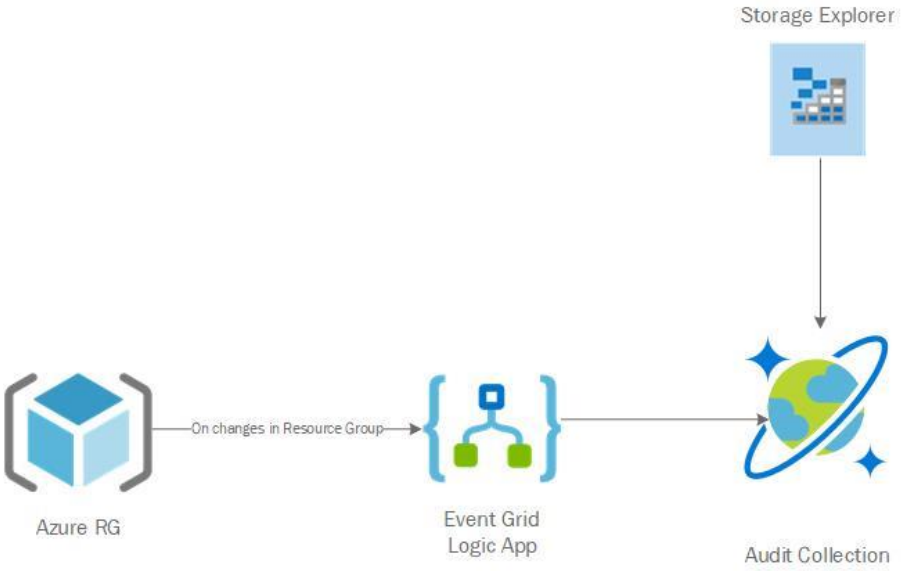
Creating audit solution for Azure Resource Groups

Harris Kristanto

Contents

Objective

In this lab we will be setting up a DevOps auditing solution that will generate and send audit logs to CosmosDB upon any changes in Azure resource group.



Prerequisites

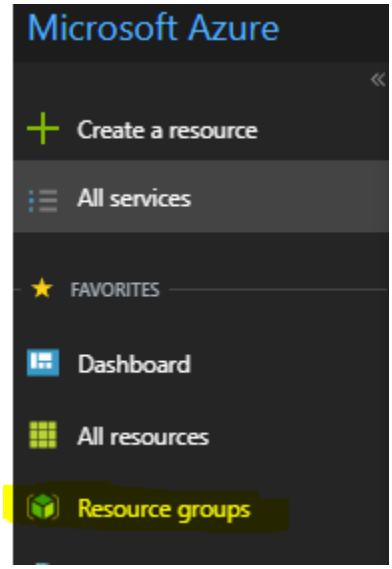
- Azure Subscription
- Azure Storage Explorer: https://azure.microsoft.com/en-us/features/storage-explorer/

Step-by-step guide

Setting up Resource Groups

We will start off by creating resource groups in Azure, navigate to https://portal.azure.com and sign in using Office365 or Microsoft account.

On the main Azure dashboard page, select “Resource groups” located under the Favorites tab.



Under Resource groups, select the option “+Add “, and fill in the following details:

- Resource group name: GIB2018-Labs-AdminRG
- Subscription: <Any available subscription>
- Resource group location: Australia East

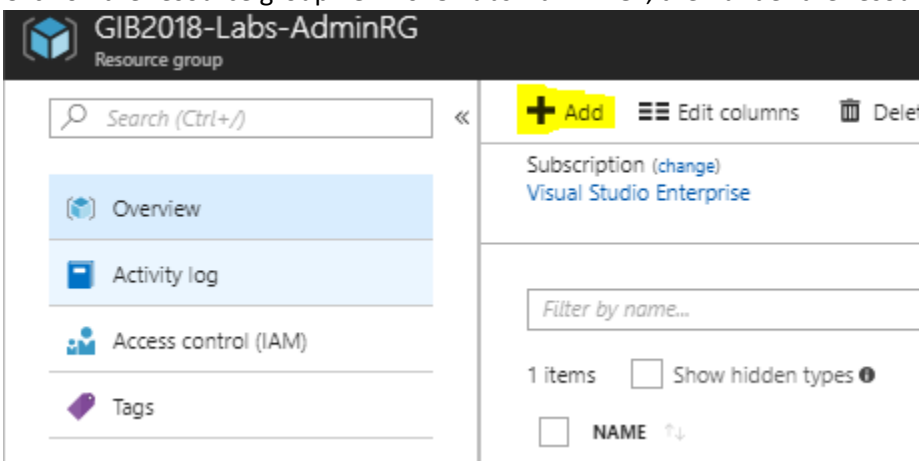
Create another resource groups with the following details:

- Resource group name: GIB2018-Labs-UserRG
- Subscription: <Use the same subscription as per “GIB2018-Labs-AdminRG”>
- Resource group location: Australia East

We should now see the newly created resource groups

Setting up CosmosDB

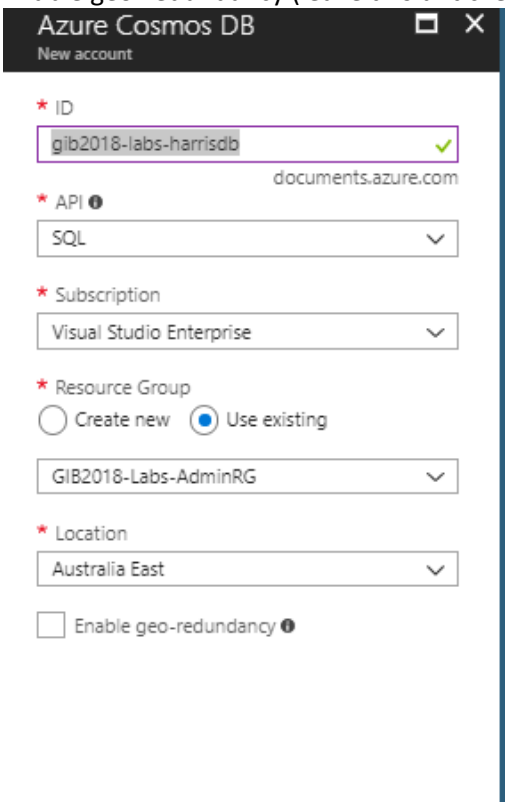
Click on the resource group "GIB2018-Labs-AdminRG", then under the resource group tab, select "+Add"



Search for Azure Cosmos DB and click create, and fill in the required details with the following:

- ID (all in lower case): gib2018-labs-<yourname>db
- API: SQL
- Subscription: <Use the same subscription as per "GIB2018-Labs-AdminRG">
- Resource Group (Use existing): GIB2018-Labs-AdminRG
- Location: Australia East

- Enable geo-redundancy (leave this unticked)

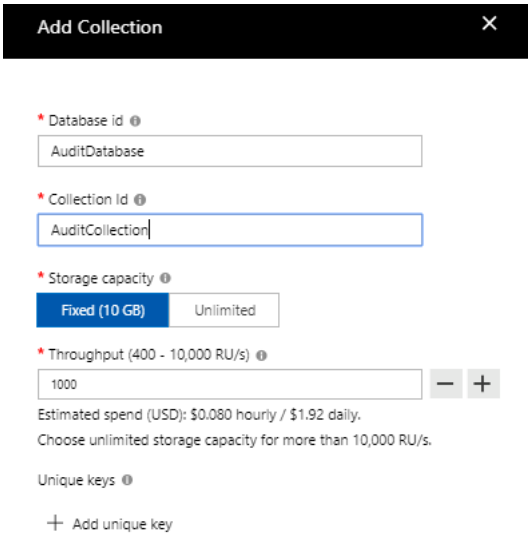


Select create and wait for the deployment to finish.

Click on the CosmosDB resource, and select "+Add collection"

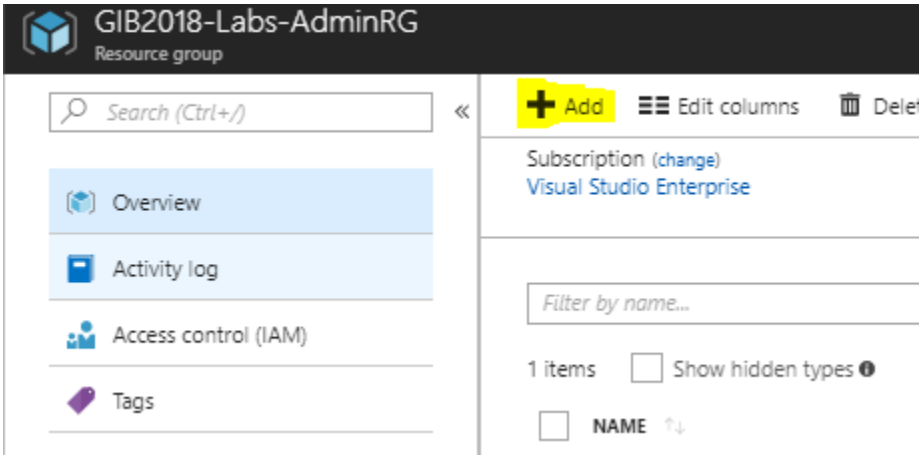
When prompted, create a new collection using the following details and click Ok:

- Database id: AuditDatabase
- Collection id: AuditCollection
- Storage capacity: Fixed(10GB)
- Throughput: 1000



Setting up Logic App

Click on the resource group "GIB2018-Labs-AdminRG", then under the resource group tab, select "+Add"



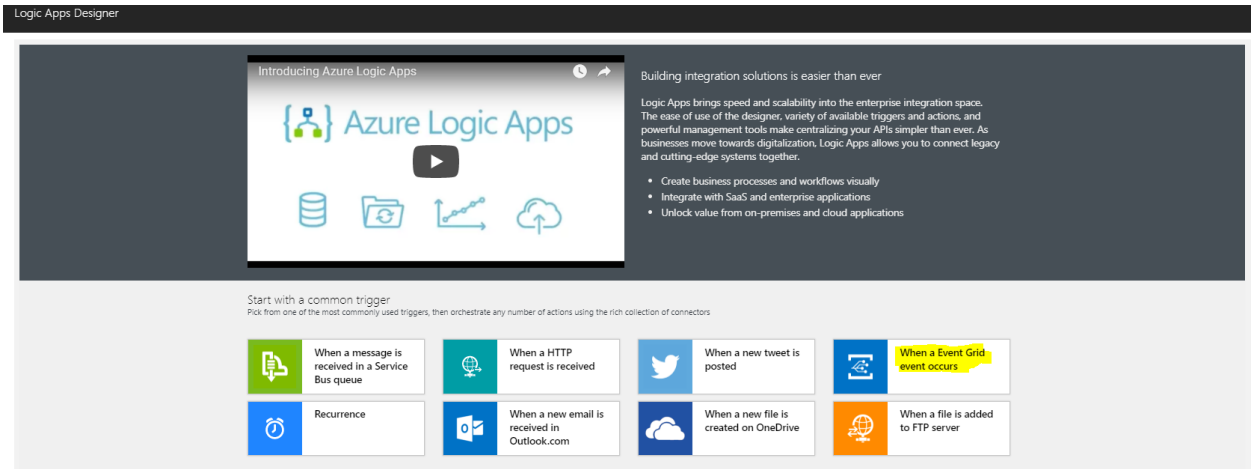
Search for Logic App and click create, and fill in the required details with the following:

- Name: GIB2018-Labs-AuditLogicApp
- Subscription: <Use the same subscription as per "GIB2018-Labs-AdminRG">
- Resource Group (Use existing): GIB2018-Labs-AdminRG

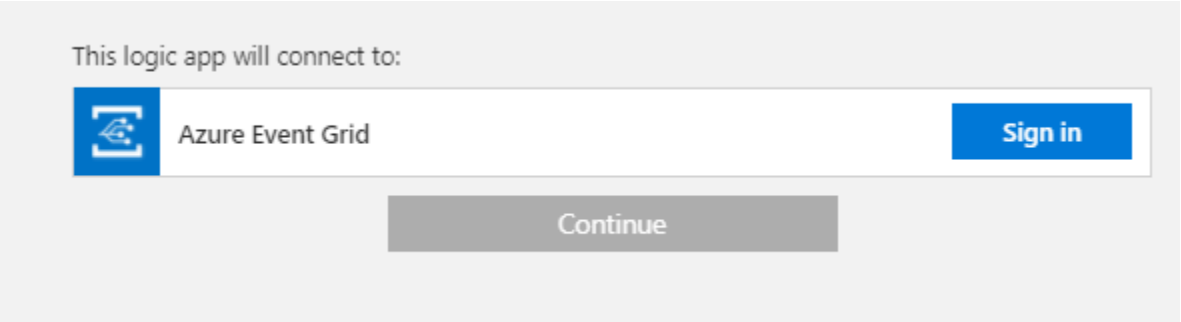
- Location: Australia East
- Log Analytics (Off)

Select create and wait for the deployment to finish.

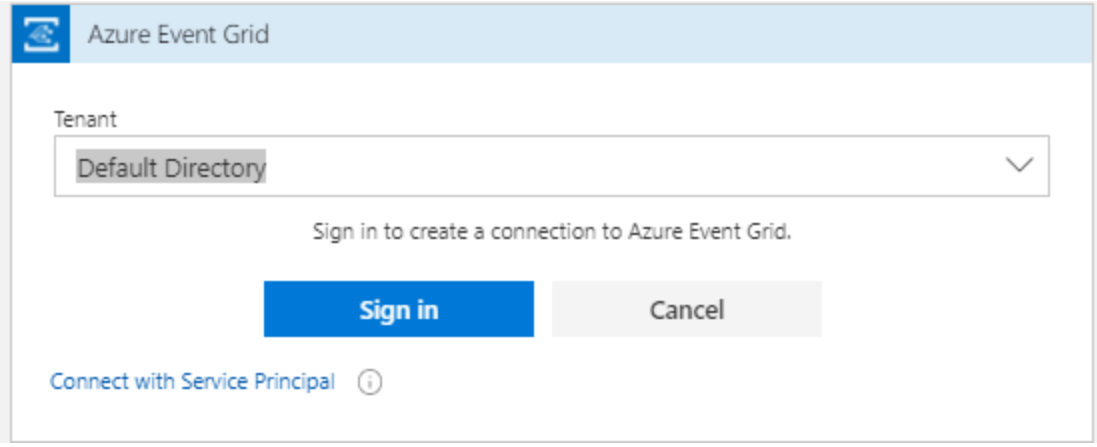
Click on the newly created Logic App resource, when taken to Logic App Designer page choose “When a Event Grid Event occurs”.



Still on the Logic Apps Designer, click Sign In.



Select the tenant where the resource groups we created earlier is located at and click Sign in.

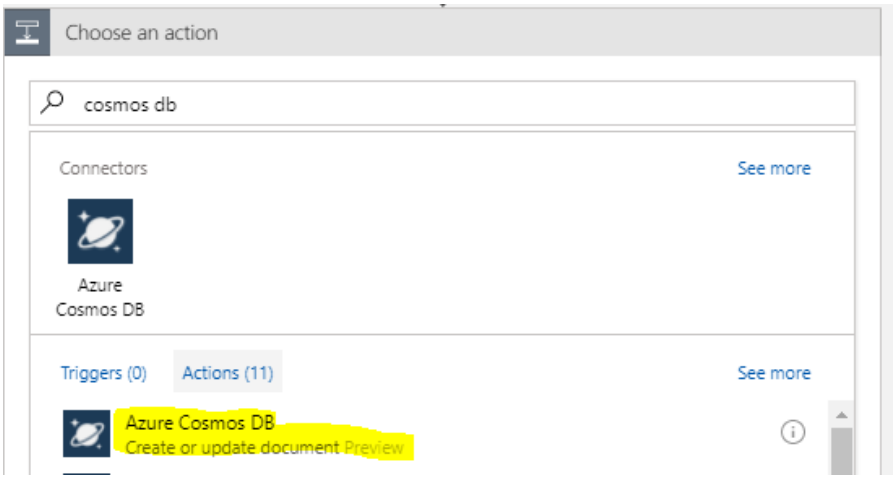


Sign in to your Office365/Microsoft account if required, then click Continue.

Fill in the details on the Logic App trigger with the following:

- Subscription: <Use the same subscription as per "GIB2018-Labs-AdminRG">
- Resource Type: Microsoft.Resources.ResourceGroups
- Resource Name: GIB2018-Labs-UserRG

Click "+ New step" > Add an action, search for "Cosmos DB" and select the action below



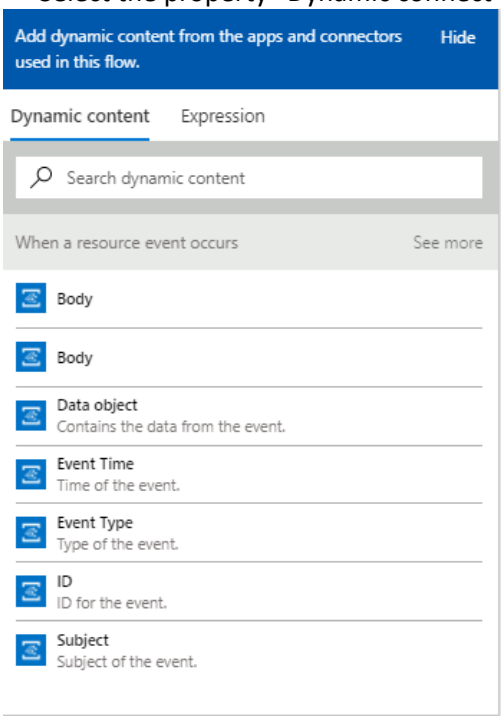
Name the connection "gib2018-labs-<yourname>db", choose the previously created CosmosDB and select Create

Fill in the details on the CosmosDB action with the following:

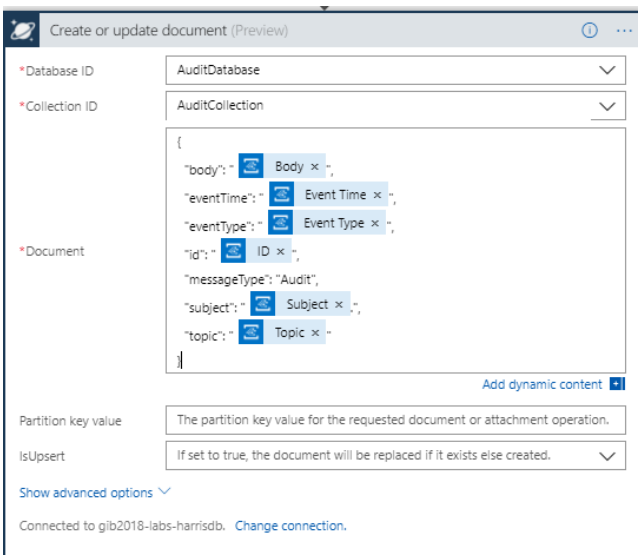
- DatabaseID: AuditDatabase
- CollectionID: AuditCollection
- Document:

```
{
  "body": "Body*"
  "eventTime": "Event Time*",
  "eventType": "Event Type*"
  "id": "ID*",
  "messageType": "Audit",
  "subject": "Subject*",
  "topic": "Topic*"
}
```

- *= Select the property “Dynamic connect” box

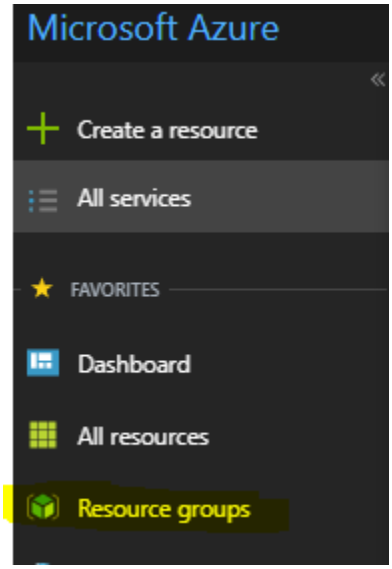


The CosmosDB action should now look like below, save the Logic App:

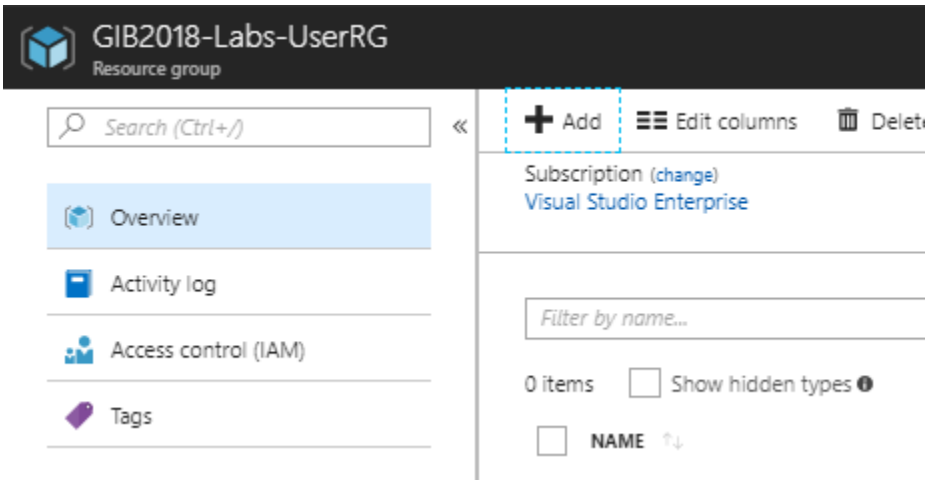


Testing the solution

Select “Resource groups” located under the Favorites tab.



Click on the resource group “GIB2018-Labs-UserRG”, then under the resource group tab, select “+Add”



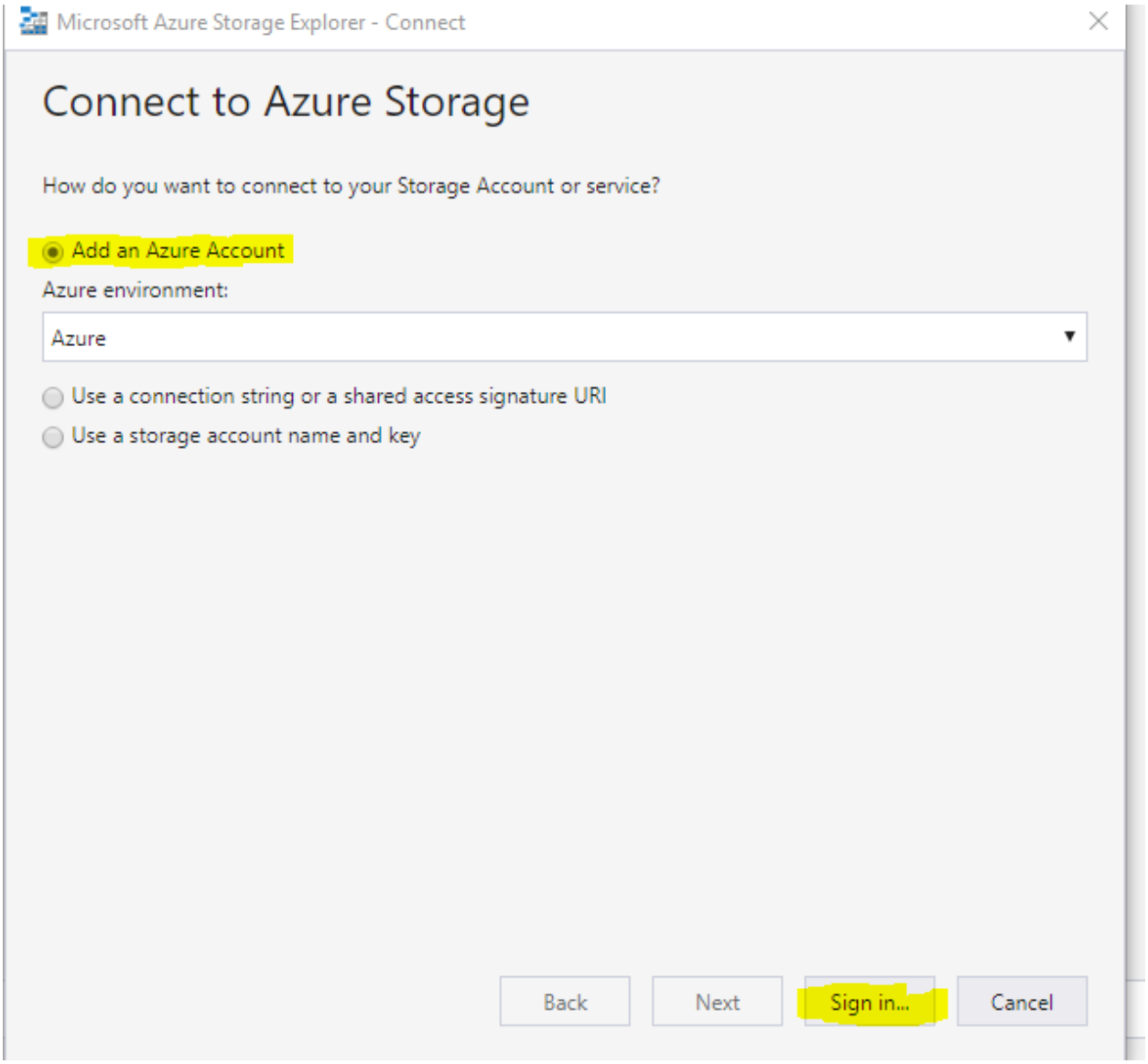
Search for Storage Account and click create, and fill in the required details with the following:

- Name: “gib2018labs<yourname>storage”
- Deployment model (Resource manager)
- Account kind: “Storage(General purpose v1)
- Performance (Standard)
- Replication (Read-access geo-redundant storage (RA-GRS))
- Secure transfer required (Disabled)

- Subscription: <Use the same subscription as per “GIB2018-Labs-UserRG”>
- Resource group (Use existing): GIB2018-Labs-UserRG
- Location: Australia East
- Configure virtual networks (Disabled)

Wait for the deployment to complete.

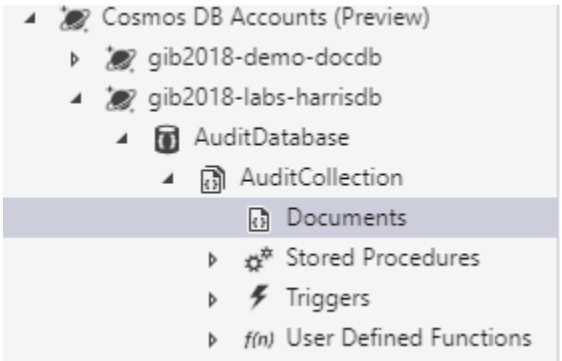
Open Azure Storage Explorer, click on the  icon on the left hand corner, click “Add an account”, the pop-up below should then appear.



Sign in using your Office365/Microsoft account.

Click on the  icon on the left hand corner, you should now see your Azure subscription with its resources.

Select your Azure subscription > Cosmos DB accounts (Preview) > gib2018-labs-<yourname>db > AuditDatabase > AuditCollection > Documents



Verify that the audit logs has been successfully written to Cosmos DB


```
1 {
2     "body": "
{\"subject\":\"/subscriptions/da0aec67-4acd-4c64-82f6-a080dd9beada/resourceGroups/GIB2018-Labs-UserRG/providers/Microsoft.EventGrid/eventSubscriptions/LogicAppcf1848d0-0b1c-
9e-b14e-c6daf0ef425e\",\"eventType\":\"Microsoft.Resources.ResourceWriteSuccess\",\"eventTime\":\"2018-03-22T19:24:48.831563Z\",
\"id\":\"067313d6-6169-421a-8c90-8879d096ccd4\",\"data\":{\"authorization\":\"
{\\\"scope\\\":\\\"/subscriptions/da0aec67-4acd-4c64-82f6-a080dd9beada/resourceGroups/GIB2018-Labs-UserRG/providers/Microsoft.
EventGrid/eventSubscriptions/LogicAppcf1848d0-0b1c-429e-b14e-c6daf0ef425e\\\",\\\"action\\\":\\\"Microsoft.EventGrid/eventSubscriptions/write\\\",\\\"evidence\\\":
{\\\"role\\\":\\\"Subscription Admin\\\"}}\",\"claims\":\"{\\\"aud\\\":\\\"https://management.core.windows.net/\\\",
\\\"iss\\\":\\\"https://sts.windows.net/977d1ffe-13ee-4afb-9163-800e7c8929d4/\\\",\\\"iat\\\":\\\"1521746370\\\",\\\"nbf\\\":\\\"1521746370\\\",\\\"exp\\\":\\\"1521750270\\\
\\\"http://schemas.microsoft.com/claims/authnclassreference\\\":\\\"1\\\",\\\"aio\\\":\\\"Y2NgYFjmkZLe9cgy7aaZVN69guOPTfhuO9okhDBNnzAt8bn+/a8A\\\",
\\\"altsecid\\\":\\\"1:live.com:00034001CBEC2550\\\",\\\"http://schemas.microsoft.com/claims/authnmethodsreferences\\\":\\\"pwd\\\",
\\\"appid\\\":\\\"7ab7862c-4c57-491e-8a45-d52a7e023983\\\",\\\"appidacr\\\":\\\"2\\\",\\\"e_exp\\\":\\\"262800\\\",
\\\"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress\\\":\\\"mr.kristanto@gmail.com\\\",
\\\"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname\\\":\\\"Kristanto\\\",\\\"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname\\\":\\\"Harris\\\
\\\"groups\\\":\\\"2b6e0861-d2c3-440e-af8a-c92a206686d4\\\",\\\"http://schemas.microsoft.com/identity/claims/identityprovider\\\":\\\"live.com\\\",
\\\"ipaddr\\\":\\\"49.50.214.17\\\",\\\"name\\\":\\\"Harris Kristanto\\\",
\\\"http://schemas.microsoft.com/identity/claims/objectidentifier\\\":\\\"f15a6112-a923-4ecf-bcea-b1f60bb5fbc7\\\",\\\"puid\\\":\\\"1003000099D1F289\\\",
\\\"http://schemas.microsoft.com/identity/claims/scope\\\":\\\"user_impersonation\\\",
\\\"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier\\\":\\\"6kF3somgPMOxDY3afetPJ4p569B3kC2o6ASRUJVL7u0\\\",
\\\"http://schemas.microsoft.com/identity/claims/tenantid\\\":\\\"977d1ffe-13ee-4afb-9163-800e7c8929d4\\\",
\\\"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name\\\":\\\"live.com#mr.kristanto@gmail.com\\\",\\\"uti\\\":\\\"t1VREQZZLEiSJfYQO6U-AA\\\",\\\"ver\\\":\\\"1.0\\\"
\\\"wids\\\":\\\"62e90394-69f5-4237-9190-012177145e10\\\"}\",\"correlationId\":\"826d3ff5-c54e-4490-8cb5-96602007e31e\",\"httpRequest\":\"\",
\"resourceProvider\":\"Microsoft.EventGrid\",
\"resourceUri\":\"/subscriptions/da0aec67-4acd-4c64-82f6-a080dd9beada/resourceGroups/GIB2018-Labs-UserRG/providers/Microsoft.EventGrid/eventSubscriptions/LogicAppcf1848d0-0b
-429e-b14e-c6daf0ef425e\",\"operationName\":\"Microsoft.EventGrid/eventSubscriptions/write\",\"status\":\"Succeeded\",
\"subscriptionId\":\"da0aec67-4acd-4c64-82f6-a080dd9beada\",\"tenantId\":\"977d1ffe-13ee-4afb-9163-800e7c8929d4\"},\"dataVersion\":\"\",\"metadataVersion\":\"1\",
\"topic\":\"/subscriptions/da0aec67-4acd-4c64-82f6-a080dd9beada/resourceGroups/GIB2018-Labs-UserRG\"}",
3     "eventTime": "2018-03-22T19:24:48.831563Z",
4     "eventType": "Microsoft.Resources.ResourceWriteSuccess",
5     "id": "067313d6-6169-421a-8c90-8879d096ccd4",
6     "messageType": "Audit",
7     "subject":
"/subscriptions/da0aec67-4acd-4c64-82f6-a080dd9beada/resourceGroups/GIB2018-Labs-UserRG/providers/Microsoft.EventGrid/eventSubscriptions/LogicAppcf1848d0-0b1c-429e-b14e-c6da
ef425e.",
```