

Manage Security for Virtual Machines and Databases

Understand the scenario

You are an Azure® administrator. You need to manage security for virtual machines and databases. First, you will create a virtual machine, and then you will enable security recommendations for the virtual machine. Next, you will enable Azure Defender for SQL for a new Azure SQL database, and then you will perform a vulnerability assessment. Finally, you will deploy an Azure Cosmos DB account, and then you will use role-based access control (RBAC) to control security access to the Azure Cosmos DB® account.

Understand your environment

You will be using an Azure resource group named corp-datalod26435135 that contains no resources.

# **Create a virtual machine**

* Sign in to the Azure portal

Select the Copy to clipboard icon to copy the text string to the clipboard.

A cloud slice is a subset of an Azure subscription that has been assigned to a user account that was provisioned for you for the duration of this challenge lab. A cloud slice provides temporary access to a subset of resources available in a cloud subscription so that you can learn the concepts in this challenge lab without having to configure your own subscription.

A cloud slice has restrictions on the types of administrative activities that are allowed. Please follow the instructions carefully, especially with regard to names and other configuration details.

* 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-datalod26435135** |
| Virtual machine name | webVM1 |
| Image | **Windows Server 2019 Datacenter - Gen2** |
| Size | **Standard\_B2ms** |
| Username | AzureAdmin |
| Password | Az!26435135! |
| Public inbound ports | **Allow selected ports** |
| Select inbound ports | **RDP (3389)** |
| OS disk type | **Standard HDD** |
| Boot diagnostics | **Disable** |

* Install the Microsoft Antimalware extension on the **webVM1** virtual machine by using the default settings.
* Delete the **RDP** inbound security rule in the **webVM1-nsg** network security group to deny RDP traffic for the **webVM1** virtual machine.

# **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-datalod26435135** |
| Key vault name | KV26435135 |
| Pricing tier | **Standard** |
| Azure Virtual Machines for deployment | **Selected** |
| Azure Resource Manager for template deployment | **Selected** |
| Azure Disk Encryption for volume encryption | **Selected** |

* Launch 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** |
| --- | --- |
| Cloud Shell region | **East US** |
| Resource group | **corp-datalod26435135** |
| Storage account | cs26435135 |
| File share | cloudshell |

* Enable Azure Disk Encryption for webVM1 by using the Set-AzVMDiskEncryptionExtension PowerShell cmdlet, and then store the encryption key in the KV26435135 key vault in the corp-datalod26435135 resource group.

# **Enable Azure Defender for SQL on a new Azure SQL database**

* Create an Azure SQL Database on a new logical SQL server by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod26435135** |
| Database name | db26435135 |
| Server name | sql26435135 |
| Server admin login | AzureAdmin |
| Password | AzPwd26435135! |
| Compute + storage | **Standard S0** |
| DTUs | **10 (S0)** |
| Data max size | **250 GB** |
| Connectivity method | **Public endpoint** |
| Allow Azure services and resources to access this server | **Yes** |
| Add current client IP address | **Yes** |
| Enable Azure Defender for SQL | **Not now** |
| Use existing data | **Sample** |

* Log in to the **db26435135** database as AzureAdmin using AzPwd26435135! as the password, and then create a query to retrieve all of the rows in the SalesLT.Customer table.
* Enable Azure Defender for SQL for the **db26435135** database.

If the Getting Started page is displayed when you open Security Center for the database, close the page in order to continue.

* Perform a vulnerability assessment for the **db26435135** database.

# **Create a Cosmos DB account**

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

| **Property** | **Value** |
| --- | --- |
| API | **Core (SQL)** |
| Resource Group | **corp-datalod26435135** |
| Account Name | cosmos26435135 |
| Location | **(US) East US** |
| Apply Free Tier Discount | **Do Not Apply** |
| Geo-Redundancy | **Disable** |
| Multi-region Writes | **Disable** |

* Allow requests from your **current IP** address, and then **accept connections from within public Azure datacenters** to the cosmos26435135 Cosmos DB account.
* Create a container in a new database in the cosmos26435135 account by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Database id | Database1 |
| Container id | Customers |
| Partition key | /\_partitionKey |
| Throughput | **Manual** |
| Estimate your required RU/s with capacity calculator | 500 |

* Create a new item in the **Customers** container by using the following JSON code:
* {
* "firstName": "Tracy",
* "lastName": "Nguyen",
* "age": 32,
* "salary": 90000.00,
* "company": "Veraq",
* "isVested": false

}

* Create a second item in the Customers container by using the following JSON code:
* {
* "firstName": "Shrestha",
* "lastName": "Patel",
* "company": "BEC"

}

* Execute a new query that selects all of the items in the **Customers** container.

# **Enable RBAC**

* Assign the Cosmos DB Account Reader Role role to User1-26435135 for the cosmos26435135 Cosmos DB account.
* In an InPrivate or incognito browser window, go to the Azure portal at http://portal.azure.com, and then sign in.
* Display the **Database1** database in the **cosmos26435135** account, and then execute a new query that selects all of the items in the **Customers** container.

You should see the two new items in the result set because the user has read-only access.

# **Summary**

Congratulations, you have completed the **Can You Manage Security for Virtual Machines and Databases?** challenge.

In this challenge, you have accomplished the following:

* Created a virtual machine.
* Enabled Azure Disk Encryption on a virtual machine.
* Created an Azure SQL Database.
* Enabled Azure Defender for SQL.
* Created an Azure Cosmos DB account.
* Enabled RBAC.