

Enable Secure Virtual Machines and Application Services

Understand the scenario

You are an Azure® administrator. You need to enable secure virtual machines and application services. First, you will create a virtual machine, and then you will install the Microsoft Antimalware extension. Next, you will deny RDP traffic for the virtual machine, and then you will enable Azure Disk Encryption. Finally, you will deploy a web app, and then you will enable Application Insights for security monitoring.

Understand your environment

You will be using an Azure resource group named corp-datalod26433360 that contains a Log Analytics workspace.

# **Create an Azure virtual machine**

* If necessary, sign in to Windows 10 - RDP Jumpbox as LabUser using Passw0rd! as the password.

Select the Type Text icon to enter the associated text into the virtual machine.

* Open Microsoft Edge, and then sign in to http://portal.azure.com

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod26433360** |
| Virtual machine name | webVM1 |
| Image | **Windows Server 2019 Datacenter - Gen2** |
| Size | **Standard\_B2ms** |
| Username | AzureAdmin |
| Password | Az!26433360! |
| Public inbound ports | **Allow selected ports** |
| Select inbound ports | **RDP (3389)** |
| OS disk type | **Standard HDD** |
| 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" \l "create-virtual-machines" \o "Create virtual machines" \t "_blank).

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

The deployment should take approximately 3–5 minutes. Wait for the deployment to complete before moving on to the next step.

## Check your work

Verify that you created a virtual machine named webVM1.

# **Enable recommended security features**

* Install the **Microsoft Antimalware** extension on **webVM1** by using the default settings.

Expand this hint for guidance on adding the Microsoft Antimalware extension.

* + Review the documentation on [adding the Microsoft Antimalware extension](https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware" \l "antimalware-deployment-scenarios" \o "Antimalware Deployment Scenarios" \t "_blank).
* Delete the **RDP** inbound security rule in the **webVM1-nsg** network security group to deny RDP traffic for webVM1.

Expand this hint for guidance on deleting an inbound security rule.

* + Review the documentation on [deleting an inbound security rule](https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group" \l "delete-a-security-rule" \o "Delete a security rule" \t "_blank).
* 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-datalod26433360** |
| Key vault name | KV26433360 |
| Pricing tier | **Standard** |
| Enable Access to | **Azure Disk Encryption for volume encryption** |

* 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" \l "create-a-vault" \o "Create a vault" \t "_blank).
* Create an Azure Cloud Shell **PowerShell** session in the **East US** region by using the **corp-datalod26433360** resource group, a storage account named cs26433360, and a file share named cloudshell.

Expand this hint for guidance on creating an Azure Cloud Shell session.

* + Review the documentation on creating an [Azure Cloud Shell](https://docs.microsoft.com/en-us/azure/key-vault/general/quick-create-portal#use-azure-cloud-shell) session
* Enable Azure Disk Encryption for the virtual machine by using the Set-AzVMDiskEncryptionExtension PowerShell cmdlet and the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| ResourceGroupName | corp-datalod26433360 |
| VaultName | KV26433360 |
| VMName | webVM1 |

* Expand this hint for guidance on enabling Azure Disk Encryption by using PowerShell.
  + Review the documentation on [enabling Azure Disk Encryption](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-powershell-quickstart" \l "encrypt-the-virtual-machine" \o "Encrypt the virtual machine" \t "_blank) by using PowerShell.

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

## Check your work

Verify that you have added the Microsoft Antimalware extension on the webVM1 virtual machine.

Verify that you have deleted the RDP inbound security rule in the webVM1-nsg network security group.

Verify that you have created a key vault.

Verify that you have enabled Azure Disk Encryption on the webVM1 virtual machine.

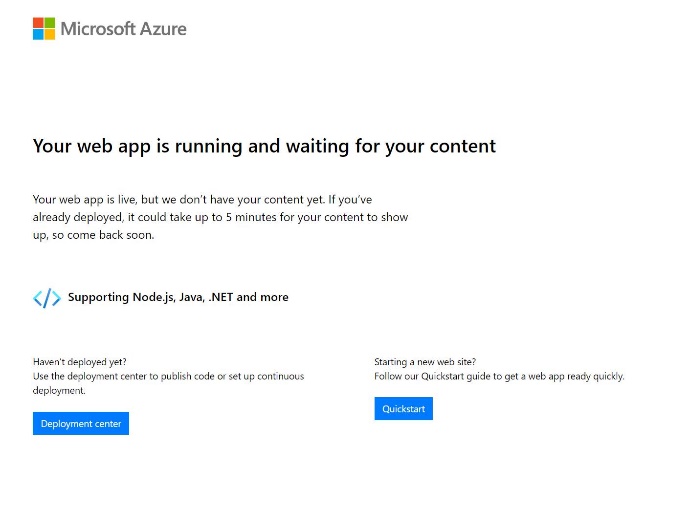
# **Enable Application Insights to monitor security**

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

| **Property** | **Value** |
| --- | --- |
| Resource Group | **corp-datalod26433360** |
| Name | wa26433360 |
| Publish | **Code** |
| Runtime stack | **ASP.NET V4.8** or the latest version that is not preview or early access |
| Region | **East US** |
| Windows Plan (East US) | AppPlan1 |
| Sku and size | **Standard S1** |
| Continuous deployment | **Disable** |
| Enable network injection | **Off** |
| Enable Application Insights | **No** |

* In a new browser tab, go to the URL for the new web app at https://wa26433360.azurewebsites.net to verify that it is up and running.

You should see a default home page.



* Deploy the source code for the **wa26433360** web app by using the values in the following table. For any property that is not specified, use the default value.

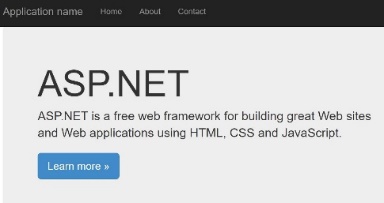
| **Property** | **Value** |
| --- | --- |
| Source | **External Git** |
| Repository | https://github.com/LODSContent/LODSOC\_app-service-web-dotnet-get-started |
| Branch | main |
| Repository Type | **Public** |

* Expand this hint for guidance on deploying source code to a web app.
  + Review the documentation on [deploying source code to a web app](https://docs.microsoft.com/en-us/azure/app-service/deploy-continuous-deployment" \o "Continuous deployment to Azure App Service" \t "_blank).

You may have to wait approximately 1-2 minutes for the new code to fully deploy.

* In a new browser tab, go to the URL for the web app at https://wa26433360.azurewebsites.net to verify that it is up and running.

You should see an updated home page.



If you do not see the updated page, refresh the browser.

* Enable **Application Insights** for the wa26433360 web app by using the new resource name wa26433360 and the **laws-26433360** Log Analytics Worspace.

Expand this hint for guidance on enabling Application Insights for a web app.

* + Review the documentation on [enabling Application Insights](https://docs.microsoft.com/en-us/azure/azure-monitor/app/azure-web-apps?tabs=net" \l "enable-agent-based-monitoring" \o "Enable agent-based monitoring" \t "_blank) for a web app.

You may have to wait approximately 1–2 minutes for Application Insights to be fully enabled.

* Open the **Live metrics** report on the **Application Dashboard** for the wa26433360 web app.

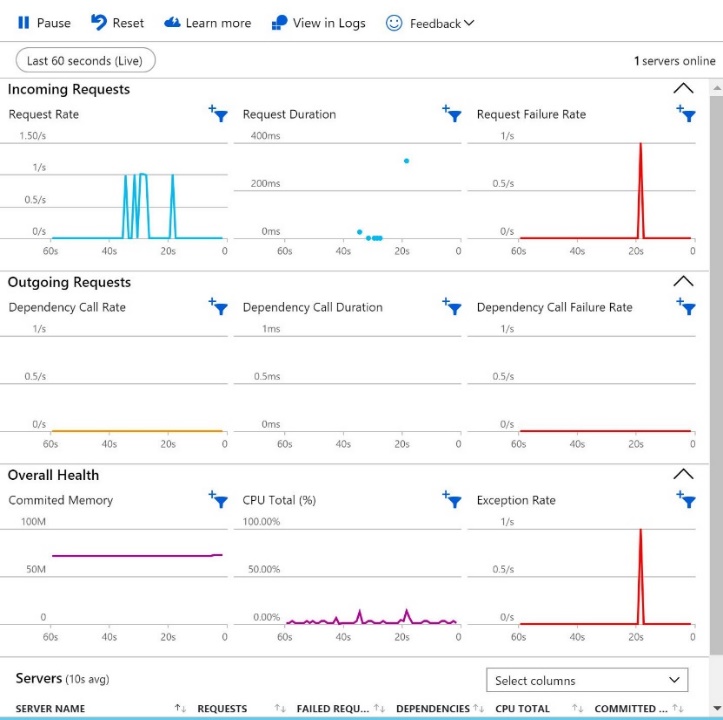
Expand this hint for guidance on using Application Insights for a web app.

* + Review the documentation on [using Application Insights](https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview" \l "how-do-i-use-application-insights" \o "How do I use Application Insights?" \t "_blank) for a web app.

Keep the Live metrics report open. You will use this to display requests in an upcoming step.

* In a new browser window, go to the URL for the web app at https://wa26433360.azurewebsites.net, and then refresh the browser a few times to generate valid requests.
* Generate a failed request for the web app by using the URL https://wa26433360.azurewebsites.net/default.
* Return to the **Live metrics** report, and then review the successful and failed requests.

You should see the successful and failed requests from the last 60 seconds.



## Check your work

Verify that you have created a web app.

Verify that you have enabled Application Insights for the web app.

# **Summary**

Congratulations, you have completed the **Can You Enable Secure Virtual Machines and Application Services?** challenge.

You have accomplished the following:

* Created an Azure virtual machine.
* Installed the Microsoft Antimalware extension.
* Denied RDP access to a virtual machine.
* Enabled Azure Disk Encryption.
* Enabled Application Insights to monitor security.