< Previous Unit 9 of 14 ˅ Next >

✓ 100 XP

Exercise - Configure network access

10 minutes

This module requires a sandbox to complete. A **sandbox** gives you access to free resources. Your personal subscription will not be charged. The sandbox may only be used to complete training on Microsoft Learn. Use for any other reason is prohibited, and may result in permanent loss of access to the sandbox.

Microsoft provides this lab experience and related content for educational purposes. All presented information is owned by Microsoft and intended solely for learning about the covered products and services in this Microsoft Learn module.

Sign in to activate sandbox

In this exercise, you'll configure the access to the virtual machine (VM) you created earlier in this module. The Microsoft Learn sandbox should still be running. If the sandbox timed out, you'll need to redo the previous exercise (**Exercise - Create an Azure virtual machine**).

Right now, the VM you created and installed Nginx on isn't accessible from the internet. You'll create a network security group that changes that by allowing inbound HTTP access on port 80.

Task 1: Access your web server

In this procedure, you get the IP address for your VM and attempt to access your web server's home page.

1. Run the following `az vm list-ip-addresses` command to get your VM's IP address and store the result as a Bash variable:

   Azure CLI

   ```
   IPADDRESS="$(az vm list-ip-addresses \
     --resource-group [sandbox resource group name] \
     --name my-vm \
     --query "[].virtualMachine.network.publicIpAddresses[*].ipAddress" \
   ```

```
  --output tsv)"
```

2. Run the following `curl` command to download the home page:

   Bash

   ```
   curl --connect-timeout 5 http://$IPADDRESS
   ```

   The `--connect-timeout` argument specifies to allow up to five seconds for the connection to occur. After five seconds, you see an error message that states that the connection timed out:

   Output

   ```
   curl: (28) Connection timed out after 5001 milliseconds
   ```

   This message means that the VM was not accessible within the timeout period.

3. As an optional step, try to access the web server from a browser:

   a. Run the following to print your VM's IP address to the console:

   Bash

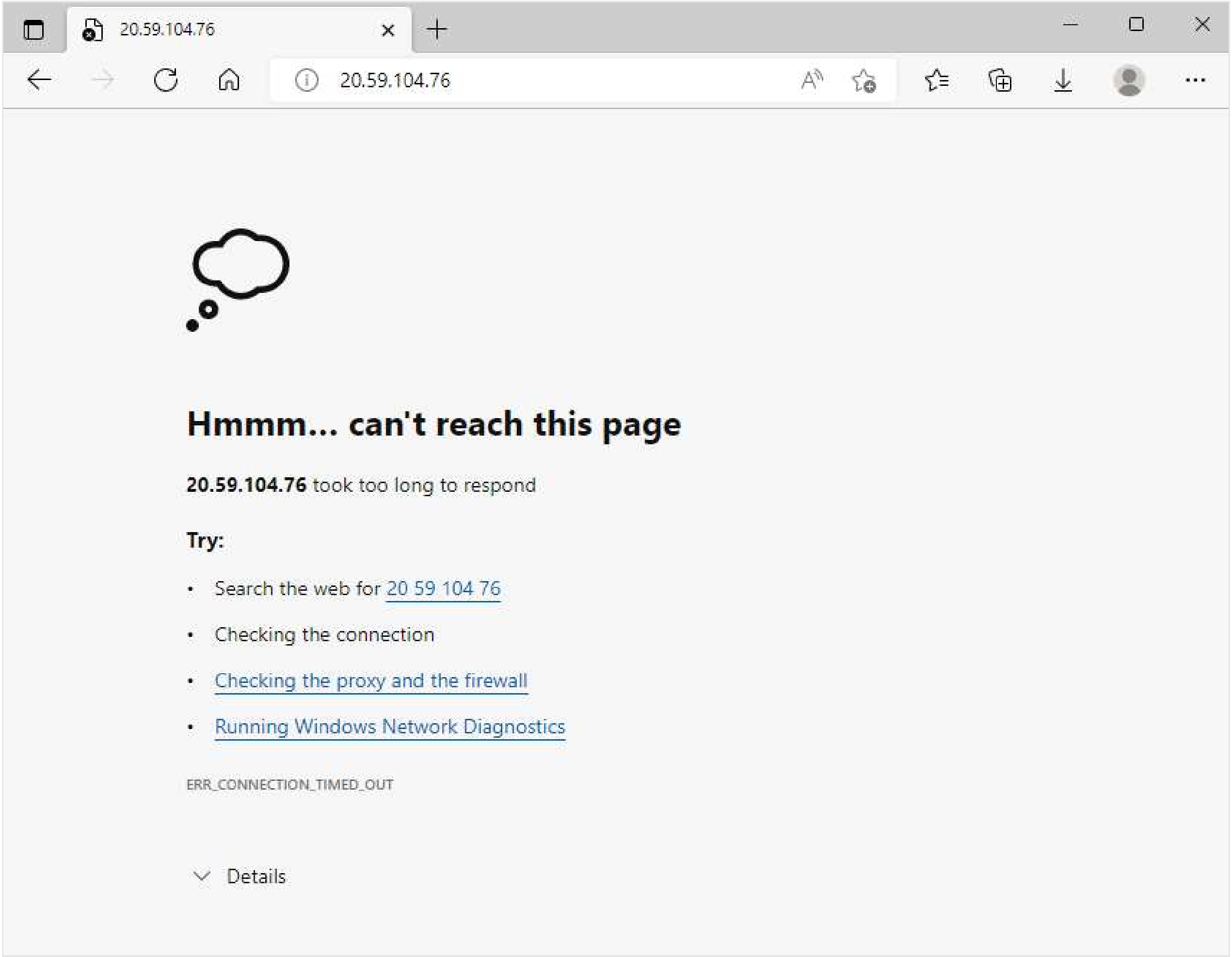
   ```
   echo $IPADDRESS
   ```

   You see an IP address, for example, *23.102.42.235*.

   b. Copy the IP address that you see to the clipboard.

   c. Open a new browser tab and go to your web server. After a few moments, you see that the connection isn't happening.

   If you wait for the browser to time out, you'll see something like this:



Hmmm... can't reach this page

20.59.104.76 took too long to respond

Try:

- Search the web for 20 59 104 76
- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT

Details

d. Keep this browser tab open for later.

Task 2: List the current network security group rules

Your web server wasn't accessible. To find out why, let's examine your current NSG rules.

1. Run the following `az network nsg list` command to list the network security groups that are associated with your VM:

Azure CLI

```
az network nsg list \
  --resource-group [sandbox resource group name] \
  --query '[].name' \
  --output tsv
```

You see this:

Output

```
my-vmNSG
```

Every VM on Azure is associated with at least one network security group. In this case, Azure created an NSG for you called *my-vmNSG*.

2. Run the following `az network nsg rule list` command to list the rules associated with the NSG named *my-vmNSG*:

Azure CLI

```
az network nsg rule list \
  --resource-group [sandbox resource group name] \
  --nsg-name my-vmNSG
```

You see a large block of text in JSON format in the output. In the next step, you'll run a similar command that makes this output easier to read.

3. Run the `az network nsg rule list` command a second time. This time, use the `--query` argument to retrieve only the name, priority, affected ports, and access (**Allow** or **Deny**) for each rule. The `--output` argument formats the output as a table so that it's easy to read.

Azure CLI

```
az network nsg rule list \
  --resource-group [sandbox resource group name] \
  --nsg-name my-vmNSG \
  --query '[].{Name:name, Priority:priority, Port:destinationPortRange, 
Access:access}' \
  --output table
```

You see this:

Output

```
Name                 Priority    Port    Access
-----------------  ----------  ------  --------
```

```
default-allow-ssh  1000        22      Allow
```

You see the default rule, *default-allow-ssh*. This rule allows inbound connections over port 22 (SSH). SSH (Secure Shell) is a protocol that's used on Linux to allow administrators to access the system remotely. The priority of this rule is 1000. Rules are processed in priority order, with lower numbers processed before higher numbers.

By default, a Linux VM's NSG allows network access only on port 22. This enables administrators to access the system. You need to also allow inbound connections on port 80, which allows access over HTTP.

Task 3: Create the network security rule

Here, you create a network security rule that allows inbound access on port 80 (HTTP).

1. Run the following `az network nsg rule create` command to create a rule called *allow-http* that allows inbound access on port 80:

   Azure CLI

   ```
   az network nsg rule create \
     --resource-group [sandbox resource group name] \
     --nsg-name my-vmNSG \
     --name allow-http \
     --protocol tcp \
     --priority 100 \
     --destination-port-range 80 \
     --access Allow
   ```

   For learning purposes, here you set the priority to 100. In this case, the priority doesn't matter. You would need to consider the priority if you had overlapping port ranges.

2. To verify the configuration, run `az network nsg rule list` to see the updated list of rules:

   Azure CLI

   ```
   az network nsg rule list \
     --resource-group [sandbox resource group name] \
     --nsg-name my-vmNSG \
     --query '[].{Name:name, Priority:priority, Port:destinationPortRange, 
   Access:access}' \
   ```

```
    --output table
```

You see this both the *default-allow-ssh* rule and your new rule, *allow-http*:

Output

```
Name              Priority    Port    Access
-----------------  ----------  ------  --------
default-allow-ssh  1000        22      Allow
allow-http        100        80      Allow
```

Task 4: Access your web server again

Now that you've configured network access to port 80, let's try to access the web server a second time.

> ⓘ **Note**
>
> After you update the NSG, it may take a few moments before the updated rules propagate. Retry the next step, with pauses between attempts, until you get the desired results.

1. Run the same `curl` command that you ran earlier:

   Bash

   ```
   curl --connect-timeout 5 http://$IPADDRESS
   ```

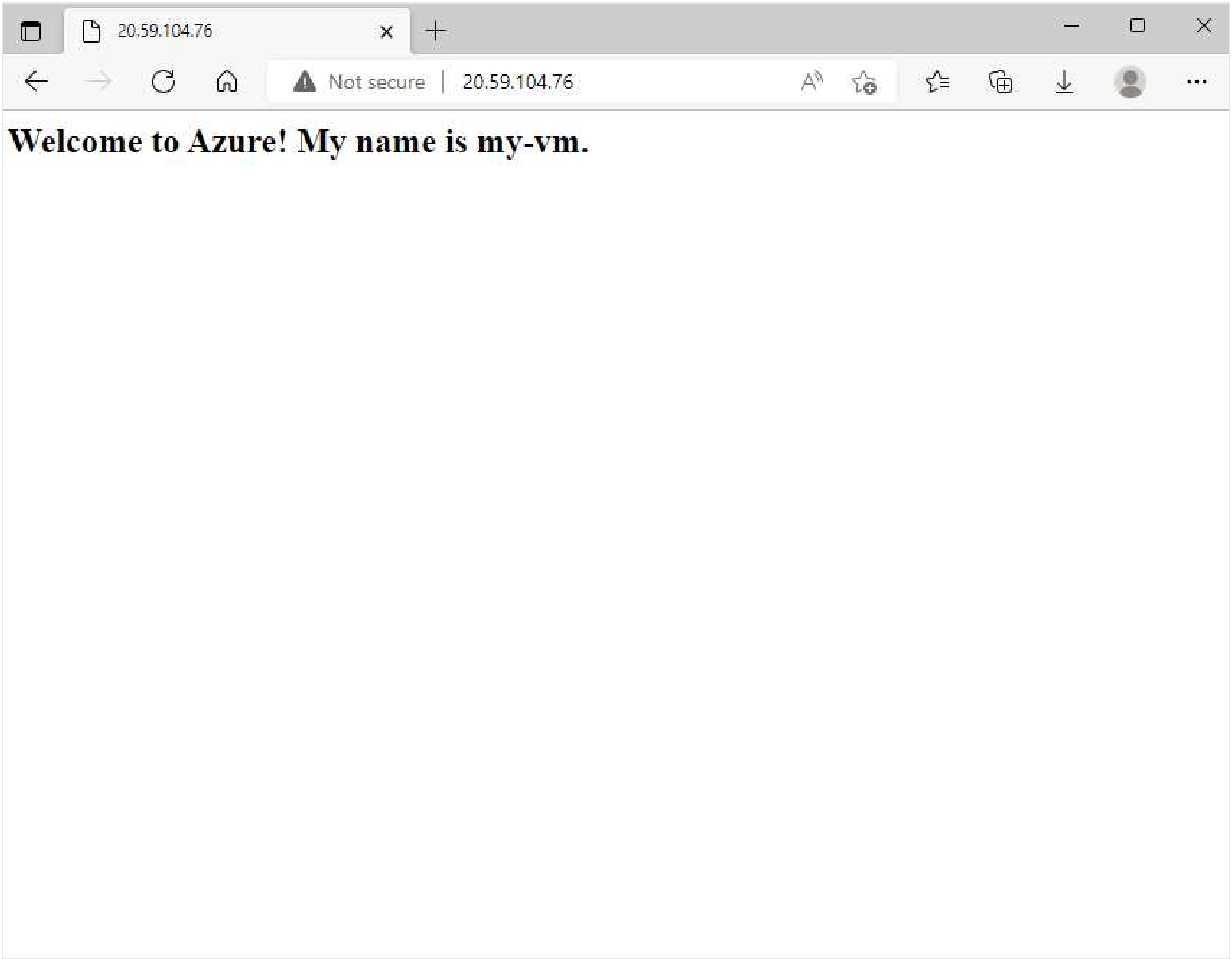
   You see this:

   HTML

   ```
   <html><body><h2>Welcome to Azure! My name is my-vm.</h2></body></html>
   ```

2. As an optional step, refresh your browser tab that points to your web server.

   You see this:



Welcome to Azure! My name is my-vm.

Nice work. In practice, you can create a standalone network security group that includes the inbound and outbound network access rules you need. If you have multiple VMs that serve the same purpose, you can assign that NSG to each VM at the time you create it. This technique enables you to control network access to multiple VMs under a single, central set of rules.

Clean up

The sandbox automatically cleans up your resources when you're finished with this module.

When you're working in your own subscription, it's a good idea at the end of a project to identify whether you still need the resources you created. Resources that you leave running can cost you money. You can delete resources individually or delete the resource group to delete the entire set of resources.

Next unit: Describe Azure Virtual Private Networks

Continue >

English (United States)   ☼ Theme ∨

Previous Versions   Blog   Contribute   Privacy   Terms of Use   Trademarks

Azure Cloud Shell

This module requires a sandbox to complete.

A sandbox gives you access to Azure resources. Your Azure subscription will not be charged. The sandbox may only be used to complete training on Microsoft Learn. Use for any other reason is prohibited, and may result in permanent loss of access to the sandbox.

Microsoft provides this lab experience and related content for educational purposes. All presented information is owned by Microsoft and intended solely for learning about the covered products and services in this Microsoft Learn module.