.

© 2017 Microsoft Corporation. All rights reserved.

Microsoft Proprietary and Confidential Information

This training package content is proprietary and confidential, and is intended only for users described in the training materials. Some elements of this document are subject to change. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

This content and information is provided to you under a Non-Disclosure Agreement and cannot be distributed. Copying or disclosing all or any portion of the content and/or information included in this package is strictly prohibited. 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 example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

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

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

Participant Guide

WorkShopPLUS

Azure Site Recovery

Module 1 Lab: Backing Up with ASR

Table of Contents

[Lab 1: 3](#_Toc435460474)

[Overview 3](#_Toc435460475)

[Exercise 1: Protect your client to Microsoft Azure 5](#_Toc435460476)

[Exercise 2: Protecting Azure IaaS VM 14](#_Toc435460477)

[Exercise 3: Protecting SQL Databases to Azure from DPM 21](#_Toc435460478)

[Exercise 4: Restoring Databases using DPM and Microsoft Azure 29](#_Toc435460479)

[Appendix A - Post-protection activities 35](#_Toc435460480)

[Installation of the backup extension 35](#_Toc435460481)

[Appendix B - Consistency of recovery points 38](#_Toc435460482)

## Lab 1:

|  |  |
| --- | --- |
|  |  |
|  | The time to complete this module, including exercises, is 180 minutes. |
|  | The key takeaways from this lab are:   * DPM is a simple and powerful backup solution which can backup data & applications from a server’s client * DPM enables customers to easily extend their on-premises protection to Azure. * Administrators can monitor DPM (physical, virtual, running on premises, running in Azure) from a single console. |
|  |  |

### Overview

Fabrikam Inc is a Silicon Valley enterprise which specializes in building custom turnkey solutions in the real estate space. They have 17 branch offices in the U.S and are supported by 3000 full time employees.

Their line of business applications are based on Windows and their endpoint client laptop/desktop are on either Windows 7 or Windows 10

For the purpose of this hands on lab, as an IT administrator of Fabrikam Inc, you have been tasked to define the business continuity & protection policy for the applications, data and client machines (desktop, laptop).

As your IT infrastructure is managed by System Center, you intend to use System Center Data Protection Manager (DPM) to define your backup strategy. You are also interested in exploring how Microsoft Azure can bring down your operational and infrastructure cost by providing a robust offsite backup technology which can replace your aging, expensive tape media. The hands on lab is aimed at bringing you to speed on some of the key capabilities of DPM.

#### Exercise Details

1. Protect files and folders from your laptop and desktop to Azure in 10 minutes

* Register a Windows 10 client to Azure Backup Service
* Backup a folder on that client to Azure
* Restore a folder on that client from Azure

1. Backup Azure Iaas VMs

* Create a VM on Azure
* Backup IaaS VM

1. DPM Attach to Azure

* Register DPM to Azure Backup
* Configure SQL Database backup to Azure
* Recover a SQL Database from Azure Backup

#### Prerequisites

* Internet access
* An Azure Pass subscription already setup and configured and access to the hosted Hands On Lab environment.

#### Virtual machine technology

This lab is completed using virtual machines that run on Windows Server 2012 Hyper-V technology. To log on to the virtual machines, press CTRL+ALT+END and enter your logon credentials. Alternatively, you can use the Commands menu in the Learn On Demand Systems (LODS) console.

#### Computers in these labs

This lab uses computers as described in the following table.

|  |  |  |
| --- | --- | --- |
| Computer | Role | Configuration |
| AB-HOL-DC1 | Domain controller, DNS, WSUS, SQL | Domain Controller that exposes Domain called AB-HOL-FABRIKAM.loc |
| AB-HOL-DPM1 | DPM 2012 R2 | DPM Server that has DPM bits already installed |
| AB-HOL-SQL-PS | SQL | SQL Server with a DB created. Above DPM will protect these DBs to disk and to Azure. |
| AB-HOL-Win10-PS | Windows 10 | Windows 10 client that will be used to backup to Azure Backup |

* All user accounts in this lab use the password **DPMDOMAIN~1**
* All of these VMs have BkpAdmin1 as administrator

### Exercise 1: Protect your client to Microsoft Azure

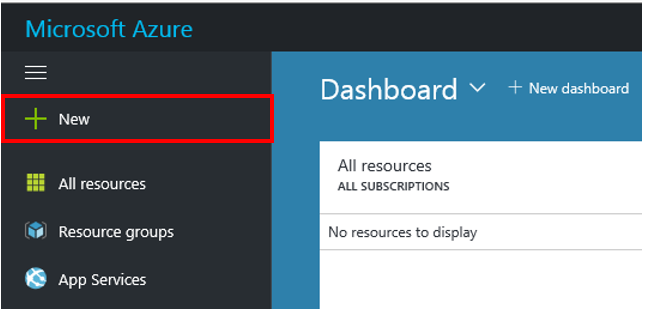
|  |  |
| --- | --- |
|  | The time to complete this exercise is 45 minutes. |
|  | The key takeaways from this lab are:   * Demonstrate client backup to Azure |
|  |  |

#### Create Azure Backup Vault

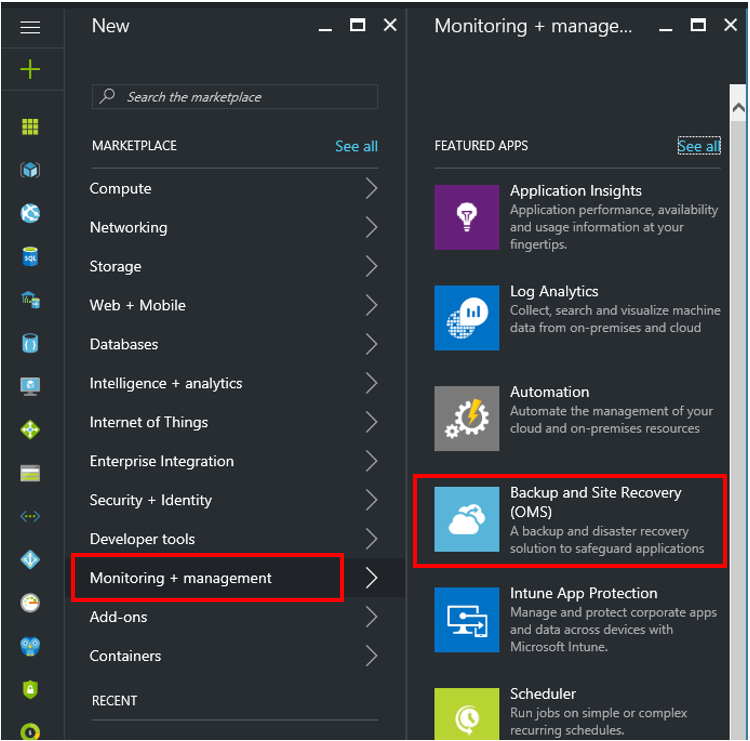
1. Logon to VM AB-HOL-Win10-PS using the domain admin credentials AB-HOL-FABRIKAM\Administrator .
2. To create an Azure Backup Vault to store backup data, Open Internet Explorer and navigate to the Azure Management Portal, <https://portal.azure.com>

**Note:** *You will need to use the AB-HOL-Win10-PS computer from the lab to do this*.

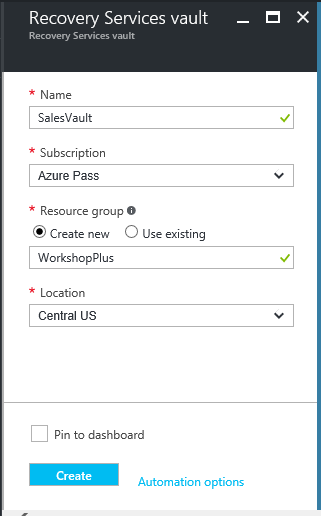
1. Browse to the “+ New” icon top right corner of the portal:



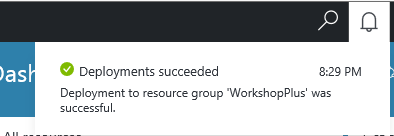
1. **Select** *Monitoring + Management, Backup and Site Recovery OMS*



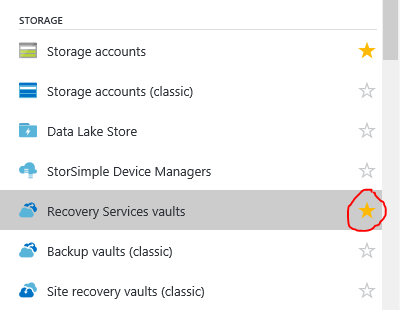
1. From the resulting blade, give the Recovery Services Vault the Name *SalesVault* and create a new Resource Group called *WorkshopPlus* in the Location *CentralUS* the click the large blue Create button at the bottom of the blade.



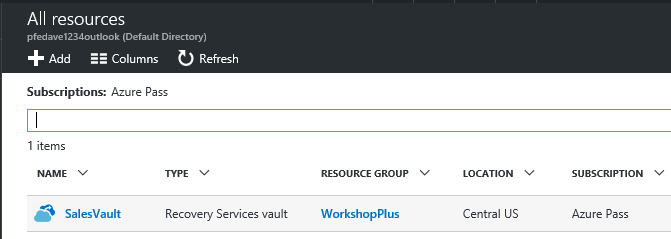
1. Wait a short while until the deployment completes successfully. You will see a notice in the top right corner of the window next the “Bell” icon which is for notifications.



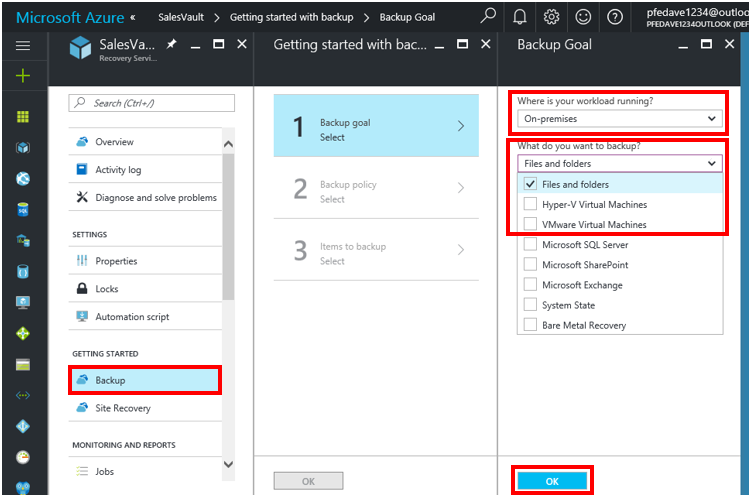
1. For easy access to Recovery Services Vaults for the rest of the course, and for future use, you can add a shortcut to your Recovery Services Vaults to the left side menu. From the bottom of the left side menu choose More Options and scroll down to find the Storage section. In that section, you will see an option for Recovery Services vaults. Click the star at the end of the row and that will add the Recovery Services vaults icon to the left side menu bar.



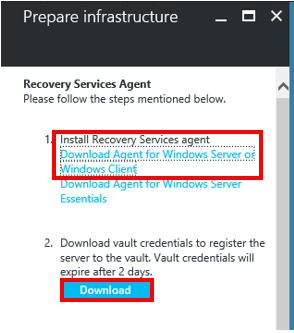
1. Use this new shortcut and click on the SalesVault item in the resulting pane.



Choose the *Backup* option from the Getting Started section in the first column, and in the blade for the Backup Goal, choose that your workload is running *On-premises* and in the What do you want to backup section, choose *Files and Folders*. Then click the OK button.

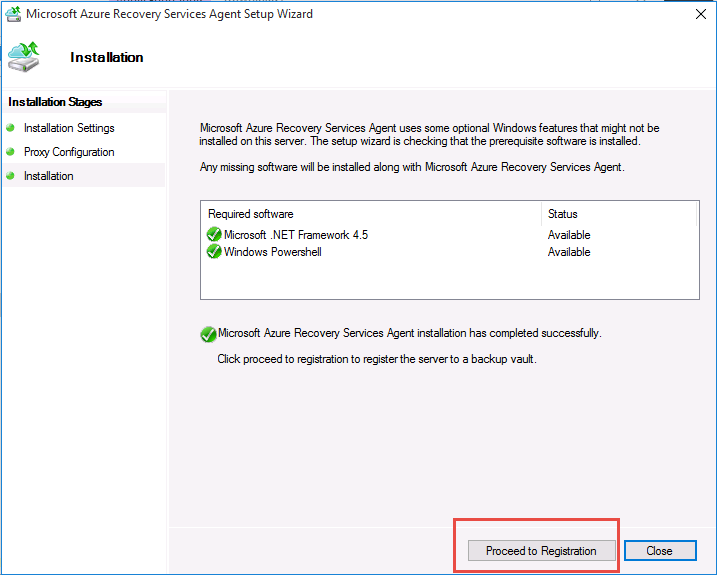


1. You will need to download to your local machine the Recovery Services Agent. There will be two options to choose from at Step 1. Choose Download Agent for Windows Server or Windows Client and save the file locally on the desktop of the hosted Windows 10 machine you are running this from which is *AB-HOL-Win10-PS*. Also click the blue Download button and save a copy of the vault credentials file to the local desktop on *AB-HOL-Win10-PS*.

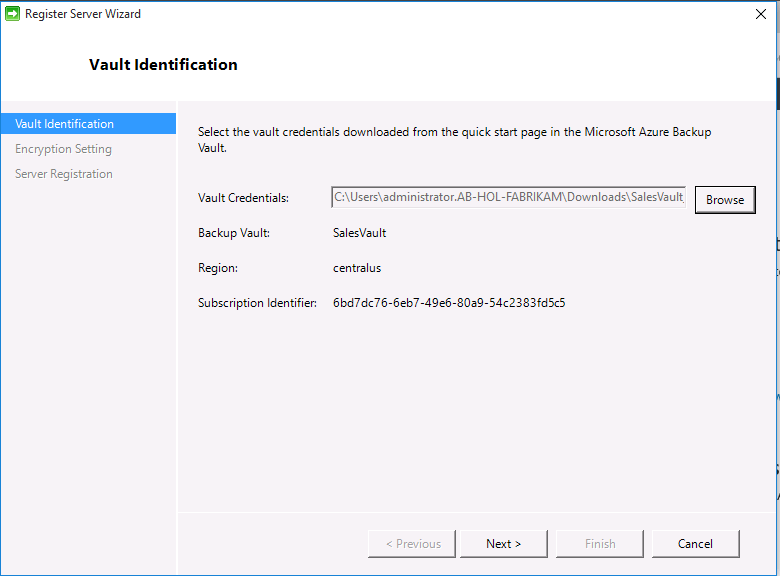


#### Register AB-HOL-Win10-PS to the Azure Backup Service

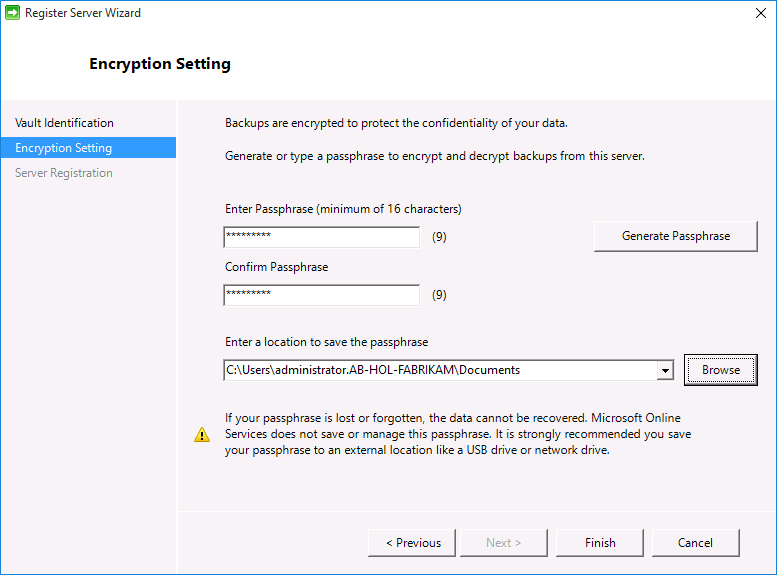
1. Install the MARSAgent by **clicking** on the *MARSAgentInstaller.exe* downloaded in the previous section. Once installation has completed, **click** on *Proceed to Registration*:



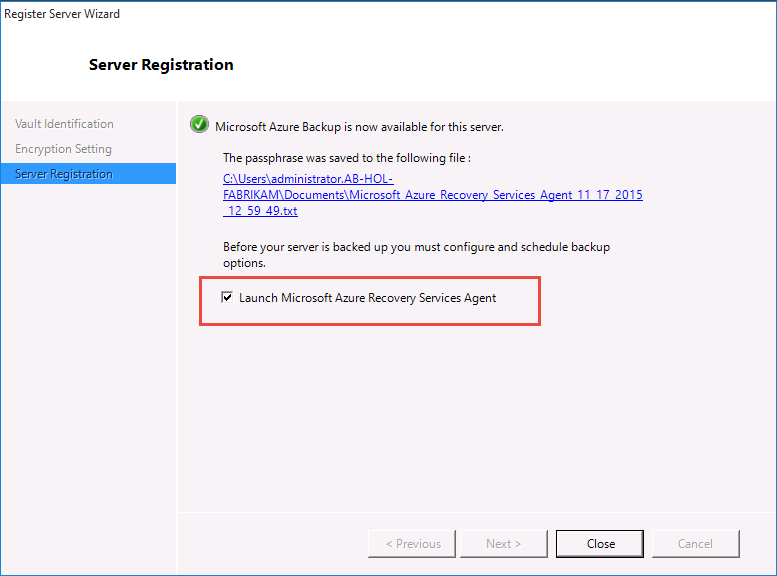
1. In the *Vault Identification* dialog, **browse** to and **select** the vault credential file that was downloaded in the last section and then **click** Next:



1. **Enter** a PassPhrase at least 16 characters or longer. **Store** the PassPhrase file on local directory and **click** Finish as shown:

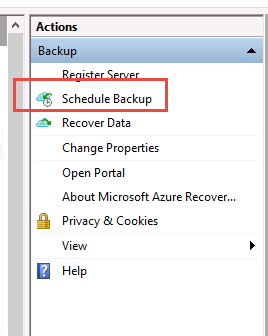


1. In the ending dialog, keep the *“Launch Microsoft Azure Recovery Service Agent”* checked and **click** *Close.*

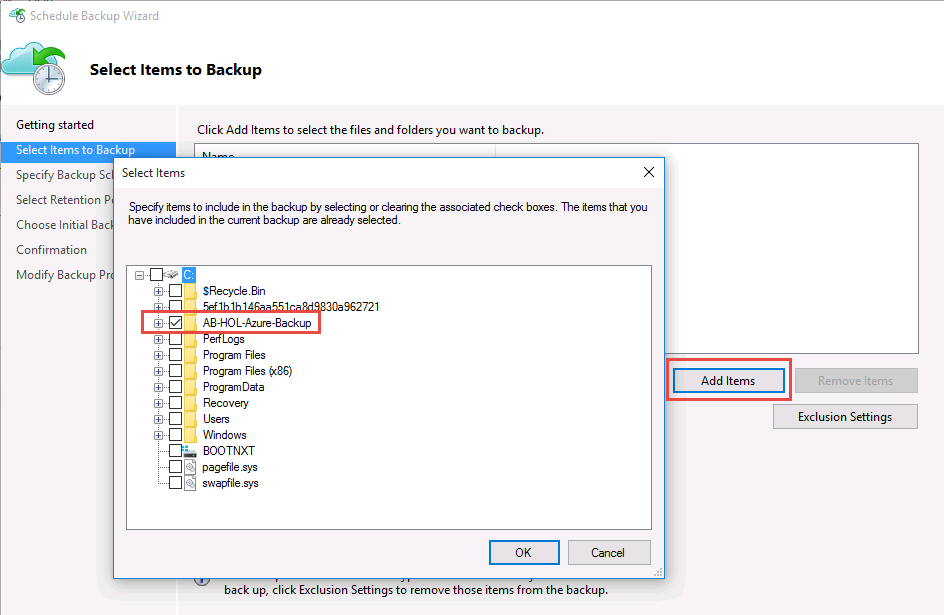


#### Protecting your Client using Microsoft Azure Backup

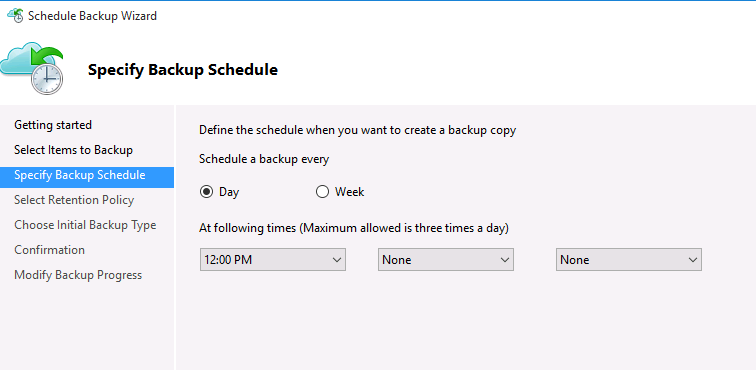
1. **Create** a folder called *AB-HOL-Azure-Backup* in the C:\ folder and copy some files into it. (**For example**: *Copy the MARSagent installer and your Vault Credential settings into the folder.*)
2. Navigate back to the *Microsoft Azure Backup* application and **click** on *Schedule Backup*.



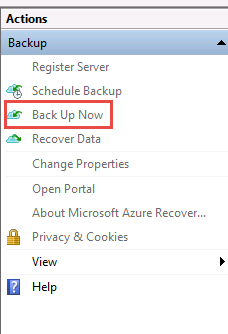
1. **Click** *Next* at the *Getting Started* dialog.
2. In the *Select Items to Backup* dialog, **select** the *Add Items* button and select the folder that you created in Step A. **Click** OK and then *Next*.



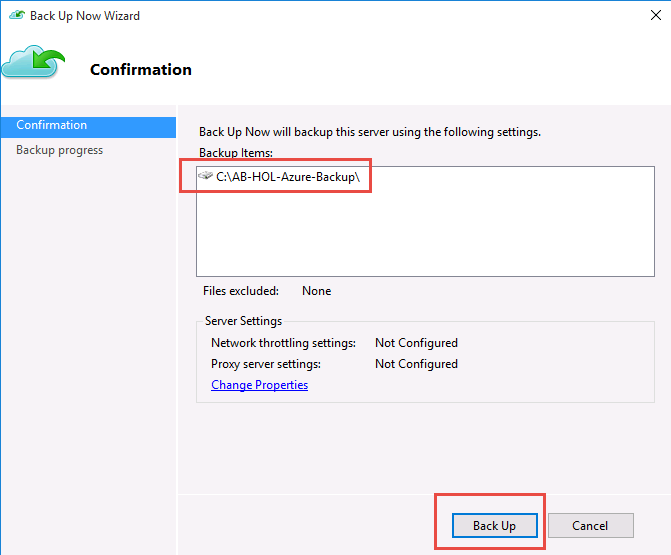
1. In the *Specify Backup Schedule* dialog, specify daily time to backup data as shown below and then **click** *Next*:



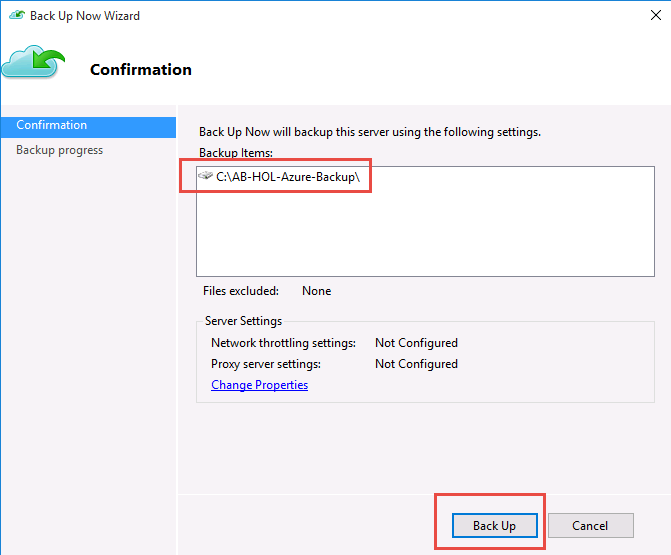
1. In the *Select Retention Policy* dialog, leave the default settings and then **click** *Next*.
2. In the *Choose Initial Backup Type* dialog, leave the default settings and then **click** *Next.*
3. In the *Confirmation* dialog, leave the default settings and then **click** *Finish*.
4. In the main window of the *Microsoft Azure Backup* application, **click** on *Backup Now* in the *Actions* menu:



1. In the *Confirmation* dialog of the *Back Up Now Wizard*, ensure that the folder you created at the beginning of this section is listed in the backup and then **select** *Backup*.

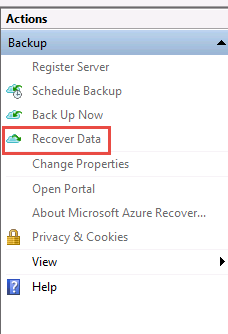


1. Your files will now be backed up to Azure.



#### Restoring files to your Client using Microsoft Azure Backup

1. On your C:\ drive, **delete** the *AB-HOL-Azure-Backup* folder using File Explorer.
2. In the *Microsoft Azure Backup* application, **select** *Recover Data* from the *Actions* menu:

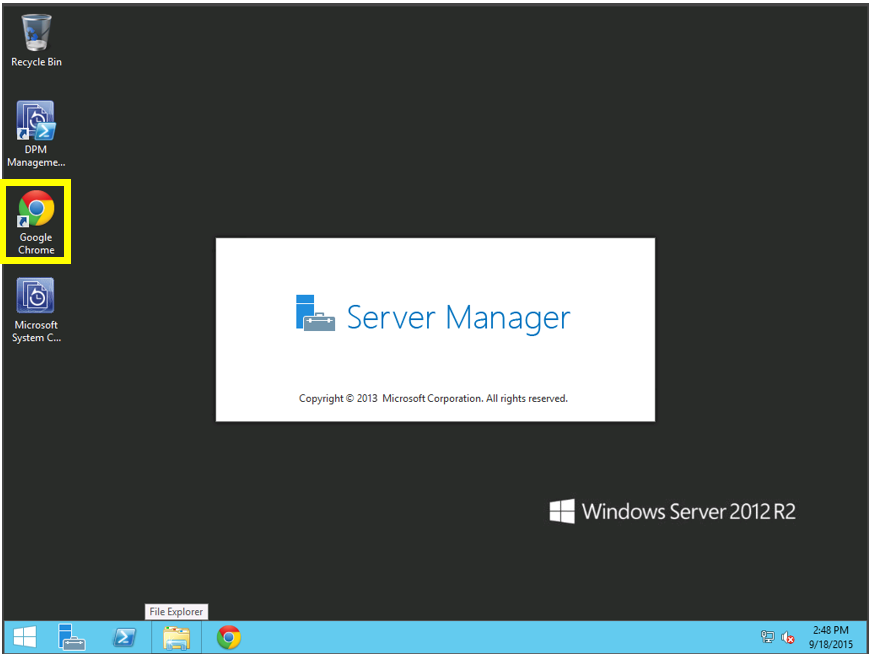


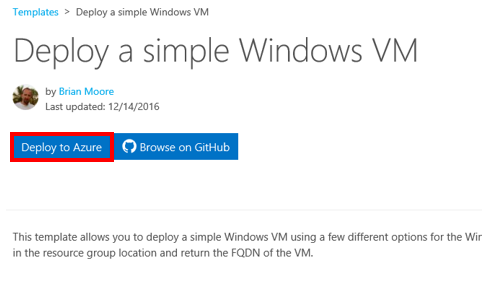
1. In the *Getting Started* dialog, leave the defaults and **click** *Next*.
2. In the *Select Recovery Mode* dialog, keep the defaults and **click** *Next*.
3. In the *Select Volume and Data* dialog, select volume C:\ and then **click** *Next*.
4. In the *Select Items to Recover* dialog, leave the defaults and then **click** *Next.*
5. In the *Specify Recovery Items* dialog, leave the defaults and then **click** *Next*.
6. In the *Confirmation* dialog, **click** *Recover*.
7. After the restore has completed, verify that your files were indeed recovered using File Explorer.

### Exercise 2: Protecting Azure IaaS VM

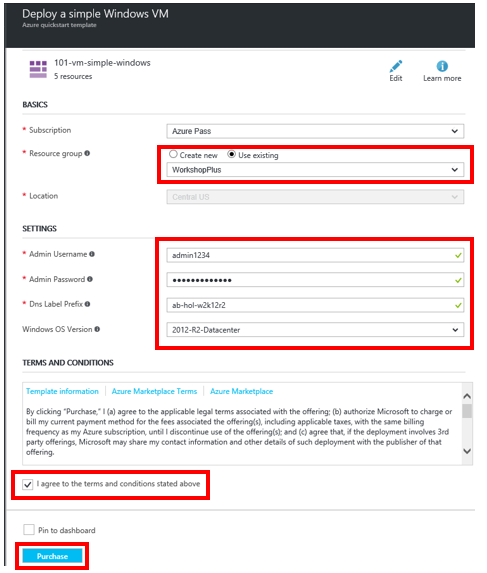
|  |  |
| --- | --- |
|  | The time to complete this exercise, is 45 minutes. |
|  | The key takeaways from this lab are:   * Protecting Azure VMs |
|  |  |

1. Log into AB-HOL-DPM1. Login name is AB-HOL-FABRIKAM\BkpAdmin1 and password is DPMDOMAIN~1
2. Launch Chrome Browser by clicking Chrome icon as shown below:



1. Navigate to [https://azure.microsoft.com/en-us/resources/templates/101-vm-simple-windows/](https://azure.microsoft.com/en-us/resources/templates/101-vm-simple-windows/%20) which is the Azure Quick Start templates page for a Simple Windows VM. Click on the large blue Deploy to Azure button at the top of the page.   
     
   

* This process will load this template into the Azure portal and it will be ready for you to deploy into Azure.



Use the existing Resource Group named *WorkshopPlus* that was from the previous section.

Use *admin1234* as the username for the local administrator

Create a password that meets complexity requirements: 12 characters in length, at least three of the four character types (uppercase, lowercase, number, special character) – remember this password.

Choose a name as the DNS label prefix – it is critical that this be all in lowercase and ***it must be globally unique within your deployment region.***

Choose *2012 R2 Datacenter* as the Windows OS Version

Check the box to agree to the stated terms.

Click the *Purchase* button.

This process will deploy a new Virtual Machine into your subscription. It will take 4-6 minutes to complete. Please wait for it to complete before moving on to the next section. The notification “bell” will tell you when it is complete.

#### Configure IaaS VM Protection

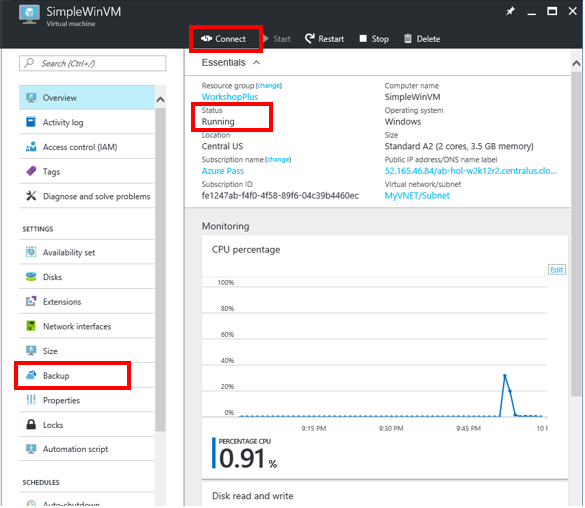
1. In the portal, if you are not already at the main Azure Dashboard, click the black area at the top left hand corner of the window that says Microsoft Azure. That will return you to the dashboard at any time. From the Dashboard, click on the Virtual Machines option in the left side menu



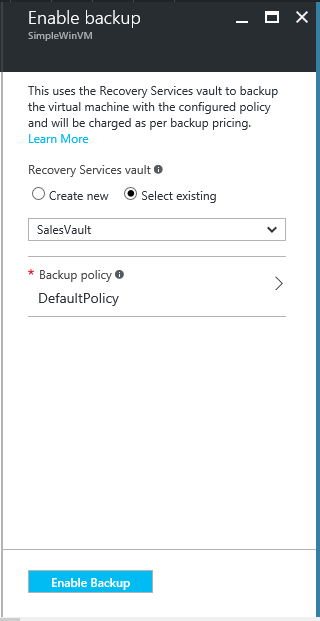
Then



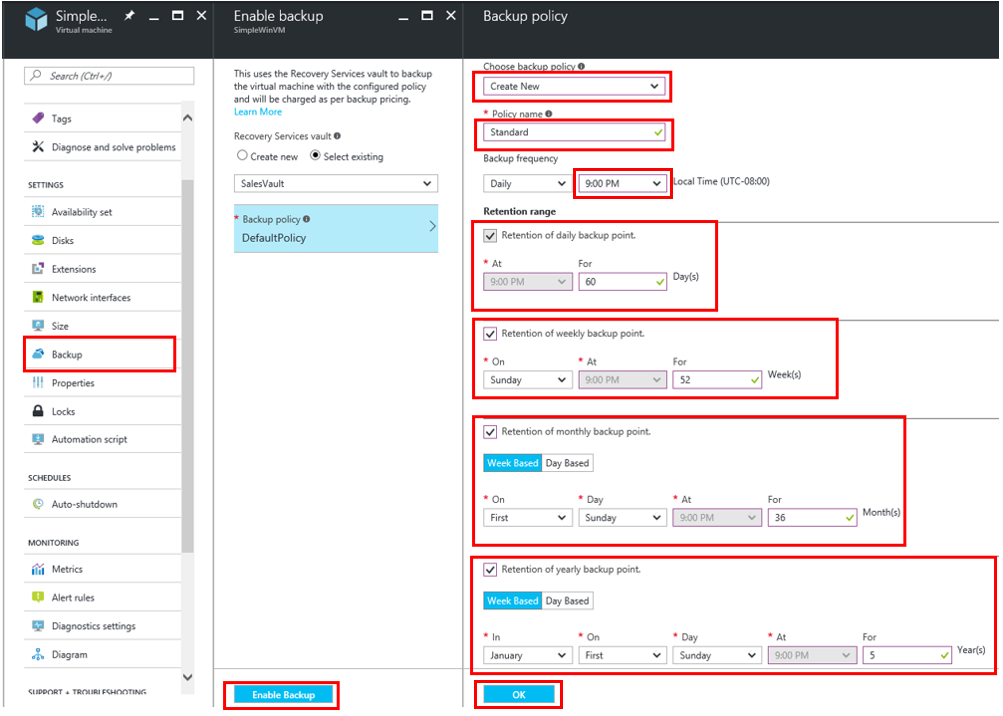
1. Click on the SimpleWinVM machine from the Virtual Machines blade. The resulting blade should verify that the VM is running and ready for use. You should see that the Status is set to *Running*, and there should be a *Connect* option available at the top of the blade.



1. If you can see that the status is listed as the above screen shot indicates, then choose the *Backup* option from the left side list of settings. You should see that the Select Existing option is chosen for you and the *SalesVault* is listed at the Recovery Services Vault to be used. It also will have defaulted to the Backup Policy named *DefaultPolicy*.



1. If this is sufficient, all you need to do is click the Enable Backup button at the bottom of the screen and you will have set up backup services for this VM using that Backup Policy.   
   While not necessary, **for the lab, a new policy will be defined and assigned to the VM.**



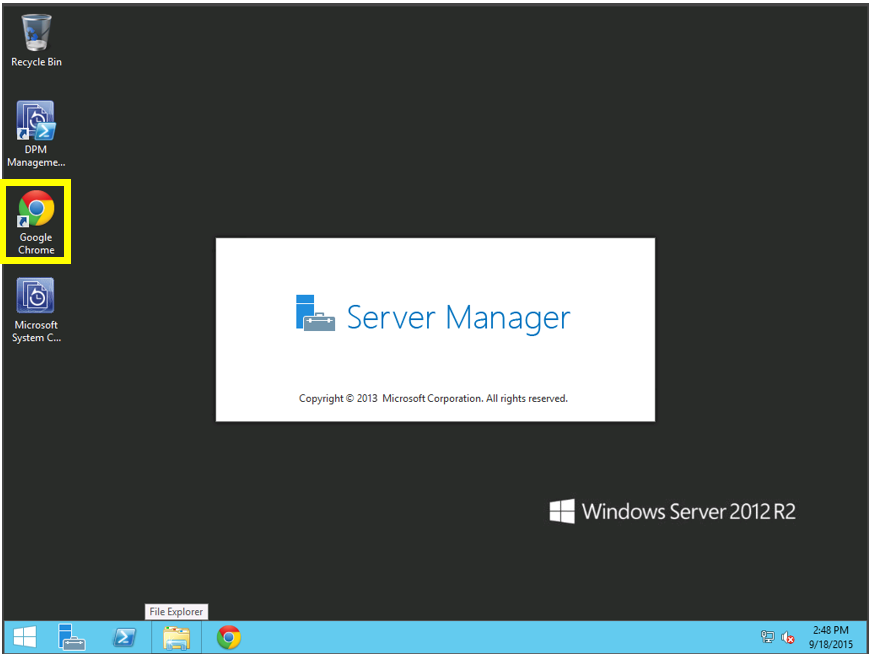
1. To create a new policy, follow the boxes from the above graphic, starting with the Backup option from the left side and go in a clockwise motion so that the last thing you choose is Enable Backup.
   * 1. Click Backup from the left menu
     2. Choose backup policy – *Create New*
     3. Policy Name – *Standard*
     4. Choose an *appropriate time* for the daily backup to run
     5. *Enable daily, weekly, monthly and yearly backup retention policies* and define values that seem reasonable to you.
     6. Click *OK* at the bottom of the Backup Policy blade
     7. Click *Enable Backup* on the Enable Backup blade, noticing that the Backup Policy selected has now changed to the new *Standard* policy you created.
2. A job is created for each virtual machine to configure the protection policy and to associate the virtual machines to the policy. **Click** the *Jobs* tab and choose the right filter to view the list of *Configure Protection* jobs.

### Exercise 3: Protecting SQL Databases to Azure from DPM

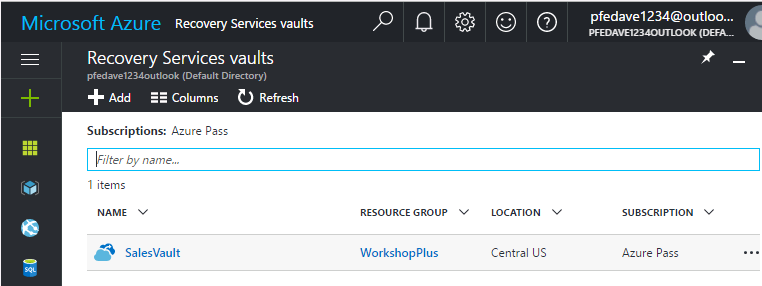
|  |  |
| --- | --- |
|  | The time to complete this module, including exercises, is 30 minutes. |
|  | The key takeaways from this lab are:   * How to protect SQL Databases to Microsoft Azure with Microsoft Data Protection Manager |
|  |  |

#### Register DPM with Azure Site Recovery

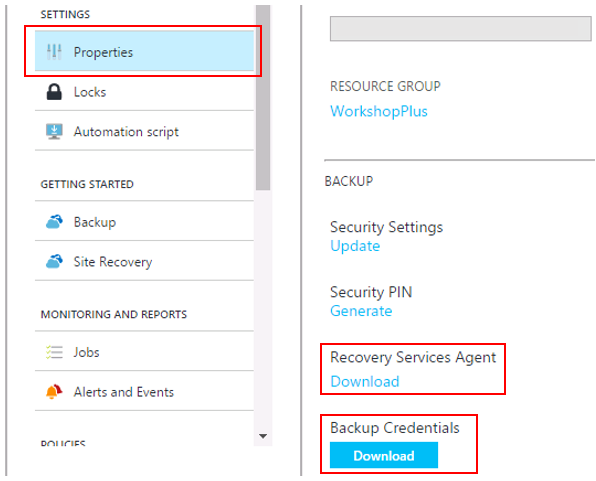
1. Log into AB-HOL-DPM1. Login name is AB-HOL-FABRIKAM\BkpAdmin1 and password is DPMDOMAIN~1
2. Launch Chrome Browser by clicking Chrome icon as shown below:



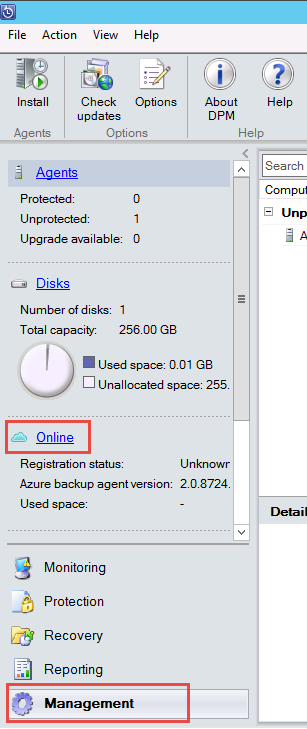
1. Navigate to Azure Management Portal, <https://portal.azure.com>
2. Login into your Azure Subscription
3. Use the new shortcut to Recovery Services Vaults and click on the SalesVault item in the resulting pane.



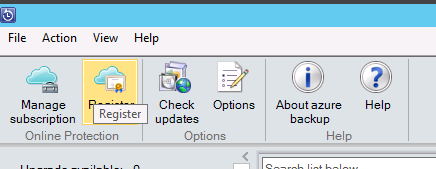
1. From the Properties item in the Settings section of the All Settings pane for the vault, you will see a backup section that allows you to download the Recovery Service Agent and the Backup Credentials file. Save both files to the Downloads folder on the DPM server.



1. On, AB-HOL-DPM1, **install** the downloaded agent (MARSAgentInstaller.exe). The installation process is similar to what was accomplished in exercise 1, however the Registration process using the vault credentials file is done differently.
2. **Open** the *System Center 2012 R2 DPM Administrator Console* shortcut located on the desktop.
3. In the *DPM Console*, **select** the *Management* pane and then **select** Online:



1. Next, **click** on *Register* on the top ribbon:

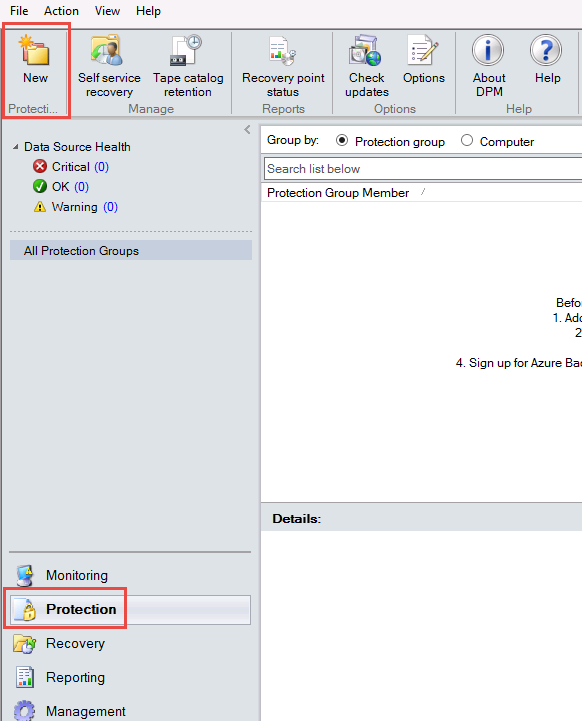


1. In the *Register Server Wizard*, **click** *Next* on the *Proxy Configuration* dialog.
2. In the *Backup Vault* dialog, **browse to** and **select** the vault credential you downloaded earlier.
3. In the *Throttling Setting* dialog, leave the defaults and **select** *Next.*
4. Using *File Explorer*, **create** a folder on the C:\ drive named *RecoveryTemp.*
5. In the *Recovery Folder* Settings dialog, **enter** *C:\RecoveryTemp* as the recovery folder and then **click** *Next*.
6. In the *Encryption Setting* dialog, **type** in or **generate** a passphrase and then click copy to Clipboard. Open Notepad, paste the clipboard contents and save the file to the Documents folder on the machine.
7. Click RegisterClick *Close* to close the *Register Server Wizard*

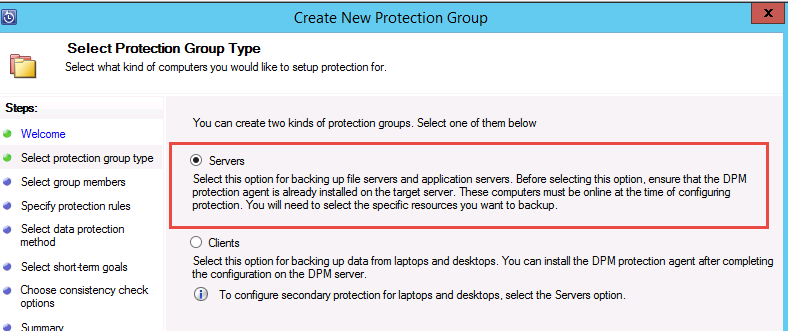
#### Configure Long Term Protection to Azure

This exercise will walk through the steps required to configure long term protection of an on-premises SQL database to Azure.

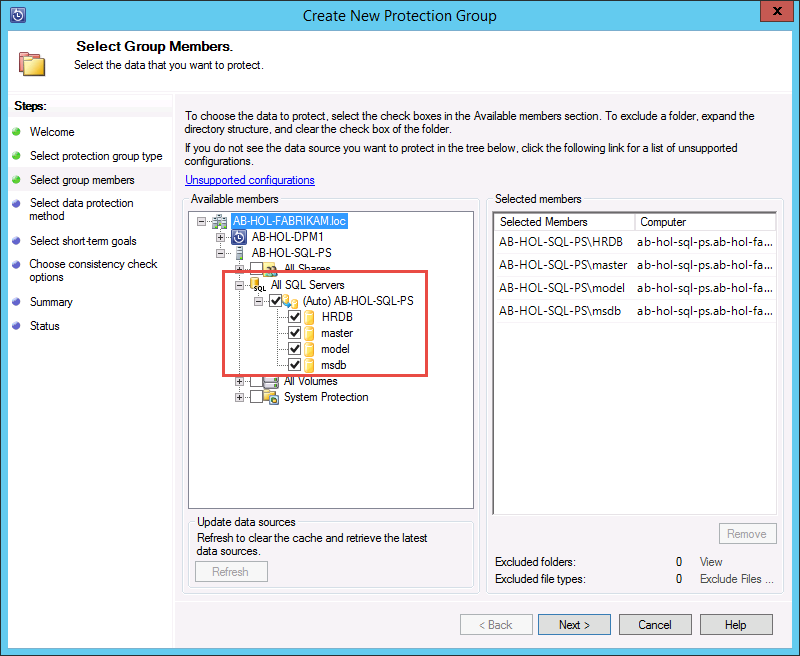
1. Log in to ‘**AB-HOL-DPM1’** server using credentials AB-HOL-FABRIKAM\BKBkpAdmin1, DPMDOMAIN~1
2. In the DPM server console, configure a new backup policy for SQL databases by creating a new Protection Group. Click on the **Protection** workspace.
3. Click on **New** icon in the main ribbon to create a new protection group.



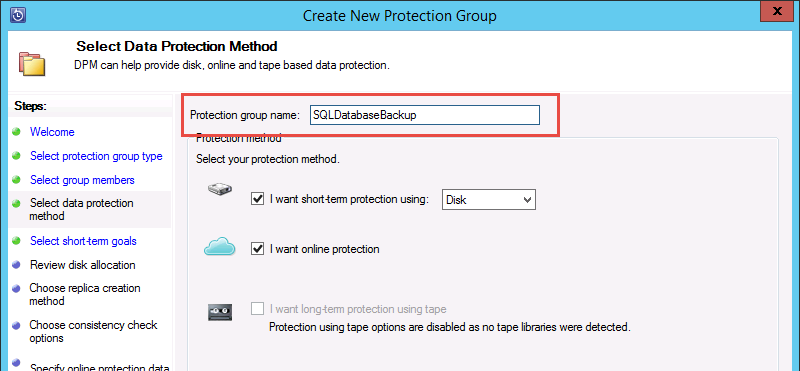
1. In the *Create New Protection Group* wizard, **click** *Next* on the *Welcome to the New Protection Group* dialog. In the *Select Protection Group Type* dialog, **select** *Servers* and then **click** *Next*



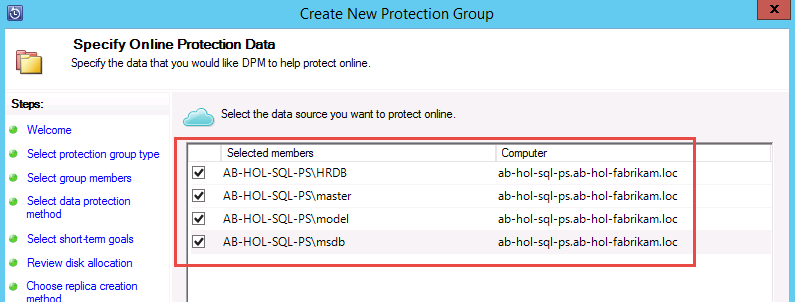
1. In the *Select Group Members* dialog, **expand** the AB-HOL-SQL-PS SQL server where the SQL databases to be backed up are installed. DPM shows various data sources that can be backed up from that server. **Expand** the All SQL Servers. Select the SQL databases to be backed up.
2. Ensure that the HRDB is selected as they would be required in the next exercise recovery scenarios when these databases are lost. **Click** *Next*.



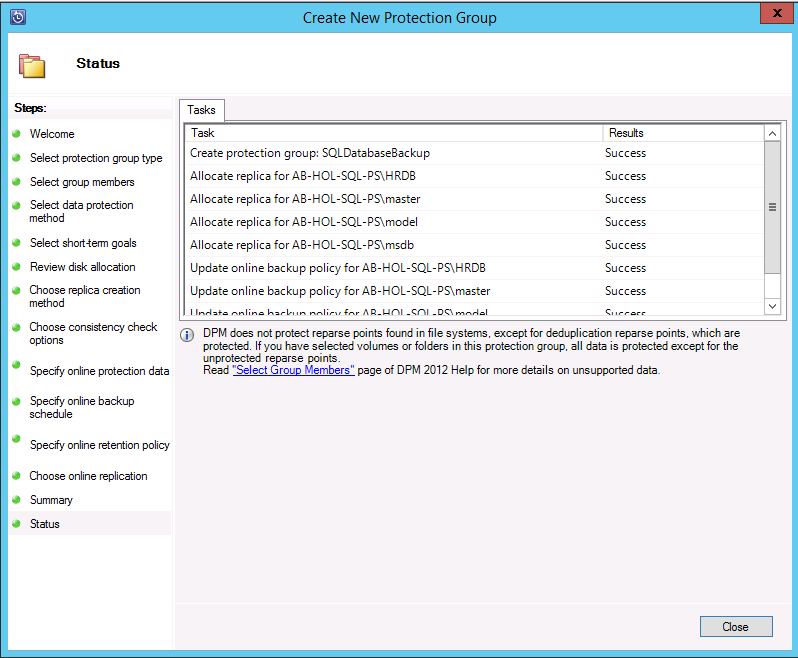
1. In the *Select Data Protection Method* dialog, **type** *SQLDatabaseBackup* as the name for the protection group you are going to create. Ensure “I want Online Protection” option is **selected** and **click** *Next*:



1. In the *Specify Short-Term Goals* dialog, accept the defaults and **click** *Next.*
2. In the *Review Disk Allocation* dialog, accept the defaults and **click** *Next.*
3. In the *Choose Replica Creation Method* dialog, accept the defaults and **click** *Next.*
4. In the *Consistency check options* dialog, accept the defaults and **click** *Next.*
5. In the *Specify Online Protection Data* dialog, **select** all members and then click *Next*:



1. In the *Specify Online Backup Schedule* dialog, accept the defaults and **click** *Next.*
2. In the *Specify Online Retention Policy* dialog, accept the defaults and **click** *Next.*
3. In the *Choose Online Replication* dialog, accept the defaults and **click** *Next.*
4. In *Summary* dialog, accept the defaults and **click** *Create Group.*
5. Watch the status and wait until the tasks have completed.



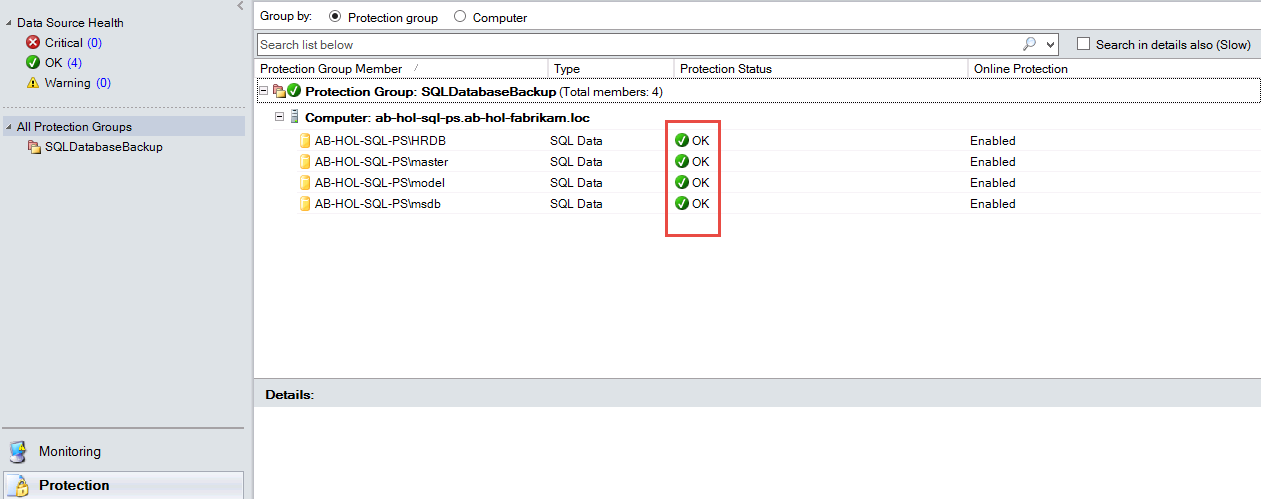
1. After the task have completed, the *Close* button is enabled. Click *Close* the end the *Create New Protection Group* wizard.

### Exercise 4: Restoring Databases using DPM and Microsoft Azure

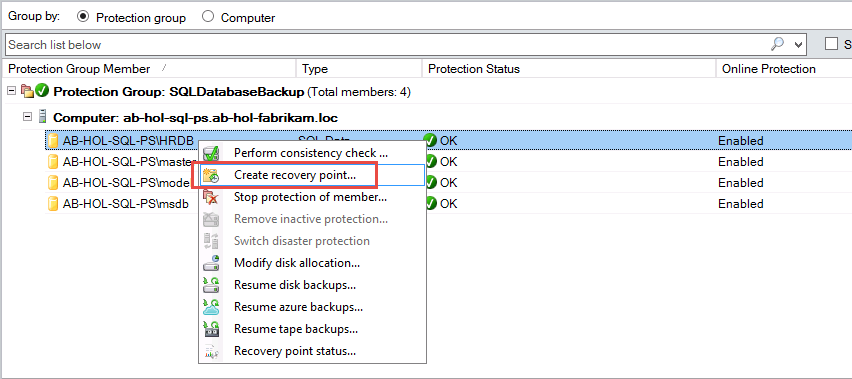
|  |  |
| --- | --- |
|  | The time to complete this module, including exercises, is 30 minutes. |
|  | The key takeaways from this lab are:   * Recovering Databases from Microsoft Azure using System Center Data Protection Manager |
|  |  |

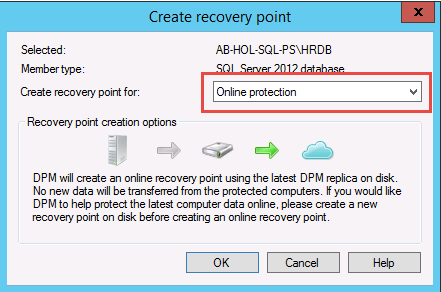
#### Manually Create a Recovery Point

While the previous exercise created a backup policy, a “recovery point” is created only when the first backup happens. Rather than waiting for the scheduler to kick in, this exercise walks through the steps required to trigger the creation of a recovery point manually.

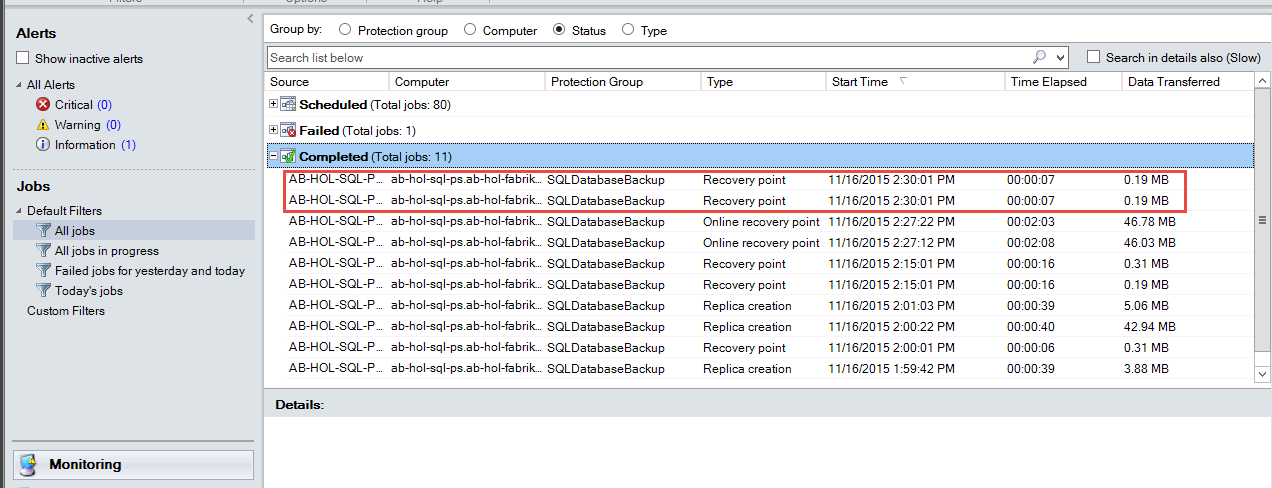


1. **Right-Click** on *AB-HOL-SQL-PS\HRDB* and **select** *Create Recovery Point*. **Choose** *Online Protection* in the drop down and **Click** *OK.* This starts the creation of a recovery point in Microsoft Azure.



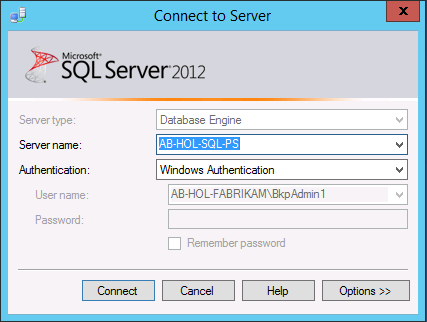


1. You can view the job progress in the Monitoring workspace. Wait for the job to finish before proceeding.

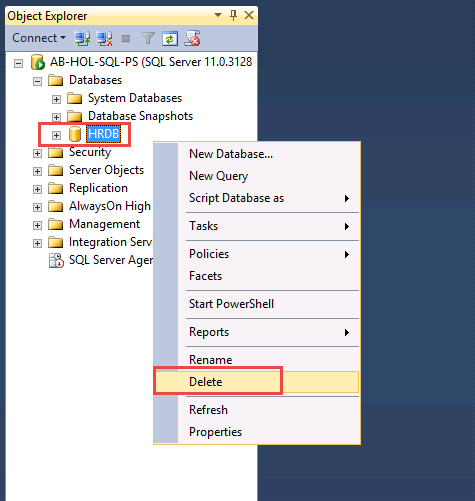


#### Delete the Database

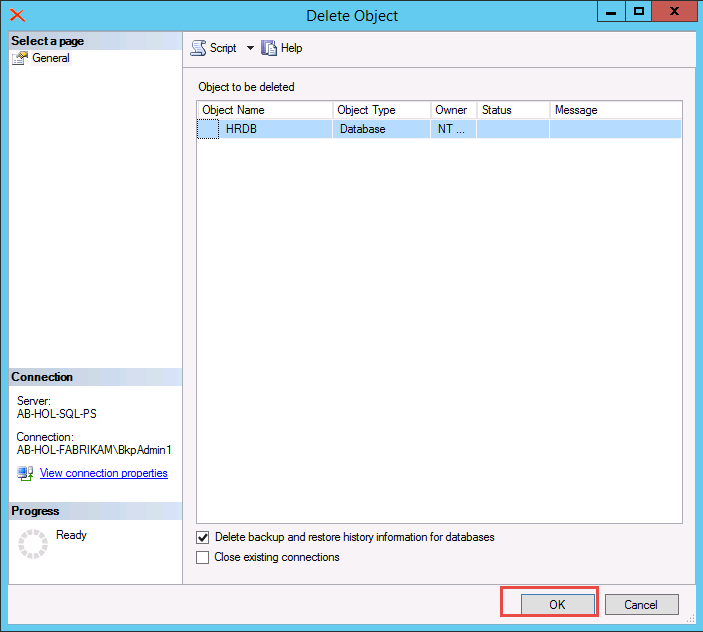
1. Before initiating a recovery workflow, let’s simulate a “disaster” by deleting the SQL database. To achieve this, **Login** to *AB-HOL-SQL-PS* Server.
2. Once you log in to the SQL server, search for *SQL Server Management Studio* and open the application. (***Note****: SQL Server Management Studio should be attached to the toolbar*.)
3. The *Connect to Server* dialog should look like this:



1. **Click** on *Connect.*
2. **Expand** *Databases* in the left-hand tree. Right-Click on the HRDB database and then **select** *Delete*.



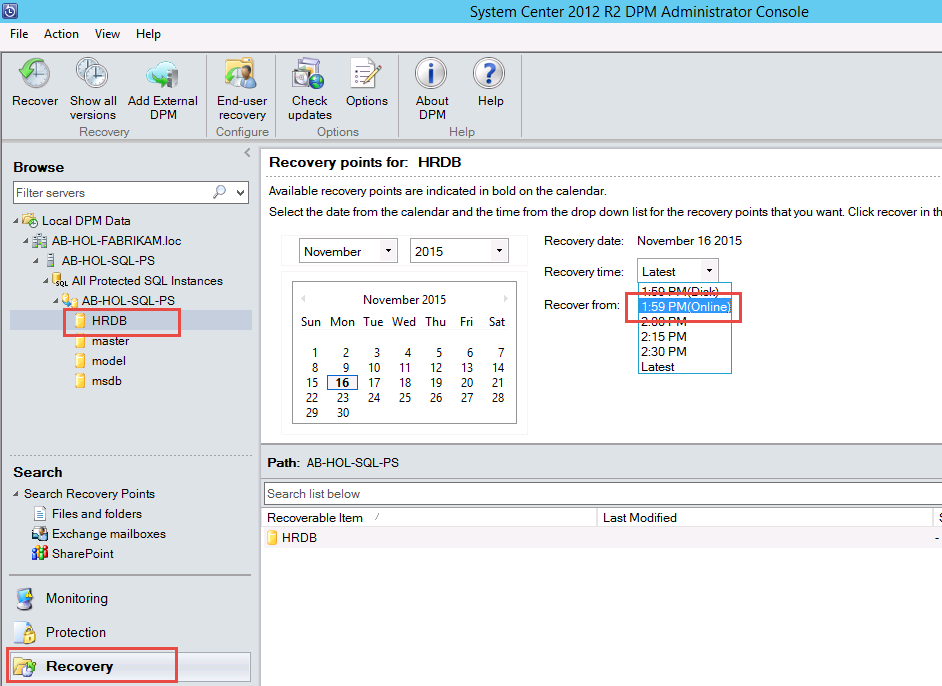
1. In the *Delete Object* dialog, **click** *OK.*



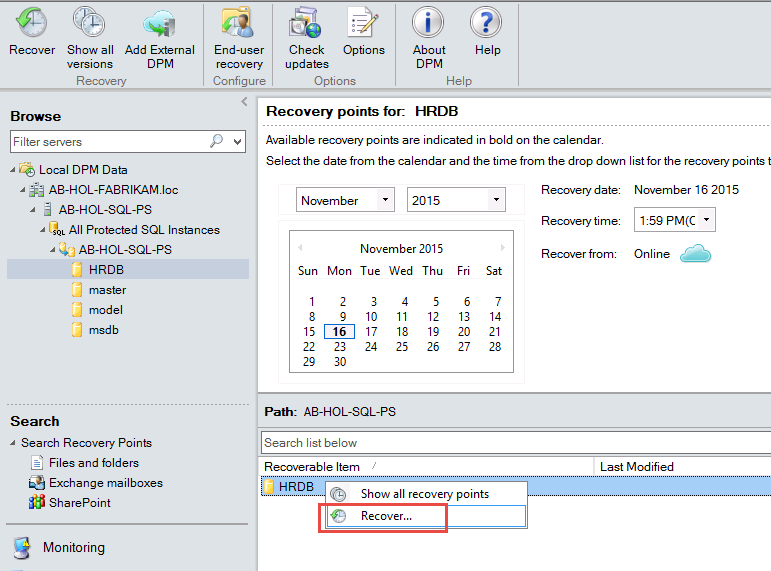
1. Verify that the database was deleted.

#### Recover the Database

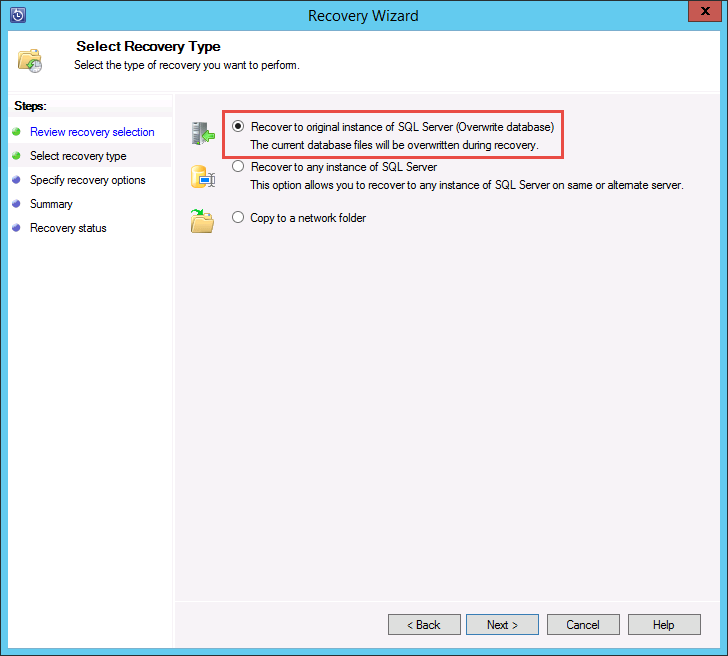
1. To initiate the recovery workflow, login to the DPM server **AB-HOL-DPM1**
2. In the DPM Console, **navigate** to the *Recovery* workspace where you will be able to see the servers backed up by DPM. Browse the database, HRDB. **Select** an entry in the *Recovery* *time* dialog box which has an entry which ends with (*Online)*.   
   After selecting such an entry the *Recover from:* indicator will refer to *Online* as well and will display a cloud icon.



1. **Right-click** on the *HRDB* database name and click *Recover*



1. In the *Recovery Wizard*, on the *Review Recovery Selection* dialog, **click** *Next.*
2. In the *Select Recovery Type* dialog, **select** *Recover to original instance of SQL Server (Overwrite database)* and then **click** *Next*.



1. In the *Specify Recovery Options* dialog, leave the defaults and **click** *Next*.
2. In the *Summary* dialog, review the selections and then **click** *Recover*.
3. Wait until recovery has completed. You might see an error that the replica is inconsistent. During a restore process, this is not usual. Ignore it until the restore is complete. Once the Recovery is complete, you can right click on the critical item and choose “Resume replication”. This will turn the critical item to a warning which will eventually go away once replication is operating correctly again.
4. After recovery is completed, you can log onto AB-HOL-SQL-PS and verify that the database has been recovered. (***Note****: You will have to refresh your view in SQL Server Management Studio in order to see the recovered database.*)

## Appendix A - Post-protection activities

### Installation of the backup extension

The Azure Backup service seamlessly handles the upgrade and patching of the backup extension without requiring any cumbersome user intervention. This relieves the user of the "agent management overhead" that is typically associated with backup products.

#### Offline VMs

The backup extension is installed if the VM is running. A running VM also provides the greatest chance of getting an application consistent point. However, the Azure Backup service will continue to back up the VM even if the VM is turned off and the extension could not be installed (aka Offline VM). The impact is seen in the consistency - in such a case the recovery point will be Crash consistent.

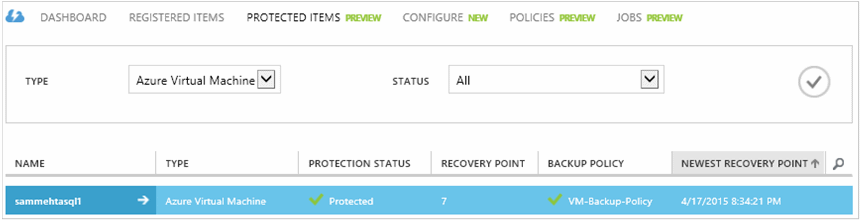
#### Initial backup

Once the virtual machine is protected with a policy, it shows up under the **Protected Items** tab with the status of Protected - (pending initial backup). By default, the first scheduled backup is the initial backup. In order to trigger the initial backup immediately after configuring protection, use the **Backup Now**button at the bottom of the **Protected Items** page.

The Azure Backup service creates a backup job for the initial backup operation. Click the **Jobs** tab to view the list of jobs. As a part of the backup operation, the Azure Backup service issues a command to the backup extension in each virtual machine to flush all writes and take a consistent snapshot.

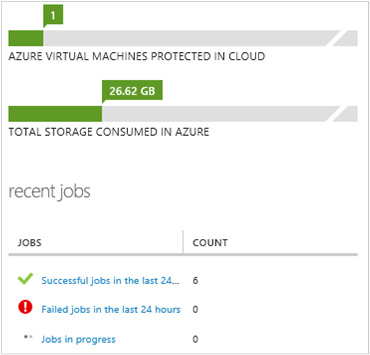


Once the initial backup is completed, the Protection Status of the virtual machine in the **Protected Items** tab will show as Protected.



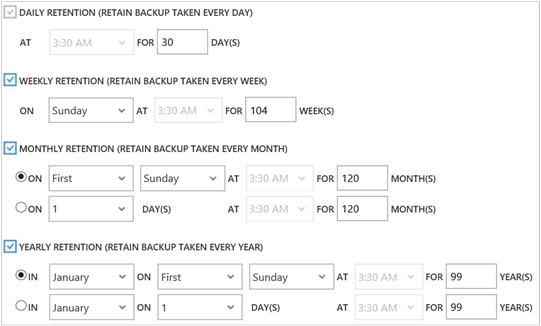
#### Viewing backup status and details

Once protected, the virtual machine count also increases in the **Dashboard** page summary. In addition, the **Dashboard** page shows the number of jobs from the last 24 hours that were successful, have failed, and are still in progress. Clicking on any one category will drill down into that category in the **Jobs**page.



#### Long term retention

Retention policy specifies the duration for which the backup must be stored. Rather than just specifying a “flat retention” for all backup points, customers can specify different retention policies based on when the backup is taken. For example, the backup point taken at the end of each quarter may need to be preserved for a longer duration for audit purposes while the backup point taken daily, which serves as an operational recovery point, needs to be preserved for 90 days.



1. **Daily retention policy**: Backups taken daily are stored for 30 days.
2. **Weekly retention policy**: Backups taken every week on Sunday will be preserved for 104 weeks
3. **Monthly retention policy**: Backups taken on the last Sunday of each month will be preserved for 120 months
4. **Yearly retention policy**: Backups taken on the first Sunday of every January will be preserved for 99 years.

## Appendix B - Consistency of recovery points

When dealing with backup data, customers worry about the behavior of the VM after it has been restored. The typical questions that customers ask are:

* Will the virtual machine boot up?
* Will the data be available on the disk (or) is there any data loss?
* Will the application be able to read the data (or) is the data corrupted?
* Will the data make sense to the application (or) is the data self-consistent when read by the application?

The following table explains the types of consistency that are encountered during Azure VM backup and restore.

| CONSISTENCY | VSS-BASED | EXPLANATION AND DETAILS |
| --- | --- | --- |
| Application consistency | Yes | This is the ideal place to be for Microsoft workloads as it ensures:   1. That the VM boots up. 2. There is no corruption. 3. There is no data loss. 4. The data is consistent to the application that uses the data, by involving the application at the time of backup - using VSS.   The Volume Snapshot Service (VSS) ensures that data is written correctly to the storage. Most Microsoft workloads have VSS writers that do workload-specific actions related to data consistency. For example, Microsoft SQL Server has a VSS writer that ensures the writes to the transaction log file and the database are done correctly.  For Azure VM backup, getting an application consistent recovery point means that the backup extension was able to invoke the VSS workflow and complete correctly before the VM snapshot was taken. Naturally, this means that the VSS writers of all the applications in the Azure VM have been invoked as well.  Learn the [basics of VSS](http://blogs.technet.com/b/josebda/archive/2007/10/10/the-basics-of-the-volume-shadow-copy-service-vss.aspx) dive deep into the details of [how it works](https://technet.microsoft.com/library/cc785914%28v=ws.10%29.aspx). |
| File system consistency | Yes - for Windows machines | There are two scenarios where the recovery point can be file-system consistent:   * Backup of Linux VMs in Azure, since Linux does not have an equivalent platform to VSS. * VSS failure during backup for Windows VMs in Azure.   In both these cases, the best that can be done is to ensure that:   1. The VM boots up. 2. There is no corruption. 3. There is no data loss.   Applications need to implement their own "fix-up" mechanism on the restored data. |
| Crash consistency | No | This situation is equivalent to a machine experiencing a "crash" (through either a soft or hard reset). This typically happens when the Azure virtual machine is shut down at the time of backup. For Azure virtual machine backup, getting a crash-consistent recovery point means that Azure Backup gives no guarantees around the consistency of the data on the storage medium - either from the perspective of the operating system or from the perspective of the application. Only data that already exists on the disk at the time of backup is what gets captured and backed up.   While there are no guarantees, in most cases the OS will boot. This is typically followed by a disk checking procedure like chkdsk to fix any corruption errors. Any in-memory data or writes that have not been completely flushed to the disk will be lost. The application typically follows with its own verification mechanism in case data rollback needs to be done. For Azure VM backup, getting a crash consistent recovery point means that Azure Backup gives no guarantees around the consistency of the data on the storage - either from the OS perspective or the application's perspective. This typically happens when the Azure VM is shut down at the time of backup.  As an example, if the transaction log has entries that are not present in the database, then the database software does a rollback till the data is consistent. When dealing with data spread across multiple virtual disks (like spanned volumes), a crash-consistent recovery point provides no guarantees for the correctness of the data. |