Microsoft Azure - Starter Kits for Partners

Hands on Lab

Archiving and Backup

Last Update: September 2015





**MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.**

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The descriptions of other companies’ products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

© 2015 Microsoft Corporation. All rights reserved. Any use or distribution of these materials without express authorization of Microsoft Corp. is strictly prohibited.

Microsoft and Windows are either registered trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

[Overview 4](#_Toc404666055)

[Objectives 4](#_Toc404666056)

[Prerequisites 5](#_Toc404666057)

[Scenarios 6](#_Toc404666058)

[Microsoft Azure Backup Vaults 7](#_Toc404666059)

[Register Server and Backup 12](#_Toc404666060)

[System Center Data Protection Manager 15](#_Toc404666061)

[Summary 22](#_Toc404666062)

[Additional References: 22](#_Toc404666063)

## Overview

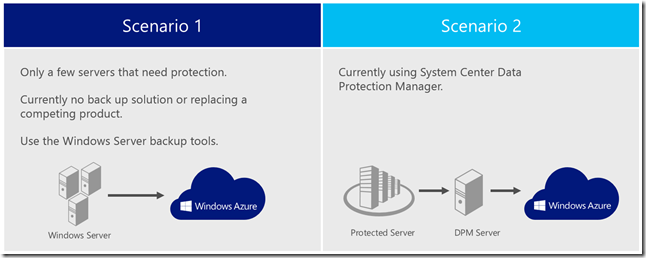
This document covers the required steps to enable Microsoft Azure Backup Service, with and without System Center 2012 R2 – Data Protection Manager Integration. This document was designed to assist the consultant responsible for delivering this solution.

## Objectives

In this hands-on lab, you will learn:

* The prerequisites for Microsoft Azure Backup
* The configuration steps for the most common protection scenarios
  + Protect a few servers with Windows Server Backup tools
  + Protect your server infrastructure with System Center Data Protection Manager

The Hands On covers the following scenarios:



**Note:** Due to constant changes in the Azure Portal this document may not reflect the most recent updates. We suggest that you consult the following online links that provide the most up-to-date steps to install and deploy a Azure Backup Vault. It includes steps to deploy:

**Scenario 1:** Configure Azure Backup to prepare for back up of Windows Server

[https://azure.microsoft.com/en-us/documentation/articles/backup-configure-vault](https://azure.microsoft.com/en-us/documentation/articles/backup-configure-vault/)/

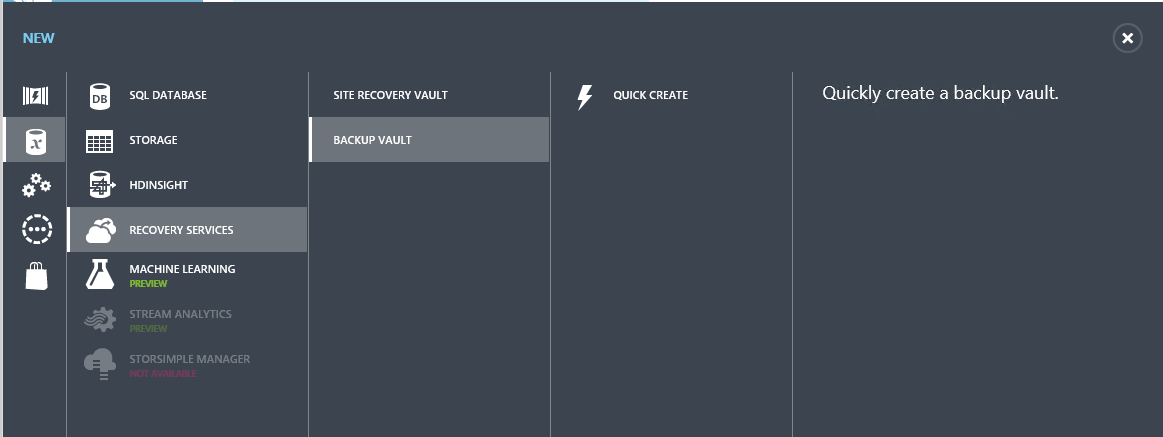
**Scenario 2:** Introduction to Azure DPM Backup

<http://azure.microsoft.com/en-us/documentation/articles/backup-azure-dpm-introduction>

### Prerequisites

The following prerequisites are required in the environment:

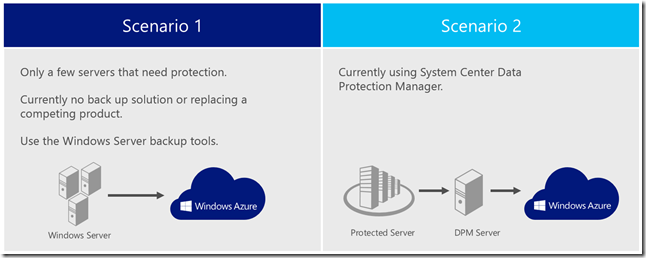
* Access to the System Center 2012 R2 – Data Protection Manager Software.
* Microsoft Azure storage subscription and management credentials.
* X.509 v3 certificate (See below for details)
* Access to the Microsoft Azure Backup feature within Microsoft Azure. You can verify if you have access by looking in Recovery Services and seeing “Backup Vault”:



## Scenarios

A cloud-based protection solution with Microsoft Azure Backupprovides an alternative to backing up System Center 2012 - Data Protection Manager (DPM) to disk or to a secondary on premise DPM server, from System Center 2012 DPM onwards you can back up DPM servers and data protected by those servers to the cloud, using Microsoft Azure Backup.

The fundamental workflow that you experience when you backup and restore files and folders to and from Microsoft Azure Backup are the same workflows that you would experience using any other type of backup, you identify the items to backup and then the items are copied to a storage where they can be used later if they are needed. Microsoft Azure Backup delivers business continuity benefits by providing a backup solution that requires no initial hardware costs other than a broadband Internet connection.



Microsoft Azure Backup can help you protect important server data offsite with automated backups to Microsoft Azure, where they are available for easy data restoration. You can manage cloud backups from the familiar backup tools in Windows Server 2012, Windows Server 2012 Essentials, or System Center 2012 - Data Protection Manager. These tools provide similar experiences for configuring, monitoring, and recovering backups, whether to a local disk or to Microsoft Azure storage. After data is backed up to the cloud, authorized users can easily recover backups to any server.

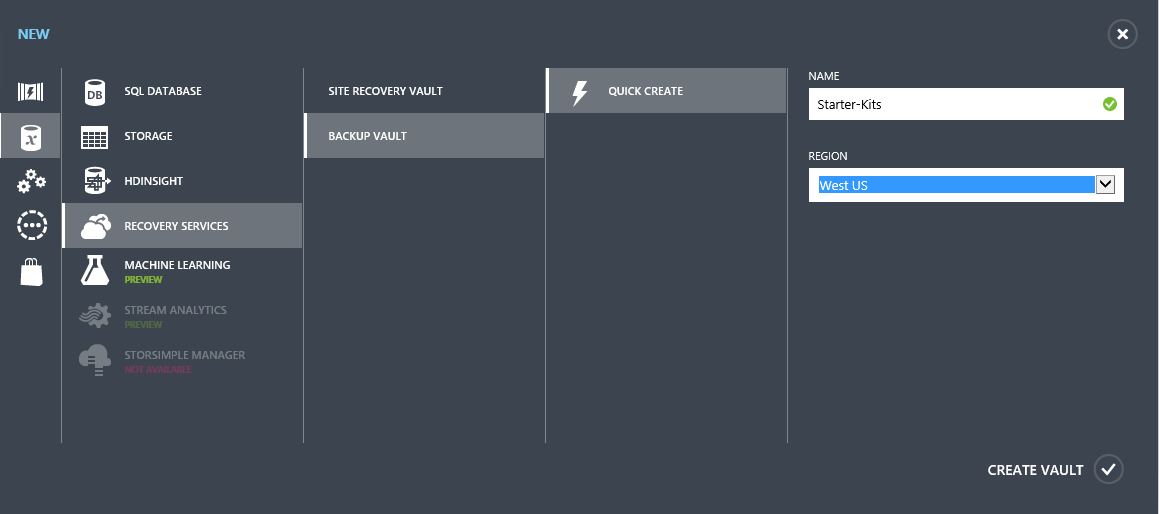
### Microsoft Azure Backup Vaults

To backup files and data from your Windows Server to Microsoft Azure, you must create a backup vault in the geographic region where you want to store the data. This document will walk you through the creation of the vault you will use to store backups, the uploading of a certificate to the vault, the installation of a backup agent, and an overview of the backup management tasks available through the management portal.

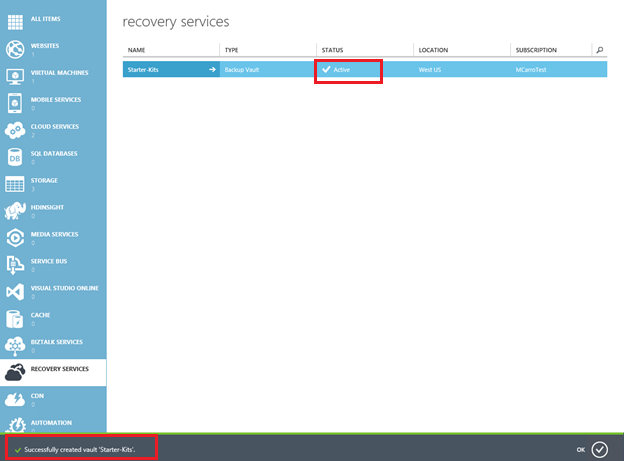
You can find a video outlining these steps at <http://www.youtube.com/watch?v=c-6CxFDGvIk>

#### Create a backup vault

1. Sign in to the [Management Portal](https://manage.windowsazure.com/).
2. Click **Recovery Services**, then click **Create New**, point to **Backup Vault**, and then click **Quick Create**.

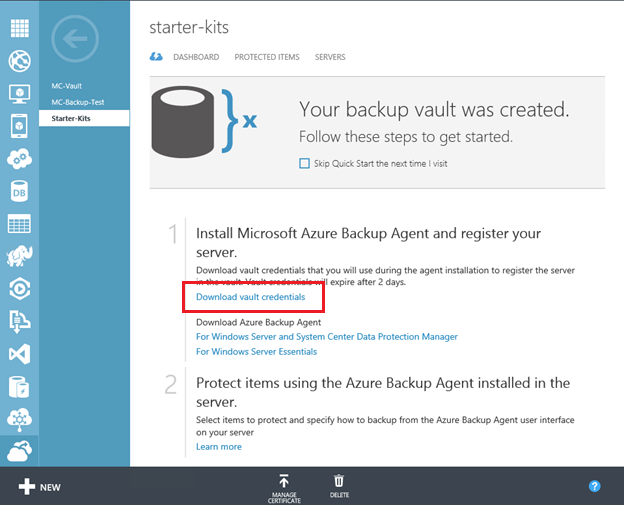


1. In **Name**, enter a friendly name to identify the backup vault.
2. In **Region**, select the geographic region for the backup vault.
3. Click **Create Backup vault**. It can take a while to create the backup vault. To check the status, you can monitor the notifications at the bottom of the portal. After the backup vault has been created, a message will tell you that the vault has been successfully created and it will be listed in the resources for Recovery Services as **Online**.

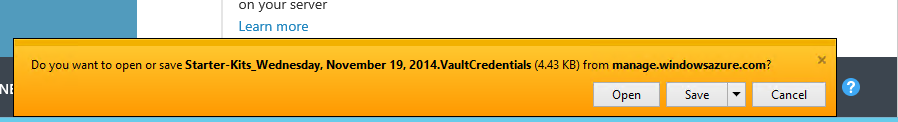


#### Download vault credentials

1. Sign in to the [Management Portal](https://manage.windowsazure.com/).
2. Click **Recovery Services**, then click the name of backup vault to use, then click on “Download vault credentials”.



Then, select where to save the .Vault Credentials file on the server.



#### Download a Backup Agent

1. Sign in to the [Management Portal](https://manage.windowsazure.com/).
2. Click **Recovery Services**, and then click the name of backup vault to view the vault dashboard.
3. Click **Download Azure Backup Agent For Windows Server and System Center Data Protection Manager**



1. You will be redirected to the Microsoft Download Center to download the agent software. Note of the location where you downloaded the MARSAgentInstaller.exe file.
2. Note:

* Using Microsoft Azure Backup does not require that you install Windows Server Backup. However, the two backup methods complement each other. Windows Server Backup can perform tasks such as bare metal and system state restores, which are not available by using Microsoft Azure Backup.

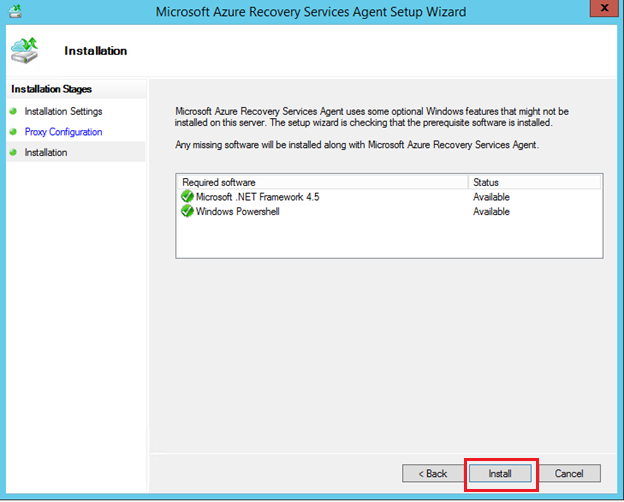
#### 

#### Installing the Microsoft Azure Recovery Services Agent

1. Sign in to your server using a local computer administrator account, and then run **MARSAgentInstaller.exe**.
2. The **Installation Settings** page will be displayed. On this page, you choose the **Installation Folder** and **Cache Location** for Microsoft Azure Backup. By default, the installation folder will be **<system drive>:\Program Files\Microsoft Azure Recovery Services Agent**. If you click **Browse,** you can navigate and choose a new location in which to create the **Microsoft Azure Backup** folder.

* By default, the cache location folder will be **<system drive>:\Program Files\Microsoft Azure Recovery Services Agent\Scratch**. The cache location must have at least 2.5 GB of free space. Only local system administrators and members of the Administrators group have access to the cache directory to prevent denial-of-service attacks. Click **”Next”** when you have identified the folders that you want the Microsoft Azure Recovery Services Agent to use.

1. On the **Proxy Configuration** page, you will get a check mark if your proxy settings are the default. You can customize if you need a proxy to get access to the internet. Click “**Next”** for the next step.
2. On the **Installation** page, you obtain a list of the software that will be installed as part of the Microsoft Azure Recovery Services Agent. Click **Install** to proceed.



1. The **Installation** page is displayed. A progress indicator displays when the installation begins and shows the progress of the installation. When the installation is complete, you will receive a message that the Microsoft Azure Recovery Services Agent has been installed successfully. At this point, you can choose to Proceed to Registration of your server or Close the Wizard. Click on **Close**.

Now, you can start the Microsoft Azure Backup management console from the Apps menu, the desktop icon, or within the Windows Server Backup MMC snap-in. Windows PowerShell cmdlets for Microsoft Azure Backup have also been installed, so you can begin using Windows PowerShell to work with Microsoft Azure Backup.

1. Note

* If you install the Microsoft Azure Backup Agent on a DPM Server, an icon will not appear. You will see the message “Next Step: Please use the DPM Administrator Console to register your DPM server with Microsoft Azure Backup and set your configurations.”

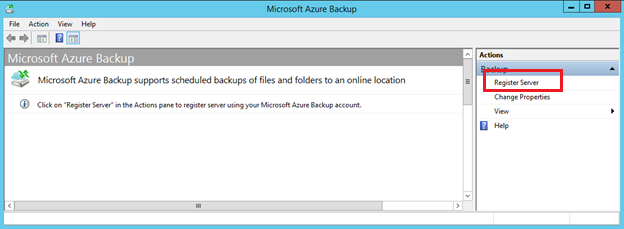
### 

### Register Server and Backup

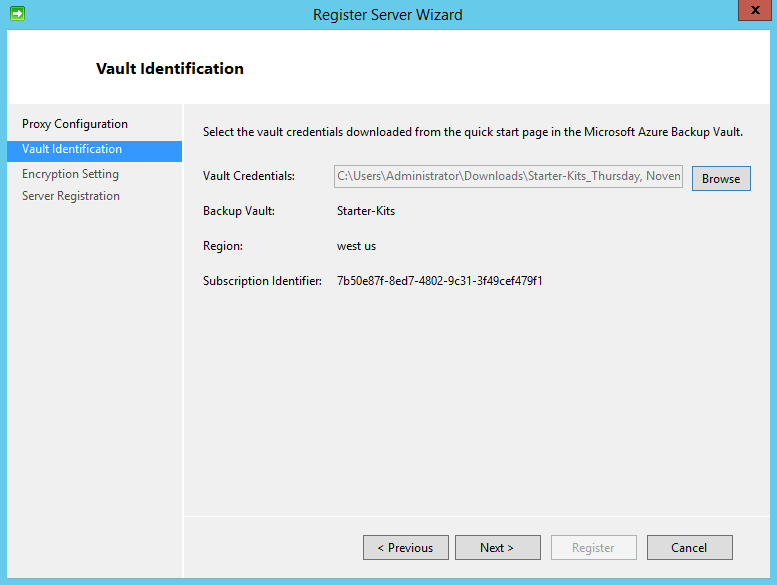
1. Sign in to your server using a local computer administrator account, and double click the Microsoft Azure Backup icon.



1. At the Microsoft Azure Backup screen, click on Register Server at the menu on the right.

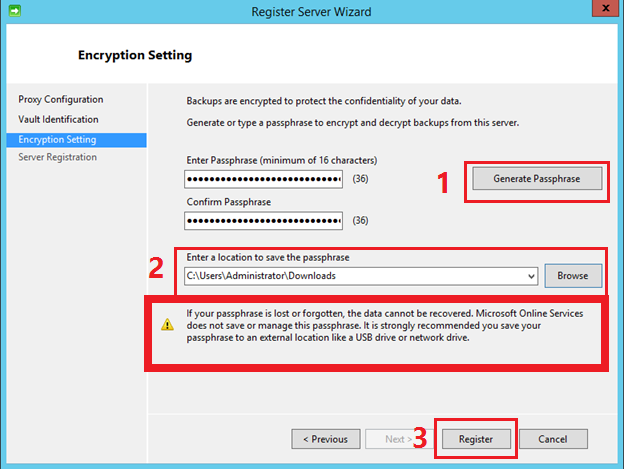


1. You get the screen of the Register Server Wizard, on the Proxy Configuration screen, capture the information for your Proxy server, If you do not need one, click **Next**.
2. You get the screen of Vault Identification. Click on Browse and look for the file you downloaded previously. Then, click “**Next”**.

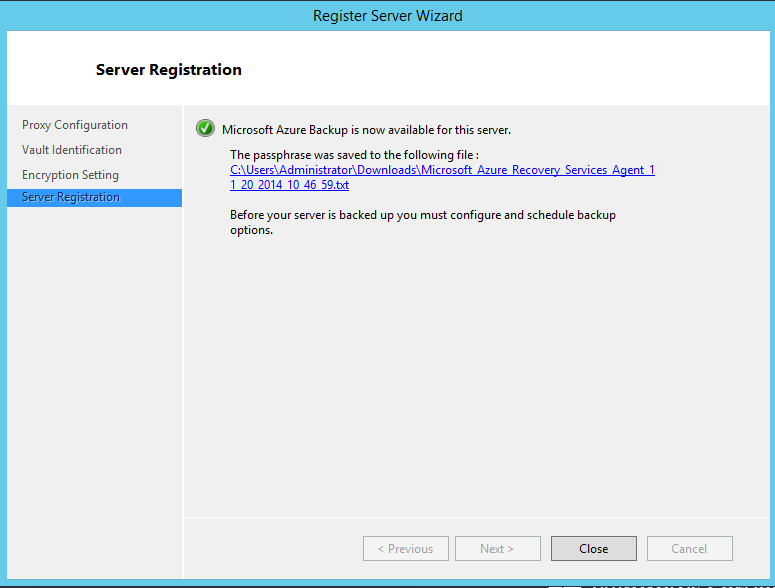


1. You get the **Encryption Setting** screen, capture your own Paraphrase or click on “Generate Paraphrase”. Click on “Browse” and select where to save your passphrase file. Then, click “**Register**”.
2. Note

* If your passphrase is lost or forgotten, the data cannot be recovered. Microsoft Online Services does not save or manage this passphrase. It is strongly recommended you save your passphrase to an external location like a USB drive or network drive.



1. Once your server is registered, your server is ready to be backed up to Microsoft Azure. You get an screen specifying the location of your passphrase file. Click Close.



### System Center Data Protection Manager

As an alternative to backing up System Center – Data Protection Manager (DPM) to disk or to a secondary on premise server, in DPM in System Center 2012 R2 you can back up DPM servers and data protected by those servers to the cloud, using Microsoft Azure Backup.

This provides the following benefits:

* Reduced costs—The Microsoft Azure Backup service can help to reduce the total cost of ownership (TCO) for customers by providing scalability, elasticity, and simplified storage management.
* Peace of mind—The Microsoft Azure Backup service provides a reliable, secure, and a robust short-term offsite backup and restore solution that is highly available.
* Simplicity—The Microsoft Azure Backup workflows are seamlessly integrated into the existing DPM backup, recovery and monitoring workflows.

#### Prerequisites for DPM backup

The following scenarios are supported when protecting data using backup vaults in Microsoft Azure Backup:

* Protection for file system
* Protection for virtual machines
* Protection for SQL Server databases
* Supported file types include:
  + Encrypted (Full backups only)
  + Compressed (Incremental backups supported)
  + Sparse (Incremental backups supported)
  + Compressed and sparse (Treated as Sparse)

The following scenarios are not supported when protecting data using Microsoft Azure Backup.

* DPM servers on case-sensitive file systems are not supported.
* Unsupported file types include:
  + Hard links (Skipped)
  + Reparse points (Skipped)
  + Encrypted and compressed (Skipped)
  + Encrypted and sparse (Skipped)
  + Compressed stream
  + Sparse stream

There are a number of deployment prerequisites required to deploy Microsoft Azure Backup for DPM:

* A server installed with Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2 with SP1, and running DPM in System Center 2012 SP1 or System Center 2012 R2.
* You must have a Microsoft Azure account that has the Microsoft Azure Backup feature enabled.
  + Charges are according to the amount of data stored in Microsoft Azure.
  + Up to 5 GB storage per month is free of charge.
  + Information about storage charges after 5 GB per month are available at Backup.
* Using Microsoft Azure Backup requires the Microsoft Azure Backup Agent installed on DPM servers you want to back up. The DPM server must have at least 2.5 GB of local free storage space for cache location, although 15 GB of free local storage space for the cache location is recommended.
* A management certificate that you will upload to the backup vault in Microsoft Azure Backup. See above for the details.

#### Microsoft Azure Backup Agent Install

From Microsoft Azure Backup, install the agent **on each DPM server** you want to backup online.

#### Register DPM Server

After configuring backup vaults and deploying the Backup agent for DPM, the servers must be registered with the vault.

1. In the DPM Administrator Console, click **Management** in the left-pane, and then click **Online**. Click **Register** on the tool ribbon. The Microsoft Azure Backup Registration Wizard starts, and backup vault information is retrieved from Microsoft Azure.
2. Enter your Azure login credentials, and then click **Next**.
3. On the Backup Vault page, select the certificate you uploaded to the vault, and then select the corresponding vault. Then click **Next**.
4. On the Proxy Configuration page, specify whether you want to use a specific proxy server to connect the backup service to Azure.
5. Select **Use a proxy server for Microsoft Azure Backup**, and then type the URL to the proxy server. If you do not specify a proxy server, the default Internet connection settings for the server will be used, as displayed in the LAN settings.

* Use the FQDN or the IP address of the proxy server (for example, http://proxy.corp.contoso.com or http://10.186.173.132) and the port number on the server configured for Internet connections.
* If the proxy server requires authentication before allowing connections, select this proxy server requires authentication, and then type the user name and password that Microsoft Azure Backup Agent should submit when it is queried for credentials. Click Next to continue.

1. On the Throttling Setting page, configure the settings for Internet bandwidth throttling. You can specific throttling settings for specific days, and for work hours and non-work hours. Note that this option is not available for Windows Server 2008 R2. Then click **Next**.
2. On the Recovery Folder Settings page, specify a folder location that to use to temporarily hold recoverable items when a recovery occurs. Allocate enough space to hold the size of data you anticipate for recovery purposes. Then click **Next**.
3. On the Encryption Setting page, in **Enter Passphrase** and **Confirm Passphrase**, specify a passphrase that will be used to encrypt backups sent to Microsoft Azure, and to decrypt backups retrieved from Microsoft Azure. Click **Copy to clipboard** and then ensure that you store the passphrase in a secure and safe location, preferably to a restricted access external location.
4. Click **Register** to complete the process. If successful, you will get a registration confirmation message and you can close the wizard.

#### [Schedule a backup](javascript:void(0))

The backup schedule is the core of the backup process. It identifies which files and folders to backup and the days and times to perform the backup.

##### [To create a scheduled backup](javascript:void(0))

1. Press the **Windows logo key + Q** to open the **Apps** menu, and then click **Azure Backup Agent**. The Azure Backup Agent snap-in should open.
2. In the **Action** menu, click **Schedule Backup** to open the **Schedule Backup Wizard**. The **Getting Started** page is displayed. Click **Next** to continue.
3. The **Select items to backup** page is displayed. The items that are specified on this page create the list of files and folders to back up.

Click **Select Items** to open a dialog box that shows the tree view of the file system. You can navigate through the files and folders and select those that you want to back up.

Click **Exclusion Settings** to open a dialog box in which you can select files or folders that you do not want to back up.

|  |
| --- |
| **noteNote** |
| The shorter the list of files for the backup, the more efficient the backup process will be. For example, imagine you want to back up folder D:, which is used to store all your users’ data files. Each user has an individual folder in this location. However, you do not want to include D:\temp because that folder is used for clean-up, and it does not contain any valuable data. To accomplish this, you could open the **Select items** dialog box, clear the check mark from D:\temp, and leave the rest of the user’s folders selected. This would create a very long backup list because each folder would be listed individually for the backup. Alternatively, you can select to back up all of D:\, and then in the **Exclusion Settings** dialog box, add D:\temp as an excluded item. This would create a two item backup list that would be processed much quicker. |

When you have specified the files and folders to back up, click **Next** to continue.

1. The **Specify backup time** page is displayed. Select the day of the week and time of day that backups will occur. **Retention range** specifies the maximum amount of time that Microsoft Azure Backup will store backed-up data. Backups can be retained for 354 recovery points. Specify the number of days backups will be retained and whether to synchronize daily or weekly. Weekly frequency can be 1 to 4 weeks. Click **Next** to continue.
2. The **Confirmation** page is displayed. This shows the backup schedule that you have specified by using the wizard. If you need to make any changes, click **Back** and make the changes, otherwise click **Finish** to create the schedule.
3. The **Summary** page is displayed with a message that the online backup schedule was successfully created. You can now close the wizard.

After you configure a schedule, details for the backup schedule are displayed in the Microsoft Azure Backup snap-in.

PowerShell Logo**Windows PowerShell equivalent commands**

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

To start a new backup from within Windows PowerShell, administrators need to define a backup policy, the data locations, the schedule for the backup job and the data retention policy for the backup policy. The following commands will set the object variables for a basic backup job.

$policy = New-OBPolicy

$filespec = New-OBFileSpec -FileSpec <C:\Documents\Contracts>

$sched = New-OBSchedule -DaysofWeek Wednesday -TimesofDay 09:30 -

WeeklyFrequency 2

$ret = New-OBRetentionPolicy -RetentionDays 300

The following Windows PowerShell script example creates a new Microsoft Azure Backup policy named $policy that can back up all of the files and folders in the C:\Documents\Contracts folder. The backup policy runs on Wednesdays at 9:30 AM, and it will keep the data in the backup for a period of 30 days.

To add the variable to the new policy, do the following:

Add-OBFileSpec -Policy $policy -FileSpec $filespec

Set-OBSchedule -policy $policy -schedule $sched

Set-OBRetentionPolicy -policy $policy -rententionpolicy $ret

These commands put all of the previous variables into the **$policy** Online Backup policy object. Finally, save the Online Backup policy. Do this by using the following cmdlet:

Set-OBPolicy -policy $policy

Windows PowerShell will prompt you to ask if you want to save this backup policy. After it is saved, the new backup policy will run the next time it is scheduled.

#### [Recover data to the same server](javascript:void(0))

1. Press the **Windows logo key + Q** to open the **Apps** menu, and then click **Azure Backup Agent**. The Azure Backup Agent snap-in should open.
2. In the **Action** menu, click **Recover Data** to open the Recover Data Wizard. The **Getting Started** page is displayed. Click **This server**, and then click **Next** to continue.
3. The **Select Recovery Mode** page is displayed. Choose one of the following modes:
   * **Browse for files**. Choose this option to browse the directory listing of the backup volume and specifically select the appropriate files or folders to recover.
   * **Search for files**. Choose this option to search for a specific file or folder by name. You can use wildcard characters to search for files or folders when you do not know the entire name.

Click **Next** to continue.

1. The **Select Volume and Date** page is displayed. From this page, you can select the volume and the point-in-time of the backup that you want to restore. If multiple backups were taken on a single day, you can use the drop-down arrow next to the time-of-day to select the backup that you want.

Click **Next** to continue.

1. The **Select items to recover page** is displayed. This page differs as follows, depending on whether you selected the **Browse for files** or **Search for files** option.
   * **Browse for files option** Presents a tree control that you can navigate to select the files you want to recover.
   * **Search for files option** Presents a text entry field where you can identify the volume to search and then type the file name or pattern to search for. Files that match the search criteria are listed so that you can select the files that you want to recover.

After you have selected all of the files or folders that you want to recover, click **Next** to continue.

1. The **Specify recovery options** page is displayed.

Choose how to handle potential file conflicts during the recovery process by choosing one of the following options:

* + **Create copies so that you have both versions** This option makes a copy of the file with a new file name in the same location as the duplicate file. The file name of the new file starts with the following text string (<recovery date>**Copy of**<original file name>)
  + **Overwrite the existing versions with the recovered versions** This option overwrites the file, and the only version that will exist in the restore location is the recovered file version.

|  |
| --- |
| **CautionCaution** |
| The overwrite restoration option removes any file with the same file name. You should ensure that there is no valuable data that will be overwritten when you choose this option. |

* + **Do not recover the items that already exist on the recovery destination** This option retains the current version of any files that already exist in the recovery destination. Recovery will occur only for data that does not exist in the recovery destination.

In **Security settings**, select the check box to restore the access control list (ACL) settings of the files and folders that are recovered, or clear the check box to have the restored files and folders inherit the ACLs that are present in the recovery destination. Click **Next** to continue.

|  |
| --- |
| **WarningWarning** |
| Sharing settings are not recoverable. If a file or folder is shared when it is backed up, it will not be shared when it is recovered. You must reset the sharing settings manually after recovery. |

1. The **Confirmation** page is displayed. Verify that the items you are going to recover are the ones that you want and that they are being recovered to the correct location with the correct settings. If everything appears as you expect, click **Recover** to start the recovery process.
2. The **Recovery Progress** page is displayed, which shows the progress of the recovery operation. You can close the wizard while the recovery is occurring and track the progress through the Microsoft Azure Backup snap-in. The **Jobs** pane shows the status of **Job completed** when the recovery is done.

PowerShell Logo**Windows PowerShell equivalent commands**

The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.

The following Windows PowerShell cmdlets provide an example of how you could perform a local recovery (data that is backed up by using and recovered to the same server):

[Copy](javascript:if%20(window.epx.codeSnippet)window.epx.codeSnippet.copyCode('CodeSnippetContainerCode_aeb81dc7-9030-40e1-867e-2b04c6c8e053');)

$source = Get-OBRecoverableSource

$item = Get-OBRecoverableItem -Source $source[0]

$FinalItem = Get-OBRecoverableItem -ParentItem $item[0]

$paging\_context = New-OBPagingContext

#To use the search function to find all .log files from a backed up location:

$search\_page1 = Get-OBRecoverableItem –RecoveryPoint $item[0] –PagingContext $paging\_context -SearchString \*.log -Location C:\Windows\Logs

#To use the browse function to locate a certain file across backups, first establish the location parameters for the top and bottom of the search range:

$recover\_levelone = Get-OBRecoverableItem –PagingContext $paging\_context -ParentItem $item

$recover\_leveltwo = Get-OBRecoverableItem –PagingContext $paging\_context -ParentItem $FinalItem

#Then run the recovery operation:

$recover\_option = New-OBRecoveryOption

Start-OBRecovery -RecoverableItem $FinalItem -RecoveryOption $recover\_option

## Summary

In this hands-on Lab, you have learnt the most efficient scenarios for protecting your server infrastructure through a cloud-based backup solution using Microsoft Azure, Windows Server and System Center Data Protection Manager.

## Additional References:

* [Azure Documentation Center](http://azure.microsoft.com/en-us/documentation/)
* [Azure Technical Documentation Library](http://msdn.microsoft.com/en-us/library/azure/dn578280.aspx)