

Configure Security for an Azure Cosmos DB Account

Understand the scenario

You are an Azure® administrator. You need to configure security for a new Azure Cosmos DB® account. First, you will deploy an Azure Cosmos DB account, and then you will create a container in a new database. Next, you will add items to the container, and then you will configure security for the account. Finally, you will test secure access to the Azure Cosmos DB account.

Understand your environment

You will be using an Azure resource group named corp-datalod26434904.

# **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-datalod26434904** |
| Account Name | cosmos26434904 |
| 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.
  + On the Azure portal home page, select **Create a resource** to open the Azure Marketplace.
  + In the Azure Marketplace, search for and select Azure Cosmos DB, and then select **Create**.



* + On the Select API option page, on the Core (SQL) – Recommended tile, select **Create**.
  + On the Create Azure Cosmos DB Account blade, on the Basics page, in Resource Group, select **corp-datalod26434904**.
  + In Account Name, enter cosmos26434904.
  + In Location, select **(US) East US**.
  + In Apply Free Tier Discount, select **Do Not Apply**.
  + On the Global Distribution page, in Geo-Redundancy, select **Disable**, and then in Multi-region Writes, select **Disable**.
  + Select **Review + create**, review the configuration, and then select **Create**.

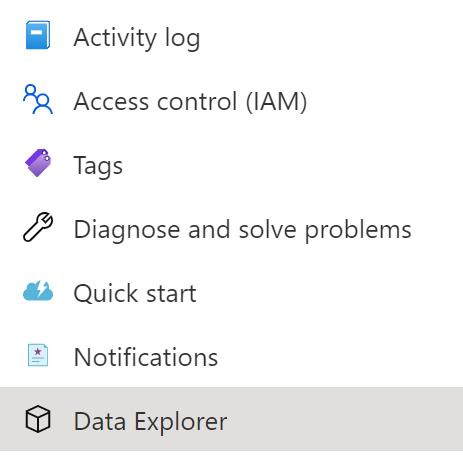
If you get an error message, ensure that you selected Do Not Apply in Apply Free Tier Discount.

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

* Create a container named Customers in a new database named Database1 in the cosmos26434904 account by using a partition key of /\_partitionKey.

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

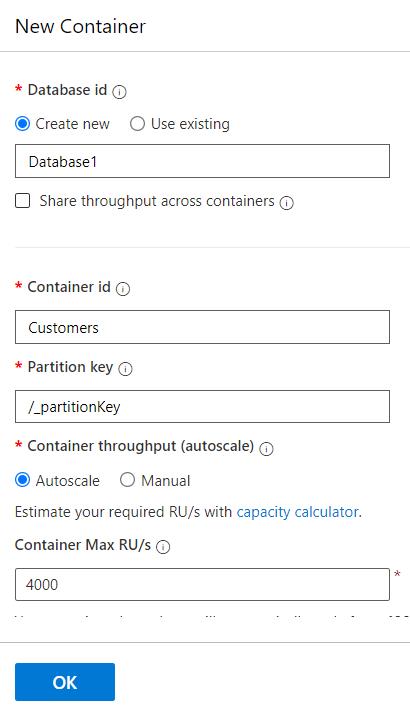
* + On the Azure portal home page, select **All resources**, and then select **cosmos26434904**.
  + On the cosmos26434904 resource menu, select **Data Explorer**.



* + On the command bar, select **New Container**.



* + On the New Container blade, in Database id, enter Database1, in Container id, enter Customers, in Partition key, enter /\_partitionKey, and then select **OK** to add the container.



You create a container in a database. The Azure portal allows you to create the database at the same time as the first container. The [partition key](https://docs.microsoft.com/en-us/azure/cosmos-db/partitioning-overview" \o "Partitioning in Azure Cosmos DB" \t "_blank) is used to automatically distribute data across multiple servers for scalability.

## Check your work

* Confirm that you created an Azure Cosmos DB account named cosmos26434904.
* Confirm that you created a database named Database1.
* Confirm that you created a container named Customers in Database1.

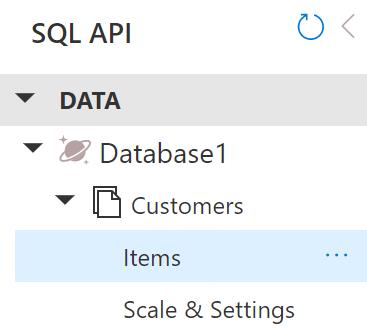
# **Add items to the container**

* 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 items in a container.

* + On the Data Explorer page, expand **Database1**, expand **Customers**, and then select **Items**.



* + On the command bar, select **New Item**.



* + On the Items page, delete the existing JSON code, and then enter the following JSON code:

{

"firstName": "Tracy",

"lastName": "Nguyen",

"age": 32,

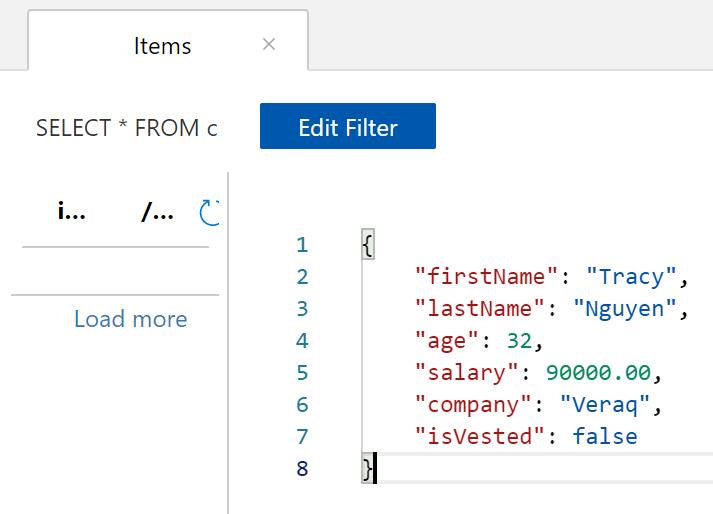
"salary": 90000.00,

"company": "Veraq",

"isVested": false

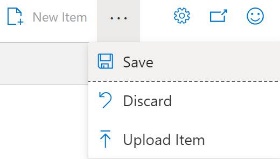
}

* + The following screenshot shows the JSON code:



* + On the command bar, select **Save** to add the new item.

Depending on your screen resolution, you may need to select the ellipsis on the command bar, and then select **Save**.



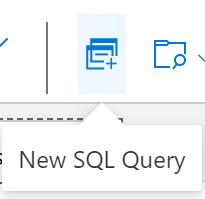
* Create a second item in the Customers container by using the following JSON code:
* {
* "firstName": "Shrestha",
* "lastName": "Patel",
* "company": "BEC"

}

* Create 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 creating a new SQL query.

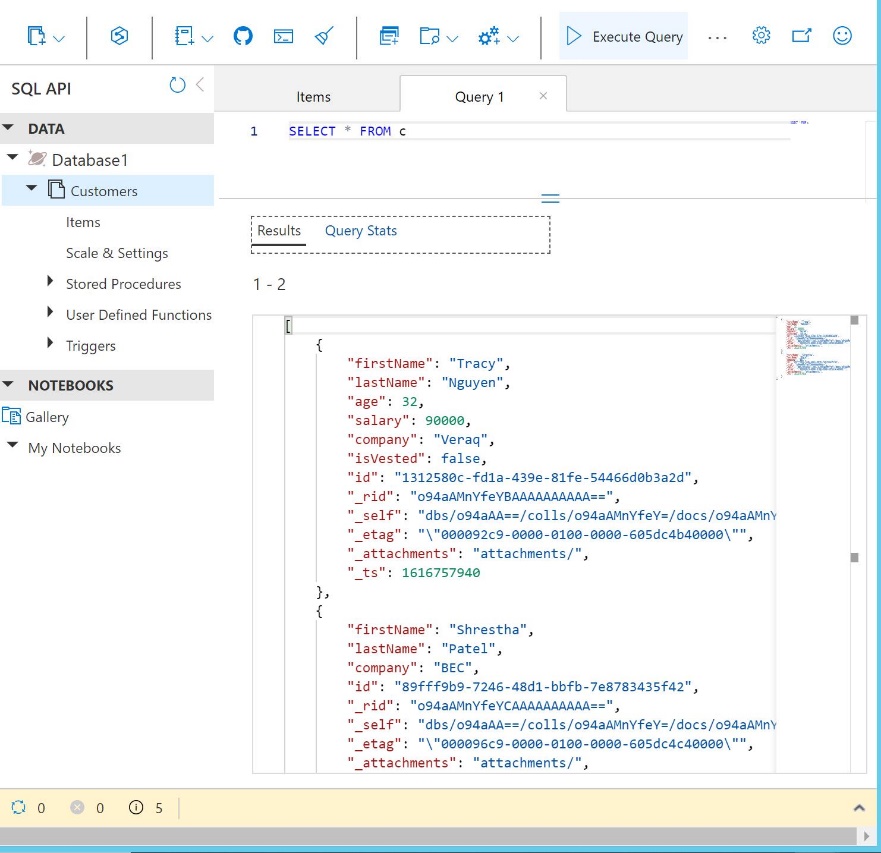
* + On the Data Explorer page, ensure that **Items** is selected, and then on the command bar, select **New SQL Query**.



* + Ensure that the new query contains the following Transact-SQL (T-SQL) code:

SELECT \* FROM c

* + On the command bar, select **Execute Query**.



You should see the two new items in the result set.

## Check your work

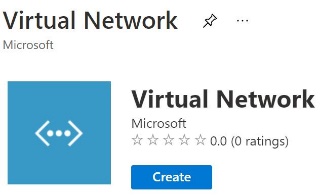
* Confirm that you created two new items in the Customers container.
* Confirm that you executed a new SQL query to display the items in the container.

# **Configure secure access**

* 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-datalod26434904** |
| Name | AppVNet |
| Address space | 10.10.0.0/16 |
| Location | **(US) East US** |
| Subnet | App |
| Subnet address range | 10.10.0.0/24 |

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

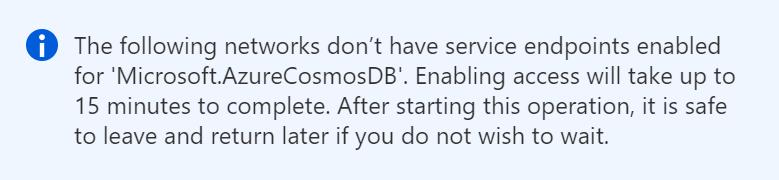


* + On the Create virtual network blade, on the Basics page, in Resource group, select **corp-datalod26434904**, and then in Name, enter AppVNet.
  + On the IP Addresses page, in IPv4 address space, select the existing address space **10.0.0.0/16**, enter 10.10.0.0/16 to replace the value, and then select **Add subnet** to open the Add subnet blade.
  + On the Add subnet blade, in Subnet name, enter App, in Subnet address range, enter 10.10.0.0/24, and then select **Add**.
  + Select **Review + create**, and then select **Create** to create the virtual network.
* Allow access to the cosmos26434904 Azure Cosmos DB account from the App subnet in the AppVNet virtual network and from your current IP address.

Expand this hint for guidance on allowing access to an Azure Cosmos DB account.

* + On the Azure portal home page, select **All resources**, and then select **cosmos26434904**.
  + On the cosmos26434904 resource menu, select **Firewall and virtual networks**.
  + On the Firewall and virtual networks page, in Allow access from, select **Selected networks**, and then in Virtual networks, select **Add existing virtual network**.
  + On the Add networks blade, in Virtual networks, select **AppVNet**, in Subnet, select **App (Service endpoint required)**, and then select **Enable**.
  + On the Add networks blade, select **Add**.
  + On the Firewall and virtual networks page, in Firewall, select **Add my current IP**.
  + On the Firewall and virtual networks page, select **Save**.

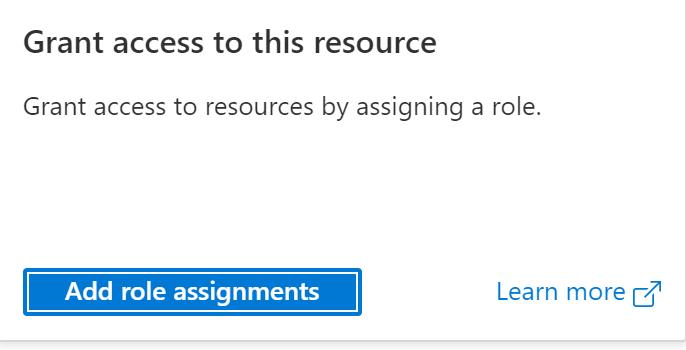
The following informational message is displayed to warn that a service endpoint will be created in the background and may take up to 15 minutes:



* Assign the **Cosmos DB Account Reader Role** to User1-26434904 for the cosmos26434904 Azure Cosmos DB account.

Expand this hint for guidance on assigning roles to a user.

* + On the cosmos26434904 resource menu, select **Access control (IAM)**.
  + On the Access control (IAM) page, in Grant access to this resource, select **Add role assignments (Preview)**.



* + On the Add role assignment blade, on the Role page, search for and select Cosmos DB Account Reader Role, and then select **Next**.
  + On the Members page, select **Select members**.
  + On the Select members blade, search for and select User1-26434904, and then select **Select**.
  + On the Members page, select **Next**, review the settings, and then select **Review + assign**.

Ensure that all update operations have completed before proceeding to the next task.

Azure Cosmos DB supports [role-based access control](https://docs.microsoft.com/en-us/azure/cosmos-db/role-based-access-control) so that you can apply security permissions by assigning roles to Azure Active Directory users and groups.

## Check your work

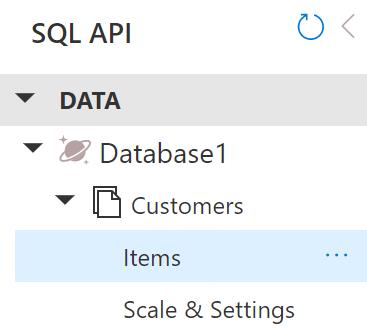
* Confirm that you allowed access to the Azure Cosmos DB account from the App subnet in the AppVNet virtual network.
* Confirm that you allowed access from your current IP address to the Azure Cosmos DB account.
* Confirm that you assigned the Cosmos DB Account Reader role to a user for the Azure Cosmos DB account.

# **Test access to the Azure Cosmos DB account**

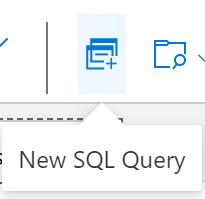
* Open an InPrivate or incognito browser window, go to the Azure portal at http://portal.azure.com, and then sign in as User1-26434904@cloudslice.onmicrosoft.com using password r!DqeSN80+.
* Create a new SQL query that selects all of the items in the **Customers** container, and then execute the query.

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

* + On the Azure portal home page, select **All resources**, and then select **cosmos26434904**.
  + On the cosmos26434904 resource menu, select **Data Explorer**.
  + On the Data Explorer page, expand **Database1**, expand **Customers**, and then select **Items**.



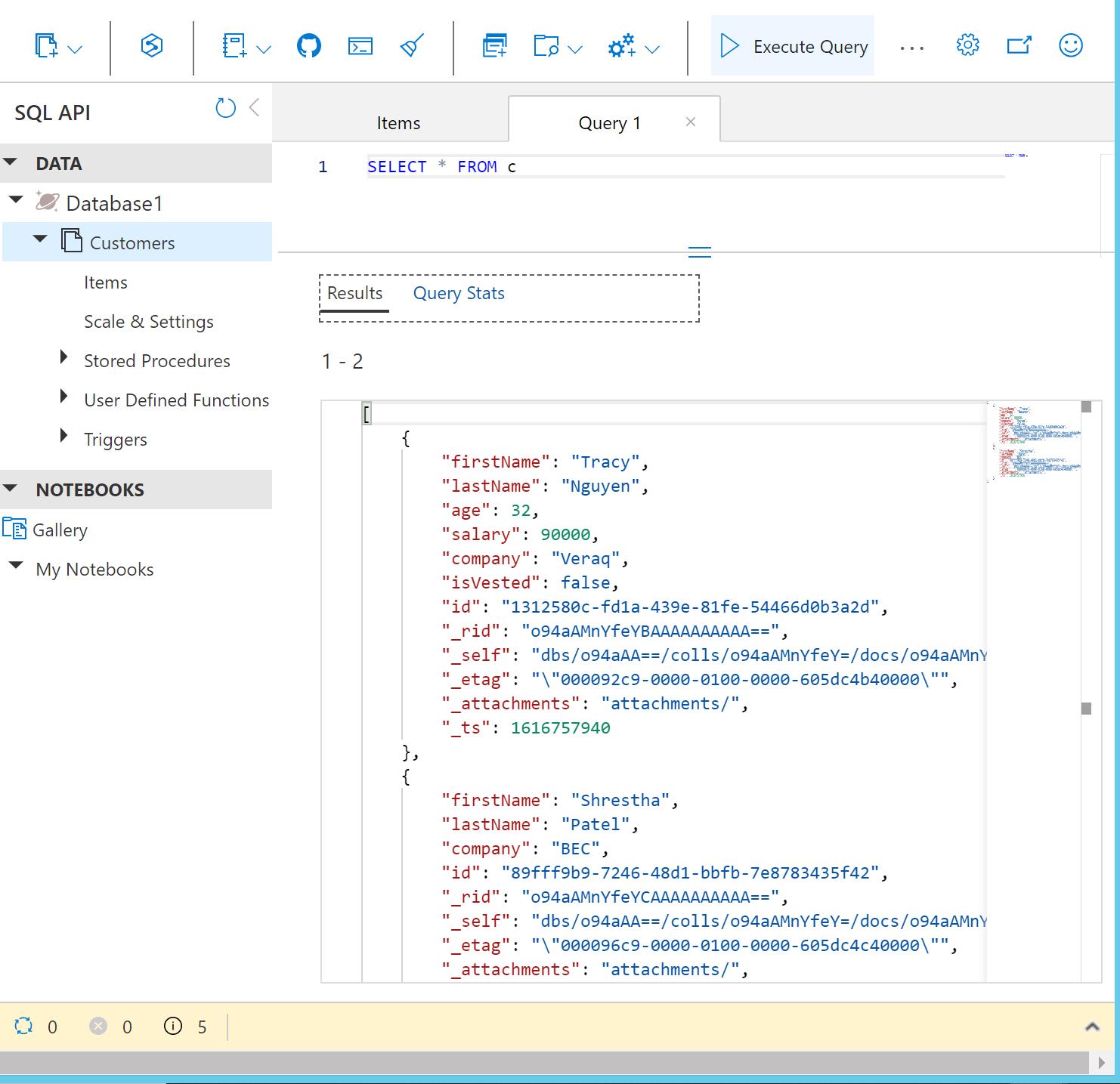
* + On the command bar, select **New SQL Query**.



* + Ensure that the new query contains the following SQL code:

SELECT \* FROM c

* + On the command bar, select **Execute Query**.

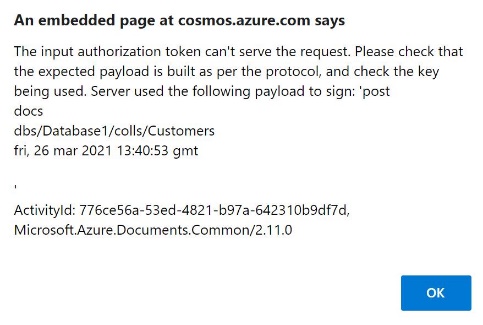


You should see the two new items in the result set because the user has read-only access.

* 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

* Confirm that you verified that User1-26434904 has read-only access to the Azure Cosmos DB account.

# **Summary**

Congratulations, you have completed the **Configure Security for an Azure Cosmos DB Account** challenge.

You have accomplished the following:

* Created an Azure Cosmos DB account.
* Created a container and added items to the container.
* Configured security for the Azure Cosmos DB account.
* Tested access to the Azure Cosmos DB account.