

[For .NET Client “On-Prem Server \(Hyper-V virtual machine\) Backups & Restoration” using Microsoft Azure Backup Server \(MABS\) & Visual Studio Code PowerShell Extensions for Backup Jobs Automation.](#)

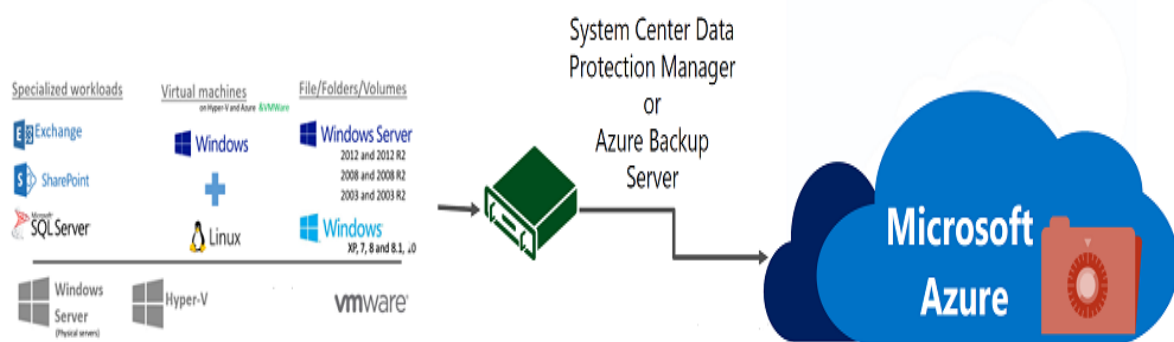
In this blog, we will see the backup solution for On-Prem Server (Hyper-V virtual machine) using Microsoft Azure Backup Server (MABS). How to configure, install, recover & automate the Backup Jobs using Visual Studio Code PowerShell Extension and a complete overview of MABS architecture provided as a service by Azure.

Problem Statement-

Being into an E-commerce domain, there are few On Prem Servers (Hyper-V virtual machines) in our infra integrated with Microsoft Azure. Both the on prem and the azure VMs work together hand in hand to maintain and follow the security perspective/parameters defined by the organization. It is a necessity to back up the servers on which any sort of data resides which may be later used for profit analytics and can provide different business expansion metrics. Azure hosted VMs has an inbuilt service known as Backup centre to back up the data that resides on those azure hosted VMs, but the challenge is faced for on prem server backup. With the increased cost of hardware, installation, and maintenance cost, also many configuration parameters come under the scope of respective on prem team. High availability of these backup data is the uttermost parameter which needs to be taken care of all the time to make sure the recovery is done on time without affecting the business profit model.

Solution Architecture:

Azure Backup: Back up workloads (on-premises and on Azure VMs) protected by DPM or Microsoft Azure Backup Server (MABS)



The Azure Backup Service offers various options for backing up on-premises and cloud-based workloads to Azure storage. Microsoft Azure Backup Server (MABS) is the most powerful option, which can perform application-aware backups of complete machines, as well as individual files and folders, from Windows and Linux machines running on-premises or in Azure VMs. In this blog, we'll see how Azure Backup Server fits into the Azure backup architecture, show how to deploy the server and use it to restore backups, with the most cost-efficient way.

What is the Microsoft Azure Backup Server (MABS)?

Microsoft Azure has the ability to backup entire on-premises machines, entire Azure VMs, or perform a backup of specific data from your workloads. The Microsoft Azure Backup Server (MABS) is a software component you can deploy either on-premises or in the Azure cloud, and is used to Backup on-premises workloads, such as databases, exchange servers, Windows and Linux machines Backup Azure VMs (only if MABS is deployed in Azure) You can configure your on-premise machines or Azure VMs to backup to MABS, and in turn, MABS backs up the data to a Recovery Services Vault in the Azure Cloud. MABS comes with the System Center Data Protection Manager (DPM), a software package that provides near-continuous data protection and data recovery in Microsoft Windows environments.

Three Different Ways to Use Azure Backup-

One thing that people find confusing is that there's different variations of Azure Backup. That can be confusing, so I like to identify the three hybrid offerings using the following names:

- **MARS:** The Microsoft Azure Recovery Services agent that is deployed onto a machine that you want to backup directly to Azure.
- **DPM:** Microsoft System Center Data Protection Manager is an on-premises backup server that will perform disk-to-disk-to-cloud backup.
- **MABS:** The Microsoft Azure Backup Server is also an on-premises backup server that you can get from Microsoft to perform disk-to-disk-to-cloud backup.

The following table differentiates the three Azure Backup hybrid, online backup solutions.

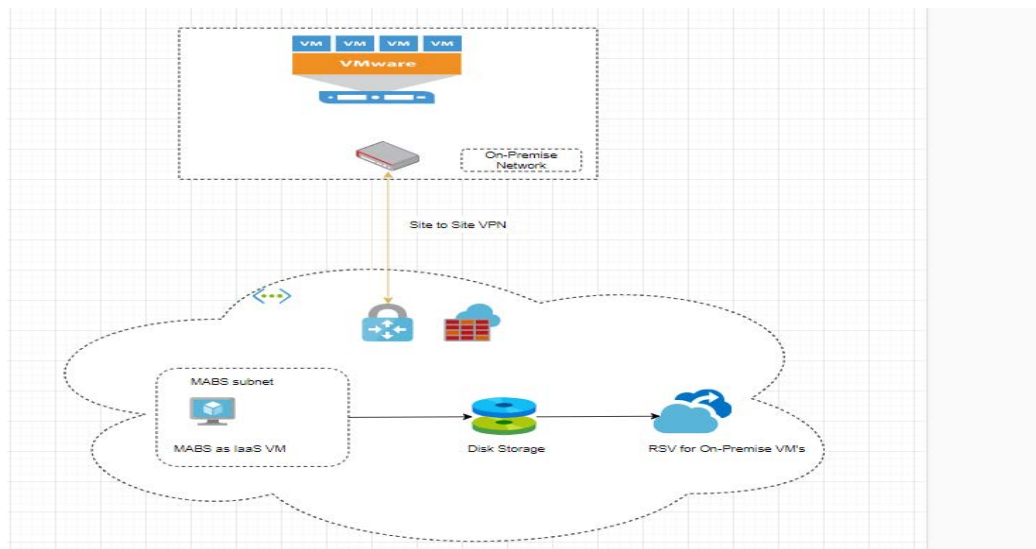
	MARS Agent	System Center DPM	Microsoft Azure Backup Server (MABS)
Description	Disk-to-Cloud	Disk-Disk-Cloud	Disk-Disk-Cloud
Point of management	Agent (Portal support coming)	DPM Server	MABS (Portal support coming)
Backups supported	Files & folders ONLY	Files & Folders Hyper-V SQL Server SharePoint Exchange (vSphere coming)	Files & Folders Hyper-V SQL Server SharePoint Exchange (vSphere coming)
Tape support?	No	Yes	No
Recovery Points in the cloud	9,999	9,999	9,999
Maximum Retention	99 years	99 years	99 years
Security Model	Trust No One	Trust No One	Trust No One
Traffic Shaping	Yes	Yes	Yes
Backup Traffic Window	No	Yes	Yes
Software Cost	Free	System Center per physical machine	Free

Technical Implementation: -

MABS Setup-

- 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.

Below diagram will illustrate more on the setup part -



Prerequisites for MABS-

1. Need to create one RG under Dev env.
2. Need to create one subnet (/27) and NSG under Dev VNET.
3. Need to create VM under Dev env.
 - Disk size: 256GB premium SSD DS3-V2
 - OS type: 2016 Datacenter
4. Need to configure the VM domain and also move it to respective OU
5. Need to add the VM in sentinel workspace and windows Defender for security purpose.
6. Need to configure networking part (Firewall rules to allow on-prem servers)
7. Need to create one RSV under Dev and configure MABS in newly created VM.
8. A secure channel needs to be setup to enable Azure Backup Server to communicate with on-prem VMware servers over HTTPS.
9. Need to get root cred from On-prem VMware end and configure the same to MABS server.
10. Need to take test VM back up (VM level full backup) and monitor the status on MABS Console.

Recovery Test-

1. Test VM has successfully back up on both disk and online.
2. 1. To recover, connection should be established between Azure MABS server and on-prem host 1.
3. 2. once step 1 done, recover the backed up VM from both (disk&online) recovery point to on-prem physical host 2.
4. 3. Once VM successfully recovered, inform on-prem team to check and recover files from recovered VM.

Install and upgrade Azure Backup Server-

The below steps will explain 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.

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.

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's recommended you start with a gallery image of Windows Server 2016 Datacenter or Windows Server 2019 Datacenter. The recommended minimum requirements for the server virtual machine (VM) should be: **Standard_A4_v2 with four cores and 8-GB RAM.**

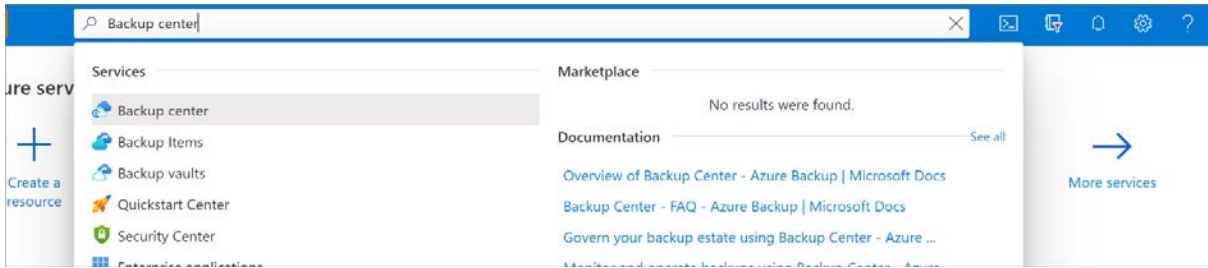
Whether you send backup data to Azure, or keep it locally, Azure Backup Server must be registered with a Recovery Services vault.

Create a Recovery Services vault

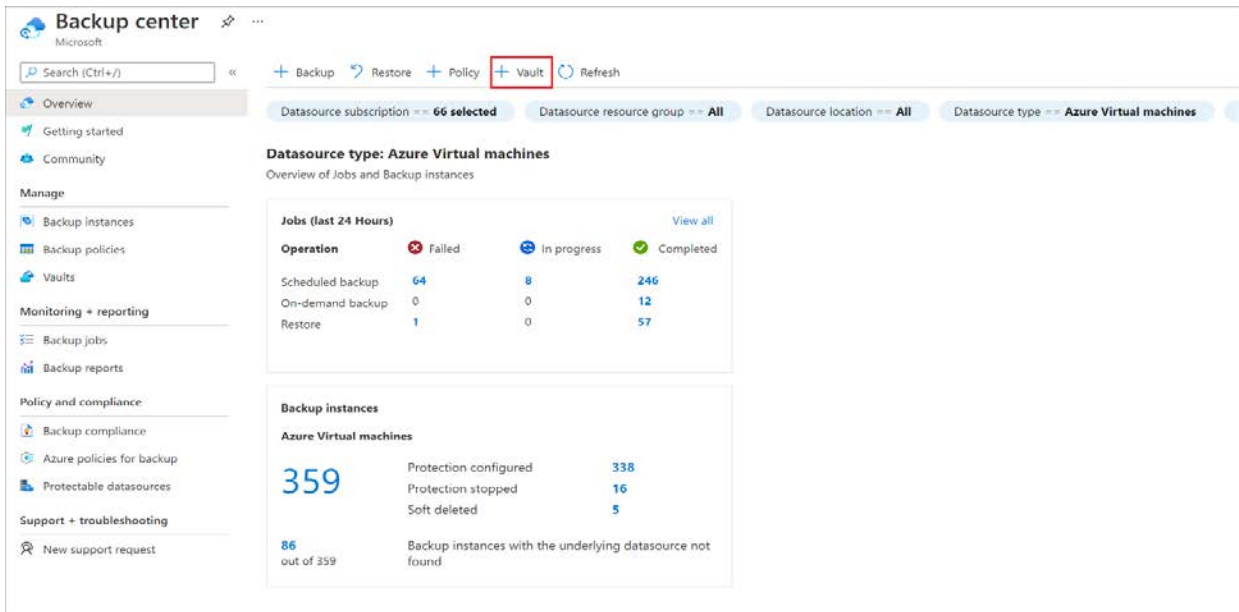
A Recovery Services vault is a management entity that stores recovery points created over time and provides an interface to perform backup-related operations. These operations include taking on-demand backups, performing restores, and creating backup policies.

To create a Recovery Services vault-

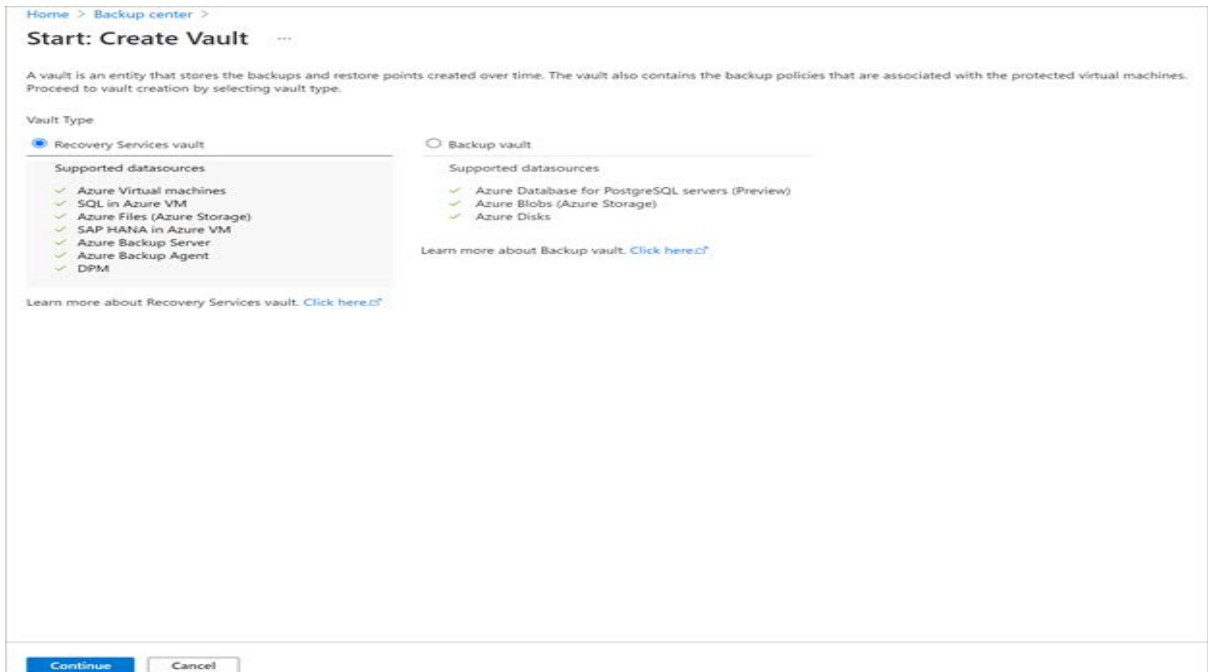
1. Sign in to your subscription in the Azure portal.
2. Search for Backup center in the Azure portal and go to the Backup Center dashboard.



3. Select **+Vault** from the **Overview** tab.



4. Select **Recovery Services vault > Continue**.



5. The **Recovery Services vault** dialog opens. Provide the following values:

Home >

Create Recovery Services vault

Preview

Basics Tags Review + create

Project Details
Select the subscription and the resource group in which you want to create the vault.

Subscription * ⓘ <subscription> ▾

Resource group * ⓘ ▾
[Create new](#)

Instance Details

Vault name * ⓘ Enter the name for your vault.

Region * ⓘ East US ▾

[Review + create](#) [Next: Tags](#)

1. After you provide the values, select **Review + create**.
2. When you're ready to create the Recovery Services vault, select **Create**.
3. 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**.

Software package

Downloading the software package

1. Sign in to the Azure portal.
2. If you already have a Recovery Services vault open, continue to step 3. If you don't have a Recovery Services vault open, but are in the Azure portal, on the main menu, select **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**, select it.
 - The list of Recovery Services vaults appears.
 - From the list of Recovery Services vaults, select a vault. The selected vault dashboard opens.
3. The **Settings** pane opens up by default. If it's closed, select **Settings** to open the settings pane.
4. Select **Backup** to open the Getting Started wizard.

In the **Getting Started with backup** pane that opens, **Backup Goals** will be auto-selected.

5. In the **Backup Goal** pane, 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 select **OK**.

The **Getting Started with backup** wizard switches the **Prepare infrastructure** option to back up workloads to Azure.

6. In the **Prepare infrastructure** pane that opens, select 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 select **Next**. Download all the files coming in from the Microsoft Azure Backup download page, and place all the files in the same folder.

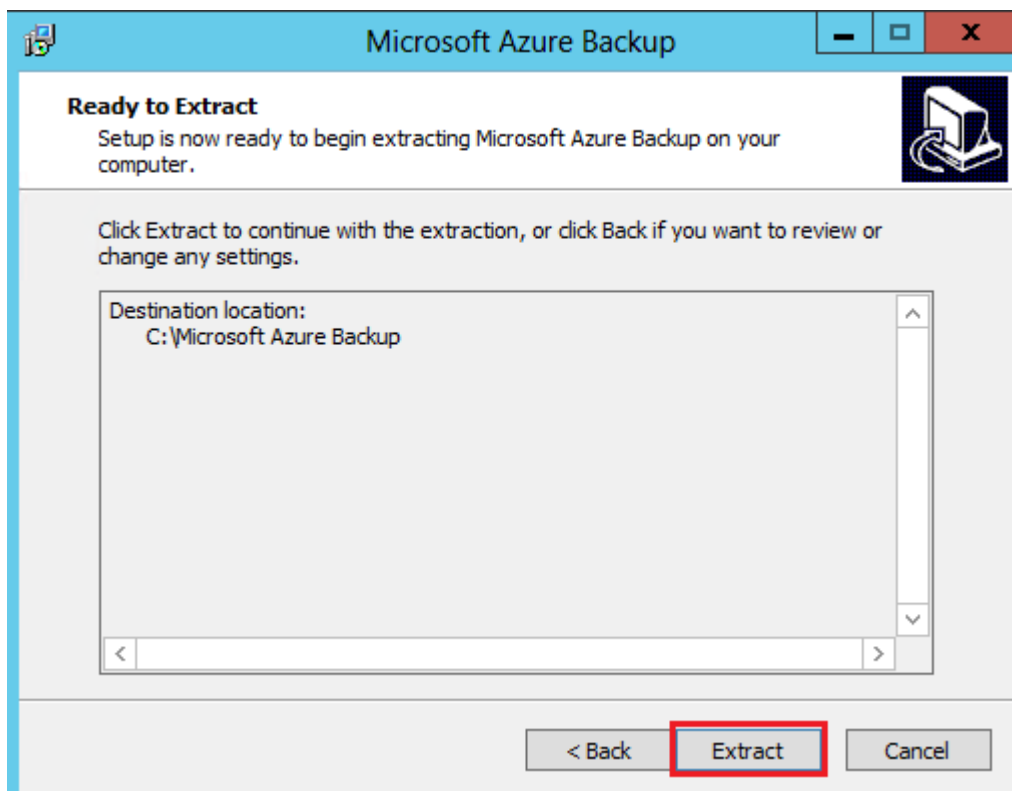
Since the download size of all the files together is > 3 GB, on a 10-Mbps download link it may take up to 60 minutes for the download to complete.

Extracting the software package

After you've downloaded all the files, select **MicrosoftAzureBackupInstaller.exe**. This will start the **Microsoft Azure Backup Setup Wizard** to extract the setup to a location specified by you. Continue through the wizard and select the **Extract** button to begin the extraction process.

Warning

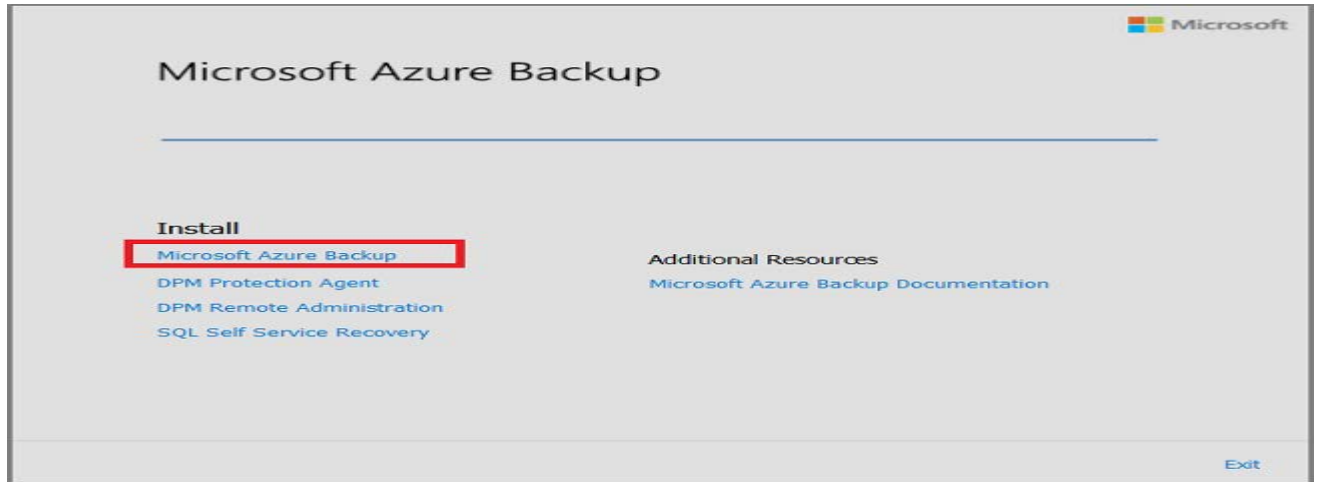
At least 4 GB of free space is required to extract the setup files.



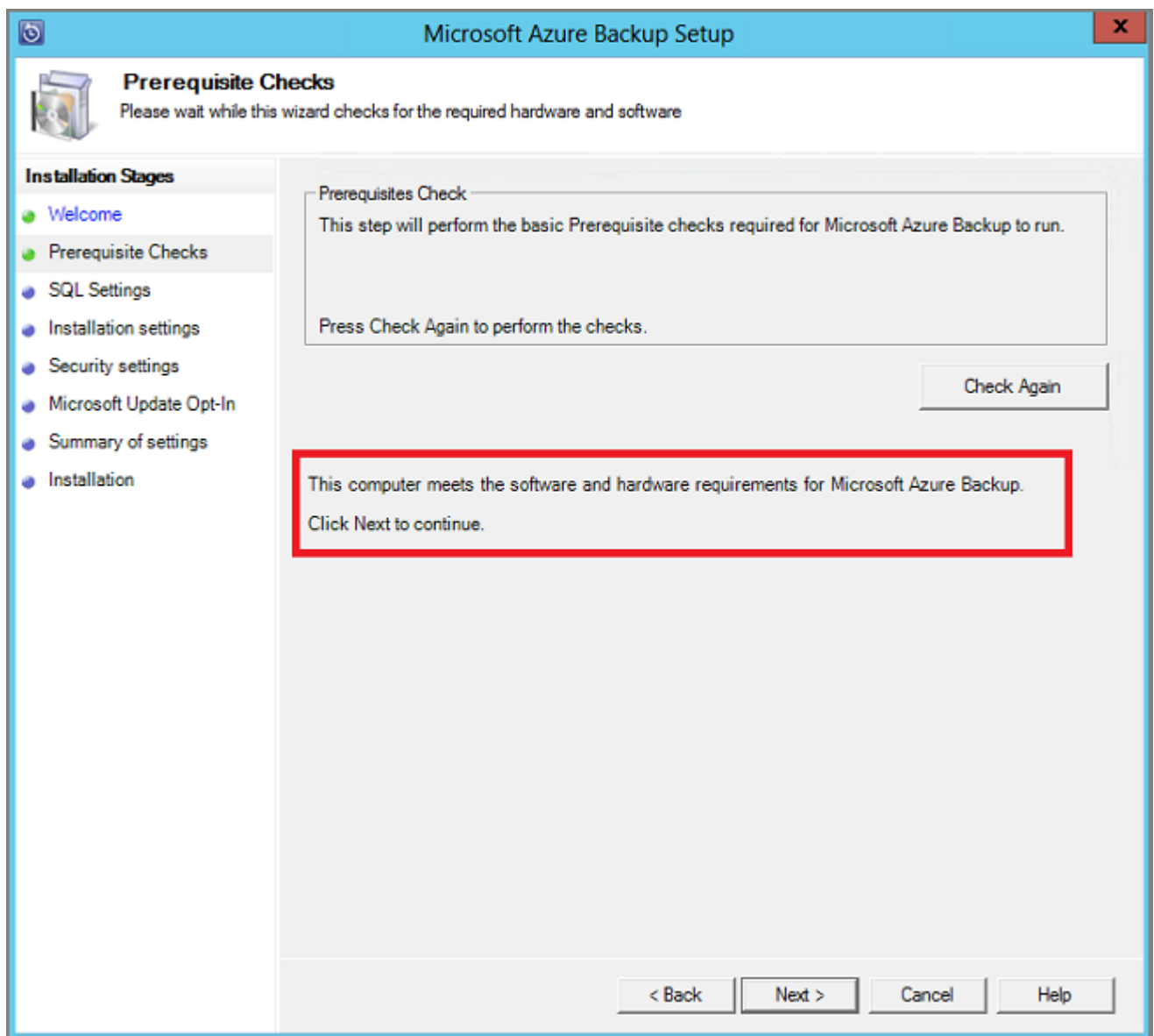
Once the extraction process complete, check the box to launch the freshly extracted setup.exe to begin installing Microsoft Azure Backup Server and select the Finish button.

Installing the software package

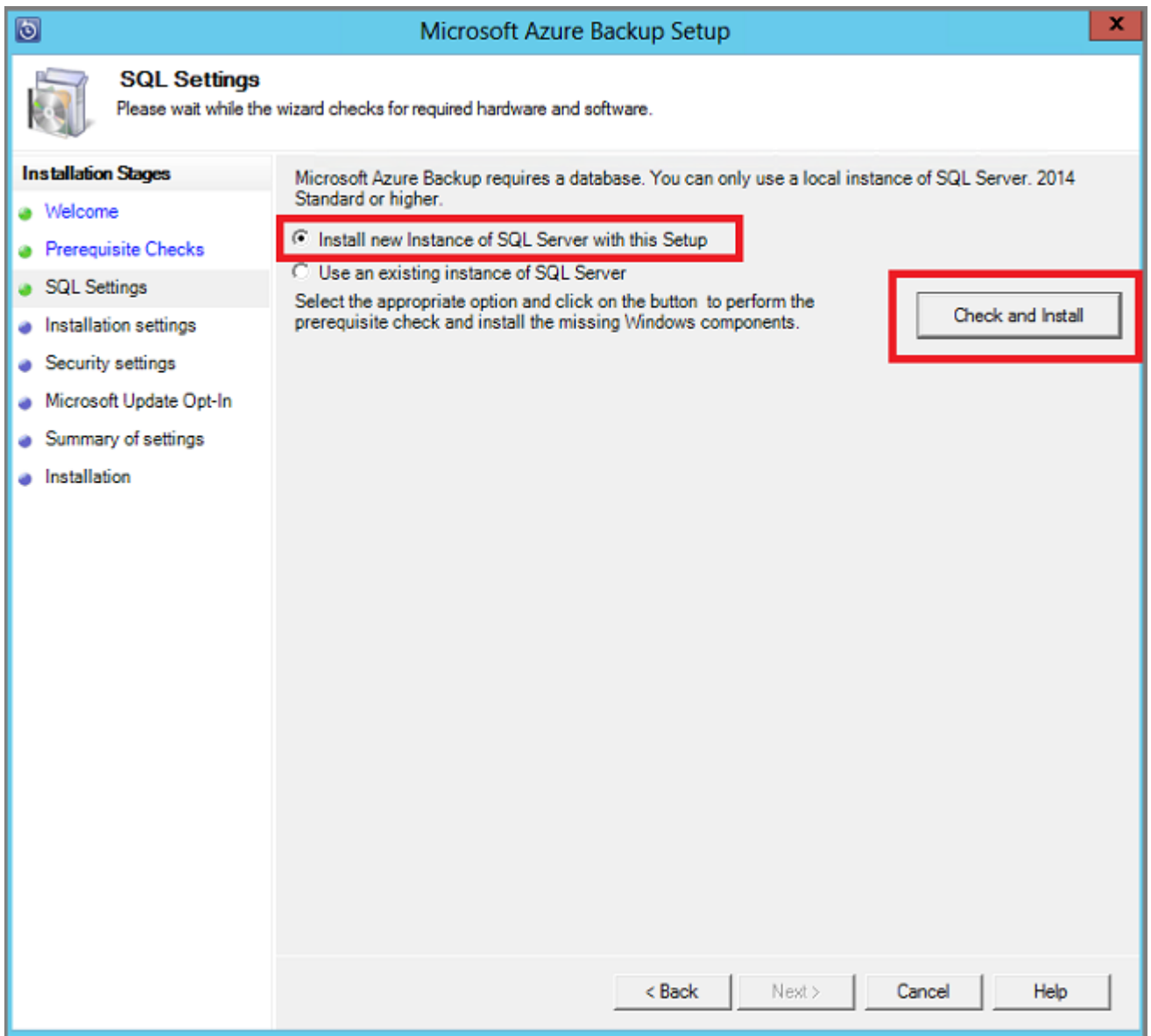
1. Select **Microsoft Azure Backup** to launch the setup wizard.



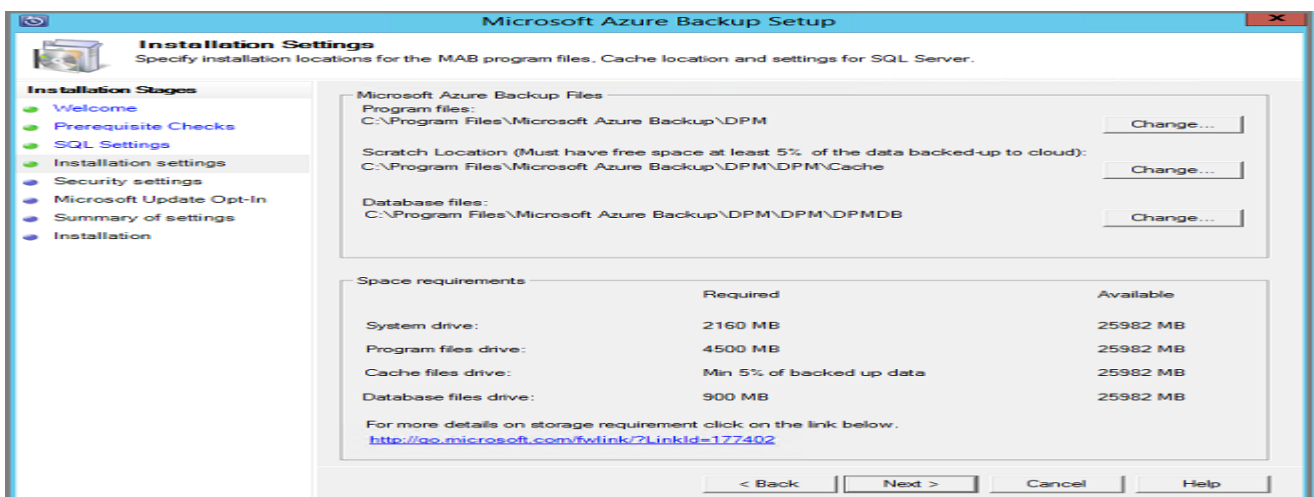
2. On the Welcome screen, select the **Next** button. This takes you to the *Prerequisite Checks* section. On this screen, select **Check** to determine if the hardware and software prerequisites for Azure Backup Server have been met. If all prerequisites are met successfully, you'll see a message indicating that the machine meets the requirements. Select 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 select the **Check and Install** button. Once the prerequisites are successfully installed, select **Next**.



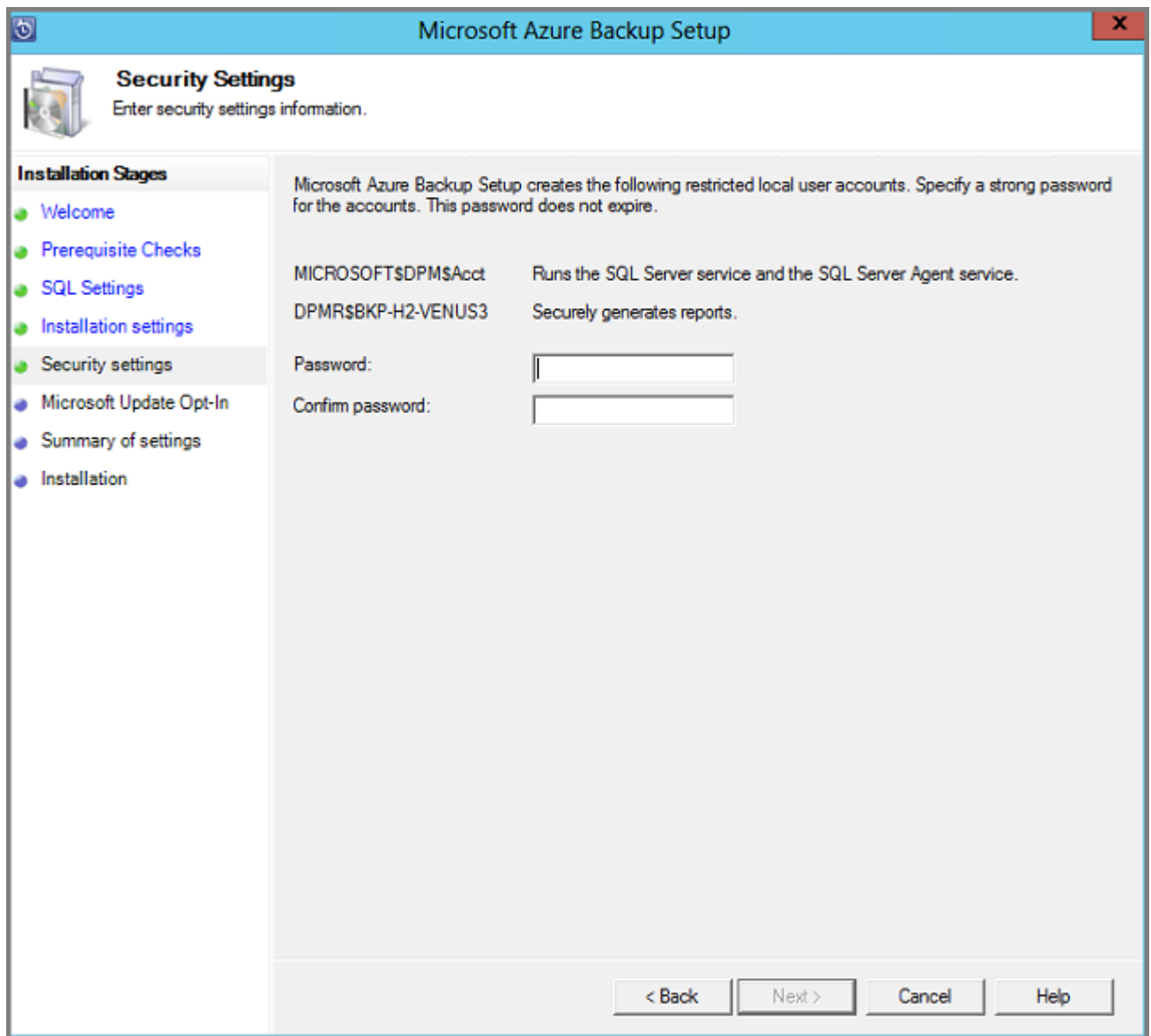
Provide a location for the installation of Microsoft Azure Backup server files and select **Next**.



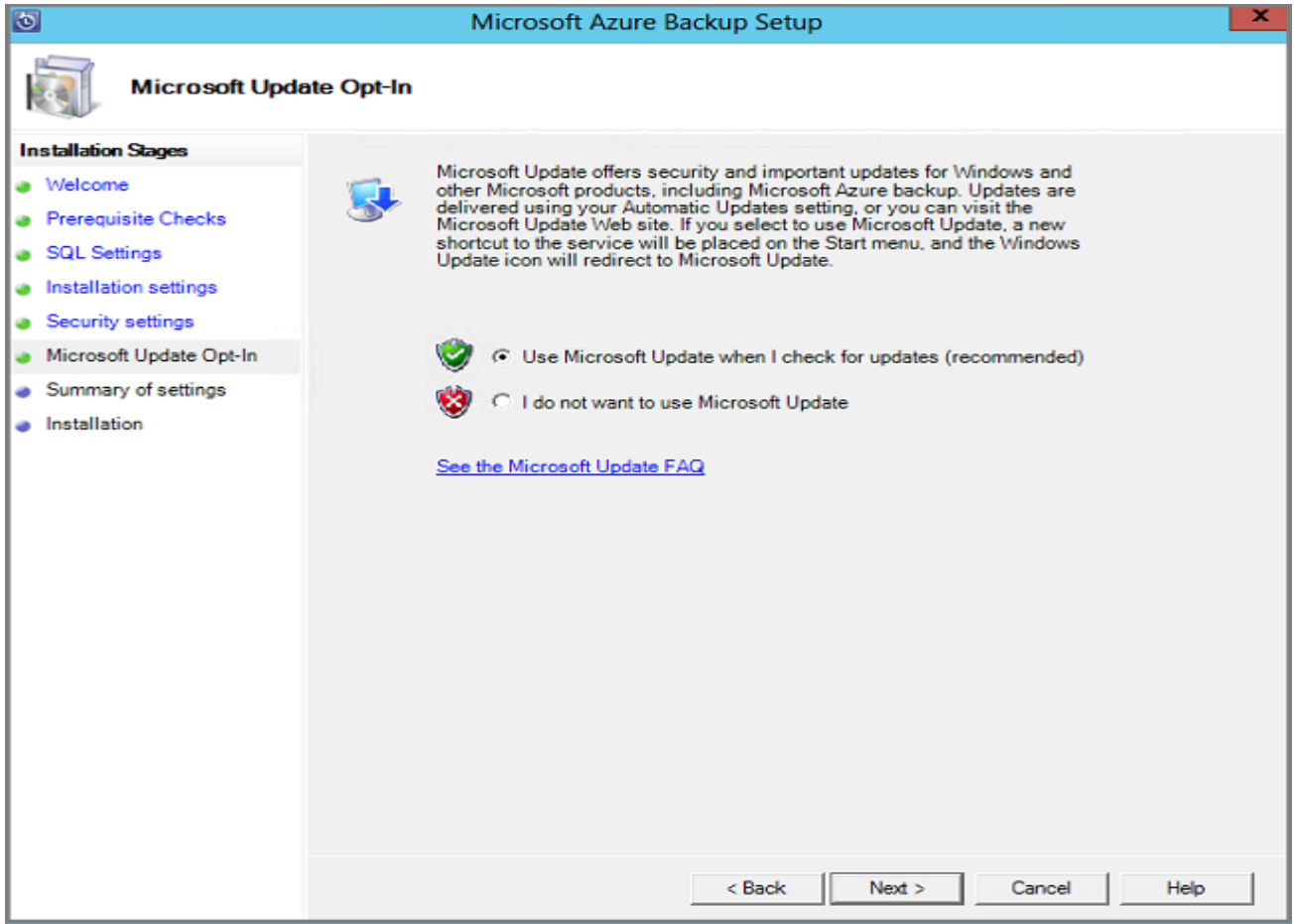
The scratch location is a requirement for back up to Azure. Ensure the scratch location is at least 5% of the data planned to be backed up to the cloud. For disk protection, separate disks need to be configured once the installation completes.

Capacity requirements for disk storage depend primarily on the size of the protected data, the daily recovery point size, expected volume data growth rate, and retention range objectives. We recommend you make the disk storage twice size of the protected data. This assumes a daily recovery point size that's 10% of the protected data size and a 10 days retention range.

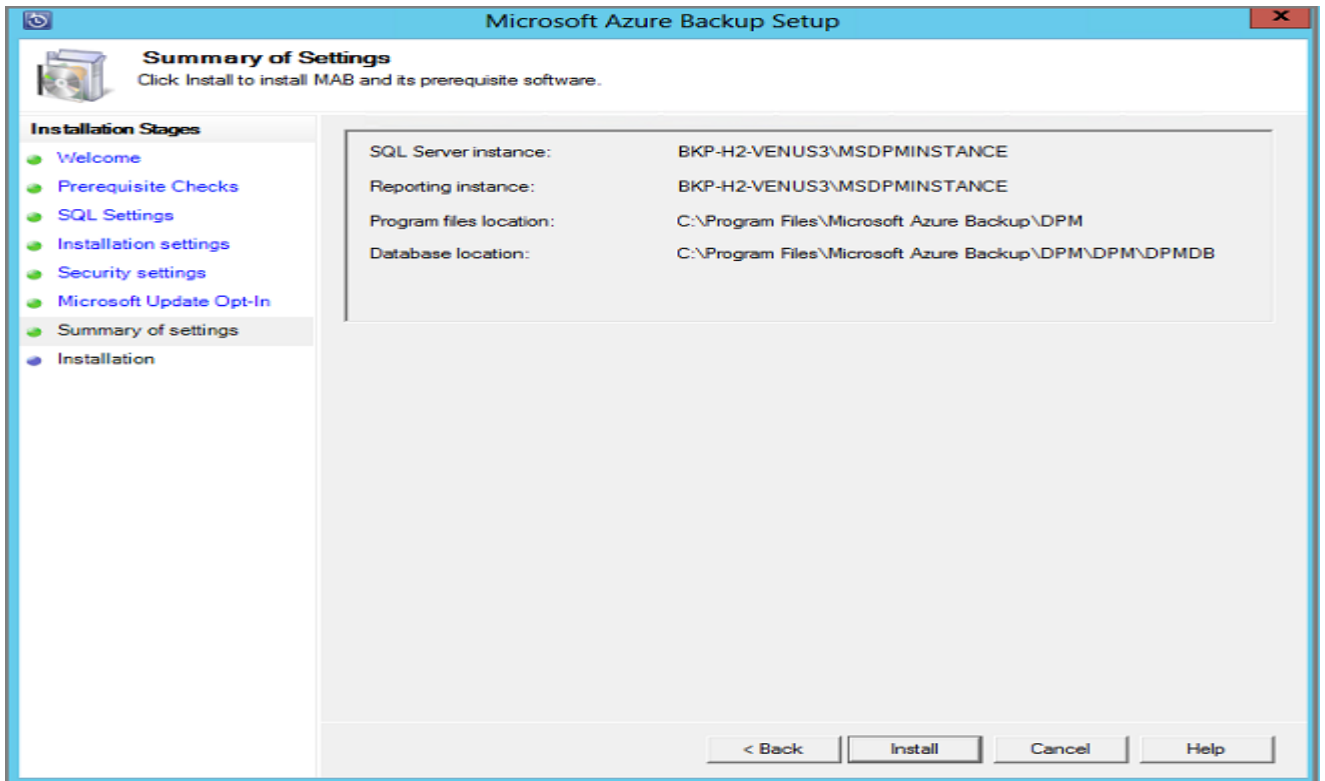
4. Provide a strong password for restricted local user accounts and select **Next**.



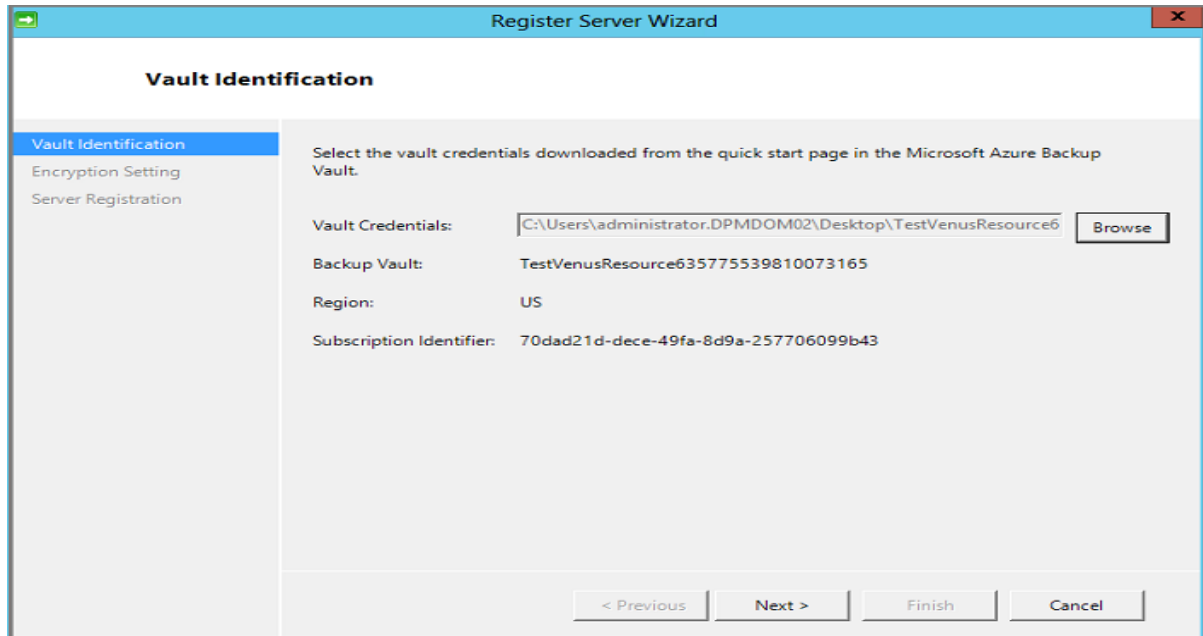
5. Select whether you want to use *Microsoft Update* to check for updates and select **Next**.



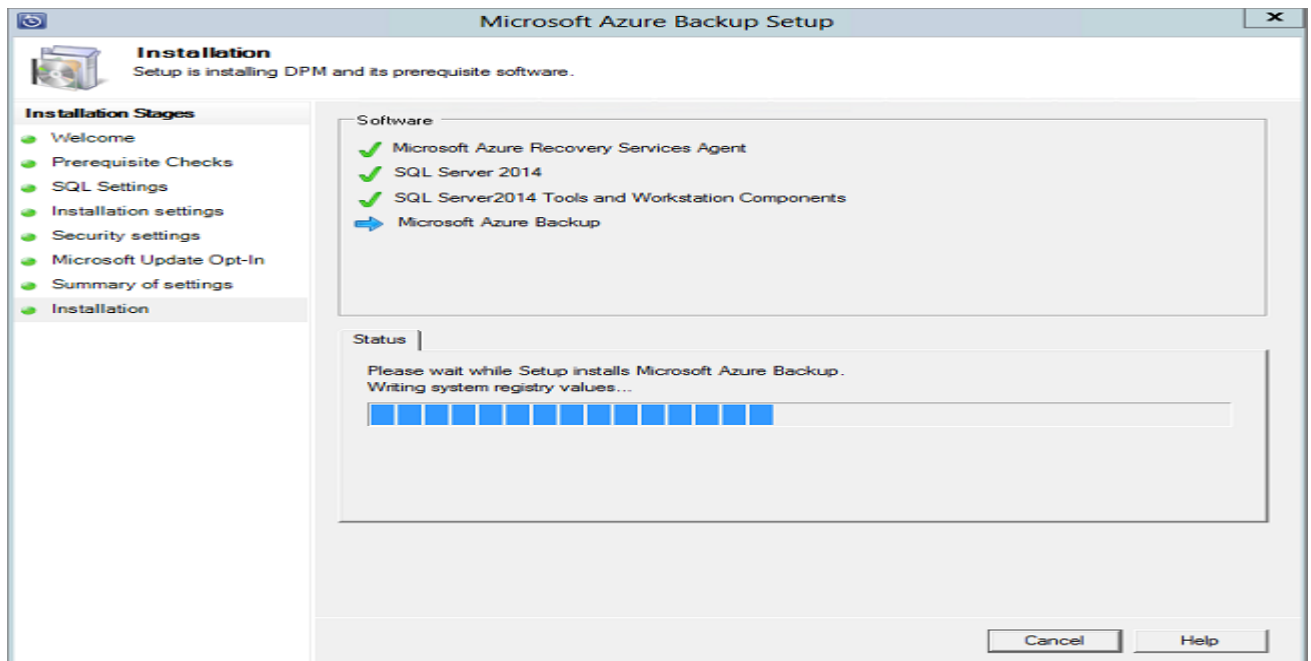
Review the *Summary of Settings* and select **Install**.



The next step is to configure the Microsoft Azure Recovery Services Agent. As a part of the configuration, you'll have to provide your vault credentials to register the machine to the Recovery Services vault. You'll 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.



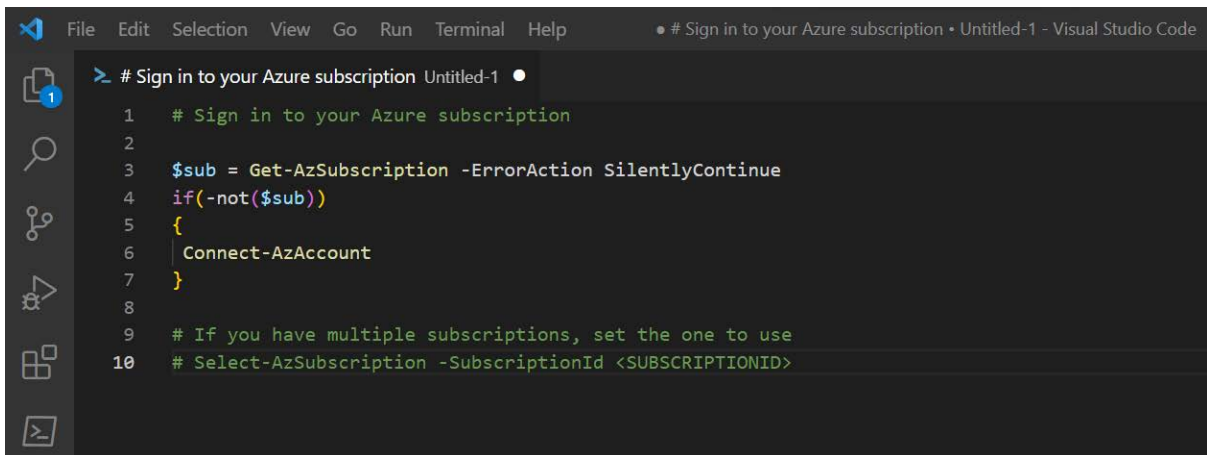
6. Once registration of the Microsoft Azure Backup server successfully completes, the overall setup wizard proceeds to the installation and configuration of SQL Server and the Azure Backup Server components. Once the SQL Server component installation completes, the Azure Backup Server components are installed.



When the installation step has completed, the product's desktop icons will have been created as well. Double-click the icon to launch the product.

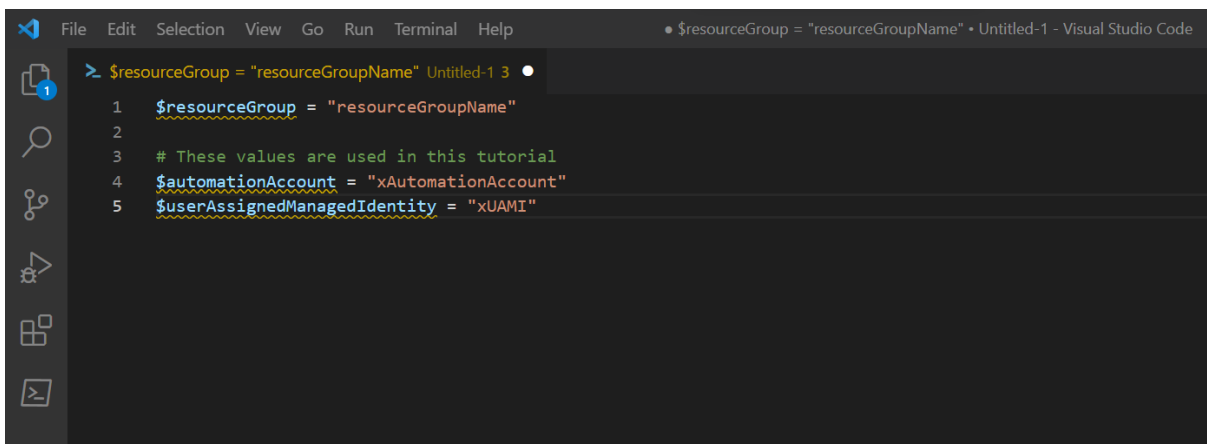
Automatic retry of failed backup jobs

Sign in to Azure interactively using the [Connect-AzAccount](#) cmdlet and follow the instructions-



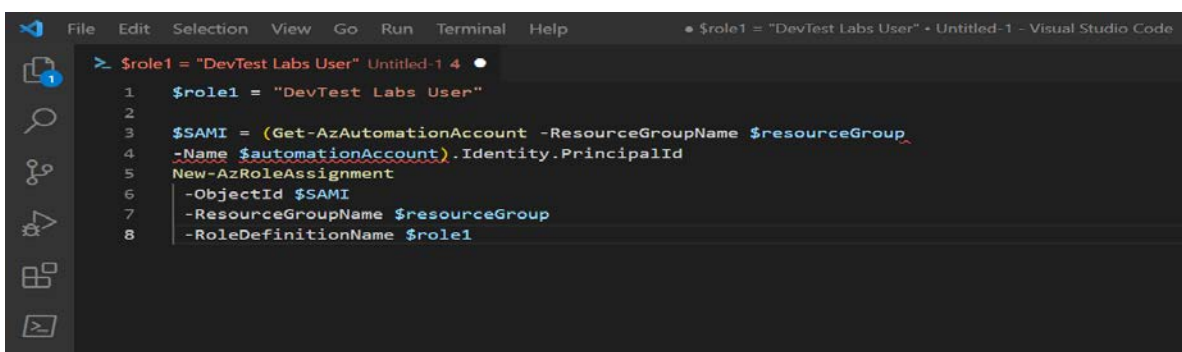
```
File Edit Selection View Go Run Terminal Help • # Sign in to your Azure subscription • Untitled-1 - Visual Studio Code
> # Sign in to your Azure subscription Untitled-1
1 # Sign in to your Azure subscription
2
3 $sub = Get-AzSubscription -ErrorAction SilentlyContinue
4 if(-not($sub))
5 {
6     Connect-AzAccount
7 }
8
9 # If you have multiple subscriptions, set the one to use
10 # Select-AzSubscription -SubscriptionId <SUBSCRIPTIONID>
```

Provide an appropriate value for the following variables and then run the script-



```
File Edit Selection View Go Run Terminal Help • $resourceGroup = "resourceGroupName" • Untitled-1 - Visual Studio Code
> $resourceGroup = "resourceGroupName" Untitled-1 3
1 $resourceGroup = "resourceGroupName"
2
3 # These values are used in this tutorial
4 $automationAccount = "xAutomationAccount"
5 $userAssignedManagedIdentity = "xUAMI"
```

Use the PowerShell cmdlet `New-AzRoleAssignment` to assign a role to the system-assigned managed identity:



```
File Edit Selection View Go Run Terminal Help • $role1 = "DevTest Labs User" • Untitled-1 - Visual Studio Code
> $role1 = "DevTest Labs User" Untitled-1 4
1 $role1 = "DevTest Labs User"
2
3 $$SAMI = (Get-AzAutomationAccount -ResourceGroupName $resourceGroup
4 -Name $automationAccount).Identity.PrincipalId
5 New-AzRoleAssignment
6 -ObjectId $$SAMI
7 -ResourceGroupName $resourceGroup
8 -RoleDefinitionName $role1
```

You need the same role assignment for the user-assigned managed identity:

```
File Edit Selection View Go Run Terminal Help • $UAMI = (Get-AzUserAssignedIdentity -Res • Untitled-1 - Visual Studio Code  
> $UAMI = (Get-AzUserAssignedIdentity -Res Untitled-1 5 •  
1 $UAMI = (Get-AzUserAssignedIdentity -ResourceGroupName  
2 $resourceGroup -Name $userAssignedManagedIdentity).PrincipalId  
3 New-AzRoleAssignment  
4 -ObjectId $UAMI  
5 -ResourceGroupName $resourceGroup  
6 -RoleDefinitionName $role1
```

You'll need extra permissions for the system-assigned managed identity to run the cmdlets: `Get-AzUserAssignedIdentity` and `Get-AzAutomationAccount-`

```
File Edit Selection View Go Run Terminal Help • $role2 = "Reader" • Untitled-1 - Visual Studio Code  
> $role2 = "Reader" Untitled-1 •  
1 $role2 = "Reader"  
2 New-AzRoleAssignment  
3 -ObjectId $SAMI  
4 -ResourceGroupName $resourceGroup  
5 -RoleDefinitionName $role2
```

Create a PowerShell runbook

To create a runbook that managed identities can run, complete the following steps:

1. Sign in to the [Azure portal](#) and navigate to your Automation account.
2. Under **Process Automation**, select **Runbooks**.
3. Select **Create a runbook**:
 1. Name the runbook *miTesting*.
 2. From the **Runbook type** dropdown menu, select **PowerShell**.
 3. Select **Create**.
4. In the runbook editor, paste the following code:

```
$connection = Get-AutomationConnection -Name AzureRunAsConnection  
  
$connectionResult = Connect-AzAccount  
-ServicePrincipal  
-Tenant $connection.TenantID  
-ApplicationId$connection.ApplicationID  
-CertificateThumbprint$connection.CertificateThumbprint
```

- 5.

```

"Login successful.."
$Query = "RecoveryServicesResources
| where type in~ ('microsoft.recoveryservices/vaults/backupjobs')
| extend vaultName = case(type =~
'microsoft.dataprotection/backupVaults/backupJobs',properties.vaultName,type =~
'Microsoft.RecoveryServices/vaults/backupJobs',split(split(id,
'/Microsoft.RecoveryServices/vaults/')[1],'/')[0],'-')
| extend friendlyName = case(type =~
'microsoft.dataprotection/backupVaults/backupJobs',strcat(properties.dataSourceSetName , '/',
properties.dataSourceName),type =~ 'Microsoft.RecoveryServices/vaults/backupJobs',
properties.entityFriendlyName, '-')
| extend dataSourceType = case(type =~
'Microsoft.RecoveryServices/vaults/backupJobs',properties.backupManagementType,type =~
'microsoft.dataprotection/backupVaults/backupJobs',properties.dataSourceType, '-')
| extend protectedItemName = split(split(properties.backupInstanceId, 'protectedItems')[1],'/')[1]
| extend vaultId = toString(split(id, '/backupJobs')[0])
| extend vaultSub = toString( split(id, '/') [2])
| extend jobStatus = case (properties.status == 'Completed' or properties.status ==
'CompletedWithWarnings','Succeeded',properties.status == 'Failed','Failed',properties.status ==
'InProgress', 'Started', properties.status), operation = case(type =~
'microsoft.dataprotection/backupVaults/backupJobs' and tolower(properties.operationCategory) =
'backup' and properties.isUserTriggered == 'true',strcat('adhoc',properties.operationCategory),type
=~ 'microsoft.dataprotection/backupVaults/backupJobs', tolower(properties.operationCategory),
type =~ 'Microsoft.RecoveryServices/vaults/backupJobs' and tolower(properties.operation) =
'backup' and properties.isUserTriggered == 'true',strcat('adhoc',properties.operation),type =~
'Microsoft.RecoveryServices/vaults/backupJobs',tolower(properties.operation), '-'),startTime =
todatetime(properties.startTime),endTime = properties.endTime, duration = properties.duration
| where startTime >= ago(24h)
| where (dataSourceType in~ ('AzureIaaSVM'))
| where jobStatus == 'Failed'
| where operation == 'backup' or operation == 'adhocBackup'
"
| project vaultSub, vaultId, protectedItemName, startTime, endTime, jobStatus, operation
| sort by vaultSub"
$subscriptions = Get-AzSubscription | foreach {$_.SubscriptionId}
$result = Search-AzGraph -Subscription $subscriptions -Query $Query -First 5
$result = $result.data
$prevsub = ""
foreach($jobresponse in $result)
{
    if($jobresponse.vaultSub -ne $prevsub)
    {
        Set-AzContext -SubscriptionId
        $jobresponse.vaultSub
        $prevsub = $jobresponse.vaultSub
    }
    $item = Get-AzRecoveryServicesBackupItem -VaultId
    $jobresponse.vaultId -BackupManagementType AzureVM -WorkloadType AzureVM -Name
    $jobresponse.protectedItemName
    Backup-AzRecoveryServicesBackupItem -ExpiryDateTimeUTC
    (get-date).AddDays(10) -Item $item -VaultId $jobresponse.vaultId
}
}

```

1. Select **Save** and then **Test** pane.

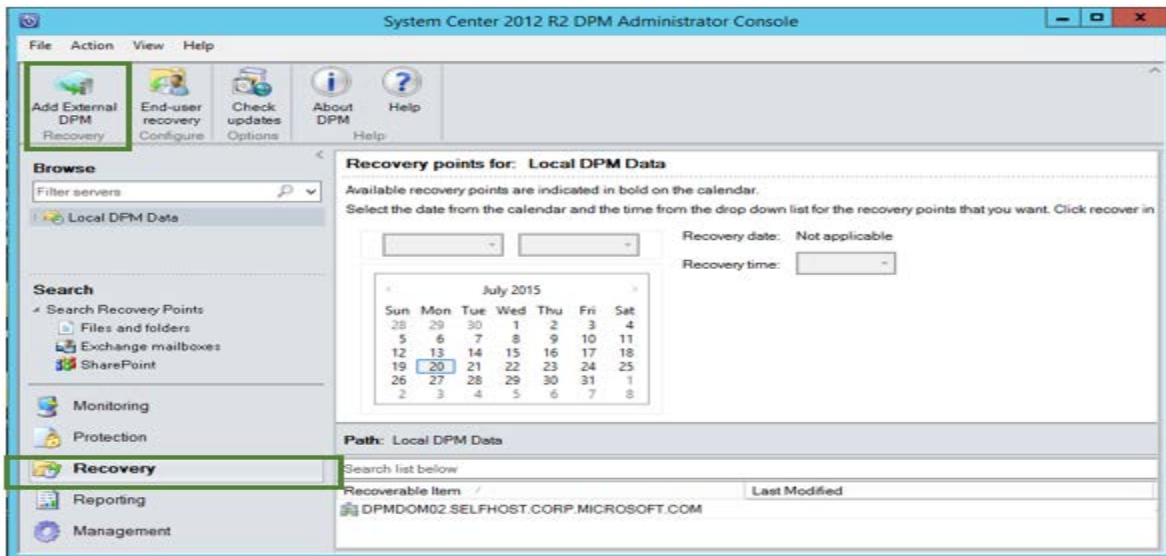
You've now successfully created a PowerShell runbook.

Recover data from Azure Backup Server

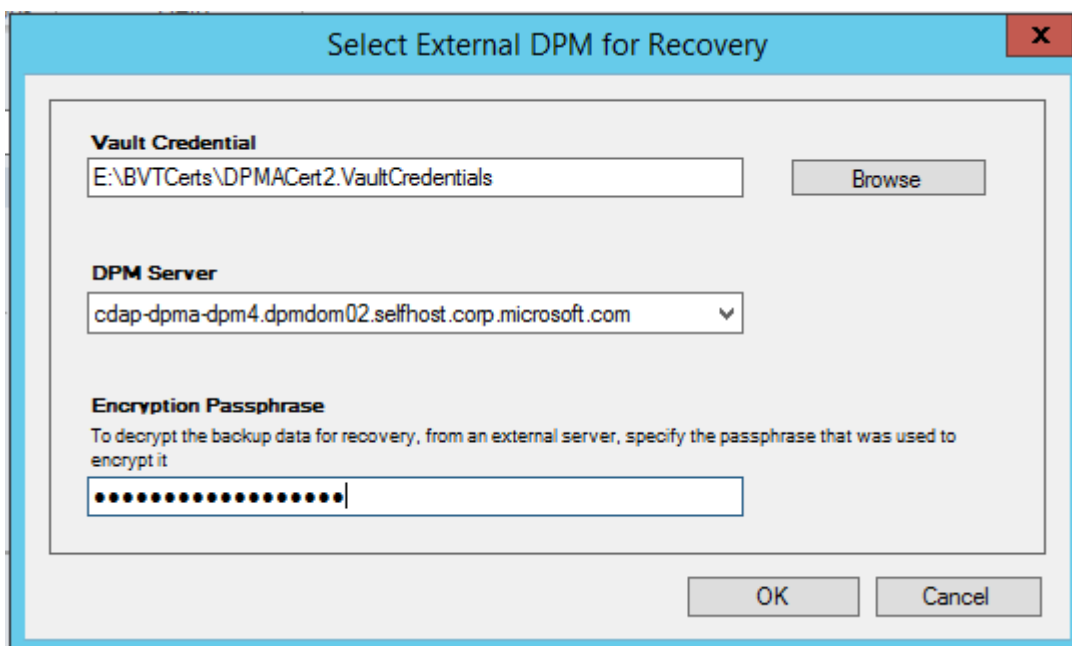
You can use Azure Backup Server to recover the data you've backed up to a Recovery Services vault. The process for doing so is integrated into the Azure Backup Server management console, and is similar to the recovery workflow for other Azure Backup components.

To recover data from an Azure Backup Server:

1. From the **Recovery** tab of the Azure Backup Server management console, select '**Add External DPM**' (at the top left of the screen).

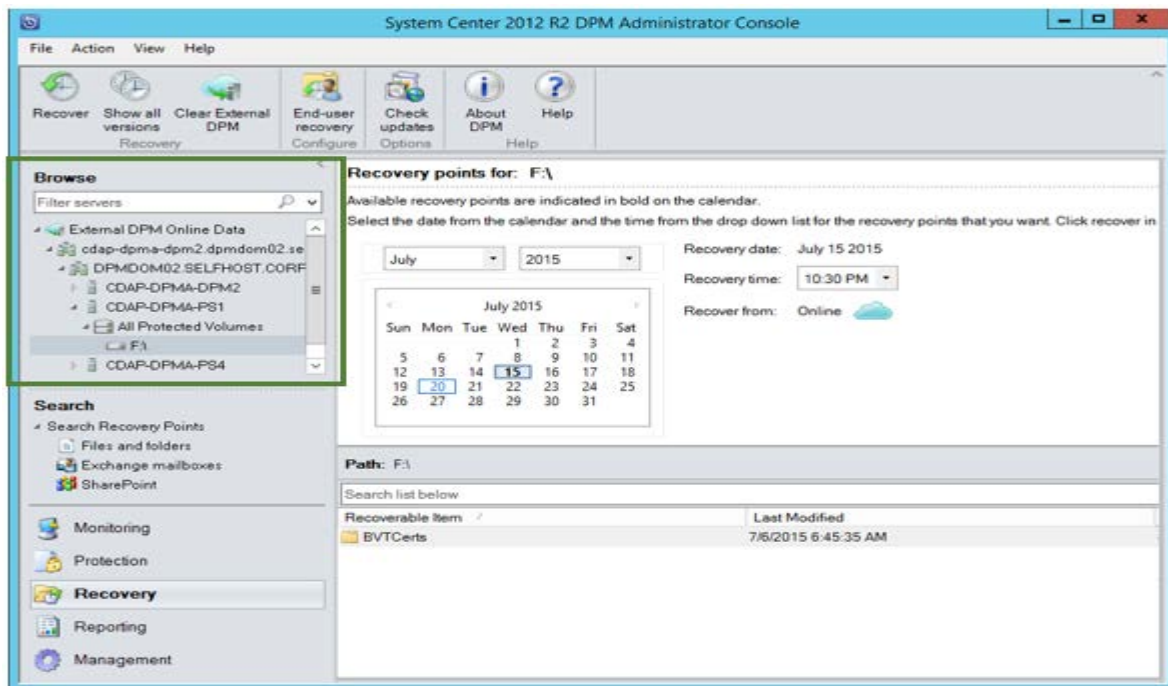


Download new **vault credentials** from the vault associated with the **Azure Backup Server** where the data is being recovered, choose the Azure Backup Server from the list of Azure Backup Servers registered with the Recovery Services vault, and provide the **encryption passphrase** associated with the server whose data is being recovered.



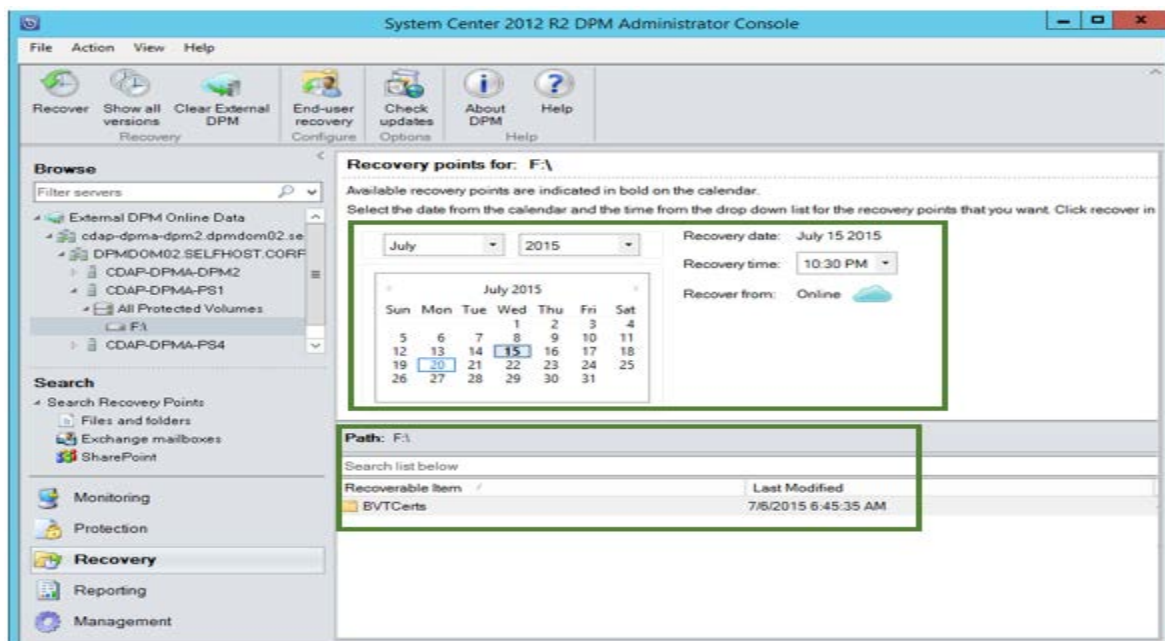
1. Once the External Azure Backup Server is successfully added, you can browse the data of the external server and the local Azure Backup Server from the **Recovery** tab.

2. Browse the available list of production servers protected by the external Azure Backup Server and select the appropriate data source.

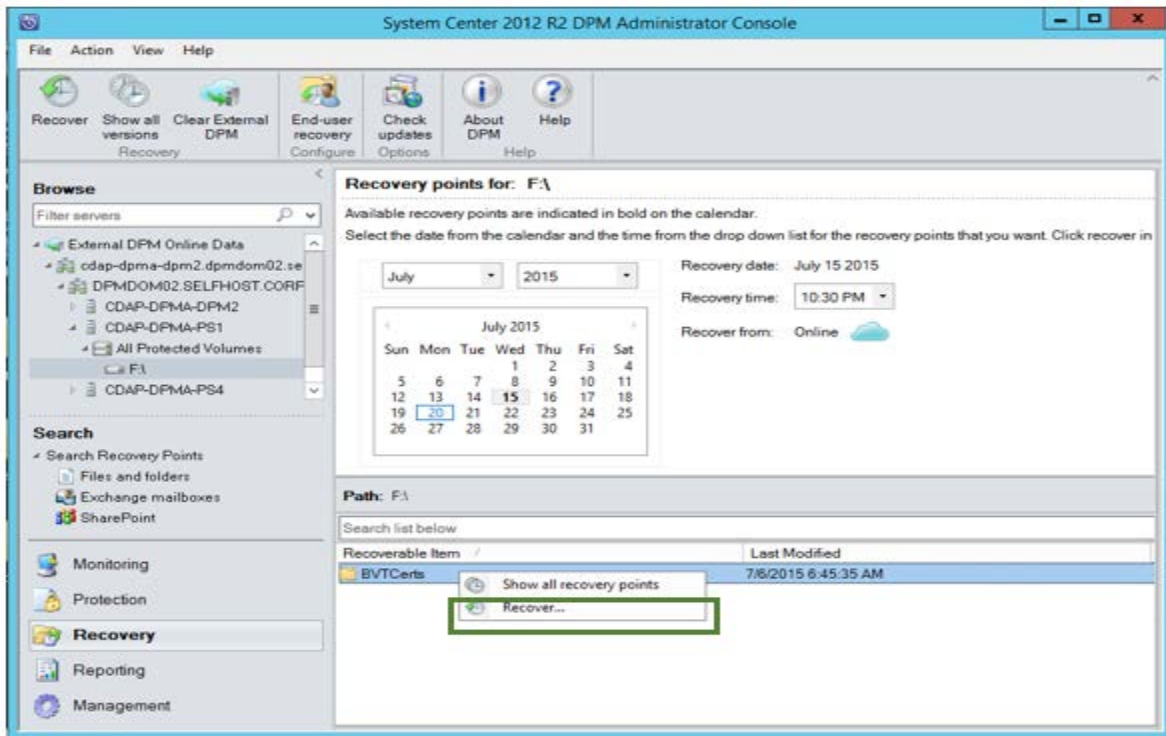


Select the **month and year** from the **Recovery points** drop down, select the required **Recovery date** for when the recovery point was created, and select the **Recovery time**.

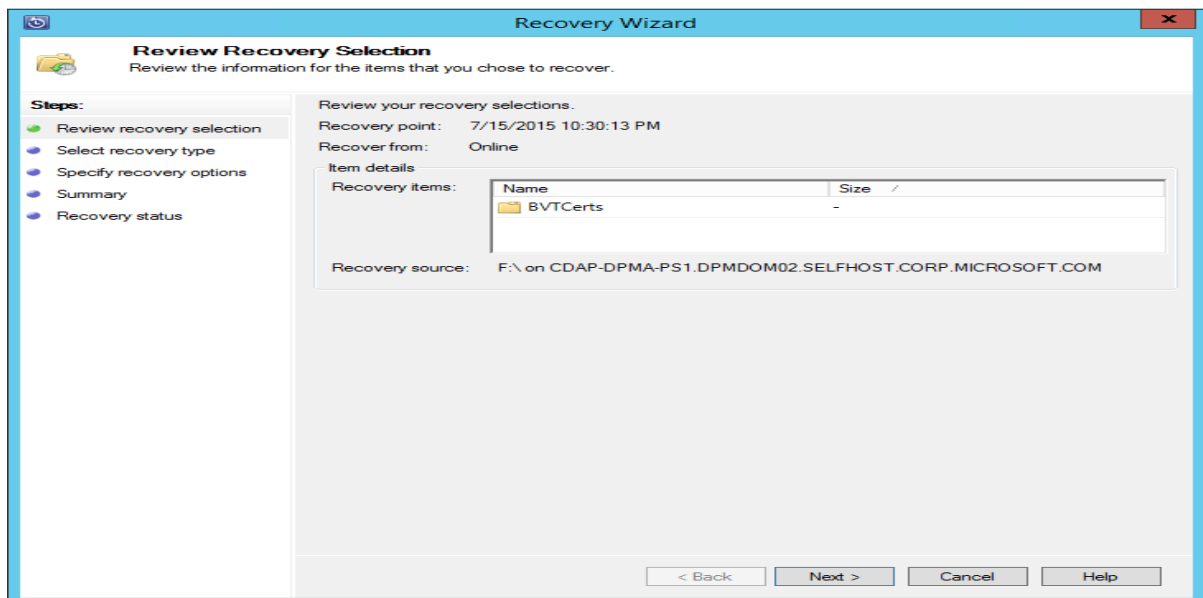
A list of files and folders appears in the bottom pane, which can be browsed and recovered to any location.



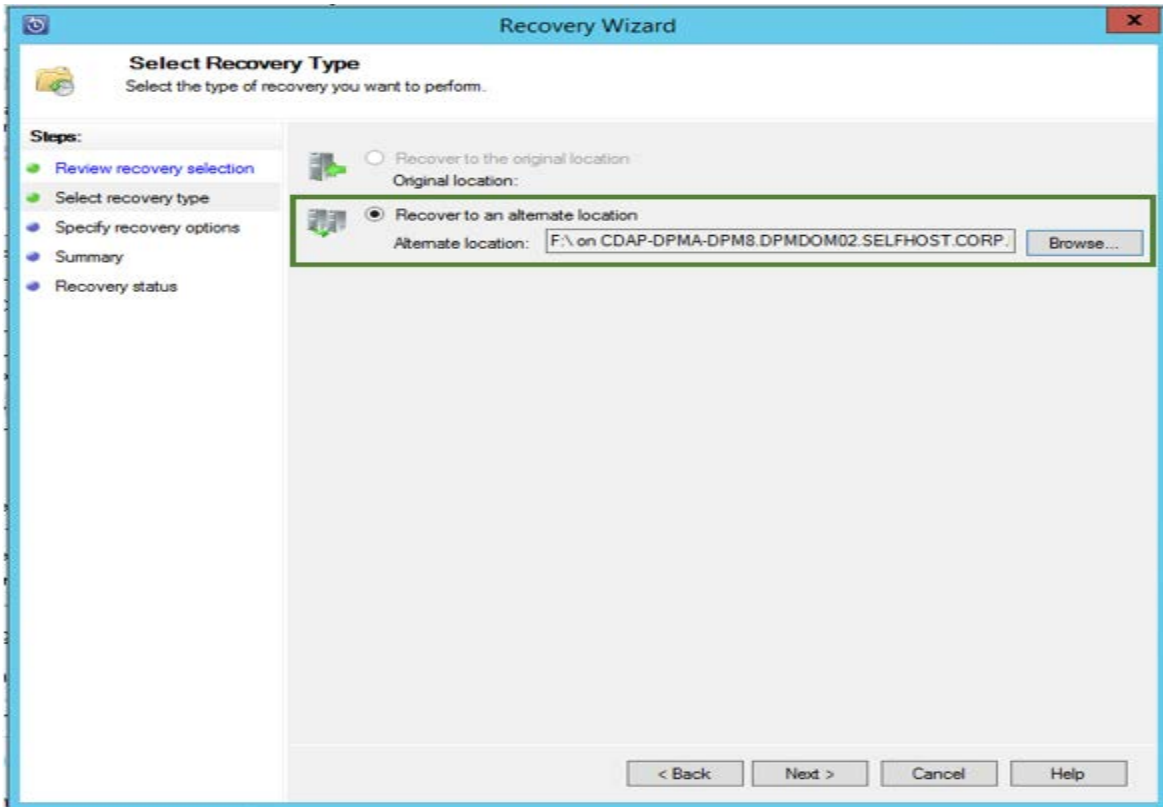
Right-click the appropriate item and select **Recover**.



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, select **Cancel** to navigate back to recovery tab to select appropriate recovery point. If the selection is correct, select **Next**.

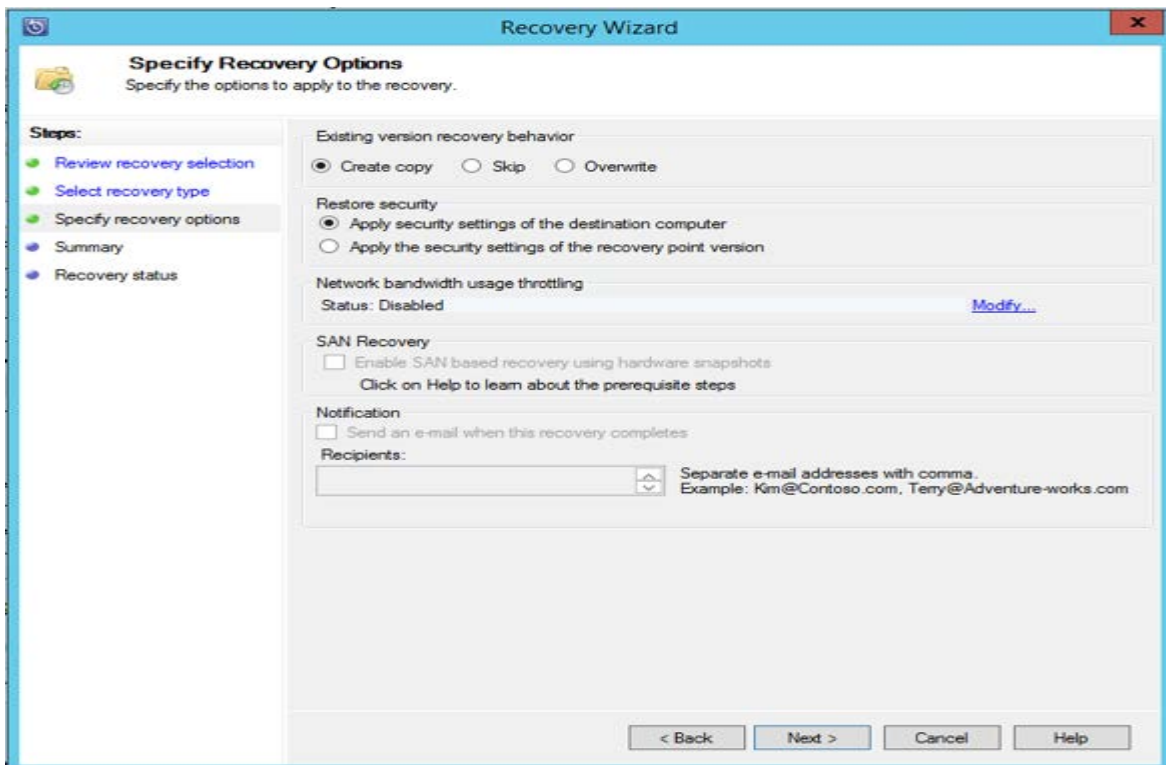


Select **Recover to an alternate location**. **Browse** to the correct location for the recovery.

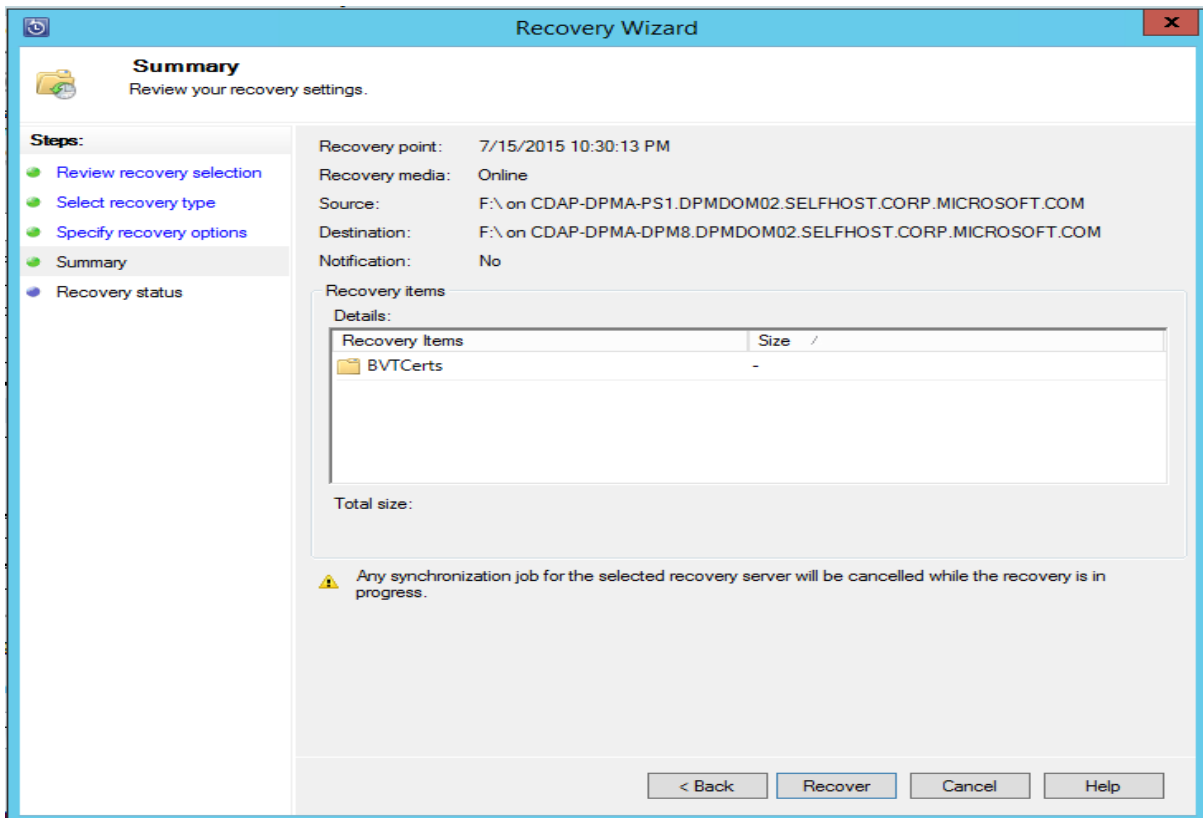


Choose the appropriate option to **Restore security**. You can apply the security settings of the destination computer where the data is being recovered or the security settings that were applicable to product at the time the recovery point was created.

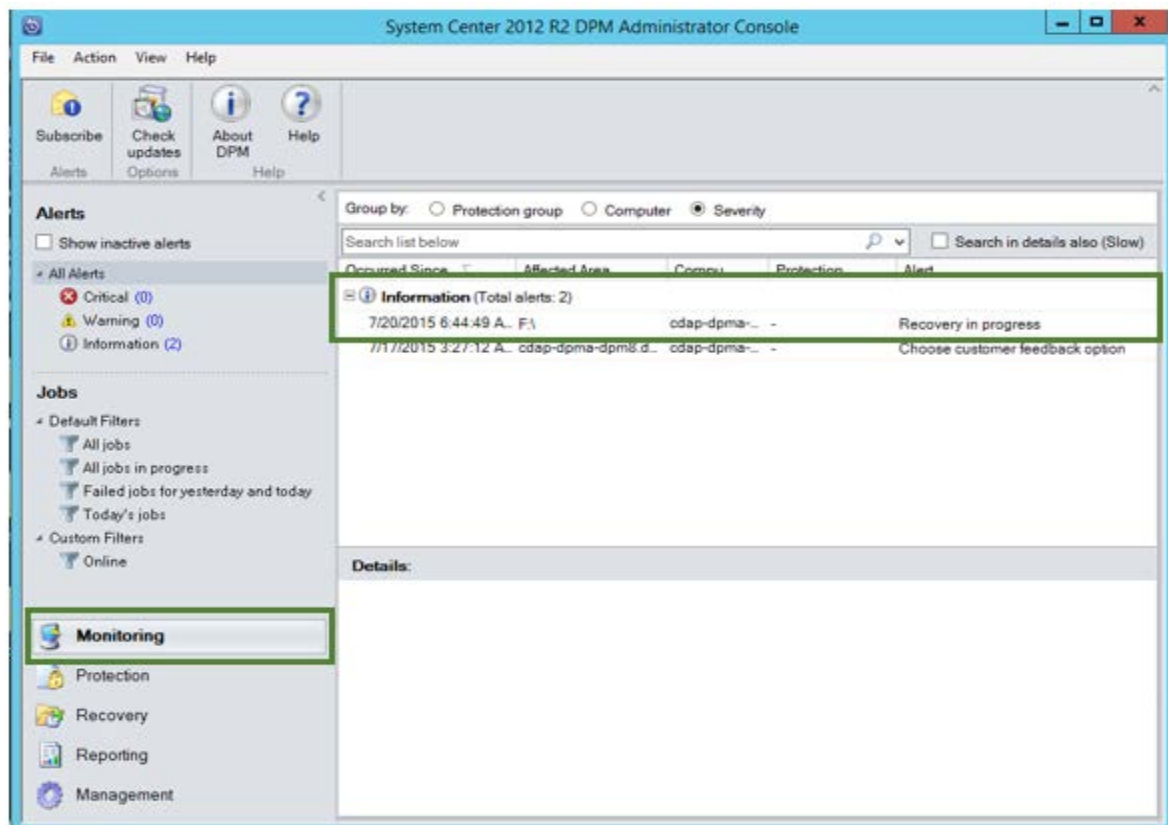
Identify whether a **Notification** is sent, once the recovery successfully completes.



The **Summary** screen lists the options chosen so far. Once you select **Recover**, the data is recovered to the appropriate on-premises location.



The recovery job can be monitored in the **Monitoring** tab of the Azure Backup Server.



Challenges Faced-

The overall implementation itself was tricky to implement due to the multiple components involved. Integrating and configuring the on prem VM with the MABS client and doing POC for same was challenging and fun!

Secondly, Configuring the backup schedule and triggering the back up for different protection group was the most difficult part to implement since there were a lot of analysis/testing done to segregate the vms as per their size and then schedule a back up to avoid Network Choke.

Business Benefits-

For businesses and organizations across industries, on prem data backups are vital. You must make sure that even in the event something happens to your sometimes confidential data, you can quickly restore it to prevent significant hurdles to continuing your normal operations. If no backup solution is in place, even getting back to regular business ops can be both costly and time intensive. Below are few Business Benefits of using MABS-

1. **Flexible Pricing**
2. **Scalability**
3. **Data Security**
4. **Backup Variations**
5. **Unlimited Data Transfer**
6. **Restore Flexibility**
7. **Cost Effective**

DOCUMENTED BY –

OMKAR SAWANT

SENIOR MICROSOFT AZURE CLOUD ENGINEER.