

Harden Virtual Machines in Azure

Understand the scenario

You are an Azure® administrator. You need to create an Azure virtual machine that adheres to security best practices. First, you will create a virtual network, and then you will create a network security group. Next, you will create an application security group, and then you will create an Azure virtual machine. Finally, you will create an Azure key vault, and then you will enable Azure Disk Encryption.

Understand your environment

You will be using an Azure resource group named corp-datalod26434050 that contains no resources.

# **Create an Azure virtual network by using a network security group**

* Open Microsoft Edge, and then sign in to http://portal.azure.com
* 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-datalod26434050** |
| Name | webVNET |
| IPv4 address space | 10.10.0.0/16 |
| Subnet name | web |
| Subnet address range | 10.10.0.0/26 |

* Expand this hint for guidance on creating a virtual network.
  + Review the documentation on [creating a virtual network](https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-connect-virtual-networks-portal#create-virtual-networks).
* Create a network security group named webNSG in the **corp-datalod26434050** resource group.

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

* + Review the documentation on [creating a network security group](https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic#create-a-network-security-group).
* Associate the webNSG network security group to the **web** subnet in the **webVNET** virtual network.

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

* + Review the documentation on [associating a network security group to a subnet](https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic#associate-network-security-group-to-subnet).

## Check your work

Verify that you have created a virtual network named webVNET.

Verify that you have created a network security group named webNSG.

Verify that you have associated the webNSG network security group to the web subnet.

# **Deploy an Azure virtual machine for a web app by using an application security group**

* Create an application security group named webASG in the **corp-datalod26434050** resource group.

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

* + Review the documentation on [creating an application security group](https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic#create-application-security-groups).
* Create an Azure virtual machine for the web tier by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod26434050** |
| Virtual machine name | VM1 |
| Image | **Windows Server 2019 Datacenter - Gen2** |
| Size | **Standard\_B2s - 2 vcpus 4 GiB memory** |
| Username | AzureAdmin |
| Password | Az!26434050! |
| Public inbound ports | **None** |
| Virtual network | **webVNET** |
| Subnet | **web (10.10.0.0/26)** |
| NIC network security group | **None** |
| Boot diagnostics | **Disable** |

* Expand this hint for guidance on creating a virtual machine.
  + Review the documentation on [creating a virtual machine](https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-connect-virtual-networks-portal#create-virtual-machines).
* Associate the VM1 virtual machine network interface to the **webASG** application security group.

Expand this hint for guidance on associating a virtual machine network interface to an application security group.

* + Review the documentation on [associating a virtual machine network interface to an application security group](https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic#associate-network-interfaces-to-an-asg).

It may take approximately 10-15 minutes to for the operation to complete in the background.

* Record the public IP address issued to the virtual machine network interface in the following **Public IP Address** text box:

**Public IP Address**  


## Check your work

Verify that you have created an application security group named webASG.

Verify that you have created a virtual machine named VM1.

Verify that you have associated the virtual machine network interface to the webASG application security group.

# **Enable web connectivity by using an application 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 group | **webASG** |
| Destination port ranges | 80,443 |
| Name | AllowAllWeb |

* Expand this hint for guidance on creating an inbound security rule.
  + Review the documentation on [creating an inbound security rule](https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic#create-security-rules).
* 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 group | **webASG** |
| Destination port ranges | 3389 |
| Name | AllowRDP |

* 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!26434050! |

* Expand this hint for guidance on connecting to a virtual machine through RDP.
  + Review the documentation on [connecting to a virtual machine through RDP](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/quick-create-portal#connect-to-virtual-machine).
* Install **IIS** on **VM1** by using **Windows PowerShell**®.

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

* + Review the documentation on [installing IIS by using Windows PowerShell](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/quick-create-portal#install-web-server).
* Open a new browser window, and then go to the public IP address of the virtual machine at http://<PublicIP>.

You should see the default IIS webpage.

## Check your work

Verify that you have added an inbound security rule named AllowAllWeb that allows HTTP and HTTPS traffic.

Verify that you have added an inbound security rule named AllowRDP that allows RDP traffic.

# **Enable Azure Disk Encryption**

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

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod26434050** |
| Key vault name | KV26434050 |
| Pricing tier | **Standard** |
| Azure Disk Encryption for volume encryption | **Selected** |

* Expand this hint for guidance on creating an Azure key vault.
  + Review the documentation on [creating an Azure key vault](https://docs.microsoft.com/en-us/azure/key-vault/general/quick-create-portal#create-a-vault).
* Launch an Azure **Cloud Shell** **PowerShell** session by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod26434050** |
| Storage account | cs26434050 |
| File share | cloudshell |

* Expand this hint for guidance on launching Azure Cloud Shell.
  + Review the documentation on [launching Azure Cloud Shell](https://docs.microsoft.com/en-us/azure/key-vault/general/quick-create-portal#use-azure-cloud-shell).
* Enable Azure Disk Encryption on VM1 in the corp-datalod26434050 resource group by using the Set-AzVMDiskEncryptionExtension PowerShell cmdlet and a vault name of KV26434050.

Expand this hint for guidance on enabling Azure Disk Encryption by using PowerShell.

* + Review the documentation on [enabling Azure Disk Encryption by using PowerShell](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-powershell-quickstart#encrypt-the-virtual-machine).

It may take 10-15 minutes to for the operation to complete in the background.

* Verify that the encryption succeeded by using the Get-AzVmDiskEncryptionStatus cmdlet.

## Check your work

Verify that you have created a key vault.

Verify that you have enabled Azure Disk Encryption on VM1.

# **Summary**

Congratulations, you have completed the **Can You Harden Virtual Machines in Azure?** challenge.

In this challenge, you have accomplished the following:

* Created an Azure virtual network by using a network security group.
* Deployed an Azure virtual machine for a web app by using an application security group.
* Enabled web connectivity by using an application security group.
* Enabled Azure Disk Encryption.