

Azure Backup Hands-on lab

-Microsoft Azure



November 1, 2017

Version 1.0

Prepared by

Gino van Essen & Gido Veekens
Technical Cloud Consultants – Copaco Nederland

Contributors

Gino van Essen
Gido Veekens

Document Revision

Change Record

Date	Author	Version	Change Reference
November 1, 2017	Gido Veekens	0.1	

Reviewers

Name	Version Approved	Position	Date
Gino van Essen	0.1		November 3, 2017

Table of Contents

Document Revision	2
Change Record	2
Introduction	4
Objectives.....	4
Activity 1: Getting Started.....	4
Objectives.....	4
Exercise 1: Connect to Azure.....	5
Exercise 2: Create a Virtual Machine	6
Exercise 3: Create a Recovery Vault.....	9
Activity 2: Backup & Recovery.....	11
Exercise 1: Create a backup of your files	11
Exercise 2: Create a backup of your Virtual Machine	16
Exercise 2: Perform a recovery of your Files and Folders	20
Exercise 3: Perform a recovery of your VM files	21
Activity 3: Clean-up	24

Introduction

Azure Backup is a simple and reliable cloud integrated backup as a service. In this lab, you will learn how to create an Azure Backup Vault, and then use this vault to backup files and system state from a Windows client device. You will then restore the backup-up files

Estimated time to complete this lab

75 minutes

Objectives

During this lab, you will learn how to get started on Azure with Azure Backup to;

- Set-up your tenant using your Azure Pass.
- Create and manage Resource Groups and Storage Accounts
- Deploy a Recovery Vault
- Create a files backup job
- Create a VM backup job
- Restore items from your Recovery Vault

Prerequisites

- Laptop/computer with Internet browser and WiFi connected
- Microsoft Account without an Azure Subscription

Activity 1: Getting Started

Estimated time to complete this activity

15 minutes

Objectives

In this activity, you will validate the necessary access to perform this lab

- Create your Microsoft account if necessary
- Activate your Azure Pass
- Create your Azure tenant
- Create a Resource Group
- Create a basic Virtual Machine

After verifying your access, you will use the Azure tenant to create a Recovery Vault you can use to store your backups.

Exercise 1: Connect to Azure

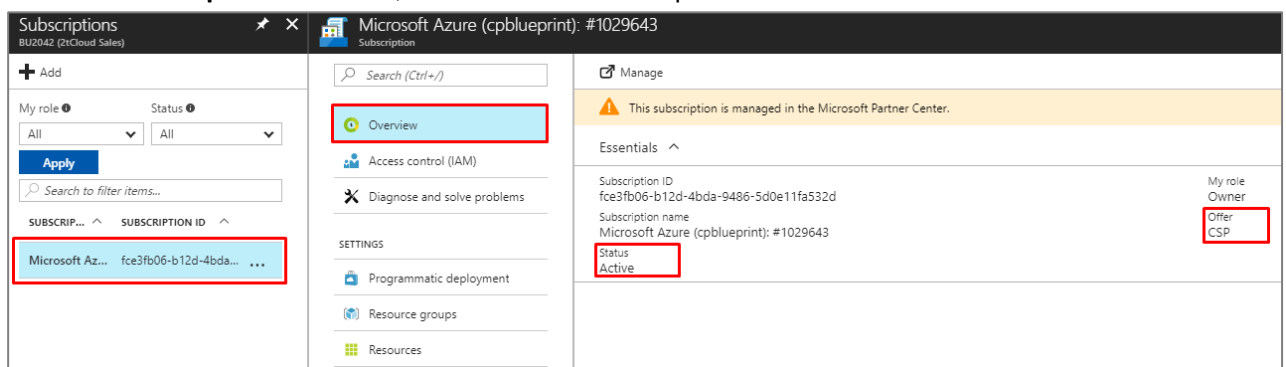
Please make sure you have a Microsoft Account which you haven't been used before with any Azure Subscription. If you don't have one, please create a new Microsoft Account;

<https://account.microsoft.com/>

You will receive an Azure pass which can be activated by browsing to the following website and follow instructions;

<https://www.microsoftazurepass.com>

1. Using your **Microsoft Account**, you can sign in to the **Azure Portal** at;
<https://portal.azure.com>
2. Using the navigation bar on the left, use the **More Services** menu to browse to the **Subscriptions** pane. The **Search** filter on the top will help you to find what you need.
3. From the **Subscriptions** overview, click the active subscription.

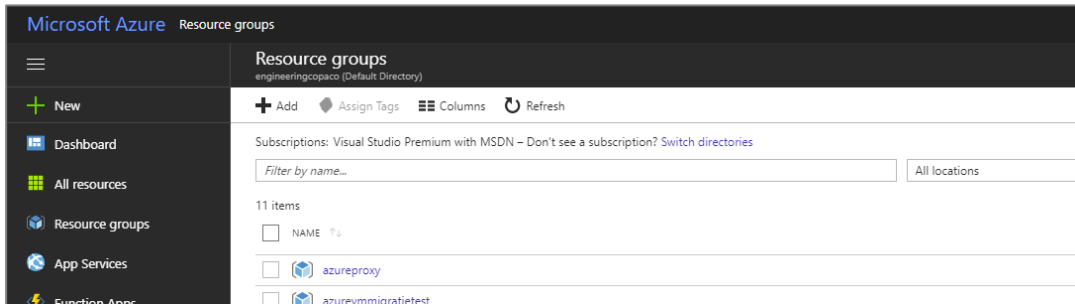


4. In the **Overview** pane, check the **Offer** type for being either Azure Pass, CSP or MSDN.
5. Check the **Status** for being Active.

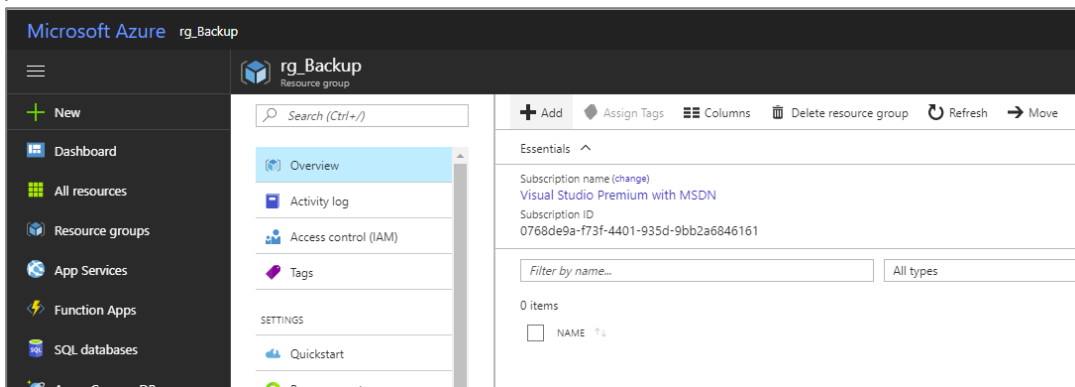
★ We also strongly recommend that you use InPrivate browsing to ensure that you are not automatically logged on with other credentials during the registration / activation process.

Exercise 2: Create a Virtual Machine

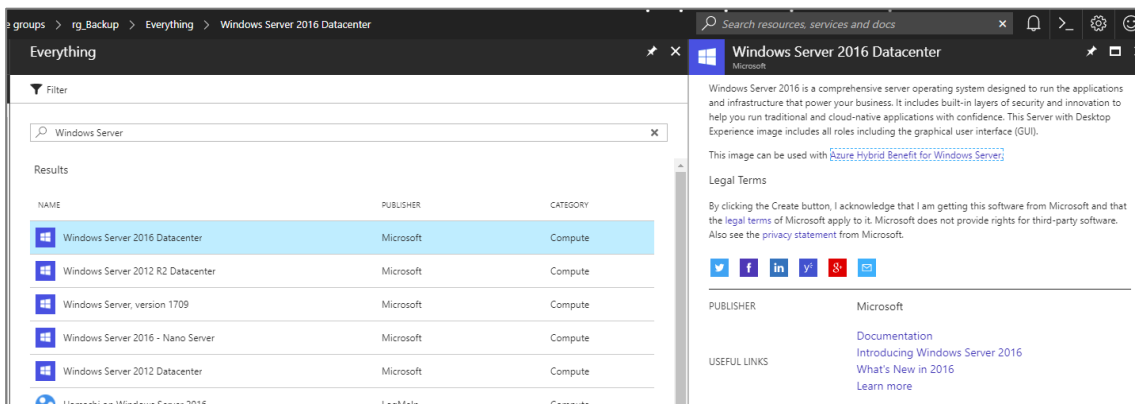
1. Using the **Navigation Pane** on the right, open the **Resource Groups**.



2. Add a new **Resource Group** using your **Azure Pass Subscription** and **West Europe** as the location.
3. After a few moments, the Resource Group is available. By opening it, you'll be presented with the **Overview** pane. From there, click **Add**



4. From the search box, search for **Windows Server** and select **Windows Server 2016 Datacenter**.



5. Fill in the **Basic** settings. Please make sure you select the **Resource Group** created before.

Create virtual machine

×

Basics

Configure basic settings

2

Size

Choose virtual machine size

3

Settings

Configure optional features

4

Summary

Windows Server 2016 Datacent...

Basics

☐

* Name

srvTest

✓

VM disk type

HDD

▼

* User name

adminuser

✓

* Password

✓

* Confirm password

✓

Subscription

Visual Studio Premium with MSDN

▼

* Resource group

☐ Create new
 ☒ Use existing

rg_Backup

▼

* Location

West Europe

▼

Save money

Save up to 40% with a license you already own.

* Already have a Windows Server license?

6. Click OK and as the machine size, select the **D2S_V3 Standard** size.

Choose a size

☐

Browse the available sizes and their features

Prices presented are estimates in your local currency that include only Azure infrastructure costs and any discounts for the subscription and location. The prices don't include any applicable software costs. If the virtual machine is currently running, changing its size will cause it to be restarted.

Supported disk type

HDD

▼

Minimum vCPUs

1

Minimum memory (GiB)

0

D2S_V3 Standard	D4S_V3 Standard	D8S_V3 Standard
2 vCPUs	4 vCPUs	8 vCPUs
8 GB	16 GB	32 GB
4 Data disks	8 Data disks	16 Data disks
4000 Max IOPS	8000 Max IOPS	16000 Max IOPS
16 GB Local SSD	32 GB Local SSD	64 GB Local SSD
Premium disk support	Premium disk support	Premium disk support
Load balancing	Load balancing	Load balancing
75,29 EUR/MONTH (ESTIMATED)	150,58 EUR/MONTH (ESTIMATED)	301,16 EUR/MONTH (ESTIMATED)
D16S_V3 Standard	D32S_V3 Standard	D64S_V3 Standard
16 vCPUs	32 vCPUs	64 vCPUs
64 GB	128 GB	256 GB
32	32	32

7. You will be asked for optional features, you can leave them default and proceed

1 Basics Done ✓

2 Size Done ✓

3 Settings Configure optional features >

4 Summary Windows Server 2016 Datacent... >

High availability

* Availability set ⓘ >

None

Storage

Use managed disks ⓘ

No Yes

Network

* Virtual network ⓘ >

(new) rg_Backup-vnet

* Subnet ⓘ >

default (10.0.1.0/24)

* Public IP address ⓘ >

(new) srvTest-ip

* Network security group (firewall) ⓘ >

(new) srvTest-nsg

Extensions

Extensions ⓘ >

No extensions

Auto-shutdown

Enable auto-shutdown ⓘ

Off On

Shutdown time ⓘ

19:00:00

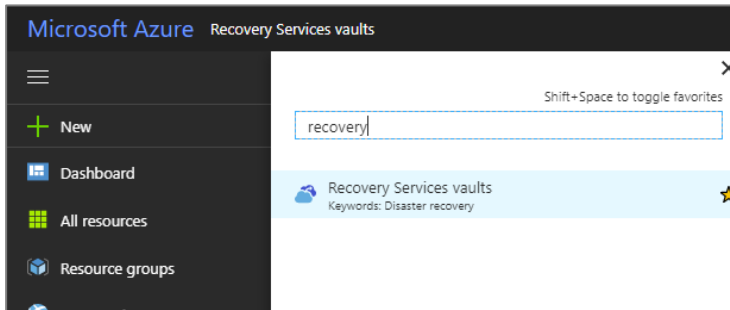
Time zone ⓘ

(UTC+01:00) Amsterdam, Berlin, Bern, ... ▼

8. Review the summary and **Create** the VM. You can check the status from the **Notifications** in the top bar on the right. We will come back later, when the machine is finished deploying.

Exercise 3: Create a Recovery Vault

1. From the navigation pane, click **More Services** and search for **Recover**



2. [Optional] Click the star to attach the Recovery Services Vault to the navigation pane for quick access
3. Click Create Recovery Services Vault and fill in the parameters. Make sure you select the existing Resource Group we just created.

The screenshot shows the 'Recovery Services vault' creation form. The fields are as follows:

- Name:** rsvBackup (with a green checkmark)
- Subscription:** Visual Studio Premium with MSDN (dropdown)
- Resource group:** rg_Backup (dropdown, with radio buttons for 'Create new' and 'Use existing', where 'Use existing' is selected)
- Location:** West Europe (dropdown)

4. Wait for the Vault to get deployed. You can check the status from the **Notifications** in the top bar.
5. Open the **Recovery Services Vault** when it's ready, the **Overview** pane will show a dashboard

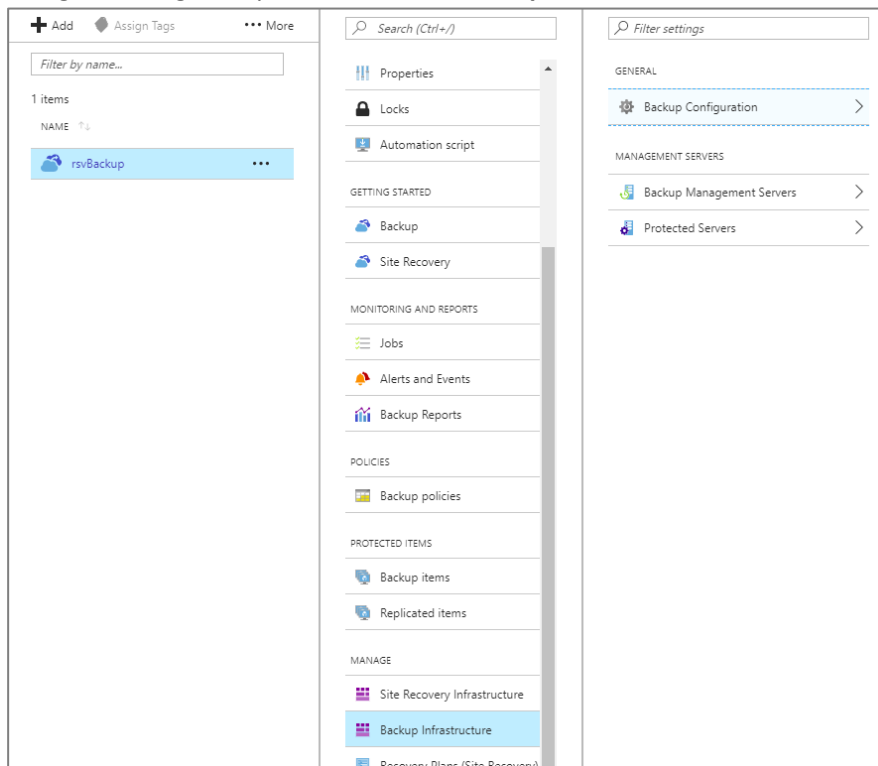
The screenshot shows the 'Recovery Services vault' overview dashboard. The left pane shows a list of items with 'rsvBackup' selected. The middle pane shows a navigation menu with options like 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'SETTINGS', 'Properties', 'Locks', 'Automation script', 'GETTING STARTED', 'Backup', and 'Site Recovery'. The right pane shows the 'Overview' dashboard with the following information:

- Resource group (change):** rg_Backup
- Status:** Active
- Location:** West Europe
- Subscription name (change):** Visual Studio Premium with MSDN
- Subscription ID:** 0768de9a-f73f-4401-935d-9bb2a6846161
- Backup items:** 0
- Backup management servers:** 0
- Replicated items:** 0

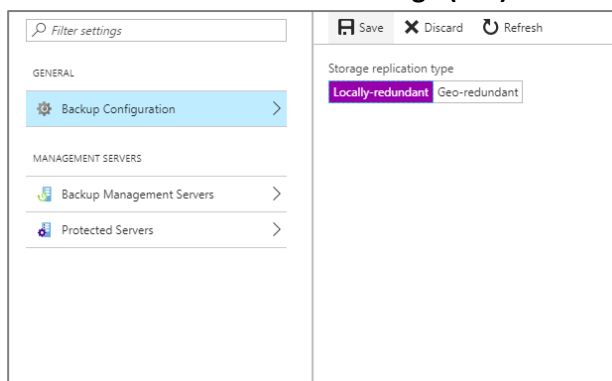
Below this information is a 'Monitoring' section with two panels:

- Backup Alerts (last 24...):** A table showing 0 Critical and 0 Warning alerts.
- Backup Pre-Check Status (Azure VMs):** A circular gauge showing 0 TOTAL, with 0 CRITICAL and 0 WARNING.

6. Using the navigation pane, browse to **Backup Infrastructure** and then **Backup Configuration**.



7. Make sure **Local Redundant Storage (LRS)** is selected. Click **Apply**.



8. You're done, we have created a Recovery Services Vault we can use to store our backups.

Activity 2: Backup & Recovery

Estimated time to complete this activity

60 minutes

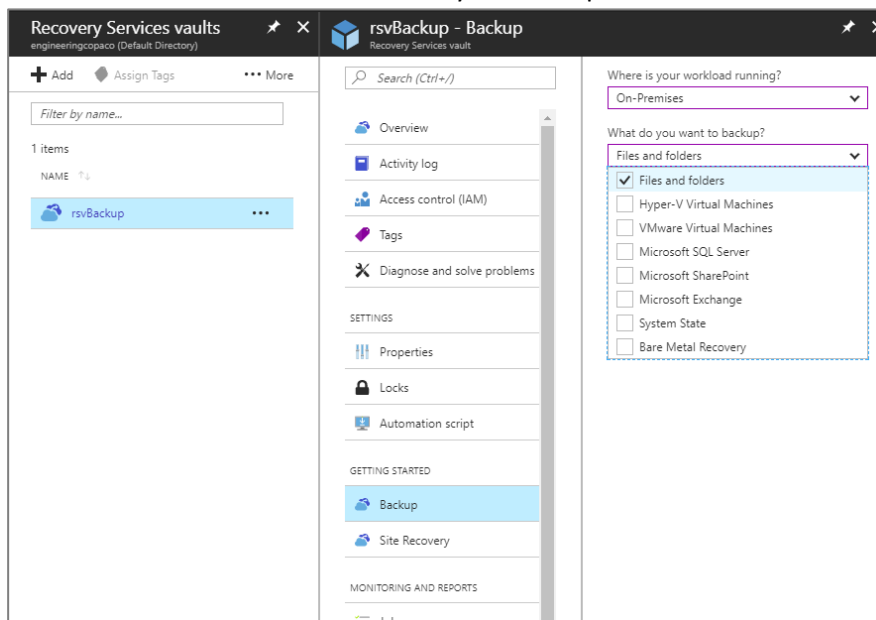
Objectives

In this activity, you will;

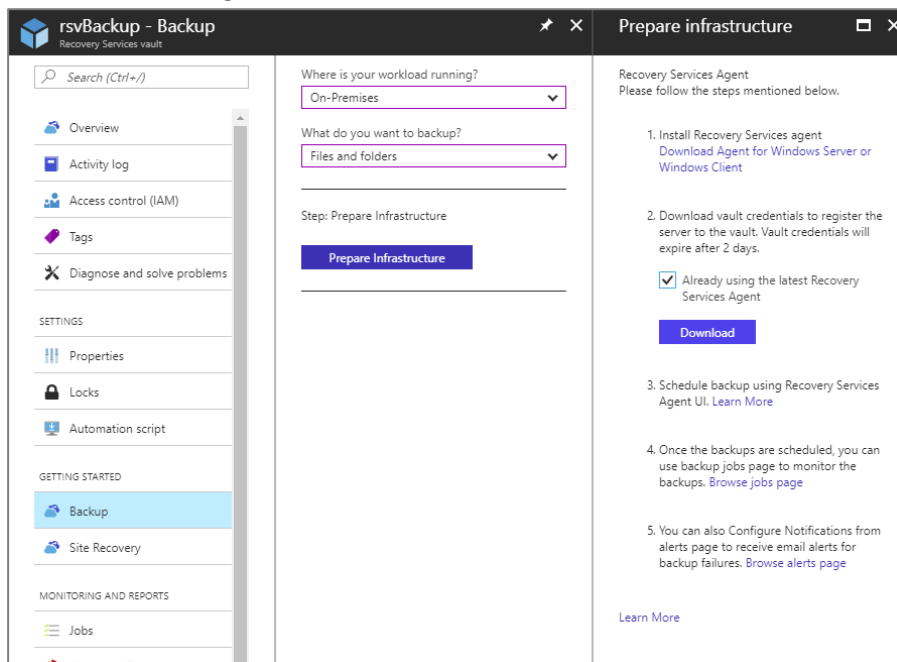
- Create a backup of you files using the Azure Recovery Agent
- Create a backup of your Azure Virtual Machine
- Perform a recovery of your files and folders using the Azure Recovery Agent
- Perform a recovery of your files and folders from your Azure Virtual Machine

Exercise 1: Create a backup of your files

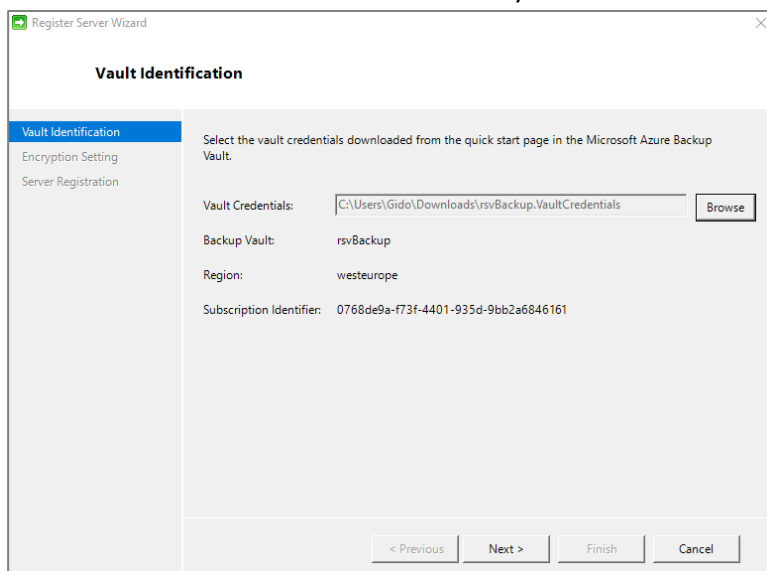
1. From the **Azure Portal**, browse to your **Recovery Services Vault** from the Navigation pane
2. Browse **Backup** from the **Getting Started** submenu
3. Choose **On Premises** as the source of your backup and choose **Files and Folders** as the backup type



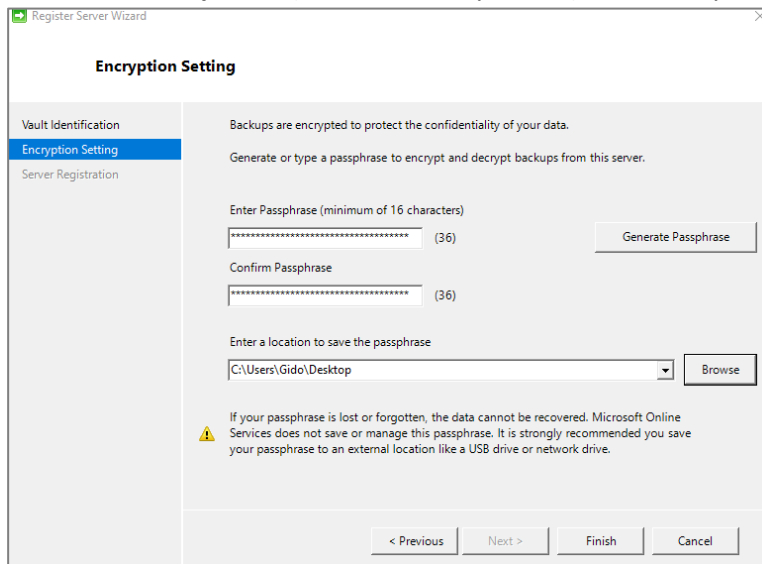
- Download the **Recovery Services Agent** with the link provided and **enable the checkbox** to confirm you have downloaded the agent.



- The **Download** button will become available, **save the Vault Credentials** to your local computer.
- When the downloads are ready, **run the installer**. Use the defaults, until you are asked for identification of the Vault. Select the **Vault Credentials** file you downloaded.



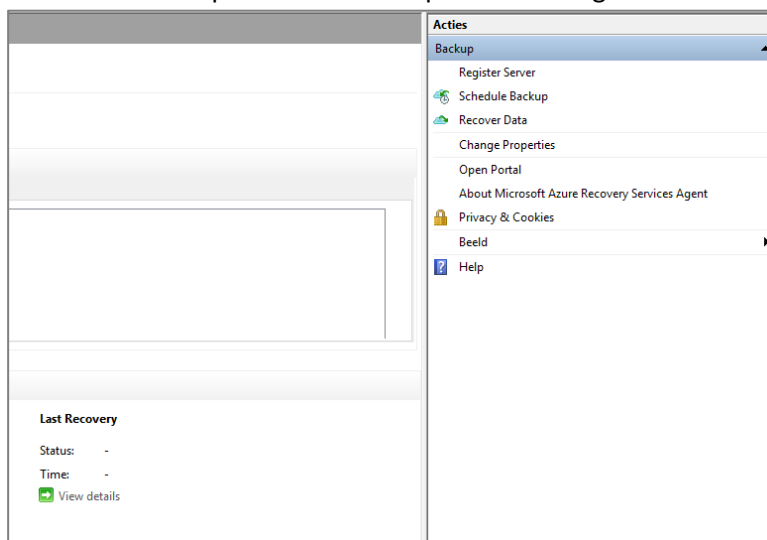
7. **Generate a Passphrase** (or choose one yourself). Save it to your computer.



The image shows the 'Register Server Wizard' window, specifically the 'Encryption Setting' step. The window has a title bar with a green icon and the text 'Register Server Wizard'. The main content area is titled 'Encryption Setting'. On the left, there is a sidebar with three items: 'Vault Identification', 'Encryption Setting' (which is selected and highlighted in blue), and 'Server Registration'. The main area contains the following text and controls:

- Backups are encrypted to protect the confidentiality of your data.
- Generate or type a passphrase to encrypt and decrypt backups from this server.
- Enter Passphrase (minimum of 16 characters): A text box with a masked passphrase (16 asterisks) and a '(36)' character count indicator. To the right is a 'Generate Passphrase' button.
- Confirm Passphrase: A second text box with a masked passphrase (16 asterisks) and a '(36)' character count indicator.
- Enter a location to save the passphrase: A dropdown menu showing 'C:\Users\Gido\Desktop' and a 'Browse...' button.
- A warning icon (yellow triangle) and text: '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.'
- At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

8. Start **Microsoft Azure Backup** from the shortcut on your desktop
9. Schedule a backup from the action pane on the right.



10. **Select** the items you want to backup. Make sure the selection only has a small amount of data, so you don't have to wait.

The screenshot shows the 'Schedule Backup Wizard' window, specifically the 'Select Items to Backup' step. The left sidebar contains a list of steps: 'Getting started', 'Select Items to Backup' (highlighted), 'Specify Backup Schedule...', 'Select Retention Policy (F...)', 'Choose Initial Backup Ty...', 'Confirmation', and 'Modify Backup Progress'. The main area has a title bar 'Schedule Backup Wizard' and a subtitle 'Select Items to Backup'. Below the subtitle, it says 'Click Add Items to select the files and folders you want to backup.' There is a large text box labeled 'Name' containing the path 'C:\Users\Gido\Documents\'. Below the text box are three buttons: 'Add Items', 'Remove Items', and 'Exclusion Settings'. At the bottom, there is a note: 'If a backup location includes file types or sub-folders that you do not want to back up, click Exclusion Settings to remove those items from the backup.' At the very bottom are navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

11. Select how often and when the backup can take place. For instance at **23.00**.

The screenshot shows the 'Schedule Backup Wizard' window, specifically the 'Specify Backup Schedule (Files and Folders)' step. The left sidebar contains a list of steps: 'Getting started', 'Select Items to Backup', 'Specify Backup Schedule...' (highlighted), 'Select Retention Policy (F...)', 'Choose Initial Backup Ty...', 'Confirmation', and 'Modify Backup Progress'. The main area has a title bar 'Schedule Backup Wizard' and a subtitle 'Specify Backup Schedule (Files and Folders)'. Below the subtitle, it says 'Define a schedule when you want to create a backup copy for selected files and folders'. There are two radio buttons: 'Day' (selected) and 'Week'. Below them, it says 'At following times (Maximum allowed is three times a day)'. There are three dropdown menus: the first is set to '23:00', the second is set to 'None', and the third is set to 'None'. At the bottom are navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

12. Select the desired Retention Policy, for instance

- a. **Daily for 14 days**
- b. **Weekly for 4 weeks**
- c. **Monthly for 6 months**
- d. **No yearly backups**

The screenshot shows the 'Select Retention Policy (Files and Folders)' window of the 'Schedule Backup Wizard'. The window has a sidebar on the left with the following options: 'Getting started', 'Select Items to Backup', 'Specify Backup Schedule...', 'Select Retention Policy (Files and Folders)' (which is highlighted), 'Choose Initial Backup by...', 'Confirmation', and 'Modify Backup Progress'. The main area is titled 'Specify the retention policy for the backup copy of files and folders'. It contains three sections: 'Daily Retention Policy' (checked), 'Weekly Retention Policy' (checked), and 'Monthly Retention Policy' (checked). The 'Daily Retention Policy' section shows 'Retain backup copies taken' at '23:00' for '30' Days. The 'Weekly Retention Policy' section shows 'Retain backup copies taken on' 'Saturday' at '23:00' for '26' Weeks. The 'Monthly Retention Policy' section shows 'Retain backup copies taken on' 'Saturday of Last Week' at '23:00' for '36' Months. There are also options for 'On day(s) 1' and 'Yearly Retention Policy' (unchecked). At the bottom, there are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

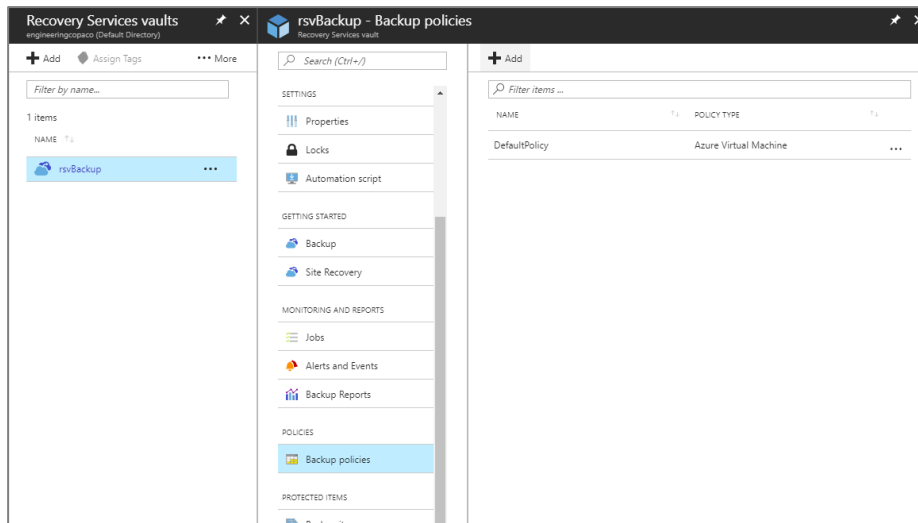
13. On the next screen, you can choose to make adjustments for a offline backup scenario. Accept the defaults for automatic configuration and proceed.

14. **Finish** the wizard and click Backup Now to do an instant backup.

15. As the backup is running, proceed with the next exercise. We will return to the results of this exercise when the job is finished.

Exercise 2: Create a backup of your Virtual Machine

1. Go to the **Azure Portal** and browse to your **Recovery Services Vault**.
2. Open **Backup Policies** from the navigation pane. Add a new **Backup Policy**



3. Use the following parameters;
 - a. Name **CustomBackupPolicy**
 - b. Frequency **Daily at 23:00**
 - c. Daily retention **30 days**
 - d. Weekly retention **26 weeks**
 - e. Monthly retention **36 months**
 - f. Yearly retention **None**

* Policy name

Backup frequency

Retention range

☒ Retention of daily backup point.

* At For Day(s)

☒ Retention of weekly backup point.

* On * At For Week(s)

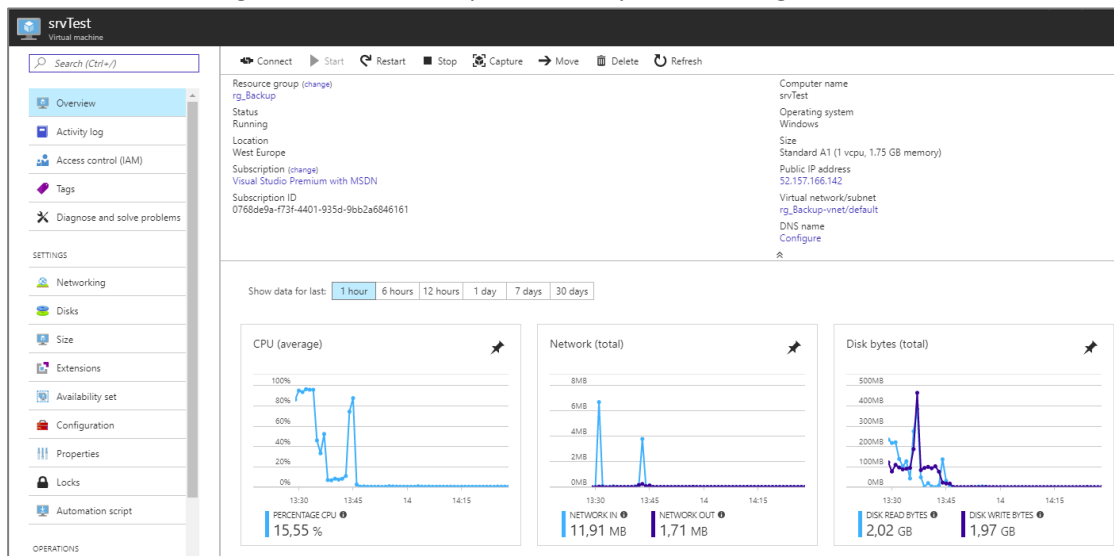
☒ Retention of monthly backup point.

* On * Day * At For Month(s)

☐ Retention of yearly backup point.

Not Configured

4. **Create** the policy
5. Browse to the **Resource Group** created before
6. Identify the **Virtual Machine** that was created in the previous exercise and select it to open the details. As you can see, it is running and the overview pane shows you basic insights on the VM.

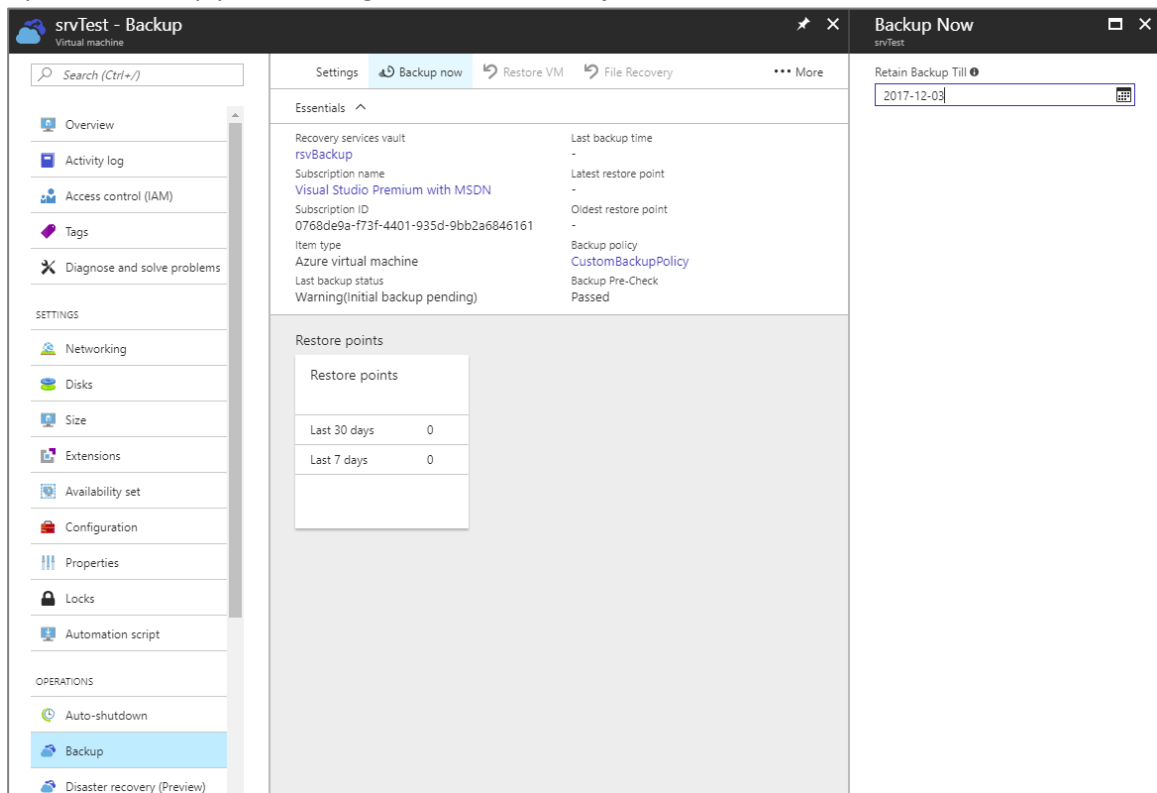


7. Open the **Backup** option from the Navigation pane. Select the correct **Resource Group** and select the customized **Backup Policy**.

The screenshot shows two side-by-side configuration windows. The left window, titled 'Enable backup', contains a description of the Recovery Services vault backup process, a 'Recovery Services vault' dropdown set to 'rsvBackup', and a 'Backup policy' dropdown set to 'DefaultPolicy'. The right window, titled 'Backup policy', shows a 'Choose backup policy' dropdown with 'DefaultPolicy' selected, a 'Create New' button, and a 'DefaultPolicy' button. Below this, the 'RETENTION RANGE' section specifies 'Retention of daily backup point' and 'Retain backup taken every day at 22:30 for 30 Day(s)'.

8. Click **OK** to create the backup, using the Backup Policy we defined earlier.

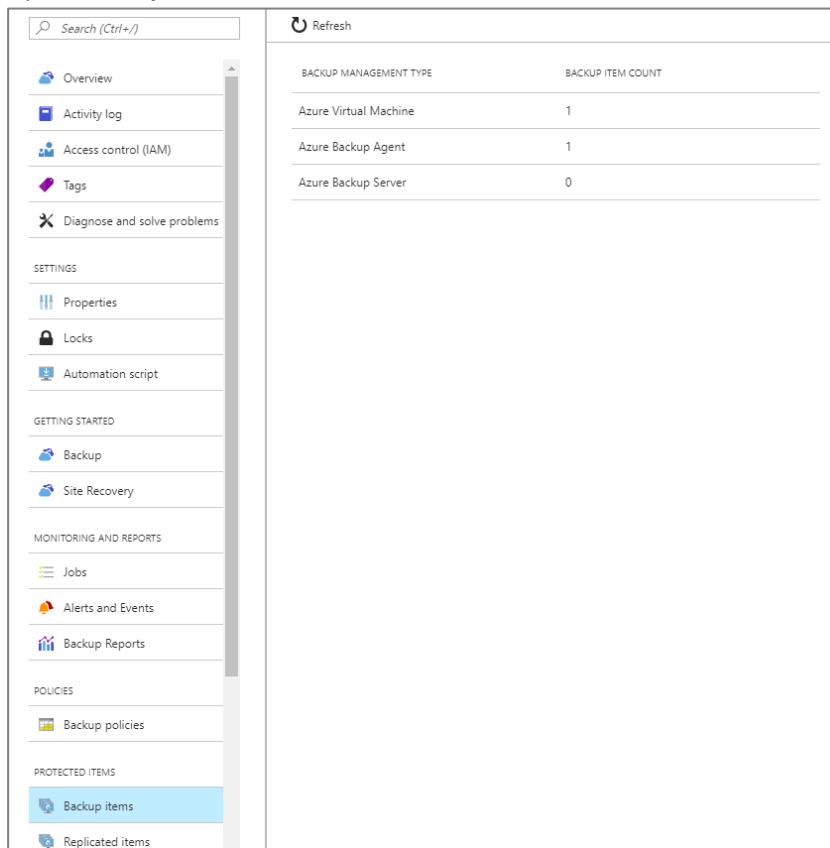
- Open the Backup pane once again and click **Backup Now**. Select the desired retention and choose **Backup**.



You can verify the job is running from the **Notification** button in the top right of the **Azure Portal**. For detailed information;

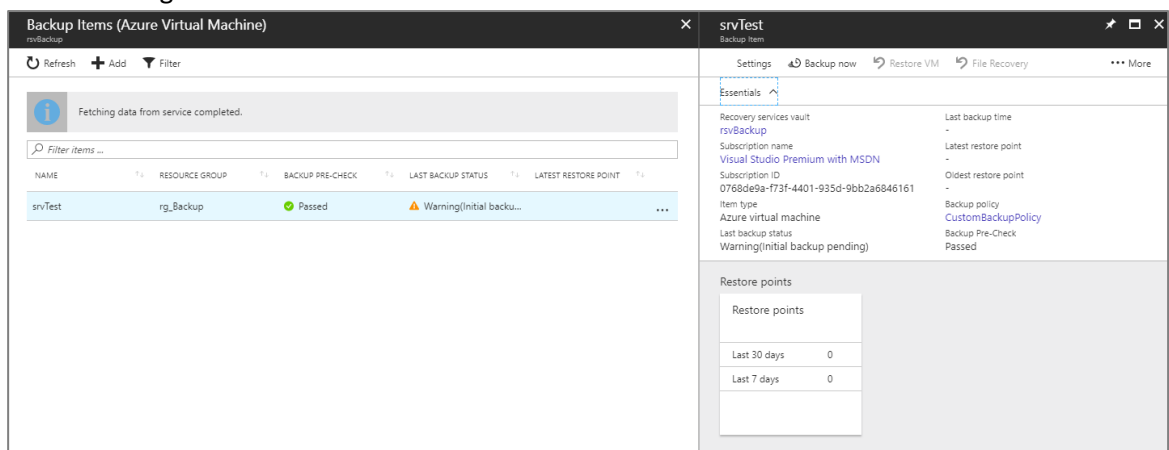
- Open your **Recovery Services Vault**

- Open **Backup Items** under **Protected Items**. Please note the **Azure Virtual Machine** Count has gone up.



BACKUP MANAGEMENT TYPE	BACKUP ITEM COUNT
Azure Virtual Machine	1
Azure Backup Agent	1
Azure Backup Server	0

- Click on it to get detailed information



NAME	RESOURCE GROUP	BACKUP PRE-CHECK	LAST BACKUP STATUS	LATEST RESTORE POINT
srvTest	rg_Backup	Passed	Warning(initial backu...	...

Recovery services vault: **rsvBackup**

Subscription name: **Visual Studio Premium with MSDN**

Subscription ID: **0768de9a-f73f-4401-935d-9bb2a6846161**

Item type: **Azure virtual machine**

Last backup status: **Warning(initial backup pending)**

Last backup time: -

Latest restore point: -

Oldest restore point: -

Backup policy: **CustomBackupPolicy**

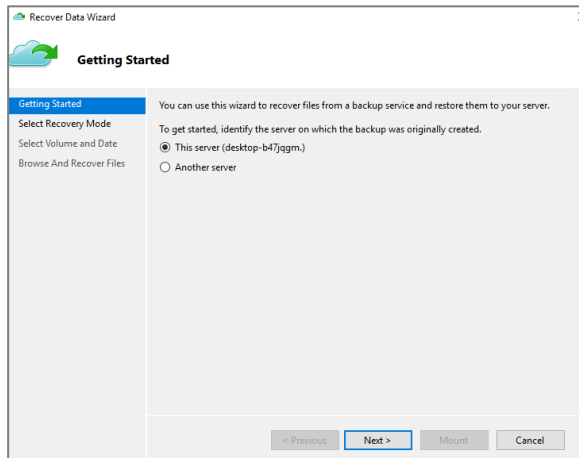
Backup Pre-Check: **Passed**

Restore points	
Last 30 days	0
Last 7 days	0

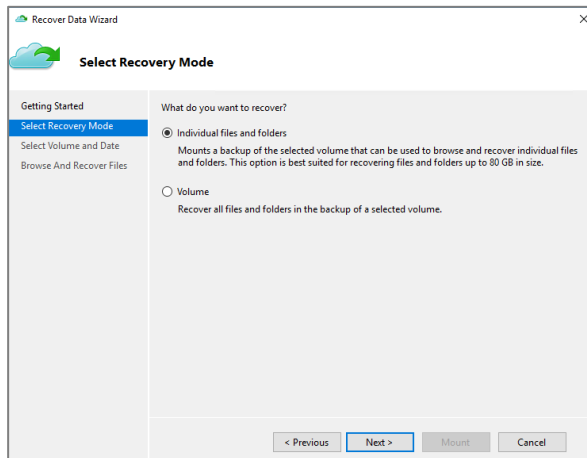
- Proceed to the next exercise. While the backup of your Virtual Machine is running, we'll check on the backup of your Files and Folders that we started before.

Exercise 2: Perform a recovery of your Files and Folders

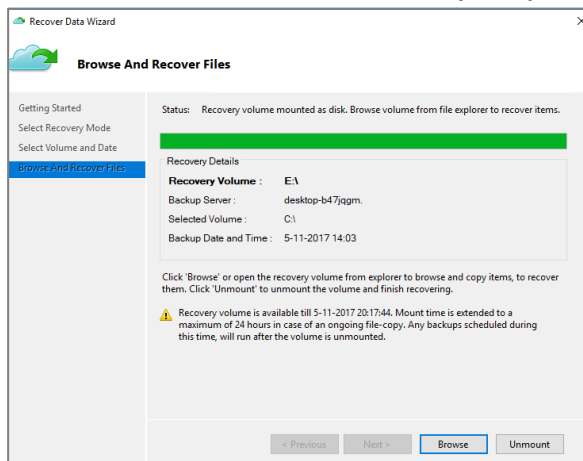
1. Start the **Microsoft Azure Backup** shortcut on your desktop.
2. The **Jobs overview** will show you if your backup job was successful. From the **Action pane** on the right, choose to **Recover Data**.
3. From the **Getting Started wizard**, choose to **Recover from this server**



4. Choose to restore individual **Files and Folders** and select **C:** as the volume



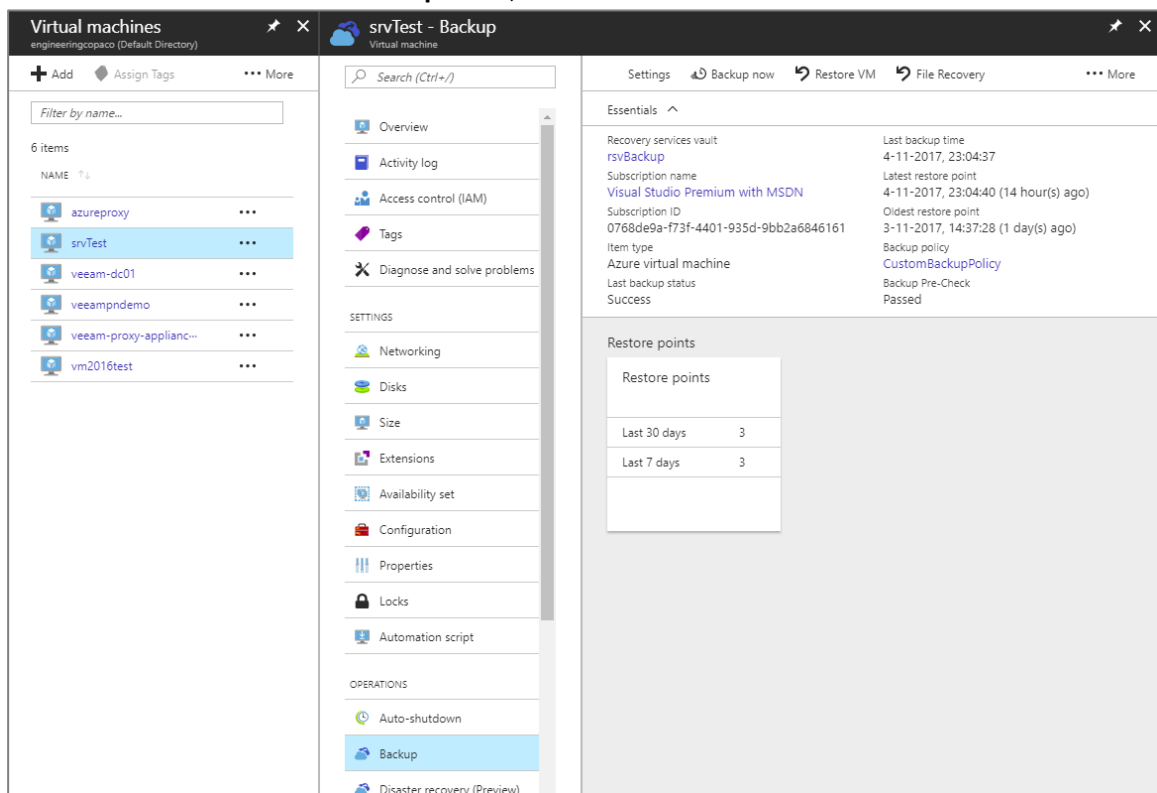
- From the calendar, **select the restore point** just created. Click **Mount**.



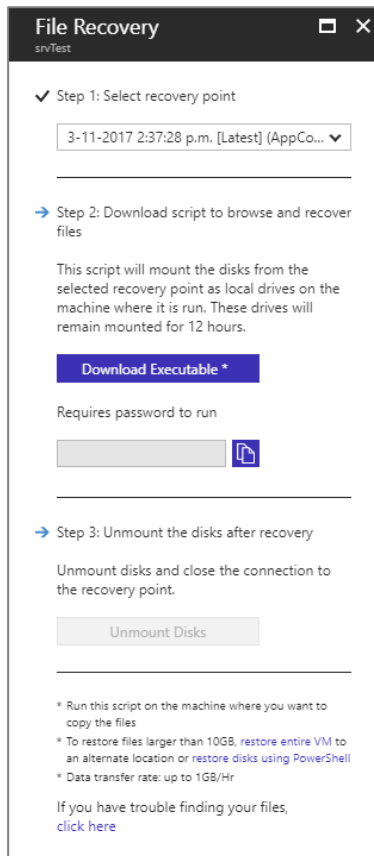
- When the volume is mounted, you can click **Browse** to recover file by using the copy and paste options from **Windows Explorer**. Try to recover your files.
- When finished, click **Unmount** from the Recover Data Wizard.

Exercise 3: Perform a recovery of your VM files

- From the **Resource Group**, open your Virtual Machine. From there, select **Backup** to see the backup state of this machine. Check the **Last Backup State**, it should now show successful.



2. Please note it is possible to restore the full VM from here. However, this activity is not included in this lab. Instead, for this exercise, open **File Recovery**.



The screenshot shows the 'File Recovery' portal window. It has a title bar with 'File Recovery' and 'snvTest'. The main content area is divided into three steps:

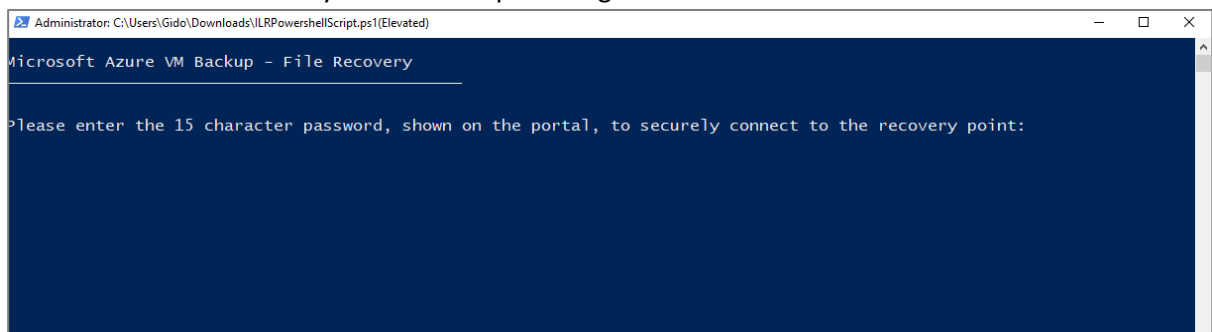
- Step 1: Select recovery point** (marked with a checkmark). It shows a dropdown menu with the selected value '3-11-2017 2:37:28 p.m. [Latest] (AppCo...)'.
- Step 2: Download script to browse and recover files** (marked with a right arrow). It contains a paragraph: 'This script will mount the disks from the selected recovery point as local drives on the machine where it is run. These drives will remain mounted for 12 hours.' Below this is a blue button labeled 'Download Executable *'. Underneath the button, it says 'Requires password to run' followed by a password input field and a copy icon.
- Step 3: Unmount the disks after recovery** (marked with a right arrow). It contains a paragraph: 'Unmount disks and close the connection to the recovery point.' Below this is a grey button labeled 'Unmount Disks'.

At the bottom, there are three asterisked notes:

- * Run this script on the machine where you want to copy the files
- * To restore files larger than 10GB, restore entire VM to an alternate location or restore disks using PowerShell
- * Data transfer rate: up to 1GB/Hr

Below the notes, it says: 'If you have trouble finding your files, [click here](#)'.

3. Select **Recovery Point** and click **Download Executable**
4. **Copy** the password to clipboard
5. Browse the executable on your local computer. Right click to **Run as Administrator**

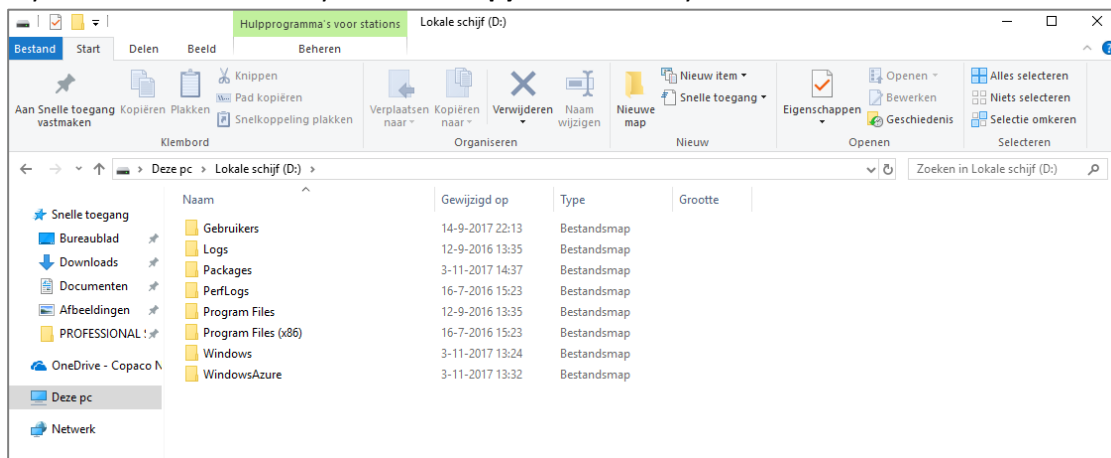


6. **Paste** (or type) the password from clipboard when asked. Please wait while the Recovery Point is mounted.

```
Administrator: C:\Users\Gido\Downloads\ILRPowershellScript.ps1 (Elevated)
Microsoft Azure VM Backup - File Recovery

Please enter the 15 character password, shown on the portal, to securely connect to the recovery point: 991bb6f216814b2
Connecting to recovery point using iSCSI service...
Connection succeeded!
Please wait while we attach volumes of the recovery point.
1 recovery volumes attached
D:\Local Disk
***** Open Explorer to browse for files *****
After recovery, to remove the disks and close the connection to the recovery point, please click 'Unmount Disks' in step
3 of the portal.
Press 'Q/q' key to exit ...
```

7. From the **Windows Explorer**, the Recovery Point is mounted as a driveletter (D:\)
8. Try to browse the Recovery Point and **copy** some files to your local drive.



9. When done, click **Unmount Disks** from the Azure Portal. After some time, the drivemapping on your local machine will disappear.

Activity 3: Clean-up

Objectives

In this activity, you will;

- Remove the Azure resources created in this lab

The resources we deployed will consume your credit. As they are only there for testing purposes, you can safely remove them. This way, the remaining credit from your Azure Pass can be used for other activities. This activity is optional.

1. From the **Azure Portal**, navigate to your **Resource Group**
2. From the **Overview** pane, click **Delete Resource Group**
3. Make sure you selected the correct Resource Group and confirm this by typing the name when asked.
4. Click to **Delete** to confirm. Check the status from the **Notifications** in the top right of the Azure Portal.