Hands-On Lab

Azure Backup

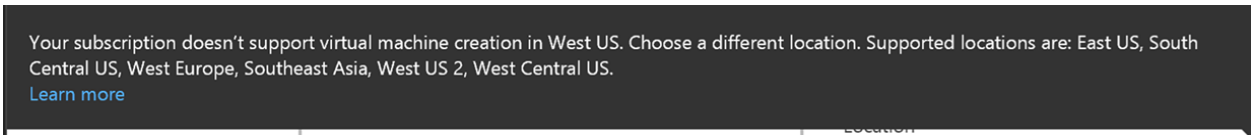
Contents

Azure Backup

In this lab you are going to backup files and folders from your local computer to Microsoft Azure. This includes installing an agent on your computer. If this is not possible, you can spin up a VM in Microsoft Azure to use as the source computer.

Before you Begin

If you are using a Microsoft Azure subscription that was provided to you by Microsoft, you are limited to a specific set of Microsoft Azure regions that you can use. **Please use either the East US, South Central US, West Europe, Southeast Asia, West US 2, or West Central US locations.**



Otherwise you will receive the following error in the portal if you select an unsupported region and attempt to build anything in Microsoft Azure.

Create a recovery services vault

To back up your files and folders, you need to create a Recovery Services vault in the region where you want to store the data.

1. On the Portal Blade menu, click **All Services** and in the list of resources, type **Recovery Services** and click **Recovery Services vaults**.
2. On the **Recovery Services vaults** menu, click **Add**.
3. The Recovery Services vault blade opens, enter the following:
    a. **Name:** EastDRVault
    b. **Subscription:** Azure Pass
    c. **Resource group:** Create New *DRaaSEast*
    d. **Location**: East US
4. At the bottom of the Recovery Services vault blade, click **Create**.

    It can take several minutes for the Recovery Services vault to be created. Monitor the status notifications in the upper right-hand area of the portal. Once your vault is created, it appears in the list of Recovery Services vaults. If after several minutes you don't see your vault, click **Refresh**.

Configure the vault

1. On the Recovery Services vault blade in the Getting Started section, click **Backup**, then on the **Getting Started with Backup** blade, select **Backup goal**.
2. From the **Where is your workload running?** drop-down menu, select **On-Premises**.
3. From the **What do you want to backup?** menu, select **Files and folders**, and click **Prepare infrastructure**.
4. On the **Prepare infrastructure** blade, click **Download Agent for Windows Server or Windows Client**. A pop-up menu prompts you to run or save MARSAgentInstaller.exe. In the download pop-up menu, click **Save**.

   You don't need to install the agent yet. You can install the agent after you have downloaded the vault credentials.

5. On the **Prepare infrastructure** blade, click the checkbox for **Already downloaded or using the latest Recovery Services Agent** and then click **Download**.

   The vault credentials download to your Downloads folder. After the vault credentials finish downloading, you see a pop-up asking if you want to open or save the credentials. Click **Save**. If you accidentally click **Open**, let the dialog that attempts to open the vault credentials, fail. You cannot open the vault credentials. Proceed to the next step. The vault credentials are in the Downloads folder.

Install and register the agent

Locate and double-click the **MARSagentinstaller.exe** from the Downloads folder (or other saved location).

Complete the Microsoft Azure Recovery Services Agent Setup Wizard. The setup may take 10 minutes if required components need to be installed.

Note:

> If you lose or forget the passphrase, Microsoft cannot help recover the backup data. Save the file in a secure location. It is required to restore a backup.

The agent is now installed and your machine is registered to the vault. You're ready to configure and schedule your backup.

Back up your files and folders

The initial backup includes key tasks:

- Initialize the agent
- Schedule the backup
- Back up files and folders for the first time

To complete the initial backup:

1) Open Microsoft Azure Backup from your desktop. It may take several minutes to initialize.
2) Click on **Register Server**.
3) On the **Proxy Configuration** screen click **Next.**
4) On the **Vault Credential** screen click **Browse** to find your vault credentials. Note that it may take several minutes to validate the Vault credentials. Click **Next.**
5) On the **Encryption Setting** screen, click **Generate Passphrase** and save the passphrase to your downloads folder. Click **Register**, then click **Close.** (if you get an error here, proceed ignoring the Encryption error)
6) Click **Schedule Backup**.
7) Click **Next**, then **Add items**. Add your documents folder and click **Next.**
8) Click **Next** four times**,** then **Finish**, then **Close**.
9) On the Actions menu choose **Back Up Now,** click **Next** and then **Back Up**.
10) Congratulations! You are now performing a Cloud First Backup!

Recover Your Data

In this lab you will restore an innocuous file you just backup up to Azure.

1) Once you see that the Back Up job has completed, In the Azure Backup Agent select **Recover Data.**
2) On the **Getting Started** screen choose this server and click **Next**.
3) On the **Select Recovery Mode** screen select **Individual files and folders** and click **Next**.
4) On the Select Volume and Date screen select C:\ and then click Mount.
5) Click on **Browse** and notice File Explorer will open. At this point you would copy the file or folder you want to recover over to your computer.
6) Click **Unmount**.

Stop and Remove Backups

If you do not want to permanently keep these files backed up (charges may apply), please follow these steps to stop the agent from creating additional backups and remove the existing backups in Azure.

1) Launch the Microsoft Azure Backup agent from the source machine
2) Click on **Schedule Backup**

3) Select **Stop using this backup schedule and delete all of the stored backups**
4) Click **Next** and **Finish** to stop all future backups and delete all existing backups