



# Azure for On-Premises Administrators – Practice Exercises

## Overview

This course includes optional practical exercises where you can try out the techniques demonstrated in the course for yourself. This guide lists the steps for the individual practical exercises.

See the Overview page under Practical Exercises in your course for information about getting started.

## Azure Setup

If you already have a Microsoft Azure subscription, you can skip this section. Otherwise, follow these steps to create a free trial subscription. You will need to provide a valid credit card number for verification, but you will not be charged for Azure services – for more information, see the [frequently asked questions](#) on the Azure sign-up page.

1. If you already have a Microsoft account that has not already been used to sign up for a free Azure trial subscription, you're ready to get started. If not, don't worry, just [create a new Microsoft account](#).
2. After you've created a Microsoft account, create your [free Microsoft Azure account](#). You'll need to sign-in with your Microsoft account if you're not already signed in. Then you'll need to:
  - Enter your cellphone number and have Microsoft send you a text message to verify your identity.
  - Enter the code you have been sent to verify it.

- Provide valid payment details. This is required for verification purposes only – your credit card won't be charged for any services you use during the trial period, and the account is automatically deactivated at the end of the trial period unless you explicitly decide to keep it active.

## PowerShell Setup

Before you begin, make sure that your lab computer has a minimum of PowerShell 4 installed. You can install the latest version of the management framework (including PowerShell 5.0) by downloading and installing the Windows Management Framework 5.0 software. You can download it from <https://www.microsoft.com/en-us/download/details.aspx?id=50395>. Once you verify that your computer has the minimum required version of PowerShell, you can proceed to download the necessary modules:

1. From your lab computer, open an elevated PowerShell prompt.
2. Verify Azure related modules are available. If Azure modules are not available proceed with the following steps.

### **Get-Module -All**

3. Install the AzureRM module for *resource management*.

### **Install-Module AzureRM**

4. If you get prompted to install and import the NuGet provider, Type **Y** and then press the **Enter** key.
5. If you are notified that the repository is untrusted, confirm that you want to install the modules by typing **Y** and then pressing the **Enter** key. The installation process will take several minutes as packages are downloaded and installed.
6. After the download and installation is finished, import the module.

### **Import-Module AzureRM**

7. Install the Azure module for *service management*.

### **Install-Module Azure** command.

8. If you are notified that the repository is untrusted, confirm that you want to install the modules by typing **Y** and then pressing the **Enter** key. The

installation process will take several minutes as packages are downloaded and installed.

9. Once the download and installation is finished, import the module.

**Import-Module Azure** command.

10. Verify Azure related modules are available.

**Get-Module -All**

If you have trouble installing the PowerShell modules from the PowerShell gallery, you can try the WebPI method instead. Visit <http://aka.ms/webpi-azps> to download and install the modules.

## 1 | Identity



### Add a Custom Domain

In this exercise you will register a new domain and then add that domain as a custom domain to Microsoft Azure.

1. Use a registrar to register a test domain for 1 year. Since this is a test, choose an inexpensive registrar and top-level domain (TLD). For example, [www.namecheap.com](http://www.namecheap.com) has some domains that you can register for 1 year for \$0.88 cents.
2. Navigate to the new Azure Portal at <https://portal.azure.com> and sign in.
3. From the Microsoft Azure dashboard, in the left pane, click **More Services**.
4. Click **Active Directory**.
5. Click **DOMAINS** and then click **Add a custom domain**.
6. In the Domain Name textbox, type <YourDomainName> where <yourDomainName> is the name of the domain that you registered. Click **add**.
7. An informational message will state that the domain was successfully added.

8. In the bottom-right corner, click on the right arrow icon to proceed.
9. To verify your domain, add the appropriate TXT record to DNS then click **verify**.
10. An informational message will state that the domain was successfully verified.
11. Click the check mark in the bottom-right corner to complete the process.



## Add Users and Groups

In this exercise you will explore some user and group management tasks using the Azure Portal. You will create a new user, create a new group, and add a user to a group.

1. From the Microsoft Azure Classic Portal, click **Active Directory**.
2. Click **Default Directory**.
3. If a dialog box showcasing the features of Azure Active Directory is displayed, close the window.
4. Once the directory is ready, at the top of the page, click **USERS**.
5. On the bottom of the page, click **ADD USER**.
6. On the first page of the ADD USER wizard, use the following information to complete the form:
  - a. TYPE OF USER: New user in your organization
  - b. USER NAME: <YourUserName> @ <YourDomainName>
7. In the lower-right corner of the page, click the right arrow icon.
8. On the user profile page, use the following information to complete the form:
  - a. FIRST NAME: <YourFirstName>
  - b. LAST NAME: <YourLastName>
  - c. DISPLAY NAME: <YourDisplayName>
  - d. ROLE: User
9. In the lower-right corner of the page, click the right arrow icon.
10. Click **create** on the get temporary password page.
11. Note the password.
12. In the lower-right corner of the page, click the checkmark to complete the wizard.
13. Click **GROUPS** at the top of the page.
14. In the middle of the page, click **ADD A GROUP**.
15. In the Add Group wizard, use the following information to complete the form:

- a. NAME: <YourGroupName>
  - b. GROUP TYPE: Security
  - c. Description: <YourDescription>
16. In the lower-right corner of the page, click the checkmark to complete the wizard.
17. To add a user to this group, click on the group that you just created.
18. Click **ADD MEMBERS**.
19. The Azure interface will display a list of users. Click the user account that you just created.
20. In the lower-right corner of the page, click the checkmark to complete the wizard.



## Enable MFA for Admin Accounts

In this exercise you will create a new admin account and enable MFA for the account. Note that you can enable MFA in multiple ways. This particular method shows how to do it in the process of creating a new user.

1. Navigate to the new Azure Portal at <https://portal.azure.com> and sign in.
2. From the Microsoft Azure Classic Portal, click **Active Directory**.
3. Click **Default Directory**.
4. At the top of the page, click **USERS**.
5. On the bottom of the page, click **ADD USER**.
6. On the first page of the ADD USER wizard, use the following information to complete the form:
  - TYPE OF USER: New user in your organization
  - USER NAME: <YourUserName> @ <YourDomain>
7. In the lower-right corner of the page, click the right arrow icon.
8. On the user profile page, use the following information:
  - FIRST NAME: <YourFirstName>
  - LAST NAME: <YourLastName>
  - DISPLAY NAME: <YourDisplayName>
  - ROLE: Global Admin
  - ALTERNATE EMAIL ADDRESS: <YourAlternateEmailAddress>
9. Click the checkbox to enable Multi-Factor Authentication.
10. In the lower-right corner of the page, click the right arrow icon.
11. Click **create** on the get temporary password page.
12. Note the password.
13. In the lower-right corner of the page, click the checkmark to complete the wizard.

## 2 | Security



### Enable Azure Security Center

In this exercise, you will enable the Security Center in the Azure portal and then configure some of the basic settings.

1. Navigate to the Azure portal and sign in.
2. In the left pane, click **Security Center**.
3. On the Security Center – Welcome screen, click **Yes! I want to Launch Azure Security Center**.
4. You will notice a blue information message stating Security Center is starting and analyzing your data for the first time. This might take a couple of minutes.
5. You may receive a prompt to enable data collection for your subscription(s) to enable all security controls. Click the message at the top of the Security Center blade. On the Security policy blade, ensure Data collection is set to **On**.
6. Under Policy components, click **Prevention policy** and review the listed recommendations. For example, you can enable or disable recommendations for System updates or OS vulnerabilities by turning them on or off.
7. Under Policy components, click **Email notifications**.
8. Enter your contact email address and phone number information.
9. Under Send me emails, set the **Send me emails about alerts** option to **On** and then click **OK**.
10. Under Policy components, click **Pricing tier**.
11. Click **Standard – Free Trial** and click **Select**. The standard tier adds additional features, such as advanced threat detections and is free for 90 days.
12. On the Security policy blade, click **Save**.



13. On the menu bar, monitor the alerts for progress as settings are processed.
14. On the Security Center – Security policy blade, pin the blade to your dashboard.



## Using Security Center

In this exercise, you will use the Azure Security Center to review security health and recommendations. Once the scans are run and the recommendations are available, you will walk through some of the remediation steps.

1. Navigate to the Azure Portal and sign in.
2. On the Dashboard, click **Security Center**.
3. On the Security Center – Overview blade, under Prevention, you will be presented with a high level status of all resources containing both High Severity and Low Severity indicators.
4. You will notice a Recommendations graphic that encompasses all resources. Click **Recommendations** to review the list. When viewing the recommendations for the first time, it may take a few minutes for Azure to generate the list.
5. On the Recommendations blade, you will see a recommendation to Install Endpoint Protection on two virtual machines with a High Severity designation. Click **Install Endpoint Protection**.
6. On the Install Endpoint Protection blade, click **Install on 2 VMs**.
7. On the Select Endpoint Protection blade, click **Microsoft Antimalware** then click **Create**.
8. On the Install Microsoft Antimalware blade, click **OK**.
9. On the menu bar, monitor the alerts for progress as endpoint protection is being installed to your two Windows virtual machines.
10. Return to the Recommendations blade and click **Add a Next Generation Firewall** for your 3 endpoints.

11. On the Add a Next Generation Firewall blade, click **Linux-ip** and then click **Create New**.
12. On the Create a New Next Generation Firewall, click **Barracuda Networks, Inc.** then click **Create**.
13. On the Create virtual machine menu, on the Basics blade, configure the virtual machine with the standard configuration and click **OK**.
14. On the Purchase blade, click **Purchase** to purchase the Barracuda NextGen Firewall F-Series then click **Create**.
15. On the menu bar, monitor the alerts for progress as the next generation firewall virtual machine is being deployed.
16. On the Recommendations blade, click **Enable Transparent Data Encryption** for the Sample database.
17. On the Enable Transparent Data Encryption on SQL databases blade, click **Sample**.
18. On the Transparent data encryption blade, select **On** then click **Save**.
19. You can review the Encryption status in real time on this blade. After a few moments, encryption will be enabled.
20. On the Recommendations blade, you will eventually see that some of the items have an updated state showing that they have been resolved.
21. Click **Filter** under Recommendations and uncheck the **Resolved** status.
22. In the background, you will see some of the recommendations disappear.
23. Close the Filter blade to return to the Recommendations menu.
24. Once you receive the alert that the Next Generation Firewall solution has been successfully provisioned, click **Add a Next Generation Firewall** on the Recommendations blade.
25. You should see the two previously deployed Windows Server 2016 virtual machines. Click **SERVER-01-ip**.
26. Select the Barracuda Networks, Inc. Next Generation Firewall from this menu and click **OK**.
27. Repeat the steps for SERVER-02-ip.
28. Explore the partner solutions (optional) by clicking **Partner solutions** on the Security Center blade. This will enable you to view all partner solutions connected to Azure Security Center. It also provides recommendations for resources that are linked to this partner solution.

## 3 | Virtual Machines



### Deploy a New Virtual Machine

In this exercise you will create a new virtual machine with a Resource Manager deployment model.

1. Navigate to the new Azure Portal at <https://portal.azure.com> and sign in.
2. On the Hub menu, click **New**.
3. On the New blade, search for **Server 2012 R2**.
4. In the search results, click **Windows Server 2012 R2 Datacenter**.
5. In the Everything blade, click **Windows Server 2012 R2 Datacenter**.
6. On the Windows Server 2016 R2 Datacenter blade, notice the default deployment model is set to Resource Manager. Click **Create**.
7. On the Create Virtual Machine blade, fill in the following values for basic settings (substituting your information for the user name, subscription, and location) and click **OK**.
  - Name: **SERVER-01**
  - VM disk type: **HDD**
  - User name: **<Your first name>**
  - Password: **Pa\$\$w0rd12345**
  - Subscription: **<Your subscription>**
  - Resource group: Create a new one named **"Server2012R2-template"**
  - Location: **<Your location>**
8. On the Choose a size blade, click **View all**. Click the **A0 Basic** size and then click **Select**.
9. On the Settings blade, review the default options for storage, network, extensions, high availability, and monitoring. Click **OK**.

10. On the Summary blade, review the configuration and then click **OK**.
11. When the VM creation finishes, click **Virtual machines** in the left pane.
12. In the Virtual machines blade, click the server name for the VM that you deployed.
13. In the Server-01 blade, click **Stop** at the top of the blade to stop the VM. This ensures that you don't consume resources unnecessarily.



## Create a Windows Server 2016 Nano Server in Azure

In this task, you will create a Windows Nano virtual machine in Azure.

1. If you are not signed in to the Azure portal from the previous steps, navigate to <https://portal.azure.com/> and, when prompted, sign in with the credentials provided to you for this lab.
2. In the hub menu, on the left-hand side of the portal page, click **New (+) > Compute > See all**
3. Select **Windows Server**. A scroll list of **Windows Servers** is displayed on the right side of the portal.
4. Scroll down and select **Windows Server 2016 – Nano Server**, then click **Create**.
5. On the Basics blade, enter a **Name** for the virtual machine. The name must be 1-15 characters long and it cannot contain special characters. For this exercise, use the name:
  - **Nano-VM1**
6. Select the **VM disk type**. You have the choice between **SSD** and **HDD**. For this exercise, make sure to select:
  - **HDD**.
7. Enter a User name, and a strong Password that will be used to create a local account on the VM. The local account is used to sign in to and manage the VM. For this exercise, use the following username and password:
  - **Student**

- **Pa55w0rd1234**
8. Select an existing **Resource group** or type the name for a new one. (see terminology in Module 2 for Resource group information). In this exercise, you will use the existing resource group that automatically appears in the **Resource group** drop down list.
  9. Select an Azure Datacenter Location such as East US. Click **OK**.
  10. Choose a VM size, and then click **Select** to continue. For this exercise, use:
    - **Standard\_A1**
  11. Select not to use managed disks.
  12. To allow PowerShell Remoting, click on the **Network Security Group (firewall)** blade.
  13. Select **Create New**.
  14. On the **Create network security group**, remove the predefined **default-allow-rdp** rule and replace it with a new rule with the following settings:
    - Name: **WinRM-https**
    - Priority: **1000**
    - Source: **Any**
    - Service: **WinRM**
    - Action: **Allow**
  15. Make sure that the validation passes and, on the Summary blade, click **OK**.

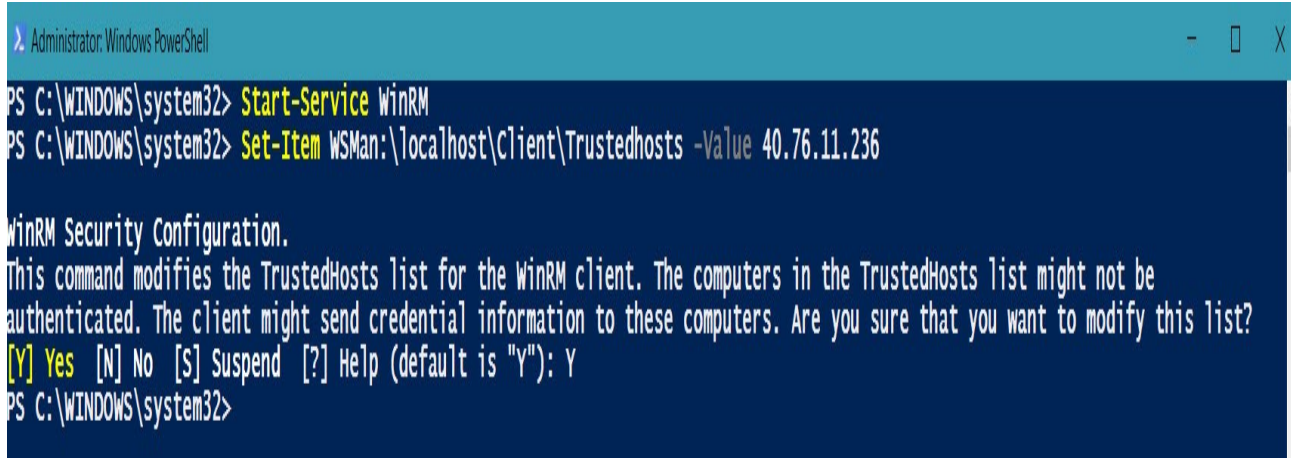
On the Azure portal dashboard, you will see the Nano Server being deployed. Once it is up and running you will see the **Overview > Essentials** section of the blade of the new server.



## Connect to Windows Server 2016 Nano Server in Azure

In this task, you will connect to a Windows Nano virtual machine in Azure.

In this task, you will connect to the Nano server you deployed in the previous task. In the Azure portal, in the **Overview > Essentials** section of the blade of the new Nano server, take the note of its public IP address. You can connect to the Nano server using the public IP address and PowerShell remoting. Note: PowerShell Remoting must be setup on the machine you are using to connect to the Nano server. Also, you will need to add the Nano Server to your trusted host group.



```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Start-Service WinRM
PS C:\WINDOWS\system32> Set-Item WSMan:\localhost\Client\Trustedhosts -Value 40.76.11.236

WinRM Security Configuration.
This command modifies the TrustedHosts list for the WinRM client. The computers in the TrustedHosts list might not be
authenticated. The client might send credential information to these computers. Are you sure that you want to modify this list?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
PS C:\WINDOWS\system32>
```

You can now connect to your Nano Server running in Azure. Watch this video “Nano Server and Azure PowerShell” for a look at some of PowerShell’s new features running on Nano Server in Azure. [Here](#)

## 4 | Storage



### Create a Storage Account (Portal)

In this exercise, you will create a new storage account in the Azure portal. Once created you will explore some of the basic file management capabilities, including the use of file shares.

1. Navigate to the new Azure Portal at <https://portal.azure.com> and sign in.
2. Click **Storage Accounts** on the Hub menu.
  - If you do not see Storage Accounts on the Hub menu, click **More Services**.
  - Type **storage accounts** in the filter to reveal the available options for managing storage accounts in the Azure Portal. Mark Storage Accounts as a favorite to pin it to your Hub menu.
3. On the **Storage accounts** blade, if you have any existing storage accounts they will appear in the list.
4. On the Storage accounts blade, click **Add**.
5. On the Create storage account blade, fill in the following values to create a new storage account. Click **Create** when you are finished entering the information. As you enter the information take a moment to use the **Information** icon to view details about the required information.
  - Name: **<your choice>**
  - Deployment model: **Resource Manager**
  - Account kind: **General purpose**
  - Performance: **Standard**
  - Replication: **Read-access geo-redundant storage (RA-GRS)**
  - Storage service encryption: **Disabled**
  - Subscription: **<YourSubscription>**
  - Resource Group: **<Create a new resource group>**
  - Location: **<YourLocation>**
6. On the menu bar, monitor the alerts for progress as the new storage account is created.
7. On the Hub menu, click **Storage accounts**. Confirm that the new storage account has been created.
8. Double-click your storage account and review the options that are available. Review the storage account Essentials area. Explore the Blobs, Files, Tables, and Queues areas.



## Install Azure Storage Explorer

In this exercise, you will install the Microsoft Azure Storage Explorer desktop application, connect to your Azure account, and explore the various options for managing your data in the Azure cloud.

1. Navigate to the [Storage Explorer](#) download site.
2. Download and install the appropriate version (Windows, Mac, or Linux).
3. Launch the tool.
4. In the Connect to Azure Storage window, ensure that the option to sign in using your Azure account is selected and then click **Connect**.
5. In the Sign in to your account window, enter your Azure administrative credentials and then click **Sign in**. Complete your authentication as needed (for example, if you have two-factor authentication enabled, you might be prompted for the second factor).
6. On the menu bar, click the person icon for Azure account settings.
7. Your Azure subscriptions for your account will be displayed. Click the checkbox for your Azure subscription (or click **All subscriptions**) and then click **Apply**.
8. Notice that you are able to view Local and Attached storage as well as your subscription storage.
9. If you followed the previous exercises you should see two storage accounts under your subscription.
10. Take a moment to browse the storage accounts. You may see diagnostic tables capturing metric data.

**Note:** Throughout the course make an effort to try to use this tool. You will find it easy to use.







## Install AZCopy

In this exercise you will install the AzCopy tool and explore the syntax.

1. Download and install the latest version of AzCopy -  
<http://aka.ms/downloadazcopy>.
2. Locate the executable which is typically installed in either  
%ProgramFiles(x86)%\Microsoft SDKs\Azure\AzCopy or  
%ProgramFiles%\Microsoft SDKs\Azure\AzCopy.
3. Open an elevated Command Prompt and navigate to the AZCopy installation directory.
4. View the Help pages for the utility.  
**AzCopy /?**
5. Read through the examples at the end of the Help page.

**Note:** Throughout the course make an effort to try to use this tool. You will find it easy to use.



## Working with Files (Portal and Storage Explorer)

In this exercise, you will explore some of the basic file management capabilities, including the use of file shares.

### Manage files in the portal

1. Navigate to the new Azure Portal at <https://portal.azure.com> and sign in.
2. On the Hub menu, click **Storage accounts**.
3. Select the storage account you created in Module 1.
4. On the storage account blade, review the list of available management options. Under File Services, click **Files**.
5. On the File service blade, click **+ File Share**.
6. On the New file share blade, fill in the following values to create a new file share. Use the information icon to learn about the quota. Click **Create** when you are finished entering the information.
  - Name: **<your choice>**
  - Quota: **5**
7. On the menu bar, monitor the alerts for progress as the new file share is created.
8. On the File service blade, click your new file share.
9. Notice the ability to **Connect**, **Upload**, **Add Directory**, and **Delete** share.
10. Select **More** and then **Properties**.
11. Copy the file share URL to Notepad. You will need this information to use Azcopy.
12. On the share blade, click **Upload**.
13. Create a new text file on your desktop. browse to and click the text file. Click **Upload**.
14. On the menu bar, monitor the alerts for progress as the text file is uploaded.
15. On the file share blade, confirm that the new file appears in the list.

16. Return to the storage account blade, and select your storage account,
17. Under Settings, click **Access Keys**.
18. Copy the primary key to the Notepad. You will need this information to use Azcopy.

## Manage files in Storage Explorer

1. When you are finished exploring the new storage account and file share, close the web page.
2. Switch to **Storage Explorer**.
3. Navigate to your storage account.
4. Click **File Shares**. Review the list of available files shares. Ensure your uploaded file is listed.
5. Notice that you can also right-click on File Shares and **Create File Share**.
6. As you have time experiment with creating other files shares, download, open, rename, and delete.

## Manage file with Azcopy

1. Open a command prompt and navigate to the Azcopy directory.
2. To copy files to your file share use this format:  
**AzCopy Source:<location of files to copy> /Dest:<file share URL>  
/Destkey:<access key>**
3. As you have time experiment with other Azcopy functionality such as creating a directory in your file share and downloading files.



## Files and Folders Backup

In this exercise, you will set up Azure Backup to backup on-premises files and folders.

**Note:** If you are having trouble with this lab, return to the course and watch the demonstration on backing up files and folders.

1. Navigate to the new Azure Portal at <https://portal.azure.com> and sign in.
2. On the Hub menu, click **More services**.
3. Type **recovery services** in the filter to reveal the available options for managing recovery services in the Azure Portal. Mark Recovery Services vault as a favorite to add it to your Hub menu.
4. On the Recovery Services vault blade, fill in the following values to create a new recovery services vault. Click **Create** when you are finished entering the information.

**Note:** You must select a resource group with a virtual machine in your location.

- Name: **<your choice>**
  - Subscription: **<your subscription>**
  - Resource Group: Create a new resource group **<your choice>**
  - Location: **<your location>**
5. On the menu bar, monitor the alerts for progress as the new recovery services vault is created.
  6. On the Hub menu, click **Recovery Services vault**. Confirm that the new recovery services vault has been created.
  7. Select your recovery services vault.
  8. On the **Settings** blade, explore the available options for managing the recovery services vault, such as backup, site recovery, jobs, and backup policies. Click **Backup**.
  9. For the backup goal, use the following information and then click **OK**.
    - Where is your workload running? **On-Premises**
    - What do you want to backup? **Files and Folders** {notice the other choices}
  10. Click the **Click here to prepare your infrastructure for backup to Azure** icon.
  11. Install the appropriate Backup Agent to your client or server machine and step through the Wizard.
    - Select an installation and cache folder.

- Specify how you want to connect to the Internet.
  - Acknowledge any prerequisite software that needs to be installed.
12. While you wait for the backup installation to complete, download the vault credentials from the portal. These credentials will be used to register the machine in the vault.
  13. When the Wizard finishes, click the **Proceed to Registration** link.
  14. Browse to your **vault credentials file**.
  15. Provide encryption settings for **passphrase** and **location** to save the passphrase.
  16. Wait for the server registration to complete.
  17. When the **Microsoft Azure Backup** wizard displays, select **Schedule Backup**.
  18. Proceed through the Wizard making your selections.
  19. After you have created the backup schedule, select **Backup Now**. Monitor the backup to ensure it succeeds.
  20. Return the portal and your recovery services vault.
  21. Confirm that your files and folders have been backed up and are now safely in the vault.



## Virtual Machine Backup

In this exercise, you will set up Azure Backup to backup a virtual machine. For this exercise you will need a virtual machine.

1. Navigate to the new Azure Portal at <https://portal.azure.com> and sign in.
2. On the Hub menu, click **More services**.
3. Click **Recovery Services vault**.
4. On the Recovery Services vault blade, click **Add**.
5. On the Recovery Services vault blade, fill in the following values to create a new recovery services vault. Click **Create** when you are finished entering the information.

**Note:** You must select a resource group with a virtual machine in your location.

- Name: **<your choice>**
  - Subscription: **<your subscription>**
  - Resource Group: Create a new resource group **<your choice>**
  - Location: **<your location>**
6. On the menu bar, monitor the alerts for progress as the new recovery services vault is created.
  7. On the Hub menu, click **Recovery Services vault**. Confirm that the new recovery services vault has been created.
  8. Select your recovery services vault.
  9. On the **Settings** blade, explore the available options for managing the recovery services vault, such as backup, site recovery, jobs, and backup policies. Click **Backup**.
  10. For the backup goal, use the following information and then click **OK**.
    - Where is your workload running? **Azure**
    - What do you want to backup? **Virtual machine**
  11. On Backup policy, notice there are two backup policies: **DefaultPolicy** and **Create New**.
  12. Select **Create New** and take a minute to review the different frequency and retention settings.
  13. Select **DefaultPolicy**, and click OK.
  14. For items to backup, click the checkbox next to your virtual machine and then click **Select**.
  15. Click **OK** to complete the backup configuration.
  16. On the menu bar, monitor the alerts for progress as the new backup configuration is deployed.
  17. On the Recovery Services vault page you can also monitor your backup job.

