

Azure Backup V4

Click-to-Run™ Solution Deployment Guide



Azure Backup V4 Deployment Guide

This guide was designed to provide channel partners with the post deployment steps required to successfully deploy Azure Backup V4.

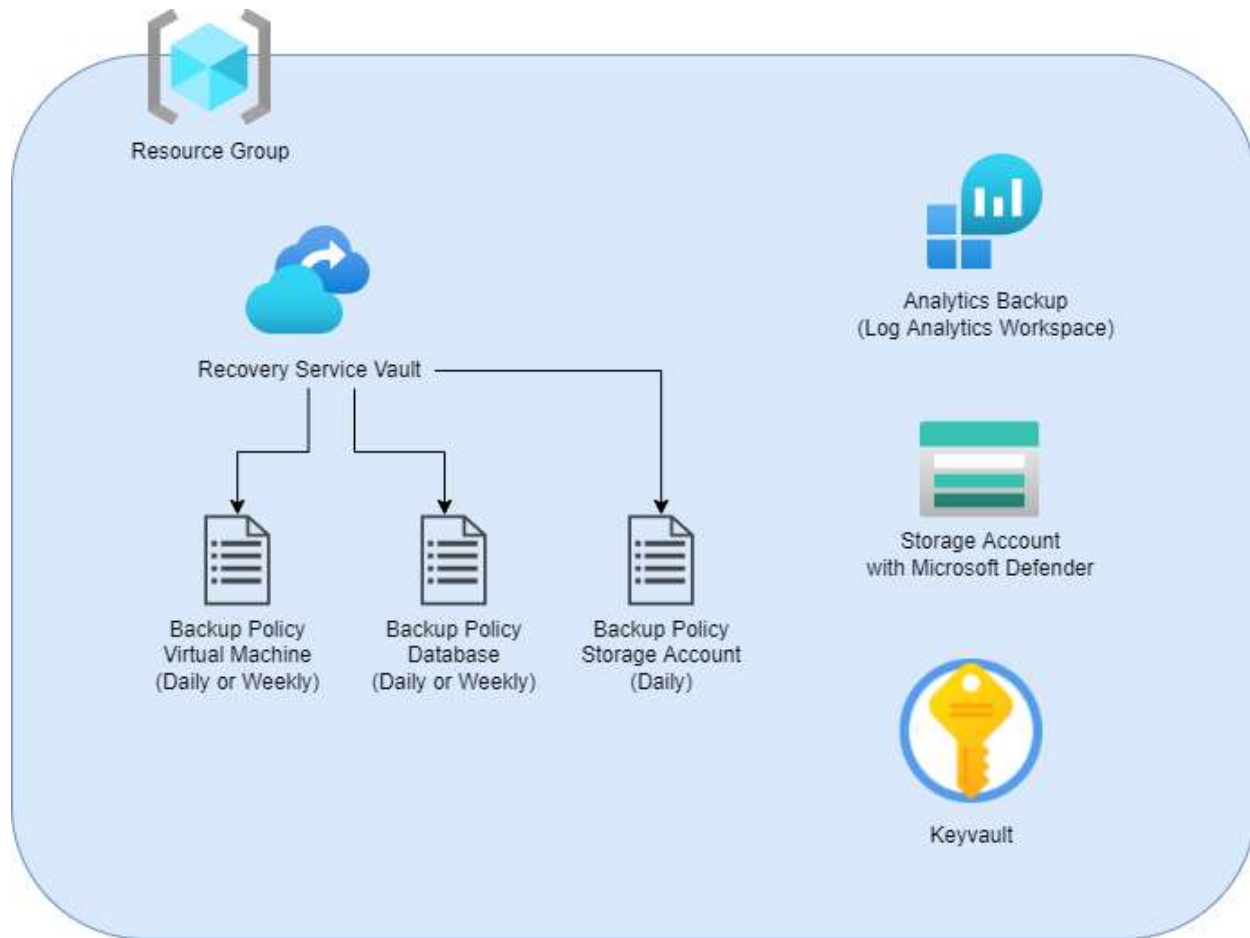
Azure Backup V4 allows you to backup and secure your cloud environment by creating a Recovery Services Vault. In this vault, you will be able to create backup policies and apply them to your VMs, SQL server databases or Azure File Shares.

You will also have the possibility to deploy a Log Analytics Workspace, an Azure Keyvault to secure your private keys, and enable Microsoft Defender for the Azure Storage Accounts you select.

Table of Contents

- Architectural Diagram
- User Interface
- Post-deployment

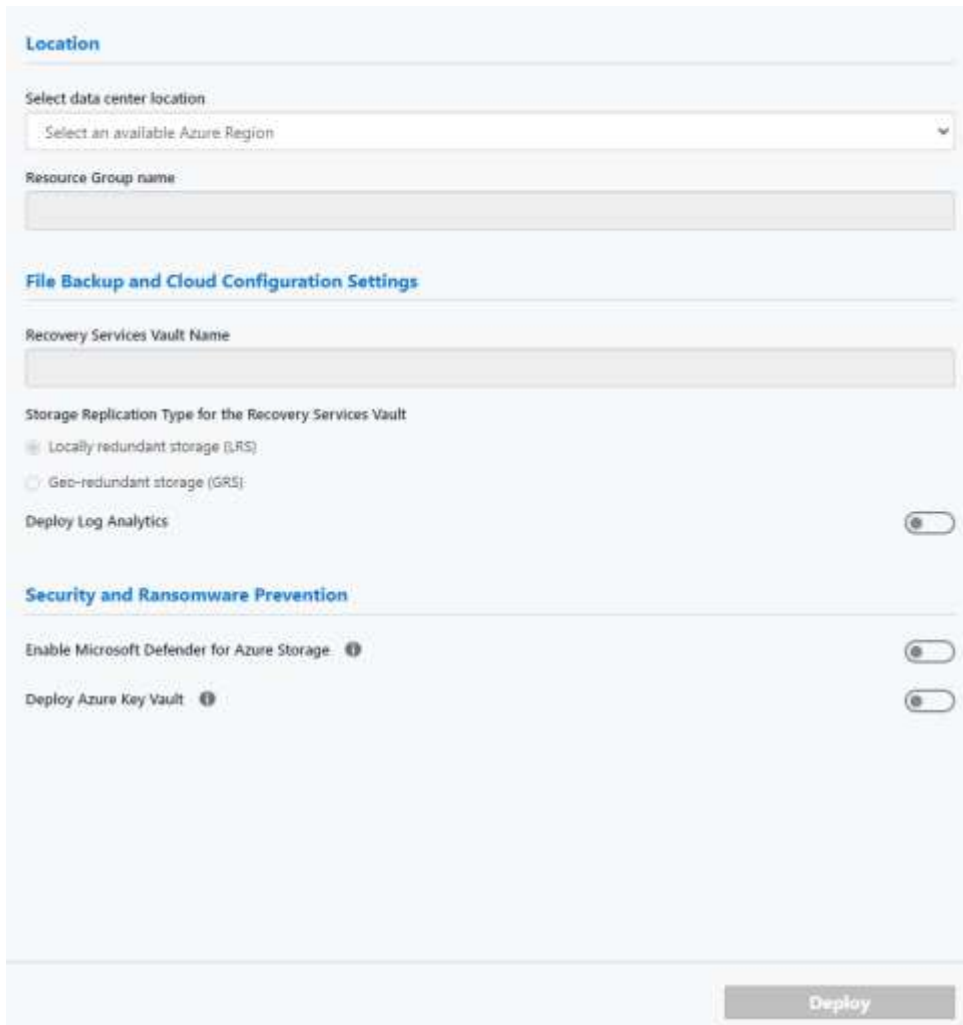
Architectural Diagram



* Once the backup policies are created, you can attach them to the resources you select in the solution UI.

User Interface

When opening the solution, you will see this form:

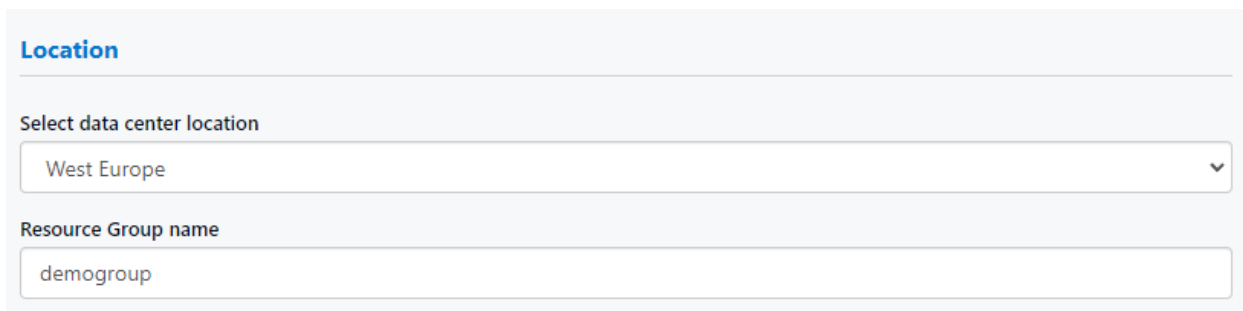


The screenshot shows a deployment configuration form with the following sections and fields:

- Location**
 - Select data center location: A dropdown menu with the text "Select an available Azure Region".
 - Resource Group name: A text input field.
- File Backup and Cloud Configuration Settings**
 - Recovery Services Vault Name: A text input field.
 - Storage Replication Type for the Recovery Services Vault:
 - Locally redundant storage (LRS)
 - Geo-redundant storage (GRS)
 - Deploy Log Analytics: A toggle switch, currently turned off.
- Security and Ransomware Prevention**
 - Enable Microsoft Defender for Azure Storage: A toggle switch, currently turned off.
 - Deploy Azure Key Vault: A toggle switch, currently turned off.

A "Deploy" button is located at the bottom right of the form.

Below you can find an explanation of each field:



This section provides a detailed view of the "Location" section of the form:

- Location**
- Select data center location: A dropdown menu with "West Europe" selected.
- Resource Group name: A text input field containing "demogroup".

First, you need to select a data center location and a new resource group name that will contain all the resources that will be created during the deployment.

File Backup and Cloud Configuration Settings

Recovery Services Vault Name

demorecoveryvault

Storage Replication Type for the Recovery Services Vault

Locally redundant storage (LRS)

Geo-redundant storage (GRS)

Then, you need to specify a new name for the Recovery Services Vault that will be created. This Vault will contain all the backup policies. You can specify if you prefer a Locally redundant storage (LRS) or Geo-redundant storage (GRS).

Deploy Log Analytics

Log Analytics Region

West Europe

You also have the possibility to deploy a Log Analytics Workspace, which can be used to store, retain, and query data collected from various resources that have been monitored in Azure to provide valuable insights for those resources.

Backup Policies

Virtual Machines

SQL Server databases

Azure File Share

Create a Backup Policy for Virtual Machines

In this section you can create the backup policies for your Virtual Machines, SQL Server databases and Azure File Share. Enabling the toggle will display a new set of options.

Virtual Machines SQL Server databases Azure File Share

Create a Backup Policy for Virtual Machines

Backup Frequency

Daily

Weekly

Time Zone

(UTC) Coordinated Universal Time

Schedule Run Time ⓘ

23:00

Schedule Run Day

Sunday

Apply Backup Policy ⓘ

Available Virtual Machines for applying the Backup Policy ⓘ

advm1, ia-jb01

Here, for example, we have created a backup policy for Virtual Machines that will run every Sunday at 11pm UTC and will backup the VMs *advm1* and *ia-jb01*. NOTE: make sure the VMs are ON when deploying the solution.

Virtual Machines | **SQL Server databases** | Azure File Share

Create a Backup Policy for SQL Server databases

Backup Frequency

Daily

Weekly

Time Zone

(UTC) Coordinated Universal Time ▼

Schedule Run Time ⓘ

22:30 ⌚

Apply Backup Policy ⓘ

i Please, select only the Virtual Machines that contain the SQL server you want to backup. Also, make sure that the selected Virtual Machines are powered ON before deploying the solution.

Available Virtual Machines for applying the SQL Server Backup Policy ⓘ

advm1 ▼

In this other example, we have applied a SQL Server database backup policy that will run every day at 10:30pm UTC and we have linked it with the VM advm1. Note: make sure that the selected VMs contain a SQL server and the VM is ON when deploying the solution.

Virtual Machines | SQL Server databases | **Azure File Share**

Create a Backup Policy for Azure File Shares (Daily only)

Backup Frequency:
Daily

Time Zone
(UTC) Coordinated Universal Time

Schedule Run Time ⓘ
00:00

Apply Backup Policy ⓘ

Available Azure File Shares for applying the Backup Policy ⓘ
sapbits (Storage Account: ujjjfezpofjez), userprofiles (Storage Account: s...▼

In this final example, we have created an Azure File Share backup policy that will run daily (this type of backup policy can only run daily, not weekly) at 00am UTC and we have applied it to two different Azure File Shares.

Security and Ransomware Prevention

Enable Microsoft Defender for Azure Storage ⓘ

Available Storage Accounts for applying Microsoft Defender ⓘ
csb10032000f4454afd, csb10032001b46e3b9e, ofjezmfmozwa ▼

In this section you can enable Microsoft Defender for Azure Storage.

"Microsoft Defender for Storage is an Azure-native layer of security intelligence that detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption."

You can apply this feature to the storage accounts you select in the dropdown.

Deploy Azure Key Vault ?

Key Vault SKU

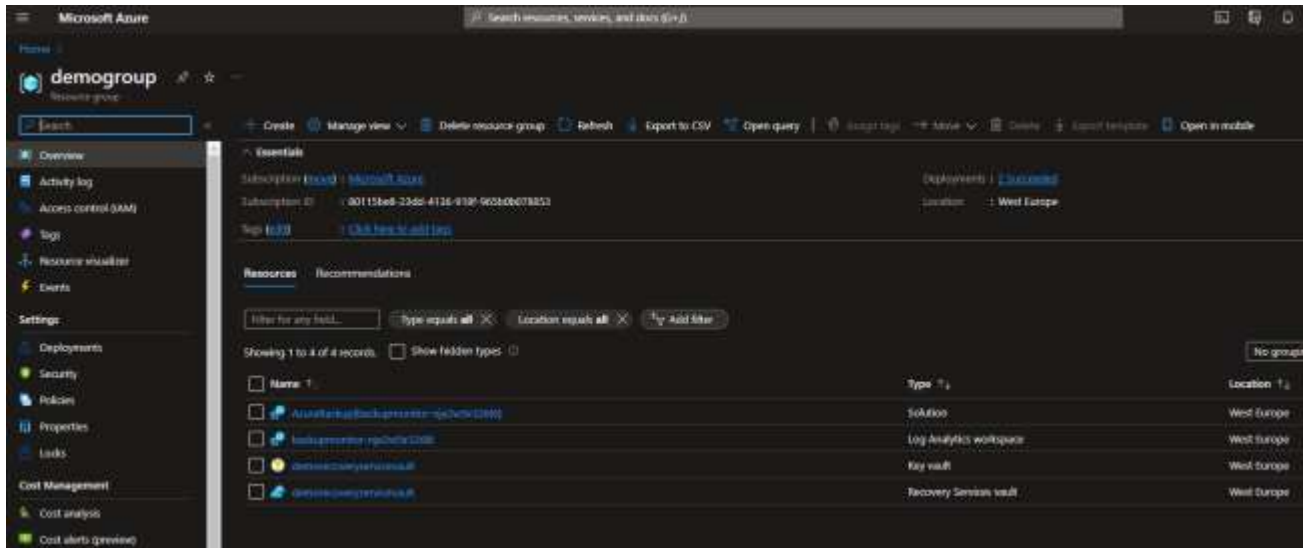
Standard ▼

Soft Delete Retention (in days) ?

10 15 20 25 30

Finally, you can deploy an Azure Key Vault to secure your private keys, certificates, etc. You can select between a Standard or Premium SKU as well as define the number of days for the Soft Delete Retention.

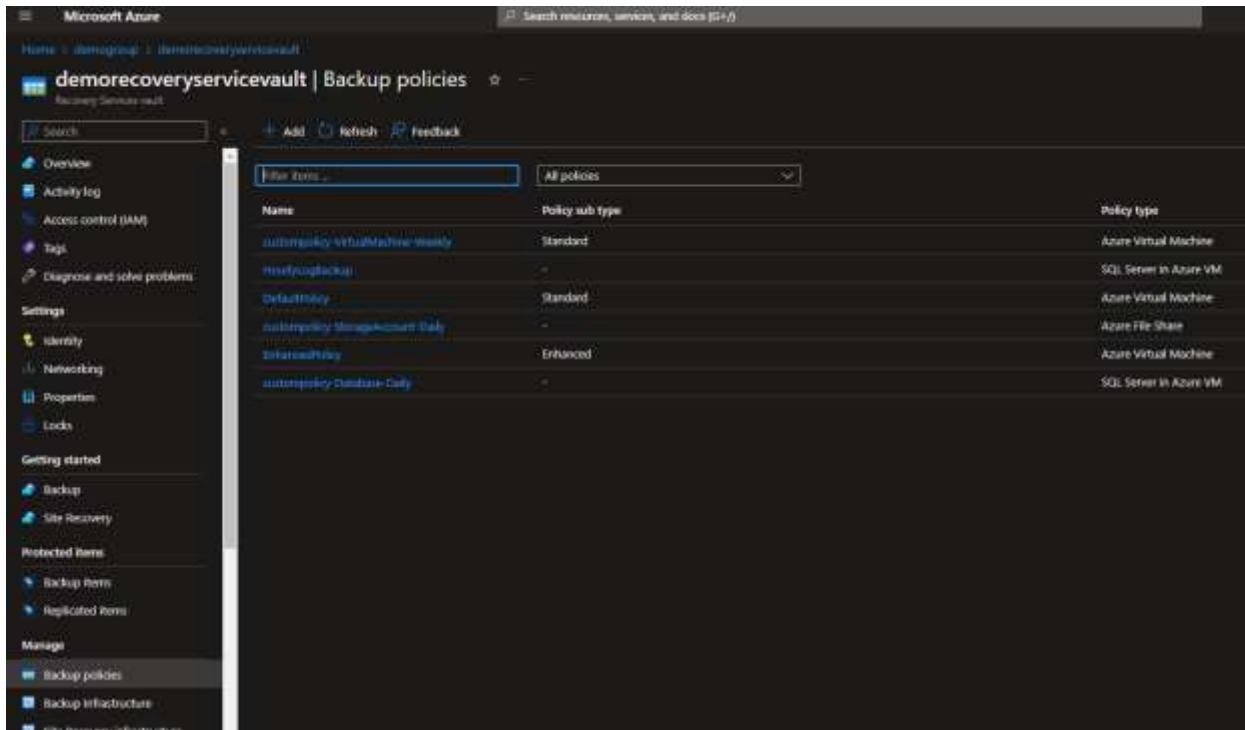
Post-deployment



To check the deployment, you can go to the Azure Portal and in Resource Groups, select the one you created. The resource group will contain all the different resources that were created during the deployment. In this case, we will get:

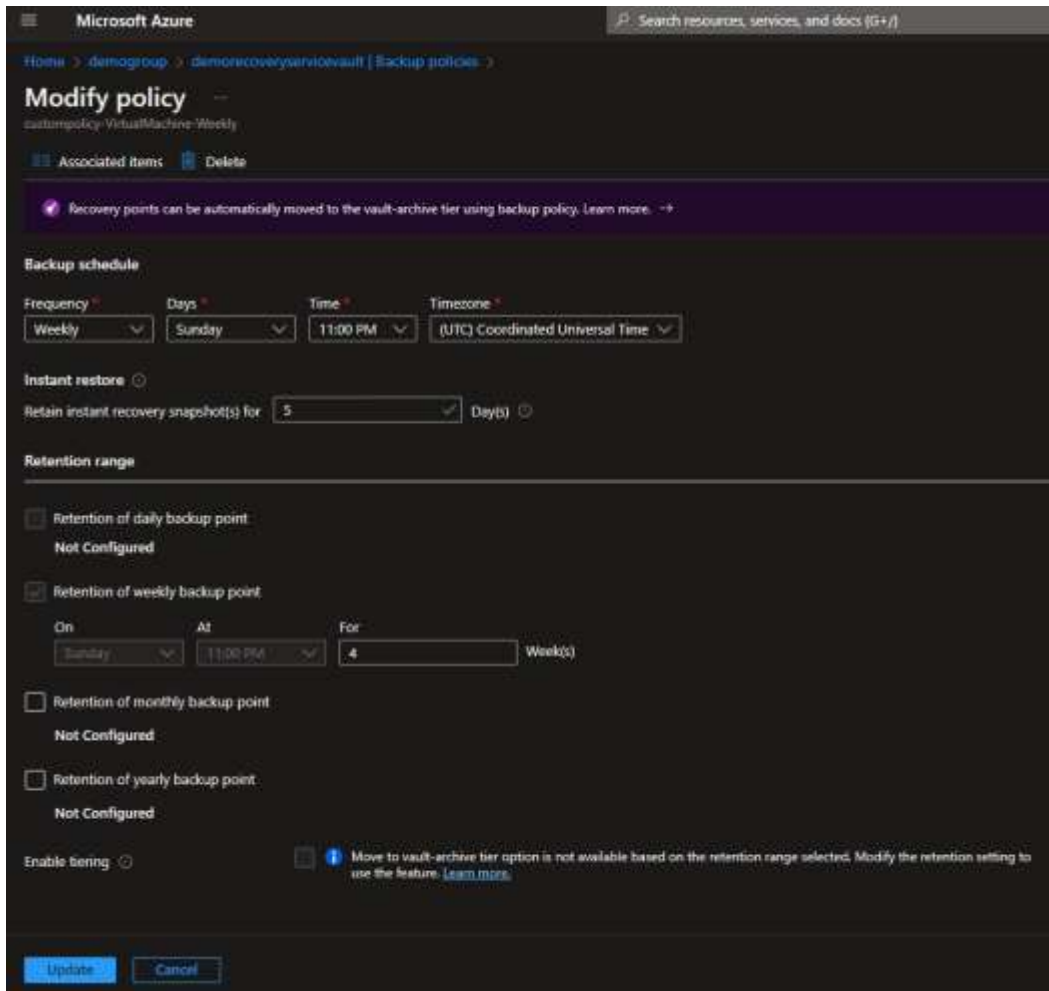
- A Solution and a Log Analytics Workspace (if we turned on the *Deploy Log Analytics* option).
- A Key vault (if we turned on the *Deploy Azure Key Vault* option).
- A Recovery Services vault.

Let's review the Recovery Services vault.



Opening the Recovery Services vault and clicking on **Backup policies** will show us the custom policies we have created (the ones that start with **custompolicy**, the others are created by default). You can see that one is for Azure Virtual Machines, another is for Azure File Share, and another for SQL Server in Azure VM.

If we open one of these policies, we can see more details (some of them were specified in the solution form, like in this example where we applied a policy to be executed on Sundays at 11pm UTC):



Microsoft Azure | Search resources, services, and docs (G+)

Home > demogroup > demorecoveryvault | Backup policies >

Modify policy

custompolicy-VirtualMachine-Weekly

Associated items | Delete

Recovery points can be automatically moved to the vault-archive tier using backup policy. [Learn more.](#)

Backup schedule

Frequency: Weekly | Days: Sunday | Time: 11:00 PM | Timezone: (UTC) Coordinated Universal Time

Instant restore

Retain instant recovery snapshot(s) for: 5 Days

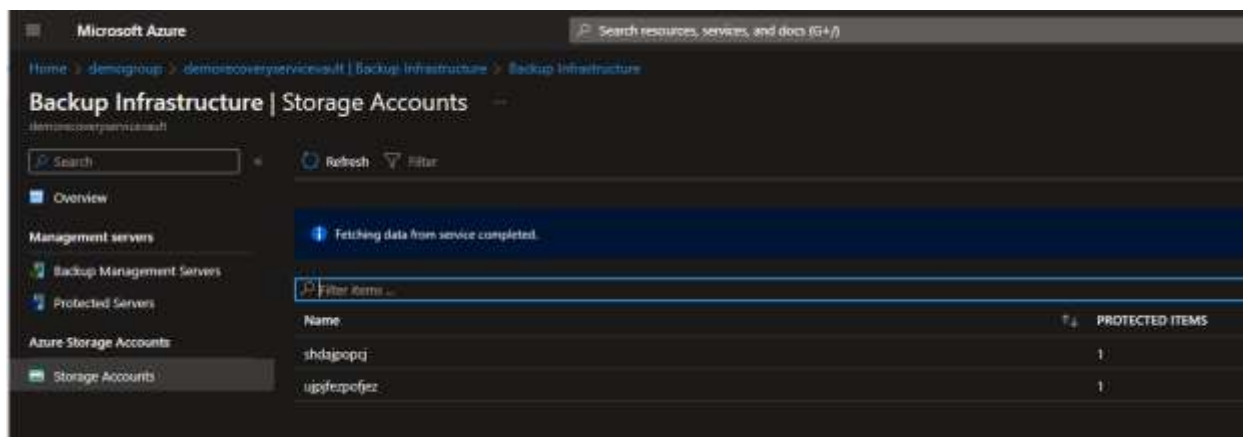
Retention range

- Retention of daily backup point: Not Configured
- Retention of weekly backup point:
 - On: Sunday | At: 11:00 PM | For: 4 Week(s)
- Retention of monthly backup point: Not Configured
- Retention of yearly backup point: Not Configured

Enable tiering: Move to vault-archive tier option is not available based on the retention range selected. Modify the retention setting to use the feature. [Learn more.](#)

Update | Cancel

Clicking on **Backup Infrastructure > Storage Accounts** will show us the Storage Accounts where the Azure File Share policy was applied:



Microsoft Azure | Search resources, services, and docs (G+)

Home > demogroup > demorecoveryvault | Backup Infrastructure > Backup Infrastructure

Backup Infrastructure | Storage Accounts

demorecoveryvault

Search | Refresh | Filter

Overview

Management servers

- Backup Management Servers
- Protected Servers

Azure Storage Accounts

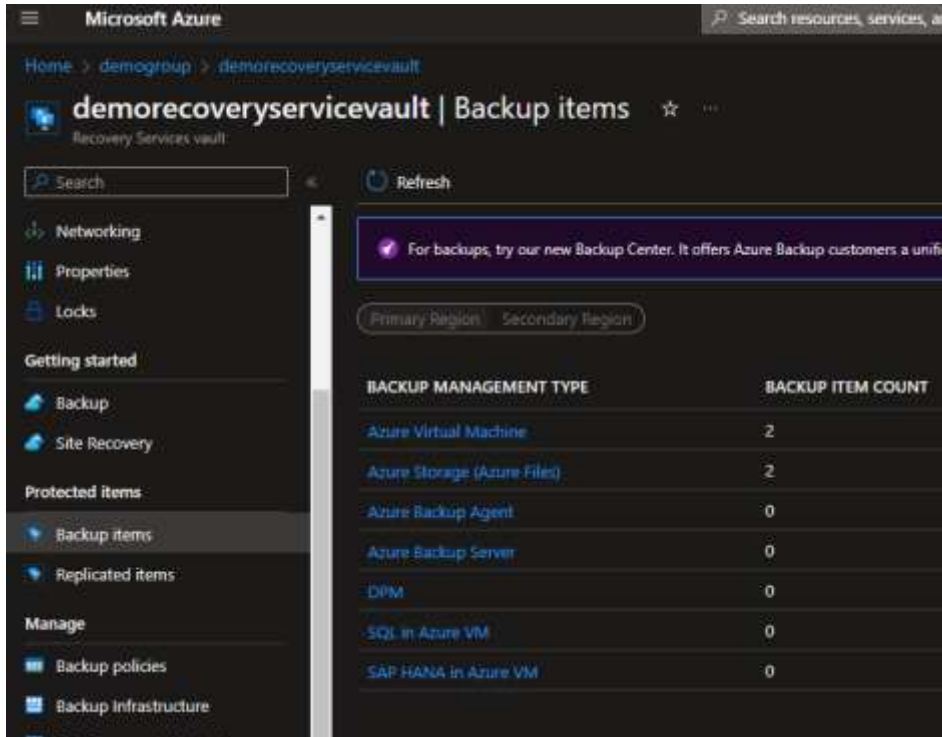
- Storage Accounts

Fetching data from service completed.

Filter items...

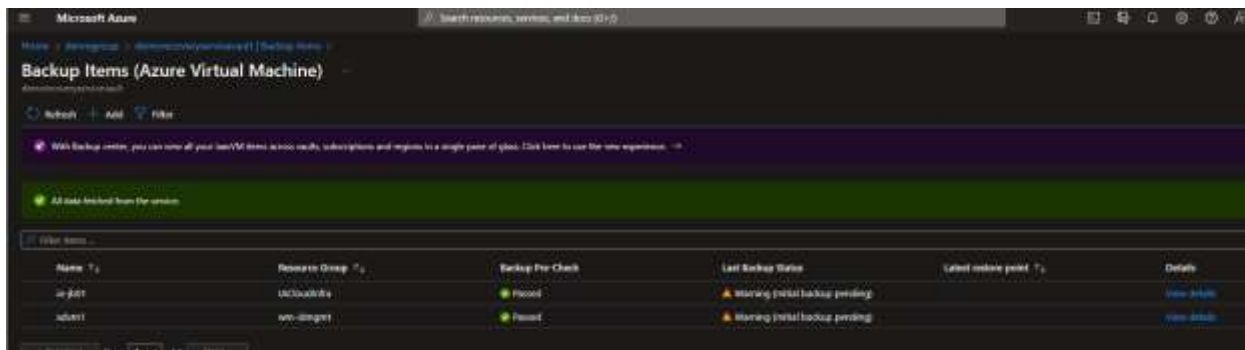
Name	PROTECTED ITEMS
shdajpqpj	1
ujgfepefjez	1

We can also see all the resources (items) that have been backed up by clicking on Backup items:

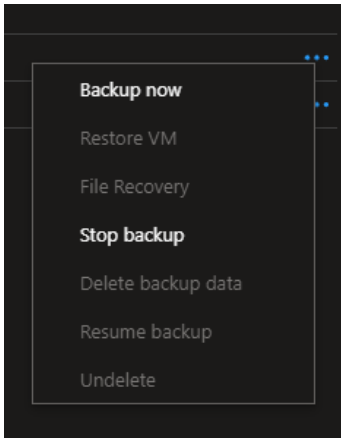


In this case, 2 VMs and 2 Azure File Shares.

Clicking on each of these entries will show more details on the items that are backed up:



You have the option to stop the backup at any moment, or backup the item now.

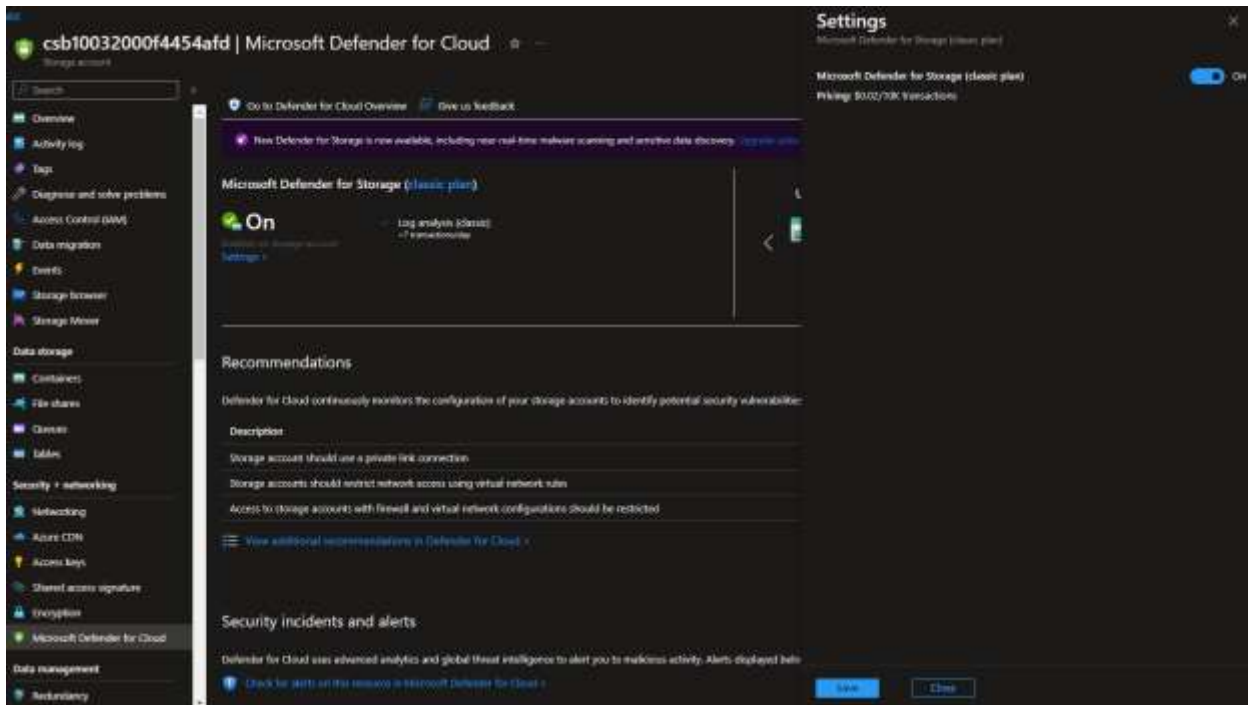


To review if Microsoft Defender for Azure Storage Accounts was correctly applied, you can go to Storage Accounts > (select the Storage Account) > Capabilities.

Here you should see that the **Security** feature has the status Configured.



In case you decide to turn off Microsoft Defender, you can click on **Security** and then Click on the **Settings** link and then turn off the toggle **Microsoft Defender for Storage (classic plan)** on the right menu.



The screenshot displays the Microsoft Defender for Cloud console interface. At the top, the account ID 'csb10032000f4454afd' and the service name 'Microsoft Defender for Cloud' are visible. The left-hand navigation pane lists various security services, with 'Microsoft Defender for Cloud' selected. The main content area shows the 'Settings' page for 'Microsoft Defender for Storage (classic plan)'. A toggle switch is set to 'On', and the pricing is listed as '\$0.02/GB Transactions'. Below this, a 'Recommendations' section provides guidance on storage account configurations, such as using private link connections and restricting network access. A 'Security incidents and alerts' section at the bottom offers to check for alerts on the resource.