Contents

1 AZ-900T00 and AZ-900T01: Microsoft Azure Fundamentals

There is a Lab Recordings and Demos repo with links to videos of labs used in Microsoft Official Curriculum. The intent is to provide Microsoft Certified Trainers an easy way to access a non-audio version recording of hands-on labs used in the portfolio.

- **Link to Walkthroughs (HTML format)**
- **Are you a MCT?** - Have a look at our GitHub User Guide for MCTs

1.1 What are we doing?

- To support these courses, we will need to make frequent updates to the course content to keep it current with the Azure services used in the course. We are publishing the lab instructions on GitHub to allow for open contributions between the course authors and MCTs to keep the content current with changes in the Azure platform.
- We hope that this brings a sense of collaboration to the labs like we've never had before - when Azure changes and you find it first during a live delivery, go ahead and make an enhancement right in the lab source. Help your fellow MCTs.

1.2 How should I use these files relative to the released MOC files?

- The instructor handbook and PowerPoints are still going to be your primary source for teaching the course content.
- These files on GitHub are designed to be used in conjunction with the student handbook, but are in GitHub as a central repository so MCTs and course authors can have a shared source for the latest lab files.
- It will be recommended that for every delivery, trainers check GitHub for any changes that may have been made to support the latest Azure services, and get the latest files for their delivery.

1.3 What about changes to the student handbook?

- We will review the student handbook on a quarterly basis and update through the normal MOC release channels as needed.

1.4 How do I contribute?

- Any MCT can submit a pull request to the code or content in the GitHub repo, Microsoft and the course author will triage and include content and lab code changes as needed.
- You can submit bugs, changes, improvement and ideas. Find a new Azure feature before we have? Submit a new demo!

1.5 Notes

1.5.1 Classroom Materials

1.6 It is strongly recommended that MCTs and Partners access these materials and in turn, provide them separately to students. Pointing students directly to GitHub to access Lab steps as part of an ongoing class will require them to access yet another UI as part of the course, contributing to a confusing experience for the student. An explanation to the student regarding why they are receiving separate Lab instructions can highlight the nature of an always-changing cloud-based interface and platform. Microsoft Learning support for accessing files on GitHub and support for navigation of the GitHub site is limited to MCTs teaching this course only.

1.7 title: Online Hosted Instructions permalink: index.html layout: home

2 Content Directory

Hyperlinks to each of the walkthroughs. Instructors may choose to use the walkthrough as a demonstration or a student lab.

2.1 Walkthroughs

{% assign wts = site.pages | where_exp:"page", "page.url contains '/Instructions/Walkthroughs'" %} | Module | Walkthrough | | --- | --- | {% for activity in wts %}| {{ activity.wts.module }} | [{{ activity.wts.title }}{% if activity.wts.type %} - {{ activity.wts.type }}{% endif %}](/home/ll/Azure_clone/Azure_new/AZ-900T0x-MicrosoftAzureFundamentals/{{ site.github.url }}{{ activity.url }}) | {% endfor %}

2.2 wts: title: '00 - Readme - Error Log' module: 'Module 00 - Course Introduction'

2.3 wts: title: '01 - Create a virtual machine in the portal (10 min)' module: 'Module 02 - Core Azure Services (Workloads)'

3 01 - Create a virtual machine in the portal

In this walkthrough, we will create a virtual machine in the Azure portal, connect to the virtual machine, install the web server role and test.

Note: Take time during this walk-through to click and read the Informational icons.

4 Task 1: Create the virtual machine (10 min)

In this task, we will create a Windows Server 2019 Datacenter - Gen1 virtual machine.

1. Sign in to the Azure portal (https://portal.azure.com).
2. From the **All services** blade, search for and select **Virtual machines**, and then click **+ Add** and choose **+Virtual machine**.
3. On the **Basics** tab, fill in the following information (leave the defaults for everything else):

Settings	Values
Subscription	**Choose your subscription**
Resource group	**myRGVM** (create new)
Virtual machine name	**myVm**
Location	**(US) East US**
Image	**Windows Server 2019 Datacenter - Gen1**
Size	Standard D2s v3
Administrator account username	**azureuser**
Administrator account password	**Pa$$w0rd1234**
Inbound port rules - Allow select ports	**RDP (3389)** and **HTTP (80)**

4. Switch to the Networking tab, and look for the **Select inbound ports**:

Settings	Values
Select inbound ports	**HTTP (80), RDP (3389)**

   Note - Verify that both port 80 and 3389 are selected

5. Switch to the Management tab, and in its **Monitoring** section, select the following setting:

Settings	Values
Boot diagnostics	**Disable**

6. Leave the remaining defaults and then click the **Review + create** button at the bottom of the page.
7. Once Validation is passed click the **Create** button. It can take anywhere from five to seven minutes to deploy the virtual machine.
8. You will receive updates on the deployment page and via the **Notifications** area (the bell icon in the top menu).

- **Verify Port 80 and 3389 were opened**

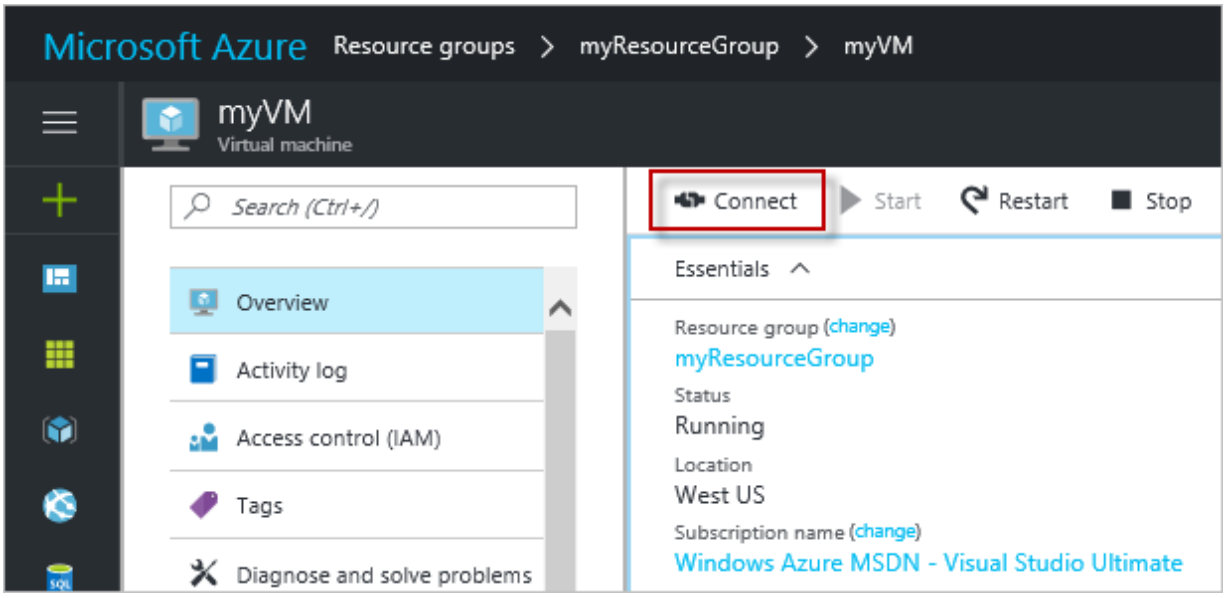
5 Task 2: Connect to the virtual machine

In this task, we will connect to our new virtual machine using RDP.

1. Search for **myVM** and select your new virtual machine.

   Note: You could also use the **Go to resource** link on the deployment page or the link to the resource in the **Notification** area.

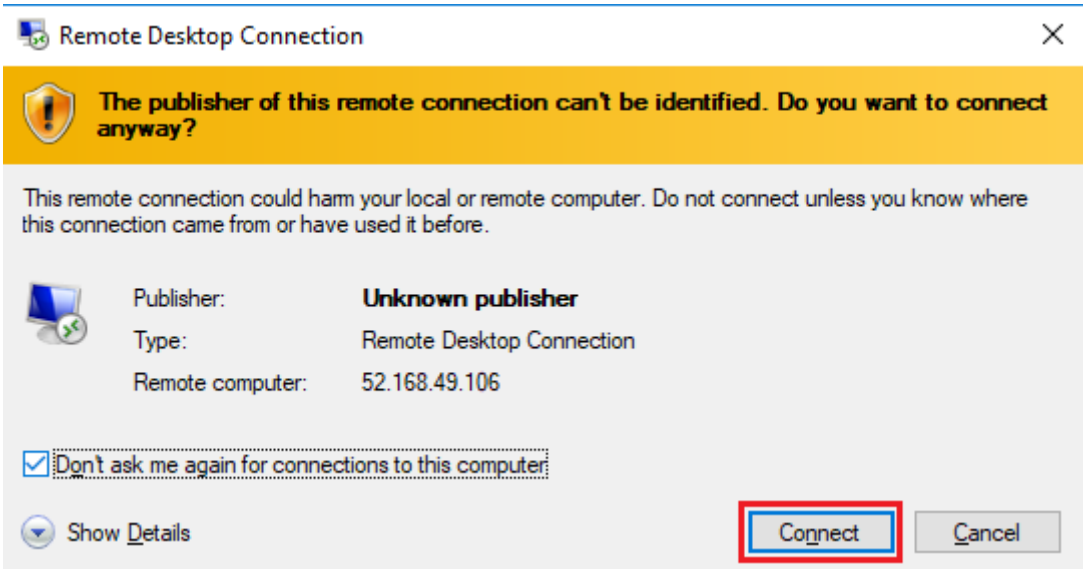
2. On the virtual machine **Overview** blade, click the **Connect** button and choose **RDP**.



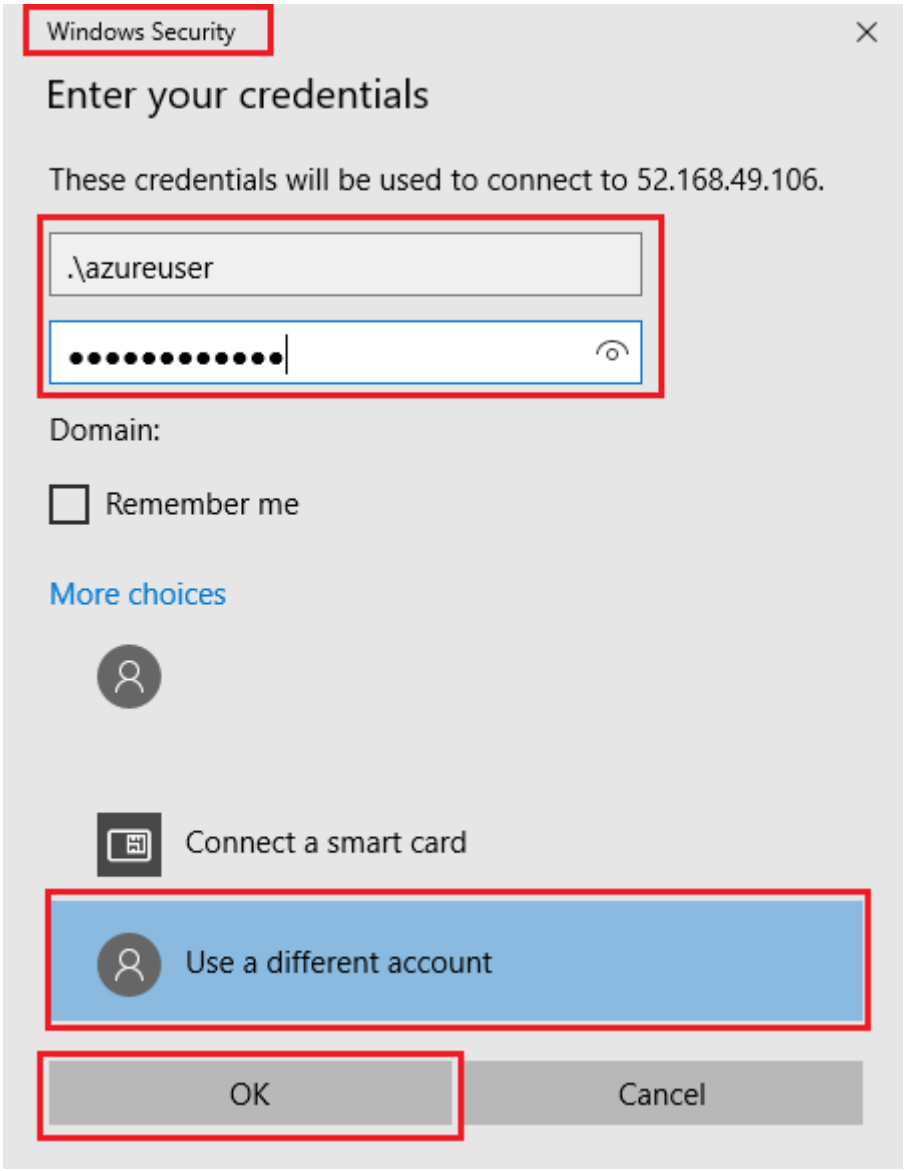
   Note: The following directions tell you how to connect to your VM from a Windows computer. On a Mac, you need an RDP client such as this Remote Desktop Client from the Mac App Store and on a Linux computer you can use an open source RDP client.

3. In the **Connect to virtual machine** page, keep the default options to connect with the public IP address over port 3389 and click **Download RDP File**.

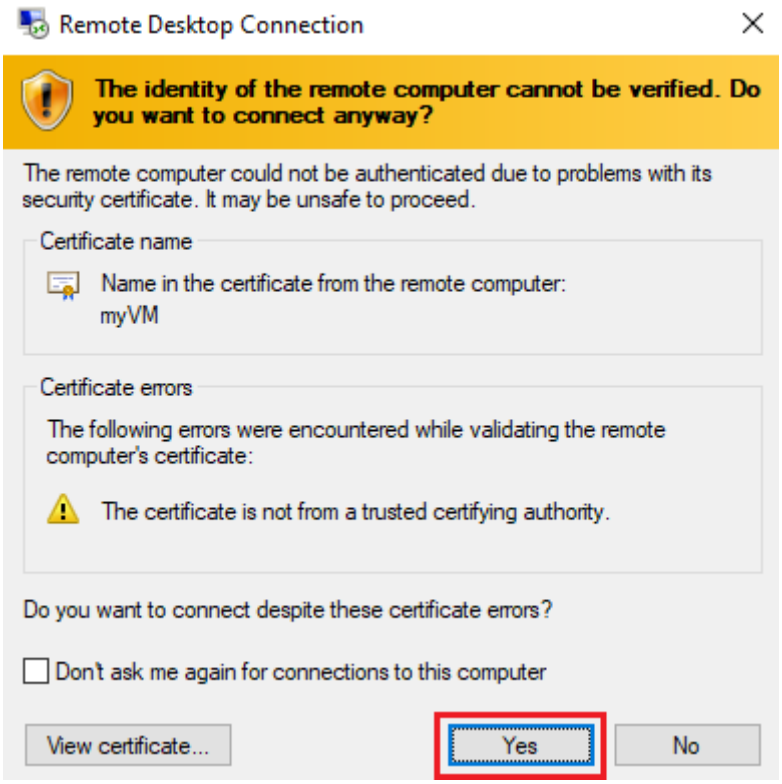
4. **Open** the downloaded RDP file and click **Connect** when prompted.



5. In the **Windows Security** window, select **More choices** and then **Use a different account**. Provide the username (.\azureuser) and the password (Pa$$w0rd1234). Click **OK** to connect.



6. You may receive a certificate warning during the sign-in process. Click **Yes** or to create the connection and connect to your deployed VM. You should connect successfully.

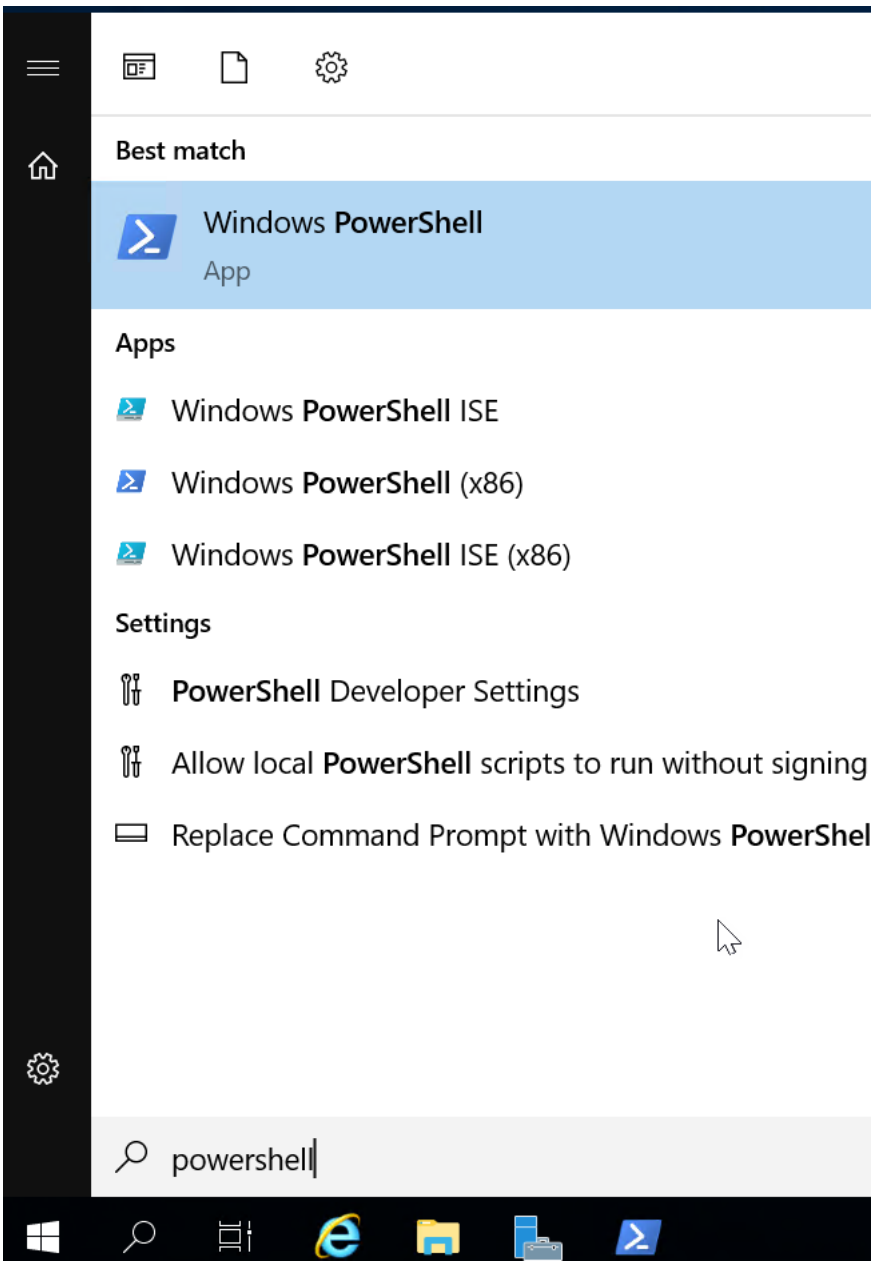


Congratulations! You have deployed and connected to a Windows Server virtual machine in Azure

6 Task 3: Install the web server role and test

In this task, install the Web Server role on the server and ensure the default IIS welcome page can be displayed.

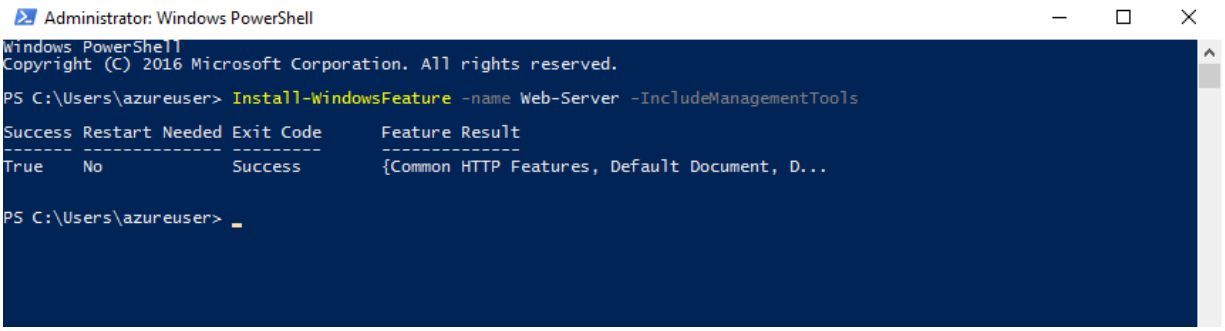
1. Open up a PowerShell command prompt on the virtual machine, by clicking the **Start** button, typing **PowerShell**, right clicking **Windows PowerShell**, and selecting **Run as administrator** in the right-click menu.



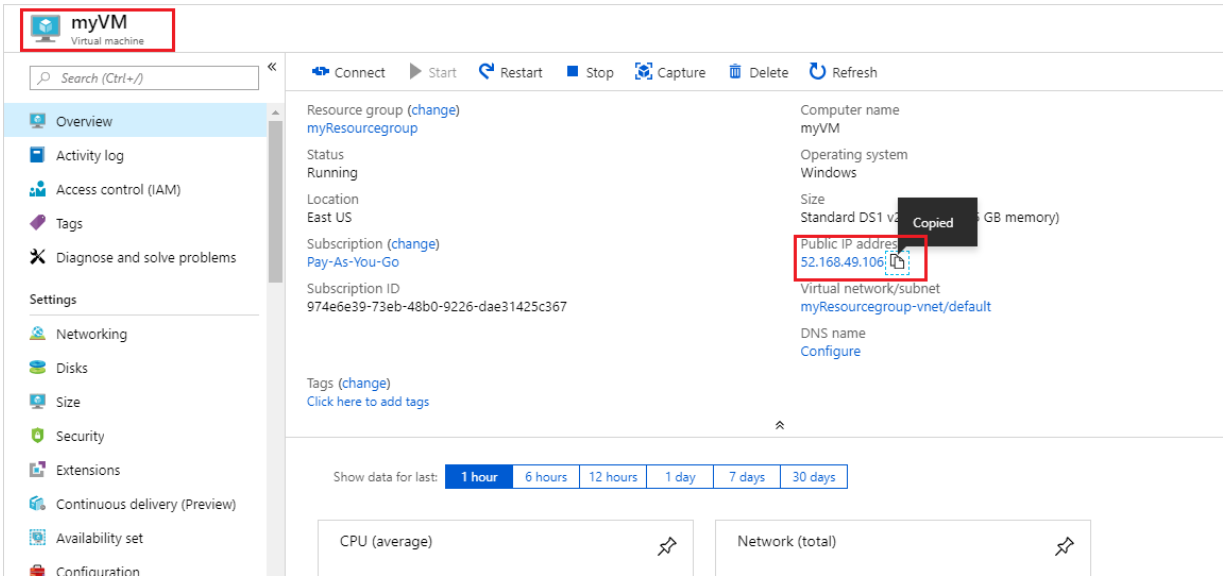
2. Install the **Web-Server** feature in the virtual machine by running the following command in the PowerShell command prompt. You can copy and paste this command.

```
Install-WindowsFeature -name Web-Server -IncludeManagementTools
```

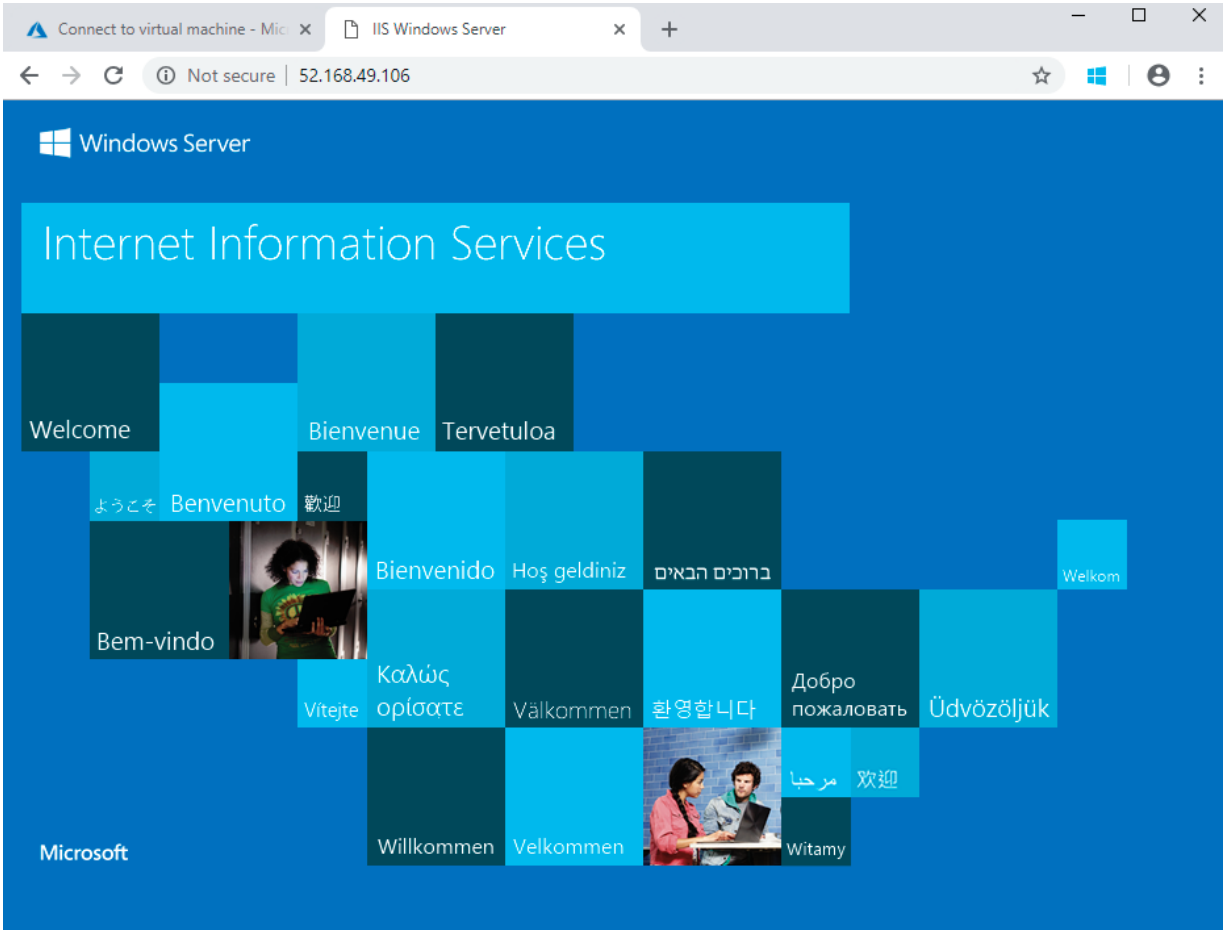
3. When completed there will be a prompt stating **Success** with a value **True**. You do not need to restart the virtual machine to complete the installation. Close the RDP connection to the VM.



4. Back in the portal, navigate back to the **Overview** blade of myVM and, use the **Click to clipboard** button to copy the public IP address of myVM, open a new browser tab, paste the public IP address into the URL text box, and press the **Enter** key to browse to it.



5. The default IIS Web Server welcome page will open.



Congratulations! You have created a web server that is accessible via its public IP address. If you had a web application to host, you could deploy application files to the virtual machine and host them for public access on the deployed virtual machine.

6.1 Note: To avoid additional costs, you can remove this resource group. Search for resource groups, click your resource group, and then click Delete resource group. Verify the name of the resource group and then click Delete. Monitor the Notifications to see verify that the deletion completed successfully.

6.2 wts: title: '02 - Create a Web App (10 min)' module: 'Module 02 - Core Azure Services (Workloads)'

7 02 - Create a Web App

In this walkthrough, we will create a new web app that runs a Docker container. The container displays a Welcome message.

8 Task 1: Create a Web App (10 min)

Azure App Service is actually a collection of four services, all of which are built to help you host and run web applications. The four services (Web Apps, Mobile Apps, API Apps, and Logic Apps) look different, but in the end they all operate in very similar ways. Web Apps are the most commonly used of the four services, and this is the service that we will be using in this lab.

In this task, you will create an Azure App Service Web App.

1. Sign-in to the Azure portal.
2. From the **All services** blade, search for and select **App Services**, and click **+ Add, + Create, or + New**
3. On the **Basics** tab of the **Web App** blade, specify the following settings (replace **xxxx** in the name of the web app with letters and digits such that the name is globally unique). Leave the defaults for everything else, including the App Service Plan.

Setting	Value
Subscription	**Choose your subscription**
Resource Group	**myRGWebApp1** (create new)
Name	**myDockerWebAppxxxx**
Publish	**Docker Container**
Operating System	**Linux**
Region	**East US** (ignore any service plan availability warnings)

   Note - Remember to change the **xxxx** so that it makes a unique **Name**

4. Click **Next > Docker** and configure the container information. The startup command is optional and not needed in this exercise.

   Note: This is same container that was used in the Container Instances walkthrough to display a hello world message.

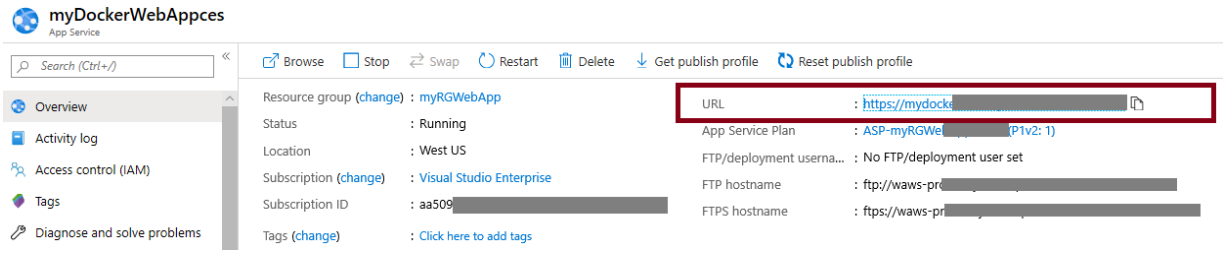
Setting	Value
Options	**Single container**
Image Source	**Docker Hub**
Access Type	**Public**
Image and tag	**microsoft/aci-helloworld**

5. Click **Review + create**, and then click **Create**.

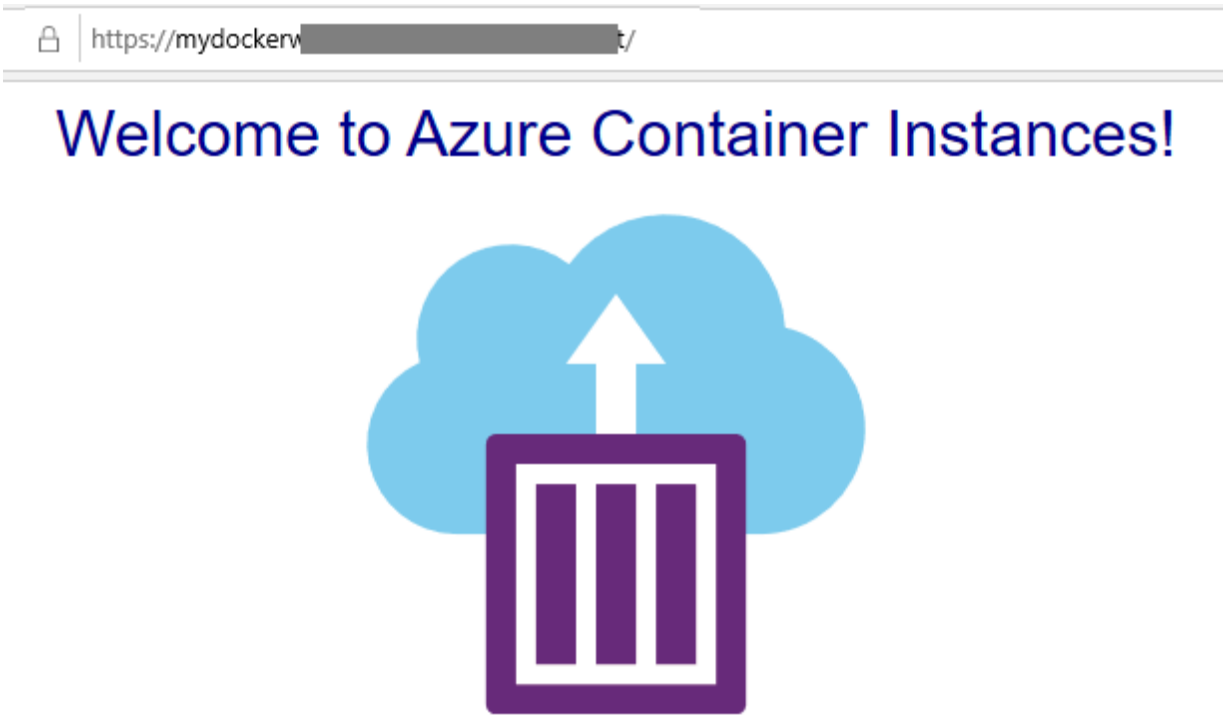
9 Task 2: Test the Web App

In this task, we will test the web app.

1. Wait for the Web App to deploy.
2. From **Notifications** click **Go to resource**.
3. On the **Overview** blade, locate the **URL** entry.



4. Click on the **URL** to open the new browser tab and display the Welcome to Azure Container Instances page.



5. Switch back to the **Overview** blade of your web app and note that it includes several charts. If you repeat step 4 a few times, you should be able to see correspoding telemetry being displayed in the charts. This includes number of requests and average response time.

Note: To avoid additional costs, you can remove this resource group. Search for resource groups, click your resource group, and then click **Delete resource group**. Verify the name of the resource group and then click **Delete**. Monitor the **Notifications** to see how the delete is proceeding.

9.1 wts: title: '03 - Deploy Azure Container Instances (10 min)' module: 'Module 02 - Core Azure Services (Workloads)'

10 03 - Deploy Azure Container Instances

In this walkthrough we create, configure, and deploy a Docker container by using Azure Container Instances (ACI) in the Azure Portal. The container is a Welcome to ACI web application that displays a static HTML page.

11 Task 1: Create a container instance (10 min)

In this task, we will create a new container instance for the web application.

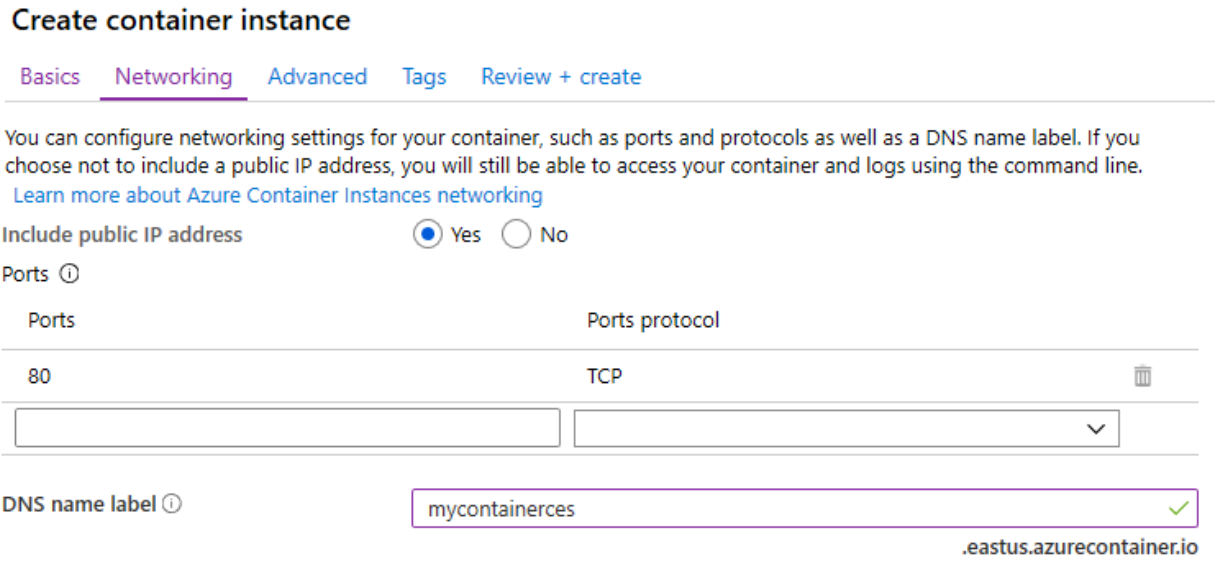
1. Sign in to the Azure portal.
2. From the **All services** blade, search for and select **Container instances** and then click **+ Add, + Create, or + New**.
3. Provide the following Basic details for the new container instance (leave the defaults for everything else)):

Setting	Value
Subscription	**Choose your subscription**
Resource group	**myRGContainer** (create new)
Container name	**mycontainer**
Region	**(US) East US**
Image source	**Docker Hub or other registry**
Image type	**Public**
Image	**microsoft/aci-helloworld**
OS type	**Linux**
Size	***Leave at the default***

4. Configure the Networking tab (replace **xxxx** with letters and digits such that the name is globally unique). Leave all other settings at their default values .

Setting	Value
DNS name label	**mycontainerdnsxxxx**

Note: Your container will be publicly reachable at dns-name-label.region.azurecontainer.io. If you receive a **DNS name label not available** error message following the deployment, specify a different DNS name label (don't use xxxx) and re-deploy.

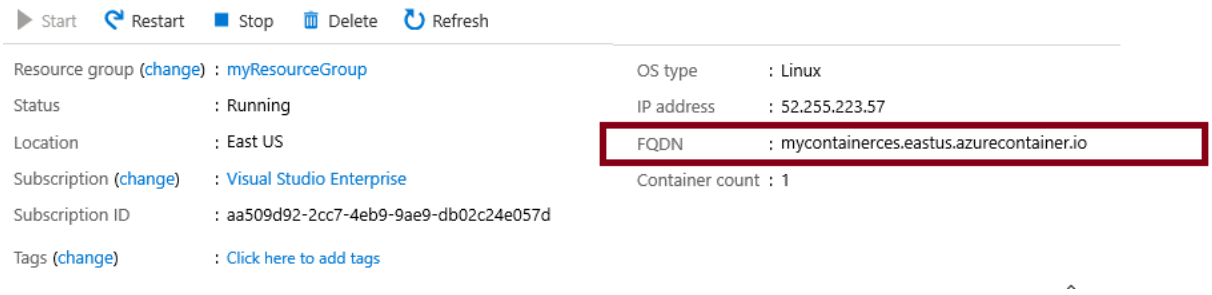


5. Click **Review and Create** to start the automatic validation process.
6. Click **Create** to create the container instance.
7. Monitor the deployment page and the **Notifications** page.
8. While you wait you may be interested in viewing the sample code behind this simple application. Browse the \app folder.

12 Task 2: Verify deployment of the container instance

In this task, we verify that the container instance is running by ensuring that the welcome page displays.

1. After the deployment is complete, click the **Go to resource** link the deployment blade or the link to the resource in the Notification area.
2. On the **Overview** blade of **mycontainer**, ensure your container **Status** is **Running**.
3. Locate the Fully Qualified Domain Name (FQDN).



4. Copy the container's FQDN into the URL text box web browser and press **Enter**. The Welcome page should display.

Note: You could also use the container IP address in your browser.

Congratulations! You have used Azure Portal to successfully deploy an application to a container in Azure Container Instance.

12.1 Note: To avoid additional costs, you can remove this resource group. Search for resource groups, click your resource group, and then click Delete resource group. Verify the name of the resource group and then click Delete. Monitor the Notifications to see how the delete is proceeding.

12.2 wts: title: '04 - Create a virtual network (20 min)' module: 'Module 02 - Core Azure Services (Workloads)'

13 04 - Create a virtual network

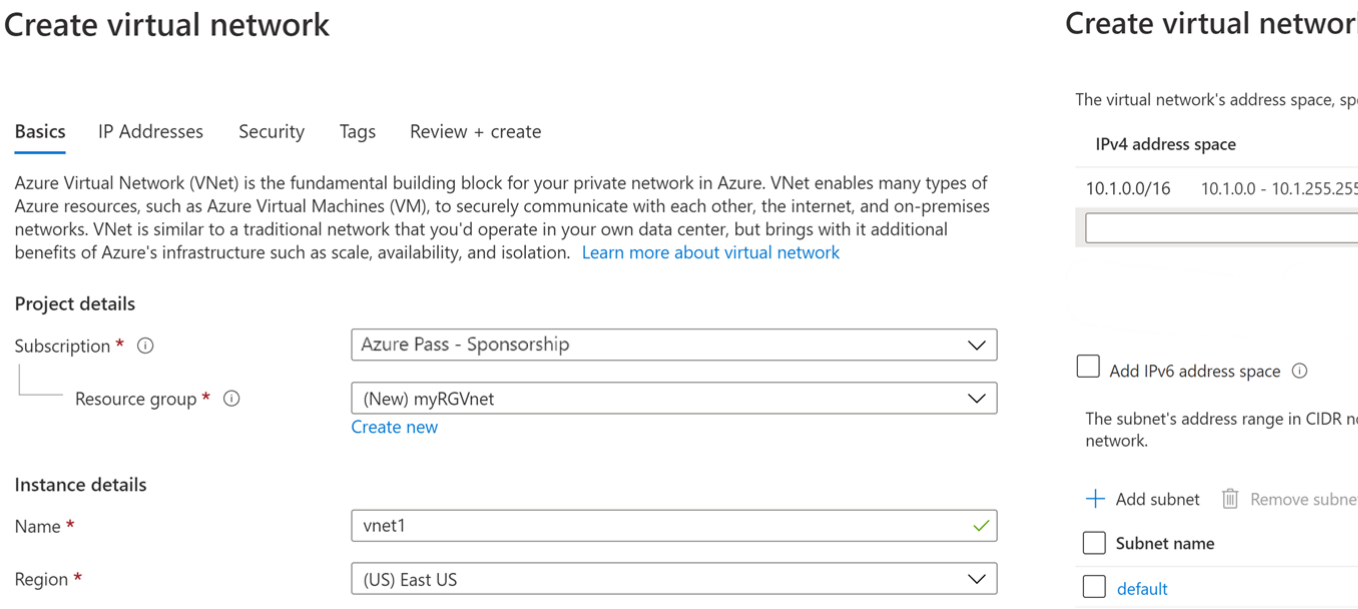
In this walkthrough, we will create a virtual network, deploy two virtual machines onto that virtual network and then allow one virtual machine to ping the other within that virtual network.

14 Task 1: Create a virtual network (20 min)

In this task, we will create a virtual network.

1. Sign in to the Azure portal at https://portal.azure.com
2. From the **All services** blade, search for and select **Virtual networks**, and then click **+ Add, + Create, or + New**.
3. On the **Create virtual network** blade, fill in the following (leave the defaults for everything else):

Setting	Value
Subscription	**Select your subscription**
Resource group	**myRGVNet** (create new)
Name	**vnet1**
Location	**(US) East US**
Address space	**10.1.0.0/16**
Subnet - Name	**default**
Subnet Address range	**10.1.0.0/24**



4. Click the **Review + create** button. Ensure the validation passes.
5. Click the **Create** button to deploy the virtual network.

   Note: In your organization, how will you know which virtual networks and IP addressing you will need?

15 Task 2: Create two virtual machines

In this task, we will create two virtual machines in the virtual network.

1. From the **All services** blade, search for **Virtual machines** and then click **+ Add** and choose **+ Virtual machine**.
2. On the **Basics** tab, fill in the following information (leave the defaults for everything else):

Setting	Value
Subscription	**Choose your subscription**
Resource group	**myRGVNet**
Virtual machine name	**vm1**
Region	**(US) East US**
Image	**Windows Server 2019 Datacenter**

Setting	Value
Username	**azureuser**
Password	**Pa$$w0rd1234**
Public inbound ports	Select **Allow selected ports**
Selected inbound ports	**RDP (3389)**

3. Select the **Networking** tab. Make sure the virtual machine is placed in the vnet1 virtual network. Review the default settings, but do not make any other changes.

Setting	Value
Virtual network	**vnet1**

4. Click **Review + create**. After the Validation passes, click **Create**. Deployment times can vary but it can generally take between three to six minutes to deploy.
5. Monitor your deployment, but continue on to the next step.
6. Create a second virtual machine by repeating steps **2 to 4** above. Make sure you use a different virtual machine name, that the virtual machine is within the same virtual network, and is using a new public IP address:

Setting	Value
Resource group	**myRGVNet**
Virtual machine name	**vm2**
Virtual network	**vnet1**
Public IP	(new) **vm2-ip**

7. Wait for both virtual machines to deploy.

16 Task 3: Test the connection

In this task, we will allow log into one VM and ping the other.

1. From the **All resources** blade, search for **vm1**, open its **Overview** blade, and make sure its **Status** is **Running**. You may need to **Refresh** the page.
2. On the **Overview** blade, click the **Connect** button.

   Note: The following directions tell you how to connect to your VM from a Windows computer.
3. On the **Connect to virtual machine** blade, keep the default options to connect by IP address over port 3389 and click **Download RDP File**.
4. Open the downloaded RDP file and click **Connect** when prompted.
5. In the **Windows Security** window, type the username **azureuser** and password **Pa$$w0rd1234** and then click **OK**.
6. You may receive a certificate warning during the sign-in process. Click **Yes** or to create the connection and connect to your deployed VM. You should connect successfully.
7. Open up a PowerShell command prompt on the virtual machine, by clicking the **Start** button, typing **PowerShell**, right clicking **Windows PowerShell** in the right-click menu, and clicking **Run as administrator**
8. In Powershell, type the following command to try to communicate with vm2, you will notice you are successful.

   ```
   ping vm2
   ```

Congratulations! You have configured and deployed two virtual machines in a virtual network. And you have tested that you can communicate between the two VMs.

16.1 Note: To avoid additional costs, you can remove this resource group. Search for resource groups, click your resource group, and then click Delete resource group. Verify the name of the resource group and then click Delete. Monitor the Notifications to see how the delete is proceeding.

16.2 wts: title: '05 - Create blob storage (5 min)' module: 'Module 02 - Core Azure Services (Workloads)'

17 05 - Create blob storage

In this walkthrough, we will create a storage account, then work with blob storage files.

18 Task 1: Create a storage account (5 min)

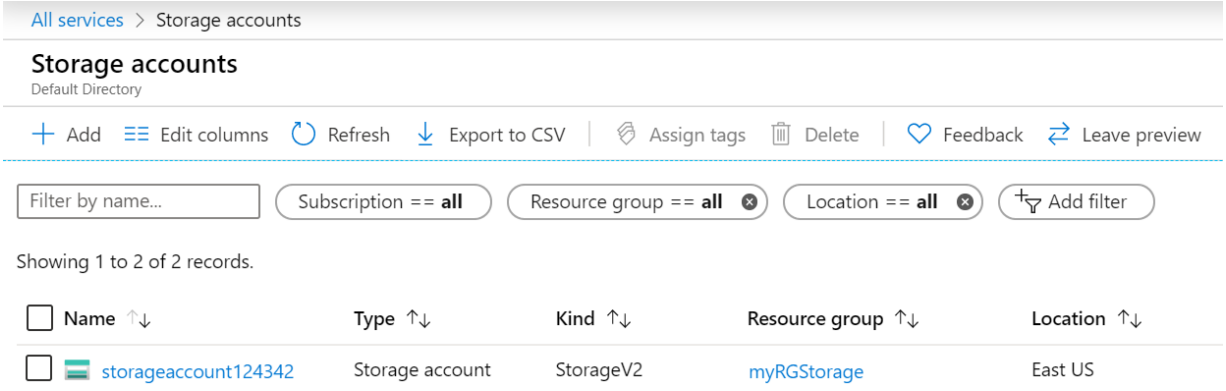
In this task, we will create a new storage account.

1. Sign in to the Azure portal at https://portal.azure.com
2. From the **All services** blade, search for and select **Storage accounts**, and then click **+ Add, + Create, or + New**.
3. On the **Basics** tab of the **Create storage account** blade, fill in the following information (replace **xxxx** in the name of the storage account with letters and digits such that the name is globally unique). Leave the defaults for everything else.

Setting	Value
Subscription	**Choose your subscription**
Resource group	**myRGStorage** (create new)
Storage account name	**storageaccountxxxx**
Location	**(US) East US**
Performance	**Standard**
Account kind	**StorageV2 (general purpose v2)**
Replication	**Locally redundant storage (LRS)**

Note - Remember to change the **xxxx** so that it makes a unique **Storage account name**

4. Click **Review + Create** to review your storage account settings and allow Azure to validate the configuration.
5. Once validated, click **Create**. Wait for the notification that the account was successfully created.
6. From the Home page, search for and select **Storage accounts** and ensure your new storage account is listed.

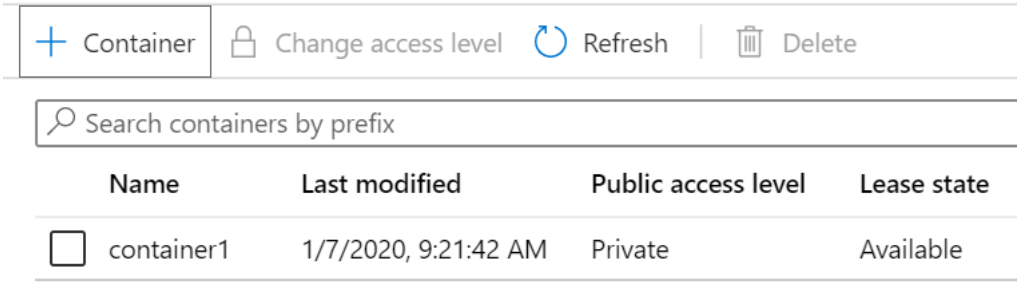


19 Task 2: Work with blob storage

In this task, we will create a Blob container and upload a blob file.

1. Click the name of the new storage account, scroll to the **Blob service** section, and then click **Containers**.
2. Click + **Container** and complete the information. Use the Information icons to learn more. When done click **Create**.

Setting	Value
Name	**container1**
Public access level	**Private (no anonymous access)**



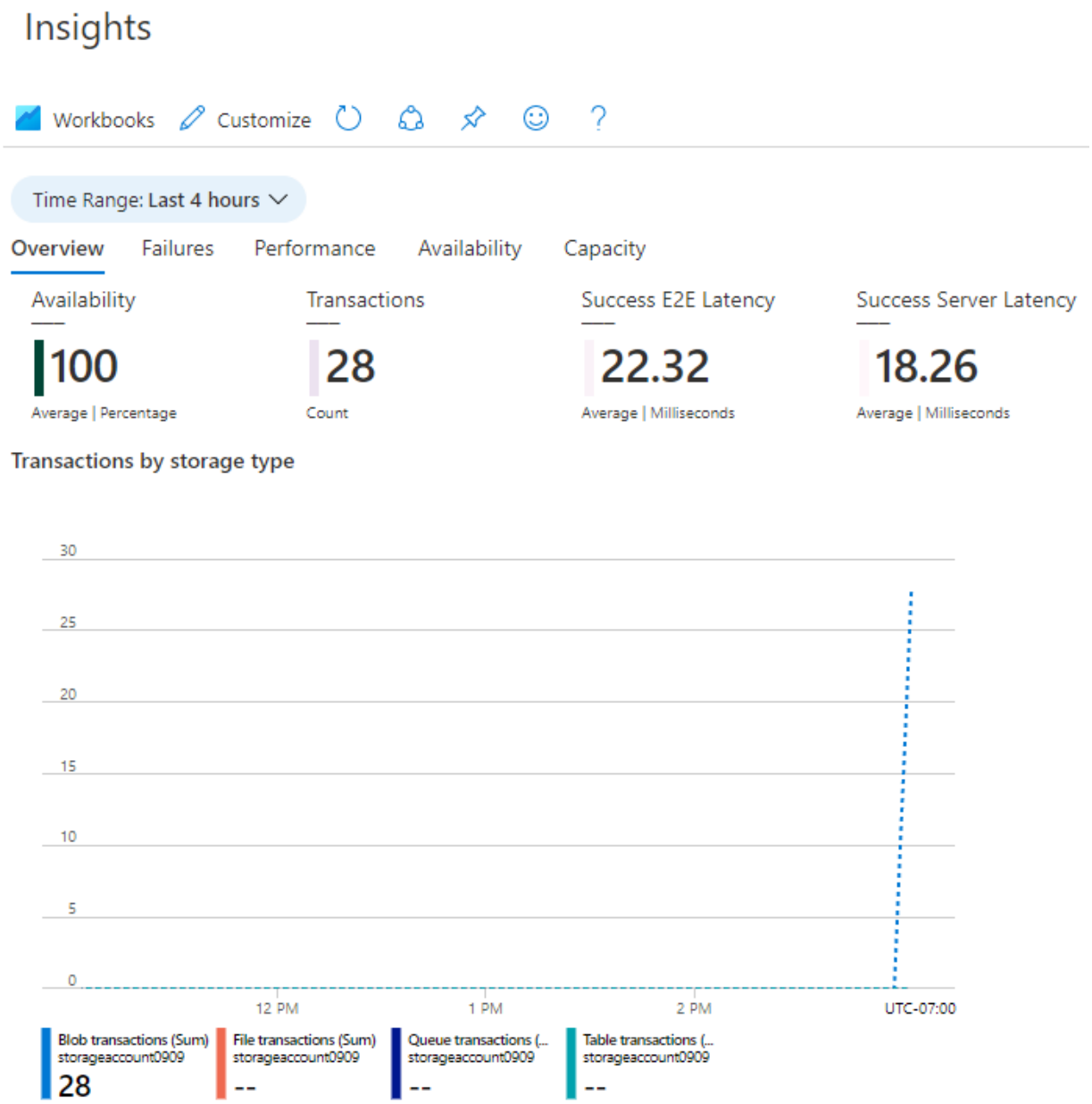
3. Click the **container1** container, and then click **Upload**.
4. Browse to a file on your local computer.

   Note: You can create an empty `.txt` file or use any existing file. Consider chooosing a file of a small size to minimize the upload time.
5. Click the **Advanced** arrow, leave the default values but review the available options, and then click **Upload**.

   Note: You can upload as many blobs as you like in this way. New blobs will be listed within the container.
6. Once the file is uploaded, right-click on the file and notice the options including View/edit, Download, Properties, and Delete.
7. As you have time, from the storage account blade, review the options for Files, Tables, and Queues.

20 Task 3: Monitor the storage account

1. If needed, return to the storage account blade and click **Diagnose and solve problems**.
2. Explore some of the most common storage problems. Notice there are multiple troubleshooter.
3. On the storage account blade, scroll down to the **Monitoring** section and click **Insights**. Notice there is information on Failures, Performance, Availability, and Capacity. Your information will be different.



Congratulations! You have created a storage account, then worked with storage blobs.

20.1 Note: To avoid additional costs, you can remove this resource group. Search for resource groups, click your resource group, and then click Delete resource group. Verify the name of the resource group and then click Delete. Monitor the Notifications to see how the delete is proceeding.

20.2 wts: title: '06 - Create a SQL database (5 min)' module: 'Module 02 - Core Azure Services (Workloads)'

21 06 - Create a SQL database

In this walkthrough, we will create a SQL database in Azure and then query the data in that database.

22 Task 1: Create the database (5 min)

In this task, we will create a SQL database based on the AdventureWorksLT sample database.

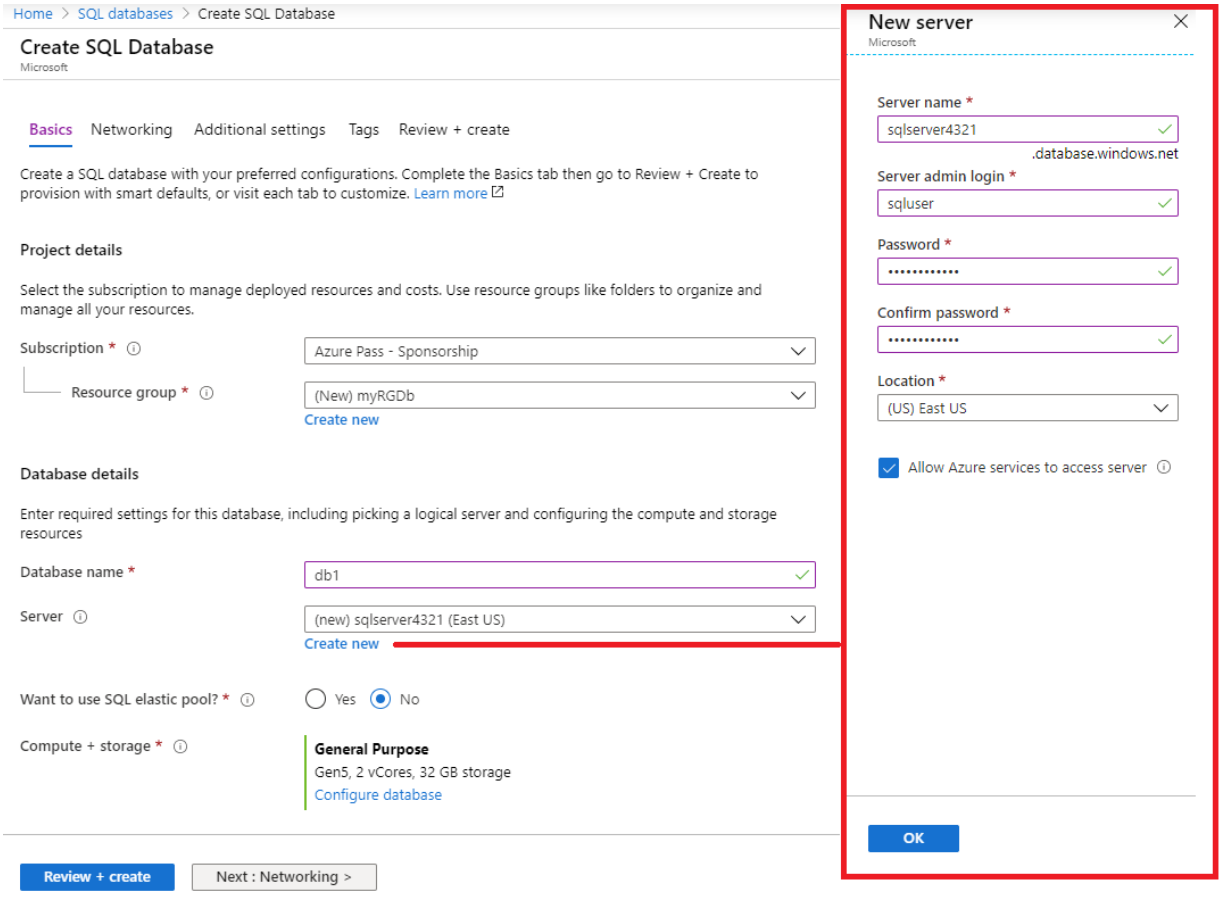
1. Sign in to the Azure portal at **https://portal.azure.com**.

2. From the **All services** blade, search for and select **SQL databases**, and then click **+ Add, + Create, or + New**.
3. On the **Basics** tab, fill in this information.

Setting	Value
Subscription	**Choose your subscription**
Resource group	**myRGDb** (create new)
Database name	**db1**

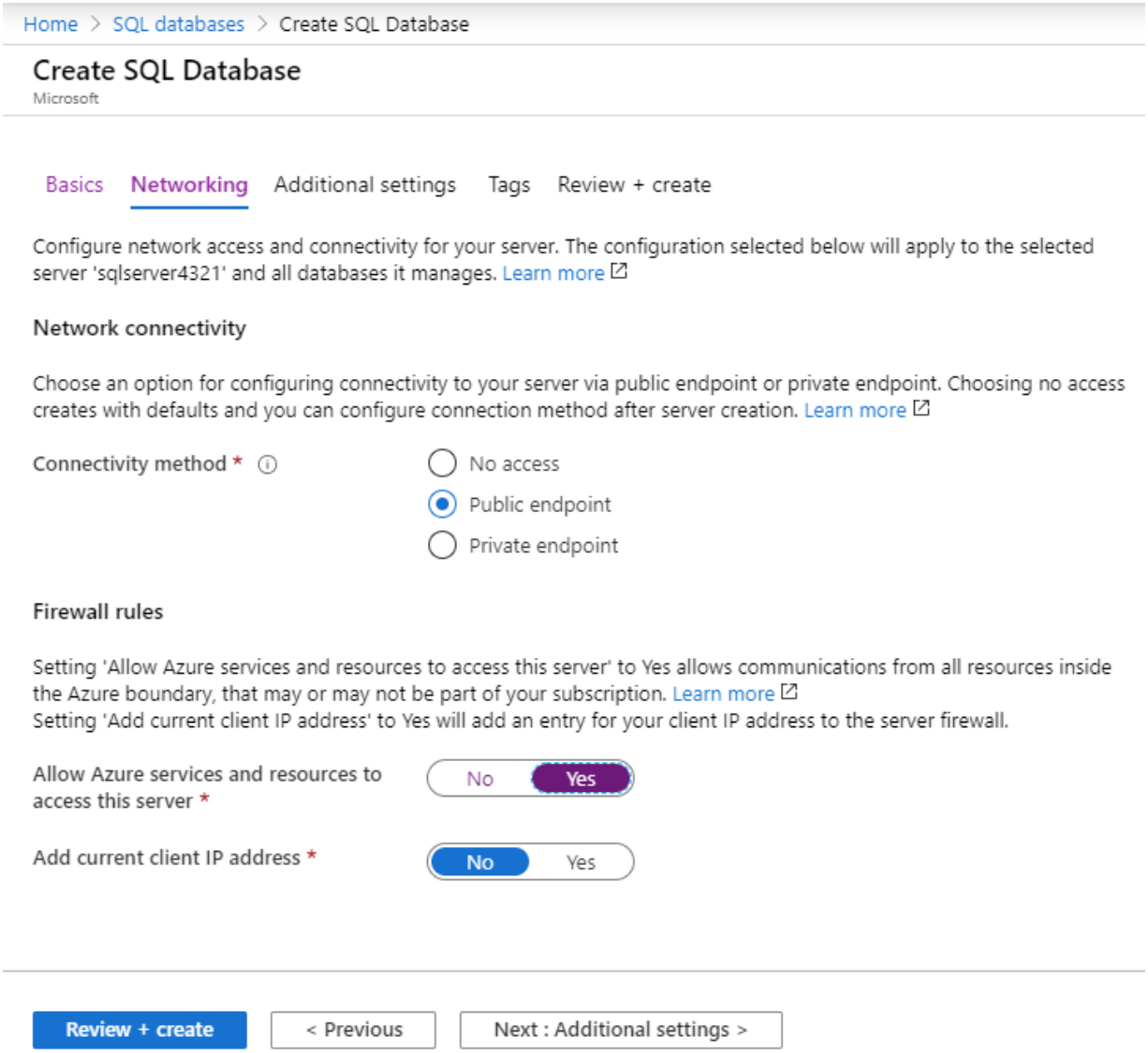
4. Next to the **Server** drop down list, click **Create new** and enter this information (replace **xxxx** in the name of the server with letters and digits such that the name is globally unique). Click **OK** when finished.

Setting	Value
Server name	**sqlserverxxxx** (must be unique)
Server admin login	**sqluser**
Password	**Pa$$w0rd1234**
Location	**(US) East US**
Allow Azure services to access server	***Select the checkbox***



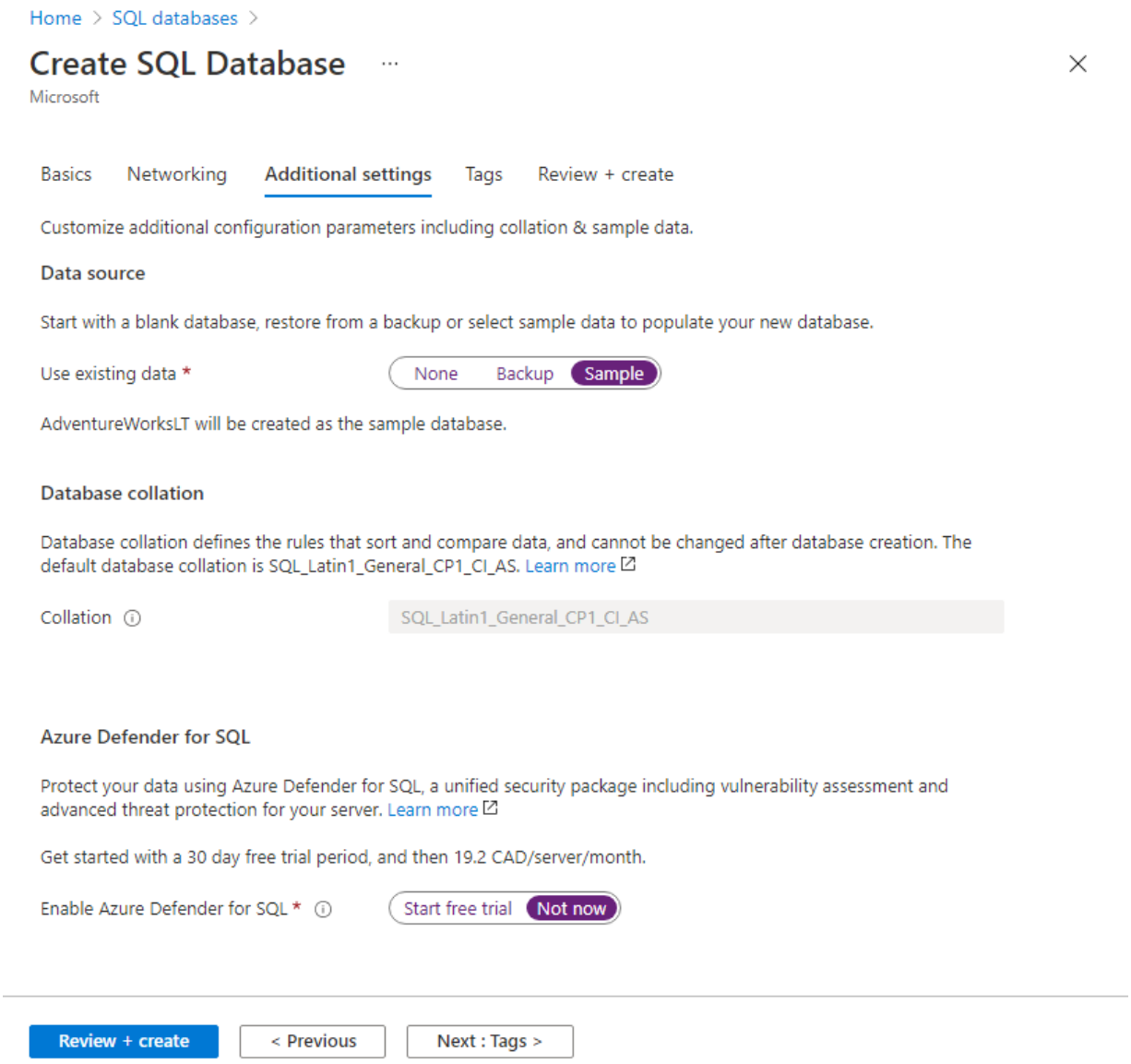
5. Move to the **Networking** tab and configure the following settings (leave others with their defaults)

Setting	Value
Connectivity method	**Public endpoint**
Allow Azure services and resources to access this server	**Yes**
Add current client IP address	**No**



6. Move to the **Additional settings** tab. We will be using the AdventureWorksLT sample database.

Setting	Value
Use existing data	**Sample**
Collation	***use default***
Enable Azure Defender for SQL	**Not now**

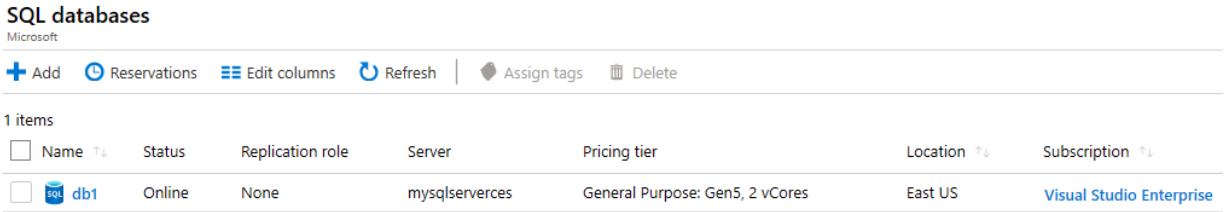


7. Click **Review + create** and then click **Create** to deploy and provision the resource group, server, and database. It can take approx. 2 to 5 minutes to deploy.
8. Go to the resource tab to locate the SQL database you created. You may need to refresh.

23 Task 2: Test the database.

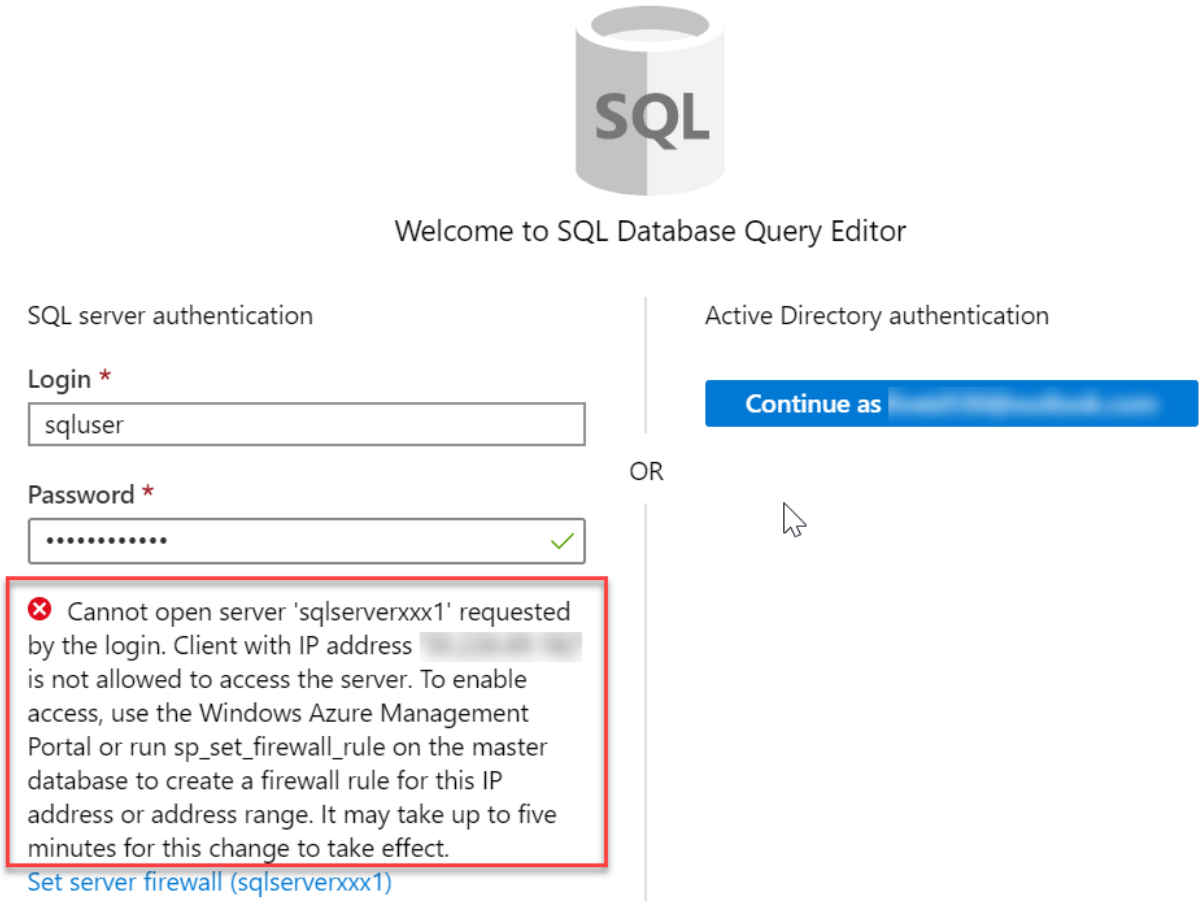
In this task, we will configure the SQL server and run a SQL query.

1. From the **All services** blade, search and select **SQL databases** and ensure your new database was created. You may need to **Refresh** the page.

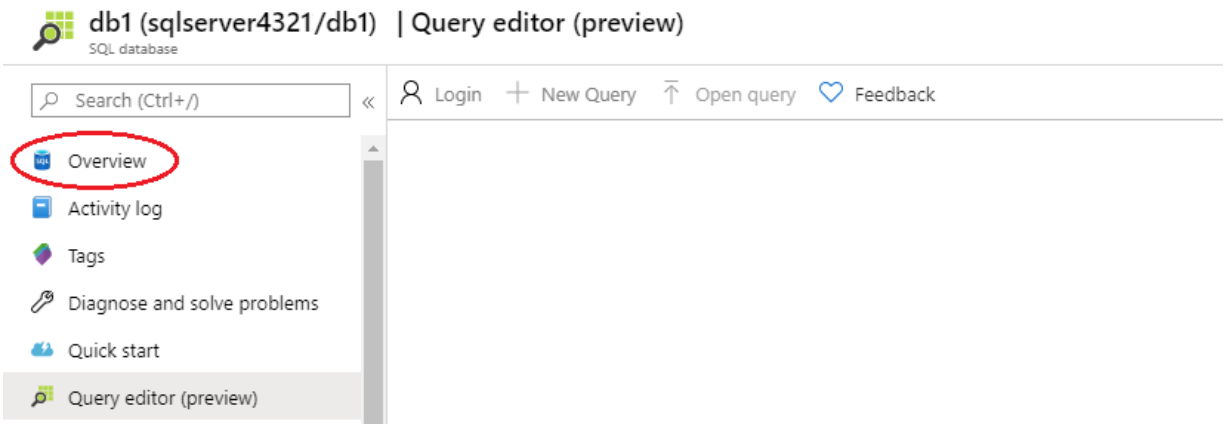


2. Click the **db1** entry representing the SQL database you created, and then click **Query editor (preview)**.
3. Login as **sqluser** with the password **Pa$$w0rd1234**.

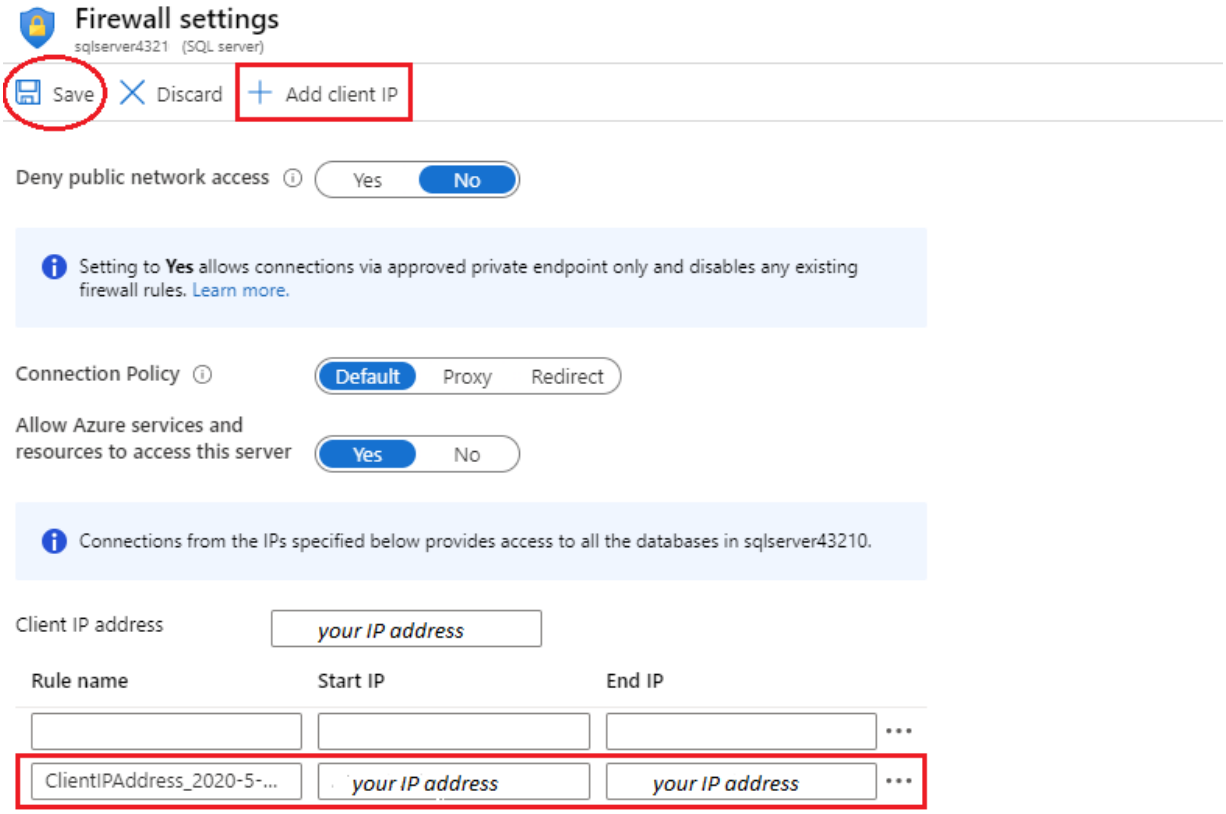
4. You will not be able to login. Read the error closely and make note of the IP address that needs to be allowed through the firewall.



5. From the **db1** blade, click **Overview**.



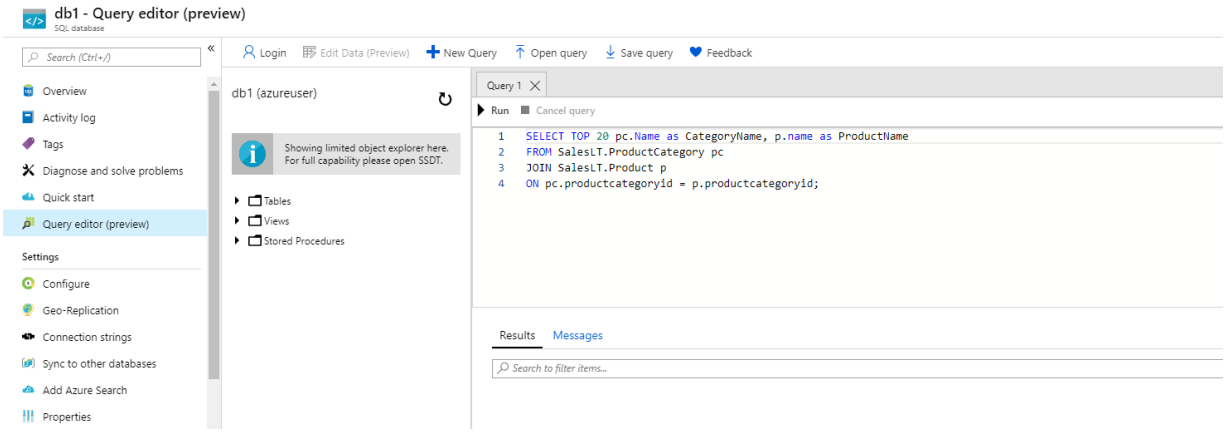
6. From the SQL server **Overview** blade, click **Set server firewall**.
7. Click **Add client IP** (top menu bar) to add the IP address referenced in the error. Be sure to **Save** your changes.



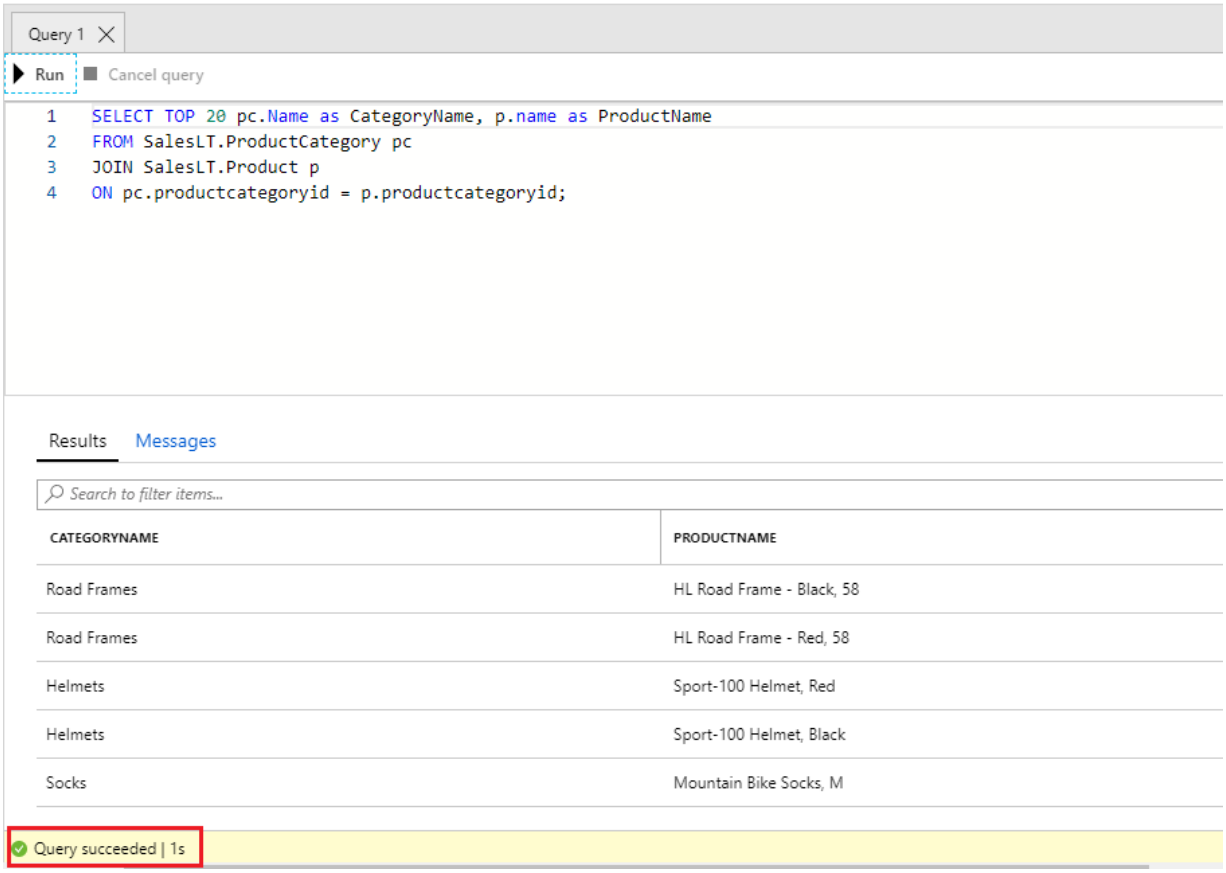
8. Return to your SQL database and the **Query Editor (Preview)** login page. Try to login again as **sqluser** with the password **Pa$$w0rd1234**. This time you should succeed. Note that it may take a couple of minutes for the new firewall rule to be deployed.

9. Once you log in successfully the query pane appears, enter the following query into the editor pane.

```
SELECT TOP 20 pc.Name as CategoryName, p.name as ProductName
FROM SalesLT.ProductCategory pc
JOIN SalesLT.Product p
ON pc.productcategoryid = p.productcategoryid;
```



10. Click **Run**, and then review the query results in the **Results** pane. The query should run successfully.



Congratulations! You have created a SQL database in Azure and successfully queried the data in that database.

23.1 Note: To avoid additional costs, you can remove this resource group. Search for resource groups, click your resource group, and then click Delete resource group. Verify the name of the resource group and then click Delete. Monitor the Notifications to see how the delete is proceeding.

23.2 wts: title: '07 - Implement an Azure IoT Hub (10 min)' module: 'Module 03: Describe core solutions and management tools'

24 07 - Implement an Azure IoT Hub

In this walkthrough, we will configure a new Azure IoT Hub in Azure Portal, and then authenticate a connection to an IoT device using the online Raspberry Pi device simulator. Sensor data and messages are passed from the Raspberry Pi simulator to your Azure IoT Hub, and you view metrics for the messaging activity in Azure Portal.

25 Task 1: Create an IoT hub (10 min)

In this task, we will create an IoT hub.

1. Sign in to the Azure portal.
2. From the **All services** blade, search for and select **IoT Hub** and then click **+ Add, + Create, or + New**.
3. On the **Basics** tab of the **IoT hub** blade, fill in the fields with the following details (replace **xxxx** in the name of the storage account with letters and digits such that the name is globally unique):

Settings	Value
Subscription	**Choose your subscription**
Resource Group	**myRGIoT** (create new)
Region	**East US**

Settings	Value
IoT Hub Name	**my-hub-groupxxxx**

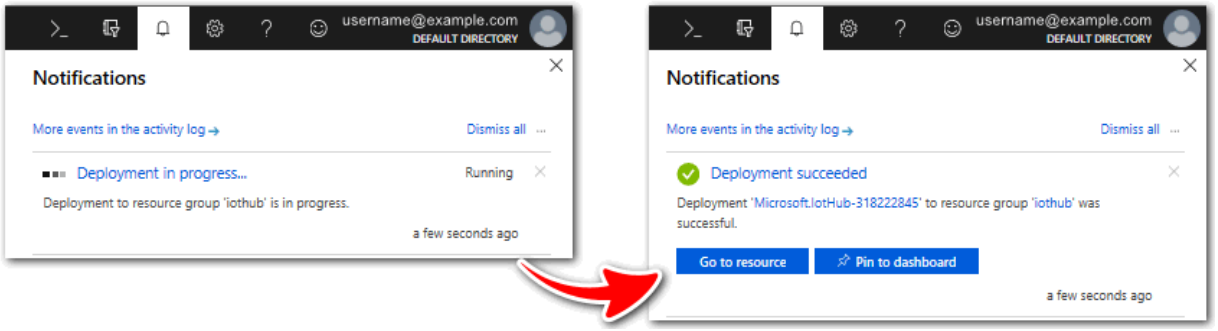
Note - Remember to change the **xxxx** so that it makes a unique **IoT Hub Name**.

4. Go to the **Management** tab, and use the dropdown list to set the **Pricing and scale tier** to **S1: Standard tier**.
5. Click the **Review + create** button.
6. Click the **Create** button to begin creating your new Azure IoT Hub instance.
7. Wait until the Azure IoT Hub instance is deployed.

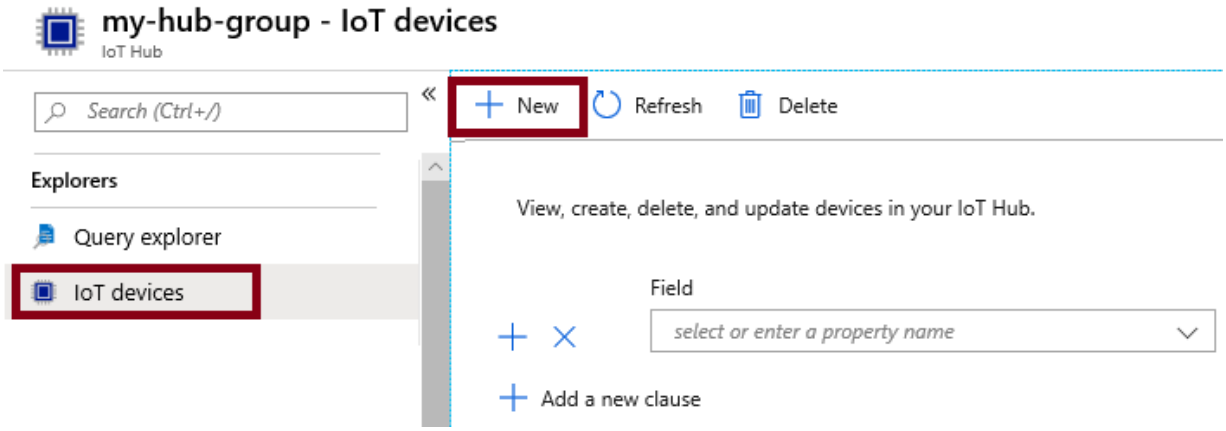
26 Task 2: Add an IoT device

In this task, we will add an IoT device to the IoT hub.

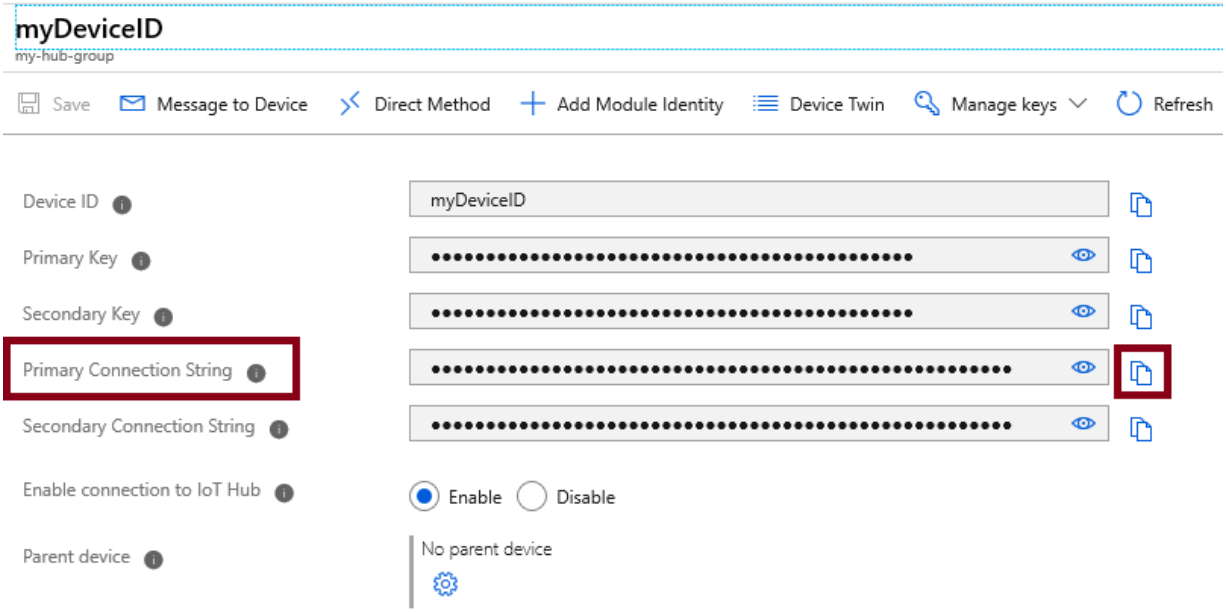
1. When the deployment has completed, click **Go to resource** from the deployment blade. Alternatively, from the **All services** blade, search for and select **IoT Hub** and locate your new IoT Hub instance



2. To add a new IoT device, scroll down to the **Explorers** section and click **IoT Devices**. Then, click **+ New**.



3. Provide a name for your new IoT device, **myRaspberryPi**, and click the **Save** button. This will create a new IoT device identity in your Azure IoT Hub.
4. If you do not see your new device, **Refresh** the IoT Devices page.
5. Select **myRaspberryPi** and copy the **Primary Connection String** value. You will use this key in the next task to authenticate a connection to the Raspberry Pi simulator.



27 Task 3: Test the device using the Raspberry Pi Simulator

In this task, we will test our device using the Raspberry Pi Simulator.

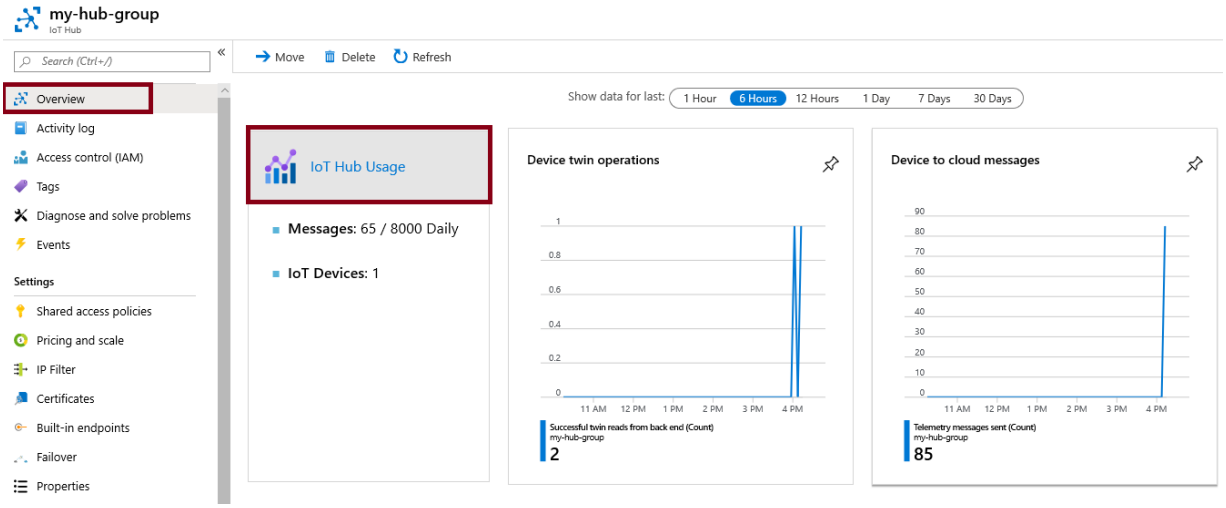
1. Open a new tab in the web browser and browse to the online Raspberry Pi simulator.
2. Read about the Raspberry Pi simulator. If there is an overview pop-up select "**X**" to close the window.
3. In the code area, right side, locate the line with 'const connectionString ='. Replace it with the connection string you copied from the Azure portal. Note that the connection sting includes the DeviceId (**myRaspberryPi**) and SharedAccessKey entries.

```
14
15  const connectionString = 'HostName=my-hub-group.azure-devices.net;DeviceId=myRaspberryPi;SharedAccessKey=Aurv5HwS9TLRbj
16  const LEDPin = 4;
17
```

4. Click **Run** (below the code area) to run the application. The console output should show the sensor data and messages that are sent from the Raspberry Pi simulator to your Azure IoT Hub. Data and messages are sent each time the Raspberry Pi simulator LED flashes.

```
Running   Reset
Type `npm start` to run your app.
We don't support stop the app, so you may need referesh the page to kill your thread.
We keep your changes to the editor even you referesh the page. You can click the 'reset' to reset the code
>
Sending message: {"messageId":1,"deviceId":"Raspberry Pi Web Client","temperature":25.584710773750324,"humidity"
>
Message sent to Azure IoT Hub
```

5. Click **Stop** to stop sending data.
6. Return to the Azure portal and your IoT Hub.
7. Switch the IoT Hub **Overview** blade and scroll down to the **IoT Hub Usage** information.



Congratulations! You have set up Azure IoT Hub to collect sensor data from an IoT device.

27.1 Note: To avoid additional costs, you can remove this resource group. Search for resource groups, click your resource group, and then click Delete resource group. Verify the name of the resource group and then click Delete. Monitor the Notifications to see how the delete is proceeding.

27.2 wts: title: '08 - Implement Azure Functions (5 min)' module: 'Module 03: Describe core solutions and management tools'

28 08 - Implement Azure Functions

In this walkthrough, we will create a Function App to display a Hello message when there is an HTTP request.

29 Task 1: Create a Function app (5 min)

In this task, we will create a Function app.

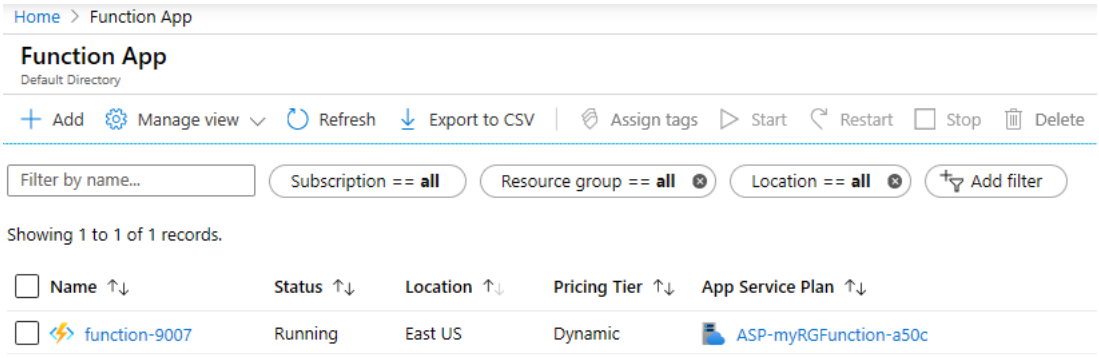
1. Sign in to the Azure portal.
2. In the **Search resources, services, and docs** text box at the top of the portal, search for and select **Function App** and then, from the **Function App** blade, click **+ Add, + Create, or + New**.
3. On the **Basic** tab of the **Function App** blade, specify the following settings (replace **xxxx** in the name of the function with letters and digits such that the name is globally unique and leave all other settings with their default values):

Settings	Value
Subscription	the name of your Azure subscription
Resource group	the name of a new resource group **myRGFunction**
Function App name	**function-xxxx**
Publish	**Code**
Runtime stack	**.NET**
Version	**3.1**
Region	**East US**

Note - Remember to change the **xxxx** so that it makes a unique **Function App name**

4. Click **Review + Create** and, after successful validation, click **Create** to begin provisioning and deploying your new Azure Function App.
5. Wait for the notification that the resource has been created.
6. Navigate back to the **Function App** blade, click **Refresh** and verify that the newly created function app

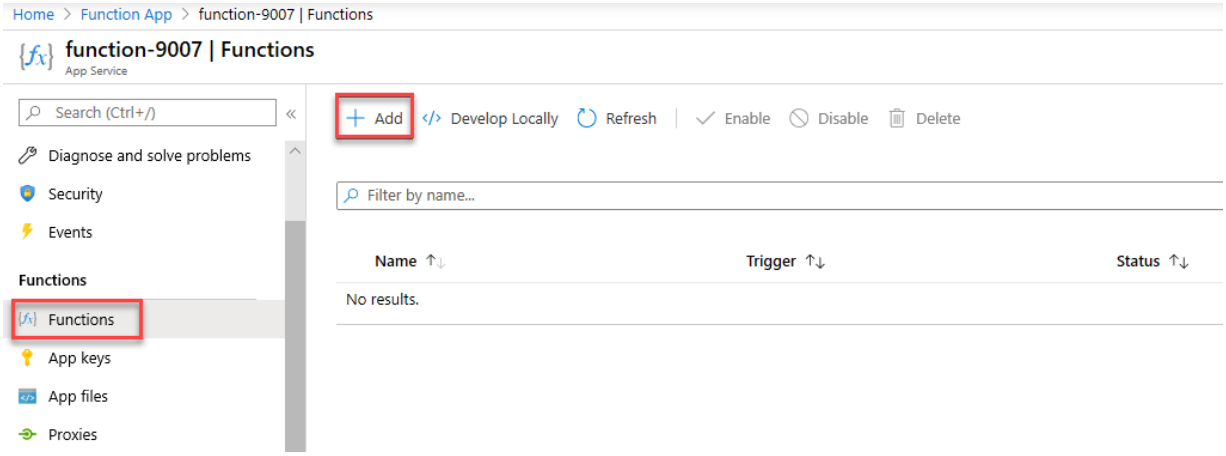
has the **Running** status.



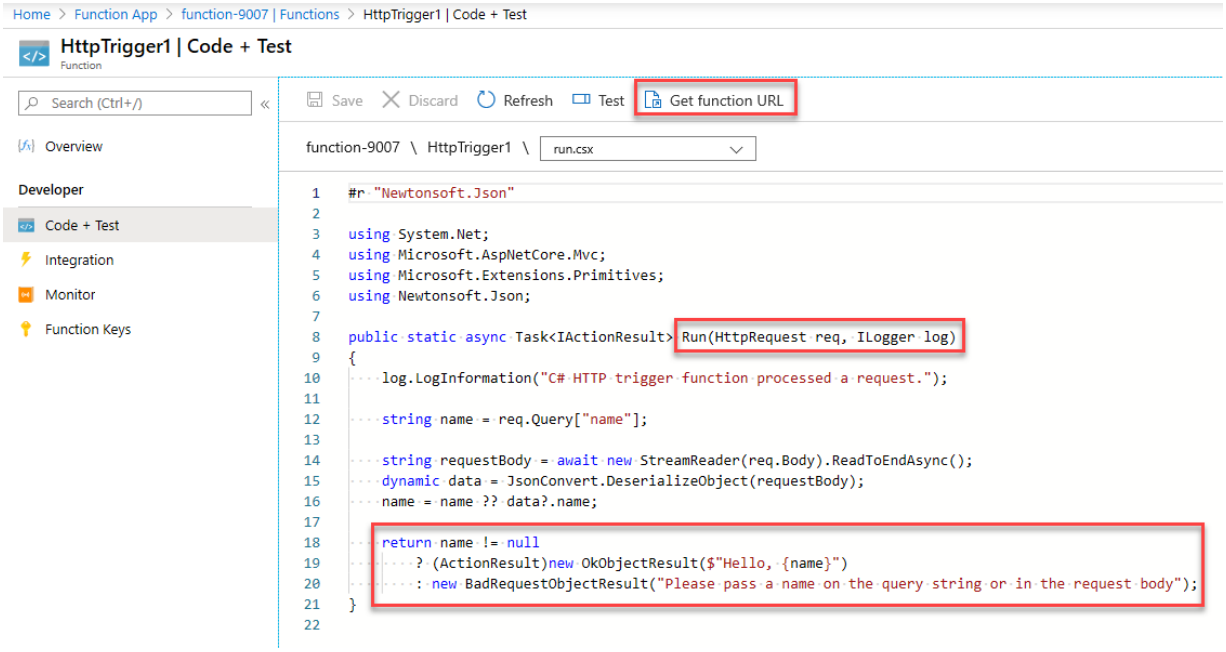
30 Task 2: Create a HTTP triggered function and test

In this task, we will use the Webhook + API function to display a message when there is an HTTP request.

1. On the **Function App** blade, click the newly created function app.
2. On the function app blade, in the **Functions** section, click **Functions** and then click + **Add**.

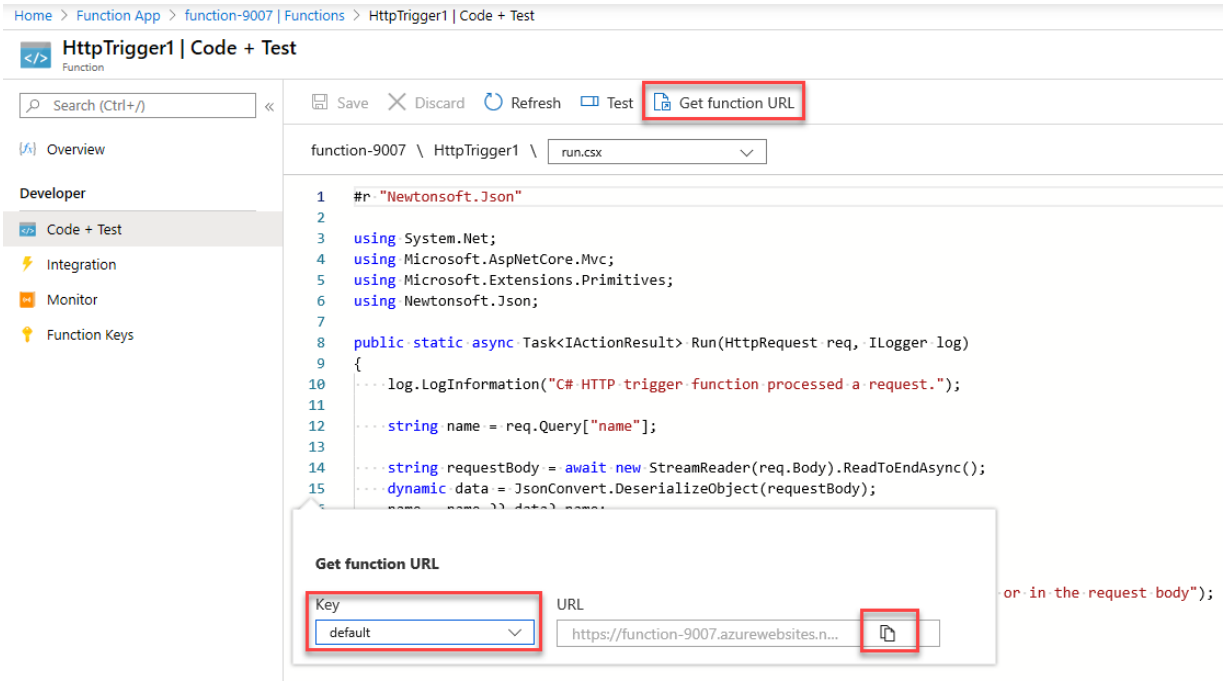


3. In the **Select a template** section of the **Add function** blade, click **HTTP trigger**, under the **Template details** section accept the defaults, then click **Add**.
4. On the **HttpTrigger1** blade, in the **Developer** section, click **Code + Test**.
5. On the **HttpTrigger1 | Code + Test** blade, review the auto-generated code and note that the code is designed to run an HTTP request and log information. Also, notice the function returns a Hello message with a name.

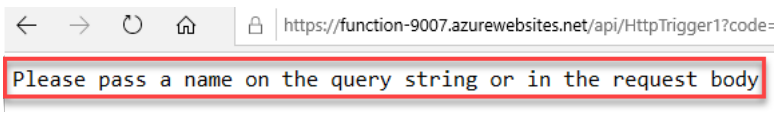


6. Click **Get function URL** from the top section of function editor.

7. Ensure that the value in the **Key** drop-down list is set to **default** and click **Copy** to copy the function URL.

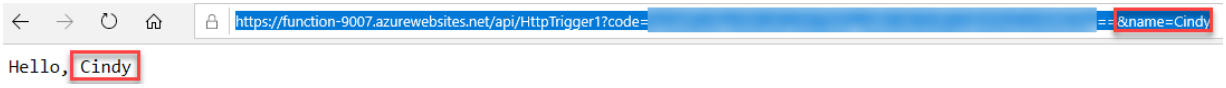


8. Open a new browser tab and paste the copied function URL into your web browser's address bar. When the page is requested the function will run. Notice the returned message stating that the function requires a name in the request body.

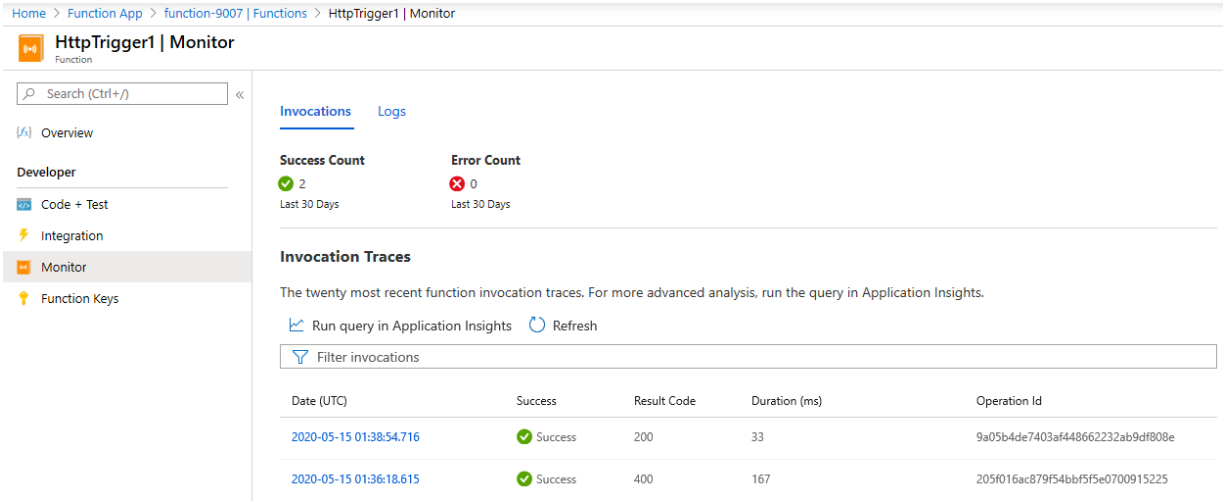


9. Append **&name=*yourname*** to the end of the URL.

   Note: Replace ***yourname*** with your first name. For example, if your name is Cindy, the final URL will resemble the following `https://azfuncxxx.azurewebsites.net/api/HttpTrigger1?code=X9xx9999xXXXXX9x9xxxXX==`



10. When your function runs, every invocation is traced. To view the traces in Azure portal, return to the **HttpTrigger1 | Code + Test** blade and click **Monitor**.



Congratulations! You have created a Function App to display a Hello message when there is an HTTP request.

30.1 Note: To avoid additional costs, you can remove this resource group. Search for resource groups, click your resource group, and then click Delete resource group. Verify the name of the resource group and then click Delete. Monitor the Notifications to see how the delete is proceeding.

30.2 wts: title: '09 - Create a VM with a Template (10 min)' module: 'Module 03: Describe core solutions and management tools'

31 09 - Create a VM with a Template

In this walkthrough, we will deploy a virtual machine with a QuickStart template and examine monitoring capabilities.

32 Task 1: Explore the gallery and locate a template (10 min)

In this task, we will browse the Azure QuickStart gallery and deploy a template that creates a virtual machine.

1. In a browser, access the Azure Quickstart Templates gallery. In the gallery you will find a number of popular and recently updated templates. These templates automate deployment of Azure resources, including installation of popular software packages.
2. Browse through the many different types of templates that are available.

   Note: Are there are any templates that are of interest to you?
3. Search for or directly access the Deploy a Virtual Machine template.

   Note: The **Deploy to Azure** button enables you to deploy the template via the Azure portal. During such deployment, you will be prompted only for small set of configuration parameters.
4. Click the **Deploy to Azure** button. Your browser session will be automatically redirected to the Azure portal.
5. If prompted, sign in to the Azure subscription you want to use in this lab.
6. Click **Edit template**. The Resource Manager template format uses the JSON format. Review the parameters and variables. Then locate the parameter for virtual machine name. Change the name to **myVMTemplate**. **Save** your changes. You are returned to the **Custom deployment** blade in the Azure portal.

7. On the **Custom deployment** blade configure the parameters required by the template (replace ***xxxx*** in the DNS label prefix with letters and digits such that the label is globally unique). Leave the defaults for everything else.

Setting	Value
Subscription	**Choose your subscription**
Resource group	**myRGTemplate** (create new)
Location	**(US) East US**
Admin username	**azureuser**
Admin password	**Pa$$w0rd1234**
DNS label prefix	**myvmtemplate*xxxx***
Windows OS version	**2019-Datacenter**

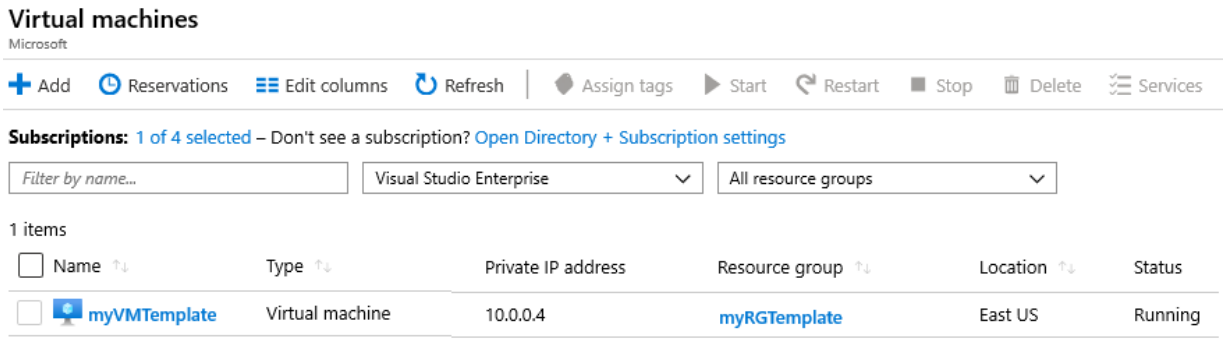
** Note: There is no cost associated with this template.

8. Click **Review + Create**.
9. Once Validation is passed click the **Create** button. It can take anywhere from five to seven minutes to deploy the virtual machine.

33 Task 2: Verify and monitor your virtual machine deployment

In this task, we will verify the virtual machine deployed correctly.

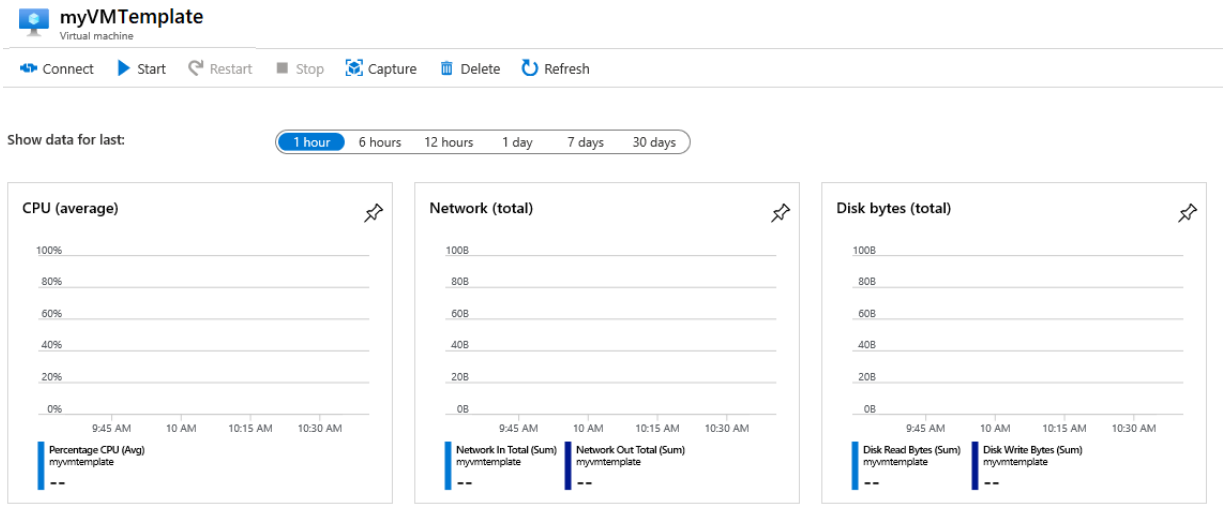
1. From the **All services** blade, search for and select **Virtual machines**.
2. Ensure your new virtual machine was created.



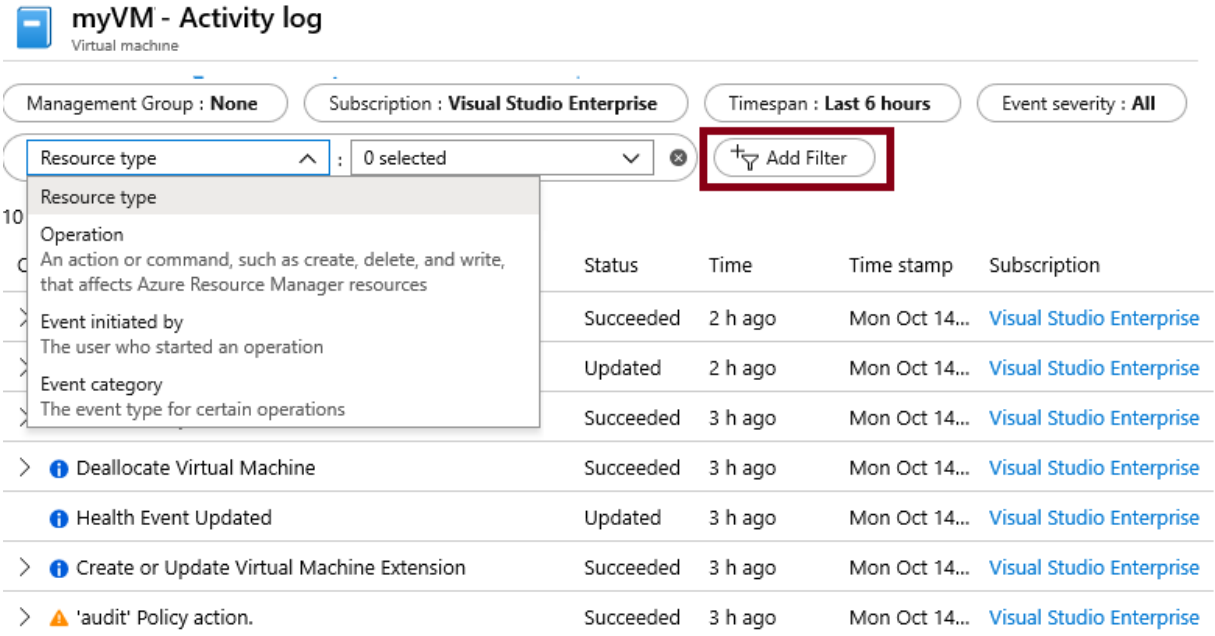
3. Select your virtual machine and on the **Overview** pane scroll down to view monitoring data.

   Note: The monitoring timeframe can be adjusted from one hour to 30 days.

4. Review different charts that are provided including **CPU (average)**, **Network (total)**, and **Disk bytes (total)**.



5. Click on any chart. Note that you can **Add metric** and change the chart type.
6. Return to the **Overview** blade.
7. Click on the **Activity log** (left pane). Activity logs record such events as creation or modification of resources.
8. Click **Add filter**, and experiment with searching for different event types and operations.



33.1 Note: To avoid additional costs, you can remove this resource group. Search for resource groups, click your resource group, and then click Delete resource group. Verify the name of the resource group and then click Delete. Monitor the Notifications to see how the delete is proceeding.

33.2 wts: title: '10 - Create a VM with PowerShell (10 min)' module: 'Module 03: Describe core solutions and management tools'

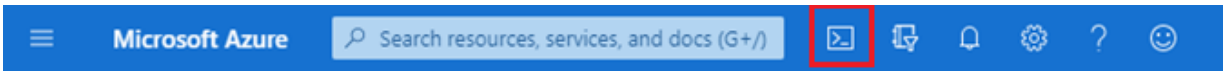
34 10 - Create a VM with PowerShell

In this walk-through, we will configure the Cloud Shell, use Azure PowerShell module to create a resource group and virtual machine, and review Azure Advisor recommendations.

35 Task 1: Configure the Cloud Shell (10 min)

In this task, we will configure Cloud Shell.

1. Sign in to the Azure portal.
2. From the Azure portal, open the **Azure Cloud Shell** by clicking on the icon in the top right of the Azure Portal.



3. If you have previously used the Cloud Shell, proceed to the next task.
4. When prompted to select either **Bash** or **PowerShell**, select **PowerShell**.
5. When prompted, click **Create storage**, and wait for the Azure Cloud Shell to initialize.

36 Task 2: Create a resource group and virtual machine

In this task, we will use PowerShell to create a resource group and a virtual machine.

1. Ensure **PowerShell** is selected in the upper-left drop-down menu of the Cloud Shell pane.
2. In the PowerShell session, within the Cloud Shell pane, create a new resource group.

```
New-AzResourceGroup -Name myRGPS -Location EastUS
```

3. Verify your new resource group.

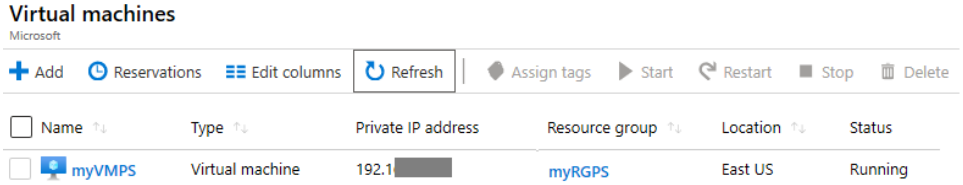
```
Get-AzResourceGroup | Format-Table
```

4. Create a virtual machine. When prompted provide the username (**azureuser**) and the password (**Pa$$w0rd1234**) that will be configured as the local Administrator account on that virtual machines. Ensure that you include the tick (‘) characters at the end of each line except for the last one (there should not be any tick characters if you type entire command on a single line).

```
New-AzVm `
-ResourceGroupName "myRGPS" `
-Name "myVMPS" `
-Location "East US" `
-VirtualNetworkName "myVnetPS" `
-SubnetName "mySubnetPS" `
-SecurityGroupName "myNSGPS" `
-PublicIpAddressName "myPublicIpPS"
```

** Wait for VM to deploy before closing PowerShell

5. Close the PowerShell session Cloud Shell pane.
6. In the Azure portal, search for **Virtual machines** and verify the **myVMPS** is running. This may take a few minutes.



7. Access the new virtual machine and review the Overview and Networking settings to verify your information was correctly deployed.

37 Task 3: Execute commands in the Cloud Shell

In this task, we will practice executing PowerShell commands from the Cloud Shell.

1. From the Azure portal, open the **Azure Cloud Shell** by clicking on the icon in the top right of the Azure Portal.

2. Ensure **PowerShell** is selected in the upper-left drop-down menu of the Cloud Shell pane.
3. Retrieve information about your virtual machine including name, resource group, location, and status. Notice the PowerState is **running**.

```
Get-AzVM -name myVMPS -status | Format-Table -autosize
```

4. Stop the virtual machine. When prompted confirm (Yes) to the action.

```
Stop-AzVM -ResourceGroupName myRGPS -Name myVMPS
```

5. Verify your virtual machine state. The PowerState should now be **deallocated**. You can also verify the virtual machine status in the portal.

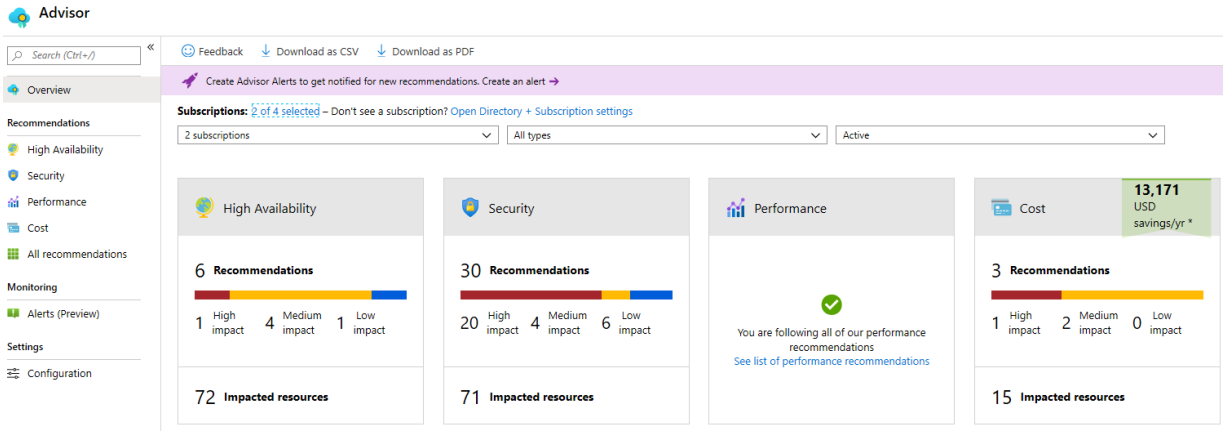
```
Get-AzVM -name myVMPS -status | Format-Table -autosize
```

38 Task 4: Review Azure Advisor Recommendations

Note: This same task is in the Create a VM with Azure CLI lab.

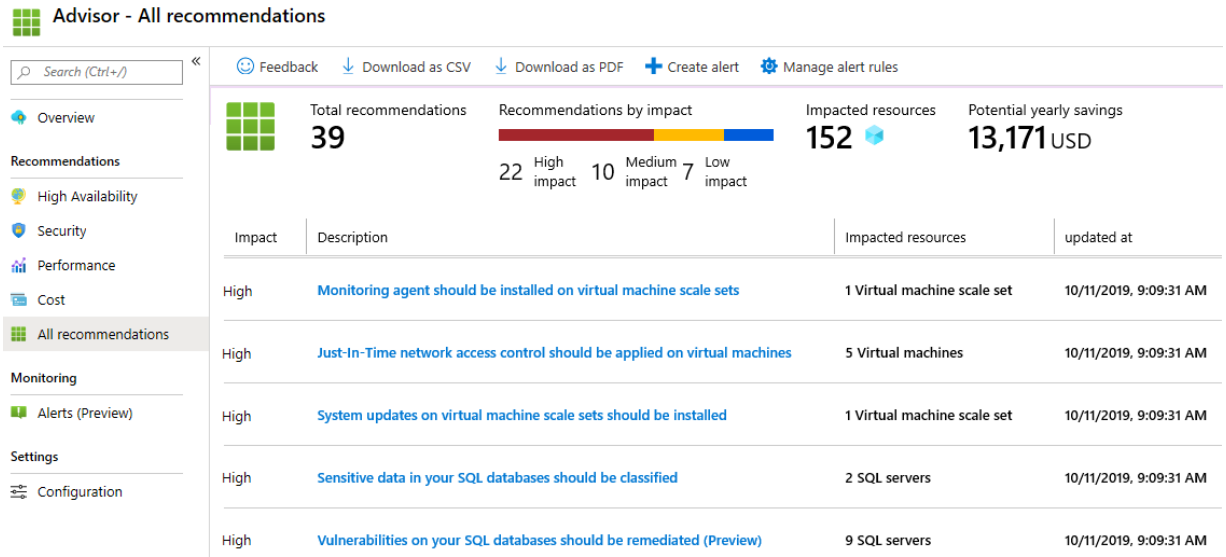
In this task, we will review Azure Advisor recommendations for our virtual machine.

1. From the **All services** blade, search for and select **Advisor**.
2. On the **Advisor** blade, select **Overview**. Notice recommendations are grouped by High Availability, Security, Performance, and Cost.



3. Select **All recommendations** and take time to view each recommendation and suggested actions.

Note: Depending on your resources, your recommendations will be different.



4. Notice that you can download the recommendations as a CSV or PDF file.
5. Notice that you can create alerts.

6. If you have time, continue to experiment with Azure PowerShell.

Congratulations! You have configured Cloud Shell, created a virtual machine using PowerShell, practiced with PowerShell commands, and viewed Advisor recommendations.

38.1 Note: To avoid additional costs, you can remove this resource group. Search for resource groups, click your resource group, and then click Delete resource group. Verify the name of the resource group and then click Delete. Monitor the Notifications to see how the delete is proceeding.

38.2 wts: title: '11 - Create a VM with the CLI (10 min)' module: 'Module 03: Describe core solutions and management tools'

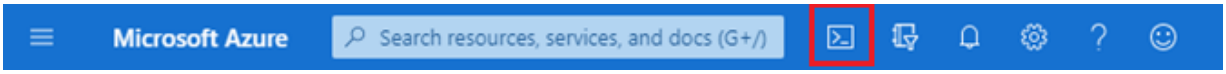
39 11 - Create a VM with the CLI

In this walk-through, we will configure the Cloud Shell, use Azure CLI to create a resource group and virtual machine, and review Azure Advisor recommendations.

40 Task 1: Configure the Cloud Shell (10 min)

In this task, we will configure Cloud Shell.

1. Sign in to the Azure portal.
2. From the Azure portal, open the **Azure Cloud Shell** by clicking on the icon in the top right of the Azure Portal.

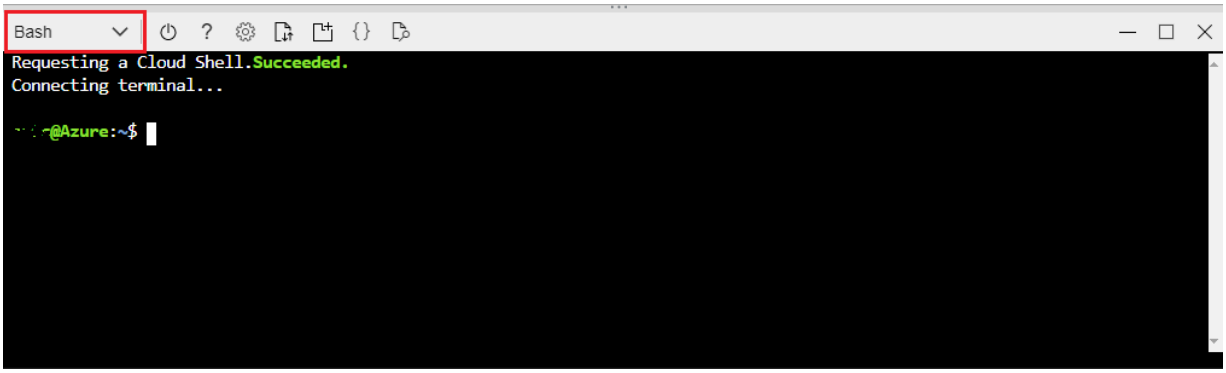


3. If you have previously used the Cloud Shell, proceed to the next task.
4. When prompted to select either **Bash** or **PowerShell**, select **Bash**.
5. When prompted, click **Create storage**, and wait for the Azure Cloud Shell to initialize.

41 Task 2: Create a resource group and a virtual machine

In this task, we will use Azure CLI to create a resource group and a virtual machine.

1. Ensure **Bash** is selected in the upper-left drop-down menu of the Cloud Shell pane (and if not, select it).



2. In the Bash session, within the Cloud Shell pane, create a new resource group.

```
az group create --name myRGCLI --location EastUS
```

3. Verify the resource group was created.

```
az group list --output table
```

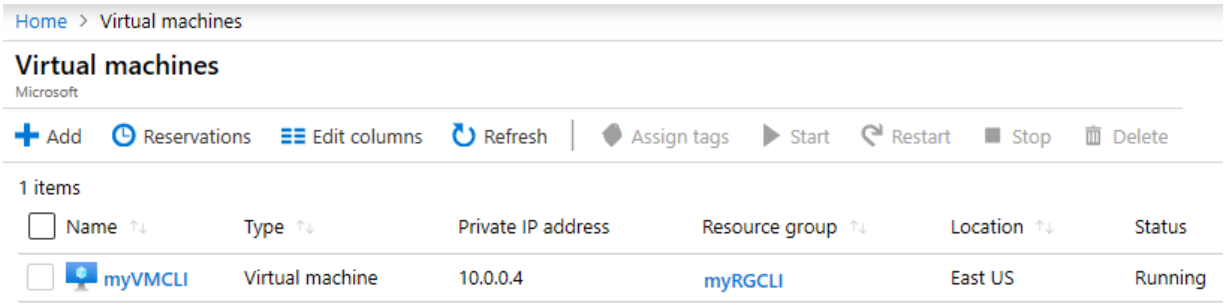
4. Create a new virtual machine. Make sure that each line except for the last one is followed by the backslash (\) character. If you type the whole command on the same line, do not use any backslash characters.

```
az vm create \
--name myVMCLI \
--resource-group myRGCLI \
--image UbuntuLTS \
--location EastUS \
--admin-username azureuser \
--admin-password Pa$$w0rd1234
```

> **Note**: If you are using the command line on a Windows computer, replace the backslash (\) character with the caret (^) character.

Note: The command will take 2 to 3 minutes to complete. The command will create a virtual machine and various resources associated with it such as storage, networking and security resources. Do not continue to the next step until the virtual machine deployment is complete.

5. When the command finishes running, in the browser window, close the Cloud Shell pane.
6. In the Azure portal, search for **Virtual machines** and verify that **myVMCLI** is running.



42 Task 3: Execute commmands in the Cloud Shell

In this task, we will practice executing CLI commands from the Cloud Shell.

1. From the Azure portal, open the **Azure Cloud Shell** by clicking on the icon in the top right of the Azure Portal.
2. Ensure **Bash** is selected in the upper-left drop-down menu of the Cloud Shell pane.
3. Retrieve information about the virtual machine you provisioned, including name, resource group, location, and status. Notice the PowerState is **running**.

   ```
   az vm show --resource-group myRGCLI --name myVMCLI --show-details --output table
   ```

4. Stop the virtual machine. Notice the message that billing continues until the virtual machine is deallocated.

   ```
   az vm stop --resource-group myRGCLI --name myVMCLI
   ```

5. Verify your virtual machine status. The PowerState should now be **stopped**.

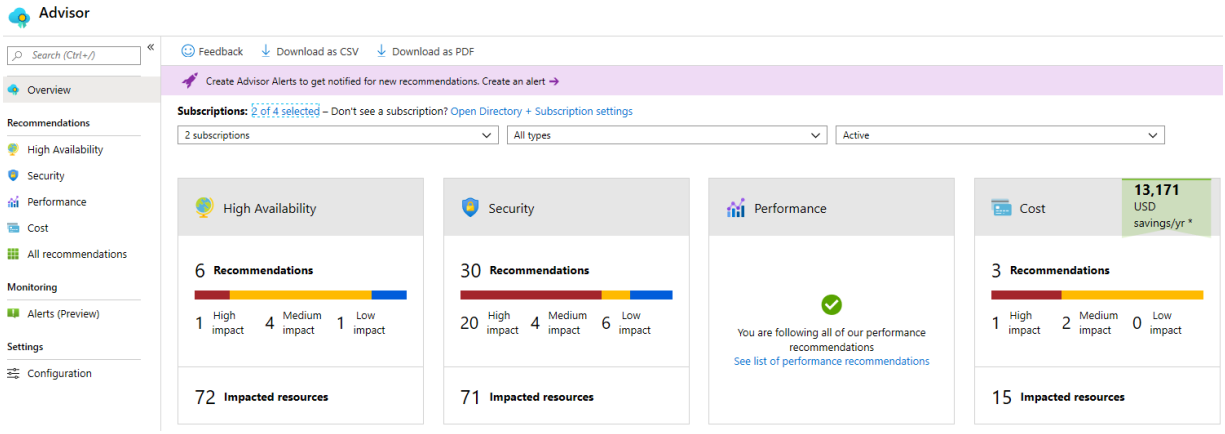
   ```
   az vm show --resource-group myRGCLI --name myVMCLI --show-details --output table
   ```

43 Task 4: Review Azure Advisor Recommendations

In this task, we will review Azure Advisor recommendations.

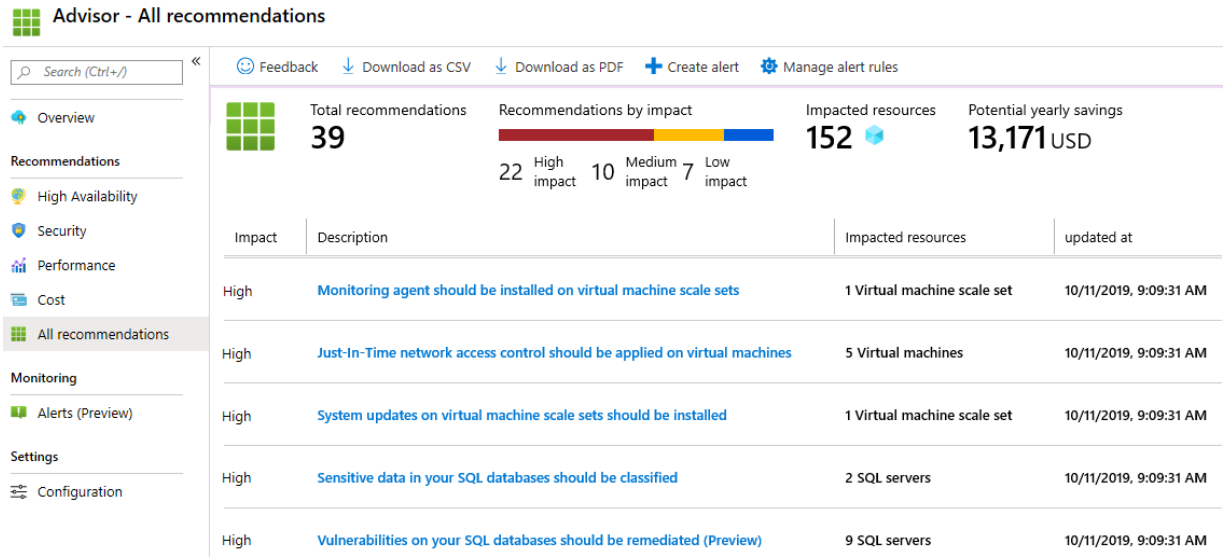
Note: If you have completed the previous lab (Create a VM with PowerShell), then you have already performed this task.

1. From the **All services** blade, search for and select **Advisor**.
2. On the **Advisor** blade, select **Overview**. Notice recommendations are grouped by High Availability, Security, Performance, and Cost.



3. Select **All recommendations** and take time to view each recommendation and suggested actions.

   Note: Depending on your resources, your recommendations will be different.



4. Notice that you can download the recommendations as a CSV or PDF file.
5. Notice that you can create alerts.
6. If you have time, continue to experiment with Azure CLI.

Congratulations! You have configured Cloud Shell, created a virtual machine using Azure CLI, practiced with Azure CLI commands, and viewed Advisor recommendations.

43.1 Note: To avoid additional costs, you can remove this resource group. Search for resource groups, click your resource group, and then click Delete resource group. Verify the name of the resource group and then click Delete. Monitor the Notifications to see how the delete is proceeding.

43.2 wts: title: '12 - Implement Azure Key Vault (5 min)' module: 'Module 04: Describe general security and network security features'

44 12 - Implement Azure Key Vault

In this walkthrough, we will create an Azure Key vault and then create a password secret within that key vault, providing a securely stored, centrally managed password for use with applications.

45 Task 1: Create an Azure Key Vault (5 min)

1. Sign in to the Azure portal.

2. From the **All services** blade, search for and select **Key vaults**, then select **+ Add, + Create, or + New**.
3. Configure the key vault (replace **xxxx** in the name of the key vault with letters and digits such that the name is globally unique). Leave the defaults for everything else.

Setting	Value
Subscription	**Use your subscription**
Resource group	**myRGKV** (create new)
Key vault name	**keyvaulttestxxx**
Location	**East US**
Pricing tier	**Standard**

4. Click **Review + create** and then after the validation click **Create**.
5. Once the new key vault is provisioned, click **Go to resource**. Or you can locate your new key vault by searching for it.
6. Click on the key vault **Overview** tab and take note of the **DNS name**. Applications that use your vault through the REST API will need this URI.
7. Take a moment to browse through some of the other key vault options. Under **Settings** review **Keys**, **Secrets**, **Certificates**, **Access Policies**, **Firewalls and virtual networks**.

   Note: Your Azure account is the only one authorized to perform operations on this new vault. You can modify this if you wish in the **Settings** and then the **Access policies** section.

46 Task 2: Add a secret to the Key Vault

In this task, we will add a password to the key vault.

1. Under **Settings** click **Secrets**, then click **+ Generate/Import**.
2. Configure the secret. Leave the other values at their defaults. Notice you can set an activation and expiration date. Notice you can also disable the secret.

Setting	Value
Upload options	**Manual**
Name	**ExamplePassword**
Value	**hVFkk96**

3. Click **Create**.
4. Once the secret has been successfully created, click on the **ExamplePassword**, and note it has a status of **Enabled**
5. Click the current version, note the the **Secret Identifier**. This is the url value that you can now use with applications. It provides a centrally managed and securely stored password.
6. Click the button **Show Secret Value**, to display the password you specified earlier.

Congratulations! You have created an Azure Key vault and then created a password secret in that key vault, providing a securely stored, centrally managed password for use with applications.

46.1 Note: To avoid additional costs, you can remove this resource group. Search for resource groups, click your resource group, and then click Delete resource group. Verify the name of the resource group and then click Delete. Monitor the Notifications to see how the delete is proceeding.

46.2 wts: title: '13 - Secure network traffic (10 min)' module: 'Module 04: Describe general security and network security features'

47 13 - Secure network traffic

In this walk-through, we will configure a network security group.

48 Task 1: Create a virtual machine (10 min)

In this task, we will create a Windows Server 2019 Datacenter virtual machine.

1. Sign in to the Azure portal.
2. From the **All services** blade, search for and select **Virtual machines**, and then click **+ Add**.
3. On the **Basics** tab, fill in the following information (leave the defaults for everything else):

Settings	Values
Subscription	**Choose your subscription**
Resource group	**myRGSecure** (create new)
Virtual machine name	**SimpleWinVM**
Location	**(US) East US**
Image	**Windows Server 2019 Datacenter**
Size	**Standard D2s v3**
Administrator account username	**azureuser**
Administrator account password	**Pa$$w0rd1234**
Inbound port rules	**None**

4. Switch to the **Networking** tab, and configure the following setting:

Settings	Values
NIC network security group	**None**

5. Switch to the **Management** tab, and in its **Monitoring** section, select the following setting:

Settings	Values
Boot diagnostics	**Disable**

6. Leave the remaining defaults and then click the **Review + create** button at the bottom of the page.
7. Once Validation is passed click the **Create** button. It can take about five minutes to deploy the virtual machine.
8. Monitor the deployment. It may take a few minutes for the resource group and virtual machine to be created.
9. From the deployment blade or from the Notification area, click **Go to resource**.
10. On the **SimpleWinVM** virtual machine blade, click **Networking**, review the **Inbound port rules** tab, and note that there is no network security group associated with the network interface of the virtual machine or the subnet to which the network interface is attached.

Note: Identify the name of the network interface. You will need it in the next task.

49 Task 2: Create a network security group

In this task, we will create a network security group and associate it with the network interface.

1. From the **All services** blade, search for and select **Network security groups** and then click **+ Add**
2. On the **Basics** tab of the **Create network security group** blade, specify the following settings.

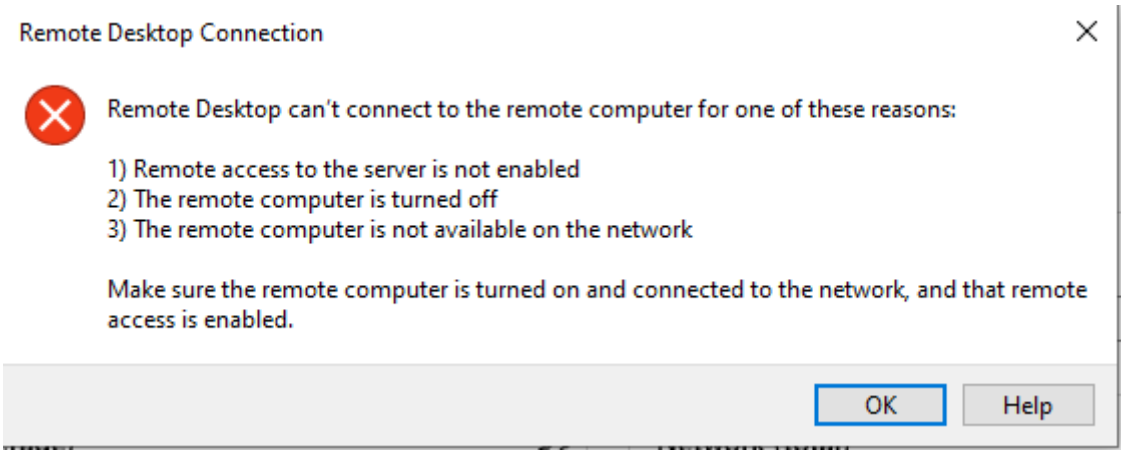
Setting	Value
Subscription	**Choose your subscription**
Resource group	**myRGSecure**
Name	**myNSGSecure**
Region	**(US) East US**

3. Click **Review + create** and then after the validation click **Create**.
4. After the NSG is created, click **Go to resource**.
5. Under **Settings** click **Network interfaces** and then **+ Associate**.
6. Select the network interace you identified in the previous task.

50 Task 3: Configure an inbound security port rule to allow RDP

In this task, we will allow RDP traffc to the virtual machine by configuring an inbound security port rule.

1. In the Azure portal, navigate to the blade of the **SimpleWinVM** virtual machine.
2. On the **Overview** pane, click **Connect**.
3. Attempt to connect to the virutal machine using RDP. By default the network security group does not allow RDP. Close the error window.



4. On the virtual machine blade, scroll down to the **Settings** section, click on **Networking**, and notice the inbound rules for the **myNSGSecure (attached to network interface: myVMNic)** network security group deny all inbound traffic except traffic within the virtual network and load balancer probes.
5. On the **Inbound port rules** tab, click **Add inbound port rule** . Click **Add** when you are done.

Setting	Value
Source	**Any**
Source port ranges	*****
Destination	**Any**
Destination port ranges	**3389**
Protocol	**TCP**

Setting	Value
Action	**Allow**
Priority	**300**
Name	**AllowRDP**

6. Wait for the rule to be provisioned and then try again to RDP into the virtual machine. This time you should be successful. Remember the user is **azureuser** and the password is **Pa$$w0rd1234**.

51 Task 4: Configure an outbound security port rule to deny Internet access

In this task, we will create a NSG outbound port rule that will deny Internet access and then test to ensure the rule is working.

1. Continue in your virtual machine RDP session.
2. After the machine starts, open an **Internet Explorer** browser.
3. Verify that you can access **https://www.bing.com** and then close Internet Explorer. You will need to work through the IE enhanced security pop-ups.

   Note: We will now configure a rule to deny outbound internet access.
4. In the Azure portal, navigate back to the blade of the **SimpleWinVM** virtual machine.
5. Under **Settings**, click **Networking**, and then **Outbound port rules**.
6. Notice there is a rule, **AllowInternetOutbound**. This a default rule and cannot be removed.
7. Click **Add outbound port rule** to the right of the **myNSGSecure (attached to network interface: myVMNic)** network security group and configure a new outbound security rule with a higher priority that will deny internet traffic. Click **Add** when you are finished.

Setting	Value
Source	**Any**
Source port ranges	*****
Destination	**Service Tag**
Destination service tag	**Internet**
Destination port ranges	*****
Protocol	**TCP**
Action	**Deny**
Priority	**4000**
Name	**DenyInternet**

8. Return to your RDP session.
9. Browse to **https://www.microsoft.com**. The page should not display. You may need to work through additional IE enhanced security pop-ups.

51.1 Note: To avoid additional costs, you can remove this resource group. Search for resource groups, click your resource group, and then click Delete resource group. Verify the name of the resource group and then click Delete. Monitor the Notifications to see how the delete is proceeding.

51.2 wts: title: '14 - Manage access with RBAC (5 min)' module: 'Module 05: Describe identity, governance, privacy, and compliance features'

52 14 - Manage access with RBAC

In this walkthrough, we will assign roles and view activity logs.

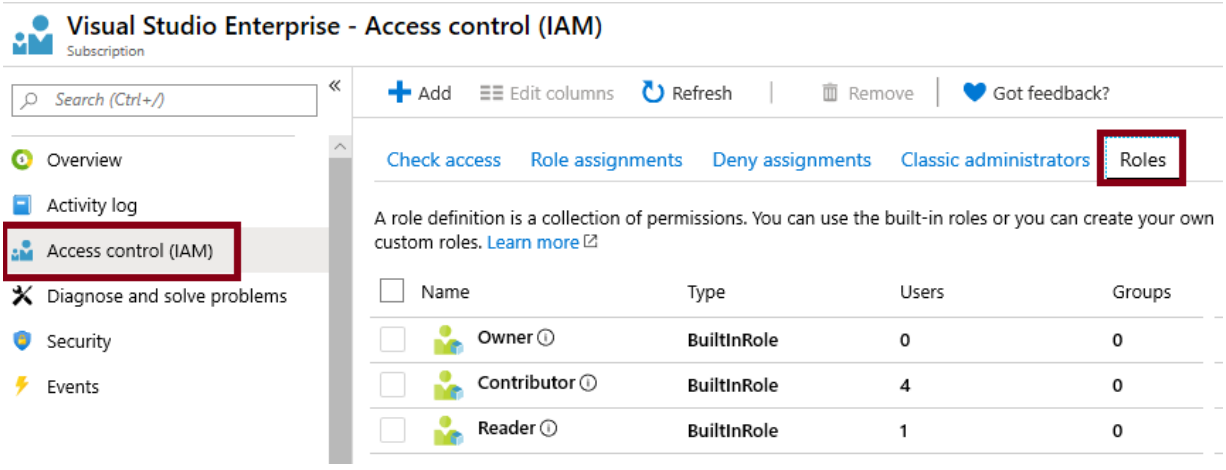
53 Task 1: View and assign roles (5 min)

In this task, we will assign the Virtual machine contributor role.

1. Sign in to the Azure portal.
2. From the **All services** blade, search for and select **Resource groups**, then click **+ Add**, **+ Create**, **or + New**.
3. Create a new resource group. Click **Create** when you are finished.

Setting	Value
Subscription	**Choose your subscription**
Resource group	**myRGRBAC**
Region	**(US) East US**

4. Create **Review + create** and then click **Create**.
5. **Refresh** the resource group page and click the entry representing the newly created resource group.
6. Click on the **Access control (IAM)** blade, and then switch to the **Roles** tab. Scroll through the large number of roles definitions that are available. Use the Informational icons to get an idea of each role's permissions. Notice there is also information on the number of users and groups that are assigned to each role.

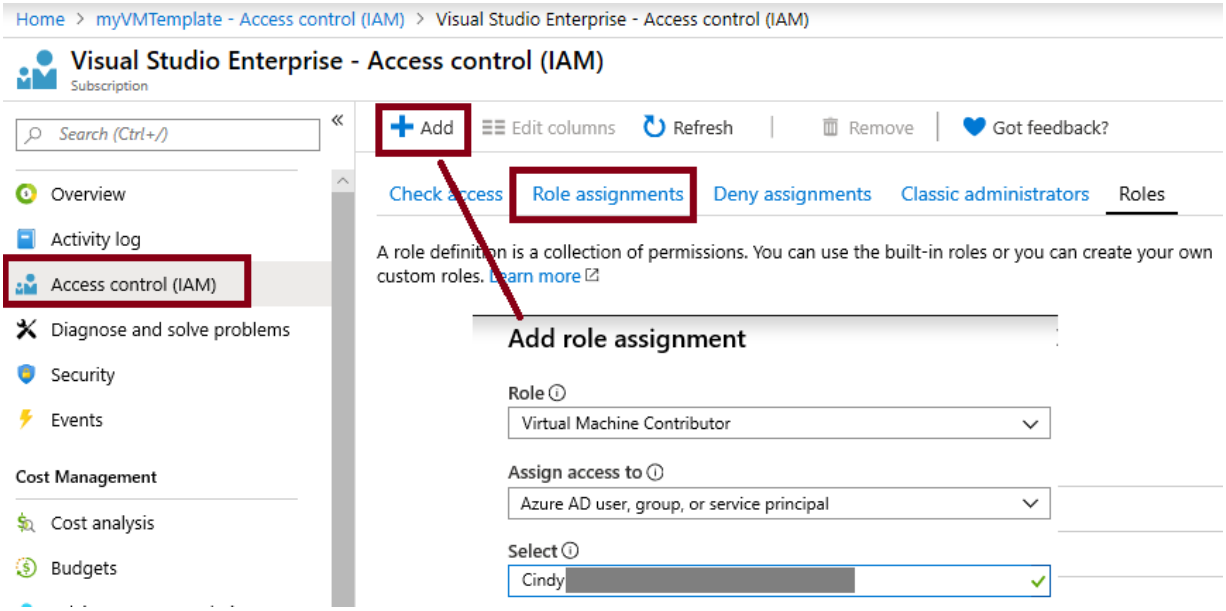


7. Switch to the **Role assignments** tab of the **myRGRBAC - Access control (IAM)** blade, click **+ Add** and then click **Add role assignment**. Assign the Virtual Machine Contributor role to your user account, then click **Save**.

Setting	Value
Role	**Virtual machine contributor**
Assign access to	**user, group, or service principal**
Select	your user account

Setting	Value

Note: The Virtual machine contributor role lets you manage virtual machines, but not access their operating system or manage the virtual network and storage account they are connected to.



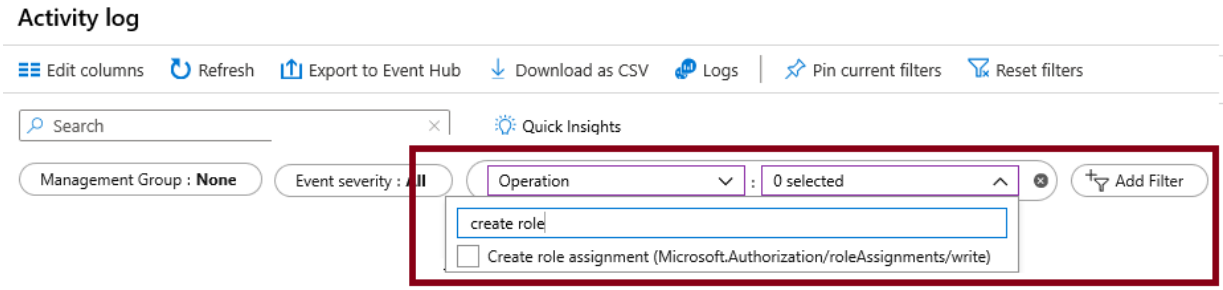
8. **Refresh** the Role assignments page and ensure you are now listed as a Virtual machine contributor.

   Note: This assignment does not actually grant you any additional provileges, since your account has already the Owner role, which includes all privilges associated with the Contributor role.

54 Task 2: Monitor role assignments and remove a role

In this task, we will view the activity log to verify the role assignment, and then remove the role.

1. On the myRGRBAC resource group blade, click **Activity log**.
2. Click **Add filter**, select **Operation**, and then **Create role assignment**.



3. Verify the Activity log shows your role assignment.

   Note: Can you figure out how to remove your role assignment?

Congratulations! You have assigned roles and viewed activity logs.

Note: To avoid additional costs, you can remove this resource group. Search for resource groups, click your resource group, and then click **Delete resource group**. Verify the name of the resource group and then click **Delete**. Monitor the **Notifications** to see how the delete is proceeding.

54.1 wts: title: '15 - Manage resource locks (5 min)' module: 'Module 05: Describe identity, governance, privacy, and compliance features'

55 15 - Manage resource locks

In this walkthrough, we will add a lock to the resource group and test deleting the resource group. Locks can be applied in a subscription to resource groups, or individual resources to prevent accidental deletion or modification of critical resources.

56 Task 1: Create a resource group (5 min)

In this task, we will create a resource group for this exercise.

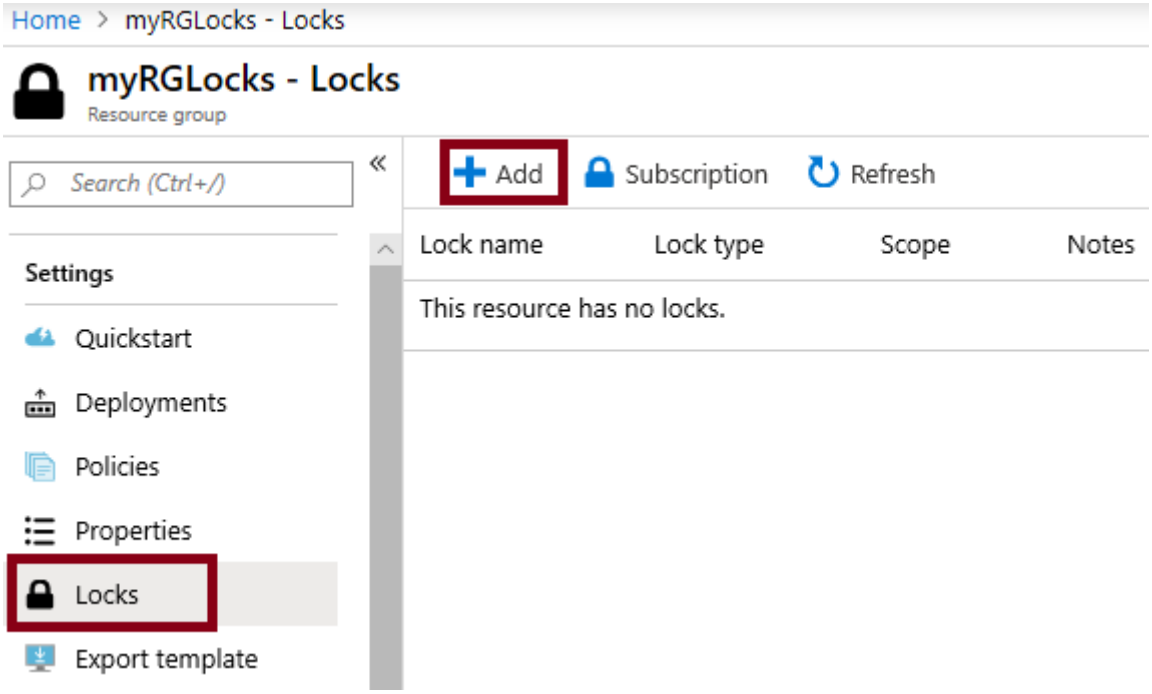
1. Sign in to the Azure portal.
2. In the **Search** bar at the top of the portal, search for **Resource groups**.
3. Then click **+Add +New +Create **.

Setting	Value
Subscription	**Use your subscription**
Name	**myRGLocks**
Region	**(US) East US**

57 Task 2: Add a Lock to the resource group and test deletion

In this task, we will add a resource lock to the resource group and test deleting the resource group.

1. In the Azure portal, navigate to the newly created resource group **myRGLocks**.
2. You can apply a lock to a subscription, resource group, or individual resource to prevent accidental deletion or modification of critical resources.
3. In the **Settings** section, click **Locks**, and then click **+ Add**.

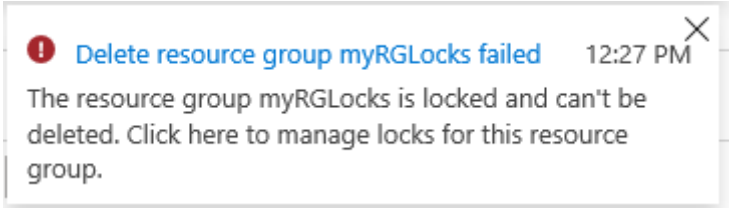


4. Configure the new lock. When you are done click **OK**.

Setting	Value
Lock name	**RGLock**

Setting	Value
Lock Type	**Delete**

5. Click **Overview** and click **Delete resource group**. Type the name of the resource group and click **OK**. You receive an error message stating the resource group is locked and can't be deleted.



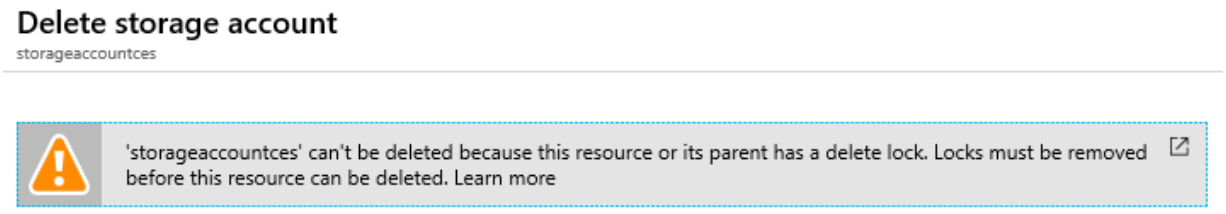
58 Task 3: Test deleting a member of the resource group

In this task, we will test if the resource lock protects a storage account in the resource group.

1. From the **All services** blade, search for and select **Storage accounts**, and then click **+ Add, + Create, or + New**.
2. On the **Storage Accounts** page **+Add +New +Create ** blade, fill in the following information (replace **xxxx** in the name of the storage account with letters and digits such that the name is globally unique). Leave the defaults for everything else.

Setting	Value
Subscription	**Select your subscription**
Resource group	**myRGLocks**
Storage account name	**storageaccountxxxx**
Location	**(US) East US**
Performance	**Standard**
Account kind	**StorageV2 (general purpose v2)**
Replication	**Locally redundant storage (LRS)**
Access tier (default)	**Hot**

3. Click **Review + Create** to review your storage account settings and allow Azure to validate the configuration.
4. Once validated, click **Create**. Wait for the notification that the account was successfully created.
5. Wait for the notification that the storage account was successfully created.
6. Access your new storage account and from the **Overview** pane, click **Delete**. You receive an error message stating the resource or its parent has a delete lock.

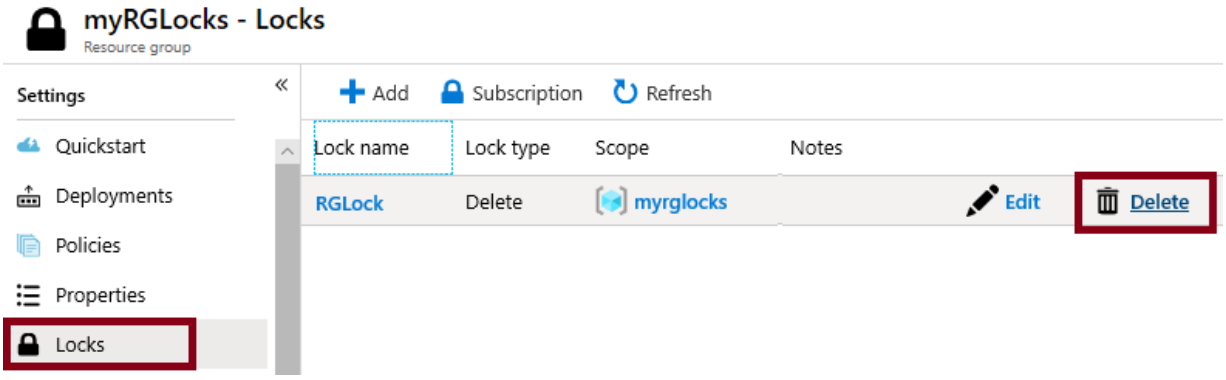


Note: Although we did not create a lock specifically for the storage account, we did create a lock at the resource group level, which contains the storage account. As such, this *parent* level lock prevents us from deleting the resource and the storage account inherits the lock from the parent.

59 Task 4: Remove the resource lock

In this task, we will remove the resource lock and test.

1. Return to the **myRGLocks-XXXXXXXX** resource group blade and, in the **Settings** section, click **Locks**.
2. Click **Delete** link to the far right of the **myRGLocks-XXXXXXXX** entry, to the right of **Edit**.



3. Return to the storage account blade and confirm you can now delete the resource.

Congratulations! You created a resource group, added a lock to resource group and tested deletion, tested deleting a resource in the resource group, and removed the resource lock.

59.1 Note: To avoid additional costs, you can remove this resource group. Search for resource groups, click your resource group, and then click Delete resource group. Verify the name of the resource group and then click Delete. Monitor the Notifications to see how the delete is proceeding.

59.2 wts: title: '16 - Implement resource tagging (5 min)' module: 'Module 05: Describe identity, governance, privacy, and compliance features'

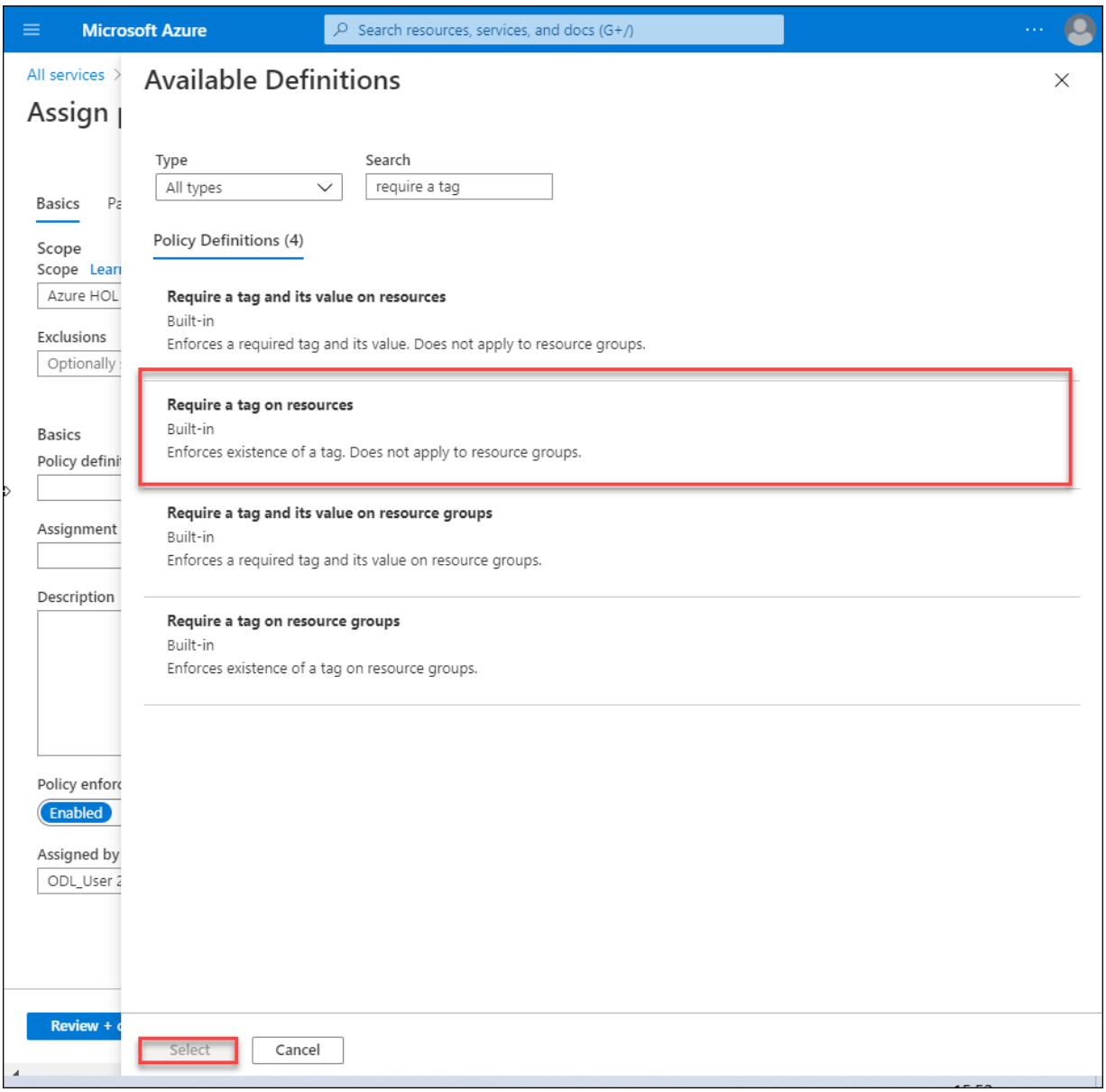
60 16 - Implement resource tagging

In this walkthrough, we will create a policy assignment that requires tagging, created a storage account and test the tagging, view resources with a specified tag, and remove the tagging policy.

61 Task 1: Create a Policy assignment (5 min)

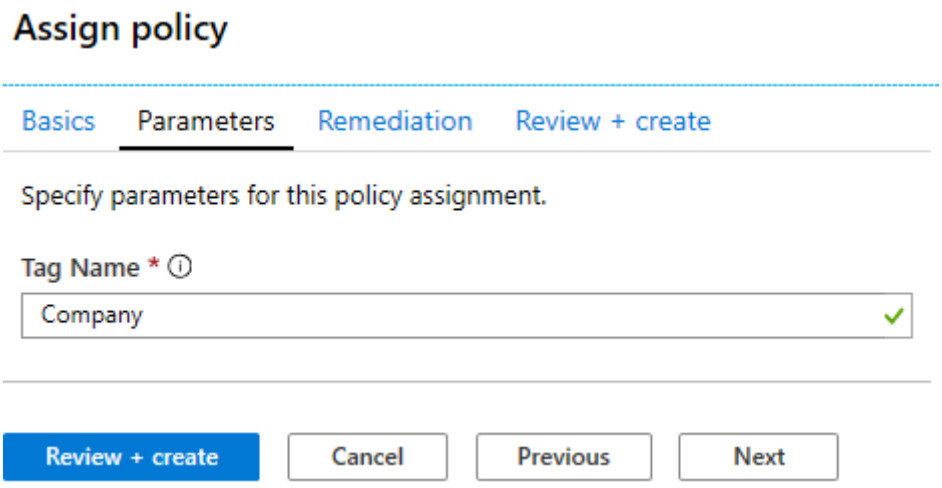
In this task, we will configure the **Require a tag on resources** policy and assign it to our subscription.

1. Sign in to the Azure portal.
2. From the **All services** blade, search for and select **Policy**.
3. Scroll down to the **Authoring** section, click **Assignments**, and then click **Assign Policy** from the top of the page.
4. Notice the **Scope** for our policy will be subscription wide.
5. Under **Basics** Select the **Policy definition** ellipsis button (right side of textbox). In the **Search** box, enter the value **tag**. A list of related Policies with the word **tag** will appear. Scroll down till you find the **Require a tag on resources** definition, click on it and click **Select**.



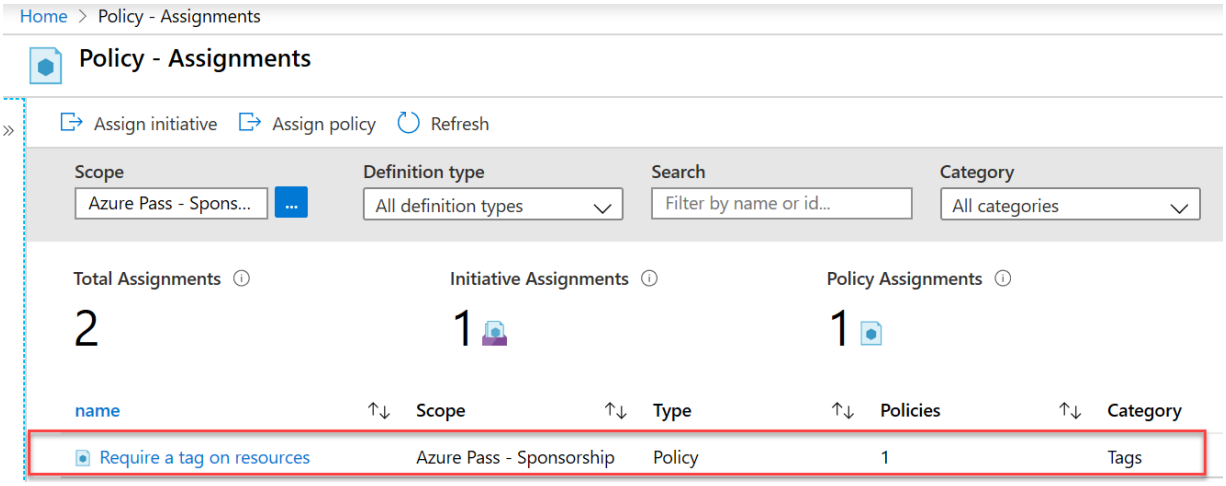
6. On the **Parameters** tab, type in **Company** for the tag name. And **Contoso** for the Value. Click **Review + create**, and then **Create**.

   Note: This is a simple example to demonstrate tagging. Please note that the assignment takes around 30 minutes to take effect.



7. The **Require a tag on resources** policy assignment is now in place. When a resource is created, it must

include a tag with the Company key.



62 Task 2: Create a storage account to test the required tagging

In this task, we will create storage accounts to test the required tagging.

1. In the Azure Portal, from the **All services** blade, search for and select **Storage accounts**, and then click **+ Add, + Create, or + New**.
2. On the **Basics** tab of the **Create storage account** blade, fill in the following information (replace **xxxx** in the name of the storage account with letters and digits such that the name is globally unique). Leave the defaults for everything else.

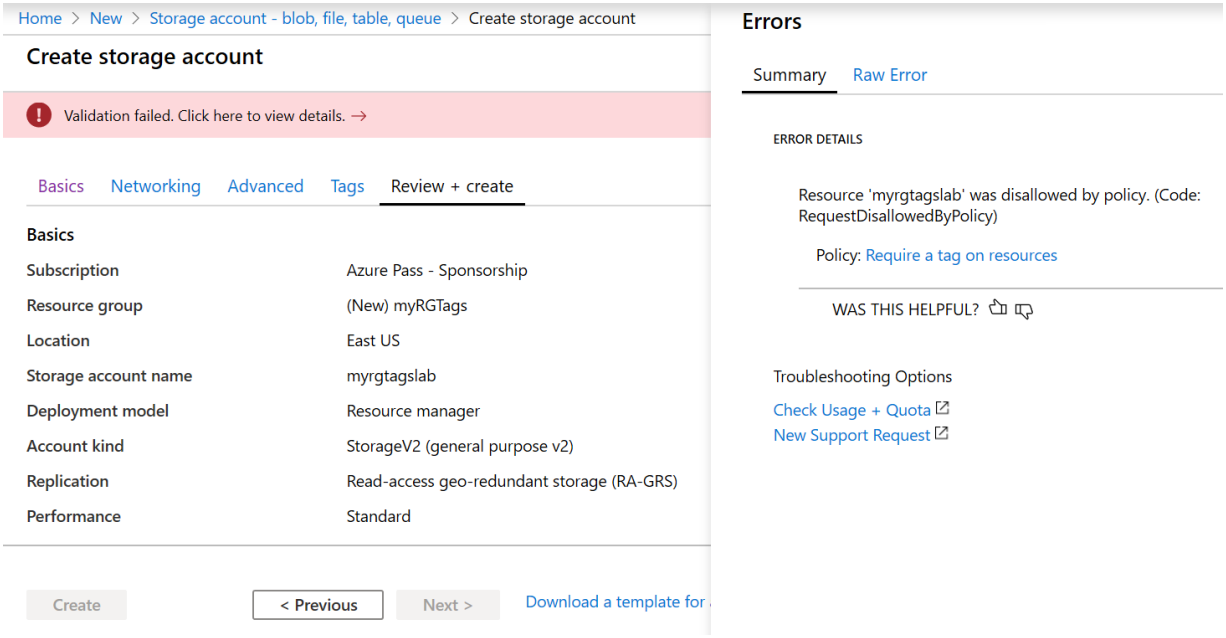
Setting	Value
Subscription	**Use your subscription**
Resource group	**myRGTags**
Storage account name	**storageaccountxxxx**
Location	**(US) East US**

3. Click **Review + create**.

   Note: We are testing to see what happens when the tag is not supplied.

4. You will receive a Validation failed message. Click the **Click here to view details** message. On the **Errors** blade, on the **Summary** tab note the error message stating that resource was disallowed by Policy.

   Note: If you view the Raw Error tab you will see the specific tag name that is required.



Note - you need to wait 30 minutes for tagging to be complete.

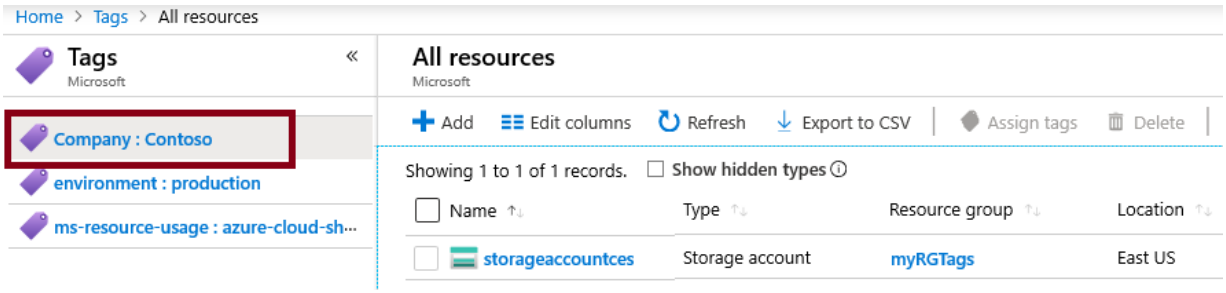
5. Close the **Error** pane and click **Previous** (bottom of the screen). Provide the tagging information.

Setting	Value
Tag name	**Company** (may not be in the drop-down list)
Tag value	**Contoso**

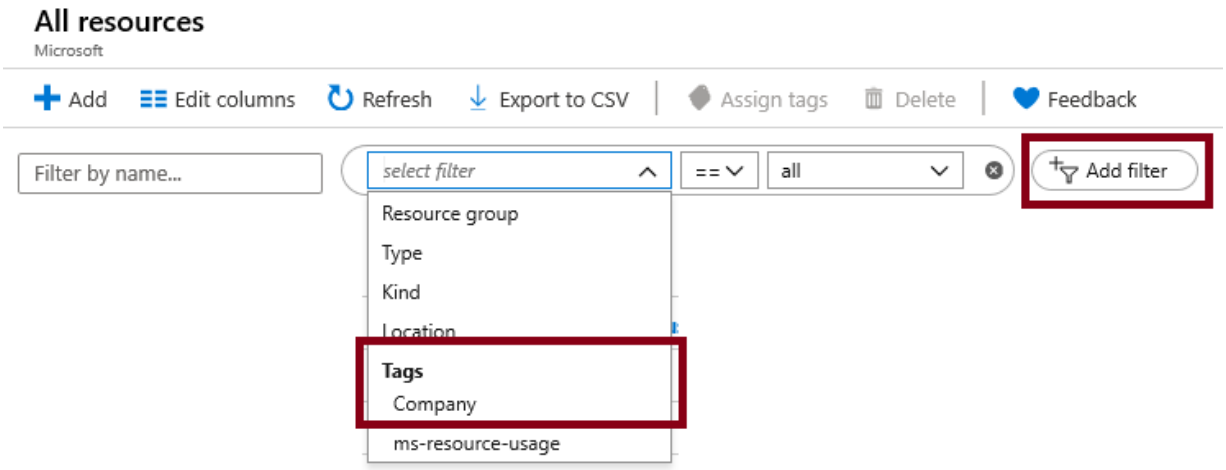
6. Click **Review + create** and verify that the validation was successful. Click **Create** to deploy the storage account.

63 Task 3: View all resources with a specific tag

1. In the Azure Portal, from the **All services** blade, search for and select **Tags**.
2. Note all tags and their values. Click the **Company : Contoso** key/value pair. This will display a blade showing the newly created storage account, as long as you included the tag during its deployment.



3. In the Portal, display the **All resources** blade.
4. Click **Add filter** and add the **Company** tag key as the filter category. With the filter applied, only your storage account will be listed.



64 Task 4: Delete the policy assignment

In this task, we will remove the **Require a tag on resources** policy so it does not affect our future work.

1. In the portal, from the **All services** blade, search for and select **Policy**.
2. Click the **Require a tag on resources** policy entry.
3. Click **Delete Assignment** in the top menu.
4. Confirm you wish to delete the policy assignment in the **Delete assignment** dialogue by clicking **Yes**
5. If you have time, create another resource without a tag to ensure the policy is no longer in effect.

In this walkthrough, we created a policy assignment that required tagging, created a storage account and tested the tagging, viewed resources with a specified tag, and removed the tagging policy.

64.1 Note: To avoid additional costs, you can remove this resource group. Search for resource groups, click your resource group, and then click Delete resource group. Verify the name of the resource group and then click Delete. Monitor the Notifications to see how the delete is proceeding.

64.2 wts: title: '17 - Create an Azure Policy (10 min)' module: 'Module 05: Describe identity, governance, privacy, and compliance features'

65 17 - Create an Azure Policy

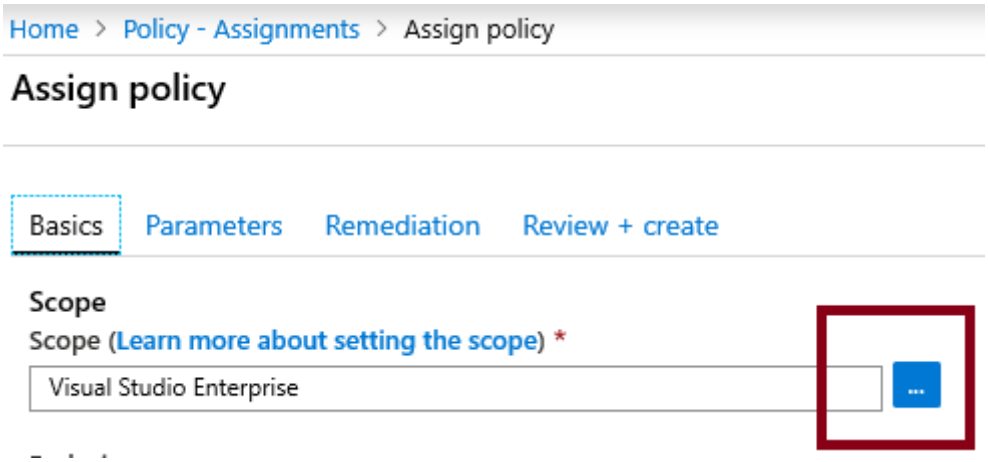
In this walkthrough, we will create an Azure Policy to restrict deployment of Azure resources to a specific location.

66 Task 1: Create a Policy assignment (10 min)

In this task, we will configure the allowed location policy and assign it to our subscription.

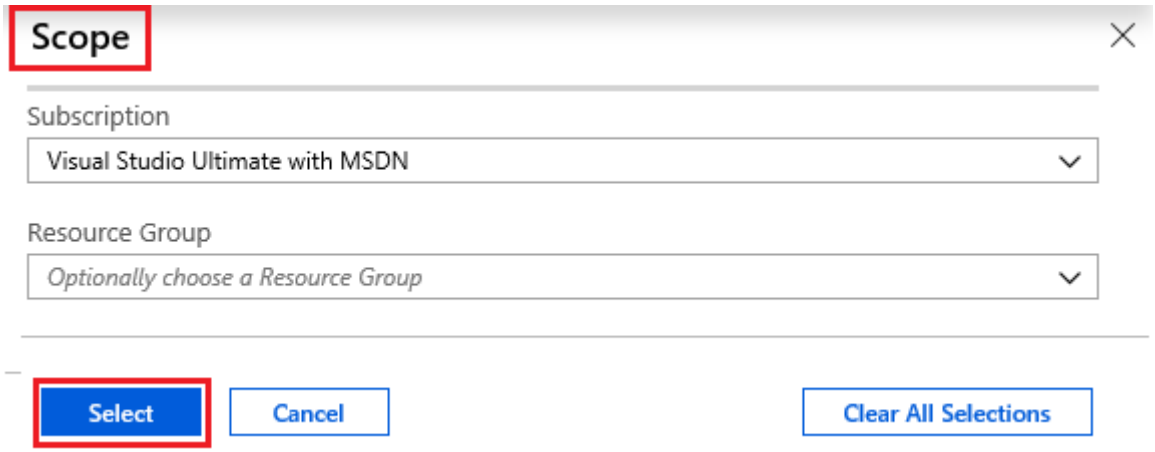
1. Sign in to the Azure portal.
2. From the **All services** blade, search for and select **Policy**, under the **Authoring** section click **Definitions**. Take a moment to review the list of built-in policy definitions. For example, in the **Category** drop-down select only **Compute**. Notice the **Allowed virtual machine SKUs** definition enables you to specify a set of virtual machine SKUs that your organization can deploy.
3. Return to the **Policy** page, under the **Authoring** section click **Assignments**. An assignment is a policy that has been assigned to take place within a specific scope. For example, a definition could be assigned to the subscription scope.
4. Click **Assign Policy** at the top of the **Policy - Assignments** page.

5. On the **Assign Policy** page, select the Scope selector by clicking the ellipsis.



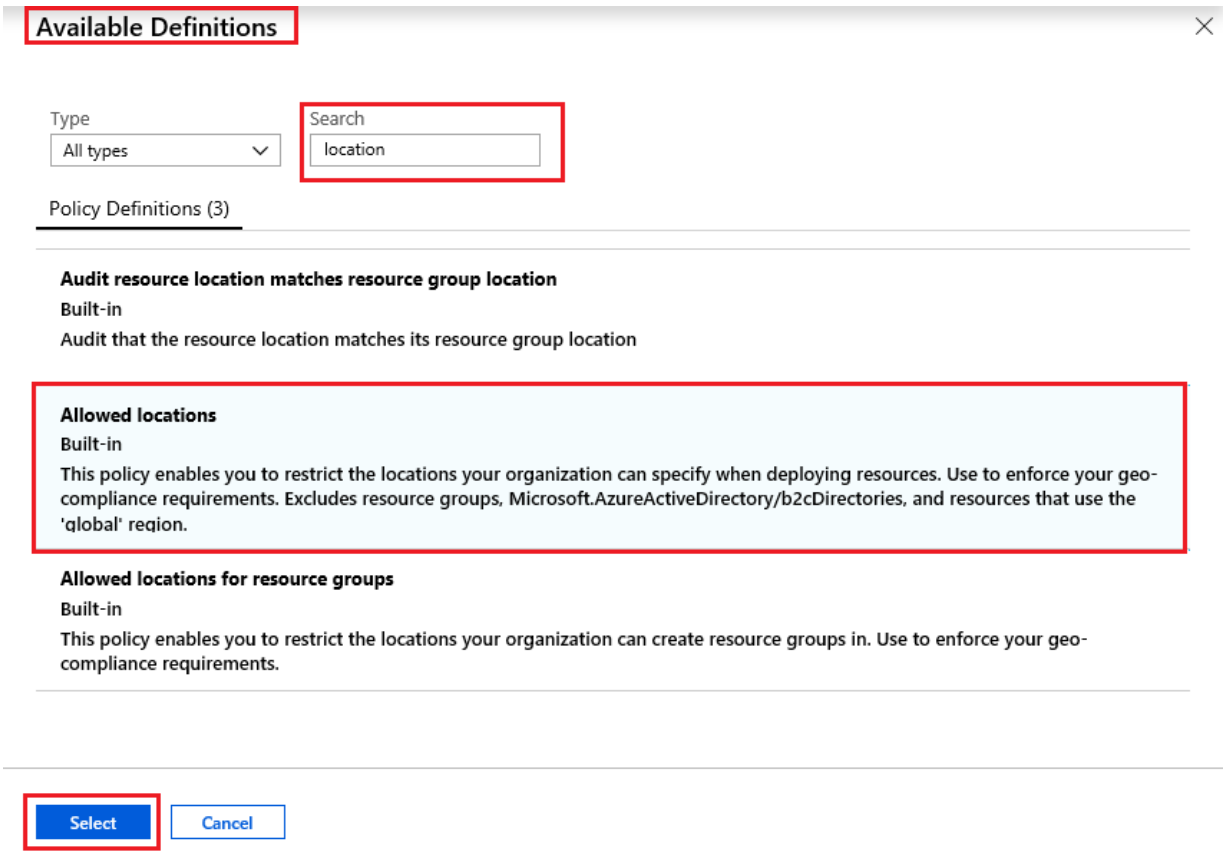
6. Ensure your subscription is selected. Your subscription name might be different. Notice you can optionally scope the policy to a resource group. Leave the defaults and click **Select**.

   Note: A scope determines what resources or grouping of resources the policy assignment applies to. In our case we could assign this policy to a specific resource group, however we chose to assign the policy at subscription level. Be aware that resources can be excluded based on the scope configuration. Exclusions are optional.

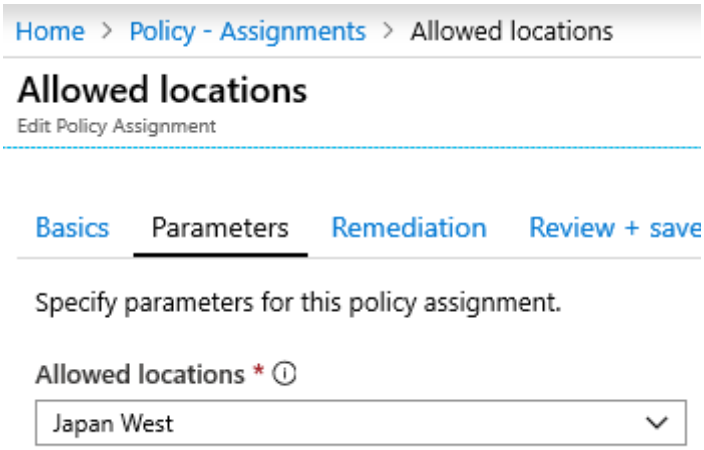


7. Select the **Policy definition** ellipsis button. In the **Search** box type **location** and click on the **Allowed locations** definition, then click **Select**.

   Note: This **Allowed Locations** policy definition will specify a location into which all resources must be deployed. If a different location is chosen, deployment will not be allowed. For more information view the Azure Policy Samples page.



8. In the **Assign policy** pane, switch to the **Parameters** tab, click on the arrow at the end of the **Allowed locations** box and from the subsequent list choose **Japan West**. Leave all other values as they are and click **Review + create**, and then **Create**.



9. The **Allowed locations** policy assignment is now listed on the **Policy - Assignments** pane and it is now in place, enforcing the policy at the scope level we specified (subscription level).

67 Task 2: Test Allowed location policy

In this task, we will test the Allowed location policy.

1. In the Azure Portal, from the **All services** blade, search for and select **Storage accounts**, and then click **+ Add, + Create, or + New**.
2. Configure the storage account (replace **xxxx** in the name of the storage account with letters and digits such that the name is globally unique). Leave the defaults for everything else.

Setting	Value
Subscription	**Use your subscription**
Resource group	**myRGPolicy** (create new)
Storage account name	**storageaccountxxxx**
Location	**(US) East US**

3. Click **Review + create** and then click **Create**.
4. You will receive the deployment failed error stating that resource was disallowed by policy, including the **Allowed locations** policy name.

68 Task 3: Delete the policy assignment

In this task, we will remove the Allowed location policy assignment and test.

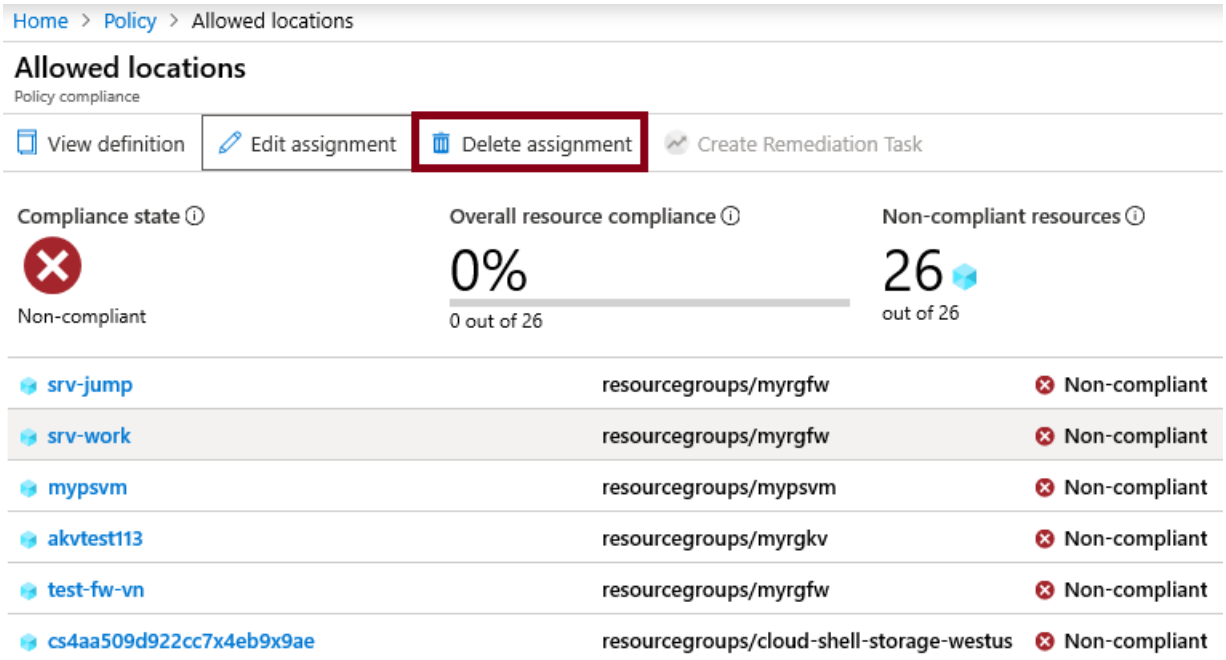
We will delete the policy assignment to ensure we are not blocked on any future work we wish to do.

1. From the **All services** blade, search for and select **Policy**, and then click your **Allowed locations** policy.

   Note: On the **Policy** blade, you can view the compliance state of the various policies you have assigned.

   Note: The Allowed location policy may show non-compliant resources. If so, these are resources created prior to the policy assignment.

2. Click **Delete Assignment** in the top menu.



3. Confirm you wish to delete the policy assignment in the **Delete assignment** dialogue by clicking **Yes**
4. Try to create another storage account to ensure the policy is no longer in effect.

   Note: Common scenarios where the **Allowed locations** policy can be useful include:

   - *Cost Tracking*: You could have different subscriptions for different regional locations. The policy will ensure that all resources are deployed in the intended region to help cost tracking.
   - *Data Residency and Security compliance*: You could also have data residency requirements, and create subscriptions per customer or specific workloads, and define that all resources must be deployed in a particular datacenter to ensure data and security compliance requirements.

Congratulations! You have created an Azure Policy to restrict deployment of Azure resources to a particular datacenter.

68.1 Note: To avoid additional costs, you can remove this resource group. Search for resource groups, click your resource group, and then click Delete resource group. Verify the name of the resource group and then click Delete. Monitor the Notifications to see how the delete is proceeding.

68.2 wts: title: '18 - Explore the Trust Center (5 min)' module: 'Module 05: Describe identity, governance, privacy, and compliance features'

69 18 - Explore the Trust Center

In this walkthrough, we will access the Trust Center, Service Trust Portal (STP), and Compliance Manager.

70 Task 1: Access the Trust Center (5 min)

1. In a browser, access the Microsoft Trust Center compliance offerings page.
2. Notice the offerings are grouped into **Global**, **US Government**, **Industry**, and **Regional**.
3. In the **Global** group, click **ISO 27001**.

   Note: The ISO 27001 Information Security Management Standards page is typical of the type of complaince information we provide.
4. Notice there is an overview of the standard; in-scope cloud services; audits, reports and certificates; assessments and reports; FAQs; resources; and white papers.
5. Browse through any content of interest to you.

   Note: Is there a compliance offering your organization is most interested in?

71 Task 2: Access the Service Trust Portal (STP)

1. In a browser, access the Service Trust Portal (STP)
2. Notice the **Audit** section. In this section are independent audit reports for different Microsoft's Cloud services.

   Note: At this time of this writing, **ISO 27001** related content is accessible via a clickable label. Click the label to open the page displaying ISO 27001 related content. If that is not available, choose another item.
3. It may take a couple of minutes for all the audits to load. You will need to login to your Microsoft account to view specific reports.
4. If you have time, review any other information that is of interest to you.

72 Task 3: Access the Compliance Manager

1. The Compliance Manager makes it easy to perform risk assessments of Microsoft's cloud services. Use Compliance Manager to manage your organization's compliance activities from implementation to reporting. If you want to try the Compliance Manager you will need to login.
2. Instead, visit the Compliance Guides page.
3. If you have time, review any other information that is of interest to you.

72.1 Congratulations! In this walkthrough, you accessed the Trust Center, Service Trust Portal (STP), and Compliance Manager.

72.2 wts: title: '19 - Use the Azure Pricing Calculator (10 min)' module: 'Module 06: Describe Azure cost management and service level agreements'

73 19 - Use the Pricing Calculator

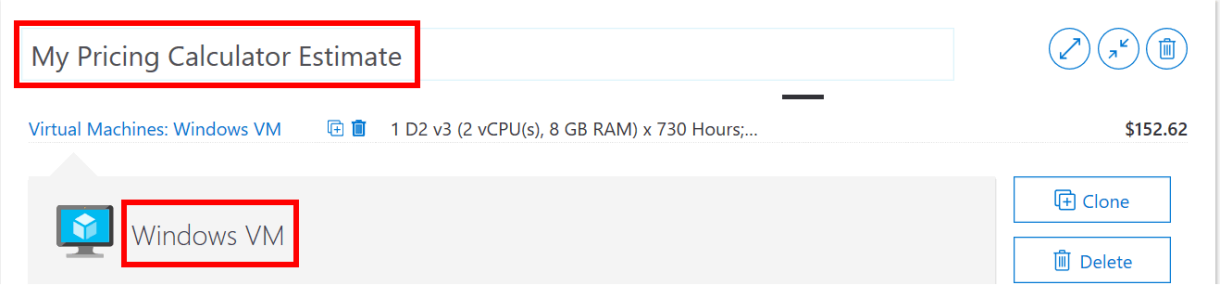
In this walkthrough, we will use the Azure Pricing Calculator to generate a cost estimate for an Azure virtual machine and related network resources.

74 Task 1: Configure the pricing calculator (10 min)

In this task, we will estimate cost of a sample infrastructure by using the Azure Pricing Calculator.

Note: To create an Azure Pricing Calculator estimate, this walkthrough provides example configurations for the VM and related resources. Use this example configurations or provide the Azure Pricing Calculator with details of your *actual* resource requirements instead.

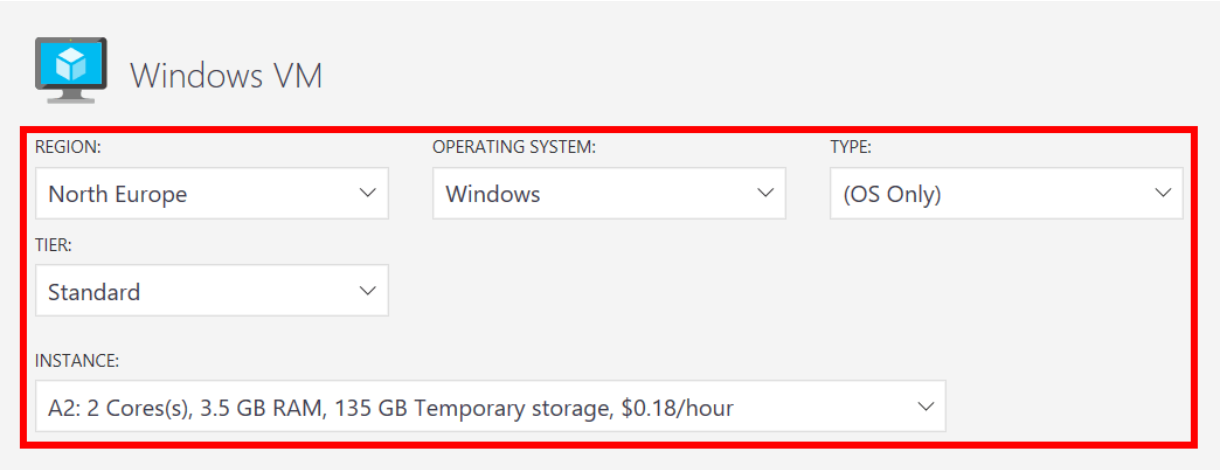
1. In a browser, navigate to the Azure Pricing Calculator webpage.
2. To add details of your VM configuration, click **Virtual Machines** on the **Products** tab. Scroll down to view the virtual machine details.
3. Replace **Your Estimate** and **Virtual Machines** text with more descriptive names for your Azure Pricing Calculator estimate and your VM configuration. This walkthrough example uses **My Pricing Calculator Estimate** for the estimate, and **Windows VM** for the VM configuration.



4. Modify the default VM configuration.

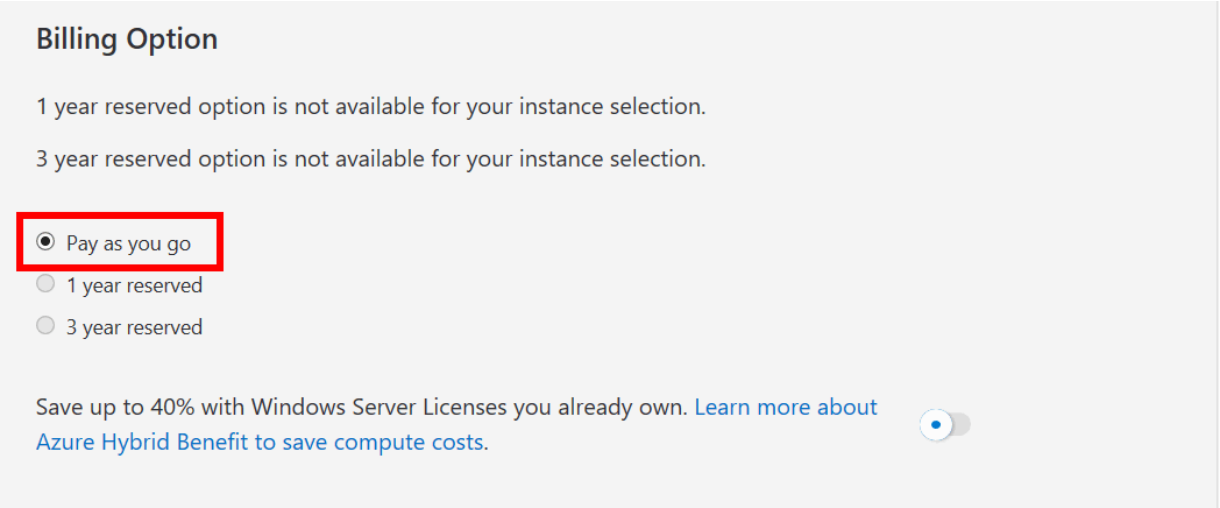
Region	Operating system	Type
North Europe	Windows	(OS only)

Tier	Instance
Standard	A2: 2 Core(s), 3.5 GB RAM, 135 GB Temporary storage



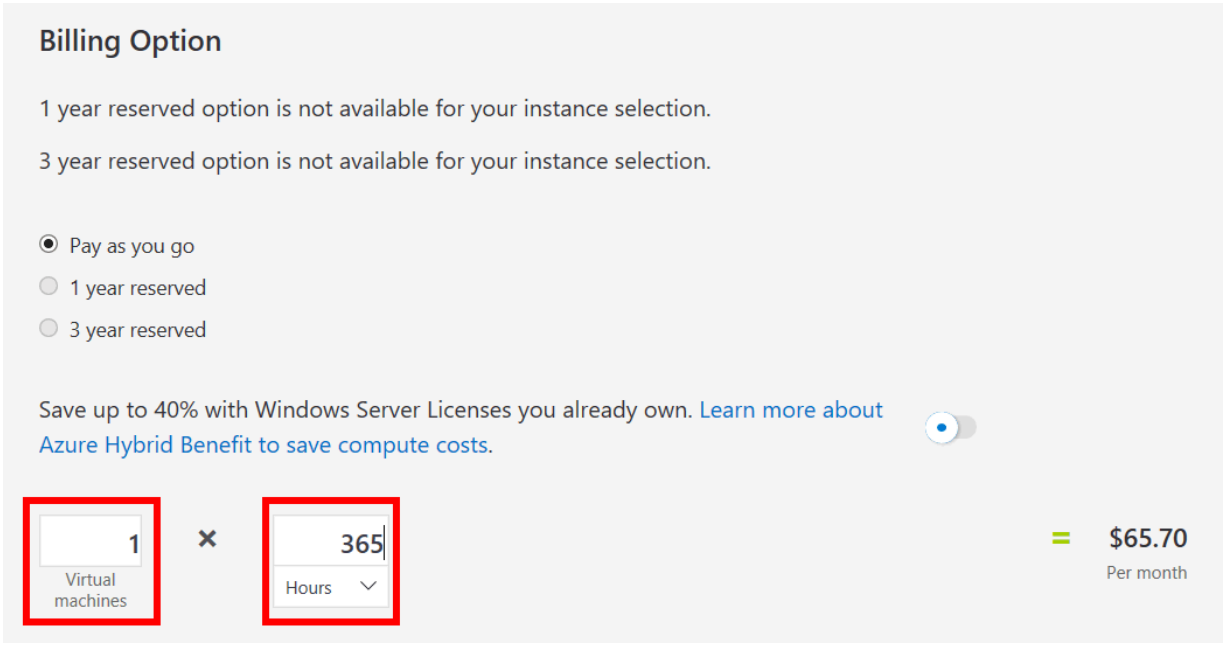
Note: The VM instance specifications and pricing may differ from those in this example. Follow this walkthrough by choosing an instance that matches the example as closely as possible. To view details about the different VM product options, choose **Product details** from the **More info** menu on the right.

5. Set the **Billing Option** to **Pay as you go**.



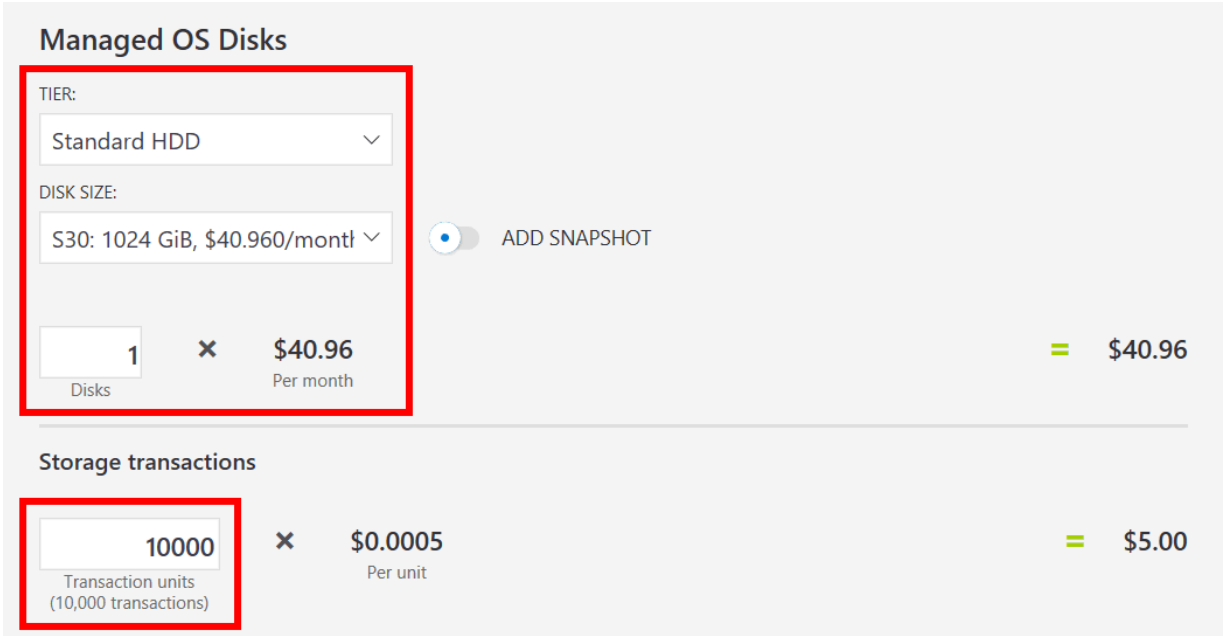
6. In Azure, a month is defined as 730 hours. If your VM needs to be available 100 percent of the time each month, you set the hours-per-month value to 730. This walkthrough example requires one VM to be available 50 percent of the time each month.

   Leave the number of VMs set at 1, and change the hours-per-month value to 365.

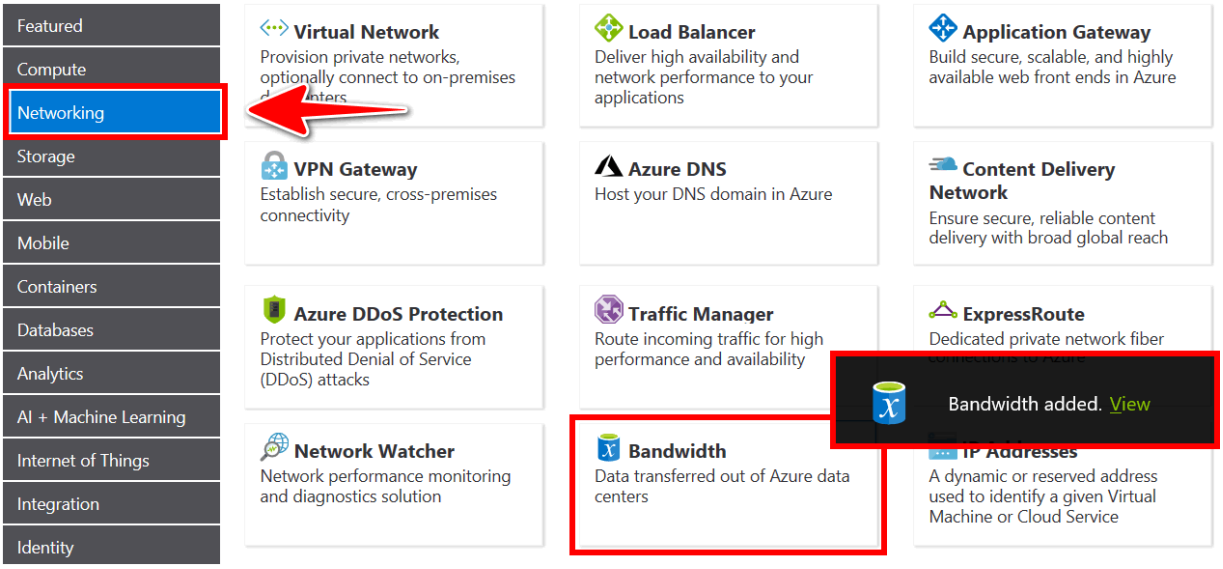


7. In the **Managed OS Disks** pane, modify the default VM storage configuration.

Tier	Disk size	Number of disks	Snapshot	Storage transactions
Standard HDD	S30: 1024 GiB	1	Off	10,000

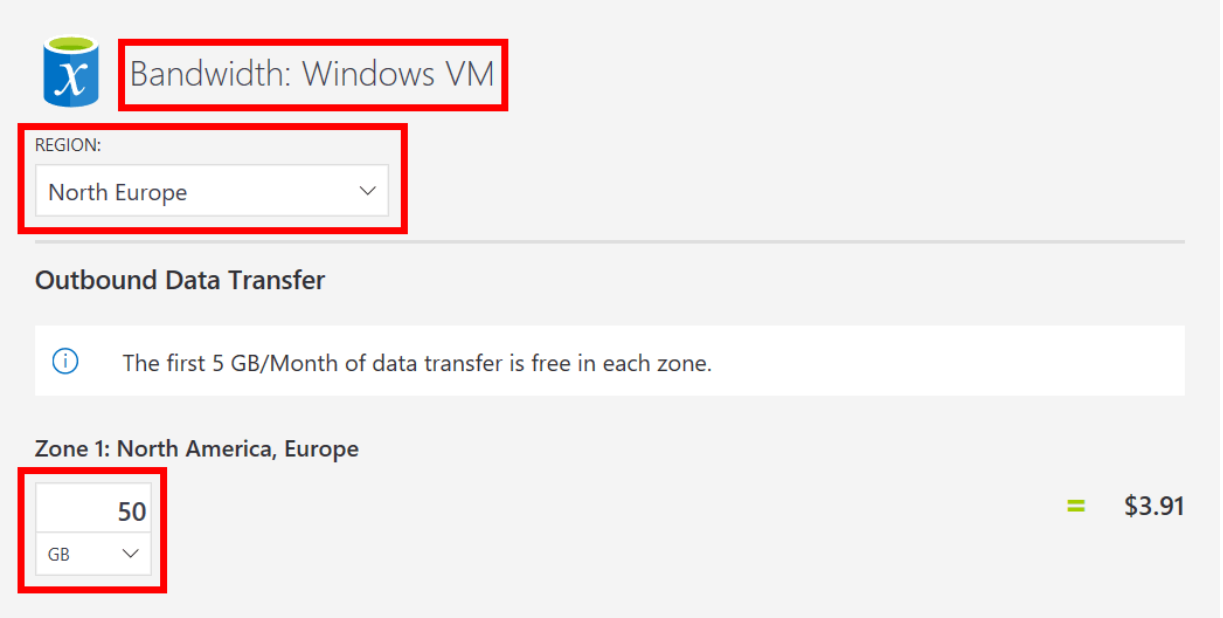


8. To add networking bandwidth to your estimate, go to the top of the Azure Pricing Calculator webpage. Click **Networking** in the product menu on the left, then click the **Bandwidth** tile. In the **Bandwidth added** message dialog, click **View**.

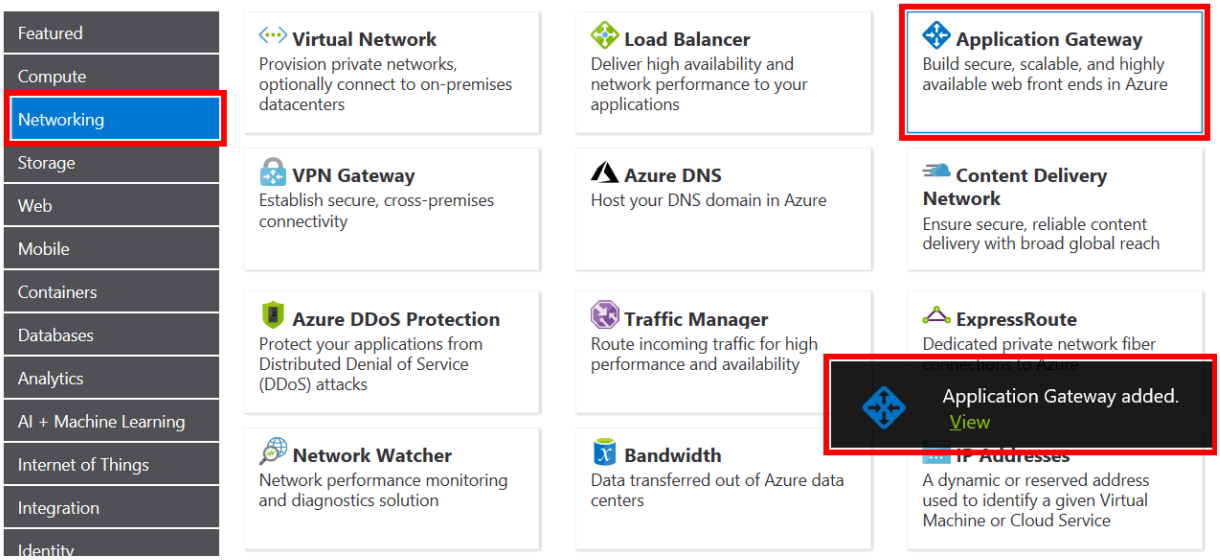


9. Add a name for your VM bandwidth configuration. This walkthrough example uses the name **Bandwidth: Windows VM**. Modify the default bandwidth configuration by adding the following details.

Region	Zone 1 Outbound Data Transfer Amount
North Europe	50 GB



10. To add an Application Gateway, return to the top of the Azure Pricing Calculator webpage. In the **Networking** product menu, click the **Application Gateway** tile. In the **Application Gateway** message dialog, click **View**.



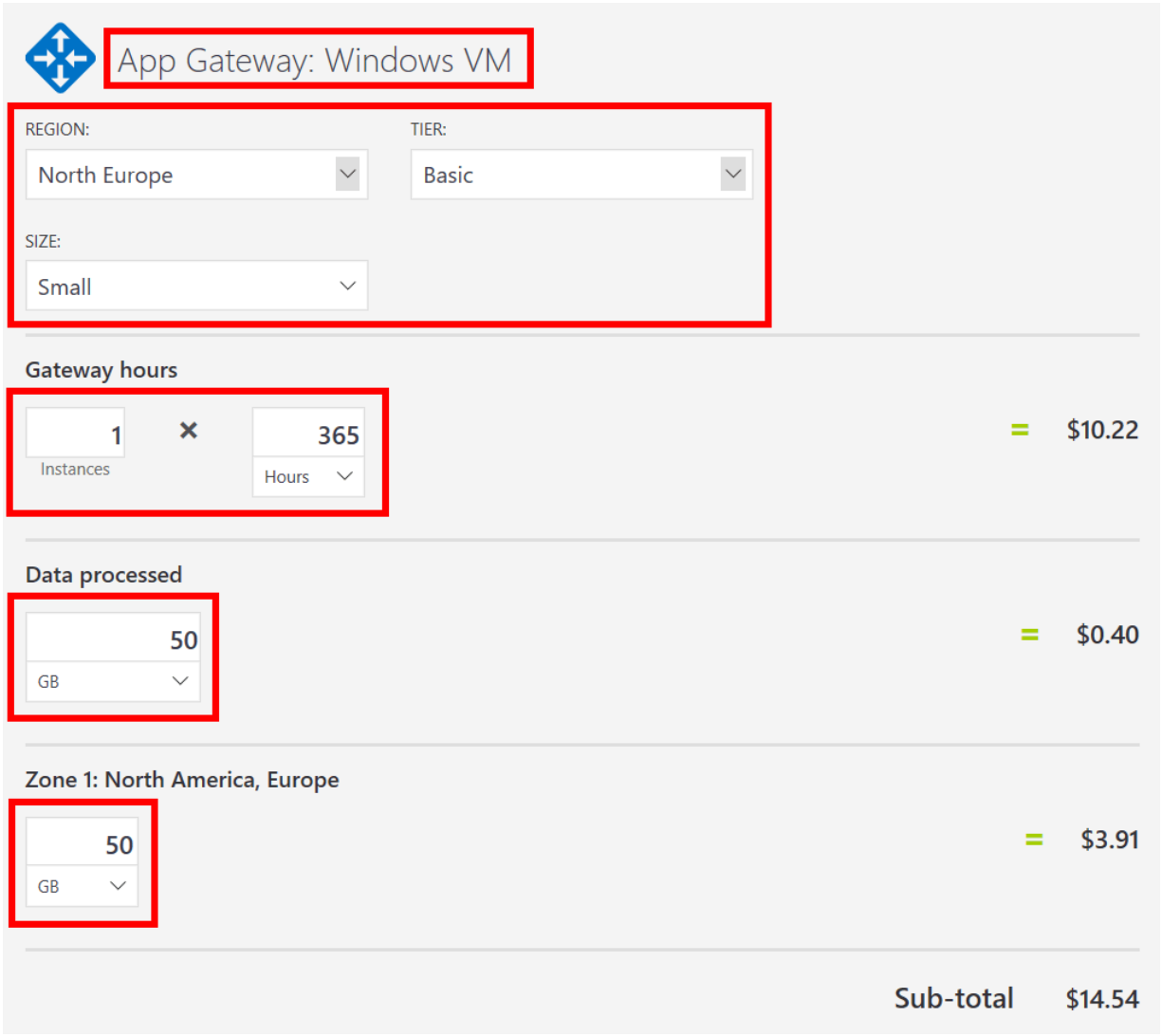
11. Add a name for your Application Gateway configuration. This walkthrough uses the name **App Gateway: Windows VM**. Modify the default Application Gateway configuration by adding the following details.

Region	Tier	Size
North Europe	Basic	Small

Instances	Hours
1	365

Data processed
50 GB

Zone 1: North America, Europe
50 GB



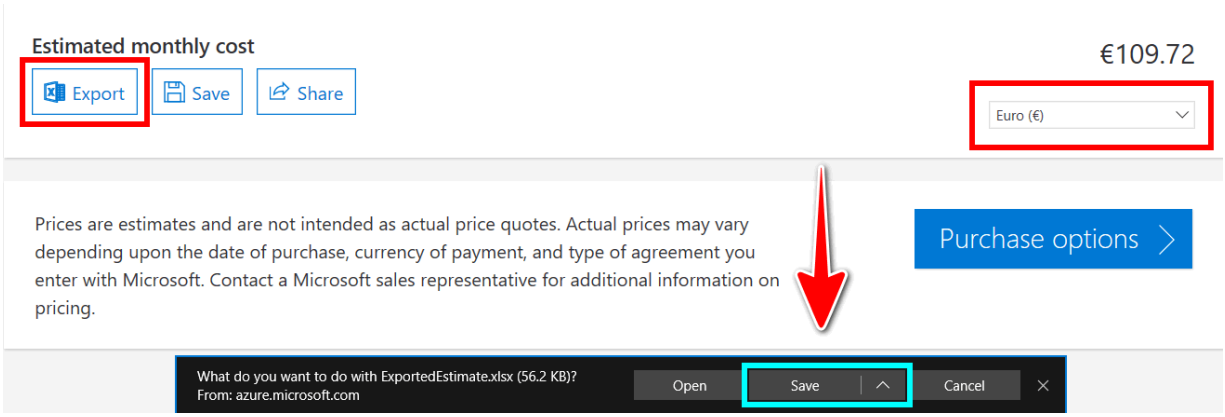
75 Task 2: Review the pricing estimate

In this task, we will review the results of the Azure Pricing Calculator.

1. Scroll to the bottom of the Azure Pricing Calculator webpage to view total **Estimated monthly cost**.

   Note: Explore the various options available within the Azure Pricing Calculator. For example, this walkthrough requires you to update the currency to Euro.

2. Change the currency to Euro, then select **Export** to download a copy of the estimate for offline viewing in Microsoft Excel (`.xlsx`) format.



Microsoft Azure Estimate

My Pricing Calculator Estimate

Service type	Custom name	Region	Description	Estimated Cost
Virtual Machines	Windows VM	North Europe	1 A2 (2 vCPU(s), 3.5 GB RAM) x 365 Hours; Windows – (OS Only); P	€94.16
Bandwidth	Bandwidth: Windows VM	North Europe	Zone 1: North America, Europe, 50 GB	€3.30
Application Gateway	App Gateway: Windows VM	North Europe	Basic tier, Small Instance size: 1 Gateway hours instance(s) x 365 H	€12.26
Support			Support	€0.00
			Licensing Program	Microsoft Online S
			Monthly Total	€109.72
			Annual Total	€1,316.66

Disclaimer

All prices shown are in Euro (€). This is a summary estimate, not a quote. For up to date pricing information please visit
This estimate was created at 3/30/2019 10:01:38 PM UTC.

75.1 Congratulations! You downloaded an estimate from the Azure Pricing Calculator.

75.2 wts: title: '20 - Use the Azure TCO Calculator (10 min)' module: 'Module 06: Describe Azure cost management and service level agreements'

76 20 - Use the Azure TCO Calculator

In this walkthrough, you will use the Total Cost of Ownership (TCO) Calculator to generate cost comparison report for an on-premises environment.

Note: This walkthrough provides example definitions of on-premises infrastructure and workloads for a typical datacenter. To create a TCO Calculator report, use the example definitions or provide details of your *actual* on-premises infrastructure and workloads.

77 Task 1: Configure the TCO calculator (10 min)

In this task, we will add infrastructure information to the calculator.

1. In a browser, navigate to the Total Cost of Ownership (TCO) Calculator page.
2. To add details of your on-premises server infrastructure, click + **Add server workload** in the **Define your workloads** pane.

Settings	Value
Name	**Servers: Windows VMs**
Workload	**Windows/Linux server**
Environment	**Virtual Machines**
Operating system	**Windows**
VMs	**50**
Virtualization	**Hyper-V**
Core(s)	**8**
RAM (GB)	**16**
Optimize by	**CPU**
Windows Server 2008/2008 R2	**Off**

3. Select + **Add server workload** to make a row for a new server workloads definition.

Settings	Value
Name	**Servers: Linux VMs**
Workload	**Windows/Linux server**
Environment	**Virtual Machines**
Operating system	**Linux**
VMs	**50**
Virtualization	**VMware**

Settings	Value
Core(s)	**8**
RAM (GB)	**16**
Optimize by	**CPU**
Windows Server 2008/2008 R2	**Off**

4. In the **Storage** pane, click **Add storage**.

Settings	Value
Name	**Server Storage**
Storage type	**Local Disk/SAN**
Disk type	**HDD**
Capacity	**60 TB**
Backup	**120 TB**
Archive	**0 TB**

5. In the **Networking** pane, add bandwidth.

Settings	Value
Outbound bandwidth	15 TB

6. Click **Next**.
7. Explore the options and make any adjustments that you require.

Settings	Value
Currency	**Euro**

8. Click **Next**.

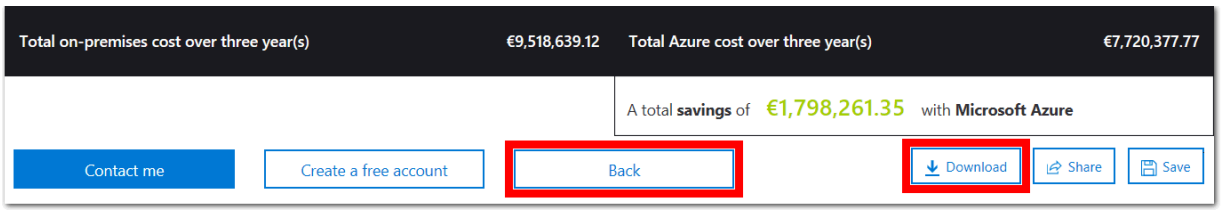
78 Task 2: Review the results and save a copy

In this task, we will review cost saving recommendations and download a report.

1. Review the Azure cost saving recommendations and visualizations.

Settings	Value
Timeframe	**3 years**
Region	**North Europe**

2. To modify the information you provided, go to the bottom of the page, and click **Back**.
3. To save or print a PDF copy of the report, click **Download**.



78.1 Congratulations! You have used the TCO Calculator to generate a cost comparison report for an on-premises environment.

78.2 wts: title: '21 - Calculate Composite SLAs (5 min)' module: 'Module 06: Describe Azure cost management and service level agreements'

79 21 - Calculate Composite SLAs

In this walkthrough, we will determine availability SLA of Azure services and then calculate application composite SLA-based expected availability.

Our example application consists of these Azure services. We will not go in to deep architectural configuration and considerations, the intention here is to give an high level example.

- **App service**: To host the application.
- **Azure AD B2C**: To authenticate user logins and manage profiles.
- **Application Gateway**: To manage application access, and scaling.
- **Azure SQL Database**: To store application data.

80 Task 1: Determine the SLA uptime percentage values for our application (5 min)

1. In a browser, go to the SLA summary for Azure services page.
2. Locate the **App Service** SLA uptime value, **99.95%**. Click **View full details**, and then expand **SLA details**. Notice the **Monthly uptime percentages** and **Service Credits**.
3. Return to the SLA webpage and locate the **Azure Active Directory B2C** service and determine the SLA uptime value, **99.9%**.
4. Locate the **Application Gateway** SLA uptime value, **99.95%**.
5. The Azure SQL database uses Premium tiers but is not configured for Zone Redundant Deployments. Locate the **Azure SQL Database** SLA uptime value, **99.99%**.

   Note: There are different uptime values for different configurations and deployments of Azure SQL Database. It is important you are clear on your required uptime values, when planning and costing your deployment and configuration. Small changes in uptime can have impact on service costs as well as potentially increase complexity in configuration. Some other services that may be of interest on the Azure SLA summary web page would include **Virtual Machines**, **Storage Accounts** and **Cosmos DB**.

81 Task 2: Calculate the Application Composite SLA percentage uptime

1. If any of the services that comprises our application are not available our application will not be available for users to sign in to and use. As such the total uptime for our application consists of the following:

   App Service % uptime X **Azure AD B2C % uptime** X **Azure Application Gateway % uptime** X **Azure SQL Database % uptime** = **Total % Uptime**

   which in percentage term is as follows:

   99.95% X **99.9%** X **99.95%** X **99.99%** = **99.79%**

   This is the SLA-based expected availability of our application with the current services and architecture.

81.1 Congratulations! You have determined the SLA-based uptime for each of the services in our sample application and then calculated the composite SLA-based expected availability for the application.

81.2 wts: title: '22 - Open a Support Request (5 min)' module: 'Not currently utilized in current exam'

82 22 - Open a Support Request

In this walkthrough, we will view available support plan options and then practice creating and monitoring a new support request.

83 Task 1: View available support plan options and a technical support request (5 min)

1. Sign in to the **Azure portal**.
2. From the **All services** blade, search for and select **Help + support**, then select **Support plans**.
3. Take a few minutes to review the different support plans. Notice what is included in the **Basic** plan.
4. Click **+ New support request**. The ticket is created based on the values you specify.

Setting	Value
Issue Type	**Technical**
Subscription	**Choose your subscription**
Service	**All services**, **Virtual Machine running Linux**
Summary	**Disk access is very slow for large files**
Problem type	**VM performance**
Problem subtype	**Disk throughput is lower than expected**

5. Click **Next: Solutions >>** and read through the recommended solutions.
6. Click **Next: Details >>**. When submitting an actual support request, you would provide as much information as possible to allow for a speedy resolution of the issue. Your contact choices on this page depend on your support plan.

   Note: We will stop at this point. Do you understand how to submit a technical request?

84 Task 2: Create a billing support request

1. Return to the **New support request** section and the **Basics** tab.

Setting	Value
Issue Type	**Billing**
Subscription	**Choose your subscription**
Summary	**Monthly charge is not correct**
Problem type	**Pricing**
Problem subtype	**Help me discover the service prices**

2. Click **Next: Solutions** and read through the recommended solutions.
3. Click **Next: Details**. When submitting a real support request you would provide as much information as possible to allow for a speedy resolution of the issue.

   Note: We will stop at this point. Do you understand how to submit a support request?
4. Click **All support requests**. This is where your support requests are shown. An email is also sent to

your email address containing details of the support request.

Congratulations! You have viewed the available support plan options and practiced creating and monitoring a new support request.

Note: Click for more information about **creating an Azure support ticket**.