

Configure an Application Security Group

Understand the scenario

You are an Azure administrator. You need to create an Azure virtual machine that uses an application security group. First, you will create a virtual network. Next, you will create an application security group, and then you will create a network security group. Finally, you will create an Azure virtual machine to be used as a web server, and then you will test the security configuration.

Understand your environment

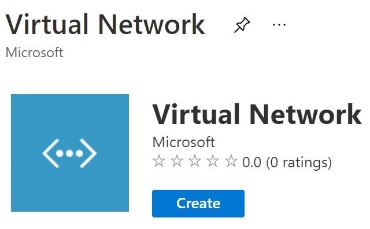
You will be using an Azure resource group named corp-datalod26433645 that contains no resources.

# **Create a virtual network**

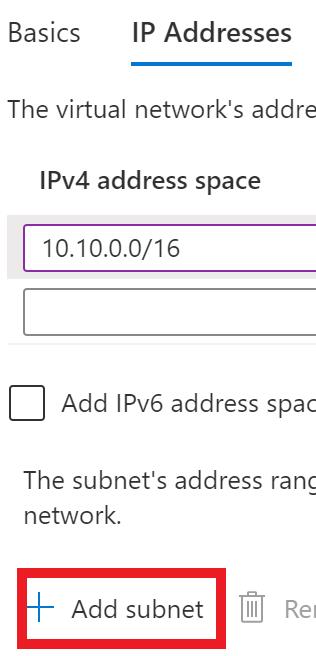
* Sign in to the Azure portal
* Create a virtual network in the Azure portal by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod26433645** |
| Name | webVNET |
| IPv4 address space | 10.10.0.0/16 |
| Subnet name | web |
| Subnet address range | 10.10.0.0/25 |

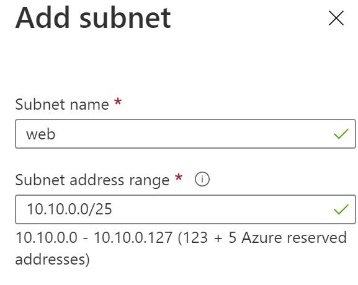
* Expand this hint for guidance on creating a virtual network by using the Azure portal.
  + In the Azure portal, select **Create a resource** to display the Azure Marketplace.
  + In Search services and marketplace, search for and select Virtual Network, and then select **Create**.



* + On the Create virtual network blade, on the Basics page, in Resource group, select **corp-datalod26433645**, in Name, enter webVNET, and then select **Next : IP Addresses**.
  + On the IP Addresses page, in IPv4 address space, select the existing address space **10.0.0.0/16**, enter 10.10.0.0/16 to overwrite the value, and then select **Add subnet** to open the Add subnet blade.



* + On the Add subnet blade, in Subnet name, enter web, in Subnet address range, enter 10.10.0.0/25, and then select **Add**.



* + On the Create virtual network blade, select **Review + create**, and then select **Create** to create the virtual network.

You will use this virtual network for the web tier.

You can use an [Azure virtual network](https://docs.microsoft.com/en-us/azure/virtual-network/concepts-and-best-practices) to create a network address space in the cloud that you will use to host resources—for example, virtual machines, load balancers, and application gateways—for secure access from on-premises networks and other virtual networks.

## Check your work

* Confirm that you created a virtual network named webVNET.
* Confirm that you created a subnet named web in the webVNET virtual network.

# **Create an application security group and an associated network security group**

* Create an application security group named webASG in the **corp-datalod26433645** resource group.

Expand this hint for guidance on creating an application security group.

* + On the Azure portal menu, select **Create a resource** to display the Azure Marketplace.
  + In Search services and marketplace, search for and select Application security group, and then select **Create**.



* + On the Create an application security group blade, in Resource group, select **corp-datalod26433645**, and then in Name, enter webASG.
  + Select **Review + create**, and then select **Create** to create the application security group.

You can continue without waiting for the deployment to finish.

* Create a network security group named webNSG in the **corp-datalod26433645** resource group.

Expand this hint for guidance on creating a network security group.

* + On the Azure portal menu, select **Create a resource** to display the Azure Marketplace.
  + In Search services and marketplace, search for and select Network security group, and then select **Create**.



* + On the Create an network security group blade, in Resource group, select **corp-datalod26433645**, and then in Name, enter webNSG.
  + Select **Review + create**, and then select **Create** to create the network security group.
* Add an inbound security rule to **webNSG** to allow HTTP and HTTPS traffic by using the values in the following table. For any property that is not specified, use the default value.

| **Setting** | **Value** |
| --- | --- |
| Destination | **Application security group** |
| Destination application security groups | **webASG** |
| Destination port ranges | 80,443 |
| Name | AllowAllweb |

* Expand this hint for guidance on adding an inbound security rule.
  + On the Azure portal menu, select **All services**, in Categories, select **Networking**, and then select **Network security groups**.
  + On the Network security groups page, select **webNSG**.
  + On the webNSG resource menu, in Settings, select **Inbound security rules**, and then on the command bar, select **Add**.
  + On the Add inbound security rule blade, in Destination, select **Application security group**, and then in Destination application security groups, select **webASG**.
  + In Destination port ranges, enter 80,443, in Name, enter AllowAllweb, and then select **Add** to add the inbound security rule.

Wait for the new inbound security rule to be created. This will take approximately 1–2 minutes.

* Add a second inbound security rule to **webNSG** to allow RDP traffic by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Destination | **Application security group** |
| Destination application security groups | **webASG** |
| Destination port ranges | 3389 |
| Name | AllowAllRDP |

* Wait for the new inbound security rule to be created.
* Associate the network security group to the **web** subnet in **webVNET**.

Expand this hint for guidance on associating a network security group to a subnet.

* + On the webNSG resource menu, in Settings, select **Subnets**, and then on the command bar, select **Associate**.
  + On the Associate subnet blade, in Virtual network, select **webVNET**, in Subnet, select **web**, and then select **OK** to associate the network security group to the selected subnet.

Wait for the webNSG to be associated with the web subnet. This will take approximately 1–2 minutes.

## Check your work

* Confirm that you created an application security group named webASG.
* Confirm that you created a network security group named webNSG.
* Confirm that you created inbound security rules that allow RDP, HTTP, and HTTPS traffic to flow to webASG.
* Confirm that you associated the web subnet with the webNSG network security group.

# **Create an Azure virtual machine**

* Create an Azure virtual machine by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod26433645** |
| Virtual machine name | VM1 |
| Image | **Windows Server 2019 Datacenter - Gen1** |
| Size | **Standard\_B2s - 2 vcpus 4 GiB memory** |
| Username | AzureAdmin |
| Password | Az!26433645! |
| Public inbound ports | **None** |
| Virtual network | **webVNET** |
| Subnet | **web (10.10.0.0/25)** |
| NIC network security group | **None** |
| Boot diagnostics | **Disable** |

* Expand this hint for guidance on creating an Azure virtual machine.
  + On the Azure portal menu, select **Create a resource** to display the Azure Marketplace.
  + In Categories, select **Compute**, and then select **Virtual machine**.
  + On the Create a virtual machine blade, on the Basics page, in Resource group, select **corp-datalod26433645**.
  + In Virtual machine name, enter VM1.
  + In Image, select **Windows Server 2019 Datacenter - Gen1**.
  + In Size, select **See all sizes**.
  + On the Select a VM size page, in Search by VM size, enter B2, in VM Size, select **B2s**, and then select **Select**.
  + On the Basics page, in Username, enter AzureAdmin, in Password and Confirm password, enter Az!26433645!, and then in Public inbound ports, select **None**.
  + On the Networking page, in Virtual network, ensure that **webVNET** is selected, in Subnet, ensure that **web (10.10.0.0/25)** is selected, and then in NIC network security group, ensure that **None** is selected.
  + On the Management page, in Boot diagnostics, select **Disable**.
  + Select **Review + create**, review the virtual machine specifications, and then select **Create** to deploy the virtual machine.

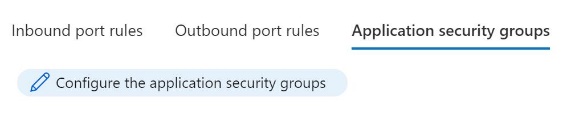
Ignore any warnings about RDP ports as this virtual machine is only being used for testing.

The deployment will take approximately 3–5 minutes.

* Associate the **webASG** application security group with the VM1 virtual machine NIC.

Expand this hint for guidance on associating an application security group with a virtual machine NIC.

* + On the Azure portal menu, select **All resources**, and then select **VM1**.
  + On the VM1 resource menu, in Settings, select **Networking**.
  + On the Networking page, select **Application security groups**, and then select **Configure the application security groups**.



* + On the Configure the application security groups blade, in Application security groups, select **webASG**, and then on the command bar, select **Save**.

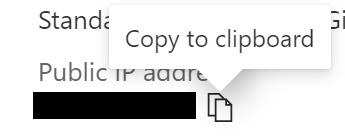
It will take approximately 1–2 minutes to save the network settings in the background.

* Record the public IP address of VM1 in the following **VM1 Public IP Address** text box:

**VM1 Public IP Address**  


Expand this hint for guidance on locating the public IP address of a virtual machine.

* + On the VM1 Overview page, in Public IP address, select the **Copy to clipboard** icon, and then paste the Public IP address into the **VM1 Public IP Address** text box above.



* Connect to VM1 through **RDP** by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| IP address | **Public IP address** |
| Username | AzureAdmin |
| Password | Az!26433645! |

* Expand this hint for guidance on connecting to a virtual machine by using RDP.
  + On the Azure portal home page, select **Virtual machines**, and then select **VM1**.
  + On the VM1 Overview page, on the command bar, select **Connect**, and then select **RDP**.
  + On the Connect page, in IP address, ensure that **Public IP address** is selected, and then select **Download RDP File**.
  + Open the RDP file, and then in the Remote Desktop Connection window, select **Connect**.
  + When prompted for credentials, select **More choices**, and then select **Use a different account**.
  + In User name, enter AzureAdmin, in Password, enter Az!26433645!, and then select **OK**.
  + In the Remote Desktop Connection warning message box, select **Yes**, and then wait for the RDP session to initialize.
  + In the RDP session, if prompted to allow your PC to be discoverable by other PCs and devices on this network, select **No**, and then minimize Server Manager.

Resize the RDP session window so that you can view the instructions for the challenge at the same time.

* On **VM1**, run the following command in **Windows PowerShell®** to install Internet Information Services (IIS):

Install-WindowsFeature -name web-Server -IncludeManagementTools

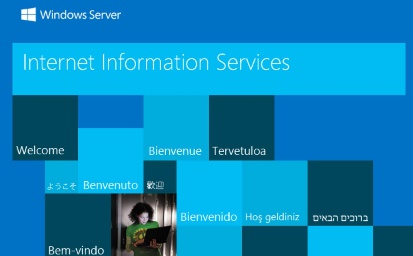
Expand this hint for guidance on installing IIS by using Windows PowerShell.

* + In the Remote Desktop Connection window, on the Start menu, select **Windows PowerShell**.
  + In Windows PowerShell, run the following command to install IIS on VM1:

Install-WindowsFeature -name web-Server -IncludeManagementTools

* + Verify that the IIS installation was successful.
  + Close the Remote Desktop Connection window, and then select **OK** to disconnect.
* Open a new browser window, and then go to the public IP address of VM1 at http://<PublicIP> .

You should see the default Internet Information Services (IIS) webpage. This will verify that web traffic has been routed correctly by using an application security group and a network security group.



## Check your work

* Confirm that you created an Azure virtual machine named VM1.
* Confirm that you associated the webASG application security group with the virtual machine NIC.
* Confirm that you installed IIS on the virtual machine via RDP.
* Confirm that you verified that web traffic has been routed correctly.

# **Summary**

Congratulations, you have completed the **Configure an Application Security Group** challenge.

You have accomplished the following:

* Created a virtual network for a web server tier.
* Created an application security group and associated network security group.
* Created an Azure virtual machine and tested application security