1. Objective – Evaluate effective security rules

1. Select **Home > Resource groups**, then choose your resource group, such as *oreilly-az104*
2. Choose your network security group from the previous labs, such as *nsg-frontend-westus*
3. Under **Support + troubleshooting** from the menu on the left-hand side, select **Effective security rules**.
4. Make sure that your Windows VM, such as *winvm01*, and the default network interface, such as *winvm01492*, are selected. It takes a few moments to validate what security rules apply across the connected subnets and network interfaces.

   As this VM was associated with the *nsg-frontend-westus* network security group, the inbound rule to allow TCP port 80 is applied from a previous exercise. These effective security rules are a good way to validate what rules are applied to a VM when the subnet, network interface, or network security group association can provide the configuration.

2. Objective – Implement Network Security Groups

1. Select **Home > Resource groups**, then choose your resource group, such as *oreilly-az104*
2. Choose your Windows VM from the previous labs, such as *winvm*
3. Under **Operations** from the menu on the left-hand side, select **Run command**, then choose **RunPowerShellScript**
4. Install the IIS web server components using the following PowerShell command:

   ```
   Add-WindowsFeature Web-Server
   ```

5. Select **Run**, and wait for the output to confirm that the Windows feature was successfully installed. It takes a minute or two for the script to execute and feedback to be presented. It looks like just a black screen without much user feedback.
6. From the **Overview** page, copy and paste the *Public IP address* into a new web browser tab or window. The default IIS web page should load. This shows the network security group correctly allows traffic to the VM.

3. Objective – Implement Azure load balancer

1. Select **Home > Resource groups**, then choose your resource group, such as *oreilly-az104*
2. Choose your load balancer from the previous labs, such as *loadbalancer-westus*
3. Select **Backend pools** from the menu on the left-hand side, then **+ Add** a new pool. Enter the following configuration information. If not noted below, use the defaults:

   Name: *webservers*

   Virtual network: *vnet-westus*

   Associated to: *Virtual machine*

   Select your VM, such as winvm01

   Choose the VMs IP address, such as 10.10.1.4

4. Select **Add** and wait a few moments for the backend pool to be created and the selected VMs to be connected to the load balancer.
5. Select **Load balancing rules** from the menu on the left-hand side, then **+ Add.** Enter the following configuration information. If not noted below, use the defaults:

   Name: *http_rule*

   Note that the default settings are for TCP port 80 for common HTTP traffic.

   The backend pool and health probe created in previous steps are automatically used.

   You can configure session persistence, idle timeout, and floating IP as needed.

6. Select **OK** and wait a few moments for the rule to be created. Select the load balancer **Overview** page, then copy and paste the *Public IP address* into a new browser tab or window. The default IIS web page should load from the VM.

   This is a basic example with only one VM connected to the backend pool, but it shows that traffic correctly flows through the load balancer.