

Implement Security for an Azure Cosmos DB Account and a Storage Account

Understand the scenario

You are an Azure® administrator. You need to implement security for an Azure Cosmos DB® account and a storage account. First, you will deploy an Azure Cosmos DB account, and then you will create a container in a new database. Next, you will create a storage account, and then you will create a container in the storage account. Finally, you will generate a shared access signature (SAS) key for secure access to the storage account, and then you will assign a role to a user for secure access to the Azure Cosmos DB account.

Understand your environment

You will be using an Azure resource group named corp-datalod26435036.

# **Create an Azure Cosmos DB account**

* 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 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) - Recommended** |
| Resource Group | **corp-datalod26435036** |
| Account Name | cosmos26435036 |
| Location | **(US) East US** |
| Apply Free Tier Discount | **Do Not Apply** |
| Geo-Redundancy | **Disable** |
| Multi-region Writes | **Disable** |

* Expand this hint for guidance on creating an Azure Cosmos DB account.
  + Review the documentation on [creating an Azure Cosmos DB account](https://docs.microsoft.com/en-us/azure/cosmos-db/create-cosmosdb-resources-portal" \l "create-an-azure-cosmos-db-account" \o "Create an Azure Cosmos DB account" \t "_blank).

It will take approximately 2-3 minutes to deploy the Azure Cosmos DB account.

* Allow requests from your current IP address to the cosmos26435036 Cosmos DB account, and then configure a firewall exception to accept connections from within public Azure datacenters.

Expand this hint for guidance on configuring an IP firewall in Azure Cosmos DB.

* + Review the documentation on [configuring an IP firewall in Azure Cosmos DB](https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-configure-firewall" \l "configure-ip-policy" \o "Configure an IP firewall by using the Azure portal" \t "_blank).
* Create a container in a new database in the cosmos26435036 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 throughput with capacity calculator | 500 |

* Expand this hint for guidance on creating a container in a new database.
  + Review the documentation on [creating a container in a new database](https://docs.microsoft.com/en-us/azure/cosmos-db/create-cosmosdb-resources-portal" \l "add-a-database-and-a-container" \o "Add a database and a container" \t "_blank).
* 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

}

Expand this hint for guidance on creating a new item in a container.

* + Review the documentation on [creating a new item in a container](https://docs.microsoft.com/en-us/azure/cosmos-db/create-cosmosdb-resources-portal" \l "add-data-to-your-database" \o "Add data to your database" \t "_blank).
* Create a second item in the **Customers** container by using the following JSON code:
* {
* "firstName": "Shrestha",
* "lastName": "Patel",
* "company": "BEC"

}

* Execute a new SQL query that selects all of the items in the **Customers** container, and then execute the query.

Expand this hint for guidance on executing a new SQL query.

* + Review the documentation on [executing a new SQL query](https://docs.microsoft.com/en-us/azure/cosmos-db/create-cosmosdb-resources-portal" \l "query-your-data" \o "Query your data" \t "_blank).

## Check your work

Verify that you have created an Azure Cosmos DB account.

Verify that you have created a database named Database1 in the Azure Cosmos DB account.

Verify that you have created a container named Customers in Database1.

# **Create a storage account**

* Create a storage account by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod26435036** |
| Storage account name | sa26435036 |
| Region | **(US) East US** |
| Performance | **Standard** |
| Redundancy | **Geo-redundant storage (GRS)** |
| Allow Blob public access | **Enabled** |

* Expand this hint for guidance on creating a storage account.
  + Review the documentation on [creating a storage account](https://docs.microsoft.com/en-us/azure/storage/common/storage-account-create?tabs=azure-portal" \l "create-a-storage-account-1" \o "Create a storage account" \t "_blank).
* Create a container named images in the **sa26435036** storage account.

Expand this hint for guidance on creating a storage container.

* + Review the documentation on [creating a storage container](https://docs.microsoft.com/en-us/azure/storage/blobs/storage-quickstart-blobs-portal" \l "create-a-container" \o "Create a container" \t "_blank).
* Upload any image file on your computer to the **images** container as a **64 KB** block blob by using an authentication type of **Account key** and the **Hot (Inferred)** access tier.

Expand this hint for guidance on uploading a file to a storage container.

* + Review the documentation on [uploading a file to a storage container](https://docs.microsoft.com/en-us/azure/storage/blobs/storage-quickstart-blobs-portal" \l "upload-a-block-blob" \o "Upload a block blob" \t "_blank).
* Generate a SAS key for the blob file that you uploaded by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Signing method | **Account key** |
| Signing key | **Key 1** |
| Permissions | **Read** |
| Start | The current date at 12:00:00 AM |
| Expiry | Tomorrow's date at 12:00:00 AM |
| Allowed protocols | **HTTPS only** |

* Expand this hint for guidance on generating a SAS key for a blob file.
  + Review the documentation on [generating a SAS key for a blob file](https://docs.microsoft.com/en-us/rest/api/storageservices/create-service-sas" \o "Create a service SAS" \t "_blank).
* Copy the **Blob SAS URL**, and then paste it into the following **Blob SAS URL** text box:

**Blob SAS URL**  


* Open a new browser window, and then go to the Blob SAS URL at <Blob\_SAS\_URL> to verify that you can access the blob file.

The blob file should be displayed by using HTTPS and the SAS key.

If you receive a This site has been reported as unsafe error message, select **More information**, and then select **Continue to the unsafe site (not recommended)** as you are only testing access to the blob.

* Close the new browser window.

## Check your work

Verify that you have created a storage account.

Verify that you have created a container named images in the storage account.

# **Configure role-based access control for the Azure Cosmos DB account**

* Assign the Cosmos DB Account Reader Role to User1-26435036 for the cosmos26435036 Cosmos DB account.

Expand this hint for guidance on configuring role-based access control in Azure Cosmos DB.

* + Review the documentation on [role-based access control in Azure Cosmos DB](https://docs.microsoft.com/en-us/azure/cosmos-db/role-based-access-control).
* Open an InPrivate or incognito browser window, go to the Azure portal at http://portal.azure.com, and then sign in.
* Create a new SQL query that selects all of the items in the **Customers** container in the **Database1** database in the **cosmos26435036** account.

Expand this hint for guidance on executing a new SQL query.

* + Review the documentation on [executing a new SQL query](https://docs.microsoft.com/en-us/azure/cosmos-db/create-cosmosdb-resources-portal" \l "query-your-data" \o "Query your data" \t "_blank).

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

* Attempt to create a new item in the **Customers** container by using the following JSON code:
* {
* "firstName": "Harry",
* "lastName": "Oneal",
* "company": "Veraq"

}

The operation should fail with an The input authorization token can't serve the request error message because the user has read-only access.

## Check your work

Verify that you have assigned the Cosmos DB Account Reader Role to User1 for the Azure Cosmos DB account.

# **Summary**

Congratulations, you have completed the **Can You Implement Security for an Azure Cosmos DB Account and a Storage Account?** challenge.

You have accomplished the following:

* Created an Azure Cosmos DB account.
* Created a storage account.
* Generated an SAS key for the storage account.
* Assigned a role to a user for the Azure Cosmos DB account.