Azure Security Step by Step Guide

Credit goes to Microsoft, these are the step by step examples at the end of each module in AZ-500 study material.

Table of Contents

Generate SAS tokens

Note

This demonstration requires a storage account with a blob container and an uploaded file. For the best results, upload a PNG or JPEG file.

In this task, we'll generate and test a Shared Access Signature.

1. Open the Azure portal.
2. Navigate to your **Storage Account**.
3. Under **Settings,** select **Access keys**.
4. Explain how Storage Account access keys can be used. Review regenerating keys.
5. Under **Settings,** select **Shared access signature**.
6. Explain how an account-level SAS can be used. Review the configuration settings, including **Allowed services**, **Allowed resource type**, **Allowed permissions**, and **Start and expiry date/times**.
7. Back at the Storage Account page, under **Blob service,** select **Containers**.
8. Right-click the blob file that you want to share and select **Generate SAS**.
9. Click **Generate SAS token and URL**.
10. Copy the **Blob SAS URL**. There's a clipboard icon on the far right of the text box.
11. Copy the URL into a browser, and your file should display.

Key Rollover

Note

Always use the latest version of Azure Storage Explorer.

In this task, we'll use Storage Explorer to test key rollover.

1. Download and install Azure Storage Explorer - https://azure.microsoft.com/features/storage-explorer/
2. After the installation, launch the tool.
3. Review the Release Notes and menu options.
4. If this is your first time using the tool, you'll need to re-enter your credentials.
5. After you've been authenticated, you can select the subscriptions of interest. Explain Storage Explorer can also be used for **Local and attached accounts**.
6. Right-click **Storage Accounts** and select **Connect to Azure storage**. Discuss the various connection options.
7. Select **Use a storage account name and key**.
8. In the **portal,** select your storage account.
9. Under **Settings,** select **Access Keys**. Retrieve the **Storage account name** and **key1** key.
10. In **Storage Explorer**, provide the account and key information, then click **Connect**.
11. Verify that you can navigate to your storage account content.
12. In the **portal** and your storage account.
13. Under **Settings,** select **Access Keys**.
14. Next to **key1** click the **Regenerate** icon.
15. Acknowledge the message that the current key will become immediately invalid and isn't recoverable.
16. In **Storage Explorer,** refresh the storage account.
17. You should receive an error that the server failed to authenticate the request.
18. Reconnect so you can continue with the demonstration.

Storage Access Policies

In this task, we'll create a blob storage access policy.

1. In the **Portal**, navigate to your Blob container.
2. Under **Settings**, select **Access Policy**.
3. Review the two policies: **Storage access policies** and **Blob immutable storage**.
4. Under **Stored access polices** click **Add policy**.
5. Create a policy with **Read** and **List** permissions and usable for a restricted period of time.
6. Under **Blob immutable storage,** click **Add policy**.
7. Review the two policy types: **Time-based retention** and **Legal hold**.
8. Create a policy based on time-based retention.
9. Be sure to **Save** your changes.
10. In Storage Explorer, right-click your container and select **Get shared access signature**.
11. The **Access Policy** drop-down enables you to create a SAS based on a pre-defined configuration.
12. As you have time, show how Storage Explorer can be used to perform security tasks.

Azure AD User Account Authentication

In this task, we will configure Azure AD user account authentication for storage.

1. In the portal, navigate to and select your blob container.
2. Notice at the top the authentication method. There are two choices: **Access key** and **Azure AD User Account**. Explain the differences between the two methods.
3. Switch to **Azure AD User Account**.
4. You should receive an error stating you don't have access permissions.
5. Click **Access Control (IAM)**.
6. Select **Add role assignment**.
7. Select the **Storage Blob Data Owner** role. Discuss the other storage roles that are shown.
8. Assign the role to your account and **Save** your changes.
9. Return to the **Overview** blade.
10. Switch to **Azure AD User Account**.
11. Notice that you're now able to view the container.
12. Take a minute to select **Change access level** and review the **Public access level** choices.

Storage Endpoints

Note

This task requires a storage account and virtual network with subnet. Storage Explorer is also required.

In this task, we'll secure a storage endpoint.

1. In the **Portal**.
2. Locate your storage account.
3. Create a **file share**, and **upload** a file.
4. Use the **Shared Access Signature** blade to **Generate SAS and connection string**.
5. Use Storage Explorer and the connection string to access the file share.
6. Ensure you can view your uploaded file.
7. Locate your virtual network, and then select a subnet in the virtual network.
8. Under **Service Endpoints**, view the **Services** drop-down and the different services that can be secured with an endpoint.
9. Check the **Microsoft.Storage** option.

10. **Save** your changes.
11. Return to your storage account.
12. Select **Firewalls and virtual networks**.
13. Change to **Selected networks**.
14. Add your virtual network and verify your subnet with the new service endpoint is listed.
15. **Save** your changes.
16. Return to the Storage Explorer.
17. **Refresh** the storage account.
18. Verify you can no longer access the file share.

Configure an app registration via the Azure portal

Note

The application registration process is constantly being updated and improved. Validate before your demo

In this exercise, we will demo how to register an application.

1. In the **Portal** search for and select **Azure Active Directory**.
2. Under **Manage** select **App registrations**.
3. Click **New registration**.
    - Name: **AZ500 app**
    - Review the **Supported app types**
    - Select **Accounts in this organizational directory only (Single tenant)**
    - Redirect URL > **Web**: **https://oauth.pstmn.io/v1/browser-callback**
    - Click **Register**
4. Wait for the application to register.
5. On the **Overview** tab, review the **Application (Client ID)**, **Directory (tenant ID)**, and **Object ID**.
6. Under **Manage** click **Certificates and Secrets**.
7. Review the use of client secrets that an application uses to prove its identity when requesting a token.
8. Click **New client secret**.
    - Description: **key1**
    - Expires: **In 1 year**
    - Click **Add**
9. Wait for the application credentials to update.

Create a key vault

In this task, we will create a key vault.

1. Sign in to the Azure portal and search for **Key Vaults**.
2. On the Key vaults page, click **+ Create**.
3. On the **Basics** tab, fill out the required information.
    - Discuss the **Pricing tier** selections, Standard and Premium. Premium supports HSM-backed keys.
    - Discuss **Soft delete** and **Retention period**.
4. Click **Review and Create** and then **Create**.
5. Wait for the new key vault to be created, or move to a key vault that has already been created.

Review key vault settings

In this task, we will review key vault settings.

1. In the Portal, navigate to the key vault.
2. Under the **Name** list, click the newly created **Key Vault**.
3. Under the **Objects**, click **Keys**.
4. Click **Generate/Import** and review the Keys configuration information.
5. Under **Settings**, click **Secrets**.
6. Click **Generate/Import**, review the Secrets configuration information, and click **Create**.
7. View the new Secret and note that keys support versioning.
8. Under **Settings**, click **Certificates**.
9. Click **Generate/Import** and review the Certificates configuration information.

Configure access policies

Note

To complete this demonstration you will need a non-privileged test user.

In this task, we will configure access policies and test access.

1. Continue in the Portal with your key vault.
2. Under **Settings**, click **Access Policies**.
3. Review the **Enable access to** choices: Azure Virtual Machines for deployment, Azure Resource Manager for template deployment, and Azure Disk Encryption for volume encryption.
4. Review the creator account **Key Permissions**. Note the **Cryptographic operation** permissions aren't assigned.
5. Review the creator account **Secret Permissions**. Note the **Purge** permission.
6. Review the creator account **Certificate Permissions**.
7. Open the **Cloud Shell** with the **Bash** option. You should be signed in as a Global Administrator.
8. Use your key information to verify the secret you created in the previous task displays successfully for this role.

   CLICopy

   ```
   az keyvault secret show --name <secret_name> --vault-name <keyvault_name>'
   ```

9. In another browser tab, open the portal, and sign-in as the test user.
10. Open the **Cloud Shell** with the **Bash** option.
11. Verify that the secret doesn't display for the test user. Access is denied.

    CLICopy

    ```
    az keyvault secret show --name <secret_name> --vault-name <keyvault_name>
    ```

12. Return to the Global Administrator account in the portal.
13. Add the Key Vault Contributor role to your test user.

14. Try the test user's access. Access is denied.

    CLICopy

    ```
    az keyvault secret show --name <secret_name> --vault-name <keyvault_name>
    ```

15. Explain that adding the RBAC role grants access to the Key Vault control plane. It doesn't grant access to the date in the Key Vault.
16. Return to your Key Vault and create an access policy.
17. Under **Settings**, select **Access policies** and then **Add Access Policy**.
    - Configure from the template (optional): **Key, Secret, & Certificate Management**
    - Key permissions: **none**
    - Secret permissions: **Get, List**
    - Certificate permissions: **none**
    - Select principal: **select your test user**
18. Be sure to **Add** your new access policy. And to **Save** your changes.
19. Try the test user's access. The user should now have access and the key should display.

    CLICopy

    ```
    az keyvault secret show --name <secret_name> --vault-name <keyvault_name>
    ```

20. As you have time, return to the Secret configuration settings and change **Enabled** to **No**. Be sure to save your changes, then try access the key again.

Use the Bastion service

Note

This task requires a virtual machine. If you are doing the next task, virtual machine updates, use a Windows virtual machine and keep the session running.

In this task, we will configure the Bastion service and connect to a virtual machine with service.

Configure the Bastion service

1. In the **Portal** navigate to your Windows virtual machine.
2. Ensure the virtual machine is **Running**.
3. Click **Connect** and select **Bastion**.
4. Click **Use Bastion**. Note installing the service is only required once.
5. Because you are creating the Bastion service from the target virtual machine, mention that most of the networking information has automatically been filled in. Note the Bastion service will be assigned a public IP address.
6. To create the Bastion subnet in the virtual network, click **Manage subnet configuration**.
7. On the virtual network subnet blade, click **+ Subnet**.
8. On the Add subnet page, type **AzureBastionSubnet** as the subnet name. Note this name cannot be changed.
9. Specify the address range in CIDR notation. For example, **10.1.1.0/27**.
10. Click **Ok**, then click **Create**. It will take a few minutes for the service to deploy.

Connect to the virtual machine using Bastion

1. From the target virtual machine's **Overview** blade, select **Connect** and then **Bastion**
2. On the **Connect to Bastion** page, enter the virtual machine login credentials.
3. Notice the checkbox to open the session in a new window.
4. Click **Connect**. If you receive a message that popup windows are blocked, allow the session.
5. Once your session is connected, launch the Bastion clipboard access tool palette by selecting the two arrows. The arrows are located on the left center of the session. Explain this copy and paste feature.
6. In the **Portal**, navigate to the Bastion host and under **Settings** select **Sessions**.
7. Review the session management experience and the ability to delete a session.
8. As you have time, review the Bastion components and how this provides a secure way to access your virtual machines.

Virtual Machine Updates

Note

This task requires a virtual machine in the **running** state. You may want to enable **Update management** prior to this lesson.

In this task, we will review virtual machine update management.

1. In the **Portal**, navigate to your virtual machine.
2. Under **Operations** select **Update management**.
3. Select the Azure Log Analytics workspace and Automation account, and then click **Enable**.
4. Wait for update management to deploy. It can take up to 15 minutes for the deployment and longer for results to be provided.
5. Select **Missing Updates** and use the **Information link** to open the support article for the update.
6. Select **Schedule update deployment**.
7. Review the various options including maintenance windows, reboot options, scheduling, classifications, kbs to include and exclude.
8. You can view the status for the deployment on the **Update deployments** tab. The available values are not attempted, succeeded, and failed.

Virtual Machine Extensions

In this task, we will install the IaaSAntimalware extension.

1. In the **Portal**, select your virtual machine.
2. Under **Settings**, click **Extensions**. Review how extensions are used.
3. On the **Extensions** page, click **+ Add**.
4. Scroll through the available extensions and review what extensions are available.
5. Select **Microsoft Antimalware**. Discuss the features of this extension.
6. Click **Create**.
7. On the **Install extension** page use the informational icons to explain **Excluded files and locations**, **Excluded file extensions**, and **Excluded processes**.
8. Review **Real-time protection** and **Run a scheduled scan**.
9. Review other options of interest.
10. After the extension is deployed, the extensions page will show the **IaaSAntimalware** extension.

Disk Encryption

Note

This task requires a storage account.

In this task, we will enable disk encryption for a storage account.

Review encryption key options

1. In the Portal, access your storage account.
2. Under **Settings** select **Encryption**.
3. Review Storage Service Encryption and why it is used.
4. Review the two types of keys: Microsoft Managed Keys and Customer Managed Keys.
5. Select **Customer Managed Keys**.

Create the customer managed key

1. For **Encryption key** choose **Select from key vault**.
2. Click **Select a key vault and key**.
3. You will now create a new key vault. If you already had a key vault you could use that.
4. For **Key vault** select **Create new**.
    - Notice the key vault will be created in the same region as the storage account.
    - Give your key vault a name.
    - Click **Review + create**.
    - Once the validation passes, click **Create**.
    - Wait for the key vault to be created.
5. You will now create a key in the key vault. If you already had a key you could use that.
6. On the **Select key from Azure key vault page**, for **Key** select **Create new**.
    - Review the options for creating a key.
    - Give your key a name.
    - Notice the activation and expiration options.
    - Click **Create**.
7. Now that you have created a key vault and key, **Select** the key vault and key.
8. **Save** your changes on the **Encryption** page.
9. Review the information that is now available: **Current key**, **Automated key rotation**, and **Key version in use**.

Review the key options

1. Return to the resource group that includes your storage account.
2. **Refresh** the page and ensure your new key vault is listed as a resource.
3. Select the key vault.
4. Under **Settings** click **Keys**.
5. Ensure your new key is **Enabled**. Notice the ability to regenerate the key.
6. Select the key and review the current version information.
7. Return to the key vault page.
8. Under **Settings** select **Access policies**.
9. Under **Current access policies** your storage account will be listed.
10. Notice the drop-downs for **Key Permissions**, **Secret Permissions**, and **Certificate Permissions**.

11. Select **Key Permissions** and notice the properties that are checked (Get, Unwrap key, and Wrap key).

Use RDP to connect to a Windows VM (optional)

Note

This task requires a Windows VM with a public IP address. You also need the login credentials for the machine.

In this task, we will use RDP to connect to a Windows virtual machine.

1. In the **Portal** navigate to your Windows virtual machine.
2. Ensure the virtual machine is **Running**.
3. From the **Overview** blade select **Connect** and then **RDP**.
4. In the **Connect to virtual machine** page, keep the default options to connect by DNS name over port 3389 and click **Download RDP file**.
5. Mention that if the VM has a just-in-time policy set, you first need to select the **Request access** button to request access before you can download the RDP file.
6. Open the downloaded RDP file and then click **Connect**.
7. In the **Windows Security** window, select **More choices** and then **Use a different account**.
8. Type the username as localhost\username, enter password you created for the virtual machine, and then select **OK**.
9. You may receive a certificate warning during the sign-in process. Select **Yes** or **Continue** to create the connection.
10. Explain how RDP is different from the Bastion service.

Use SSH to connect to a Linux VM (optional)

Note

This task requires a Linux VM. Ensure port 22 is open.

In this task, we will create a SSH private key with PuTTYgen, and then use SSH to connect to a Linux virtual machine.

Create the SSH Keys

1. Download the PuTTY tool. This will include PuTTYgen - https://putty.org/.
2. Once installed, locate and open the **PuTTYgen** program.
3. In the **Parameters** option group choose **RSA**.
4. Click the **Generate** button.
5. Move your mouse around the blank area in the window to generate some randomness.
6. Copy the text of the **Public key for pasting into authorized keys file**.
7. Optionally you can specify a **Key passphrase** and then **Confirm passphrase.** You will be prompted for the passphrase when you authenticate to the VM with your private SSH key. Without a passphrase, if someone obtains your private key, they can sign in to any VM or service that uses that key. We recommend you create a passphrase. However, if you forget the passphrase, there is no way to recover it.
8. Click **Save private key**.
9. Choose a location and filename and click **Save**. You will need this file to access the VM.

Create the Linux machine and assign the public SSH key

1. In the portal navigate to your Linux machine.
2. Choose **SSH Public Key** for the **Authentication type** (instead of **Password**).
3. Provide a **Username**.
4. Paste the public SSH key from PuTTY into the **SSH public key** text area. Ensure the key validates with a checkmark.
5. Create the VM. Wait for it to deploy.
6. Access the running VM.
7. From the **Overview** blade, click **Connect**.
8. Make a note of your login information including user and public IP address.

Access the server using SSH

1. Open the **PuTTY** tool.
2. Enter **username@publicIpAddress** where username is the value you assigned when creating the VM and publicIpAddress is the value you obtained from the Azure portal.
3. Specify **22** for the **Port**.
4. Choose **SSH** in the **Connection Type** option group.
5. Navigate to **SSH** in the Category panel, then click **Auth**.
6. Click the **Browse** button next to **Private key file for authentication**.
7. Navigate to the private key file saved when you generated the SSH keys and click **Open**.
8. From the main PuTTY screen click **Open.**
9. You will now be connected to your server command line.
10. Explain how SSH is different from the Bastion service.

Network security groups

This task requires a Windows virtual machine associated with a network security group. The NSG should have an inbound security rule that allows RDP. The virtual machine should be in a running state and have a public IP address.

In this task, we will review networking rules, confirm the public IP page does not display, configure an inbound NSG rule, and confirm the public IP page now displays.

Review networking rules

1. In the **Portal**, navigate to your virtual machine.
2. Under **Settings**, click **Networking**.
3. Discuss the default inbound and outbound rules.
4. Review the inbound rules and ensure RDP is allowed.
5. Make a note of the public IP address.

Connect to the virtual machine and test the public IP address

1. From the **Overview** blade, click **Connect** and RDP into the virtual machine.
2. On the **virtual machine**, open a **browser**.
3. Test the default localhost IIS HTML page: `http://localhost/default.htm`. This page should appear.
4. Test the default public IP IIS HTML page: `http://public_IP_address/default.htm`. This page should not display.

Configure an inbound rule to allow public access on port 80

1. Return to the **Portal** and the **Networking** blade.
2. Make a note of the virtual machine's **private IP** address.
3. On the **Inbound port rules** tab, click **Add inbound port rule**. This rule will only allow certain IP addresses on port 80. As you go through the configuration settings, be sure to discuss each one.
    - Source: **Service Tag**
    - Source service tag: **Internet**
    - Destination: **IP addresses**
    - Destination IP addresses/CIDR range: **private_IP_address/32**
    - Destination port range: **80**
    - Protocol: **TCP**
    - Action: **Allow**
    - Name: **Allow_Port_80**
    - Click **Add**
4. Wait for your new inbound rule to be added.

Retest the public IP address

1. On the **virtual machine,,** return to the **browser**.
2. Refresh the default public IP IIS HTML page: `http://public_IP_address/default.htm`. This page should now display.

Application service groups

This task requires a Windows virtual machine with IIS installed. These steps use VM1. Your machine name may be different.

In this task, we will connect to a virtual machine, create an inbound deny rule, configure an application security group, and test connectivity.

Connect to the virtual machine

1. In the **Portal**, navigate to **VM1**.
2. On the **Networking** blade, make a note of the private IP address.
3. Ensure there is an **Inbound port rule** that allows **RDP**.
4. From the **Overview** blade, ensure VM1 is **running**.
5. Click **Connect** and RDP into the VM1.
6. On **VM1**, open a browser.
7. Ensure the default IIS page display for the private IP address: `http://private_IP_address/default.htm`.

Add an inbound deny rule and test the rule

1. Continue in the **Portal** from the **Networking** blade.
2. On the **Inbound port rules** tab, click **Add inbound port rule**. Add a rule that denies all inbound traffic.
    - Destination port ranges: *
    - Action: **Deny**
    - Name: **Deny_All**
    - Click **Add**
3. Wait for your new inbound rule to be added.
4. On **VM1**, refresh the browser page: **`http://private_IP_address/default.htm`**.
5. Verify that the page does not display.

Configure an application security group

1. In the **Portal**, search for and select **Application security groups**.
2. Create a new Application security group.
3. Provide the required information: subscription, resource group, name, and region.
4. Wait for the ASG to deploy.
5. In the **Portal**, return to **VM1**.
6. On the **Networking** blade, select the **Application security groups** tab.
7. Click **Configure the application security groups**.
8. Select your new application security group, and **Save** your changes.
9. From the **Inbound port rules** tab, click **Add inbound rule**. This will allow the ASG.
    - Source: **Application security group**
    - Source application security group: **your_ASG**
    - Destination: **IP addresses**
    - Destination IP addresses: **private_IP_address/32**
    - Destination port range: **80**
    - Priority: **250**
    - Name: **Allow_ASG**
    - Click **Add**
10. Wait for your new inbound rule to be added.

Test the application security group

1. On **VM1**, refresh the browser page: `http://private_IP_address/default.htm`.
2. Verify that the page now displays.

VNet Peering

This lab requires two virtual machines. Each virtual machine should be in a different virtual network. For these instructions, we have AZ500vm01, AZ500vm02, AZ500-vnet, AZ500-vnet1, and az500-rg.

To save time, you can connect to each virtual machine. Also, it might be helpful to edit the default.htm page on each machine, so the page provides the virtual machine name. For example, This is AZ500vm01.

In this demonstration, you will configure and test VNet peering.

Review the infrastructure setup

In this task, you will review the infrastructure that has been configured for this demonstration.

1. In the **Portal**, navigate to **Virtual Machines**.
2. Show there are two virtual machines, **AZ500vm01** and **AZ500vm02**.
3. Select **AZ500vm01** and review the IP addresses.
4. Select **AZ500vm02** and review the IP addresses. Make a note of the private IP address.
5. Based on the addressing, discuss how each machine is in a different subnet.
6. In the **Portal** navigate to **Virtual networks**.
7. Show there are two virtual networks, **AZ500-vnet** and **AZ500-vnet1**.

Test the virtual machine connections

In this task, you will test connecting from AZ500vm01 to AZ500vm02's private IP address. This connection will not work. The virtual machines are in different virtual networks.

1. Use RDP to connect to **AZ500vm01**.
2. In a **browser**, view the **http://localhost.default.htm** page.
3. This page should display without error.
4. Use RDP to connect to **AZ500vm02**
5. In a **browser**, view the **http://localhost.default.htm** page.
6. This page should display without error.
7. The above steps show that IIS is working on the virtual machines.
8. Return to your **AZ500vm01** RDP session.
9. We will now try to access **AZ500vm02**.
10. In a browser, view the **http://private_IP_address_of_AZ500vm02/default.htm** page.
11. The page will not display.
12. AZ500vm01 cannot access AZ500vm02 using the private address.

Configure VNet peering and test the connections

In this task, you will configure VNet peering and test the previous connection. The connection will now work.

1. In the **Portal**, navigate to the **AZ500-vnet** virtual network.
2. Under **Settings** select **Peerings**.
3. **+ Add** a virtual network peering. The page adapts as you make selections.
    - Name of the peering from az500-vnet to remote virtual network: **Peering-A-to-B**
    - Virtual network: **AZ500-vnet1 (az500-rg)**
    - Name of the peering from az500-vnet1 to az500-vnet: **Peering-B-to-A**
    - Discuss the other configuration options.
    - Click **OK**.
4. Follow the notifications while the virtual network peerings are deployed.
5. Return to your **AZ500vm01** RDP session.
6. In the browser, refresh the **http://private_IP_address_of_AZ500vm02/default.htm** page.
7. This page should now display.

Azure Firewall

This task requires a virtual network with two subnets, Subnet1 and Jumpnet. Subnet1 has the 10.0.0.0/24 address range. Jumpnet has the 10.0.1.0/24 address range. Subnet1 includes a Windows virtual machine. Your resource names may be different.

Configure the firewall subnet

1. In the **Portal**, select your virtual network.
2. Under **Settings**, select **Subnets**.
3. Click **+ Subnet** to add a new subnet for the firewall.
    - Name: **AzureFirewallSubnet**
    - Address range: **10.0.2.0/24**
    - There is not need for a NAT Gateway, NSG, Route table, or services.
    - Click **Add**.
4. Wait for the subnet to deploy.

Add and configure the firewall

1. Search for and select **Firewalls**.
2. Discuss the benefits of a firewall and how it can be used to increase perimeter security.
3. Click **+ Add**.
4. Complete the required configuration information: subscription, resource group, name, and region.
5. Select your **Virtual network**.
6. Add a new **Firewall public IP address**.
7. Create the firewall and wait for it to deploy.
8. Navigate to your new firewall.
9. On the **Overview** blade, locate the **Firewall private IP**.
10. Copy the address to the clipboard.

Create a route table and route that uses the firewall

1. Search for and select **Route tables**.
2. **Add** a new route table.
3. Complete the required configuration information: name, subscription, resource group, and location.
4. Disable **Virtual network gateway route propagation**. Review what this means.
5. Create the route table and wait for it to deploy.
6. Navigate to the new route table.
7. Under **Settings**, click **Routes**.
8. **Add** a new route. This route will ensure traffic goes through the firewall. Discuss the different next hop types.
    - Route name: **your choice**
    - Address prefix: **0.0.0.0/0/**
    - Next hop type: **Virtual appliance**
    - Next hope address: **Firewall_private_IP_address**
9. When finished click **Ok** and wait for the new route to deploy.

Associate the route table with Subnet1

1. Still in the route table resource, under **Settings** click **Subnets**.
2. **Associate** your virtual network and **Subnet1**. This will ensure Subnet1 uses the route table.
3. When you are finished click **Ok** and wait for the association to complete.

Test the firewall

1. In the **Portal**, navigate to a virtual machine in Subnet1.
2. From the **Overview** blade, ensure the VM is **running**.
3. Click **Connect** and RDP into the VM.
4. On the virtual machine, open a browser.
5. Try to access: www.msn.com.
6. Notice the error. Action denied. No rule matches.

Add a firewall application rule

1. In the **Portal**, navigate to your firewall.
2. Under **Settings** select **Rules**.
3. Select the **Application rule selection** tab.
4. Click **Add application rule collection**.
5. Review how application rules work and complete the required information.
    - Name: **your choice**
    - Priority: **300**
    - Action: **Allow**

6. Continue completing the rule, under **Target FQDNs**. This will allow Subnet1 IP address to traverse the firewall.
    - Name: **Allow-MSN**
    - Source type: **IP address**
    - Source: **10.0.0.0/24**
    - Protocol:Port: **http,https**
    - Target FQDNs: **www.msn.com**
7. Click **Add** and wait for the firewall to be updated.

Test the firewall again

1. In your VM RDP session, refresh the browser page.
2. The MSN.com page should now display.

Azure AD PIM for roles

In this task, we will configure PIM activation settings, add the Billing Administrator as a PIM role, activate the role, and test activation.

Configure PIM settings

Note

This task requires a **AZ500User1** account with no assigned roles.

In this task, we will review and configure the basic PIM settings.

1. In the **Portal**, search for and select **Azure AD Privileged Identity Management**.
2. Under **Manage** select **Azure AD Roles**.
3. Under **Manage** select **Settings**.
4. Select the **Billing Administrator** role.
5. Click **Edit**.
6. Notice the **Activation**, **Assignment**, and **Notification** tabs.
7. By default, MFA is required on activation. For this demonstration, change the requirement to **None**.
8. Check the box to **Require approval to activate**.
9. Discuss the other possible settings including **Activation maximum duration** and **Require approval to activate**.
10. Switch to the **Assignment** tab and require the settings.
11. Notice the ability to expire eligible and active assignments.
12. Switch to the **Notifications** tab and discuss the settings.
13. Notice you can send notifications when members are assigned and activated.
14. Click **Update**.

Configure PIM for Roles

In this task, we will add the Billing Administrator role to PIM.

1. In the **Portal**, search for and select **Azure AD Privileged Identity Management**.
2. Under **Manage** select **Azure AD Roles**.
3. Under**Manage** select **Roles**.
4. Review the list of roles.

5. Select the **Billing Administrator** role.
6. Review **Eligible roles** and **Active roles**.
7. Click **Add member**.
8. Click **Select member** and **Select** the **AZ500User1** user. You are now a Billing Administrator.
9. Select **Set membership settings**. Notice the settings can be permanent or limited in time.
    - Assignment type: **Eligible**
    - Permanently eligible: **check the box**.
10. **Save** your changes and **Add** the assignment.
11. Verify the Billing Administrator is listed as an eligible role.

Activate a role

In this task, we will activate the Billing Administrator role.

1. In the **Portal**, search for and select **Azure Active Directory**.
2. Under **Manage** click **Users**.
3. Select **AZ500User1**.
4. Under **Manage** click **Assigned roles**.
5. Verify the user is not assigned to any roles.
6. Sign in the **Portal** as **AZ500User1**.
7. Search for and select **Azure AD Privileged Identity Management**.
8. Under **Tasks** select **My roles**.
9. Under **Activate** select **Azure AD Roles**.
10. Select the **Active roles** and verify there are no roles listed.
11. On the **Eligible roles** tab notice the **Billing Administrator** role.
12. Under the **Action** column, select **Activate**.
13. **Assignment details** are shown in the Portal. This includes start and end times, and the ability to add a reason.
14. Add a reason and then click **Activate**.
15. The **Activation status** should show all the activation stages have been completed.
16. Use the link to **Sign out**.
17. You must sign out and log back in to start using your newly activated role.

Test the role access

In this task, test the Billing Administrator role.

1. Sign in to the Portal as **AZ500User1**.
2. Search for and select **Azure AD Privileged Identity Management**.
3. Under **Activate** select **Azure AD Roles**.
4. Select the **Active roles** tab and verify the **Billing Administrator** role has been activated.
5. The role should show **Activated**.
6. Notice the ability to **Deactivate** the role.

Azure AD PIM for resources

In this task, we will configure PIM for Azure resources, activate the Virtual Machine Contributor role, and test the role access.

Configure PIM for Azure resources

In this task, we will add the subscription to PIM, then add the Virtual Machine Contributor role as an Active role.

1. In the **Portal**, search for and select **Azure AD Privileged Identity Management**.
2. Under **Manage** select **Azure Resources**.
3. Click **Discover resources**.
4. Notice the **Resource state** is **Unmanaged**.
5. Select the subscription you want to manage.
6. Click **Manage resource**.
7. Click **Yes** to confirm that PIM will manage all child objects for the selected resource.
8. Return to the **Azure resources** blade.
9. Select your subscription.
10. Under **Manage** click **Roles**.
11. Search for and select the **Virtual machine contributor** role.
12. Click **Add assignments**, then click **Select member(s)** and add the **AZ500User1** to the group.
13. On the **Membership settings** page set the **Assignment type** is **Active**.
14. **Add** the role and **Save** your changes.
15. Sign out of the Portal.

Activate the role

In this task, we will sign-in as a user and activate the role.

1. Sign in to the **Portal** and **AZ500User1**.
2. Search for and select **Azure AD Privileged Identity Management**.
3. Under **Tasks** select **My roles**.
4. Under **Activate** select **Azure resources**.
5. On the **Active roles** tab notice you have no assigned roles.
6. On the **Eligible roles** tab scroll to the right and **Activate** the role.
7. Notice the **Start time** and **Duration**.
8. Provide a reason for the activation. For example, 'Need to add a NIC'.
9. Click **Activate**.
10. The **Activation status** should show all the activation stages have been completed.
11. Use the link to **Sign out**.
12. You must sign out and log back in to start using your newly activated role.

Test the role access

In this task, we will check to ensure the role has been assigned.

1. Sign in to the Portal as **AZ500User1**.
2. Search for and select **Azure AD Privileged Identity Management**.
3. Under **Activate** select **Azure resources**.
4. Select the **Active roles** tab and verify the **Virtual Machine Contributor** role has been activated.
5. Sign out of the Portal.
6. Sign in to the Portal using a Global Admin account.
7. Search for and select **Azure Active Directory**.
8. Under **Manage** click **Users**.
9. Select **AZ500User1**.
10. Under **Manage** click **Assigned roles**.

11. Verify there are no roles listed.
12. Under **Manage** select **Azure role assignments**.
13. Verify the **Virtual machine contributor** role is listed.

Configure conditional access (require MFA)

Note

This task requires a user account, AZ500User1. If you want to show the MFA verification, the user account must have a phone number.

This task will review conditional access policy settings and create a policy that requires MFA when signing in to the Portal.

Configure the policy

1. In the **Portal,** search for and select **Azure Active Directory**.
2. Under **Manage,** select **Security**.
3. Under **Protect,** select **Conditional access**.
4. Click **New Policy**.
    - Name: **AZ500Policy1**
    - Users and groups > Select users and groups > Users and Groups > Select: **AZ500User1**
    - Cloud apps or actions > Select apps > Select: **Microsoft Azure Management**
    - Review the warning that this policy impacts Portal access.
    - Conditions > Sign-in risk > Review the risk levels
    - Device platforms > Review the devices that can be included, such as Android and iOS.
    - Locations > Review the physical location selections.
    - Under **Access controls** click **Grant**.
    - Review the Grant options such as MFA. You may require one or more of the controls.
    - Select **Require multi-factor authentication**.
    - For **Enable policy,** select **On**.
5. Click **Create**.

Test the policy

1. Sign in to the **Portal** as the **AZ500User1**.
2. Before you can sign in, a second authentication is required.
3. If you have a phone number associated with the user, provide and verify the text code. You should be able to sign in to the Portal successfully.
4. If you do not have a phone number associated with the user, this demonstrates that MFA is in effect.
5. You may want to return to the **AZ500Policy1** and turn the policy **Off**.

Access review

In this task, we will configure an access review.

Configure an access review

1. In the **Portal**, search for and select **Identity Governance**.

2. Under **Access Reviews,** select **Access Reviews**.
3. Click **New Access Review**.
4. We will create an access review to ensure we validate the AZ500Admin group membership.
5. Complete the required information and discuss each setting. Configuration settings are added as you make your selections. For example, if you select a weekly access review, you will be prompted for the duration.
    - Review name: **AZ500Review**
    - Start date: **current date**
    - Frequency: **One-time**
    - Users to review: **Members of a group**
    - Scope: **Everyone**
    - Select a group: **AZ500Admins**
    - Reviewers: **Selected user**
    - Select reviewers: **add yourself as a reviewer**
    - Review the **Upon completion settings**, specifically the action if a reviewer doesn't respond.
    - Review **Advanced settings**.
6. **Start** the access review.
7. On the **Access review** page, ensure the new access review is listed.
8. The **Status** will change from **Not started** to **Initializing**.

Conduct an access review

In this task, we will conduct an access review.

1. When the access review is complete, you will receive an email. This is the email associated with your reviewer account.
2. View the email and discuss the review instructions. Note when the review period will end.
3. In the email, click **Start review**.
4. On the **Access reviews** page, click the **AZ500Review**.
5. Notice you are reviewing the AZ500Admin group members. There are two members.
6. Use the **Details** link to view information about the user.
7. Select **Approve** for one user and **Deny** for the other. Be sure to provide a **Reason**.
8. **Submit** your reviews.

Review the access review results

In this task, we will review the access review results.

1. Return to the **Portal**.
2. Click the **AZ500Review**.
3. From the **Overview** blade, review the results.
4. There should be one member **approved** and one member **denied**.
5. Click **Results** for more detailed information about the reviewer and their reasons.
6. From the **Overview** blade, click **Stop** and confirm you want to stop the review.
7. The **Review status** should now be **Complete**.

Apply the access review

In this task, we will apply the review results.

1. In the **Portal**, search for and select **Azure Active Directory**.

2. Under **Manage,** select **Groups**.
3. Locate the **AZ500Admins** group.
4. Review the members of the group.
5. Confirm there are two members.
6. Return to the **AZ500Review**.
7. Click **Apply**.
8. Confirm that you want to remove the denied member.
9. The **Review status** will change from **Applying** to **Result applied**.
10. Verify the **AZ500Admins** group now only has one member.

Review Azure AD

In this task, we'll review Azure Active Directory licensing and tenants.

1. In the **Portal**, search for and select **Azure Active Directory**.
2. On the **Overview** page, locate the license information.
3. Go to the Azure AD pricing page and review the features and pricing for each edition.

Manage users and groups

Note

This task requires some users and groups to be populated. Dynamic groups requires a Premium P1 license.

In this task, we'll create users and groups.

1. Under the **Manage** blade, click **Users**.
2. Review the different **Sources** such as **Windows Server AD**, **Invited User**, **Microsoft Account**, and **External Azure Active Directory**.
3. Notice the choice for **New guest user**.
4. Click **New user**.
5. Review the two ways to create a user: **Create user** and **Invite user**.
6. Create a new user. Review **Identity**, **Groups and roles**, **Settings**, and **Job Info**.
7. Navigate to Azure AD, under **Manage** click **Groups**.
8. Review the **Group types**: **Security** and **Microsoft 365**.
9. Create a new group by clicking "New Group" with the **Membership type** as **Assigned**.
10. Add a user to the same group.
11. Create another new group with **Membership type** as **Dynamic user**.
12. Review the details to construct dynamic group membership rules.

Multifactor authentication in Azure

Note

This task requires a user account, **AZ500User1**.

In this demonstration, we will configure and test MFA.

Configure MFA

In this task, we'll enable MFA for a user.

1. In the **Portal**, search for and select **Azure Active Directory**.
2. Under **Manage** select **Security**.
3. Under **Manage** select **MFA**.
4. In the center pane, under **Configure** select **Additional cloud-based MFA settings**.
5. Select the **Users** tab.
6. Select **AZ500User1**. Make a note of their user name in the form user@domain.com.
7. On the far right click **Enable**.
8. Read the information about enabling multifactor authentication in Azure.
9. Click **enable multi-factor auth**.
10. Wait for update. AZ500User1 will now be required to provide two factor authentication.

Test MFA

Note

To test MFA a phone number is required.

In this task, we'll test the MFA requirement.

1. Sign in to the **Portal** as **AZ500User1**. Use their user name from a previous step.
2. Provide the password, click **Next**.
3. More information is required. Click **Next**.
4. Review the **Additional security** verification page.
5. In Step 1, enter your phone number and ensure the **send me a code by text message** is selected.
6. Click **Next**.
7. In Step 2, enter the verification code from the text message.
8. Click **Verify**.
9. In Step 3, read about how to keep your existing applications working.
10. Click **Get started with this app password**.
11. If prompted, **Allow access**.
12. Click **Done**.
13. On the **Update password** screen, provide and confirm a new password.
14. Click **Sign-in**.
15. Confirm that you can now access the Portal.

Microsoft Defender for Cloud overview and recommendations

In this task, you will review Microsoft Defender for Cloud.

1. In the Portal, navigate to Microsoft Defender for Cloud.
2. Under **General**, select **Overview**.
3. Discuss the Overview page.
4. Under **Management**, select **Pricing and Settings**.
5. Select your subscription, and then review the **Microsoft Defender for Cloud features**.
6. Return to the main **Microsoft Defender for Cloud** blade.
7. Under **General**, select **Recommendations**.
8. Review **Secure Score**, **Recommendations status**, and **Resource Health**.
9. From the main **Microsoft Defender for Cloud** blade, under **Cloud Security**, select **Regulatory compliance**.
10. Review the compliance assessment and available compliance controls.

11. Scroll down and, under **Controls,** review several recommendations. For example, **Restrict unauthorized network access**, **Manage access and permissions**, and **Enable endpoint protection**.
12. From the main **Microsoft Defender for Cloud** blade, under **Cloud Security,** select **Workload protections**.
13. Review the **Defender for Cloud coverage**, **Security alerts**, and **Advanced protection** features.

Activity Logs and Alerts

In this task, we will configure an alert.

1. Sign into the **Portal**.
2. Search for and launch **Monitor**.
3. Review the capabilities of Monitor: **Monitor & Visualize Metrics**, **Query & Analyze Logs**, and **Setup Alerts & Actions**.
4. Select **Activity log**.
5. Under the filters, click **Timespan** and review the drop-down choices.
6. Open an event and discuss.
7. Back in the Monitor main page, click **Alerts** then click **+ New alert rule**.
8. Under **Resource** click **Select**.
9. Discuss how alerts can be scoped by subscription, resource type, and location.
10. Select a resource for the alert and then click **Done**.
11. Under **Condition** click **Add**.
12. Select a signal, such as **All Administrative operations**, and then click **Done**.
13. Under **Action group**, click **Create**. Review how action groups are used.
14. Under **Select an action type** review the various ways the action group can be alerted.
15. Select **Email/SMS/Push/Voice**.
16. Review the configuration choices and finish creating your action group.
17. Complete the **Alert details** and click **Create alert rule**.
18. On the **Alerts** page, review how you can search your alerts by resource and time range.

Log Analytics

This lab requires a virtual machine in a running state.

In this task, we will configure Log Analytics and run a query.

1. Sign into the **Portal**.
2. Search for and launch **Log Analytics workspaces**.
3. Click **Add** or **Create**.
4. On the **Basics** tab, review and complete the required information.
5. Under the Essentials view, review the **Pricing tier** detail (example: Pricing tier: Pay-as-you-go)
6. Finish creating the workspace and wait for it to deploy.
7. **Go to resource** and discuss how Log Analytics is used and configured.
8. Under **Workspace Data Sources** select **Virtual machines**.
9. Select a virtual machine and click **Connect**.
10. While you wait for the connection, under **Settings** click **Advanced settings**.
11. Click **Connected sources**. Discuss the possible sources like virtual machines and storage accounts.
12. Click **Data**. Review the different data sources.
13. Show how **Windows event logs** can be collected.
14. Save any changes you make.
15. Back at the Log Analytics workspace, Under **General** select **Logs**.
16. Review how log data is stored in tables and can be queried.
17. Select the **Event** table and then click **Run**.

18. Review the results.

Navigating Azure

In this task, you'll learn how to access and use the Azure portal.

Locate the Azure portal

In this task, you'll access the lab environment and the Azure portal.

1. Ask your instructor how to access the lab environment.
2. After accessing the lab environment, navigate to the Azure portal.
3. Bookmark this page. You'll use the Portal throughout the course labs and demonstrations.
4. In the top right corner of the Portal, select your user account.
5. Notice you can View account and Switch directory.
6. Switch directory lets you view My permissions and View my bill.
7. Select the **Settings** icon (top right menu bar - cog icon).
8. Review the **Portal settings** including the **General** and **Language & region** settings.
9. Use the Search resources, services, and docs textbox to search for Virtual machines.
10. You can search for not only general Azure resources but specifically but named resources.
11. Select Use the **Portal menu** (left corner three bars icon).
12. Notice you can Create a resource, view All services, and view All resources.
13. Take some time to browse around the interface, search and explore different areas.
14. Launch the **Cloud Shell** (first icon top menu bar).
15. Notice the drop-down for **PowerShell** or **Bash**.

Azure RBAC Role Assignments

In this task, we'll learn about role assignments.

Locate Access Control blade

1. Access the Azure portal, and select a resource group. Make a note of what resource group you use.
2. Select the Access Control (IAM) blade.
3. This blade is available for many different resources so you can control access.

Review role permissions

1. Click the **Roles** tab (top).
2. Select a desired role from the list by clicking the associated box next to the Role Name.
3. Click the **View** link under the **Details** column on the far right of the page.
4. The Permissions view is displayed including three columns from left to right that is (i.e., Other, Read, Write, and Delete) **Permissions**, and **Description**.
5. Return to the **Access Control (IAM)** blade.

Manage resource locks

Note: This task requires a resource group.

In this task, we'll create resource locks.

1. In the **Portal** navigate to a resource group.
2. In the **Settings** section, click **Locks**, and then click **+ Add**.
3. Discuss the different types of locks and applying the locks at different levels.
4. Create a new lock with a **Lock type** of **Delete**.
5. From the **Overview** blade, click **Delete resource group**. Type the name of the resource group and click **OK**.
6. You should receive an error message stating the resource group is locked and can't be deleted.
7. Add a **Storage Account** to the resource group.
8. After the storage account is created, try to delete the storage account.
9. You receive an error message stating the resource or its parent has a delete lock.
10. Review how the storage account inherits the lock from the parent and can't be deleted.
11. Return to the resource group blade and, in the **Settings** section, click **Locks**.
12. Scroll all the way to the right, then click the **Delete** link to the right of the lock.
13. Return to the storage account and confirm you can now delete the resource.

Azure SQL: Advanced Data Security and Auditing

In this task, we will explore vulnerability assessments, data discovery and classification, and auditing.

Install the AdventureWorks sample database

Skip this section if you already have a database to work with.

1. In the **Portal**, search for and a select **SQL databases**.
2. On the **Basics** tab, give your database a name, and create a new server.
3. On the **Additional settings** tab, select **Sample** for **Use existing data**. Also, **Enable advanced data security** and **Start free trial**.
4. **Review & create**, and then **Create**.
5. Wait for the database to deploy.

Review Vulnerability Assessments

1. Navigate to your SQL database.
2. Under **Security** select **Microsoft Defender for Cloud**.
3. Select **Vulnerability Assessment**.
4. Review vulnerability assessments and the risk levels.
5. Click **Scan**.
6. The scan doesn't need to be fully complete for results to show.
7. Review the **Findings**.
8. Click any **Security Check** to get more details.
9. Review the **Passed** checks.
10. Notice **Export Scan Results** and **Scan History**

Review Data Discovery and Classification

1. Return to the **Security** blade.
2. Select **Data Discovery & Classification**.
3. On the **Classification** tab, select **Add classification**.
    - Schema name: **SalesLT**
    - Table name: **Customer**
    - Column name: **Phone**

    - Information type: **Contact Info**
    - Sensitivity label: **Confidential**
4. When finished click **Add classification**.
5. Click the blue bar **columns with classification recommendations**.
6. Notice the data that has been recommended for classification.
7. Select the data of interest and then click **Accept selected recommendations**.
8. **Save** your changes.

Review Auditing

1. Return to your SQL database.
2. Under **Security** select **Auditing**.
    - Select **On** for auditing.
    - Click **Storage** for the destination.
    - Select on the Storage account for logs.
    - Set Retention day to **45** days.
    - Set storage access key to Primary.
3. **Save** your changes.
4. Discuss **Server level auditing** and when how it could be used.

Azure SQL: Diagnostics

Note

This demonstration requires an Azure SQL database.

In this task, we will review and configure SQL database diagnostics.

1. In the **Portal**, search for and launch **SQL databases**.
2. From the **Overview** blade, review the **Compute utilization** data graphic. Data is available for different time frames (1 hour, 24 hours, 7 days).
3. Under **Monitoring** select **Diagnostic settings**.
4. Click **Add diagnostic setting**.
5. Give your setting a name.
6. Under **Destination details** select **Send to Log Analytics**. Make a note of the Log Analytics workspace that will be used.
7. Under **Destination details** select **Archive to Storage Account**.
    - Select the **Errors** log.
    - Select the **Automatic tuning** log.
    - Select the **Basic** metric.
    - Give each item a **retention time** of 45 days. Retention only applies to storage account.
8. **Save** your diagnostic setting.
9. In the **Portal**, search for and launch the **Log Analytics workspace**.
10. Select the workspace that is being using for your database diagnostics.
11. Under **General** select **Usage and estimated costs**.
12. Click **Data retention**. Use the slider to show how to increase the data retention time. Discuss how additional charges can incur, depending on the pricing plan.
13. Under **General** select **Workspace summary**.
14. Click **Add** and then search the Marketplace for **Azure SQL**. This feature may be in Preview. Explain the benefits of using this product.
15. Select and then create **Azure SQL Analytics**.

16. It will take few minutes for the product to deploy.
17. Click **Go to resource** once the deployment is completed.
18. Click **Azure SQL databases**.
19. Review the additional metrics that are provided by this product.
20. You can drill into any graphic for additional details.

Azure SQL: Azure AD Authentication

Note

This task requires an Azure SQL database that has not had Azure AD configured. This task also requires SQL Server Management Studio.

In this task, we will configure Azure AD authentication.

1. In the **Portal**.
2. Navigate to your SQL database.
3. On the **Overview** page, there's an **Active Directory admin** box that shows the current status, configured or not configured.
4. Under **Settings** select **Active Directory admin**.
5. Click **Set admin**.
6. Search for and **Select** the new Active Directory admin. Remember this user you'll need in following steps.
7. Be sure to **Save** your changes.
8. In **SQL Server Management Studio** connect to the database server using your credentials.
9. Select the SQL database you configured with a new Active Directory admin.
10. Construct a query to create a new user. Insert the admin user and domain. For example, user@contoso.com
    - Create user [user@contoso.com] from external provider;
11. Run the query and ensure it completes successfully.
12. In the **Object Explorer** navigate your database and **Security** and **Users** folder.
13. Verify that the new admin user is shown.
14. **Connect** to the new database with the new admin credentials.
15. Verify that you can successfully access the database.