

Select the recovery point and create the request body as specified below to create another Azure Virtual machine with the data from the recovery point.

The following request body defines properties required to trigger a virtual machine restore.

```
{
 "parameters": {
 "subscriptionId": "00000000-0000-0000-0000-000000000000",
 "resourceGroupName": "testVaultRG",
 "vaultName": "testVault",
 "fabricName": "Azure",
 "containerName": "IaaSVMContainer;iaasvmcontainerv2;testRG;testVM",
 "protectedItemName": "VM;iaasvmcontainerv2;testRG;testVM",
 "recoveryPointId": "348916168024334",
 "api-version": "2019-05-13",
 "parameters": {
 "properties": {
 "objectType": "IaaSVMRestoreRequest",
 "recoveryPointId": "348916168024334",
 "recoveryType": "AlternateLocation",
 "sourceResourceId": "/subscriptions/00000000-0000-0000-0000-
000000000000/resourceGroups/testRG/providers/Microsoft.Compute/virtualMachines/testVM",
 "targetVirtualMachineId": "/subscriptions/00000000-0000-0000-0000-
000000000000/resourceGroups/targetRG/providers/Microsoft.Compute/virtualmachines/targetVM",
 "targetResourceGroupId": "/subscriptions/00000000-0000-0000-0000-
000000000000/resourceGroups/targetRG",
 "storageAccountId": "/subscriptions/00000000-0000-0000-0000-
000000000000/resourceGroups/testRG/providers/Microsoft.Storage/storageAccounts/testingAccount",
 "virtualNetworkId": "/subscriptions/00000000-0000-0000-0000-
000000000000/resourceGroups/targetRG/providers/Microsoft.Network/virtualNetworks/testNet",
 "subnetId": "/subscriptions/00000000-0000-0000-0000-
000000000000/resourceGroups/targetRG/providers/Microsoft.Network/virtualNetworks/testNet/subnets/default",
 "region": "westus",
 "createNewCloudService": false,
 "originalStorageAccountOption": false,
 "encryptionDetails": {
 "encryptionEnabled": false
 }
 }
 }
}
```

The response should be handled in the same way as [explained above for restoring disks](#).

## Next steps

For more information on the Azure Backup REST APIs, see the following documents:

- [Azure Recovery Services provider REST API](#)
- [Get started with Azure REST API](#)

# Track backup and restore jobs using REST API

11/18/2019 • 2 minutes to read • [Edit Online](#)

Azure Backup service triggers jobs that run in background in various scenarios such as triggering backup, restore operations, disabling backup. These jobs can be tracked using their IDs.

## Fetch Job information from operations

An operation such as triggering backup will always return a jobID. For example: The final response of a [trigger backup REST API operation](#) is as follows:

```
{
 "id": "cd153561-20d3-467a-b911-cc1de47d4763",
 "name": "cd153561-20d3-467a-b911-cc1de47d4763",
 "status": "Succeeded",
 "startTime": "2018-09-12T02:16:56.7399752Z",
 "endTime": "2018-09-12T02:16:56.7399752Z",
 "properties": {
 "objectType": "OperationStatusJobExtendedInfo",
 "jobId": "41f3e94b-ae6b-4a20-b422-65abfcf03e5"
 }
}
```

The Azure VM backup job is identified by "jobId" field and can be tracked as mentioned [here](#) using a simple *GET* request.

## Tracking the job

GET

```
https://management.azure.com/Subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.RecoveryServices/vaults/{vaultName}/backupJobs/{jobName}?api-version=2019-05-13
```

The `{jobName}` is "jobId" mentioned above. The response is always 200 OK with the "status" field indicating the current status of the job. Once it is "Completed" or "CompletedWithWarnings", the 'extendedInfo' section reveals more details about the job.

### Response

| NAME   | TYPE                        | DESCRIPTION |
|--------|-----------------------------|-------------|
| 200 OK | <a href="#">JobResource</a> | OK          |

### Example response

Once the *GET* URL is submitted, a 200 (OK) response is returned.

HTTP/1.1 200 OK  
Pragma: no-cache  
X-Content-Type-Options: nosniff  
x-ms-request-id: e9702101-9da2-4681-bdf3-a54e17329a56  
x-ms-client-request-id: ba4dff71-1655-4c1d-a71f-c9869371b18b; ba4dff71-1655-4c1d-a71f-c9869371b18b  
Strict-Transport-Security: max-age=31536000; includeSubDomains  
x-ms-ratelimit-remaining-subscription-reads: 14989  
x-ms-correlation-request-id: e9702101-9da2-4681-bdf3-a54e17329a56  
x-ms-routing-request-id: SOUTHINDIA:20180521T102317Z:e9702101-9da2-4681-bdf3-a54e17329a56  
Cache-Control: no-cache  
Date: Mon, 21 May 2018 10:23:17 GMT  
Server: Microsoft-IIS/8.0  
X-Powered-By: ASP.NET

```
{
 "id": "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/Default-RecoveryServices-
ResourceGroup-centralindia/providers/microsoft.recoveryservices/vaults/abdemovault/backupJobs/7ddead57-bcb9-
4269-ac31-6a1b57588700",
 "name": "7ddead57-bcb9-4269-ac31-6a1b57588700",
 "type": "Microsoft.RecoveryServices/vaults/backupJobs",
 "properties": {
 "jobType": "AzureIaaSVMJob",
 "duration": "00:20:23.0896697",
 "actionsInfo": [
 {
 "virtualMachineVersion": "Compute",
 "extendedInfo": {
 "tasksList": [
 {
 "taskId": "Take Snapshot",
 "duration": "00:00:00",
 "status": "Completed"
 },
 {
 "taskId": "Transfer data to vault",
 "duration": "00:00:00",
 "status": "Completed"
 }
],
 "propertyBag": {
 "VM Name": "uttestvmub1",
 "Backup Size": "2332 MB"
 }
 },
 "entityFriendlyName": "uttestvmub1",
 "backupManagementType": "AzureIaaSVM",
 "operation": "Backup",
 "status": "Completed",
 "startTime": "2018-05-21T08:35:40.9488967Z",
 "endTime": "2018-05-21T08:56:04.0385664Z",
 "activityId": "7df8e874-1d66-4f81-8e91-da2fe054811d"
 }
]
 }
}
```

# Azure Resource Manager templates for Azure Backup

11/18/2019 • 2 minutes to read • [Edit Online](#)

The following table includes links to Azure Resource Manager templates for use with Recovery Services vaults and Azure Backup features. To learn about the JSON syntax and properties, see [Microsoft.RecoveryServices resource types](#).

| <b>Recovery Services vault</b>                               |                                                                                                                                                                                                                      |
|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Create a Recovery Services vault</a>             | Create a Recovery Services vault. The vault can be used for Azure Backup and Azure Site Recovery.                                                                                                                    |
| <b>Back up virtual machines</b>                              |                                                                                                                                                                                                                      |
| <a href="#">Back up Resource Manager VMs</a>                 | Use the existing Recovery Services vault and Backup policy to back up Resource Manager-virtual machines in the same resource group.                                                                                  |
| <a href="#">Back up IaaS VMs to Recovery Services vault</a>  | Template to back up classic and Resource Manager-virtual machines.                                                                                                                                                   |
| <a href="#">Create Weekly Backup policy for IaaS VMs</a>     | Template creates Recovery Services vault and a weekly backup policy, which is used to back up classic and Resource Manager-virtual machines.                                                                         |
| <a href="#">Create Daily Backup policy for IaaS VMs</a>      | Template creates Recovery Services vault and a daily backup policy, which is used to back up classic and Resource Manager-virtual machines.                                                                          |
| <a href="#">Deploy Windows Server VM with backup enabled</a> | Template creates a Windows Server VM and Recovery Services vault with the default backup policy enabled.                                                                                                             |
| <b>Monitor Backup jobs</b>                                   |                                                                                                                                                                                                                      |
| <a href="#">Use Azure Monitor logs with Azure Backup</a>     | Template deploys Azure Monitor logs with Azure Backup, which allows you to monitor backup and restore jobs, backup alerts, and the Cloud storage used in your Recovery Services vaults.                              |
| <b>Back up SQL Server in Azure VM</b>                        |                                                                                                                                                                                                                      |
| <a href="#">Back up SQL Server in Azure VM</a>               | Template creates a Recovery Services Vault and Workload specific Backup Policy. It Registers the VM with Azure Backup service and Configures Protection on that VM. Currently, it only works for SQL Gallery images. |
|                                                              |                                                                                                                                                                                                                      |

# Use Role-Based Access Control to manage Azure Backup recovery points

1/16/2020 • 3 minutes to read • [Edit Online](#)

Azure Role-Based Access Control (RBAC) enables fine-grained access management for Azure. Using RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs.

## IMPORTANT

Roles provided by Azure Backup are limited to actions that can be performed in Azure portal or via REST API or Recovery Services vault PowerShell or CLI cmdlets. Actions performed in Azure backup Agent Client UI or System center Data Protection Manager UI or Azure Backup Server UI are out of control of these roles.

Azure Backup provides three built-in roles to control backup management operations. Learn more on [Azure RBAC built-in roles](#)

- **Backup Contributor** - This role has all permissions to create and manage backup except deleting Recovery Services vault and giving access to others. Imagine this role as admin of backup management who can do every backup management operation.
- **Backup Operator** - This role has permissions to everything a contributor does except removing backup and managing backup policies. This role is equivalent to contributor except it can't perform destructive operations such as stop backup with delete data or remove registration of on-premises resources.
- **Backup Reader** - This role has permissions to view all backup management operations. Imagine this role to be a monitoring person.

If you're looking to define your own roles for even more control, see how to [build Custom roles](#) in Azure RBAC.

## Mapping Backup built-in roles to backup management actions

The following table captures the Backup management actions and corresponding minimum RBAC role required to perform that operation.

| MANAGEMENT OPERATION           | MINIMUM RBAC ROLE REQUIRED  | SCOPE REQUIRED                              |
|--------------------------------|-----------------------------|---------------------------------------------|
| Create Recovery Services vault | Backup Contributor          | Resource group containing the vault         |
| Enable backup of Azure VMs     | Backup Operator             | Resource group containing the vault         |
|                                | Virtual Machine Contributor | VM resource                                 |
| On-demand backup of VM         | Backup Operator             | Recovery Services vault                     |
| Restore VM                     | Backup Operator             | Recovery Services vault                     |
|                                | Contributor                 | Resource group in which VM will be deployed |

| MANAGEMENT OPERATION                                                             | MINIMUM RBAC ROLE REQUIRED  | SCOPE REQUIRED                                                                                                        |
|----------------------------------------------------------------------------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------|
|                                                                                  | Virtual Machine Contributor | Source VM that got backed up                                                                                          |
| Restore unmanaged disks VM backup                                                | Backup Operator             | Recovery Services vault                                                                                               |
|                                                                                  | Virtual Machine Contributor | Source VM that got backed up                                                                                          |
|                                                                                  | Storage Account Contributor | Storage account resource where disks are going to be restored                                                         |
| Restore managed disks from VM backup                                             | Backup Operator             | Recovery Services vault                                                                                               |
|                                                                                  | Virtual Machine Contributor | Source VM that got backed up                                                                                          |
|                                                                                  | Storage Account Contributor | Temporary Storage account selected as part of restore to hold data from vault before converting them to managed disks |
|                                                                                  | Contributor                 | Resource group to which managed disk(s) will be restored                                                              |
| Restore individual files from VM backup                                          | Backup Operator             | Recovery Services vault                                                                                               |
|                                                                                  | Virtual Machine Contributor | Source VM that got backed up                                                                                          |
| Create backup policy for Azure VM backup                                         | Backup Contributor          | Recovery Services vault                                                                                               |
| Modify backup policy of Azure VM backup                                          | Backup Contributor          | Recovery Services vault                                                                                               |
| Delete backup policy of Azure VM backup                                          | Backup Contributor          | Recovery Services vault                                                                                               |
| Stop backup (with retain data or delete data) on VM backup                       | Backup Contributor          | Recovery Services vault                                                                                               |
| Register on-premises Windows Server/client/SCDPM or Azure Backup Server          | Backup Operator             | Recovery Services vault                                                                                               |
| Delete registered on-premises Windows Server/client/SCDPM or Azure Backup Server | Backup Contributor          | Recovery Services vault                                                                                               |

#### IMPORTANT

If you specify VM Contributor at a VM resource scope and click on Backup as part of VM settings, it will open 'Enable Backup' screen even though VM is already backed up as the call to verify backup status works only at subscription level. To avoid this, either go to vault and open the backup item view of the VM or specify VM Contributor role at a subscription level.

## Minimum role requirements for the Azure File share backup

The following table captures the Backup management actions and corresponding role required to perform Azure File share operation.

| MANAGEMENT OPERATION                  | ROLE REQUIRED               | RESOURCES                                                                         |
|---------------------------------------|-----------------------------|-----------------------------------------------------------------------------------|
| Enable backup of Azure File shares    | Backup Contributor          | Recovery Services vault                                                           |
|                                       | Storage Account             | Contributor Storage account resource                                              |
| On-demand backup of VM                | Backup Operator             | Recovery Services vault                                                           |
| Restore File share                    | Backup Operator             | Recovery Services vault                                                           |
|                                       | Storage Account Contributor | Storage account resources where restore source and Target file shares are present |
| Restore Individual Files              | Backup Operator             | Recovery Services vault                                                           |
|                                       | Storage Account Contributor | Storage account resources where restore source and Target file shares are present |
| Stop protection                       | Backup Contributor          | Recovery Services vault                                                           |
| Unregister storage account from vault | Backup Contributor          | Recovery Services vault                                                           |
|                                       | Storage Account Contributor | Storage account resource                                                          |

## Next steps

- [Role Based Access Control](#): Get started with RBAC in the Azure portal.
- Learn how to manage access with:
  - [PowerShell](#)
  - [Azure CLI](#)
  - [REST API](#)
- [Role-Based Access Control troubleshooting](#): Get suggestions for fixing common issues.

# Security features to help protect cloud workloads that use Azure Backup

2/27/2020 • 12 minutes to read • [Edit Online](#)

Concerns about security issues, like malware, ransomware, and intrusion, are increasing. These security issues can be costly, in terms of both money and data. To guard against such attacks, Azure Backup now provides security features to help protect backup data even after deletion.

One such feature is soft delete. With soft delete, even if a malicious actor deletes the backup of a VM (or backup data is accidentally deleted), the backup data is retained for 14 additional days, allowing the recovery of that backup item with no data loss. The additional 14 days retention of backup data in the "soft delete" state don't incur any cost to the customer. Azure also encrypts all the backed-up data at rest using [Storage Service Encryption](#) to further secure your data.

Soft delete protection for Azure virtual machines is generally available.

## NOTE

Soft delete for SQL server in Azure VM and soft delete for SAP HANA in Azure VM workloads is now available in preview. To sign up for the preview, write to us at [AskAzureBackupTeam@microsoft.com](mailto:AskAzureBackupTeam@microsoft.com)

## Soft delete

### Soft delete for VMs

Soft delete for VMs protects the backups of your VMs from unintended deletion. Even after the backups are deleted, they are preserved in soft-delete state for 14 additional days.

## NOTE

Soft delete only protects deleted backup data. If a VM is deleted without a backup, the soft-delete feature will not preserve the data. All resources should be protected with Azure Backup to ensure full resilience.

### Supported regions

Soft delete is currently supported in the West Central US, East Asia, Canada Central, Canada East, France Central, France South, Korea Central, Korea South, UK South, UK West, Australia East, Australia South East, North Europe, West US, West US2, Central US, South East Asia, North Central US, South Central US, Japan East, Japan West, India South, India Central, India West, East US 2, Switzerland North, Switzerland West, and all National regions.

### Soft delete for VMs using Azure portal

1. To delete the backup data of a VM, the backup must be stopped. In the Azure portal, go to your recovery services vault, right-click on the backup item and choose **Stop backup**.

2. In the following window, you will be given a choice to delete or retain the backup data. If you choose **Delete backup data** and then **Stop backup**, the VM backup will not be permanently deleted. Rather, the backup data will be retained for 14 days in the soft deleted state. If **Delete backup data** is chosen, a delete email alert is sent to the configured email ID informing the user that 14 days remain of extended retention for backup data. Also, an email alert is sent on the 12th day informing that there are two more days left to resurrect the deleted data. The deletion is deferred until the 15th day, when permanent deletion will occur and a final email alert is sent informing about the permanent deletion of the data.

3. During those 14 days, in the Recovery Services Vault, the soft deleted VM will appear with a red "soft-delete" icon next to it.

**Backup Items (Azure Virtual Machine)**

sogupsoftdeletevault

Refresh Add Filter

Fetching data from service completed.

Filter items ...

| NAME            | RESOURCE GROUP | BACKUP PRE-CHECK | LAST BACKUP STATUS       | LATEST RESTORE POINT   | ... |
|-----------------|----------------|------------------|--------------------------|------------------------|-----|
| softdel-vm-am-2 | softdeleterg   | Passed           | Warning(Backup disabled) | 8/13/2019, 12:39:32 PM | ... |

#### NOTE

If any soft-deleted backup items are present in the vault, the vault cannot be deleted at that time. Please try vault deletion after the backup items are permanently deleted, and there is no item in soft deleted state left in the vault.

- To restore the soft-deleted VM, it must first be undeleted. To undelete, choose the soft-deleted VM, and then select the option **Undelete**.

softdel-vm-am-2

Backup Item

Backup now Restore VM File Recovery Stop backup Resume backup Delete backup data **Undelete**

The restore points for this backup item have been deleted and retained in the soft delete state. They were deleted 11 days ago and will be available for 3 more days to recover after which they will be permanently deleted. For more information, click here.

| Alerts and Jobs                                 | Backup status                               | Summary                                                     |
|-------------------------------------------------|---------------------------------------------|-------------------------------------------------------------|
| <a href="#">View all Alerts</a> (last 24 hours) | Backup Pre-Check Passed                     | Recovery services vault sogupsoftdeletevault                |
| <a href="#">View all Jobs</a> (last 24 hours)   | Last backup status Warning(Backup disabled) | Backup policy -                                             |
|                                                 |                                             | Oldest restore point 8/13/2019, 12:39:32 PM (13 day(s) ago) |

Restore points (1)

This list is filtered for last 30 days of restore points. To recover from restore point older than 30 days, click here.

| TIME                   | CONSISTENCY            | RECOVERY TYPE      |
|------------------------|------------------------|--------------------|
| 8/13/2019, 12:39:32 PM | Application Consistent | Snapshot and Vault |

A window will appear warning that if undelete is chosen, all restore points for the VM will be undeleted and available for performing a restore operation. The VM will be retained in a “stop protection with retain data” state with backups paused and backup data retained forever with no backup policy effective.

The screenshot shows the Azure Recovery Services vault interface. A specific backup item, 'softdel-vm-am-2', is selected. In the top right corner, there is a modal dialog titled 'Undelete softdel-vm-am-2'. The dialog contains the following information:

- Alerts and Jobs**: Shows 'View all Alerts' (last 24 hours) and 'View all Jobs' (last 24 hours).
- Backup status**: Shows 'Backup Pre-Check' as Passed and 'Last backup status' as Warning(Backup disabled).
- Summary**: Shows 'Recovery services vault' as 'sogupsoftdeletevault', 'Backup policy' as none, and 'Oldest restore point' as 8/13/2019, 12:39:32 PM.
- Restore points (1)**: Shows one restore point: 'TIME' 8/13/2019, 12:39:32 PM, 'CONSISTENCY' Application Consistent, 'RECOVERY TYPE' Snapshot and Vault.
- Action Buttons**: 'Undelete' (highlighted with a red box) and 'Cancel'.

Note: All restore points for this backup item will be undeleted and the item will come to 'Stop protection with retain data' state. You can 'Resume backup' to continue the scheduled backup operations as per the selected policy.

Note: Garbage Collection will start with resume backup operation and all the expired restore points will be cleaned.

At this point, you can also restore the VM by selecting **Restore VM** from the chosen restore point.

The screenshot shows the Azure Recovery Services vault interface. A specific backup item, 'softdel-vm-am-2', is selected. In the top right corner, there is a modal dialog with a red box around the 'Restore VM' button. The dialog contains the following information:

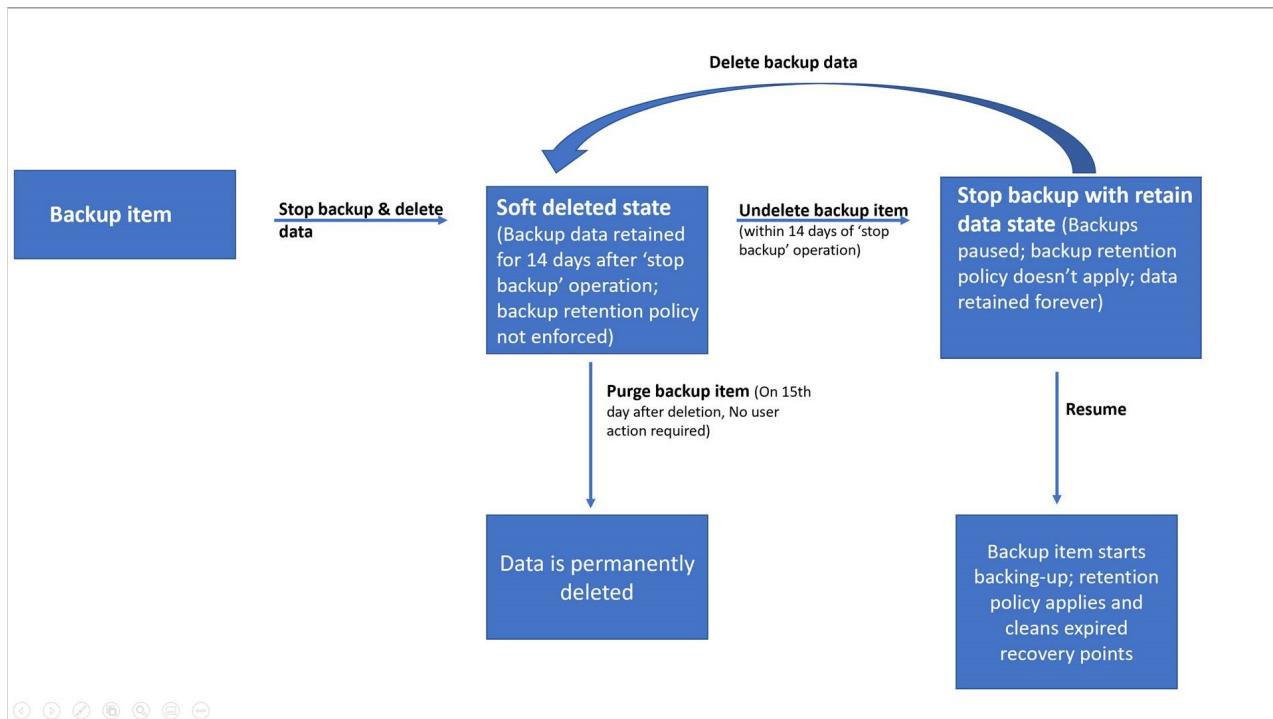
- Alerts and Jobs**: Shows 'View all Alerts' (last 24 hours) and 'View all Jobs' (last 24 hours).
- Backup status**: Shows 'Backup Pre-Check' as Passed and 'Last backup status' as Warning(Backup disabled).
- Summary**: Shows 'Recovery services vault' as 'sogupsoftdeletevault', 'Backup policy' as none, and 'Oldest restore point' as 8/13/2019, 12:39:32 PM (9 day(s) ago).
- Restore points (1)**: Shows one restore point: 'TIME' 8/13/2019, 12:39:32 PM, 'CONSISTENCY' Application Consistent, 'RECOVERY TYPE' Snapshot and Vault.
- Action Buttons**: 'Restore VM' (highlighted with a red box), 'File Recovery', and '...'. A callout box points to the 'Restore VM' and 'File Recovery' buttons.

#### NOTE

Garbage collector will run and clean expired recovery points only after the user performs the **Resume backup** operation.

- After the undelete process is completed, the status will return to "Stop backup with retain data" and then you can choose **Resume backup**. The **Resume backup** operation brings back the backup item in the active state, associated with a backup policy selected by the user defining the backup and retention schedules.

This flow chart shows the different steps and states of a backup item when Soft Delete is enabled:



For more information, see the [Frequently Asked Questions](#) section below.

## Soft delete for VMs using Azure Powershell

### IMPORTANT

The Az.RecoveryServices version required to use soft-delete using Azure PS is min 2.2.0. Use

```
Install-Module -Name Az.RecoveryServices -Force
```

As outlined above for Azure portal, the sequence of steps is same while using Azure Powershell as well.

### Delete the backup item using Azure Powershell

Delete the backup item using the [Disable-AzRecoveryServicesBackupProtection](#) PS cmdlet.

```
Disable-AzRecoveryServicesBackupProtection -Item $myBkpItem -RemoveRecoveryPoints -VaultId $myVaultID -Force
```

| WorkloadName                                   | Operation        | Status    | StartTime             | EndTime               |
|------------------------------------------------|------------------|-----------|-----------------------|-----------------------|
| JobID                                          |                  |           |                       |                       |
| AppVM1<br>0488c3c2-accc-4a91-a1e0-fba09a67d2fb | DeleteBackupData | Completed | 12/5/2019 12:44:15 PM | 12/5/2019 12:44:50 PM |

The 'DeleteState' of the backup item will change from 'NotDeleted' to 'ToBeDeleted'. The backup data will be retained for 14 days. If you wish to revert the delete operation, then undo-delete should be performed.

#### Undoing the deletion operation using Azure Powershell

First, fetch the relevant backup item that is in soft-delete state (that is, about to be deleted).

```
Get-AzRecoveryServicesBackupItem -BackupManagementType AzureVM -WorkloadType AzureVM -VaultId $myVaultID | Where-Object {$_._.DeleteState -eq "ToBeDeleted"}

Name ContainerType ContainerUniqueName
WorkloadType ProtectionStatus HealthStatus DeleteState

---- VM;iaasvmcontainerv2;selfhosted;AppVM1 AzureVM iaasvmcontainerv2;selfhosted;AppVM1
AzureVM Healthy Passed ToBeDeleted

$myBkpItem = Get-AzRecoveryServicesBackupItem -BackupManagementType AzureVM -WorkloadType AzureVM -VaultId
$myVaultID -Name AppVM1
```

Then, perform the undo-deletion operation using the [Undo-AzRecoveryServicesBackupItemDeletion](#) PS cmdlet.

```
Undo-AzRecoveryServicesBackupItemDeletion -Item $myBkpItem -VaultId $myVaultID -Force

WorkloadName Operation Status StartTime EndTime
JobID

---- AppVM1 Undelete Completed 12/5/2019 12:47:28 PM 12/5/2019 12:47:40 PM
65311982-3755-46b5-8e53-c82ea4f0d2a2
```

The 'DeleteState' of the backup item will revert to 'NotDeleted'. But the protection is still stopped. You need to [resume the backup](#) to re-enable the protection.

#### Soft delete for VMs using REST API

- Delete the backups using REST API as mentioned [here](#).
- If user wishes to undo these delete operations, refer to steps mentioned [here](#).

## Disabling soft delete

Soft delete is enabled by default on newly created vaults to protect backup data from accidental or malicious deletes. Disabling this feature is not recommended. The only circumstance where you should consider disabling soft delete is if you are planning on moving your protected items to a new vault, and cannot wait the 14 days required before deleting and reprotecting (such as in a test environment.) Only the vault owner can disable this feature. If you disable this feature, all future deletions of protected items will result in immediate removal, without the ability to restore. Backup data that exists in soft deleted state prior to disabling this feature, will remain in soft deleted state for the period of 14 days. If you wish to permanently delete these immediately, then you need to undelete and delete them again to get permanently deleted.

#### Disabling soft delete using Azure portal

To disable soft delete, follow these steps:

1. In the Azure portal, go to your vault, and then go to **Settings** -> **Properties**.
2. In the properties pane, select **Security Settings** -> **Update**.
3. In the security settings pane, under **Soft Delete**, select **Disable**.

## Disabling soft delete using Azure Powershell

### IMPORTANT

The Az.RecoveryServices version required to use soft-delete using Azure PS is min 2.2.0. Use

```
Install-Module -Name Az.RecoveryServices -Force
```

To disable, use the [Set-AzRecoveryServicesVaultBackupProperty](#) PS cmdlet.

```
Set-AzRecoveryServicesVaultProperty -VaultId $myVaultID -SoftDeleteFeatureState Disable

StorageModelType :
StorageType :
StorageTypeState :
EnhancedSecurityState : Enabled
SoftDeleteFeatureState : Disabled
```

## Disabling soft delete using REST API

To disable the soft-delete functionality using REST API, refer to the steps mentioned [here](#).

## Permanently deleting soft deleted backup items

Backup data in soft deleted state prior disabling this feature, will remain in soft deleted state. If you wish to permanently delete these immediately, then undelete and delete them again to get permanently deleted.

### Using Azure portal

Follow these steps:

1. Follow the steps to [disable soft delete](#).
2. In the Azure portal, go to your vault, go to **Backup Items**, and choose the soft deleted VM.

**Backup Items (Azure Virtual Machine)**

Fetching data from service completed.

| NAME            | RESOURCE GROUP | BACKUP PRE-CHECK | LAST BACKUP STATUS       | LATEST RESTORE POINT   |
|-----------------|----------------|------------------|--------------------------|------------------------|
| softdel-vm-am-2 | softdeleterg   | Passed           | Warning(Backup disabled) | 8/13/2019, 12:39:32 PM |

### 3. Select the option **Undelete**.

**softdel-vm-am-2**

**Undelete**

The restore points for this backup item have been deleted and retained in the soft delete state. They were deleted 11 days ago and will be available for 3 more days to recover after which they will be permanently deleted. For more information, [Click here.](#)

| Alerts and Jobs                                 | Backup status                                                                    | Summary                                                      |
|-------------------------------------------------|----------------------------------------------------------------------------------|--------------------------------------------------------------|
| <a href="#">View all Alerts</a> (last 24 hours) | Backup Pre-Check <span style="color: green;">Passed</span>                       | Recovery services vault: <b>sogupsoftdeletevault</b>         |
| <a href="#">View all Jobs</a> (last 24 hours)   | Last backup status: <span style="color: orange;">Warning(Backup disabled)</span> | Backup policy: -                                             |
|                                                 |                                                                                  | Oldest restore point: 8/13/2019, 12:39:32 PM (13 day(s) ago) |

**Restore points (1)**

This list is filtered for last 30 days of restore points. To recover from restore point older than 30 days, [click here.](#)

| TIME                   | CONSISTENCY            | RECOVERY TYPE      |
|------------------------|------------------------|--------------------|
| 8/13/2019, 12:39:32 PM | Application Consistent | Snapshot and Vault |

### 4. A window will appear. Select **Undelete**.

**Undelete softdel-vm-am-2**

All restore points for this backup item will be undeleted and the item will come to 'Stop protection with retain data' state. You can 'Resume backup' to continue the scheduled backup operations as per the selected policy.

Note: Garbage Collection will start with resume backup operation and all the expired restore points will be cleared.

**Backup item:** softdel-vm-am-2  
**Deletion time:** 8/20/2019, 6:45:57 PM (1 day(s) ago)  
**Day(s) left until permanent deletion:** 2

**Undelete** **Cancel**

| TIME                   | CONSISTENCY            | RECOVERY TYPE      |
|------------------------|------------------------|--------------------|
| 8/13/2019, 12:39:32 PM | Application Consistent | Snapshot and Vault |

### 5. Choose **Delete backup data** to permanently delete the backup data.

6. Type the name of the backup item to confirm that you want to delete the recovery points.

## Stop Backup

SkipTransMac1

Delete Backup Data

This option will stop all scheduled backup jobs, deletes backup data and can't be undone.

\* Type the name of Backup Item  
SkipTransMac1

Reason (optional)  
0 selected

Comments

**Stop backup**

7. To delete the backup data for the item, select **Delete**. A notification message lets you know that the backup data has been deleted.

### Using Azure Powershell

If items were deleted before soft-delete was disabled, then they will be in a soft-deleted state. To immediately delete them, the deletion operation needs to be reversed and then performed again.

Identify the items that are in soft-deleted state.

```
Get-AzRecoveryServicesBackupItem -BackupManagementType AzureVM -WorkloadType AzureVM -VaultId $myVaultID |
Where-Object {$_.DeleteState -eq "ToBeDeleted"}
```

| Name                                   | WorkloadType | ProtectionStatus | ContainerType                       | ContainerUniqueName |
|----------------------------------------|--------------|------------------|-------------------------------------|---------------------|
| DeleteState                            | HealthStatus | Pass             | Pass                                | Pass                |
| VM;iaasvmcontainerv2;selfhosted;AppVM1 | AzureVM      | Passed           | iaasvmcontainerv2;selfhosted;AppVM1 | ToBeDeleted         |
| AzureVM                                | Healthy      | Pass             | Pass                                | Pass                |

```
$myBkpItem = Get-AzRecoveryServicesBackupItem -BackupManagementType AzureVM -WorkloadType AzureVM -VaultId
$myVaultID -Name AppVM1
```

Then reverse the deletion operation that was performed when soft-delete was enabled.

| Undo-AzRecoveryServicesBackupItemDeletion -Item \$myBkpItem -VaultId \$myVaultID -Force |           |           |                       |                       |
|-----------------------------------------------------------------------------------------|-----------|-----------|-----------------------|-----------------------|
| WorkloadName                                                                            | Operation | Status    | StartTime             | EndTime               |
| JobID                                                                                   |           |           |                       |                       |
| -----                                                                                   | -----     | -----     | -----                 | -----                 |
| AppVM1                                                                                  | Undelete  | Completed | 12/5/2019 12:47:28 PM | 12/5/2019 12:47:40 PM |
| 65311982-3755-46b5-8e53-c82ea4f0d2a2                                                    |           |           |                       |                       |

Since the soft-delete is now disabled, the deletion operation will result in immediate removal of backup data.

| Disable-AzRecoveryServicesBackupProtection -Item \$myBkpItem -RemoveRecoveryPoints -VaultId \$myVaultID -Force |                  |           |                       |                       |
|----------------------------------------------------------------------------------------------------------------|------------------|-----------|-----------------------|-----------------------|
| WorkloadName                                                                                                   | Operation        | Status    | StartTime             | EndTime               |
| JobID                                                                                                          |                  |           |                       |                       |
| -----                                                                                                          | -----            | -----     | -----                 | -----                 |
| AppVM1                                                                                                         | DeleteBackupData | Completed | 12/5/2019 12:44:15 PM | 12/5/2019 12:44:50 PM |
| 0488c3c2-accc-4a91-a1e0-fba09a67d2fb                                                                           |                  |           |                       |                       |

## Using REST API

If items were deleted before soft-delete was disabled, then they will be in a soft-deleted state. To immediately delete them, the deletion operation needs to be reversed and then performed again.

1. First, undo the delete operations with the steps mentioned [here](#).
2. Then disable the soft-delete functionality using REST API using the steps mentioned [here](#).
3. Then delete the backups using REST API as mentioned [here](#).

## Encryption

### Encryption of backup data using Microsoft managed keys

Backup data is automatically encrypted using Azure Storage encryption. Encryption protects your data and helps you to meet your organizational security and compliance commitments. Data is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant. Azure Storage encryption is similar to BitLocker encryption on Windows.

Within Azure, data in transit between Azure storage and the vault is protected by HTTPS. This data remains on the Azure backbone network.

For more information, see [Azure Storage encryption for data at rest](#). Refer to the [Azure Backup FAQ](#) to answer any questions that you may have about encryption.

### Encryption of backup data using customer managed keys

While backing up Azure Virtual Machines, you also have the option to encrypt your backup data in the Recovery Services Vault using your encryption keys stored in the Azure Key Vault.

#### NOTE

This feature is currently under early use. Fill out [this survey](#) if you wish to encrypt your backup data using customer managed keys. Note that the ability to use this feature is subject to approval from the Azure Backup service.

### Backup of managed disk VM encrypted using customer managed keys

Azure Backup allows you to back up Azure Virtual Machines containing disks encrypted using customer managed keys. For details, refer to [Encryption of managed disks with customer managed keys](#).

## Backup of encrypted VMs

You can back up and restore Windows or Linux Azure virtual machines (VMs) with encrypted disks using the Azure Backup service. For instructions, see [Back up and restore encrypted virtual machines with Azure Backup](#).

## Other security features

### Protection of Azure Backup recovery points

Storage accounts used by recovery services vaults are isolated and cannot be accessed by users for any malicious purposes. The access is only allowed through Azure Backup management operations, such as restore. These management operations are controlled through Role-Based Access Control (RBAC).

For more information, see [Use Role-Based Access Control to manage Azure Backup recovery points](#).

## Frequently asked questions

### For Soft delete

#### Do I need to enable the soft-delete feature on every vault?

No, it's built and enabled by default for all the recovery services vaults.

#### Can I configure the number of days for which my data will be retained in soft-deleted state after delete operation is complete?

No, it is fixed to 14 days of additional retention after the delete operation.

#### Do I need to pay the cost for this additional 14-day retention?

No, this 14-day additional retention comes for free of cost as a part of soft-delete functionality.

#### Can I perform a restore operation when my data is in soft delete state?

No, you need to undelete the soft deleted resource in order to restore. The undelete operation will bring the resource back into the **Stop protection with retain data state** where you can restore to any point in time. Garbage collector remains paused in this state.

#### Will my snapshots follow the same lifecycle as my recovery points in the vault?

Yes.

#### How can I trigger the scheduled backups again for a soft-deleted resource?

Undelete followed by resume operation will protect the resource again. Resume operation associates a backup policy to trigger the scheduled backups with the selected retention period. Also, the garbage collector runs as soon as the resume operation completes. If you wish to perform a restore from a recovery point that is past its expiry date, you are advised to do it before triggering the resume operation.

#### Can I delete my vault if there are soft deleted items in the vault?

The Recovery Services vault cannot be deleted if there are backup items in soft-deleted state in the vault. The soft-deleted items are permanently deleted 14 days after the delete operation. If you cannot wait for 14 days, then [disable soft delete](#), undelete the soft deleted items, and delete them again to permanently get deleted. After ensuring there are no protected items and no soft deleted items, the vault can be deleted.

#### Can I delete the data earlier than the 14 days soft-delete period after deletion?

No. You cannot force delete the soft-deleted items, they are automatically deleted after 14 days. This security feature is enabled to safeguard the backed-up data from accidental or malicious deletes. You should wait for 14 day before performing any other action on the VM. Soft-deleted items will not be charged. If you need reprotecting the VMs marked for soft-delete within 14 days to a new vault, then contact Microsoft support.

#### Can soft delete operations be performed in PowerShell or CLI?

Soft delete operations can be performed using [Powershell](#). Currently, CLI is not supported.

#### Is soft delete supported for other cloud workloads, like SQL Server in Azure VMs and SAP HANA in Azure VMs?

No. Currently soft delete is only supported for Azure virtual machines.

## Next steps

- Read about [Security controls for Azure Backup](#).

# Security features to help protect hybrid backups that use Azure Backup

2/24/2020 • 7 minutes to read • [Edit Online](#)

Concerns about security issues, like malware, ransomware, and intrusion, are increasing. These security issues can be costly, in terms of both money and data. To guard against such attacks, Azure Backup now provides security features to help protect hybrid backups. This article covers how to enable and use these features, by using an Azure Recovery Services agent and Azure Backup Server. These features include:

- **Prevention.** An additional layer of authentication is added whenever a critical operation like changing a passphrase is performed. This validation is to ensure that such operations can be performed only by users who have valid Azure credentials.
- **Alerting.** An email notification is sent to the subscription admin whenever a critical operation like deleting backup data is performed. This email ensures that the user is notified quickly about such actions.
- **Recovery.** Deleted backup data is retained for an additional 14 days from the date of the deletion. This ensures recoverability of the data within a given time period, so there is no data loss even if an attack happens. Also, a greater number of minimum recovery points are maintained to guard against corrupt data.

## NOTE

Security features should not be enabled if you are using infrastructure as a service (IaaS) VM backup. These features are not yet available for IaaS VM backup, so enabling them will not have any impact. Security features should be enabled only if you are using:

- **Azure Backup agent.** Minimum agent version 2.0.9052. After you have enabled these features, you should upgrade to this agent version to perform critical operations.
- **Azure Backup Server.** Minimum Azure Backup agent version 2.0.9052 with Azure Backup Server update 1.
- **System Center Data Protection Manager.** Minimum Azure Backup agent version 2.0.9052 with Data Protection Manager 2012 R2 UR12 or Data Protection Manager 2016 UR2.

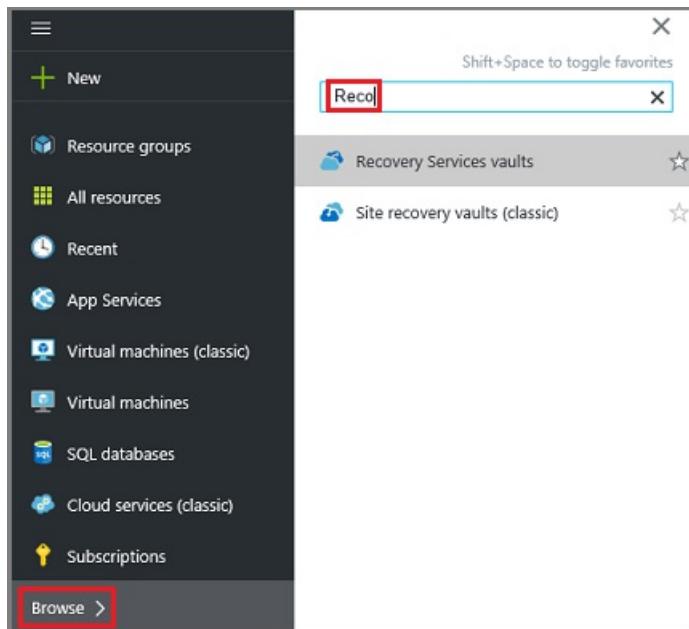
## NOTE

These features are available only for Recovery Services vault. All the newly created Recovery Services vaults have these features enabled by default. For existing Recovery Services vaults, users enable these features by using the steps mentioned in the following section. After the features are enabled, they apply to all the Recovery Services agent computers, Azure Backup Server instances, and Data Protection Manager servers registered with the vault. Enabling this setting is a one-time action, and you cannot disable these features after enabling them.

## Enable security features

If you are creating a Recovery Services vault, you can use all the security features. If you are working with an existing vault, enable security features by following these steps:

1. Sign in to the Azure portal by using your Azure credentials.
2. Select **Browse**, and type **Recovery Services**.



The list of recovery services vaults appears. From this list, select a vault. The selected vault dashboard opens.

3. From the list of items that appears under the vault, under **Settings**, click **Properties**.

IgnitelaaSDemoVault -  
Recovery Services vault

Search (Ctrl+ /)

- Overview
- Activity log
- Diagnose and solve problems

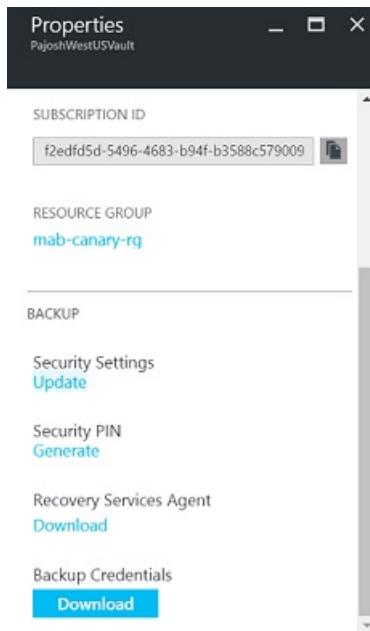
SETTINGS

- Properties
- Locks
- Automation script

GETTING STARTED

- Backup
- Site Recovery

4. Under **Security Settings**, click **Update**.



The update link opens the **Security Settings** blade, which provides a summary of the features and lets you enable them.

5. From the drop-down list **Have you configured Azure Multi-Factor Authentication?**, select a value to confirm if you have enabled [Azure Multi-Factor Authentication](#). If it is enabled, you are asked to authenticate from another device (for example, a mobile phone) while signing in to the Azure portal.

When you perform critical operations in Backup, you have to enter a security PIN, available on the Azure portal. Enabling Azure Multi-Factor Authentication adds a layer of security. Only authorized users with valid Azure credentials, and authenticated from a second device, can access the Azure portal.

6. To save security settings, select **Enable** and click **Save**. You can select **Enable** only after you select a value from the **Have you configured Azure Multi-Factor Authentication?** list in the previous step.

**Security Settings**  
IgniteSecurityDemoVault

 Save  Discard

## Configuration

Have you configured [Azure Multi-Factor Authentication](#)?

Yes



Use the following versions to enable Security features:

- MAB agent – use minimum agent version 2.0.9052
- Azure backup server – use minimum MAB agent version 2.0.9052 with Azure Backup Server upgrade 1
- DPM – use minimum MAB agent version 2.0.9052 with DPM 2012 R2 UR12 or DPM 2016 UR2

### Security Features

Enabled

Disable

\* Security features cannot be disabled, once enabled.

## Security Features

|                                         | ENABLED                                                     | DISABLED                                                      |
|-----------------------------------------|-------------------------------------------------------------|---------------------------------------------------------------|
| <b>Retention of deleted backup data</b> | ✓ Backup data retained for 14 days after delete operation   | ⚠ Instant deletion prevents recoverability from attacks       |
| <b>Minimum retention range checks</b>   | ✓ Ensures more than one recovery point in case of attacks   | ⚠ Only one recovery point available for recovery              |
| <b>Alerts and notifications</b>         | ✓ For critical operations like Stop backup with delete data | ⚠ No security alerts or notifications for critical operations |
| <b>Multiple layers of security</b>      | ✓ Security PIN required for critical operations             | ⚠ Single layer of protection                                  |

## Recover deleted backup data

Backup retains deleted backup data for an additional 14 days, and does not delete it immediately if the **Stop backup with delete backup data** operation is performed. To restore this data in the 14-day period, take the following steps, depending on what you are using:

For **Azure Recovery Services** agent users:

1. If the computer where backups were happening is still available, re-protect the deleted data sources, and use the [Recover data to the same machine](#) in Azure Recovery Services, to recover from all the old recovery points.
2. If this computer is not available, use [Recover to an alternate machine](#) to use another Azure Recovery Services computer to get this data.

For **Azure Backup Server** users:

1. If the server where backups were happening is still available, re-protect the deleted data sources, and use the [Recover Data](#) feature to recover from all the old recovery points.
2. If this server is not available, use [Recover data from another Azure Backup Server](#) to use another Azure Backup Server instance to get this data.

For **Data Protection Manager** users:

1. If the server where backups were happening is still available, re-protect the deleted data sources, and use the **Recover Data** feature to recover from all the old recovery points.
2. If this server is not available, use [Add External DPM](#) to use another Data Protection Manager server to get this data.

## Prevent attacks

Checks have been added to make sure only valid users can perform various operations. These include adding an extra layer of authentication, and maintaining a minimum retention range for recovery purposes.

### Authentication to perform critical operations

As part of adding an extra layer of authentication for critical operations, you are prompted to enter a security PIN when you perform **Stop Protection with Delete data** and **Change Passphrase** operations.

#### NOTE

Currently, security pin is not supported for **Stop Protection with Delete data** for DPM and MABS.

To receive this PIN:

1. Sign in to the Azure portal.
2. Browse to **Recovery Services vault > Settings > Properties**.
3. Under **Security PIN**, click **Generate**. This opens a blade that contains the PIN to be entered in the Azure Recovery Services agent user interface. This PIN is valid for only five minutes, and it gets generated automatically after that period.

### Maintain a minimum retention range

To ensure that there are always a valid number of recovery points available, the following checks have been added:

- For daily retention, a minimum of **seven** days of retention should be done.
- For weekly retention, a minimum of **four** weeks of retention should be done.
- For monthly retention, a minimum of **three** months of retention should be done.
- For yearly retention, a minimum of **one** year of retention should be done.

## Notifications for critical operations

Typically, when a critical operation is performed, the subscription admin is sent an email notification with details about the operation. You can configure additional email recipients for these notifications by using the Azure portal.

The security features mentioned in this article provide defense mechanisms against targeted attacks. More importantly, if an attack happens, these features give you the ability to recover your data.

## Troubleshooting errors

| OPERATION | ERROR DETAILS | RESOLUTION |
|-----------|---------------|------------|
|-----------|---------------|------------|

| OPERATION         | ERROR DETAILS                                                                                                                                                                                                                | RESOLUTION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Policy change     | The backup policy could not be modified. Error: The current operation failed due to an internal service error [0x29834]. Please retry the operation after sometime. If the issue persists, please contact Microsoft support. | <p><b>Cause:</b><br/>This error comes when security settings are enabled, you try to reduce retention range below the minimum values specified above and you are on unsupported version (supported versions are specified in first note of this article).</p> <p><b>Recommended Action:</b><br/>In this case, you should set retention period above the minimum retention period specified (seven days for daily, four weeks for weekly, three weeks for monthly or one year for yearly) to proceed with policy-related updates. Optionally, preferred approach would be to update backup agent, Azure Backup Server and/or DPM UR to leverage all the security updates.</p>    |
| Change Passphrase | Security PIN entered is incorrect. (ID: 100130) Provide the correct Security PIN to complete this operation.                                                                                                                 | <p><b>Cause:</b><br/>This error comes when you enter invalid or expired Security PIN while performing critical operation (like change passphrase).</p> <p><b>Recommended Action:</b><br/>To complete the operation, you must enter valid Security PIN. To get the PIN, sign in to Azure portal and navigate to Recovery Services vault &gt; Settings &gt; Properties &gt; Generate Security PIN. Use this PIN to change passphrase.</p>                                                                                                                                                                                                                                         |
| Change Passphrase | Operation failed. ID: 120002                                                                                                                                                                                                 | <p><b>Cause:</b><br/>This error comes when security settings are enabled, you try to change passphrase and you are on unsupported version (valid versions specified in first note of this article).</p> <p><b>Recommended Action:</b><br/>To change passphrase, you must first update backup agent to minimum version minimum 2.0.9052, Azure Backup server to minimum update 1, and/or DPM to minimum DPM 2012 R2 UR12 or DPM 2016 UR2 (download links below), then enter valid Security PIN. To get the PIN, sign in to Azure portal and navigate to Recovery Services vault &gt; Settings &gt; Properties &gt; Generate Security PIN. Use this PIN to change passphrase.</p> |

## Next steps

- [Get started with Azure Recovery Services vault](#) to enable these features.
- [Download the latest Azure Recovery Services agent](#) to help protect Windows computers and guard your backup data against attacks.
- [Download the latest Azure Backup Server](#) to help protect workloads and guard your backup data against

attacks.

- Download UR12 for System Center 2012 R2 Data Protection Manager or download UR2 for System Center 2016 Data Protection Manager to help protect workloads and guard your backup data against attacks.

# Security controls for Azure Backup

11/18/2019 • 2 minutes to read • [Edit Online](#)

This article documents the security controls built into Azure Backup.

A security control is a quality or feature of an Azure service that contributes to the service's ability to prevent, detect, and respond to security vulnerabilities.

For each control, we use "Yes" or "No" to indicate whether it is currently in place for the service, "N/A" for a control that is not applicable to the service. We might also provide a note or links to more information about an attribute.

## Network

| SECURITY CONTROL                          | YES/NO | NOTES                                                                                                            | DOCUMENTATION |
|-------------------------------------------|--------|------------------------------------------------------------------------------------------------------------------|---------------|
| Service endpoint support                  | No     |                                                                                                                  |               |
| VNet injection support                    | No     |                                                                                                                  |               |
| Network isolation and firewalling support | Yes    | Forced tunneling is supported for VM backup. Forced tunneling is not supported for workloads running inside VMs. |               |
| Forced tunneling support                  | No     |                                                                                                                  |               |

## Monitoring & logging

| SECURITY CONTROL                                             | YES/NO | NOTES                                                                                                                                                  | DOCUMENTATION |
|--------------------------------------------------------------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Azure monitoring support (Log analytics, App insights, etc.) | Yes    | Log Analytics is supported via resource logs. For more information, see <a href="#">Monitor Azure Backup protected workloads using Log Analytics</a> . |               |
| Control and management plane logging and audit               | Yes    | All customer triggered actions from the Azure portal are logged to activity logs.                                                                      |               |
| Data plane logging and audit                                 | No     | Azure Backup data plane can't be reached directly.                                                                                                     |               |

## Identity

| SECURITY CONTROL | YES/NO | NOTES                                                                                                                                                               |  | DOCUMENTATION |
|------------------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|---------------|
| Authentication   | Yes    | Authentication is through Azure Active Directory.                                                                                                                   |  |               |
| Authorization    | Yes    | Customer created and built-in RBAC roles are used. For more information, see <a href="#">Use Role-Based Access Control to manage Azure Backup recovery points</a> . |  |               |

## Data protection

| SECURITY CONTROL                                                                                      | YES/NO | NOTES                                                  |  | DOCUMENTATION |
|-------------------------------------------------------------------------------------------------------|--------|--------------------------------------------------------|--|---------------|
| Server-side encryption at rest: Microsoft-managed keys                                                | Yes    | Using storage service encryption for storage accounts. |  |               |
| Server-side encryption at rest: customer-managed keys (BYOK)                                          | No     |                                                        |  |               |
| Column level encryption (Azure Data Services)                                                         | No     |                                                        |  |               |
| Encryption in transit (such as ExpressRoute encryption, in VNet encryption, and VNet-VNet encryption) | No     | Using HTTPS.                                           |  |               |
| API calls encrypted                                                                                   | Yes    |                                                        |  |               |

## Configuration management

| SECURITY CONTROL                                                     | YES/NO | NOTES |  | DOCUMENTATION |
|----------------------------------------------------------------------|--------|-------|--|---------------|
| Configuration management support (versioning of configuration, etc.) | Yes    |       |  |               |

## Next steps

- Learn more about the [built-in security controls across Azure services](#).

# Troubleshooting backup failures on Azure virtual machines

2/25/2020 • 16 minutes to read • [Edit Online](#)

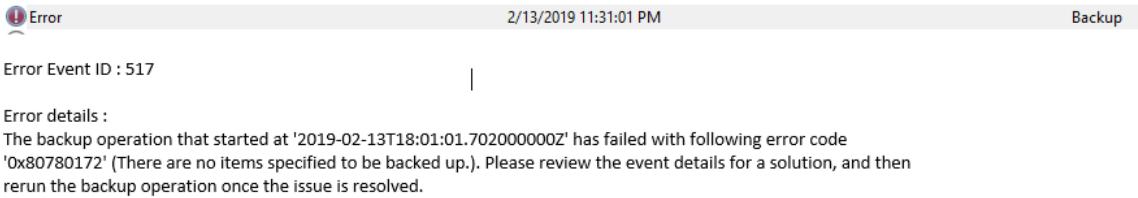
You can troubleshoot errors encountered while using Azure Backup with the information listed below:

## Backup

This section covers backup operation failure of Azure Virtual machine.

### Basic troubleshooting

- Ensure that the VM Agent (WA Agent) is the [latest version](#).
- Ensure that the Windows or Linux VM OS version is supported, refer to the [IaaS VM Backup Support Matrix](#).
- Verify that another backup service is not running.
  - To ensure there are no snapshot extension issues, [uninstall extensions to force reload and then retry the backup](#).
- Verify that the VM has internet connectivity.
  - Make sure another backup service is not running.
- From `Services.msc`, ensure the **Windows Azure Guest Agent** service is **Running**. If the **Windows Azure Guest Agent** service is missing, install it from [Back up Azure VMs in a Recovery Services vault](#).
- The **Event log** may show backup failures that are from other backup products, for example, Windows Server backup, and are not due to Azure backup. Use the following steps to determine whether the issue is with Azure Backup:
  - If there is an error with an entry **Backup** in the event source or message, check whether Azure IaaS VM Backup backups were successful, and whether a Restore Point was created with the desired snapshot type.
  - If Azure Backup is working, then the issue is likely with another backup solution.
  - Here is an example of an event viewer error 517 where Azure backup was working fine but "Windows Server Backup" was failing:



- If Azure Backup is failing, then look for the corresponding Error Code in the section Common VM backup errors in this article.

## Common issues

The following are common issues with backup failures on Azure virtual machines.

### CopyingVHDsFromBackUpVaultTakingLongTime - Copying backed up data from vault timed out

Error code: `CopyingVHDsFromBackUpVaultTakingLongTime`

Error message: Copying backed up data from vault timed out

This could happen due to transient storage errors or insufficient storage account IOPS for backup service to transfer data to the vault within the timeout period. Configure VM backup using these [best practices](#) and retry the backup operation.

## UserErrorVmNotInDesirableState - VM is not in a state that allows backups

Error code: UserErrorVmNotInDesirableState

Error message: VM is not in a state that allows backups.

The backup operation failed because the VM is in Failed state. For a successful backup, the VM state should be Running, Stopped, or Stopped (deallocated).

- If the VM is in a transient state between **Running** and **Shut down**, wait for the state to change. Then trigger the backup job.
- If the VM is a Linux VM and uses the Security-Enhanced Linux kernel module, exclude the Azure Linux Agent path **/var/lib/waagent** from the security policy and make sure the Backup extension is installed.

## UserErrorFsFreezeFailed - Failed to freeze one or more mount-points of the VM to take a file-system consistent snapshot

Error code: UserErrorFsFreezeFailed

Error message: Failed to freeze one or more mount-points of the VM to take a file-system consistent snapshot.

- Unmount the devices for which the file system state was not cleaned, using the **umount** command.
- Run a file system consistency check on these devices by using the **fsck** command.
- Mount the devices again and retry backup operation.

## ExtensionSnapshotFailedCOM / ExtensionInstallationFailedCOM / ExtensionInstallationFailedMDTC - Extension installation/operation failed due to a COM+ error

Error code: ExtensionSnapshotFailedCOM

Error message: Snapshot operation failed due to COM+ error

Error code: ExtensionInstallationFailedCOM

Error message: Extension installation/operation failed due to a COM+ error

Error code: ExtensionInstallationFailedMDTC

Error message: Extension installation failed with the error "COM+ was unable to talk to the Microsoft Distributed Transaction Coordinator"

The Backup operation failed due to an issue with Windows service **COM+ System** application. To resolve this issue, follow these steps:

- Try starting/restarting Windows service **COM+ System Application** (from an elevated command prompt - **net start COMSysApp**).
- Ensure **Distributed Transaction Coordinator** service is running as **Network Service** account. If not, change it to run as **Network Service** account and restart **COM+ System Application**.
- If unable to restart the service, then reinstall **Distributed Transaction Coordinator** service by following the below steps:
  - Stop the MSDTC service
  - Open a command prompt (cmd)

- Run command "msdtc -uninstall"
- Run command "msdtc -install"
- Start the MSDTC service
- Start the Windows service **COM+ System Application**. After the **COM+ System Application** starts, trigger a backup job from the Azure portal.

## ExtensionFailedVssWriterInBadState - Snapshot operation failed because VSS writers were in a bad state

Error code: ExtensionFailedVssWriterInBadState

Error message: Snapshot operation failed because VSS writers were in a bad state.

Restart VSS writers that are in a bad state. From an elevated command prompt, run `vssadmin list writers`. The output contains all VSS writers and their state. For every VSS writer with a state that's not **[1] Stable**, to restart VSS writer, run the following commands from an elevated command prompt:

- `net stop serviceName`
- `net start serviceName`

## ExtensionConfigParsingFailure- Failure in parsing the config for the backup extension

Error code: ExtensionConfigParsingFailure

Error message: Failure in parsing the config for the backup extension.

This error happens because of changed permissions on the **MachineKeys** directory:

**%systemdrive%\programdata\microsoft\crypto\rsa\machinekeys**. Run the following command and verify that permissions on the **MachineKeys** directory are default ones:`icacls`

**%systemdrive%\programdata\microsoft\crypto\rsa\machinekeys**.

Default permissions are as follows:

- Everyone: (R,W)
- BUILTIN\Administrators: (F)

If you see permissions in the **MachineKeys** directory that are different than the defaults, follow these steps to correct permissions, delete the certificate, and trigger the backup:

1. Fix permissions on the **MachineKeys** directory. By using Explorer security properties and advanced security settings in the directory, reset permissions back to the default values. Remove all user objects except the defaults from the directory and make sure the **Everyone** permission has special access as follows:

- List folder/read data
- Read attributes
- Read extended attributes
- Create files/write data
- Create folders/append data
- Write attributes
- Write extended attributes
- Read permissions

2. Delete all certificates where **Issued To** is the classic deployment model or **Windows Azure CRP Certificate Generator**:

- Open certificates on a local computer console.
  - Under **Personal > Certificates**, delete all certificates where **Issued To** is the classic deployment model or **Windows Azure CRP Certificate Generator**.
3. Trigger a VM backup job.

## ExtensionStuckInDeletionState - Extension state is not supportive to backup operation

Error code: ExtensionStuckInDeletionState

Error message: Extension state is not supportive to backup operation

The Backup operation failed due to inconsistent state of Backup Extension. To resolve this issue, follow these steps:

- Ensure Guest Agent is installed and responsive
- From the Azure portal, go to **Virtual Machine > All Settings > Extensions**
- Select the backup extension VmSnapshot or VmSnapshotLinux and click **Uninstall**
- After deleting backup extension, retry the backup operation
- The subsequent backup operation will install the new extension in the desired state

## ExtensionFailedSnapshotLimitReachedError - Snapshot operation failed as snapshot limit is exceeded for some of the disks attached

Error code: ExtensionFailedSnapshotLimitReachedError

Error message: Snapshot operation failed as snapshot limit is exceeded for some of the disks attached

The snapshot operation failed as the snapshot limit has exceeded for some of the disks attached. Complete the below troubleshooting steps and then retry the operation.

- Delete the disk blob-snapshots that are not required. Be cautious to not delete Disk blob, only snapshot blobs should be deleted.
- If Soft-delete is enabled on VM disk Storage-Accounts, configure soft-delete retention such that existing snapshots are less than the maximum allowed at any point of time.
- If Azure Site Recovery is enabled in the backed-up VM, then perform the steps below:
  - Ensure the value of **isanysnapshotfailed** is set as false in /etc/azure/vmbbackup.conf
  - Schedule Azure Site Recovery at a different time, such that it does not conflict the backup operation.

## ExtensionFailedTimeoutVMNetworkUnresponsive - Snapshot operation failed due to inadequate VM resources

Error code: ExtensionFailedTimeoutVMNetworkUnresponsive

Error message: Snapshot operation failed due to inadequate VM resources.

Backup operation on the VM failed due to delay in network calls while performing the snapshot operation. To resolve this issue, perform Step 1. If the issue persists, try steps 2 and 3.

### Step 1: Create snapshot through Host

From an elevated (admin) command-prompt, run the below command:

```

REG ADD "HKLM\SOFTWARE\Microsoft\BcdrAgentPersistentKeys" /v SnapshotMethod /t REG_SZ /d firstHostThenGuest
/f
REG ADD "HKLM\SOFTWARE\Microsoft\BcdrAgentPersistentKeys" /v CalculateSnapshotTimeFromHost /t REG_SZ /d True
/f

```

This will ensure the snapshots are taken through host instead of Guest. Retry the backup operation.

**Step 2:** Try changing the backup schedule to a time when the VM is under less load (less CPU/IOps etc.)

**Step 3:** Try [increasing the size of VM](#) and retry the operation

## Common VM backup errors

| ERROR DETAILS                                                                                                                                                                                                                                                                           | WORKAROUND                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Error code:</b> 320001, ResourceNotFound<br><b>Error message:</b> Could not perform the operation as VM no longer exists.<br><br><b>Error code:</b> 400094, BCMV2VMNotFound<br><b>Error message:</b> The virtual machine doesn't exist<br><br>An Azure virtual machine wasn't found. | This error happens when the primary VM is deleted, but the backup policy still looks for a VM to back up. To fix this error, take the following steps: <ol style="list-style-type: none"> <li>1. Re-create the virtual machine with the same name and same resource group name, <b>cloud service name</b>, <b>or</b></li> <li>2. Stop protecting the virtual machine with or without deleting the backup data. For more information, see <a href="#">Stop protecting virtual machines</a>.</li> </ol>                    |
| <b>Error code:</b> UserErrorBCMPremiumStorageQuotaError<br><b>Error message:</b> Could not copy the snapshot of the virtual machine, due to insufficient free space in the storage account                                                                                              | For premium VMs on VM backup stack V1, we copy the snapshot to the storage account. This step makes sure that backup management traffic, which works on the snapshot, doesn't limit the number of IOPS available to the application using premium disks.<br><br>We recommend that you allocate only 50 percent, 17.5 TB, of the total storage account space. Then the Azure Backup service can copy the snapshot to the storage account and transfer data from this copied location in the storage account to the vault. |
| <b>Error code:</b> 380008, AzureVmOffline<br><b>Error message:</b> Failed to install Microsoft Recovery Services extension as virtual machine is not running                                                                                                                            | The VM Agent is a prerequisite for the Azure Recovery Services extension. Install the Azure Virtual Machine Agent and restart the registration operation. <ol style="list-style-type: none"> <li>1. Check if the VM Agent is installed correctly.</li> <li>2. Make sure that the flag on the VM config is set correctly.</li> </ol> Read more about installing the VM Agent and how to validate the VM Agent installation.                                                                                               |
| <b>Error code:</b> ExtensionSnapshotBitlockerError<br><b>Error message:</b> The snapshot operation failed with the Volume Shadow Copy Service (VSS) operation error <b>This drive is locked by BitLocker Drive Encryption. You must unlock this drive from the Control Panel.</b>       | Turn off BitLocker for all drives on the VM and check if the VSS issue is resolved.                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Error Details                                                                                                                                                                                            | Workaround                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Error code:</b> VmNotInDesirableState<br/> <b>Error message:</b> The VM isn't in a state that allows backups.</p>                                                                                  | <ul style="list-style-type: none"> <li>If the VM is in a transient state between <b>Running</b> and <b>Shut down</b>, wait for the state to change. Then trigger the backup job.</li> <li>If the VM is a Linux VM and uses the Security-Enhanced Linux kernel module, exclude the Azure Linux Agent path <b>/var/lib/waagent</b> from the security policy and make sure the Backup extension is installed.</li> </ul>                                                                                                                                                            |
| <p>The VM Agent isn't present on the virtual machine:<br/> Install any prerequisite and the VM Agent. Then restart the operation.</p>                                                                    | <p>Read more about <a href="#">VM Agent installation</a> and <a href="#">how to validate VM Agent installation</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <p><b>Error code:</b> ExtensionSnapshotFailedNoSecureNetwork<br/> <b>Error message:</b> The snapshot operation failed because of failure to create a secure network communication channel.</p>           | <ol style="list-style-type: none"> <li>Open the Registry Editor by running <b>regedit.exe</b> in an elevated mode.</li> <li>Identify all versions of the .NET Framework present in your system. They're present under the hierarchy of registry key <b>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft</b>.</li> <li>For each .NET Framework present in the registry key, add the following key:<br/> <b>SchUseStrongCrypto</b>=dword:00000001.</li> </ol>                                                                                                                                 |
| <p><b>Error code:</b> ExtensionVCRedistInstallationFailure<br/> <b>Error message:</b> The snapshot operation failed because of failure to install Visual C++ Redistributable for Visual Studio 2012.</p> | <p>Navigate to C:\Packages\Plugins\Microsoft.Azure.RecoveryServices.VMSnapshot\agentVersion and install vcredist2013_x64. Make sure that the registry key value that allows the service installation is set to the correct value. That is, set the <b>Start</b> value in <b>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Msiserver</b> to <b>3</b> and not <b>4</b>.</p> <p>If you still have issues with installation, restart the installation service by running <b>MSIEXEC /UNREGISTER</b> followed by <b>MSIEXEC /REGISTER</b> from an elevated command prompt.</p> |

## Jobs

| Error Details                                                                                                                                                                    | Workaround                                                                                      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| <p>Cancellation isn't supported for this job type:<br/> Wait until the job finishes.</p>                                                                                         | None                                                                                            |
| <p>The job isn't in a cancelable state:<br/> Wait until the job finishes.<br/> <b>or</b><br/> The selected job isn't in a cancelable state:<br/> Wait for the job to finish.</p> | It's likely that the job is almost finished. Wait until the job is finished.                    |
| <p>Backup can't cancel the job because it isn't in progress:<br/> Cancellation is supported only for jobs in progress. Try to cancel an in-progress job.</p>                     | This error happens because of a transitory state. Wait a minute and retry the cancel operation. |
| <p>Backup failed to cancel the job:<br/> Wait until the job finishes.</p>                                                                                                        | None                                                                                            |

## Restore

| ERROR DETAILS                                                                                                                                                                                                                                         | WORKAROUND                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Restore failed with a cloud internal error.                                                                                                                                                                                                           | <ol style="list-style-type: none"><li>1. The cloud service to which you're trying to restore is configured with DNS settings. You can check:<br/><code>\$deployment = Get-AzureDeployment -ServiceName "ServiceName" -Slot "Production"</code><br/><code>Get-AzureDns -DnsSettings</code><br/><code>\$deployment.DnsSettings</code>.<br/>If <b>Address</b> is configured, then DNS settings are configured.</li><li>2. The cloud service to which you're trying to restore is configured with <b>ReservedIP</b>, and existing VMs in the cloud service are in the stopped state. You can check that a cloud service has reserved an IP by using the following PowerShell cmdlets: <code>\$deployment = Get-AzureDeployment -ServiceName "servicename" -Slot "Production"</code><br/><code>\$dep.ReservedIPName</code>.</li><li>3. You're trying to restore a virtual machine with the following special network configurations into the same cloud service:<ul style="list-style-type: none"><li>• Virtual machines under load balancer configuration, internal and external.</li><li>• Virtual machines with multiple reserved IPs.</li><li>• Virtual machines with multiple NICs.</li></ul></li><li>4. Select a new cloud service in the UI or see <a href="#">restore considerations</a> for VMs with special network configurations.</li></ol> |
| The selected DNS name is already taken:<br>Specify a different DNS name and try again.                                                                                                                                                                | This DNS name refers to the cloud service name, usually ending with <b>.cloudapp.net</b> . This name needs to be unique. If you get this error, you need to choose a different VM name during restore.<br><br>This error is shown only to users of the Azure portal. The restore operation through PowerShell succeeds because it restores only the disks and doesn't create the VM. The error will be faced when the VM is explicitly created by you after the disk restore operation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| The specified virtual network configuration isn't correct:<br>Specify a different virtual network configuration and try again.                                                                                                                        | None                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| The specified cloud service is using a reserved IP that doesn't match the configuration of the virtual machine being restored:<br>Specify a different cloud service that isn't using a reserved IP. Or choose another recovery point to restore from. | None                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| The cloud service has reached its limit on the number of input endpoints:<br>Retry the operation by specifying a different cloud service or by using an existing endpoint.                                                                            | None                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| ERROR DETAILS                                                                                                                                                                                                                                  | WORKAROUND                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>The Recovery Services vault and target storage account are in two different regions:</p> <p>Make sure the storage account specified in the restore operation is in the same Azure region as your Recovery Services vault.</p>               | None                                                                                                                                                                                          |
| <p>The storage account specified for the restore operation isn't supported:</p> <p>Only Basic or Standard storage accounts with locally redundant or geo-redundant replication settings are supported. Select a supported storage account.</p> | None                                                                                                                                                                                          |
| <p>The type of storage account specified for the restore operation isn't online:</p> <p>Make sure that the storage account specified in the restore operation is online.</p>                                                                   | This error might happen because of a transient error in Azure Storage or because of an outage. Choose another storage account.                                                                |
| <p>The resource group quota has been reached:</p> <p>Delete some resource groups from the Azure portal or contact Azure Support to increase the limits.</p>                                                                                    | None                                                                                                                                                                                          |
| <p>The selected subnet doesn't exist:</p> <p>Select a subnet that exists.</p>                                                                                                                                                                  | None                                                                                                                                                                                          |
| <p>The Backup service doesn't have authorization to access resources in your subscription.</p>                                                                                                                                                 | To resolve this error, first restore disks by using the steps in <a href="#">Restore backed-up disks</a> . Then use the PowerShell steps in <a href="#">Create a VM from restored disks</a> . |

## Backup or restore takes time

If your backup takes more than 12 hours, or restore takes more than 6 hours, review [best practices](#), and [performance considerations](#)

## VM Agent

### Set up the VM Agent

Typically, the VM Agent is already present in VMs that are created from the Azure gallery. But virtual machines that are migrated from on-premises datacenters won't have the VM Agent installed. For those VMs, the VM Agent needs to be installed explicitly.

#### Windows VMs

- Download and install the [agent MSI](#). You need Administrator privileges to finish the installation.
- For virtual machines created by using the classic deployment model, [update the VM property](#) to indicate that the agent is installed. This step isn't required for Azure Resource Manager virtual machines.

#### Linux VMs

- Install the latest version of the agent from the distribution repository. For details on the package name, see the [Linux Agent repository](#).
- For VMs created by using the classic deployment model, [use this blog](#) to update the VM property and verify that the agent is installed. This step isn't required for Resource Manager virtual machines.

### Update the VM Agent

#### Windows VMs

- To update the VM Agent, reinstall the [VM Agent binaries](#). Before you update the agent, make sure no backup

operations occur during the VM Agent update.

#### Linux VMs

- To update the Linux VM Agent, follow the instructions in the article [Updating the Linux VM Agent](#).

##### NOTE

Always use the distribution repository to update the agent.

Don't download the agent code from GitHub. If the latest agent isn't available for your distribution, contact the distribution support for instructions to acquire the latest agent. You can also check the latest [Windows Azure Linux agent](#) information in the GitHub repository.

#### Validate VM Agent installation

Verify the VM Agent version on Windows VMs:

- Sign in to the Azure virtual machine and navigate to the folder **C:\WindowsAzure\Packages**. You should find the **WaAppAgent.exe** file.
- Right-click the file and go to **Properties**. Then select the **Details** tab. The **Product Version** field should be 2.6.1198.718 or higher.

## Troubleshoot VM snapshot issues

VM backup relies on issuing snapshot commands to underlying storage. Not having access to storage or delays in a snapshot task run can cause the backup job to fail. The following conditions can cause snapshot task failure:

- VMs with SQL Server backup configured can cause snapshot task delay.** By default, VM backup creates a VSS full backup on Windows VMs. VMs that run SQL Server, with SQL Server backup configured, can experience snapshot delays. If snapshot delays cause backup failures, set following registry key:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\BCDRAGENT]
"USEVSSCOPYBACKUP"="TRUE"
```

- VM status is reported incorrectly because the VM is shut down in RDP.** If you used the remote desktop to shut down the virtual machine, verify that the VM status in the portal is correct. If the status isn't correct, use the **Shutdown** option in the portal VM dashboard to shut down the VM.
- If more than four VMs share the same cloud service, spread the VMs across multiple backup policies.** Stagger the backup times, so no more than four VM backups start at the same time. Try to separate the start times in the policies by at least an hour.
- The VM runs at high CPU or memory.** If the virtual machine runs at high memory or CPU usage, more than 90 percent, your snapshot task is queued and delayed. Eventually it times out. If this issue happens, try an on-demand backup.

## Networking

DHCP must be enabled inside the guest for IaaS VM backup to work. If you need a static private IP, configure it through the Azure portal or PowerShell. Make sure the DHCP option inside the VM is enabled. Get more information on how to set up a static IP through PowerShell:

- [How to add a static internal IP to an existing VM](#)
- [Change the allocation method for a private IP address assigned to a network interface](#)

# Troubleshoot Azure Backup failure: Issues with the agent or extension

2/27/2020 • 13 minutes to read • [Edit Online](#)

This article provides troubleshooting steps that can help you resolve Azure Backup errors related to communication with the VM agent and extension.

If your Azure issue is not addressed in this article, visit the Azure forums on [MSDN and Stack Overflow](#). You can post your issue in these forums, or post to [@AzureSupport on Twitter](#). You also can submit an Azure support request. To submit a support request, on the [Azure support](#) page, select **Get support**.

## UserErrorGuestAgentStatusUnavailable - VM agent unable to communicate with Azure Backup

**Error code:** UserErrorGuestAgentStatusUnavailable

**Error message:** VM Agent unable to communicate with Azure Backup

The Azure VM agent might be stopped, outdated, in an inconsistent state, or not installed. These states prevent the Azure Backup service from triggering snapshots.

- **Open Azure portal > VM > Settings > Properties pane** > ensure VM **Status** is **Running** and **Agent status** is **Ready**. If the VM agent is stopped or is in an inconsistent state, restart the agent
  - For Windows VMs, follow these [steps](#) to restart the Guest Agent.
  - For Linux VMs, follow these [steps](#) to restart the Guest Agent.
- **Open Azure portal > VM > Settings > Extensions** > Ensure all extensions are in **provisioning succeeded** state. If not, follow these [steps](#) to resolve the issue.

## GuestAgentSnapshotTaskStatusError - Could not communicate with the VM agent for snapshot status

**Error code:** GuestAgentSnapshotTaskStatusError

**Error message:** Could not communicate with the VM agent for snapshot status

After you register and schedule a VM for the Azure Backup service, Backup starts the job by communicating with the VM backup extension to take a point-in-time snapshot. Any of the following conditions might prevent the snapshot from being triggered. If the snapshot isn't triggered, a backup failure might occur. Complete the following troubleshooting steps in the order listed, and then retry your operation:

**Cause 1: The agent is installed in the VM, but it's unresponsive (for Windows VMs)**

**Cause 2: The agent installed in the VM is out of date (for Linux VMs)**

**Cause 3: The snapshot status can't be retrieved, or a snapshot can't be taken**

**Cause 4: The backup extension fails to update or load**

**Cause 5: VM-Agent configuration options are not set (for Linux VMs)**

## UserErrorVmProvisioningStateFailed - The VM is in failed provisioning state

**Error code:** UserErrorVmProvisioningStateFailed

**Error message:** The VM is in failed provisioning state

This error occurs when one of the extension failures puts the VM into provisioning failed state.

**Open Azure portal > VM > Settings > Extensions > Extensions status** and check if all extensions are in **provisioning succeeded** state.

- If VMSnapshot extension is in a failed state, then right-click on the failed extension and remove it. Trigger an on-demand backup. This action will reinstall the extensions, and run the backup job.
- If any other extension is in a failed state, then it can interfere with the backup. Ensure those extension issues are resolved and retry the backup operation.

## UserErrorRpCollectionLimitReached - The Restore Point collection max limit has reached

**Error code:** UserErrorRpCollectionLimitReached

**Error message:** The Restore Point collection max limit has reached.

- This issue could happen if there's a lock on the recovery point resource group preventing automatic cleanup of recovery points.
- This issue can also happen if multiple backups are triggered per day. Currently we recommend only one backup per day, as the instant restore points are retained for 1-5 days per the configured snapshot retention and only 18 instant RPs can be associated with a VM at any given time.
- The number of restore points across restore point collections and resource groups for a VM can't exceed 18. To create a new restore point, delete existing restore points.

Recommended Action:

To resolve this issue, remove the lock on the resource group of the VM, and retry the operation to trigger cleanup.

### NOTE

Backup service creates a separate resource group than the resource group of the VM to store restore point collection.

Customers are advised not to lock the resource group created for use by the Backup service. The naming format of the resource group created by Backup service is: AzureBackupRG\_<Geo>\_<number> Eg: AzureBackupRG\_northeurope\_1

### Step 1: Remove lock from the restore point resource group

### Step 2: Clean up restore point collection

## UserErrorKeyvaultPermissionsNotConfigured - Backup doesn't have sufficient permissions to the key vault for backup of encrypted VMs

**Error code:** UserErrorKeyvaultPermissionsNotConfigured

**Error message:** Backup doesn't have sufficient permissions to the key vault for backup of encrypted VMs.

For a backup operation to succeed on encrypted VMs, it must have permissions to access the key vault.

Permissions can be set through the [Azure portal](#) or through [PowerShell](#).

## ExtensionSnapshotFailedNoNetwork - Snapshot operation failed due to no network connectivity on the virtual machine

**Error code:** ExtensionSnapshotFailedNoNetwork

**Error message:** Snapshot operation failed due to no network connectivity on the virtual machine

After you register and schedule a VM for the Azure Backup service, Backup starts the job by communicating with the VM backup extension to take a point-in-time snapshot. Any of the following conditions might prevent the snapshot from being triggered. If the snapshot isn't triggered, a backup failure might occur. Complete the following troubleshooting steps in the order listed, and then retry your operation:

**Cause 1: The snapshot status can't be retrieved, or a snapshot can't be taken**

**Cause 2: The backup extension fails to update or load**

## ExtensionOperationFailedForManagedDisks - VMSnapshot extension operation failed

**Error code:** ExtensionOperationFailedForManagedDisks

**Error message:** VMSnapshot extension operation failed

After you register and schedule a VM for the Azure Backup service, Backup starts the job by communicating with the VM backup extension to take a point-in-time snapshot. Any of the following conditions might prevent the snapshot from being triggered. If the snapshot isn't triggered, a backup failure might occur. Complete the following troubleshooting steps in the order listed, and then retry your operation:

**Cause 1: The snapshot status can't be retrieved, or a snapshot can't be taken**

**Cause 2: The backup extension fails to update or load**

**Cause 3: The agent is installed in the VM, but it's unresponsive (for Windows VMs)**

**Cause 4: The agent installed in the VM is out of date (for Linux VMs)**

## BackUpOperationFailed / BackUpOperationFailedV2 - Backup fails, with an internal error

**Error code:** BackUpOperationFailed / BackUpOperationFailedV2

**Error message:** Backup failed with an internal error - Please retry the operation in a few minutes

After you register and schedule a VM for the Azure Backup service, Backup initiates the job by communicating with the VM backup extension to take a point-in-time snapshot. Any of the following conditions might prevent the snapshot from being triggered. If the snapshot isn't triggered, a backup failure might occur. Complete the following troubleshooting steps in the order listed, and then retry your operation:

**Cause 1: The agent installed in the VM, but it's unresponsive (for Windows VMs)**

**Cause 2: The agent installed in the VM is out of date (for Linux VMs)**

**Cause 3: The snapshot status can't be retrieved, or a snapshot can't be taken**

**Cause 4: The backup extension fails to update or load**

**Cause 5: Backup service doesn't have permission to delete the old restore points because of a resource group lock**

## UserErrorUnsupportedDiskSize - The configured disk size(s) is currently not supported by Azure Backup

**Error code:** UserErrorUnsupportedDiskSize

**Error message:** The configured disk size(s) is currently not supported by Azure Backup.

Your backup operation could fail when backing up a VM with a disk size greater than 32 TB. Also, backup of encrypted disks greater than 4 TB in size isn't currently supported. Ensure that the disk size(s) is less than or equal to the supported limit by splitting the disk(s).

## UserErrorBackupOperationInProgress - Unable to initiate backup as another backup operation is currently in progress

**Error code:** UserErrorBackupOperationInProgress

**Error message:** Unable to initiate backup as another backup operation is currently in progress

Your recent backup job failed because there's an existing backup job in progress. You can't start a new backup job until the current job finishes. Ensure the backup operation currently in progress is completed before triggering or scheduling another backup operations. To check the backup jobs status, do the following steps:

1. Sign in to the Azure portal, click **All services**. Type Recovery Services and click **Recovery Services vaults**.  
The list of recovery services vaults appears.
2. From the list of recovery services vaults, select a vault in which the backup is configured.
3. On the vault dashboard menu, click **Backup Jobs** it displays all the backup jobs.
  - If a backup job is in progress, wait for it to complete or cancel the backup job.
    - To cancel the backup job, right-click on the backup job and click **Cancel** or use **PowerShell**.
  - If you've reconfigured the backup in a different vault, then ensure there are no backup jobs running in the old vault. If it exists, then cancel the backup job.
    - To cancel the backup job, right-click on the backup job and click **Cancel** or use **PowerShell**
4. Retry backup operation.

If the scheduled backup operation is taking longer, conflicting with the next backup configuration, then review the [Best Practices](#), [Backup Performance](#), and [Restore consideration](#).

## UserErrorCrpReportedUserError - Backup failed due to an error. For details, see Job Error Message Details

**Error code:** UserErrorCrpReportedUserError

**Error message:** Backup failed due to an error. For details, see Job Error Message Details.

This error is reported from the IaaS VM. To identify the root cause of the issue, go to the Recovery Services vault settings. Under the **Monitoring** section, select **Backup jobs** to filter and view the status. Click on **Failures** to review the underlying error message details. Take further actions according to the recommendations in the error details page.

## Causes and solutions

### The agent is installed in the VM, but it's unresponsive (for Windows VMs)

#### Solution

The VM agent might have been corrupted, or the service might have been stopped. Reinstalling the VM agent helps get the latest version. It also helps restart communication with the service.

1. Determine whether the Windows Azure Guest Agent service is running in the VM services (services.msc). Try to restart the Windows Azure Guest Agent service and initiate the backup.
2. If the Windows Azure Guest Agent service isn't visible in services, in Control Panel, go to **Programs and Features** to determine whether the Windows Azure Guest Agent service is installed.
3. If the Windows Azure Guest Agent appears in **Programs and Features**, uninstall the Windows Azure Guest Agent.
4. Download and install the [latest version of the agent MSI](#). You must have Administrator rights to complete the installation.
5. Verify that the Windows Azure Guest Agent services appear in services.
6. Run an on-demand backup:
  - In the portal, select **Backup Now**.

Also, verify that [Microsoft .NET 4.5 is installed](#) in the VM..NET 4.5 is required for the VM agent to communicate with the service.

## The agent installed in the VM is out of date (for Linux VMs)

### Solution

Most agent-related or extension-related failures for Linux VMs are caused by issues that affect an outdated VM agent. To troubleshoot this issue, follow these general guidelines:

1. Follow the instructions for [updating the Linux VM agent](#).

#### NOTE

We strongly recommend that you update the agent only through a distribution repository. We do not recommend downloading the agent code directly from GitHub and updating it. If the latest agent for your distribution is not available, contact distribution support for instructions on how to install it. To check for the most recent agent, go to the [Windows Azure Linux agent](#) page in the GitHub repository.

2. Ensure that the Azure agent is running on the VM by running the following command: `ps -e`

If the process isn't running, restart it by using the following commands:

- For Ubuntu: `service walinuagent start`
- For other distributions: `service waagent start`

3. [Configure the auto restart agent](#).

4. Run a new test backup. If the failure persists, collect the following logs from the VM:

- `/var/lib/waagent/*.xml`
- `/var/log/waagent.log`
- `/var/log/azure/*`

If you require verbose logging for waagent, follow these steps:

1. In the `/etc/waagent.conf` file, locate the following line: **Enable verbose logging (y|n)**
2. Change the **Logs.Verbose** value from *n* to *y*.
3. Save the change, and then restart waagent by completing the steps described earlier in this section.

## VM-Agent configuration options are not set (for Linux VMs)

A configuration file (`/etc/waagent.conf`) controls the actions of waagent. Configuration File Options

**Extensions.Enable** and **Provisioning.Agent** should be set to **y** for Backup to work. For full list of VM-Agent Configuration File Options, see <https://github.com/Azure/WALinuxAgent#configuration-file-options>

## The snapshot status can't be retrieved, or a snapshot can't be taken

The VM backup relies on issuing a snapshot command to the underlying storage account. Backup can fail either because it has no access to the storage account, or because the execution of the snapshot task is delayed.

### Solution

The following conditions might cause the snapshot task to fail:

| CAUSE                                                                                               | SOLUTION                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The VM status is reported incorrectly because the VM is shut down in Remote Desktop Protocol (RDP). | If you shut down the VM in RDP, check the portal to determine whether the VM status is correct. If it's not correct, shut down the VM in the portal by using the <b>Shutdown</b> option on the VM dashboard. |

| CAUSE                                                  | SOLUTION                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The VM can't get the host or fabric address from DHCP. | DHCP must be enabled inside the guest for the IaaS VM backup to work. If the VM can't get the host or fabric address from DHCP response 245, it can't download or run any extensions. If you need a static private IP, you should configure it through the <a href="#">Azure portal</a> or <a href="#">PowerShell</a> and make sure the DHCP option inside the VM is enabled. <a href="#">Learn more</a> about setting up a static IP address with PowerShell. |

## The backup extension fails to update or load

If extensions can't load, backup fails because a snapshot can't be taken.

### Solution

Uninstall the extension to force the VMSnapshot extension to reload. The next backup attempt reloads the extension.

To uninstall the extension:

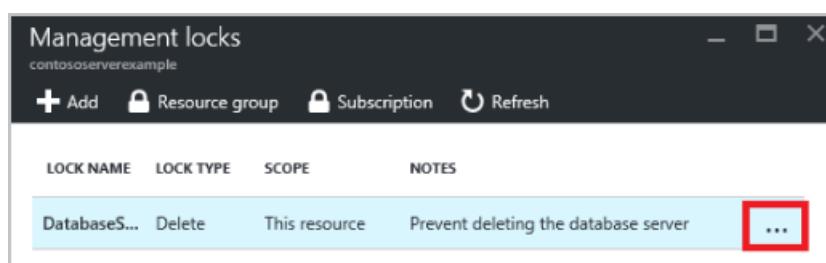
1. In the [Azure portal](#), go to the VM that is experiencing backup failure.
2. Select **Settings**.
3. Select **Extensions**.
4. Select **Snapshot Extension**.
5. Select **Uninstall**.

For Linux VM, If the VMSnapshot extension doesn't show in the Azure portal, [update the Azure Linux Agent](#), and then run the backup.

Completing these steps causes the extension to be reinstalled during the next backup.

## Remove lock from the recovery point resource group

1. Sign in to the [Azure portal](#).
2. Go to **All Resources option**, select the restore point collection resource group in the following format AzureBackupRG\_<Geo>\_<number>.
3. In the **Settings** section, select **Locks** to display the locks.
4. To remove the lock, select the ellipsis and click **Delete**.



## Clean up restore point collection

After removing the lock, the restore points have to be cleaned up.

If you delete the Resource Group of the VM, or the VM itself, the instant restore snapshots of managed disks remain active and expire according to the retention set. To delete the instant restore snapshots (if you don't need them anymore) that are stored in the Restore Point Collection, clean up the restore point collection according to the steps given below.

To clean up the restore points, follow any of the methods:

- Clean up restore point collection by running on-demand backup
- Clean up restore point collection from Azure portal

#### Clean up restore point collection by running on-demand backup

After removing the lock, trigger an on-demand backup. This action will ensure the restore points are automatically cleaned up. Expect this on-demand operation to fail the first time; however, it will ensure automatic cleanup instead of manual deletion of restore points. After cleanup, your next scheduled backup should succeed.

#### NOTE

Automatic cleanup will happen after few hours of triggering the on-demand backup. If your scheduled backup still fails, then try manually deleting the restore point collection using the steps listed [here](#).

#### Clean up restore point collection from Azure portal

To manually clear the restore points collection, which isn't cleared because of the lock on the resource group, try the following steps:

1. Sign in to the [Azure portal](#).
2. On the **Hub** menu, click **All resources**, select the Resource group with the following format AzureBackupRG\_<Geo>\_<number> where your VM is located.

3. Click Resource group, the **Overview** pane is displayed.
4. Select **Show hidden types** option to display all the hidden resources. Select the restore point collections with the following format AzureBackupRG\_<VMName>\_<number> .

| NAME                              | TYPE                          | LOCATION |
|-----------------------------------|-------------------------------|----------|
| AzureBackup_bh-vm2_35185017603181 | Microsoft.Compute/restoreP... | West US  |

5. Click **Delete** to clean the restore point collection.
6. Retry the backup operation again.

**NOTE**

If the resource (RP Collection) has a large number of Restore Points, then deleting them from the portal may timeout and fail. This is a known CRP issue, where all restore points are not deleted in the stipulated time and the operation times out; however the delete operation usually succeeds after 2 or 3 retries.

# Troubleshoot slow backup of files and folders in Azure Backup

2/25/2020 • 5 minutes to read • [Edit Online](#)

This article provides troubleshooting guidance to help you diagnose the cause of slow backup performance for files and folders when you're using Azure Backup. When you use the Azure Backup agent to back up files, the backup process might take longer than expected. This delay might be caused by one or more of the following:

- There are performance bottlenecks on the computer that's being backed up.
- Another process or antivirus software is interfering with the Azure Backup process.
- The Backup agent is running on an Azure virtual machine (VM).
- You're backing up a large number (millions) of files.

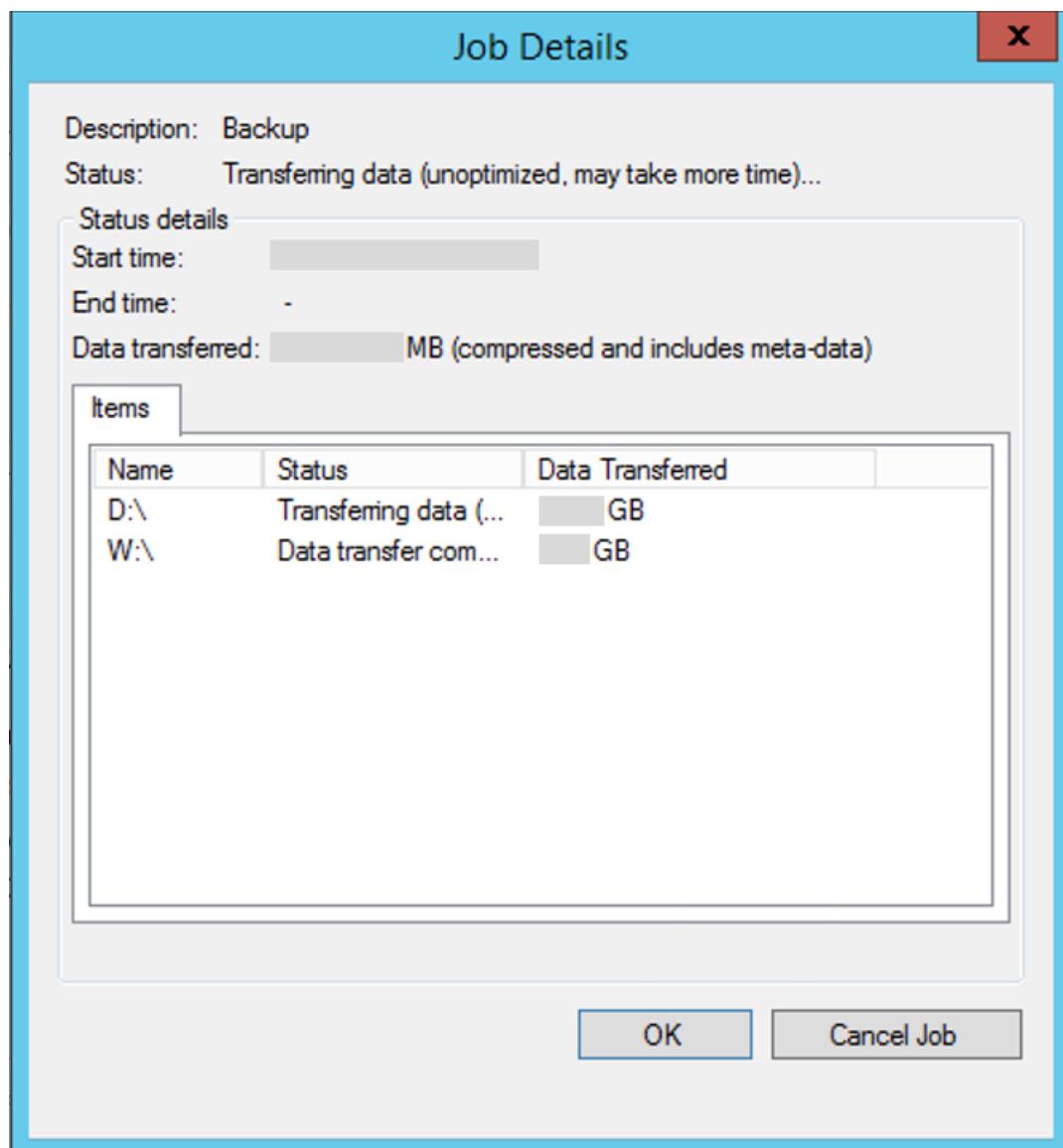
Before you start troubleshooting issues, we recommend that you download and install the [latest Azure Backup agent](#). We make frequent updates to the Backup agent to fix various issues, add features, and improve performance.

We also strongly recommend that you review the [Azure Backup service FAQ](#) to make sure you're not experiencing any of the common configuration issues.

If your Azure issue is not addressed in this article, visit the Azure forums on [MSDN and Stack Overflow](#). You can post your issue in these forums, or post to [@AzureSupport on Twitter](#). You also can submit an Azure support request. To submit a support request, on the [Azure support](#) page, select **Get support**.

## Cause: Backup job running in unoptimized mode

- The MARS agent can run the backup job in **optimized mode** using USN (update sequence number) change journal or **unoptimized mode** by checking for changes in directories or files by scanning the entire volume.
- Unoptimized mode is slow because the agent has to scan each and every file on the volume and compare against the metadata to determine the changed files.
- To verify this, open **Job Details** from the MARS agent console and check the status to see if it says **Transferring data (unoptimized, may take more time)** as shown below:



- The following conditions can cause the backup job to run in unoptimized mode:
  - First backup (also known as Initial Replication) will always run in unoptimized mode
  - If the previous backup job fails, then the next scheduled backup job will run as unoptimized.

## Cause: Performance bottlenecks on the computer

Bottlenecks on the computer that's being backed up can cause delays. For example, the computer's ability to read or write to disk, or available bandwidth to send data over the network, can cause bottlenecks.

Windows provides a built-in tool called [Performance Monitor](#) (Perfmon) to detect these bottlenecks.

Here are some performance counters and ranges that can be helpful in diagnosing bottlenecks for optimal backups.

| COUNTER                                                   | STATUS                                                                                                                                                                                        |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Logical Disk(Physical Disk)--%idle                        | <ul style="list-style-type: none"><li>• 100% idle to 50% idle = Healthy</li><li>• 49% idle to 20% idle = Warning or Monitor</li><li>• 19% idle to 0% idle = Critical or Out of Spec</li></ul> |
| Logical Disk(Physical Disk)--%Avg. Disk Sec Read or Write | <ul style="list-style-type: none"><li>• 0.001 ms to 0.015 ms = Healthy</li><li>• 0.015 ms to 0.025 ms = Warning or Monitor</li><li>• 0.026 ms or longer = Critical or Out of Spec</li></ul>   |

| COUNTER                                                                    | STATUS                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Logical Disk(Physical Disk)--Current Disk Queue Length (for all instances) | 80 requests for more than 6 minutes                                                                                                                                                                                                                                                         |
| Memory--Pool Non Paged Bytes                                               | <ul style="list-style-type: none"> <li>• Less than 60% of pool consumed = Healthy</li> <li>• 61% to 80% of pool consumed = Warning or Monitor</li> <li>• Greater than 80% pool consumed = Critical or Out of Spec</li> </ul>                                                                |
| Memory--Pool Paged Bytes                                                   | <ul style="list-style-type: none"> <li>• Less than 60% of pool consumed = Healthy</li> <li>• 61% to 80% of pool consumed = Warning or Monitor</li> <li>• Greater than 80% pool consumed = Critical or Out of Spec</li> </ul>                                                                |
| Memory--Available Megabytes                                                | <ul style="list-style-type: none"> <li>• 50% of free memory available or more = Healthy</li> <li>• 25% of free memory available = Monitor</li> <li>• 10% of free memory available = Warning</li> <li>• Less than 100 MB or 5% of free memory available = Critical or Out of Spec</li> </ul> |
| Processor--%Processor Time (all instances)                                 | <ul style="list-style-type: none"> <li>• Less than 60% consumed = Healthy</li> <li>• 61% to 90% consumed = Monitor or Caution</li> <li>• 91% to 100% consumed = Critical</li> </ul>                                                                                                         |

#### NOTE

If you determine that the infrastructure is the culprit, we recommend that you defragment the disks regularly for better performance.

## Cause: Another process or antivirus software interfering with Azure Backup

We've seen several instances where other processes in the Windows system have negatively affected performance of the Azure Backup agent process. For example, if you use both the Azure Backup agent and another program to back up data, or if antivirus software is running and has a lock on files to be backed up, the multiple locks on files might cause contention. In this situation, the backup might fail, or the job might take longer than expected.

The best recommendation in this scenario is to turn off the other backup program to see whether the backup time for the Azure Backup agent changes. Usually, making sure that multiple backup jobs are not running at the same time is sufficient to prevent them from affecting each other.

For antivirus programs, we recommend that you exclude the following files and locations:

- C:\Program Files\Microsoft Azure Recovery Services Agent\bin\cbengine.exe as a process
- C:\Program Files\Microsoft Azure Recovery Services Agent\ folders
- Scratch location (if you're not using the standard location)

## Cause: Backup agent running on an Azure virtual machine

If you're running the Backup agent on a VM, performance will be slower than when you run it on a physical machine. This is expected due to IOPS limitations. However, you can optimize the performance by switching the data drives that are being backed up to Azure Premium Storage. We're working on fixing this issue, and the fix will be available in a future release.

## Cause: Backing up a large number (millions) of files

Moving a large volume of data will take longer than moving a smaller volume of data. In some cases, backup time is related to not only the size of the data, but also the number of files or folders. This is especially true when millions of small files (a few bytes to a few kilobytes) are being backed up.

This behavior occurs because while you're backing up the data and moving it to Azure, Azure is simultaneously cataloging your files. In some rare scenarios, the catalog operation might take longer than expected.

The following indicators can help you understand the bottleneck and accordingly work on the next steps:

- **UI is showing progress for the data transfer.** The data is still being transferred. The network bandwidth or the size of data might be causing delays.
- **UI is not showing progress for the data transfer.** Open the logs located at C:\Program Files\Microsoft Azure Recovery Services Agent\Temp, and then check for the FileProvider::EndData entry in the logs. This entry signifies that the data transfer finished and the catalog operation is happening. Don't cancel the backup jobs. Instead, wait a little longer for the catalog operation to finish. If the problem persists, contact [Azure support](#).

# Troubleshoot Azure Backup Server

2/25/2020 • 12 minutes to read • [Edit Online](#)

Use the information in the following tables to troubleshoot errors that you encounter while using Azure Backup Server.

## Basic troubleshooting

We recommend you perform the below validation, before you start troubleshooting Microsoft Azure Backup Server (MABS):

- [Ensure Microsoft Azure Recovery Services \(MARS\) Agent is up to date](#)
- [Ensure there is network connectivity between MARS agent and Azure](#)
- Ensure Microsoft Azure Recovery Services is running (in Service console). If necessary, restart and retry the operation
- [Ensure 5-10% free volume space is available on scratch folder location](#)
- If registration is failing, then ensure the server on which you are trying to install Azure Backup Server is not already registered with another vault
- If Push install fails, check if DPM agent is already present. If yes, then uninstall the agent and retry the installation
- [Ensure no other process or antivirus software is interfering with Azure Backup](#)
- Ensure that the SQL Agent service is running and set to automatic in MAB server

## Invalid vault credentials provided

| OPERATION | ERROR DETAILS | WORKAROUND |
|-----------|---------------|------------|
|-----------|---------------|------------|

| OPERATION              | ERROR DETAILS                                                                                                                           | WORKAROUND                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Registering to a vault | Invalid vault credentials provided. The file is corrupted or does not have the latest credentials associated with the recovery service. | <p>Recommended action:</p> <ul style="list-style-type: none"> <li>Download the latest credentials file from the vault and try again. (OR)</li> <li>If the previous action didn't work, try downloading the credentials to a different local directory or create a new vault. (OR)</li> <li>Try updating the date and time settings as described in <a href="#">this article</a>. (OR)</li> <li>Check to see if c:\windows\temp has more than 65000 files. Move stale files to another location or delete the items in the Temp folder. (OR)</li> <li>Check the status of certificates.             <ol style="list-style-type: none"> <li>Open <b>Manage Computer Certificates</b> (in Control Panel).</li> <li>Expand the <b>Personal</b> node and its child node <b>Certificates</b>.</li> <li>Remove the certificate <b>Windows Azure Tools</b>.</li> <li>Retry the registration in the Azure Backup client. (OR)</li> </ol> </li> <li>Check to see if any group policy is in place.</li> </ul> |

## Replica is inconsistent

| OPERATION | ERROR DETAILS | WORKAROUND |
|-----------|---------------|------------|
|-----------|---------------|------------|

| OPERATION | ERROR DETAILS           | WORKAROUND                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Backup    | Replica is inconsistent | <p>Verify that the automatic consistency check option in the Protection Group Wizard is turned on. For more information about the causes of replica inconsistency and relevant suggestions, see the article <a href="#">Replica is inconsistent</a>.</p> <ol style="list-style-type: none"> <li>1. In case of System State/BMR backup, verify that Windows Server Backup is installed on the protected server.</li> <li>2. Check for space-related issues in the DPM storage pool on the DPM/Microsoft Azure Backup Server, and allocate storage as required.</li> <li>3. Check the state of the Volume Shadow Copy Service on the protected server. If it is in a disabled state, set it to start manually. Start the service on the server. Then go back to the DPM/Microsoft Azure Backup Server console, and start the sync with the consistency check job.</li> </ol> |

## Online recovery point creation failed

| OPERATION | ERROR DETAILS | WORKAROUND |
|-----------|---------------|------------|
|-----------|---------------|------------|

| OPERATION | ERROR DETAILS                         | WORKAROUND                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Backup    | Online recovery point creation failed | <p><b>Error Message:</b> Windows Azure Backup Agent was unable to create a snapshot of the selected volume.</p> <p><b>Workaround:</b> Try increasing the space in replica and recovery point volume.</p> <p><b>Error Message:</b> The Windows Azure Backup Agent cannot connect to the OBEngine service</p> <p><b>Workaround:</b> verify that the OBEngine exists in the list of running services on the computer. If the OBEngine service is not running, use the "net start OBEngine" command to start the OBEngine service.</p> <p><b>Error Message:</b> The encryption passphrase for this server is not set. Please configure an encryption passphrase.</p> <p><b>Workaround:</b> Try configuring an encryption passphrase. If it fails, take the following steps:</p> <ol style="list-style-type: none"> <li>1. Verify that the scratch location exists. This is the location that's mentioned in the registry <b>HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Azure Backup\Config</b>, with the name <b>ScratchLocation</b> should exist.</li> <li>2. If the scratch location exists, try re-registering by using the old passphrase. <i>Whenever you configure an encryption passphrase, save it in a secure location.</i></li> </ol> |

The original and external DPM servers must be registered to the same vault

| OPERATION | ERROR DETAILS                                                                                                                                                                                                  | WORKAROUND                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Restore   | <p><b>Error code:</b> CBPServerRegisteredVaultDontMatchWithCurrent/Vault Credentials Error: 100110</p> <p><b>Error message:</b> The original and external DPM servers must be registered to the same vault</p> | <p><b>Cause:</b> This issue occurs when you are trying to restore files to the alternate server from the original server using External DPM recovery option and if the server that is being recovered and the original server from where the data is backed-up are not associated with the same Recovery Service vault.</p> <p><b>Workaround</b> To resolve this issue ensure both the original and alternate server is registered to the same vault.</p> |

Online recovery point creation jobs for VMware VM fail

| OPERATION | ERROR DETAILS                                                                                                                                                                      | WORKAROUND                                                                                                                                                                                                                                                                                                      |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Backup    | Online recovery point creation jobs for VMware VM fail. DPM encountered an error from VMware while trying to get ChangeTracking information. ErrorCode - FileFaultFault (ID 33621) | <ol style="list-style-type: none"> <li>1. Reset the CTK on VMware for the affected VMs.</li> <li>2. Check that independent disk is not in place on VMware.</li> <li>3. Stop protection for the affected VMs and reprotect with the <b>Refresh</b> button.</li> <li>4. Run a CC for the affected VMs.</li> </ol> |

The agent operation failed because of a communication error with the DPM agent coordinator service on the server

| OPERATION                             | ERROR DETAILS                                                                                                       | WORKAROUND                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pushing agent(s) to protected servers | The agent operation failed because of a communication error with the DPM Agent Coordinator service on <ServerName>. | <p><b>If the recommended action shown in the product doesn't work, then perform the following steps:</b></p> <ul style="list-style-type: none"> <li>• If you are attaching a computer from an untrusted domain, follow <a href="#">these steps</a>. (OR)</li> <li>• If you are attaching a computer from a trusted domain, troubleshoot using the steps outlined in <a href="#">this blog</a>. (OR)</li> <li>• Try disabling antivirus as a troubleshooting step. If it resolves the issue, modify the antivirus settings as suggested in <a href="#">this article</a>.</li> </ul> |

Setup could not update registry metadata

| OPERATION    | ERROR DETAILS                                                                                                                                                                   | WORKAROUND                                                                                                                                       |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Installation | Setup could not update registry metadata. This update failure could lead to overusage of storage consumption. To avoid this update the ReFS Trimming registry entry.            | Adjust the registry key <b>SYSTEM\CurrentControlSet\Control\FileSystem\RefsEnableInlineTrim</b> . Set the value Dword to 1.                      |
| Installation | Setup could not update registry metadata. This update failure could lead to overusage of storage consumption. To avoid this, update the Volume SnapOptimization registry entry. | Create the registry key <b>SOFTWARE\Microsoft Data Protection Manager\Configuration\VolSnapOptimization\Writelds</b> with an empty string value. |

Registration and agent-related issues

| OPERATION                                                                         | ERROR DETAILS                                                                                                                                                                          | WORKAROUND                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pushing agent(s) to protected servers                                             | The credentials that are specified for the server are invalid.                                                                                                                         | <p><b>If the recommended action that's shown in the product doesn't work, take the following steps:</b></p> <p>Try to install the protection agent manually on the production server as specified in <a href="#">this article</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Azure Backup Agent was unable to connect to the Azure Backup service (ID: 100050) | The Azure Backup Agent was unable to connect to the Azure Backup service.                                                                                                              | <p><b>If the recommended action that's shown in the product doesn't work, take the following steps:</b></p> <ol style="list-style-type: none"> <li>Run the following command from an elevated prompt: <b>psexec -i -s "c:\Program Files\Internet Explorer\iexplore.exe</b>. This opens the Internet Explorer window.</li> <li>Go to <b>Tools &gt; Internet Options &gt; Connections &gt; LAN settings</b>.</li> <li>Change the settings to use a proxy server. Then provide the proxy server details.</li> <li>If your machine has limited internet access, ensure that firewall settings on the machine or proxy allow these <a href="#">URLs</a> and <a href="#">IP address</a>.</li> </ol> |
| Azure Backup Agent installation failed                                            | The Microsoft Azure Recovery Services installation failed. All changes that were made to the system by the Microsoft Azure Recovery Services installation were rolled back. (ID: 4024) | Manually install Azure Agent.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## Configuring protection group

| OPERATION                     | ERROR DETAILS                                                                                          | WORKAROUND                                                                                                                                                                                                                |
|-------------------------------|--------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configuring protection groups | DPM could not enumerate the application component on the protected computer (protected computer name). | Select <b>Refresh</b> on the configure protection group UI screen at the relevant datasource/component level.                                                                                                             |
| Configuring protection groups | Unable to configure protection                                                                         | If the protected server is a SQL server, verify that the sysadmin role permissions have been provided to the system account (NTAuthority\System) on the protected computer as described in <a href="#">this article</a> . |
| Configuring protection groups | There is insufficient free space in the storage pool for this protection group.                        | The disks that are added to the storage pool <a href="#">should not contain a partition</a> . Delete any existing volumes on the disks. Then add them to the storage pool.                                                |

| OPERATION     | ERROR DETAILS                                                                                                                                                                                                                            | WORKAROUND                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Policy change | <p>The backup policy could not be modified. Error: The current operation failed due to an internal service error [0x29834]. Please retry the operation after some time has passed. If the issue persists, contact Microsoft support.</p> | <p><b>Cause:</b><br/>This error occurs under three conditions: when security settings are enabled, when you try to reduce retention range below the minimum values specified previously, and when you are on an unsupported version. (Unsupported versions are those below Microsoft Azure Backup Server version 2.0.9052 and Azure Backup Server update 1.)</p> <p><b>Recommended action:</b><br/>To proceed with policy-related updates, set the retention period above the minimum retention period specified. (The minimum retention period is seven days for daily, four weeks for weekly, three weeks for monthly or one year for yearly.)</p> <p>Optionally, another preferred approach is to update the backup agent and Azure Backup Server to leverage all the security updates.</p> |

## Backup

| OPERATION | ERROR DETAILS                                                                           | WORKAROUND                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Backup    | <p>An unexpected error occurred while the job was running. The device is not ready.</p> | <p><b>If the recommended action that's shown in the product doesn't work, take the following steps:</b></p> <ul style="list-style-type: none"> <li>• Set the Shadow Copy Storage space to unlimited on the items in the protection group, and then run the consistency check.</li> </ul> <p>(OR)</p> <ul style="list-style-type: none"> <li>• Try deleting the existing protection group and creating multiple new groups. Each new protection group should have an individual item in it.</li> </ul> |

| OPERATION | ERROR DETAILS                                                                                                                               | WORKAROUND                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Backup    | If you are backing up only system state, verify that there is enough free space on the protected computer to store the system state backup. | <ol style="list-style-type: none"> <li>Verify that Windows Server Backup is installed on the protected machine.</li> <li>Verify that there is enough space on the protected computer for the system state. The easiest way to verify this is to go to the protected computer, open Windows Server Backup, click through the selections, and then select BMR. The UI then tells you how much space is required. Open <b>WSB &gt; Local backup &gt; Backup schedule &gt; Select Backup Configuration &gt; Full server</b> (size is displayed). Use this size for verification.</li> </ol> |
| Backup    | Back up failure for BMR                                                                                                                     | If the BMR size is large, move some application files to the OS drive and retry.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Backup    | The option to reprotect a VMware VM on a new Microsoft Azure Backup Server does not show as available to add.                               | <p>VMware properties are pointed at an old, retired instance of Microsoft Azure Backup Server. To resolve this issue:</p> <ol style="list-style-type: none"> <li>In VCenter (SC-VMM equivalent), go to the <b>Summary</b> tab, and then to <b>Custom Attributes</b>.</li> <li>Delete the old Microsoft Azure Backup Server name from the <b>DPMServer</b> value.</li> <li>Go back to the new Microsoft Azure Backup Server and modify the PG. After you select the <b>Refresh</b> button, the VM appears with a check box as available to add to protection.</li> </ol>                 |
| Backup    | Error while accessing files/shared folders                                                                                                  | Try modifying the antivirus settings as suggested in this article <a href="#">Run antivirus software on the DPM server</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## Change passphrase

| OPERATION | ERROR DETAILS | WORKAROUND |
|-----------|---------------|------------|
|-----------|---------------|------------|

| OPERATION         | ERROR DETAILS                                                                                                | WORKAROUND                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------|--------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Change passphrase | The security PIN that was entered is incorrect. Provide the correct security PIN to complete this operation. | <p><b>Cause:</b><br/>This error occurs when you enter an invalid or expired security PIN while you are performing a critical operation (such as changing a passphrase).</p> <p><b>Recommended action:</b><br/>To complete the operation, you must enter a valid security PIN. To get the PIN, sign in to the Azure portal and go to the Recovery Services vault. Then go to <b>Settings &gt; Properties &gt; Generate Security PIN</b>. Use this PIN to change the passphrase.</p>                                                                                                                                               |
| Change passphrase | Operation failed. ID: 120002                                                                                 | <p><b>Cause:</b><br/>This error occurs when security settings are enabled, or when you try to change the passphrase when you're using an unsupported version.</p> <p><b>Recommended action:</b><br/>To change the passphrase, you must first update the backup agent to the minimum version, which is 2.0.9052. You also need to update Azure Backup Server to the minimum of update 1, and then enter a valid security PIN. To get the PIN, sign into the Azure portal and go to the Recovery Services vault. Then go to <b>Settings &gt; Properties &gt; Generate Security PIN</b>. Use this PIN to change the passphrase.</p> |

## Configure email notifications

| OPERATION | ERROR DETAILS | WORKAROUND |
|-----------|---------------|------------|
|-----------|---------------|------------|

| OPERATION                                                  | ERROR DETAILS  | WORKAROUND                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Setting up email notifications using an Office 365 account | Error ID: 2013 | <p><b>Cause:</b><br/>Trying to use Office 365 account</p> <p><b>Recommended action:</b></p> <ol style="list-style-type: none"> <li>1. The first thing to ensure is that "Allow Anonymous Relay on a Receive Connector" for your DPM server is set up on Exchange. For more information about how to configure this, see <a href="#">Allow Anonymous Relay on a Receive Connector</a>.</li> <li>2. If you can't use an internal SMTP relay and need to set up by using your Office 365 server, you can set up IIS to be a relay. Configure the DPM server to <a href="#">relay the SMTP to O365 using IIS</a>.</li> </ol> <p>Be sure to use the user@domain.com format and <i>not</i> domain\user.</p> <ol style="list-style-type: none"> <li>3. Point DPM to use the local server name as SMTP server, port 587. Then point it to the user email that the emails should come from.</li> <li>4. The username and password on the DPM SMTP setup page should be for a domain account in the domain that DPM is on.</li> </ol> <p>When you are changing the SMTP server address, make the change to the new settings, close the settings box, and then reopen it to be sure it reflects the new value. Simply changing and testing might not always cause the new settings to take effect, so testing it this way is a best practice.</p> <p>At any time during this process, you can clear these settings by closing the DPM console and editing the following registry keys: <b>HKLM\SOFTWARE\Microsoft\Microsoft Data Protection Manager\Notification\Delete SMTPPassword and SMTPUserName keys</b>. You can add them back to the UI when you launch it again.</p> |

## Common issues

This section covers the common errors that you might encounter while using Azure Backup Server.

### CBPSourceSnapshotFailedReplicaMissingOrInvalid

| ERROR MESSAGE                                                               | RECOMMENDED ACTION                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Backup failed because the disk-backup replica is either invalid or missing. | <p>To resolve this issue, verify the below steps and retry the operation:</p> <ol style="list-style-type: none"> <li>1. Create a disk recovery point</li> <li>2. Run consistency check on datasource</li> <li>3. Stop protection of datasource and then reconfigure protection for this data source</li> </ol> |

#### **CBPSourceSnapshotFailedReplicaMetadataInvalid**

| ERROR MESSAGE                                                         | RECOMMENDED ACTION                                                            |
|-----------------------------------------------------------------------|-------------------------------------------------------------------------------|
| Source volume snapshot failed because metadata on replica is invalid. | Create a disk recovery point of this datasource and retry online backup again |

#### **CBPSourceSnapshotFailedReplicaInconsistent**

| ERROR MESSAGE                                                         | RECOMMENDED ACTION                                       |
|-----------------------------------------------------------------------|----------------------------------------------------------|
| Source volume snapshot failed due to inconsistent datasource replica. | Run a consistency check on this datasource and try again |

#### **CBPSourceSnapshotFailedReplicaCloningIssue**

| ERROR MESSAGE                                                 | RECOMMENDED ACTION                                                                                                                       |
|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Backup failed as the disk-backup replica could not be cloned. | Ensure that all previous disk-backup replica files (.vhdx) are unmounted and no disk to disk backup is in progress during online backups |

# Troubleshoot System Center Data Protection Manager

1/5/2020 • 3 minutes to read • [Edit Online](#)

This article describes solutions for issues that you might encounter while using Data Protection Manager.

For the latest release notes for System Center Data Protection Manager, see the [System Center documentation](#). You can learn more about support for Data Protection Manager in [this matrix](#).

## Error: Replica is inconsistent

A replica can be inconsistent for the following reasons:

- The replica creation job fails.
- There are issues with the change journal.
- The volume level filter bitmap contains errors.
- The source machine shuts down unexpectedly.
- The synchronization log overflows.
- The replica is truly inconsistent.

To resolve this issue, perform the following actions:

- To remove the inconsistent status, run the consistency check manually, or schedule a daily consistency check.
- Ensure that you're using the latest version of Microsoft Azure Backup Server and Data Protection Manager.
- Ensure that the **Automatic Consistency** setting is enabled.
- Try to restart the services from the command prompt. Use the `net stop dpmra` command followed by `net start dpmra`.
- Ensure that you're meeting the network connectivity and bandwidth requirements.
- Check if the source machine was shut down unexpectedly.
- Ensure that the disk is healthy and that there's enough space for the replica.
- Ensure that there are no duplicate backup jobs that are running concurrently.

## Error: Online recovery point creation failed

To resolve this issue, perform the following actions:

- Ensure that you're using the latest version of the Azure Backup agent.
- Try to manually create a recovery point in the protection task area.
- Ensure that you run a consistency check on the data source.
- Ensure that you're meeting the network connectivity and bandwidth requirements.
- When the replica data is in an inconsistent state, create a disk recovery point of this data source.
- Ensure that the replica is present and not missing.
- Ensure that the replica has sufficient space to create the update sequence number (USN) journal.

## Error: Unable to configure protection

This error occurs when the Data Protection Manager server can't contact the protected server.

To resolve this issue, perform the following actions:

- Ensure that you're using the latest version of the Azure Backup agent.
- Ensure that there's connectivity (network/firewall/proxy) between your Data Protection Manager server and the protected server.
- If you're protecting a SQL server, ensure that the **Login Properties > NT AUTHORITY\SYSTEM** property shows the **sysadmin** setting enabled.

## Error: Server not registered as specified in vault credential file

This error occurs during the recovery process for Data Protection Manager/Azure Backup server data. The vault credential file that's used in the recovery process doesn't belong to the Recovery Services vault for the Data Protection Manager/Azure Backup server.

To resolve this issue, perform these steps:

1. Download the vault credential file from the Recovery Services vault to which the Data Protection Manager/Azure Backup server is registered.
2. Try to register the server with the vault by using the most recently downloaded vault credential file.

## Error: No recoverable data or selected server not a Data Protection Manager server

This error occurs for the following reasons:

- No other Data Protection Manager/Azure Backup servers are registered to the Recovery Services vault.
- The servers haven't yet uploaded the metadata.
- The selected server isn't a Data Protection Manager/Azure Backup server.

When other Data Protection Manager/Azure Backup servers are registered to the Recovery Services vault, perform these steps to resolve the issue:

1. Ensure that the latest Azure Backup agent is installed.
2. After you ensure that the latest agent is installed, wait one day before you start the recovery process. The nightly backup job uploads the metadata for all of the protected backups to the cloud. The backup data is then available for recovery.

## Error: Provided encryption passphrase doesn't match passphrase for server

This error occurs during the encryption process when recovering Data Protection Manager/Azure Backup server data. The encryption passphrase that's used in the recovery process doesn't match the server's encryption passphrase. As a result, the agent can't decrypt the data and the recovery fails.

### IMPORTANT

If you forget or lose the encryption passphrase, there are no other methods for recovering the data. The only option is to regenerate the passphrase. Use the new passphrase to encrypt future backup data.

When you're recovering data, always provide the same encryption passphrase that's associated with the Data Protection Manager/Azure Backup server.

# Troubleshoot the Microsoft Azure Recovery Services (MARS) agent

2/24/2020 • 12 minutes to read • [Edit Online](#)

This article describes how to resolve errors you might see during configuration, registration, backup, and restore.

## Basic troubleshooting

We recommend that you check the following before you start troubleshooting Microsoft the Azure Recovery Services (MARS) agent:

- [Ensure the MARS agent is up to date.](#)
- [Ensure you have network connectivity between the MARS agent and Azure.](#)
- Ensure MARS is running (in Service console). If you need to, restart and retry the operation.
- [Ensure 5% to 10% free volume space is available in the scratch folder location.](#)
- [Check if another process or antivirus software is interfering with Azure Backup.](#)
- If scheduled backup fails but manual backup works, see [Backups don't run according to schedule](#).
- Ensure your OS has the latest updates.
- [Ensure unsupported drives and files with unsupported attributes are excluded from backup.](#)
- Ensure the clock on the protected system is configured to the correct time zone.
- [Ensure .NET Framework 4.5.2 or later is installed on the server.](#)
- If you're trying to reregister your server to a vault:
  - Ensure the agent is uninstalled on the server and that it's deleted from the portal.
  - Use the same passphrase that was initially used to register the server.
- For offline backups, ensure Azure PowerShell 3.7.0 is installed on both the source and the copy computer before you start the backup.
- If the Backup agent is running on an Azure virtual machine, see [this article](#).

## Invalid vault credentials provided

**Error message:** Invalid vault credentials provided. The file is either corrupted or does not have the latest credentials associated with recovery service. (ID: 34513)

| CAUSE                                                                                                                                                                                                          | RECOMMENDED ACTIONS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Vault credentials aren't valid</b><br><br>Vault credential files might be corrupt or might have expired. (For example, they might have been downloaded more than 48 hours before the time of registration.) | Download new credentials from Recovery Services vault on the Azure portal. (See step 6 in the <a href="#">Download the MARS agent</a> section.) Then take these steps, as appropriate: <ul style="list-style-type: none"><li>• If you've already installed and registered MARS, open the Microsoft Azure Backup Agent MMC console and then select <b>Register Server</b> in the <b>Actions</b> pane to complete the registration with the new credentials.</li><li>• If the new installation fails, try reinstalling with the new credentials.</li></ul> <p><b>Note:</b> If multiple vault credential files have been downloaded, only the latest file is valid for the next 48 hours. We recommend that you download a new vault credential file.</p> |

| CAUSE                                                                                                                                                                                                                                                            | RECOMMENDED ACTIONS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Proxy server/firewall is blocking registration</b><br/>or<br/><b>No internet connectivity</b></p> <p>If your machine or proxy server has limited internet connectivity and you don't ensure access for the necessary URLs, the registration will fail.</p> | <p>Take these steps:</p> <ul style="list-style-type: none"> <li>Work with your IT team to ensure the system has internet connectivity.</li> <li>If you don't have a proxy server, ensure the proxy option isn't selected when you register the agent. <a href="#">Check your proxy settings</a>.</li> <li>If you do have a firewall/proxy server, work with your networking team to ensure these URLs and IP addresses have access:</li> </ul> <p><b>URLs</b></p> <div style="border: 1px solid black; padding: 2px; display: inline-block;"> <a href="http://www.msftncsi.com">www.msftncsi.com</a> </div> <ul style="list-style-type: none"> <li>.Microsoft.com</li> <li>.WindowsAzure.com</li> <li>.microsoftonline.com</li> <li>.windows.net</li> </ul> <p><b>IP addresses</b></p> <ul style="list-style-type: none"> <li>20.190.128.0/18</li> <li>40.126.0.0/18</li> </ul> <p>Try registering again after you complete the preceding troubleshooting steps.<br/>If you're connection is via Azure ExpressRoute, make sure the settings are configured as described in <a href="#">Azure ExpressRoute support</a>.</p> |
| <p><b>Antivirus software is blocking registration</b></p>                                                                                                                                                                                                        | <p>If you have antivirus software installed on the server, add necessary exclusion rules to the antivirus scan for these files and folders:</p> <ul style="list-style-type: none"> <li>CBengine.exe</li> <li>CSC.exe</li> <li>The scratch folder. Its default location is C:\Program Files\Microsoft Azure Recovery Services Agent\Scratch.</li> <li>The bin folder at C:\Program Files\Microsoft Azure Recovery Services Agent\Bin.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## Additional recommendations

- Go to C:/Windows/Temp and check whether there are more than 60,000 or 65,000 files with the .tmp extension. If there are, delete these files.
- Ensure the machine's date and time match the local time zone.
- Ensure [these sites](#) are added to your trusted sites in Internet Explorer.

## Verifying proxy settings for Windows

- Download PsExec from the [Sysinternals](#) page.
- Run `psexec -i -s "c:\Program Files\Internet Explorer\iexplore.exe"` from an elevated command prompt.

This command will open Internet Explorer.

- Go to **Tools > Internet options > Connections > LAN settings**.
- Check the proxy settings for the system account.
- If no proxy is configured and proxy details are provided, remove the details.
- If a proxy is configured and the proxy details are incorrect, ensure the **Proxy IP** and **Port** details are correct.
- Close Internet Explorer.

## Unable to download vault credential file

| ERROR                                                   | RECOMMENDED ACTIONS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Failed to download the vault credential file. (ID: 403) | <ul style="list-style-type: none"><li>Try downloading the vault credentials by using a different browser, or take these steps:<ul style="list-style-type: none"><li>Start Internet Explorer. Select F12.</li><li>Go to the <b>Network</b> tab and clear the cache and cookies.</li><li>Refresh the page.</li></ul></li><li>Check if the subscription is disabled/expired.</li><li>Check if any firewall rule is blocking the download.</li><li>Ensure you haven't exhausted the limit on the vault (50 machines per vault).</li><li>Ensure the user has the Azure Backup permissions that are required to download vault credentials and register a server with the vault. See <a href="#">Use Role-Based Access Control to manage Azure Backup recovery points</a>.</li></ul> |

The Microsoft Azure Recovery Service Agent was unable to connect to Microsoft Azure Backup

| ERROR | POSSIBLE CAUSE | RECOMMENDED ACTIONS |
|-------|----------------|---------------------|
|       |                |                     |

| ERROR                                                                                                                                                                                                                                                                                         | POSSIBLE CAUSE                      | RECOMMENDED ACTIONS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>The Microsoft Azure Recovery Service Agent was unable to connect to Microsoft Azure Backup. (ID: 100050) Check your network settings and ensure that you are able to connect to the internet.</li> <li>(407) Proxy Authentication Required.</li> </ul> | A proxy is blocking the connection. | <ul style="list-style-type: none"> <li>In Internet Explorer, go to <b>Tools</b> &gt; <b>Internet options</b> &gt; <b>Security</b> &gt; <b>Internet</b>. Select <b>Custom Level</b> and scroll down to the <b>File download</b> section. Select <b>Enable</b>. You might also have to add <a href="#">URLs and IP addresses</a> to your trusted sites in Internet Explorer.</li> <li>Change the settings to use a proxy server. Then provide the proxy server details.</li> <li>If your machine has limited internet access, ensure that firewall settings on the machine or proxy allow these <a href="#">URLs and IP addresses</a>.</li> <li>If you have antivirus software installed on the server, exclude these files from the antivirus scan: <ul style="list-style-type: none"> <li>CBEngine.exe (instead of dpmra.exe).</li> <li>CSC.exe (related to .NET Framework). There's a CSC.exe for every .NET Framework version installed on the server. Exclude CSC.exe files for all versions of .NET Framework on the affected server.</li> <li>The scratch folder or cache location. The default location for the scratch folder or the cache path is C:\Program Files\Microsoft Azure Recovery Services Agent\Scratch.</li> <li>The bin folder at C:\Program Files\Microsoft Azure Recovery Services Agent\Bin.</li> </ul> </li> </ul> |

## Failed to set the encryption key for secure backups

| ERROR                                                                                                                                                     | POSSIBLE CAUSES                                                                                                                                                     | RECOMMENDED ACTIONS                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Failed to set the encryption key for secure backups. Activation did not succeed completely but the encryption passphrase was saved to the following file. | <ul style="list-style-type: none"> <li>The server is already registered with another vault.</li> <li>During configuration, the passphrase was corrupted.</li> </ul> | Unregister the server from the vault and register it again with a new passphrase. |

## The activation did not complete successfully

| ERROR                                                                                                                                                                                                                | POSSIBLE CAUSES                                                                                                                                                                                                                | RECOMMENDED ACTIONS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The activation did not complete successfully. The current operation failed due to an internal service error [0x1FC07]. Retry the operation after some time. If the issue persists, please contact Microsoft support. | <ul style="list-style-type: none"><li>The scratch folder is located on a volume that doesn't have enough space.</li><li>The scratch folder has been incorrectly moved.</li><li>The OnlineBackup.KEK file is missing.</li></ul> | <ul style="list-style-type: none"><li>Upgrade to the <a href="#">latest version</a> of the MARS agent.</li><li>Move the scratch folder or cache location to a volume with free space that's between 5% and 10% of the total size of the backup data. To correctly move the cache location, refer to the steps in <a href="#">Common questions about backing up files and folders</a>.</li><li>Ensure that the OnlineBackup.KEK file is present.<br/><i>The default location for the scratch folder or the cache path is C:\Program Files\Microsoft Azure Recovery Services Agent\Scratch.</i></li></ul> |

## Encryption passphrase not correctly configured

| ERROR                                                                                       | POSSIBLE CAUSES                                                                                                                                                                                                                | RECOMMENDED ACTIONS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Error 34506. The encryption passphrase stored on this computer is not correctly configured. | <ul style="list-style-type: none"><li>The scratch folder is located on a volume that doesn't have enough space.</li><li>The scratch folder has been incorrectly moved.</li><li>The OnlineBackup.KEK file is missing.</li></ul> | <ul style="list-style-type: none"><li>Upgrade to the <a href="#">latest version</a> of the MARS Agent.</li><li>Move the scratch folder or cache location to a volume with free space that's between 5% and 10% of the total size of the backup data. To correctly move the cache location, refer to the steps in <a href="#">Common questions about backing up files and folders</a>.</li><li>Ensure that the OnlineBackup.KEK file is present.<br/><i>The default location for the scratch folder or the cache path is C:\Program Files\Microsoft Azure Recovery Services Agent\Scratch.</i></li></ul> |

## Backups don't run according to schedule

If scheduled backups don't get triggered automatically but manual backups work correctly, try the following actions:

- Ensure the Windows Server backup schedule doesn't conflict with the Azure files and folders backup schedule.
- Ensure the online backup status is set to **Enable**. To verify the status, take these steps:
  - In Task Scheduler, expand **Microsoft** and select **Online Backup**.
  - Double-click **Microsoft-OnlineBackup** and go to the **Triggers** tab.
  - Check if the status is set to **Enabled**. If it isn't, select **Edit**, select **Enabled**, and then select **OK**.
- Ensure the user account selected for running the task is either **SYSTEM** or **Local Administrators' group** on the server. To verify the user account, go to the **General** tab and check the **Security** options.
- Ensure PowerShell 3.0 or later is installed on the server. To check the PowerShell version, run this command and verify that the **Major** version number is 3 or later:

```
$PSVersionTable.PSVersion
```

- Ensure this path is part of the `PSMODULEPATH` environment variable:

```
<MARS agent installation path>\Microsoft Azure Recovery Services Agent\bin\Modules\MSOnlineBackup
```

- If the PowerShell execution policy for `LocalMachine` is set to `restricted`, the PowerShell cmdlet that triggers the backup task might fail. Run these commands in elevated mode to check and set the execution policy to either `Unrestricted` or `RemoteSigned`:

```
Get-ExecutionPolicy -List
Set-ExecutionPolicy Unrestricted
```

- Ensure there are no missing or corrupt PowerShell module MSOnlineBackup files. If there are any missing or corrupt files, take these steps:

1. From any machine that has a MARS agent that's working properly, copy the MSOnlineBackup folder from `C:\Program Files\Microsoft Azure Recovery Services Agent\bin\Modules`.
2. On the problematic machine, paste the copied files at the same folder location (`C:\Program Files\Microsoft Azure Recovery Services Agent\bin\Modules`).

If there's already an MSOnlineBackup folder on the machine, paste the files into it or replace any existing files.

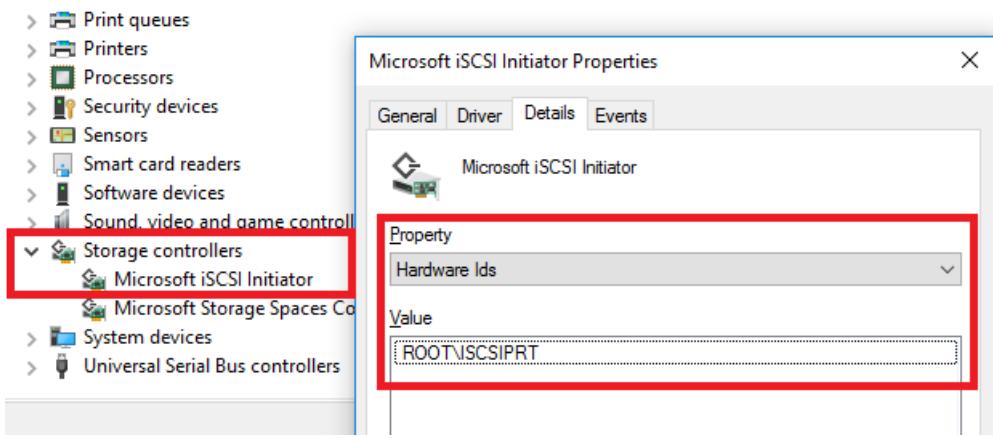
**TIP**

To ensure changes are applied consistently, restart the server after performing the preceding steps.

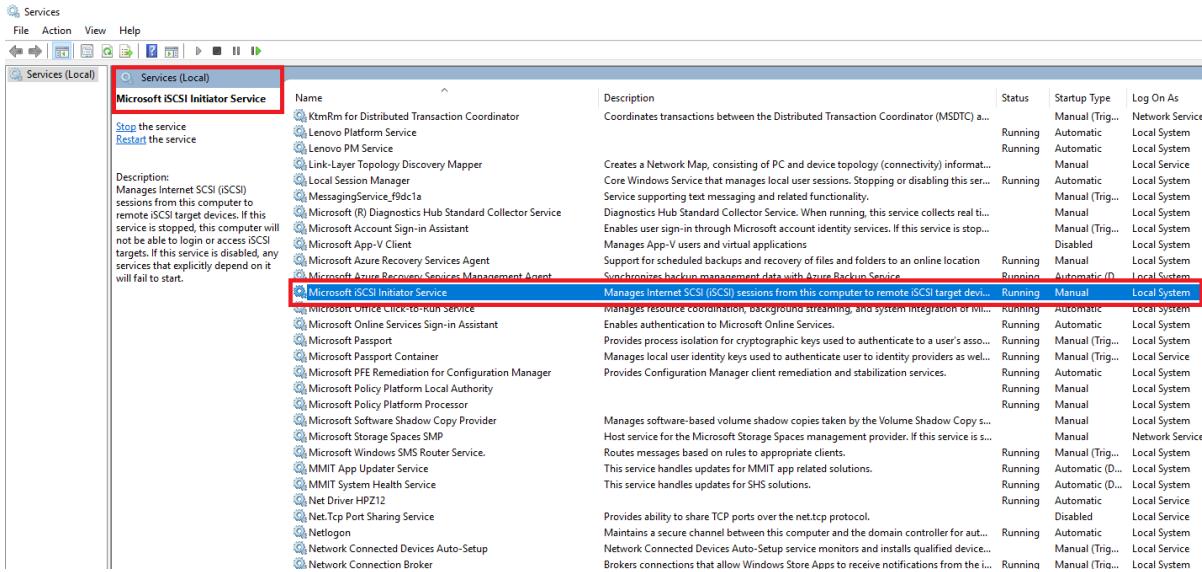
## Troubleshoot restore problems

Azure Backup might not successfully mount the recovery volume, even after several minutes. And you might receive error messages during the process. To begin recovering normally, take these steps:

1. Cancel the mount process if it's been running for several minutes.
2. Check if you have the latest version of the Backup agent. To check the version, on the **Actions** pane of the MARS console, select **About Microsoft Azure Recovery Services Agent**. Confirm that the **Version** number is equal to or higher than the version mentioned in [this article](#). Select this link to [download the latest version](#).
3. Go to **Device Manager > Storage controllers** and locate **Microsoft iSCSI Initiator**. If you locate it, go directly to step 7.
4. If you can't locate the Microsoft iSCSI Initiator service, try to find an entry under **Device Manager > Storage controllers** named **Unknown Device** with Hardware ID **ROOT\ISCSIPRT**.
5. Right-click **Unknown Device** and select **Update Driver Software**.
6. Update the driver by selecting the option to **Search automatically for updated driver software**. This update should change **Unknown Device** to **Microsoft iSCSI Initiator**.



## 7. Go to Task Manager > Services (Local) > Microsoft iSCSI Initiator Service:



8. Restart the Microsoft iSCSI Initiator service. To do this, right-click the service and select **Stop**. Then right-click it again and select **Start**.

9. Retry recovery by using [Instant Restore](#).

If the recovery still fails, restart your server or client. If you don't want to restart, or if the recovery still fails even after you restart the server, try [recovering from another machine](#).

## Troubleshoot Cache problems

Backup operation may fail if the cache folder (also referred as scratch folder) is incorrectly configured, missing prerequisites or has restricted access.

### Prerequisites

For MARS agent operations to succeed the cache folder needs to adhere to the below requirements:

- Ensure 5% to 10% free volume space is available in the scratch folder location
- Ensure scratch folder location is valid and accessible
- Ensure file attributes on the cache folder are supported
- Ensure the allocated shadow copy storage space is sufficient for backup process
- Ensure there are no other processes (ex. anti-virus software) restricting access to cache folder

### Increase shadow copy storage

Backup operations could fail if there is insufficient shadow copy storage space required to protect the data source. To resolve this issue, increase the shadow copy storage space on the protected volume using vssadmin as shown

below:

- Check the current shadow storage space from the elevated command prompt:

```
vssadmin List ShadowStorage /For=[Volume letter]:
```

- Increase the shadow storage space using the below command:

```
vssadmin Resize ShadowStorage /On=[Volume letter]: /For=[Volume letter]: /Maxsize=[size]
```

### Another process or antivirus software blocking access to cache folder

If you have antivirus software installed on the server, add necessary exclusion rules to the antivirus scan for these files and folders:

- The scratch folder. Its default location is C:\Program Files\Microsoft Azure Recovery Services Agent\Scratch
- The bin folder at C:\Program Files\Microsoft Azure Recovery Services Agent\Bin
- CBengine.exe
- CSC.exe

## Common issues

This section covers the common errors that you encounter while using MARS agent.

### SalChecksumStoreInitializationFailed

| ERROR MESSAGE                                                                                           | RECOMMENDED ACTION                                                                                                                                                                                                                                                  |
|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Microsoft Azure Recovery Services Agent was unable to access backup checksum stored in scratch location | To resolve this issue, perform the below and restart the server<br>- <a href="#">Check if there is an antivirus or other processes locking the scratch location files</a><br>- <a href="#">Check if the scratch location is valid and accessible to mars agent.</a> |

### SalVhdInitializationError

| ERROR MESSAGE                                                                                       | RECOMMENDED ACTION                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Microsoft Azure Recovery Services Agent was unable to access the scratch location to initialize VHD | To resolve this issue, perform the below and restart the server<br>- <a href="#">Check if there is an antivirus or other processes locking the scratch location files</a><br>- <a href="#">Check if the scratch location is valid and accessible to mars agent.</a> |

### SalLowDiskSpace

| ERROR MESSAGE                                                                           | RECOMMENDED ACTION                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Backup failed due to insufficient storage in volume where the scratch folder is located | To resolve this issue, verify the below steps and retry the operation:<br>- <a href="#">Ensure MARS agent is latest</a><br>- <a href="#">Verify and resolve storage issues that impact backup scratch space</a> |

### SalBitmapError

| ERROR MESSAGE | RECOMMENDED ACTION |
|---------------|--------------------|
|               |                    |

| ERROR MESSAGE                                                                                      | RECOMMENDED ACTION                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unable to find changes in a file. This could be due to various reasons. Please retry the operation | To resolve this issue, verify the below steps and retry the operation:<br>- <a href="#">Ensure MARS agent is latest</a><br>- <a href="#">Verify and resolve storage issues that impact backup scratch space</a> |

## Next steps

- Get more details on [how to back up Windows Server with the Azure Backup agent](#).
- If you need to restore a backup, see [restore files to a Windows machine](#).

# Troubleshoot problems backing up Azure File Shares

1/20/2020 • 6 minutes to read • [Edit Online](#)

You can troubleshoot issues and errors encountered while using Azure File Shares backup with information listed in the following tables.

## Limitations for Azure file share backup during Preview

Backup for Azure File shares is in Preview. Azure File Shares in both general-purpose v1 and general-purpose v2 storage accounts are supported. The following backup scenarios aren't supported for Azure file shares:

- There's no CLI available for protecting Azure Files using Azure Backup.
- The maximum number of scheduled backups per day is one.
- The maximum number of on-demand backups per day is four.
- Use [resource locks](#) on the storage account to prevent accidental deletion of backups in your Recovery Services vault.
- Do not delete snapshots created by Azure Backup. Deleting snapshots can result in loss of recovery points and/or restore failures.
- Do not delete file shares that are protected by Azure Backup. The current solution will delete all snapshots taken by Azure Backup once the file share is deleted and hence lose all restore points

Backup for Azure File Shares in Storage Accounts with [zone redundant storage](#) (ZRS) replication is currently available only in Central US (CUS), East US (EUS), East US 2 (EUS2), North Europe (NE), SouthEast Asia (SEA), West Europe (WE) and West US 2 (WUS2).

## Configuring backup

The following table is for configuring the backup:

| ERROR MESSAGES                                                             | WORKAROUND OR RESOLUTION TIPS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Could not find my Storage Account to configure backup for Azure file share | <ul style="list-style-type: none"><li>• Wait until discovery is complete.</li><li>• Check if any File share from the storage account is already protected with another Recovery Services vault. <b>Note:</b> All file shares in a Storage Account can be protected only under one Recovery Services vault.</li><li>• Be sure the File share is not present in any of the unsupported Storage Accounts.</li><li>• Make sure that the <b>Allow trusted Microsoft services to access this storage account</b> checkbox is checked in the storage account.<a href="#">Learn more</a>.</li></ul> |
| Error in portal states discovery of storage accounts failed.               | If your subscription is partner (CSP-enabled), ignore the error. If your subscription is not CSP-enabled, and your storage accounts can't be discovered, contact support.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Selected Storage Account validation or registration failed.                | Retry the operation, if the problem persists contact support.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| ERROR MESSAGES                                                                       | WORKAROUND OR RESOLUTION TIPS                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Could not list or find File shares in the selected Storage Account.                  | <ul style="list-style-type: none"> <li>Make sure the Storage Account exists in the Resource Group (and has not been deleted or moved after the last validation/registration in vault).</li> <li>Make sure the File share you are looking to protect has not been deleted.</li> <li>Make sure the Storage Account is a supported storage account for File share backup.</li> <li>Check if the File share is already protected in the same Recovery Services vault.</li> </ul> |
| Backup File share configuration (or the protection policy configuration) is failing. | <ul style="list-style-type: none"> <li>Retry the operation to see if the issue persists.</li> <li>Make sure the File share you want to protect has not been deleted.</li> <li>If you are trying to protect multiple File shares at once, and some of the file shares are failing, retry configuring the backup for the failed File shares again.</li> </ul>                                                                                                                  |
| Unable to delete the Recovery Services vault after unprotecting a File share.        | <p>In the Azure portal, open your Vault &gt; <b>Backup Infrastructure</b> &gt; <b>Storage accounts</b> and click <b>Unregister</b> to remove the storage account from the Recovery Services vault.</p>                                                                                                                                                                                                                                                                       |

## Error messages for backup or restore job failures

| ERROR MESSAGES                                                                                                                                                                  | WORKAROUND OR RESOLUTION TIPS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Operation failed as the File share is not found.                                                                                                                                | Make sure the File share you are looking to protect has not been deleted.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Storage account not found or not supported.                                                                                                                                     | <ul style="list-style-type: none"> <li>Make sure the storage account exists in the Resource Group, and was not deleted or removed from the Resource Group after the last validation.</li> <li>Make sure the Storage account is a supported Storage account for File share backup.</li> </ul>                                                                                                                                                                                                                                                                                       |
| You have reached the max limit of snapshots for this file share, you will be able to take more once the older ones expire.                                                      | <ul style="list-style-type: none"> <li>This error can occur when you create multiple on-demand backups for a File.</li> <li>There's a limit of 200 snapshots per File share including the ones taken by Azure Backup. Older scheduled backups (or snapshots) are cleaned up automatically. On-demand backups (or snapshots) must be deleted if the maximum limit is reached.</li> <li>Delete the on-demand backups (Azure file share snapshots) from the Azure Files portal. <b>Note:</b> You lose the recovery points if you delete snapshots created by Azure Backup.</li> </ul> |
| File share backup or restore failed due to storage service throttling. This may be because the storage service is busy processing other requests for the given storage account. | Retry the operation after some time.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| ERROR MESSAGES                                                                                                                                              | WORKAROUND OR RESOLUTION TIPS                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Restore failed with Target File Share Not Found.                                                                                                            | <ul style="list-style-type: none"> <li>Make sure the selected Storage Account exists and the Target File share is not deleted.</li> <li>Make sure the Storage Account is a supported storage account for File share backup.</li> </ul>                                                                                                                                                                                                                                                            |
| Backup or Restore jobs failed due to storage account being in Locked state.                                                                                 | Remove the lock on Storage Account or use delete lock instead of read lock and retry the operation.                                                                                                                                                                                                                                                                                                                                                                                               |
| Recovery failed because number of failed files are more than the threshold.                                                                                 | <ul style="list-style-type: none"> <li>Recovery failure reasons are listed in a file (path provided in Job details). Please address the failures and retry the restore operation for the failed files only.</li> <li>Common reasons for File restore failures:             <ul style="list-style-type: none"> <li>- make sure the files that failed are currently not in use,</li> <li>- a directory with the same name as the failed file exists in the parent directory.</li> </ul> </li> </ul> |
| Recovery failed as no file could be recovered.                                                                                                              | <ul style="list-style-type: none"> <li>Recovery failure reasons are listed in a file (path provided in Job details). Address the failures and retry the restore operations for the failed files only.</li> <li>Common reasons for file restore failure:             <ul style="list-style-type: none"> <li>- Make sure the files that have failed are currently not in use.</li> <li>- A directory with the same name as the failed file exists in the parent directory.</li> </ul> </li> </ul>   |
| Restore fails because one of the files in the source does not exist.                                                                                        | <ul style="list-style-type: none"> <li>The selected items aren't present in the recovery point data. To recover the files, provide the correct file list.</li> <li>The file share snapshot that corresponds to the recovery point is manually deleted. Select a different recovery point and retry the restore operation.</li> </ul>                                                                                                                                                              |
| A Recovery job is in process to the same destination.                                                                                                       | <ul style="list-style-type: none"> <li>File share backup does not support parallel recovery to the same target File share.</li> <li>Wait for the existing recovery to finish and then try again. If you don't find a recovery job in the Recovery Services vault, check other Recovery Services vaults in the same subscription.</li> </ul>                                                                                                                                                       |
| Restore operation failed as target file share is full.                                                                                                      | Increase the target file share size quota to accommodate the restore data and retry the operation.                                                                                                                                                                                                                                                                                                                                                                                                |
| Restore operation failed as an error occurred while performing pre restore operations on File Sync Service resources associated with the target file share. | Please retry after sometime, if the issue persists please contact Microsoft support.                                                                                                                                                                                                                                                                                                                                                                                                              |

| ERROR MESSAGES                                                                                                                          | WORKAROUND OR RESOLUTION TIPS                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>One or more files could not be recovered successfully. For more information, check the failed file list in the path given above.</p> | <ul style="list-style-type: none"> <li>Recovery failure reasons are listed in the file (path provided in the Job details), address the reasons and retry the restore operation for the failed files only.</li> <li>Common reasons for file restore failures are:           <ul style="list-style-type: none"> <li>- Make sure the failed files aren't currently in use.</li> <li>- A directory with the same name as the failed files exists in the parent directory.</li> </ul> </li> </ul> |

## Modify policy

| ERROR MESSAGES                                                              | WORKAROUND OR RESOLUTION TIPS                                                                    |
|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| <p>Another configure protection operation is in progress for this item.</p> | <p>Please wait for the previous modify policy operation to finish and retry after some time.</p> |
| <p>Another operation is in progress on the selected item.</p>               | <p>Please wait for the other in-progress operation to complete and retry after sometime</p>      |

## Next steps

For more information about backing up Azure file shares, see:

- [Back up Azure file shares](#)
- [Back up Azure file share FAQ](#)

# Troubleshoot SQL Server database backup by using Azure Backup

2/25/2020 • 11 minutes to read • [Edit Online](#)

This article provides troubleshooting information for SQL Server databases running on Azure virtual machines.

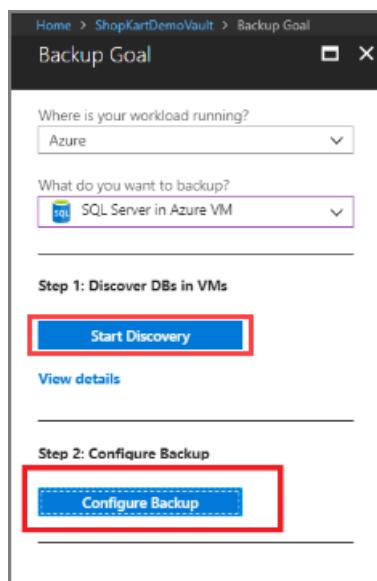
For more information about the backup process and limitations, see [About SQL Server backup in Azure VMs](#).

## SQL Server permissions

To configure protection for a SQL Server database on a virtual machine, you must install the **AzureBackupWindowsWorkload** extension on that virtual machine. If you get the error **UserErrorSQLNoSysadminMembership**, it means your SQL Server instance doesn't have the required backup permissions. To fix this error, follow the steps in [Set VM permissions](#).

## Troubleshoot discover and configure issues

After creating and configuring a Recovery Services vault, discovering databases and configuring backup is a two-step process.



During the backup configuration, if the SQL VM and its instances are not visible in the **Discovery DBs in VMs** and **Configure Backup** (refer to above image) ensure that:

### Step 1: Discovery DBs in VMs

- If the VM is not listed in the discovered VM list and also not registered for SQL backup in another vault, then follow the [Discovery SQL Server backup](#) steps.

### Step 2: Configure Backup

- If the vault in which the SQL VM is registered in the same vault used to protect the databases, then follow the [Configure Backup](#) steps.

If the SQL VM needs to be registered in the new vault, then it must be unregistered from the old vault.

Unregistration of a SQL VM from the vault requires all the protected data sources to be stop protected and then you can delete the backed up data. Deleting backed up data is a destructive operation. After you have reviewed and taken all the precautions to unregister the SQL VM, then register this same VM with a new vault and retry the

backup operation.

## Error messages

### Backup type unsupported

| Severity | Description                                                                                             | Possible causes                                                                                                                                                                                                                                                                                         | Recommended action                                                                                                                                                                                                                                                                                   |
|----------|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Warning  | Current settings for this database don't support certain backup types present in the associated policy. | <ul style="list-style-type: none"><li>Only a full database backup operation can be performed on the master database. Neither differential backup nor transaction log backup is possible.</li><li>Any database in the simple recovery model does not allow for the backup of transaction logs.</li></ul> | Modify the database settings such that all the backup types in the policy are supported. Or, change the current policy to include only the supported backup types. Otherwise, the unsupported backup types will be skipped during scheduled backup or the backup job will fail for on-demand backup. |

### UserErrorSQLPODoesNotSupportBackupType

| Error message                                                 | Possible causes                                                                                                                                                                                                                                                                                                                                                                                                                            | Recommended action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| This SQL database does not support the requested backup type. | <p>Occurs when the database recovery model doesn't allow the requested backup type. The error can happen in the following situations:</p> <ul style="list-style-type: none"><li>A database that's using a simple recovery model does not allow log backup.</li><li>Differential and log backups are not allowed for a master database.</li></ul> <p>For more detail, see the <a href="#">SQL Server recovery models</a> documentation.</p> | <p>If the log backup fails for the database in the simple recovery model, try one of these options:</p> <ul style="list-style-type: none"><li>If the database is in simple recovery mode, disable log backups.</li><li>Use the <a href="#">SQL Server documentation</a> to change the database recovery model to full or bulk logged.</li><li>If you don't want to change the recovery model, and you have a standard policy to back up multiple databases that can't be changed, ignore the error. Your full and differential backups will work per schedule. The log backups will be skipped, which is expected in this case.</li></ul> <p>If it's a master database and you have configured differential or log backup, use either of the following steps:</p> <ul style="list-style-type: none"><li>Use the portal to change the backup policy schedule for the master database, to full.</li><li>If you have a standard policy to back up multiple databases that can't be changed, ignore the error. Your full backup will work per schedule. Differential or log backups won't happen, which is expected in this case.</li></ul> |

| ERROR MESSAGE                                                                           | POSSIBLE CAUSES                                                                                | RECOMMENDED ACTION                                                                                                                                |
|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Operation canceled as a conflicting operation was already running on the same database. | See the <a href="#">blog entry about backup and restore limitations</a> that run concurrently. | Use <a href="#">SQL Server Management Studio (SSMS)</a> to monitor the backup jobs. After the conflicting operation fails, restart the operation. |

### UserErrorSQLPODoesNotExist

| ERROR MESSAGE                | POSSIBLE CAUSES                             | RECOMMENDED ACTION                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SQL database does not exist. | The database was either deleted or renamed. | <p>Check if the database was accidentally deleted or renamed.</p> <p>If the database was accidentally deleted, to continue backups, restore the database to the original location.</p> <p>If you deleted the database and don't need future backups, then in the Recovery Services vault, select <b>Stop backup with Retain Backup Data</b> or <b>Delete Backup Data</b>. For more information, see <a href="#">Manage and monitor backed-up SQL Server databases</a>.</p> |

### UserErrorSQLLSNValidationFailure

| ERROR MESSAGE        | POSSIBLE CAUSES                                                                                     | RECOMMENDED ACTION                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------|-----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Log chain is broken. | The database or the VM is backed up through another backup solution, which truncates the log chain. | <ul style="list-style-type: none"> <li>Check if another backup solution or script is in use. If so, stop the other backup solution.</li> <li>If the backup was an on-demand log backup, trigger a full backup to start a new log chain. For scheduled log backups, no action is needed because the Azure Backup service will automatically trigger a full backup to fix this issue.</li> </ul> |

### UserErrorOpeningSQLConnection

| ERROR MESSAGE | POSSIBLE CAUSES | RECOMMENDED ACTION |
|---------------|-----------------|--------------------|
|               |                 |                    |

| ERROR MESSAGE                                            | POSSIBLE CAUSES                                        | RECOMMENDED ACTION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------------|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Azure Backup is not able to connect to the SQL instance. | Azure Backup can't connect to the SQL Server instance. | <p>Use the additional details on the Azure portal error menu to narrow down the root causes. Refer to <a href="#">SQL backup troubleshooting</a> to fix the error.</p> <ul style="list-style-type: none"> <li>If the default SQL settings don't allow remote connections, change the settings. See the following articles for information about changing the settings:             <ul style="list-style-type: none"> <li><a href="#">MSSQLSERVER_-1</a></li> <li><a href="#">MSSQLSERVER_2</a></li> <li><a href="#">MSSQLSERVER_53</a></li> </ul> </li> <li>If there are login issues, use these links to fix them:             <ul style="list-style-type: none"> <li><a href="#">MSSQLSERVER_18456</a></li> <li><a href="#">MSSQLSERVER_18452</a></li> </ul> </li> </ul> |

#### UserErrorParentFullBackupMissing

| ERROR MESSAGE                                      | POSSIBLE CAUSES                                                                                                                                                                    | RECOMMENDED ACTION                |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| First full backup is missing for this data source. | Full backup is missing for the database. Log and differential backups are parents to a full backup, so be sure to take full backups before triggering differential or log backups. | Trigger an on-demand full backup. |

#### UserErrorBackupFailedAsTransactionLogIsFull

| ERROR MESSAGE                                                      | POSSIBLE CAUSES                               | RECOMMENDED ACTION                                                         |
|--------------------------------------------------------------------|-----------------------------------------------|----------------------------------------------------------------------------|
| Cannot take backup as transaction log for the data source is full. | The database transactional log space is full. | To fix this issue, refer to the <a href="#">SQL Server documentation</a> . |

#### UserErrorCannotRestoreExistingDBWithoutForceOverwrite

| ERROR MESSAGE                                                 | POSSIBLE CAUSES                                                           | RECOMMENDED ACTION                                                                                                                                  |
|---------------------------------------------------------------|---------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Database with same name already exists at the target location | The target restore destination already has a database with the same name. | <ul style="list-style-type: none"> <li>Change the target database name.</li> <li>Or, use the force overwrite option on the restore page.</li> </ul> |

#### UserErrorRestoreFailedDatabaseCannotBeOffline

| ERROR MESSAGE                                                | POSSIBLE CAUSES                                                                                                            | RECOMMENDED ACTION                                                                                                                                                 |
|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Restore failed as the database could not be brought offline. | While you're doing a restore, the target database needs to be brought offline. Azure Backup can't bring this data offline. | Use the additional details on the Azure portal error menu to narrow down the root causes. For more information, see the <a href="#">SQL Server documentation</a> . |

#### UserErrorCannotFindServerCertificateWithThumbprint

| ERROR MESSAGE                                                     | POSSIBLE CAUSES                                                                             | RECOMMENDED ACTION                                                                           |
|-------------------------------------------------------------------|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| Cannot find the server certificate with thumbprint on the target. | The master database on the destination instance doesn't have a valid encryption thumbprint. | Import the valid certificate thumbprint used on the source instance, to the target instance. |

#### UserErrorRestoreNotPossibleBecauseLogBackupContainsBulkLoggedChanges

| ERROR MESSAGE                                                                                                                                     | POSSIBLE CAUSES                                                                                                                              | RECOMMENDED ACTION                                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| The log backup used for recovery contains bulk-logged changes. It cannot be used to stop at an arbitrary point in time as per the SQL guidelines. | When a database is in bulk-logged recovery mode, the data between a bulk-logged transaction and the next log transaction can't be recovered. | Choose a different point in time for recovery. <a href="#">Learn more</a> . |

#### FabricSvcBackupPreferenceCheckFailedUserError

| ERROR MESSAGE                                                                                                                    | POSSIBLE CAUSES                                                          | RECOMMENDED ACTION                                                                                                                                                                                                                                                        |
|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Backup preference for SQL Always On Availability Group cannot be met as some nodes of the Availability Group are not registered. | Nodes required to perform backups are not registered or are unreachable. | <ul style="list-style-type: none"> <li>Ensure that all the nodes required to perform backups of this database are registered and healthy, and then retry the operation.</li> <li>Change the backup preference for the SQL Server Always On availability group.</li> </ul> |

#### VMNotInRunningStateUserError

| ERROR MESSAGE                                                                | POSSIBLE CAUSES      | RECOMMENDED ACTION                              |
|------------------------------------------------------------------------------|----------------------|-------------------------------------------------|
| SQL server VM is either shutdown and not accessible to Azure Backup service. | The VM is shut down. | Ensure that the SQL Server instance is running. |

#### GuestAgentStatusUnavailableUserError

| ERROR MESSAGE                                                                                                          | POSSIBLE CAUSES                                 | RECOMMENDED ACTION                                   |
|------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|------------------------------------------------------|
| Azure Backup service uses Azure VM guest agent for doing backup but guest agent is not available on the target server. | The guest agent is not enabled or is unhealthy. | <a href="#">Install the VM guest agent</a> manually. |

#### AutoProtectionCancelledOrNotValid

| ERROR MESSAGE                                                  | POSSIBLE CAUSES                                                                                                                                                                                                                                                   | RECOMMENDED ACTION                                                             |
|----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Auto-protection Intent was either removed or is no more valid. | When you enable auto-protection on a SQL Server instance, <b>Configure Backup</b> jobs run for all the databases in that instance. If you disable auto-protection while the jobs are running, then the <b>In-Progress</b> jobs are canceled with this error code. | Enable auto-protection once again to help protect all the remaining databases. |

#### CloudDosAbsoluteLimitReached

| ERROR MESSAGE                                                                                     | POSSIBLE CAUSES                                                                                                                                                                                                                                                                                     | RECOMMENDED ACTION                                                                                                                                |
|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Operation is blocked as you have reached the limit on number of operations permitted in 24 hours. | When you have reached the maximum permissible limit for an operation in a span of 24 hours, this error comes. For example: If you have hit the limit for the number of configure backup jobs that can be triggered per day, and you try to configure backup on a new item, you will see this error. | Typically, retrying the operation after 24 hours resolves this issue. However, if the issue persists, you can contact Microsoft support for help. |

### CloudDosAbsoluteLimitReachedWithRetry

| ERROR MESSAGE                                                                                                        | POSSIBLE CAUSES                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | RECOMMENDED ACTION                                                           |
|----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| Operation is blocked as the vault has reached its maximum limit for such operations permitted in a span of 24 hours. | When you have reached the maximum permissible limit for an operation in a span of 24 hours, this error comes. This error usually comes when there are at-scale operations such as modify policy or auto-protection. Unlike in the case of CloudDosAbsoluteLimitReached, there is not much you can do to resolve this state, in fact, Azure Backup service will retry the operations internally for all the items in question. For example: If you have a large number of datasources protected with a policy and you try to modify that policy, it will trigger configure protection jobs for each of the protected items and sometimes may hit the maximum limit permissible for such operations per day. | Azure Backup service will automatically retry this operation after 24 hours. |

### UserErrorVMInternetConnectivityIssue

| ERROR MESSAGE                                                                           | POSSIBLE CAUSES                                                                                               | RECOMMENDED ACTION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The VM is not able to contact Azure Backup service due to internet connectivity issues. | The VM needs outbound connectivity to Azure Backup Service, Azure Storage or Azure Active Directory services. | <ul style="list-style-type: none"> <li>- If you use NSG to restrict connectivity, then you should use the AzureBackup service tag to allows outbound access to Azure Backup to Azure Backup Service, Azure Storage or Azure Active Directory services. Follow these <a href="#">steps</a> to grant access.</li> <li>- Ensure DNS is resolving Azure endpoints.</li> <li>- Check if the VM is behind a load balancer blocking internet access. By assigning public IP to the VMs, discovery will work.</li> <li>- Verify there is no firewall/antivirus/proxy that is blocking calls to the above three target services.</li> </ul> |

## Re-registration failures

Check for one or more of the following symptoms before you trigger the re-register operation:

- All operations (such as backup, restore, and configure backup) are failing on the VM with one of the

following error codes: **WorkloadExtensionNotReachable**, **UserErrorWorkloadExtensionNotInstalled**, **WorkloadExtensionNotPresent**, **WorkloadExtensionDidntDequeueMsg**.

- If the **Backup Status** area for the backup item is showing **Not reachable**, rule out all the other causes that might result in the same status:

- Lack of permission to perform backup-related operations on the VM.
- Shutdown of the VM, so backups cannot take place.
- Network issues.

| Database               | Instance or AlwaysOn AG | Type                | Backup Status              |
|------------------------|-------------------------|---------------------|----------------------------|
| nopstoredata_restor... | nopcommerce\MSQLSER...  | Standalone Instance | <span>Not reachable</span> |
| master                 | nopcommerce\MSQLSER...  | Standalone Instance | <span>Not reachable</span> |
| msdb                   | nopcommerce\MSQLSER...  | Standalone Instance | <span>Not reachable</span> |
| nopstoredata           | nopcommerce\MSQLSER...  | Standalone Instance | <span>Not reachable</span> |
| model                  | nopcommerce\MSQLSER...  | Standalone Instance | <span>Not reachable</span> |

- In the case of an Always On availability group, the backups started failing after you changed the backup preference or after a failover.

These symptoms may arise for one or more of the following reasons:

- An extension was deleted or uninstalled from the portal.
- An extension was uninstalled from **Control Panel** on the VM under **Uninstall or Change a Program**.
- The VM was restored back in time through in-place disk restore.
- The VM was shut down for an extended period, so the extension configuration on it expired.
- The VM was deleted, and another VM was created with the same name and in the same resource group as the deleted VM.
- One of the availability group nodes didn't receive the complete backup configuration. This can happen when the availability group is registered to the vault or when a new node is added.

In the preceding scenarios, we recommend that you trigger a re-register operation on the VM. See [here](#) for instructions on how to perform this task in PowerShell.

## Size limit for files

The total string size of files depends not only on the number of files but also on their names and paths. For each database file, get the logical file name and physical path. You can use this SQL query:

```
SELECT mf.name AS LogicalName, Physical_Name AS Location FROM sys.master_files mf
INNER JOIN sys.databases db ON db.database_id = mf.database_id
WHERE db.name = N'<Database Name>''
```

Now arrange them in the following format:

```
[{"path": "<Location>", "logicalName": "<LogicalName>", "isDir": false}, {"path": "<Location>", "logicalName": "<LogicalName>", "isDir": false}]]
```

Here's an example:

```
[{"path": "F:\\Data\\TestDB12.mdf", "logicalName": "TestDB12", "isDir": false}, {"path": "F:\\Log\\TestDB12_log.ldf", "logicalName": "TestDB12_log", "isDir": false}]]
```

If the string size of the content exceeds 20,000 bytes, the database files are stored differently. During recovery, you won't be able to set the target file path for restore. The files will be restored to the default SQL path provided by SQL Server.

### Override the default target restore file path

You can override the target restore file path during the restore operation by placing a JSON file that contains the mapping of the database file to the target restore path. Create a `database_name.json` file and place it in the location `C:\\Program Files\\Azure Workload Backup\\bin\\plugins\\SQL`.

The content of the file should be in this format:

```
[
 {
 "Path": "<Restore_Path>",
 "LogicalName": "<LogicalName>",
 "IsDir": "false"
 },
 {
 "Path": "<Restore_Path>",
 "LogicalName": "LogicalName",
 "IsDir": "false"
 },
]
```

Here's an example:

```
[
 {
 "Path": "F:\\Data\\testdb2_1546408741449456.mdf",
 "LogicalName": "testdb7",
 "IsDir": "false"
 },
 {
 "Path": "F:\\Log\\testdb2_log_1546408741449456.ldf",
 "LogicalName": "testdb7_log",
 "IsDir": "false"
 },
]
```

In the preceding content, you can get the logical name of the database file by using the following SQL query:

```
SELECT mf.name AS LogicalName FROM sys.master_files mf
INNER JOIN sys.databases db ON db.database_id = mf.database_id
WHERE db.name = N'<Database Name>'"
```

This file should be placed before you trigger the restore operation.

## Next steps

For more information about Azure Backup for SQL Server VMs (public preview), see [Azure Backup for SQL VMs](#).

# Troubleshoot backup of SAP HANA databases on Azure

2/27/2020 • 4 minutes to read • [Edit Online](#)

This article provides troubleshooting information for backing up SAP HANA databases on Azure virtual machines. For more information on the SAP HANA backup scenarios we currently support, see [Scenario support](#).

## Prerequisites and Permissions

Refer to the [prerequisites](#) and [What the pre-registration script does](#) sections before configuring backups.

## Common user errors

### UserErrorHANAInternalRoleNotPresent

|                           |                                                                                                                                                                                                                           |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ERROR MESSAGE</b>      | AZURE BACKUP DOES NOT HAVE REQUIRED ROLE PRIVILEGES TO CARRY OUT BACKUP                                                                                                                                                   |
| <b>Possible causes</b>    | The role may have been overwritten.                                                                                                                                                                                       |
| <b>Recommended action</b> | To resolve the issue, run the script from the <b>Discover DB</b> pane, or download it <a href="#">here</a> . Alternatively, add the 'SAP_INTERNAL_HANA_SUPPORT' role to the Workload Backup User (AZUREWLBACKUPHANAUSER). |

### UserErrorInOpeningHanaOdbcConnection

|                           |                                                                                                                                                                                                                                              |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ERROR MESSAGE</b>      | FAILED TO CONNECT TO HANA SYSTEM                                                                                                                                                                                                             |
| <b>Possible causes</b>    | The SAP HANA instance may be down.<br>The required permissions for Azure backup to interact with the HANA database aren't set.                                                                                                               |
| <b>Recommended action</b> | Check if the SAP HANA database is up. If the database is up and running, check if all the required permissions are set. If any of the permissions are missing run the <a href="#">preregistration script</a> to add the missing permissions. |

### UserErrorHanaInstanceNameInvalid

|                           |                                                                                                                                                      |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ERROR MESSAGE</b>      | THE SPECIFIED SAP HANA INSTANCE IS EITHER INVALID OR CAN'T BE FOUND                                                                                  |
| <b>Possible causes</b>    | Multiple SAP HANA instances on a single Azure VM can't be backed up.                                                                                 |
| <b>Recommended action</b> | Run the <a href="#">preregistration script</a> on the SAP HANA instance you want to back up. If the issue still persists, contact Microsoft support. |

### UserErrorHanaUnsupportedOperation

|                           |                                                                                                                                              |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ERROR MESSAGE</b>      | THE SPECIFIED SAP HANA OPERATION ISN'T SUPPORTED                                                                                             |
| <b>Possible causes</b>    | Azure backup for SAP HANA doesn't support incremental backup and actions performed on SAP HANA native clients (Studio/ Cockpit/ DBA Cockpit) |
| <b>Recommended action</b> | For more information, refer <a href="#">here</a> .                                                                                           |

#### UserErrorHANAPODoesNotSupportBackupType

|                           |                                                                            |
|---------------------------|----------------------------------------------------------------------------|
| <b>ERROR MESSAGE</b>      | THIS SAP HANA DATABASE DOESN'T SUPPORT THE REQUESTED BACKUP TYPE           |
| <b>Possible causes</b>    | Azure backup doesn't support incremental backup and backup using snapshots |
| <b>Recommended action</b> | For more information, refer <a href="#">here</a> .                         |

#### UserErrorHANALSNValidationFailure

|                           |                                                                                                                              |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>ERROR MESSAGE</b>      | BACKUP LOG CHAIN IS BROKEN                                                                                                   |
| <b>Possible causes</b>    | The log backup destination may have been updated from backint to file system or the backint executable may have been changed |
| <b>Recommended action</b> | Trigger a full backup to resolve the issue                                                                                   |

#### UserErrorIncompatibleSrcTargetSystsemsForRestore

|                           |                                                                                                |
|---------------------------|------------------------------------------------------------------------------------------------|
| <b>ERROR MESSAGE</b>      | THE SOURCE AND TARGET SYSTEMS FOR RESTORE ARE INCOMPATIBLE                                     |
| <b>Possible causes</b>    | The target system for restore is incompatible with the source                                  |
| <b>Recommended action</b> | Refer to the SAP Note <a href="#">1642148</a> to learn about the restore types supported today |

#### UserErrorSDCtoMDCUpgradeDetected

|                           |                                                                                                                |
|---------------------------|----------------------------------------------------------------------------------------------------------------|
| <b>ERROR MESSAGE</b>      | SDC TO MDC UPGRADE DETECTED                                                                                    |
| <b>Possible causes</b>    | The SAP HANA instance has been upgraded from SDC to MDC. Backups will fail after the update.                   |
| <b>Recommended action</b> | Follow the steps listed in the <a href="#">Upgrading from SAP HANA 1.0 to 2.0 section</a> to resolve the issue |

#### UserErrorInvalidBackintConfiguration

|                        |                                                                   |
|------------------------|-------------------------------------------------------------------|
| <b>ERROR MESSAGE</b>   | DETECTED INVALID BACKINT CONFIGURATION                            |
| <b>Possible causes</b> | The backing parameters are incorrectly specified for Azure backup |

| ERROR MESSAGE      | DETECTED INVALID BACKINT CONFIGURATION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Recommended action | <p>Check if the following (backint) parameters are set:</p> <ul style="list-style-type: none"> <li>* [catalog_backup_using_backint:true]</li> <li>* [enable_accumulated_catalog_backup:false]</li> <li>* [parallel_data_backup_backint_channels:1]</li> <li>* [log_backup_timeout_s:900]</li> <li>* [backint_response_timeout:7200]</li> </ul> <p>If backint-based parameters are present in HOST, remove them. If parameters aren't present at HOST level but have been manually modified at a database level, revert them to the appropriate values as described earlier. Or, run <a href="#">stop protection and retain backup data</a> from the Azure portal, and then select <b>Resume backup</b>.</p> |

## Restore checks

### Single Container Database (SDC) restore

Take care of inputs while restoring a single container database (SDC) for HANA to another SDC machine. The database name should be given with lowercase and with "sdc" appended in brackets. The HANA instance will be displayed in capitals.

Assume an SDC HANA instance "H21" is backed up. The backup items page will show the backup item name as "**h21(sdc)**". If you attempt to restore this database to another target SDC, say H11, then following inputs need to be provided.

|                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Home > hanavm - Backup items > Backup Items (SAP HANA in Azure VM) > h11(sdc) > Restore > Re        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Restore                                                                                             | X                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <p><b>1</b> Choose Destination<br/>Configure &gt;</p> <p><b>2</b> Restore Point<br/>Select &gt;</p> | <h3>Restore Configuration</h3> <p>Where to Restore?</p> <p><b>Alternate Location</b>   <b>Overwrite DB</b></p> <p>If you don't see your SAP HANA Server in the below list go to 'Getting Started' &gt; 'Backup' &gt; 'Start Discovery'</p> <p>* Host (<a href="#">Can't find Host?</a>)<br/>HANAvm</p> <p>* HANA System<br/>H11</p> <p>* Restored DB Name<br/><b>h11(sdc)</b></p> <p><input checked="" type="checkbox"/> Overwrite if the DB with same name already exists on selected HANA instance</p> |
| Restore                                                                                             | <b>OK</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

Note the following points:

- By default, the restored db name will be populated with the backup item name. In this case, h21(sdc).
- Selecting the target as H11 will NOT change the restored db name automatically. **It should be edited to h11(sdc).** Regarding SDC, the restored db name will be the target instance ID with lowercase letters and 'sdc' appended in brackets.
- Since SDC can have only single database, you also need to click the checkbox to allow override of the existing database data with the recovery point data.
- Linux is case-sensitive. So be careful to preserve the case.

## Multiple Container Database (MDC) restore

In multiple container databases for HANA, the standard configuration is SYSTEMDB + 1 or more Tenant DBs.

Restoring an entire SAP HANA instance means to restore both SYSTEMDB and Tenant DBs. One restores SYSTEMDB first and then proceeds for Tenant DB. System DB essentially means to override the system information on the selected target. This restore also overrides the BackInt related information in the target instance. So after the system DB is restored to a target instance, run the pre-registration script again. Only then the subsequent tenant DB restores will succeed.

## Upgrading from SAP HANA 1.0 to 2.0

If you're protecting SAP HANA 1.0 databases and wish to upgrade to 2.0, then perform the following steps:

- [Stop protection](#) with retain data for old SDC database.
- Perform the upgrade. After completion, the HANA is now MDC with a system DB and tenant DB(s)
- Rerun [pre-registration script](#) with correct details of (sid and mdc).
- Re-register extension for the same machine in Azure portal (Backup -> view details -> Select the relevant Azure VM -> Re-register).
- Click Rediscover DBs for the same VM. This action should show the new DBs in step 2 with correct details (SYSTEMDB and Tenant DB, not SDC).
- Configure backup for these new databases.

## Upgrading without an SID change

Upgrades to OS or SAP HANA that don't cause a SID change can be handled as outlined below:

- [Stop protection](#) with retain data for the database
- Perform the upgrade.
- Rerun the [pre-registration script](#). Usually, we have seen upgrade process removes the necessary roles. Running the pre-registration script will help verify all the required roles.
- [Resume protection](#) for the database again

## Next steps

- Review the [frequently asked questions](#) about backing up SAP HANA databases on Azure VMs]

# Troubleshoot System State Backup

2/24/2020 • 5 minutes to read • [Edit Online](#)

This article describes solutions for issues that you might come across while using System State Backup.

## Basic troubleshooting

We recommend you perform the below validation, before you start troubleshooting System State backup:

- [Ensure Microsoft Azure Recovery Services \(MARS\) Agent is up to date](#)
- [Ensure there is network connectivity between MARS agent and Azure](#)
- Ensure Microsoft Azure Recovery Services is running (in Service console). If necessary, restart and retry the operation
- [Ensure 5-10% free volume space is available on scratch folder location](#)
- [Check if another process or antivirus software is interfering with Azure Backup](#)
- [Scheduled backup fails, but manual backup works](#)
- Ensure your OS has the latest updates
- [Ensure unsupported drives and files with unsupported attributes are excluded from backup](#)
- Ensure **System Clock** on the protected system is configured to correct time zone
- [Ensure that the server has at least .Net Framework version 4.5.2 and higher](#)
- If you're trying to **reregister your server** to a vault, then:
  - Ensure the agent is uninstalled on the server and it's deleted from the portal
  - Use the same passphrase that was initially used for registering the server
- If this is an offline backup, ensure that Azure PowerShell version 3.7.0 is installed on both source and copy computer before you begin offline backup operation
- [Consideration when Backup agent is running on an Azure virtual machine](#)

### Limitation

- Recovering to different hardware using System State recovery is not recommended by Microsoft
- System State backup currently supports "on-premises" Windows servers. This functionality isn't available for Azure VMs.

## Prerequisites

Before we troubleshoot System State Backup with Azure Backup, perform the below prerequisites check.

### Verify Windows Server Backup is installed

Ensure Windows Server Backup is installed and enabled in the server. To check the installation status, run this PowerShell command:

```
Get-WindowsFeature Windows-Server-Backup
```

If the output displays the **Install State as available**, then it means Windows Server backup feature is available for the installation but not installed on the server. However, if Windows Server Backup isn't installed, then use one of the methods below to install it.

#### Method 1: Install Windows Server Backup using PowerShell

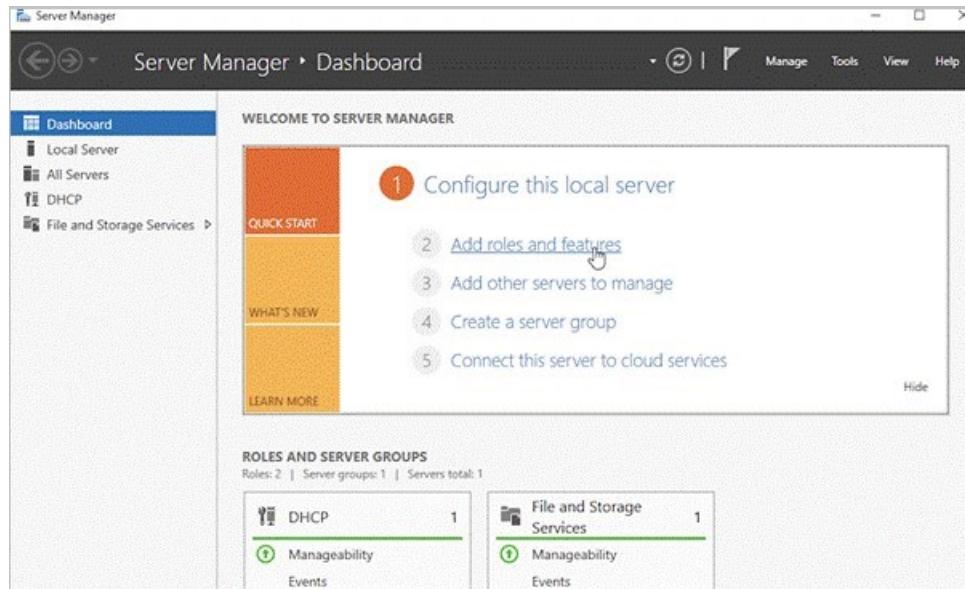
To install Windows Server Backup using PowerShell, run the below command:

```
Install-WindowsFeature -Name Windows-Server-Backup
```

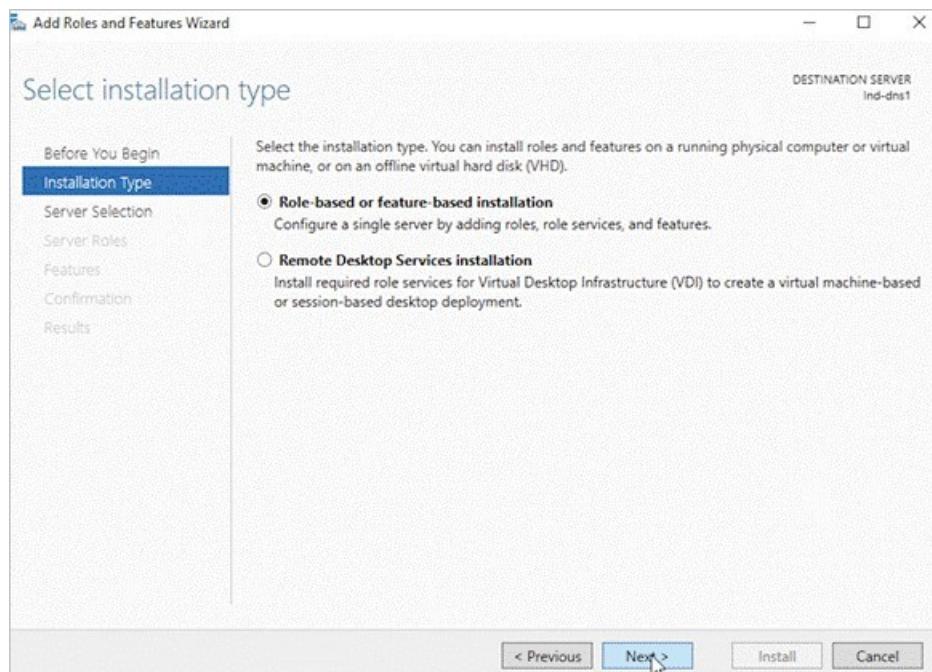
#### Method 2: Install Windows Server Backup using Server Manager

To install Windows Server Backup using Server Manager, perform the steps below:

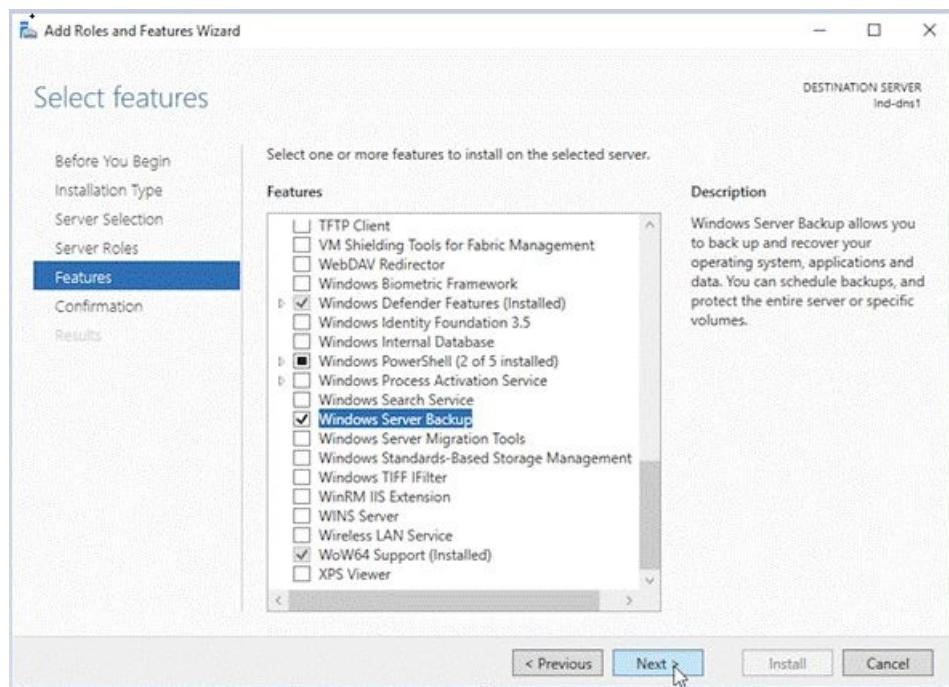
1. In **Server Manager**, click **Add roles and features**. The **Add roles and features wizard** appears.



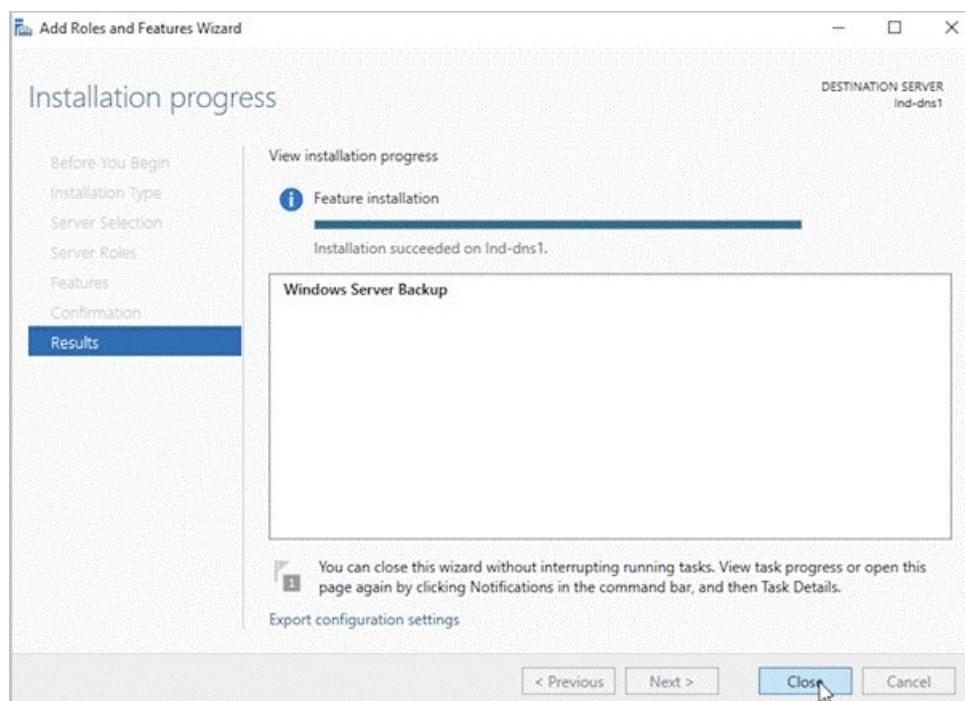
2. Select **Installation Type** and click **Next**.



3. Select a server from the server pool and click **Next**. In the Server Role, leave the default selection and click **Next**.
4. Select **Windows Server Backup** in **Features** tab and click **Next**.



5. In the **Confirmation** tab, click **Install** to start the installation process.
6. In the **Results** tab, it will display the Windows Server Backup feature is successfully installed on your Windows Server.



### System Volume information permission

Ensure that the Local SYSTEM has full control on the **System Volume Information** folder located in the volume where Windows is installed. Usually this is **C:\System Volume Information**. Windows Server backup can fail if the above permissions are not set correctly

### Dependent services

Ensure the below services are in running state:

| SERVICE NAME               | STARTUP TYPE |
|----------------------------|--------------|
| Remote Procedure Call(RPC) | Automatic    |

| Service Name                                   | Startup Type |
|------------------------------------------------|--------------|
| COM+ Event System(EventSystem)                 | Automatic    |
| System Event Notification Service(SENS)        | Automatic    |
| Volume Shadow Copy(VSS)                        | Manual       |
| Microsoft Software Shadow Copy Provider(SWPRV) | Manual       |

## Validate Windows Server Backup status

To validate Windows Server Backup status, perform the following steps:

- Ensure WSB PowerShell is running
  - Run `Get-WBJob` from an elevated PowerShell and make sure it doesn't return the following error:

### WARNING

`Get-WBJob`: The term 'Get-WBJob' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.

- If it fails with this error, then reinstall the Windows Server Backup feature on the server machine as mentioned in step 1 of the prerequisites.
- Ensure WSB backup is working properly, by running the below command from elevated command prompt:

```
wbadmin start systemstatebackup -backuptarget:X: -quiet
```

### NOTE

Replace X with the drive letter of the volume where you want to store the system state back up image.

- Periodically check the status of the job by running `Get-WBJob` command from elevated PowerShell
- After backup job completes check the final status of the job by running `Get-WBJob -Previous 1` command

If the job fails, it indicates a WSB issue that would result in MARS agent System State Backups failure.

## Common errors

### VSS Writer timeout error

| SYMPTOM                                                                                                                                                                                                                                                                                                                                                                      | CAUSE                                                                                                                                                                                                                                    | RESOLUTION                                                                                                                                                                                                                                                           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>- MARS agent fails with error message: "WSB job failed with VSS errors. Check VSS event logs to resolve the failure"</li> <li>- Following error log is present in VSS Application event logs: "A VSS writer has rejected an event with error 0x800423f2, the writer's timeout expired between the Freeze and Thaw events."</li> </ul> | <p>VSS writer is unable to complete in time due to lack of CPU and memory resources on the machine</p> <p>Another backup software is already using the VSS writer, as a result snapshot operation could not complete for this backup</p> | <p>Wait for CPU/memory to be freed up on system or abort the processes taking too much memory/CPU and try the operation again.</p> <p>Wait for the ongoing backup to complete and try the operation at a later point when no backups are running on the machine.</p> |

### Insufficient disk space to grow shadow copies

| SYMPTOM                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | RESOLUTION                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>- MARS agent fails with error message: Backup failed as the shadow copy volume could not grow due to insufficient disk space on volumes containing system files</li> <li>- Following error/warning log is present in volsnap system event logs: "There was insufficient disk space on volume C: to grow the shadow copy storage for shadow copies of C: due to this failure all shadow copies of volume C: are at risk of being deleted"</li> </ul> | <ul style="list-style-type: none"> <li>- Free up space in the highlighted volume in the event log so that there is sufficient space for shadow copies to grow while backup is in progress</li> <li>- While configuring shadow copy space we can restrict the amount of space used for shadow copy. For more information, see this <a href="#">article</a></li> </ul> |

### EFI partition locked

| SYMPTOM                                                                                                                                                                                           | RESOLUTION                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MARS agent fails with error message: "System state backup failed as the EFI system partition is locked. This can be due to system partition access by a third-party security or back up software" | <ul style="list-style-type: none"> <li>- If the issue is due to a third-party security software, then you need to contact the Anti Virus vendor so that they can allow MARS agent</li> <li>- If a third-party backup software is running, then wait for it to finish and then retry back up</li> </ul> |

## Next steps

- For more information about Windows system state in Resource Manager deployment, see [Back up Windows Server System State](#)