Microsoft Azure - Starter Kits for Partners

Hands on Lab

Archiving and Backup

Azure Backup Server

Last Update: April 2016





**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](#_Toc448491544)

[Objectives 4](#_Toc448491545)

[Scenario 4](#_Toc448491546)

[Windows Server Machine 4](#_Toc448491547)

[Microsoft Azure Backup Vaults 6](#_Toc448491548)

[The software package. 9](#_Toc448491549)

[Network connectivity. 20](#_Toc448491550)

[Next steps 21](#_Toc448491551)

[Summary 21](#_Toc448491552)

[Additional References: 21](#_Toc448491553)

## Overview

This document covers the required steps to enable Microsoft Azure Backup Service using Azure Server Backup. 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 your server infrastructure with Azure Backup Server.

**Note:** Azure Backup Server inherits the functionality of Data Protection Manager (DPM) for workload backup. You will find pointers to DPM documentation for some of these capabilities. However Azure Backup Server does not provide protection on tape or integrate with System Center.

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 link that provide the most up-to-date steps to install and deploy a Azure Backup Vault. It includes steps to deploy:

<https://azure.microsoft.com/en-us/documentation/articles/backup-azure-microsoft-azure-backup/>

## Scenario

A cloud-based protection solution with Microsoft Azure Backup Serverprovides an experience similar to backing up with System Center 2012 - Data Protection Manager (DPM) to disk or to the cloud, using Microsoft Azure Backup Vault.

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.

## Windows Server Machine

The first step towards getting the Azure Backup Server up and running is to have a Windows Server machine. Either on site or in Azure.

|  |  |  |
| --- | --- | --- |
| Location | Minimum requirements | Additional instructions |
| Azure | Azure IaaS virtual machine  A2 Standard: 2 cores, 3.5GB RAM | You can start with a simple gallery image of Windows Server 2012 R2 Datacenter. [Protecting IaaS workloads using Azure Backup Server (DPM)](https://technet.microsoft.com/library/jj852163.aspx) has many nuances. Ensure that you read the article completely before deploying the machine. |
| On-premises | Hyper-V VM, VMWare VM, or a physical host  2 cores and 4GB RAM | You can deduplicate the DPM storage using Windows Server Deduplication. Learn more about how [DPM and deduplication](https://technet.microsoft.com/library/dn891438.aspx) work together when deployed in Hyper-V VMs. |

**Note:** It is recommended that Azure Backup Server be installed on a machine with Windows Server 2012 R2 Datacenter. A lot of the prerequisites are automatically covered with the latest version of the Windows operating system.

If you plan to join this server to a domain at some point, it is recommended that the domain-joining activity be done before the Azure Backup Server installation. Moving an existing Azure Backup Server machine to a new domain after deployment is *not supported.*

## Microsoft Azure Backup Vaults

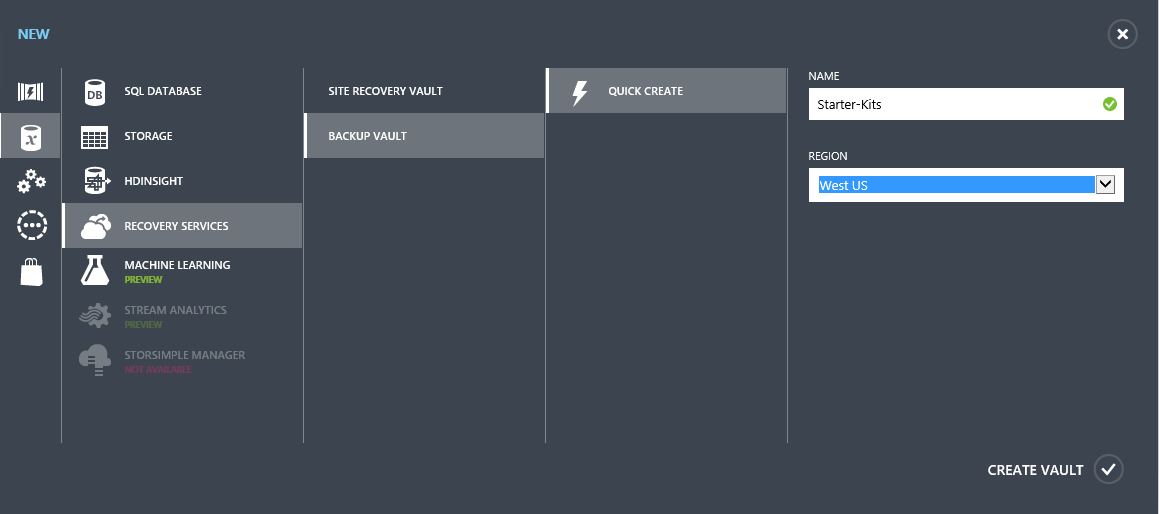
Whether you send backup data to Azure or keep it locally, the software needs to be connected to Azure. To be more specific, the Azure Backup Server machine needs to be registered with a backup vault.

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.

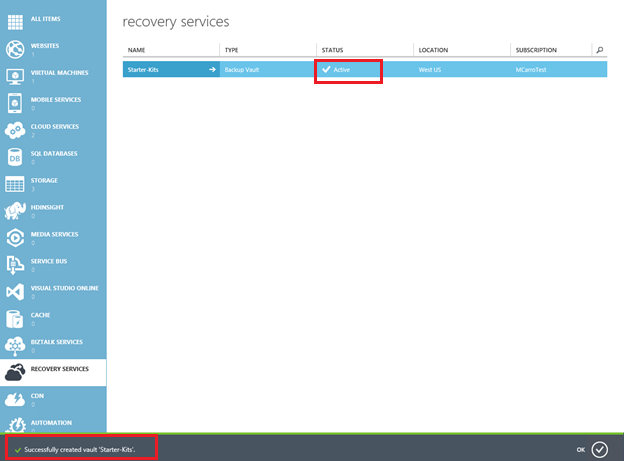
You can find a video outlining these steps at <http://www.youtube.com/watch?v=c-6CxFDGvIk>

#### 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**.

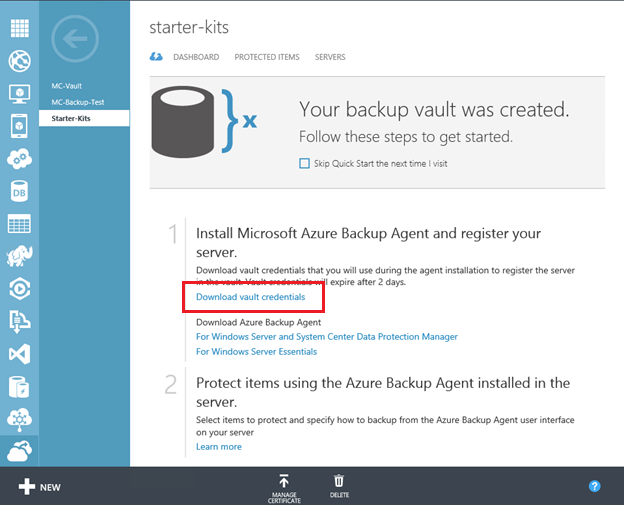


1. In **Name**, enter a friendly name to identify the backup vault.
2. In **Region**, select the geographic region for the backup vault.
3. Click **Create Backup vault**. It can take a while to create the backup vault. To check the status, you can monitor the notifications at the bottom of the portal. 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**.

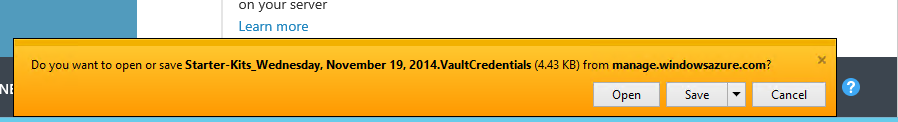


#### Download vault credentials

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”.



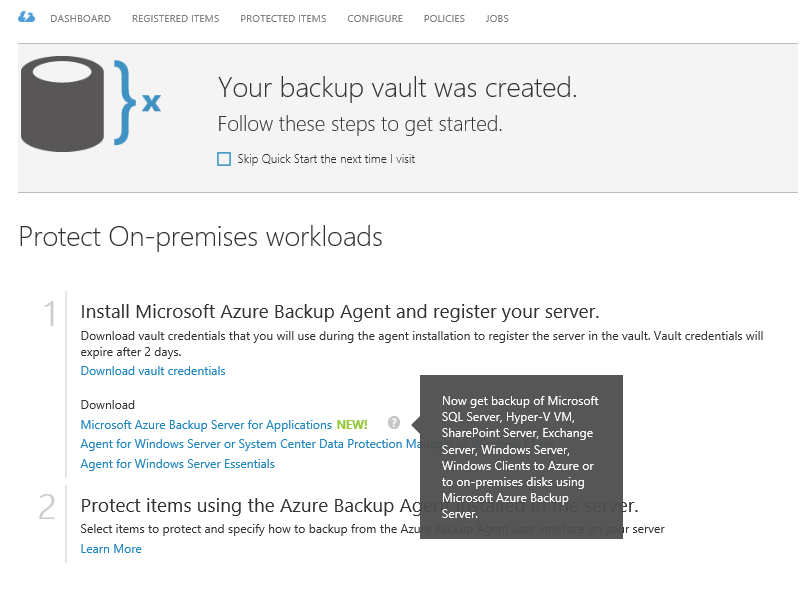
Then, select where to save the .Vault Credentials file on the server.



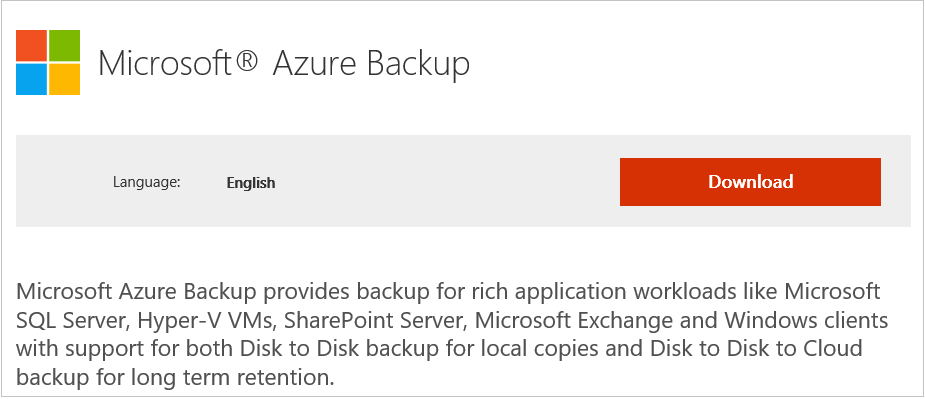
## The software package.

Similar to vault credentials, you can download Microsoft Azure Backup for application workloads from the Quick Start Page of the backup vault.

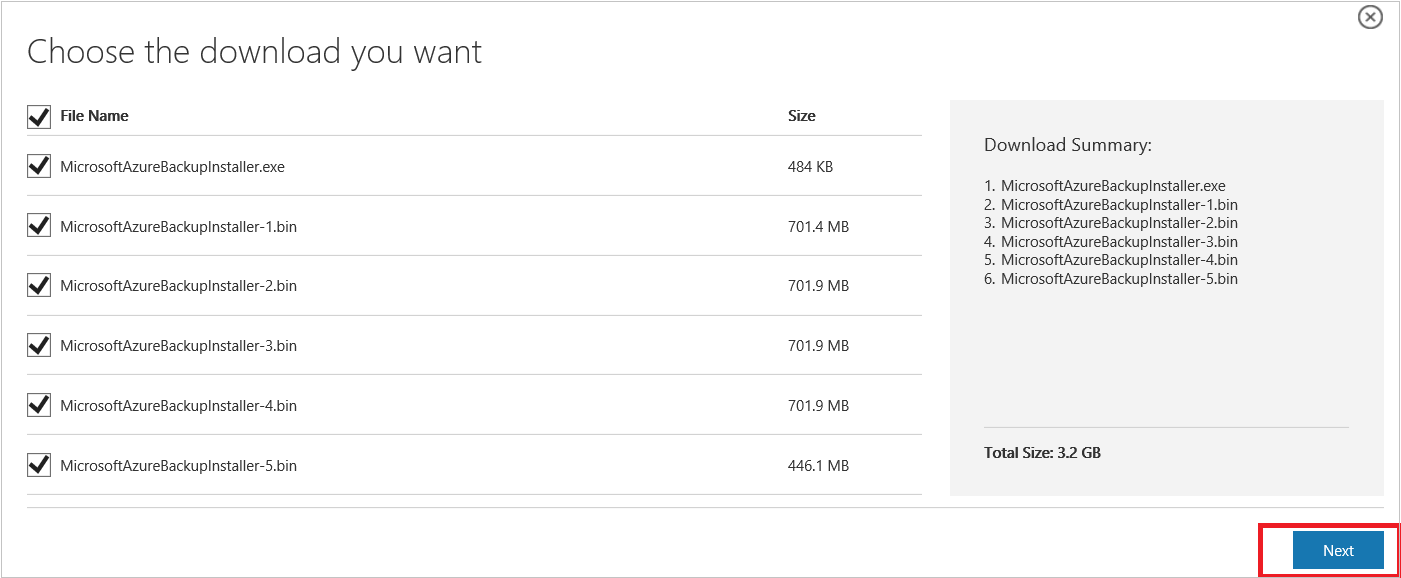
1. Sign in to the [Management Portal](https://manage.windowsazure.com/).
2. Click **Recovery Services**, and then click the name of backup vault to view the vault dashboard.
3. Click **Microsoft Azure Backup Server for Applications**. This will take you to the Download Center page from where the software package can be downloaded.



1. You will be redirected to the Microsoft Download Center to download the software. Click **Download**.



1. 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.

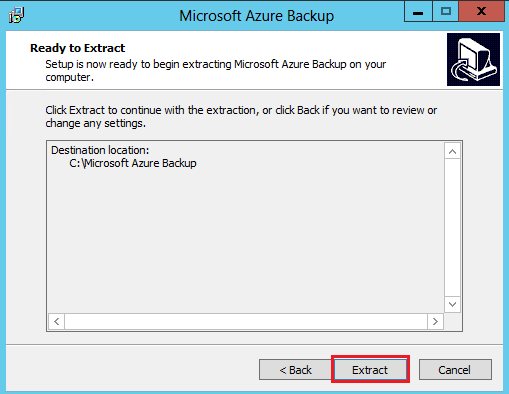


Since the download size of all the files together is > 3G, on a 10Mbps download link it may take up to 60 minutes for the download to complete.

#### 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.

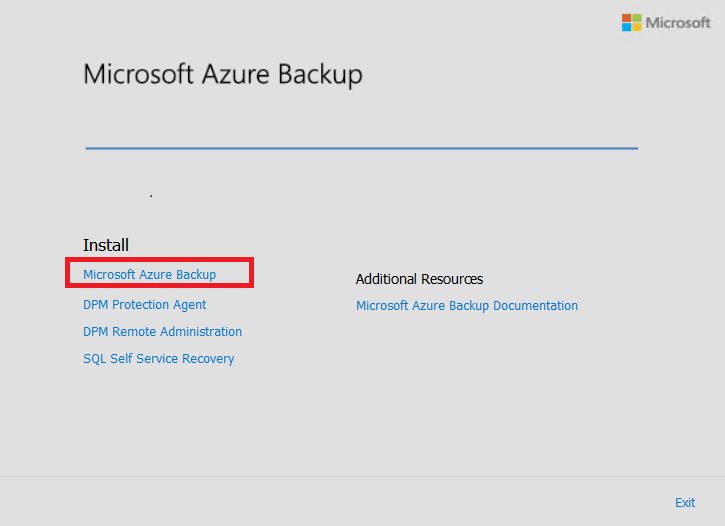
**Warning:** At least 4GB of free space is required to extract the setup files.



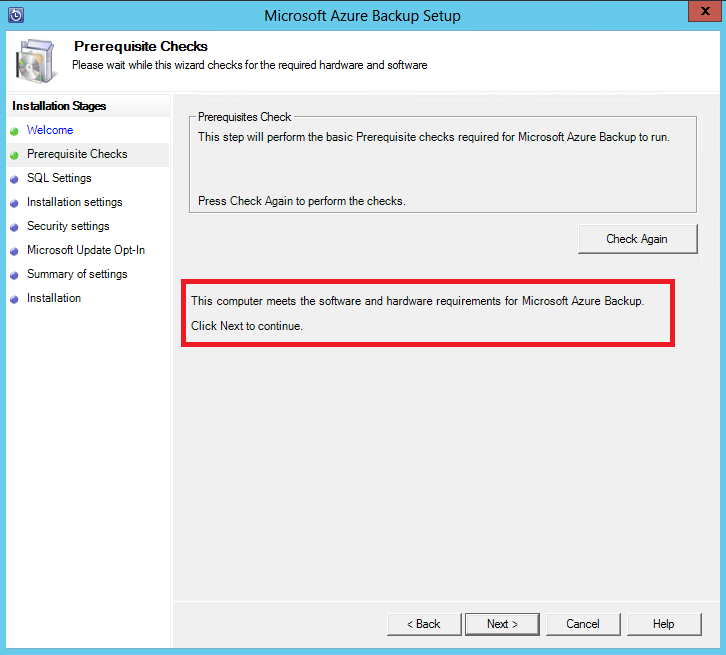
Once the extraction process complete, check the box to launch the freshly extracted *setup.exe* to begin installing Microsoft Azure Backup Server and click on the **Finish** button.

#### Installing the software package

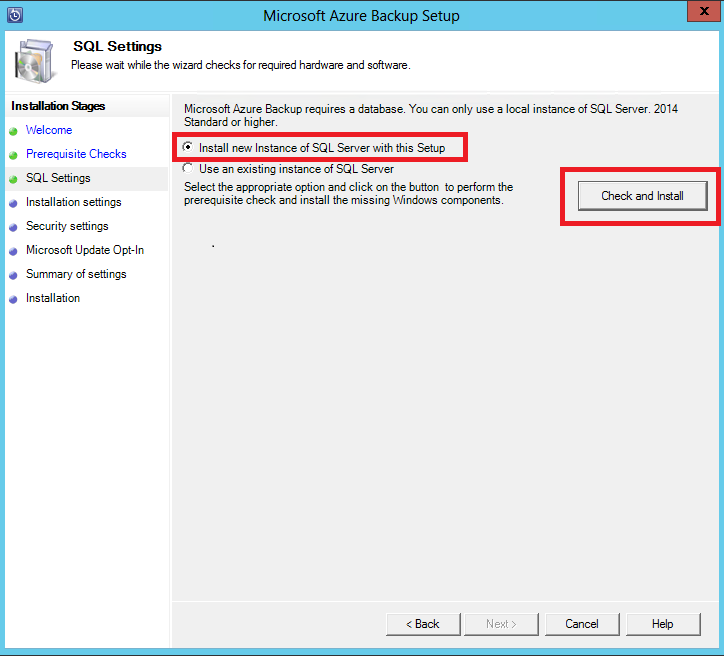
1. Click **Microsoft Azure Backup** to launch the setup wizard.

****

1. On the Welcome screen click the **Next** button. This takes you to the *Prerequisite Checks* section. On this screen, click on the **Check** button to determine if the hardware and software prerequisites for Azure Backup Server have been met. If all of the prerequisites are have been met successfully, you will see a message indicating that the machine meets the requirements. Click on the **Next** button.



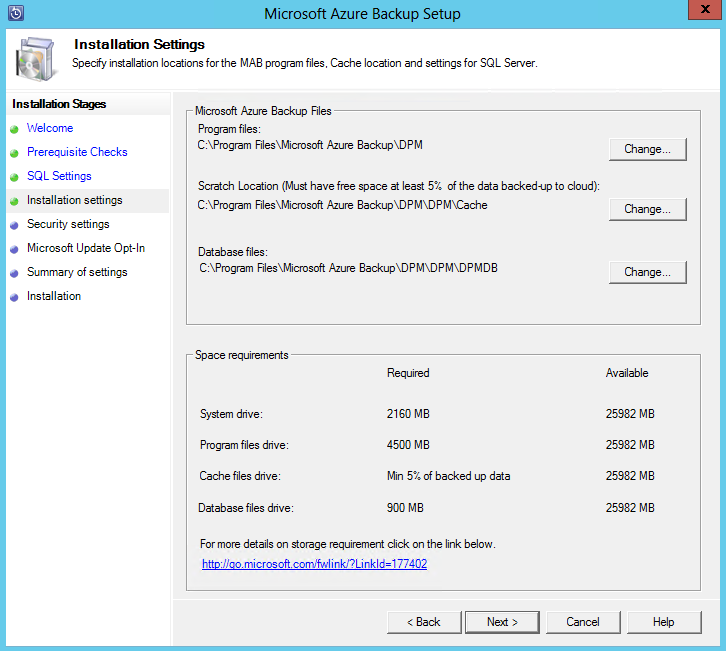
1. Microsoft Azure Backup Server requires SQL Server Standard, and the Azure Backup Server installation package comes bundled with the appropriate SQL Server binaries needed. When starting with a new Azure Backup Server installation, you should pick the option **Install new Instance of SQL Server with this Setup** and click the **Check and Install** button. Once the prerequisites are successfully installed, click **Next**.



If a failure occurs with a recommendation to restart the machine, do so and click **Check Again**.

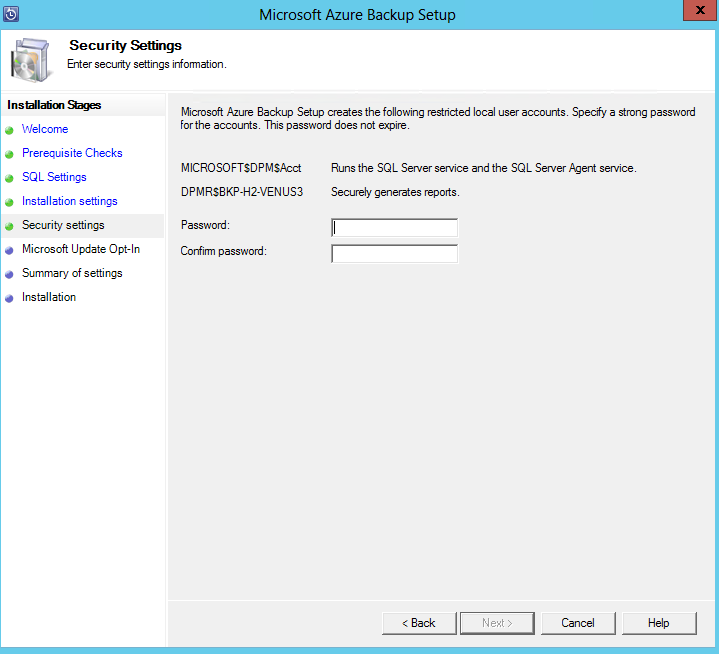
**Note:** Azure Backup Server will not work with a remote SQL Server instance. The instance being used by Azure Backup Server needs to be local.t least 4GB of free space is required to extract the setup files.

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



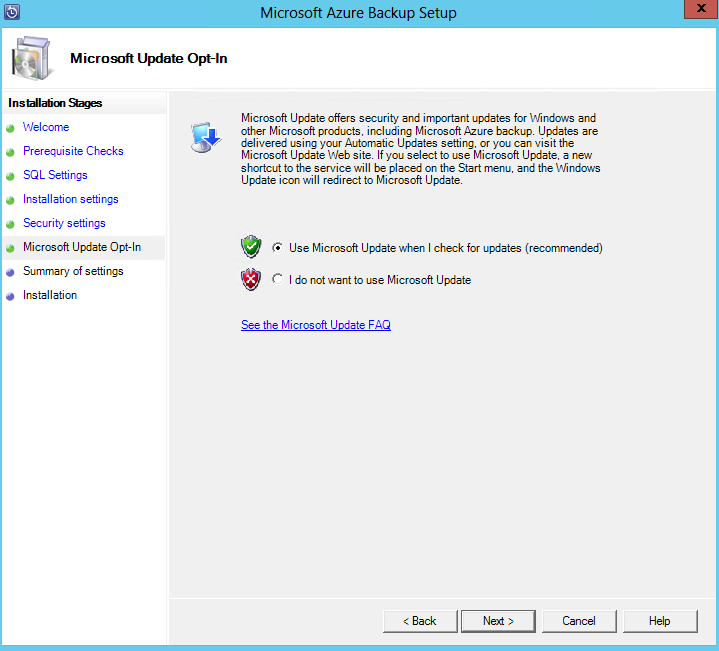
The scratch location is a requirement for back up to Azure. Ensure the scratch location is at least 5% of the data planned to be backed up to the cloud. For disk protection, separate disks need to be configured once the installation completes. For more information regarding storage pools, see [Configure storage pools and disk storage](https://technet.microsoft.com/library/hh758075.aspx).

1. Provide a strong password for restricted local user accounts and click **Next**.

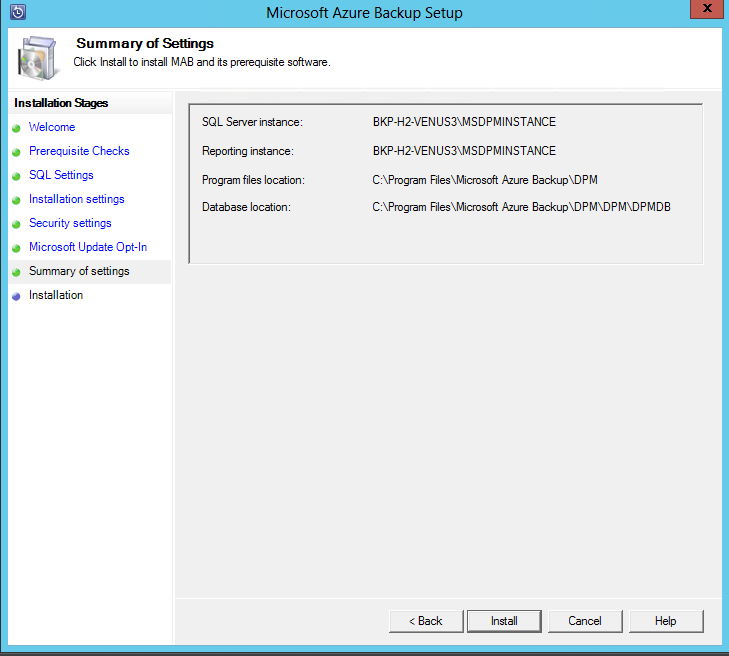


1. Select whether you want to use *Microsoft Update* to check for updates and click **Next**.

**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.

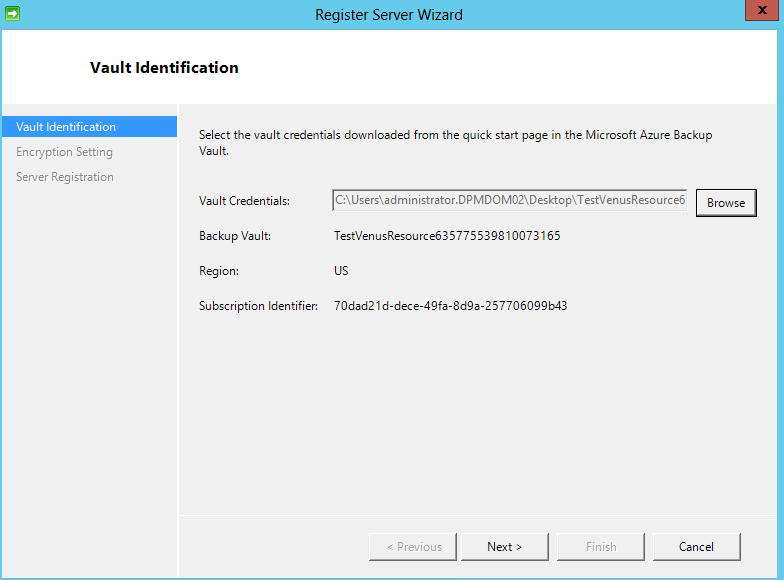


1. Review the *Summary of Settings* and click **Install**.

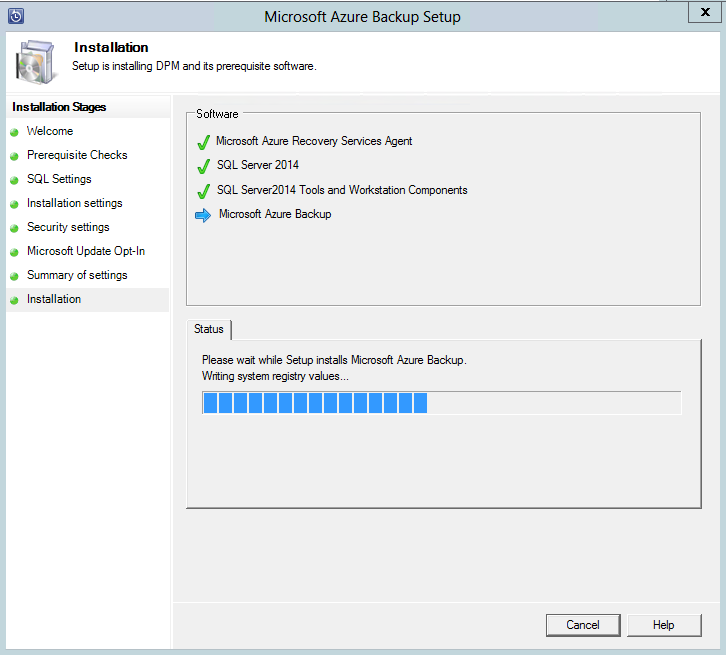


1. The installation happens in phases. In the first phase the Microsoft Azure Recovery Services Agent is installed on the server. The wizard also checks for Internet connectivity. If Internet connectivity is available you can proceed with installation, if not, you need to provide proxy details to connect 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 backup 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.



1. 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](https://technet.microsoft.com/library/hh758075.aspx).

**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.

## 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-DPMCloudConnection commandlet in the Azure Backup Server PowerShell console. If the output of the commandlet 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, log in to the [subscription portal](https://account.windowsazure.com/Subscriptions).

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 | Backup to Azure | Backup 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 whitelist the following domain addresses in the firewall/proxy profile:

* www.msftncsi.com
* \*.Microsoft.com
* \*.WindowsAzure.com
* \*.microsoftonline.com
* \*.windows.net

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.

## Next steps

Once you have your Windows Backup Server installed, you can protect the workloads according to the following table:

[DPM protection support matrix](https://technet.microsoft.com/en-us/library/jj860400.aspx)

You can use these articles to gain a deeper understanding of workload protection using Microsoft Azure Backup server.

* [SQL Server backup](https://azure.microsoft.com/en-us/documentation/articles/backup-azure-backup-sql/)
* [SharePoint server backup](https://azure.microsoft.com/en-us/documentation/articles/backup-azure-backup-sharepoint/)
* [Alternate server backup](https://azure.microsoft.com/en-us/documentation/articles/backup-azure-alternate-dpm-server/)

## Summary

In this hands-on Lab, you have learnt the scenarios for protecting your server infrastructure through a cloud-based backup solution using Microsoft Azure Backup Server.

## 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)