WorkshopPLUS

Microsoft Azure Infrastructure as a Service (IaaS)

Introduction to Microsoft Recovery Services

Student Lab Manual

V1.3, October 31, 2016

Information in this document is subject to change without notice. The example companies, organizations, products, people, and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred. 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, trademarked, 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.

© 2010 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, MS, Windows, Windows NT, MSDN, Active Directory, BizTalk, SQL Server, SharePoint, Outlook, PowerPoint, FrontPage, Visual Basic, Visual C++, Visual J++, Visual InterDev, Visual SourceSafe, Visual C#, Visual J#,  and Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

Other product and company names herein may be the trademarks of their respective owners.

Contents

[Introduction to Microsoft Azure Recovery Services 4](#_Toc465866085)

[Prerequisites 4](#_Toc465866086)

[Overview 4](#_Toc465866087)

[Exercise 1 - Azure Recovery Services (ARM) 5](#_Toc465866088)

[Task 1 - Creating a Recovery Services vault 5](#_Toc465866089)

[Task 2 – Set Storage replication 5](#_Toc465866090)

[Task 4 – Performing the Initial Backup 8](#_Toc465866091)

[Exercise 2 - Azure Recovery Services - Files/Folders 10](#_Toc465866092)

[Task 1 – Installing backup agent on Azure VM 10](#_Toc465866093)

[Task 2 - Restore data from Azure 15](#_Toc465866094)

[Restoring Domain Controller VMs 17](#_Toc465866095)

[Single DC 17](#_Toc465866096)

[Multiple DCs 17](#_Toc465866097)

# Introduction to Microsoft Azure Recovery Services

In this lab, you will create a recovery vault to protect files, folders and an ARM Azure virtual machine.

You'll learn:

* How to create an Azure Recovery Services vault
* How to backup ARM VMs using the Azure portal https://portal.azure.com
* How to protect local Windows files to Azure
* How to protect Azure virtual machines

## Prerequisites

The following is required to complete this hands-on lab:

* [Web](http://www.microsoft.com/windowsazure/sdk/) browser
* Windows client or server machine
* Two pre-created Azure ARM VMs
* A Microsoft Azure subscription

## Overview

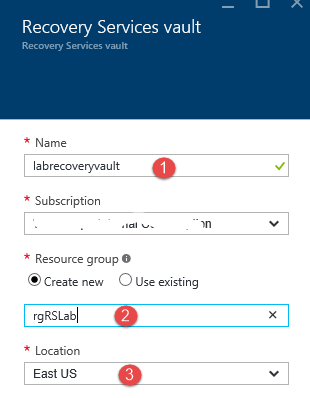
With a Recovery Service vault, you are able to protect:

* Azure Resource Manager (ARM) VMs
* Classic VMs
* Standard Storage VMs
* Premium Storage VMs

# Exercise 1 - Azure Recovery Services (ARM)

## Task 1 - Creating a Recovery Services vault

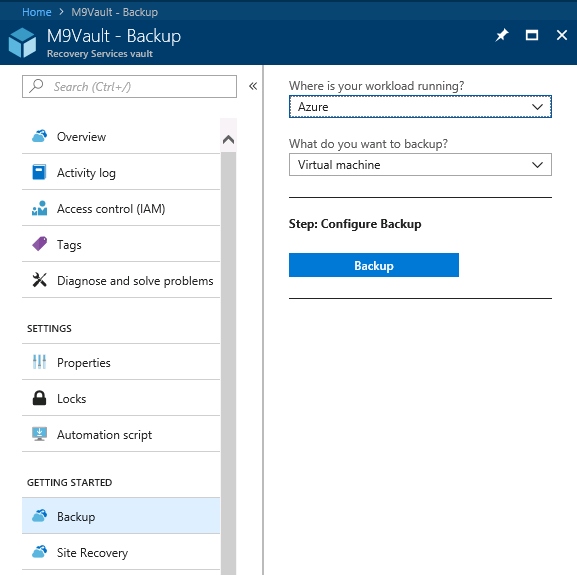
1. Navigate to https://portal.azure.com and logon to your Azure subscription.
2. Choose **+Create a resource | Monitoring + Management | Backup and Site Recovery (OMS).**
3. Configure the Recovery services vault as follows:
   1. Enter the name of your Recovery Services vault
   2. Enter the name of a new resource group
   3. Enter your selection of location



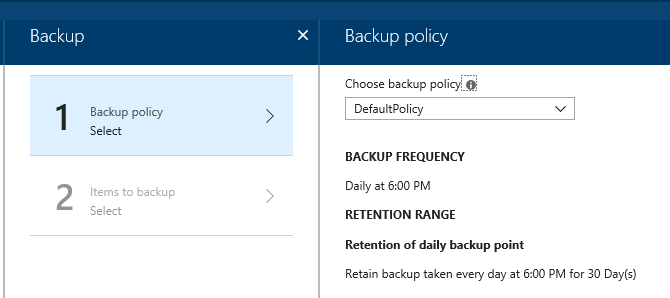
1. Click

## Task 2 – Set Storage replication

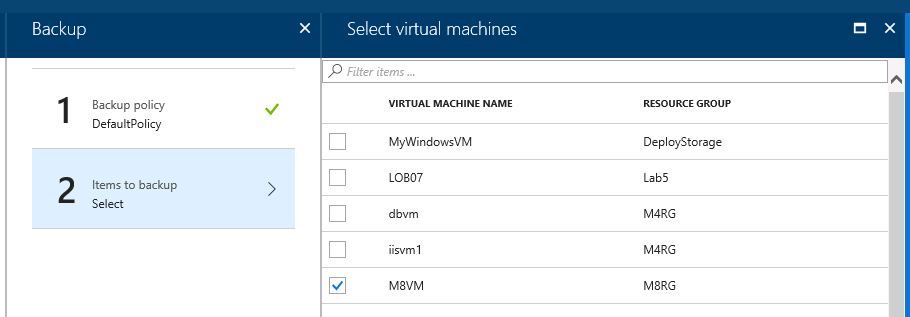
1. Open the resource group that you created for your vault.
2. In the resource group blade, click on your vault name.
3. When your vault blade opens, scroll down to the *GETTING STARTED* area and select the **Backup** menu item. Leave the settings as they are (*Azure* and *Virtual Machine*). Click **Backup**.



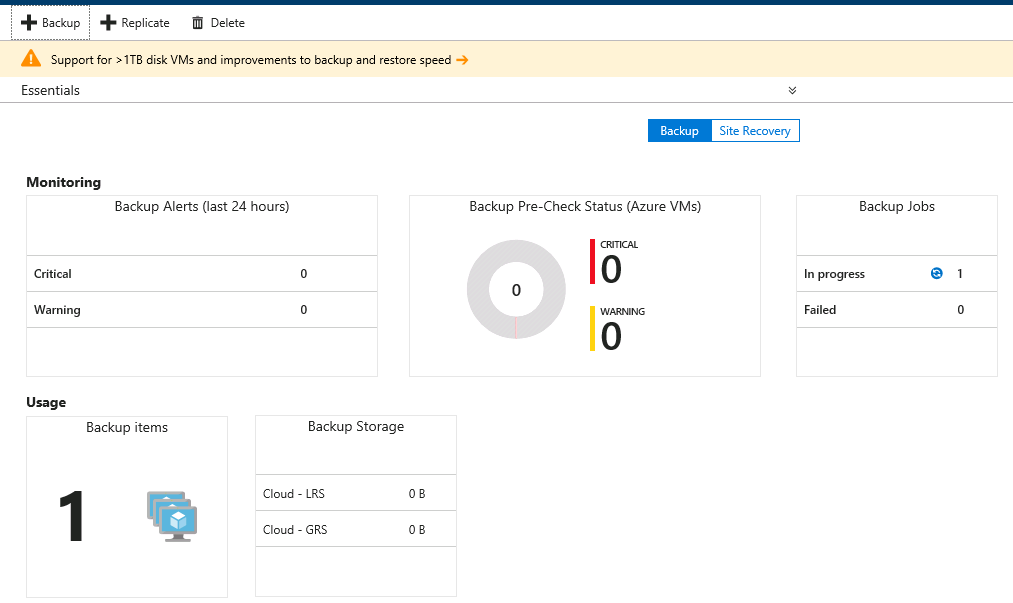
1. Select **Backup policy** and leave the settings as they are.



1. In the *Backup policy* blade, click
2. Select **Items to backup** and then select the VM(s) that you plan to back up. For lab purposes, you can choose one of the two VMs that you created as a pre-requisite to the lab.



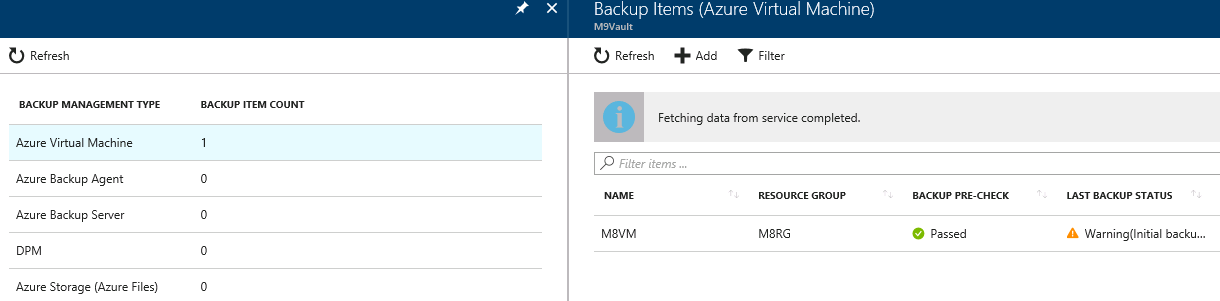
1. On the *Select virtual machines* blade, click**OK**
2. On the *Backup* blade, click the **Enable backup** button .
3. On the *Recovery Services Vault* blade, click **Overview**. You will see that the backup configuration is in progress.



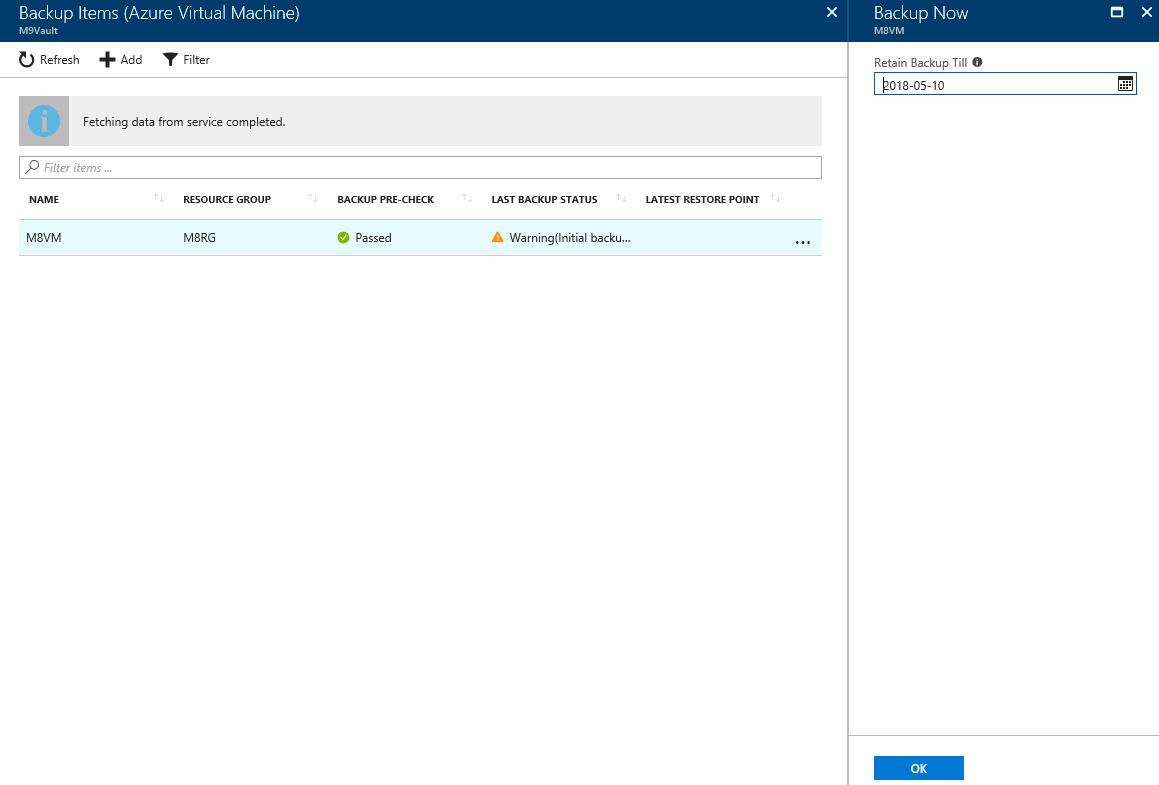
## Task 4 – Performing the Initial Backup

Once a backup policy has been deployed on the virtual machine, that does not mean the data has been backed up. By default, the first scheduled backup (as defined in the backup policy) is the initial backup. Until the initial backup occurs, the *Last Backup Status* on the *Backup Items* blade will show as *Warning (initial backup pending)*.

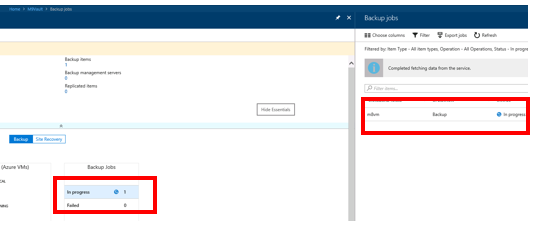
1. In the vault blade, scroll down to the *PROTECTED ITEMS* area and click **Backup items**.
2. In the right blade, under *BACKUP MANAGEMENT TYPE*, click on the **Azure Virtual Machine** link. This will open up the *Backup Items (Azure Virtual Machine)* blade.



1. Over to the right of the item that you had previously chosen to back up, select the ‘**…**’ *ellipse* and then select **Backup now.**  Click **OK**.



1. If you go back to the *Overview* blade of the Recovery Services vault, you will be able to see the running *Backup Jobs*. You can click on it to get a status for the Backup Job.



# Exercise 2 - Azure Recovery Services - Files/Folders

## Task 1 – Installing backup agent on Azure VM

If you have not already created a recovery services vault, go back to Exercise 1 to perform that task. Although we could point to an on-premises machine to get a backup of files and folders, instead we can do the same thing with a machine that is in Azure.

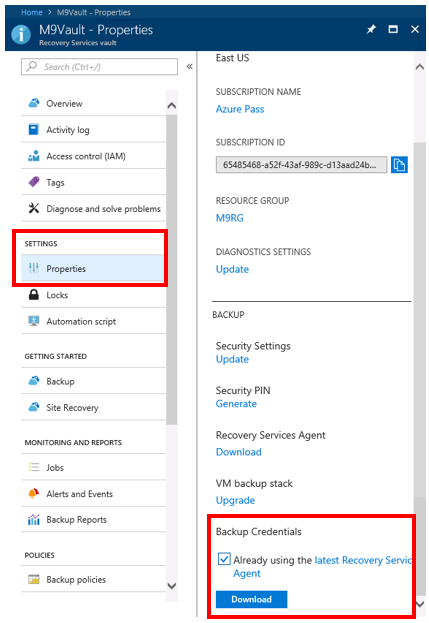
1. Choose any VM that you currently have running in Azure that DOES NOT already have the backup agent running on it (in other words, don’t use the same machine you backed up in Exercise 1).
2. Remote desktop in to this VM.
3. Open **Internet Explorer** on the machine you RDP’ed in to.

Note that you may have to turn off security for IE. You can do this by going in to the **Server Manager** and selecting **Local Server | IE Enhanced Security Configuration**.

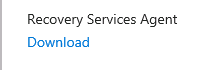
1. From inside of the machine you RDP’ed in to, log in to Azure at https://portal.azure.com.
2. Go to the resource group that contains your recovery services vault and then click on your recovery services icon. When you do this the vault blade will open.

Scroll down to the *SETTINGS* area and click on the **Properties** link.

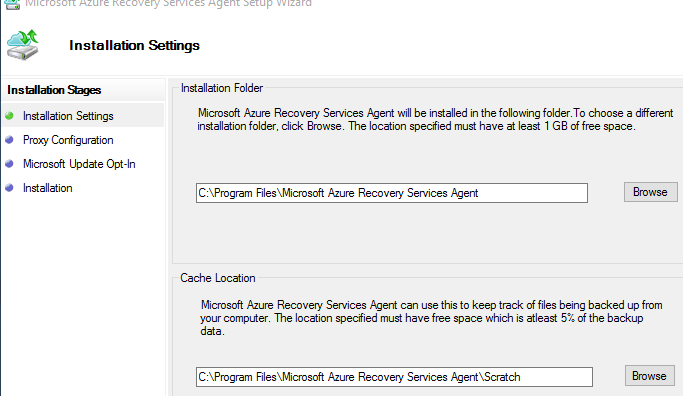
Download the **Backup Credentials** to your machine by selecting the checkbox and clicking on **Download**. These credentials are needed when you install the backup client on the machine you want to protect. Save this file to your desktop.



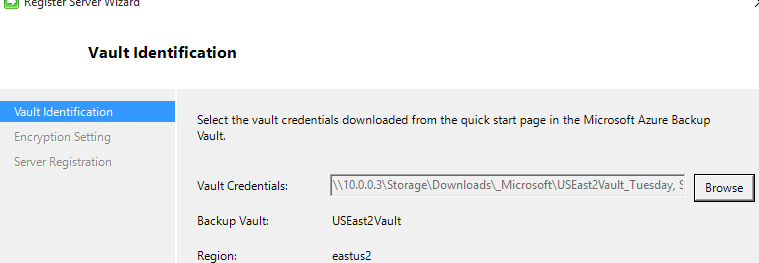
1. Next, click on the **Download** link for the **Recovery Services Agent** and download this file to your machine. This will download a file named MARSAgentInstaller.exe.



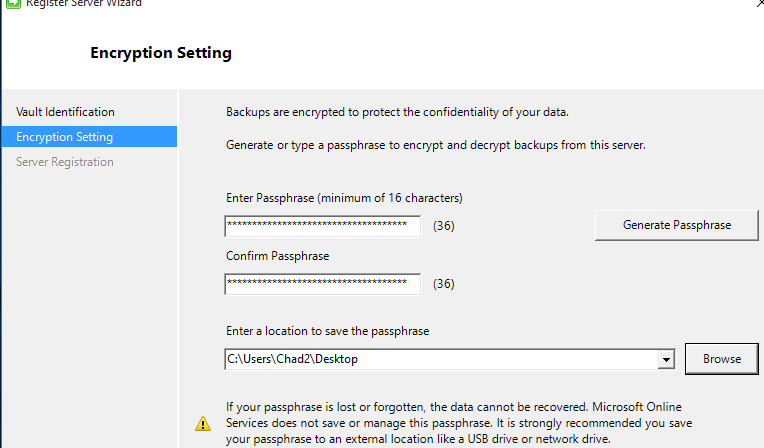
1. Install the **MARSAgentInstaller.exe** client on the machine you wish to backup. Accept UAC prompts for the software. Select an installation location and a cache location. For the lab exercise, you can just choose all the default settings.



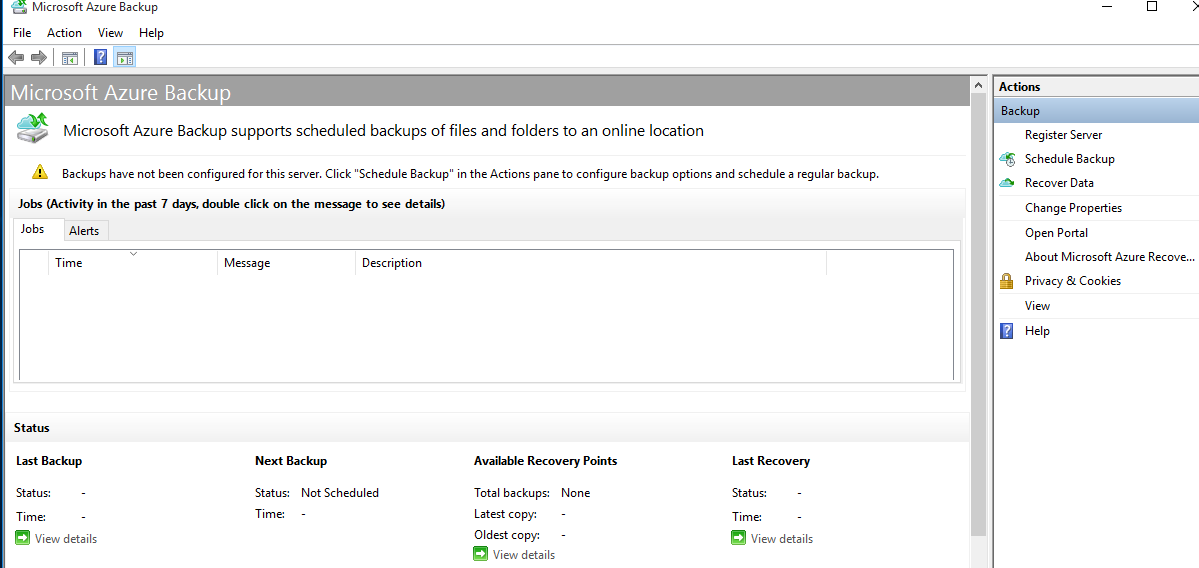
1. Click the **Proceed to Registration** button.
2. Click **Browse** and select the vault credentials file downloaded from the portal.



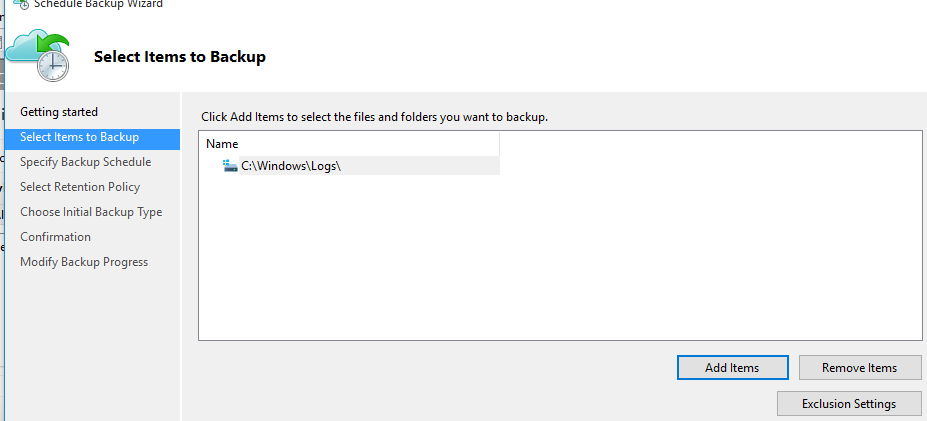
1. Click **Next**.
2. Either enter a passphrase or generate a passphrase. This is used to encrypt your data in Azure and needs to be very strong (at least 16 characters). Browse and enter a location to save the passphrase and keep that file in a safe place (Bitlocker encrypted drive for instance or Azure Key Vault storage).



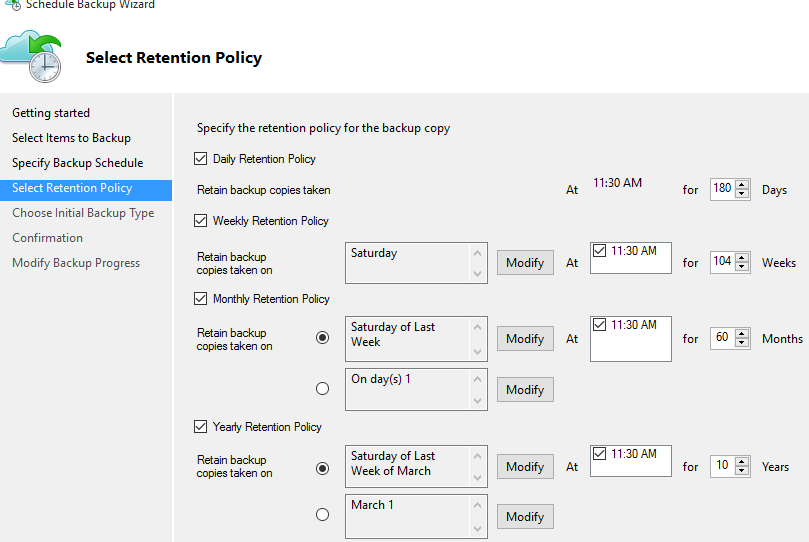
1. Make sure the **Launch Microsoft Azure Recovery Service Agent** checkbox is checked and then click the **Close** button.
2. In the *Microsoft Azure Recovery Services Agent* console, click the **Schedule Backup** link on the right side.



1. Click **Next** on the getting started screen.
2. You can add items (files, folders) to backup. You can also set exclusion settings to exclude certain files or folders. Click **Add Items** and add some files.



1. Click **Next**.
2. You can create a schedule for backing up the data (either daily or weekly, up to 3 times per day). Set a daily schedule some time in the future and click **Next**.
3. The data that is backed up can be retained. View the default retention policy. You can set daily, weekly, monthly and yearly policies for retaining data. Click **Next**.



1. Choose the initial backup type.
2. On the *Choose Initial Backup Type*… choose “*Automatically over the network*”. This will back up the files over the Internet to Azure.

If you want to backup locally and send the data to a physical drive, you would select Offline backup and enter the settings. Click the “here” link for more information on how to create the offline backup and shipping instructions.

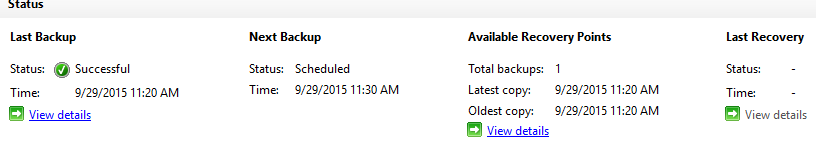
1. Click **Next**.
2. Click **Finish**.
3. You could wait for the backup to occur at the scheduled time; however, for this lab you should click the **Back Up Now** button on the *Actions* pane (right side).
4. Wait for the backup to complete before continuing.

## Task 2 - Restore data from Azure

1. On the desktop of the VM that you have RDP’ed into, there should be a Microsoft Azure Backup icon. Start the **Microsoft Azure Backup** application, if it is not already running.



1. You should have a previously successful backup listed in the status and at least 1 total backups listed.



1. Click the **Recover Data** link on the *Actions* pane (right side).
2. If running the restore to the same computer, select **This Server** on the *Getting Started* screen. Otherwise choose **Another Server**.
3. Click **Next**.
4. On the *Select Recovery Mode* screen, select **Individual files and folders** and click **Next**.
5. Select the Volume to recover and click **Mount**.
6. Click **Browse**.
7. Browse or search for the files you want to restore. Copy/Paste the files to the location where you want them restored.

