Get control of your Azure Synapse environment, define your access control the right way today!

Erwin de Kreuk

Principal Consultant – Lead Data & AI
InSpark

Erwin de Kreuk

Principal Consultant – Lead Data & AI
InSpark

@erwindekreuk

linkedin.com/in/erwindekreuk

erwindekreuk.com github.com/edkreuk

MVP Microsoft® Most Valuable Professional

We Are InSpark

We help organizations **accelerating** their **digital transformation** with impactful Microsoft solutions & expertise

INSPARK

SQL Day

15 edycja konferencji SQLDay

8-10 maja 2023, WROCŁAW + ONLINE

Data Community

partner złoty

Future Processing

partner srebrny

Objectivity

summ-it

kursySQL.pl

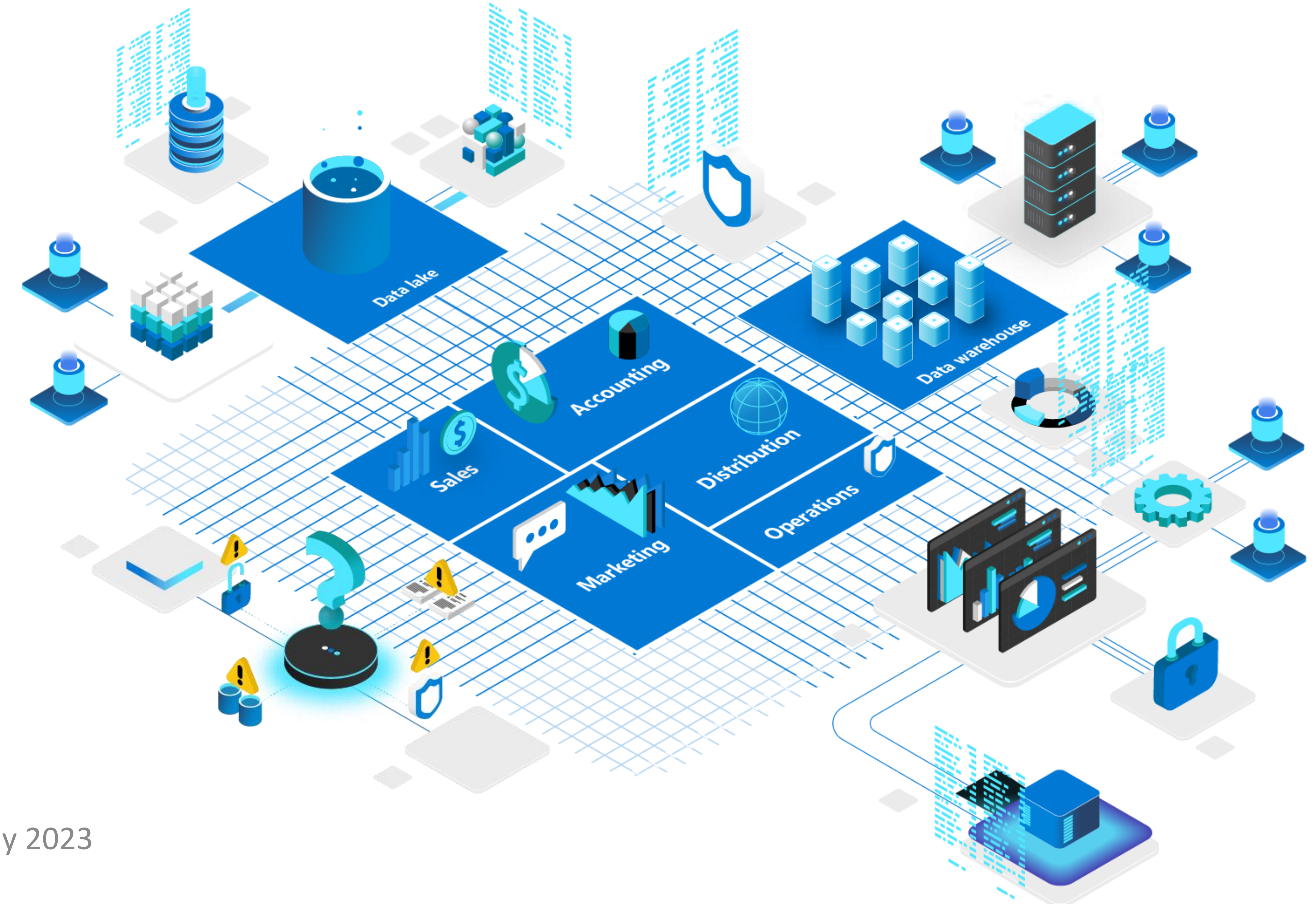
VOLVO

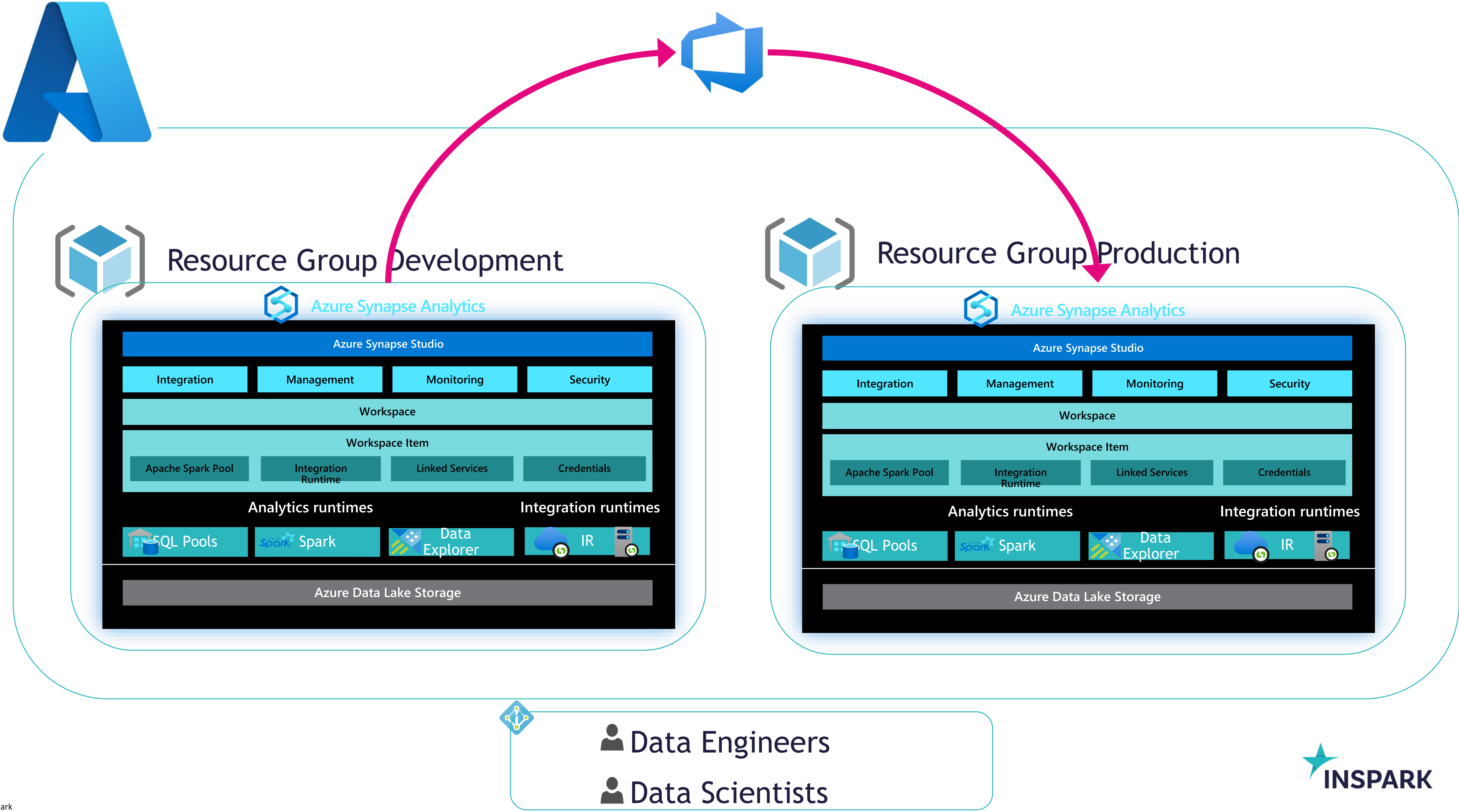
partner brązowy

devart

AGENDA

- Roles in Azure Synapse Analytics
  - Azure
  - Synapse
  - SQL
- Git Integration
- Privileged Identity Management (PIM)





Resource Group Development

Azure Synapse Analytics

- Azure Synapse Studio
- Integration | Management | Monitoring | Security
- Workspace
- Workspace Item: Apache Spark Pool | Integration Runtime | Linked Services | Credentials
- Analytics runtimes: SQL Pools | Spark | Data Explorer
- Integration runtimes: IR
- Azure Data Lake Storage

Resource Group Production

Azure Synapse Analytics

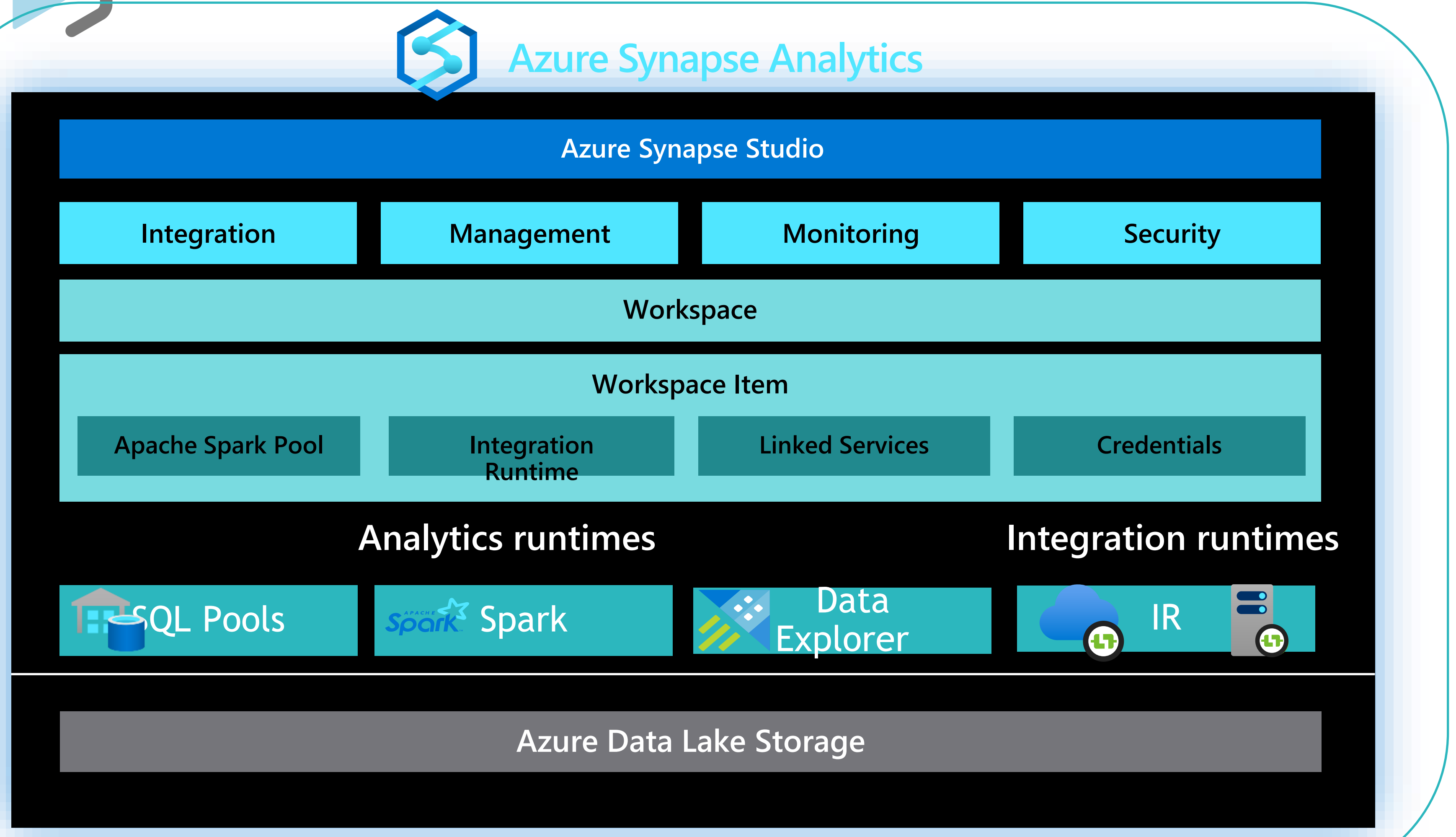
- Azure Synapse Studio
- Integration | Management | Monitoring | Security
- Workspace
- Workspace Item: Apache Spark Pool | Integration Runtime | Linked Services | Credentials
- Analytics runtimes: SQL Pools | Spark | Data Explorer
- Integration runtimes: IR
- Azure Data Lake Storage

Data Engineers

Data Scientists

INSPARK

Resource Group Development



Azure Synapse Analytics

Azure Synapse Studio

Integration | Management | Monitoring | Security

Workspace

Workspace Item

Apache Spark Pool | Integration Runtime | Linked Services | Credentials

Analytics runtimes

SQL Pools | Spark | Data Explorer

Integration runtimes

IR

Azure Data Lake Storage

Azure Roles

Resource Plane

- Azure Owner or Contributor

  Resource Group

  Create Synapse Workspace

  Manage Synapse Workspace

  Synapse Resource

  Manage Synapse Workspace

- Azure Contributor

  Resource Group

  ARM templates for automated deployment

Resource Group Development
Azure Synapse Analytics

Azure Roles

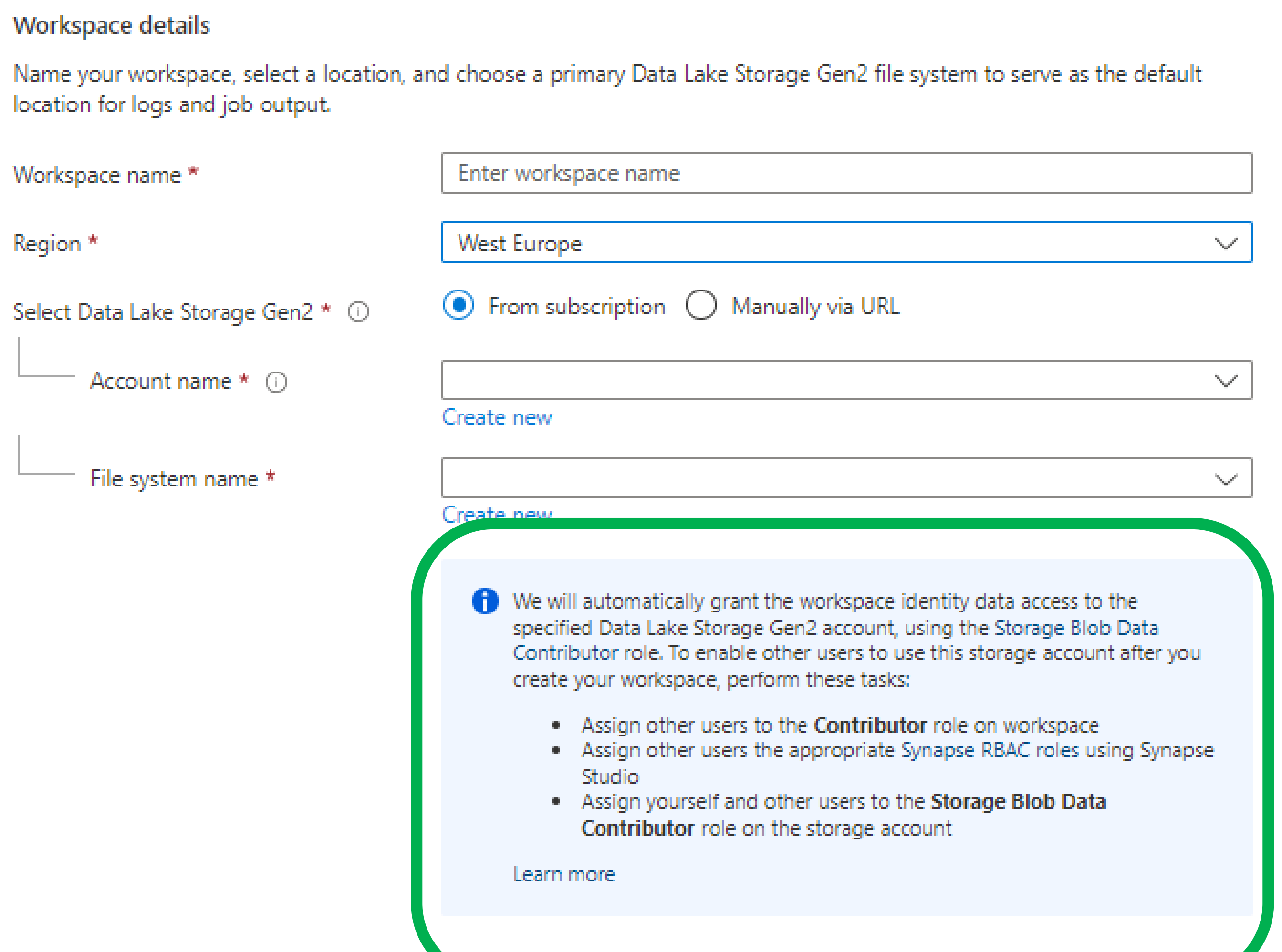
Access Management

- Azure Storage Blob Data Contributor

  User and workspace MSI

- Reader

  Resource Group or Synapse Workspace



Workspace details

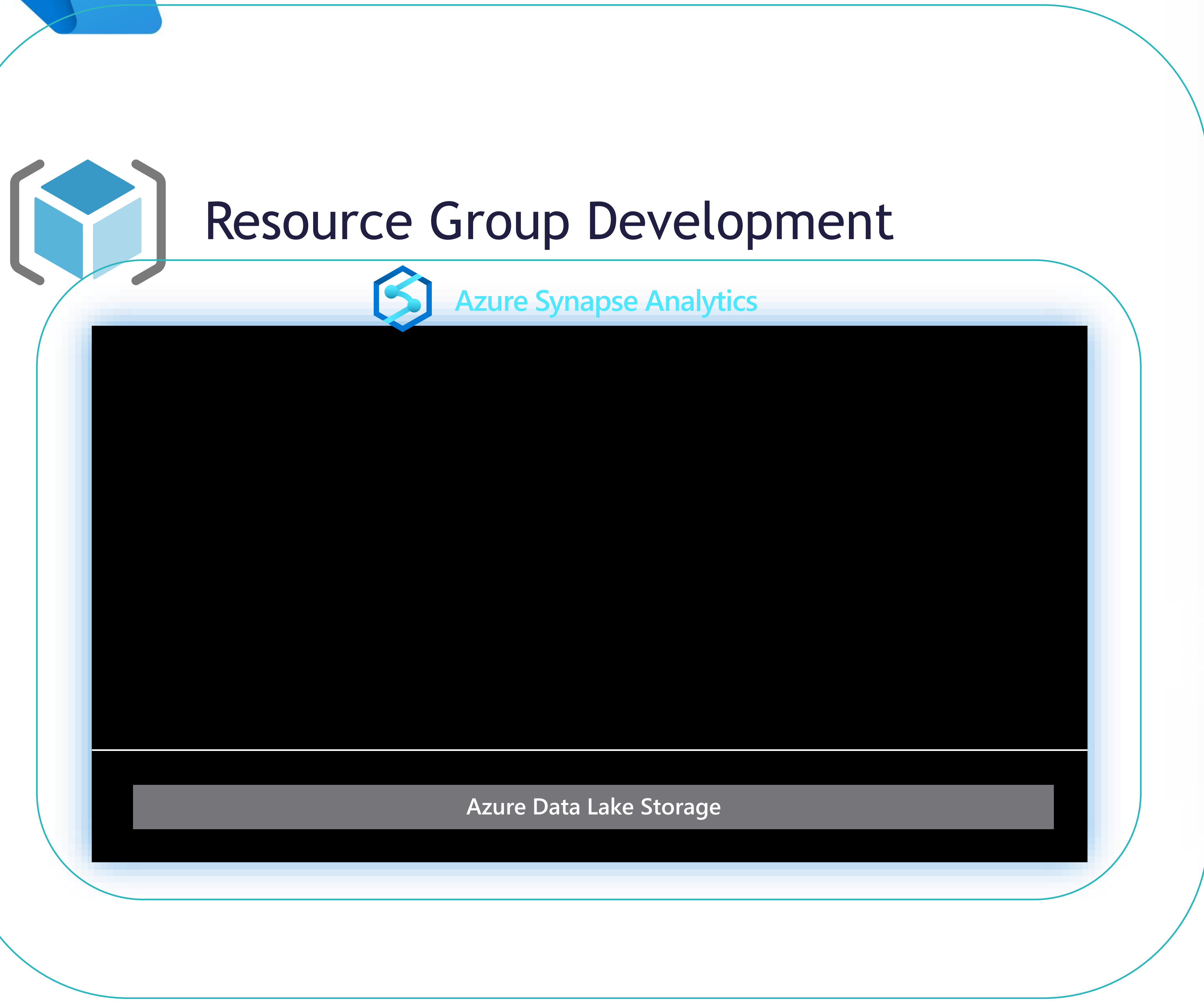
Name your workspace, select a location, and choose a primary Data Lake Storage Gen2 file system to serve as the default location for logs and job output.

Workspace name *	Enter workspace name
Region *	West Europe
Select Data Lake Storage Gen2 *	● From subscription ○ Manually via URL
Account name *	 Create new
File system name *	 Create new

We will automatically grant the workspace identity data access to the specified Data Lake Storage Gen2 account, using the Storage Blob Data Contributor role. To enable other users to use this storage account after you create your workspace, perform these tasks:

- Assign other users to the **Contributor** role on workspace
- Assign other users the appropriate Synapse RBAC roles using Synapse Studio
- Assign yourself and other users to the **Storage Blob Data Contributor** role on the storage account

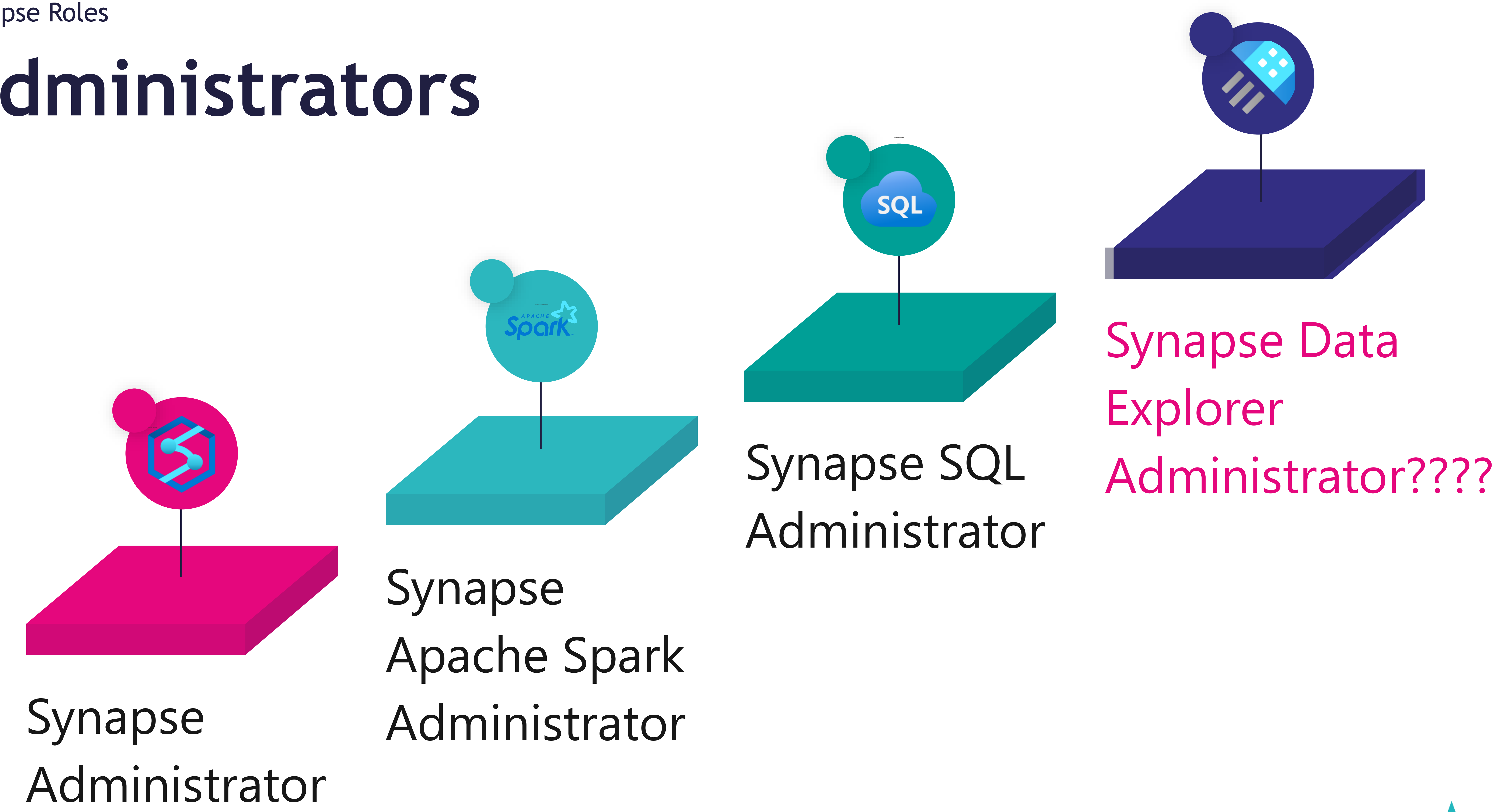
Learn more



INSPARK

Synapse Roles

Administrators



Synapse Administrator

Synapse Apache Spark Administrator

Synapse SQL Administrator

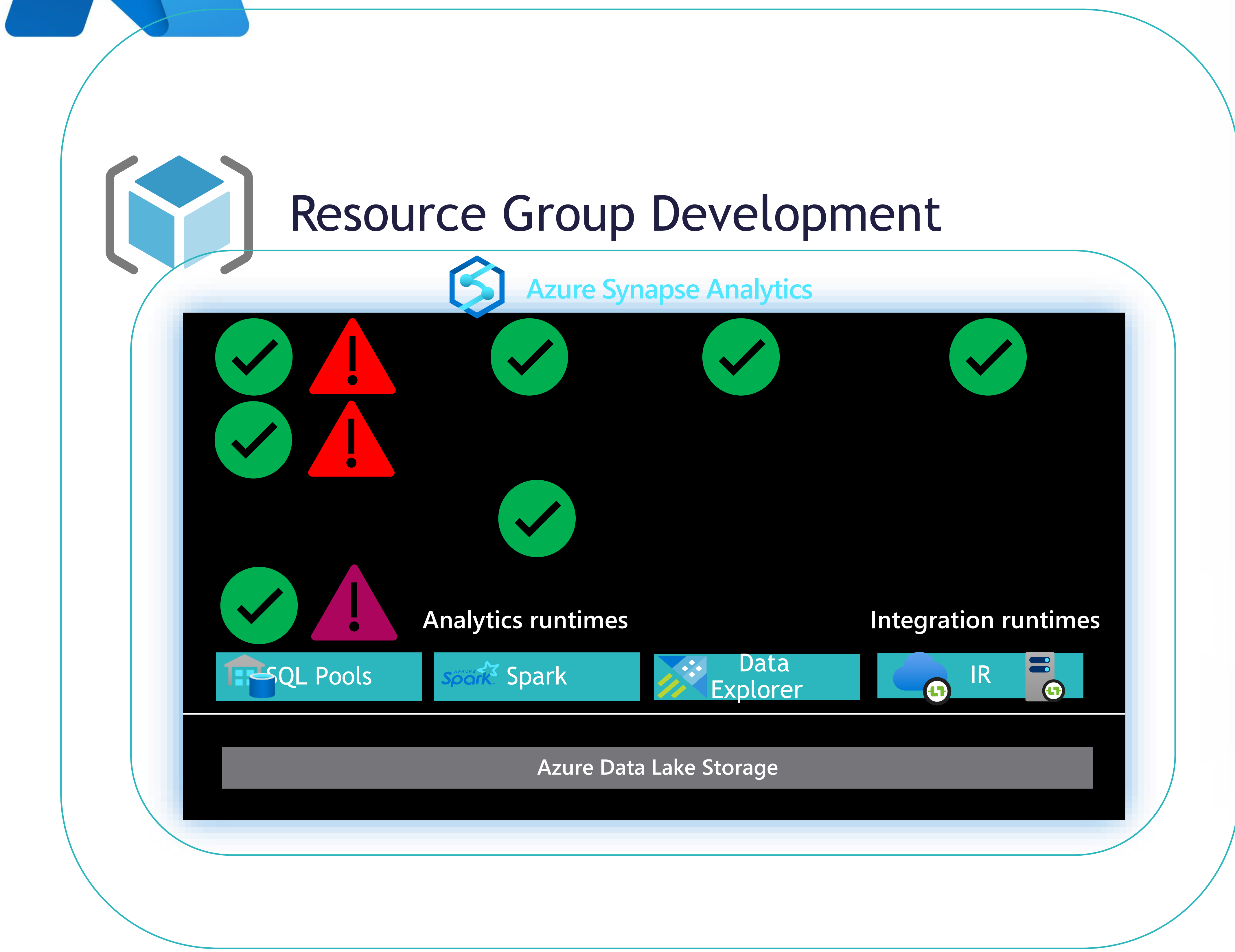
Synapse Data Explorer Administrator????

Synapse Roles

Administrators

Roles:

- Synapse Administrator
- Synapse SQL Administrator
- Synapse Apache Spark Administrator
- SQL Active Directory Admin



⚠ Only Serverless SQL Pool

⚠ Only dedicated SQL Pools

INSPARK

Synapse Roles

Synapse Administrator

- Can read and write artifacts
- Can do all actions on Spark activities.
- Can view Spark pool logs
- Can view saved notebook and pipeline output
- Can use the secrets stored by linked services or credentials
- Can assign and revoke Synapse RBAC roles at current scope

Synapse Roles

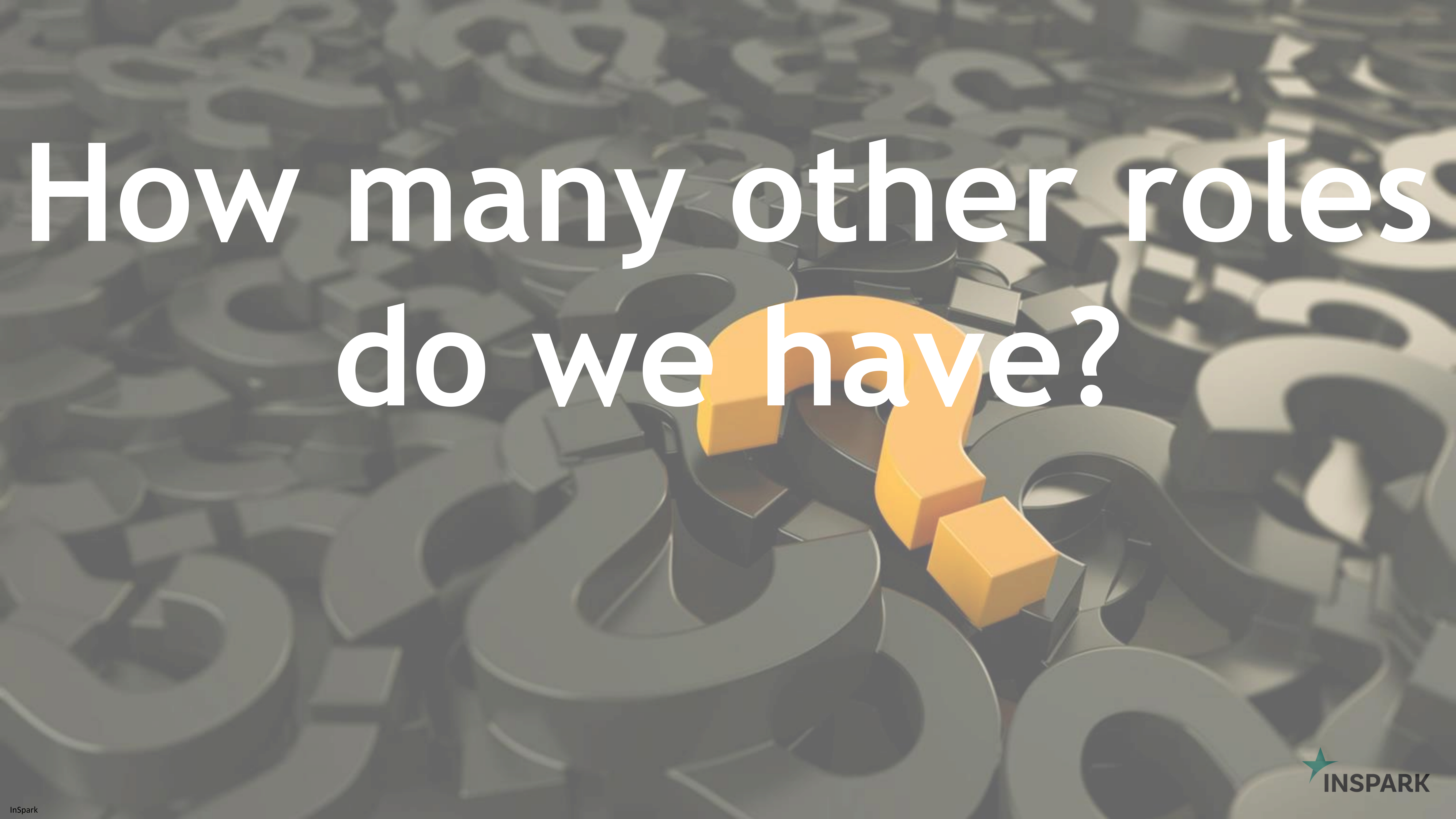
Synapse Apache Spark Administrator

- Can do all actions on Spark artifacts
- Can do all actions on Spark activities

Synapse SQL Administrator

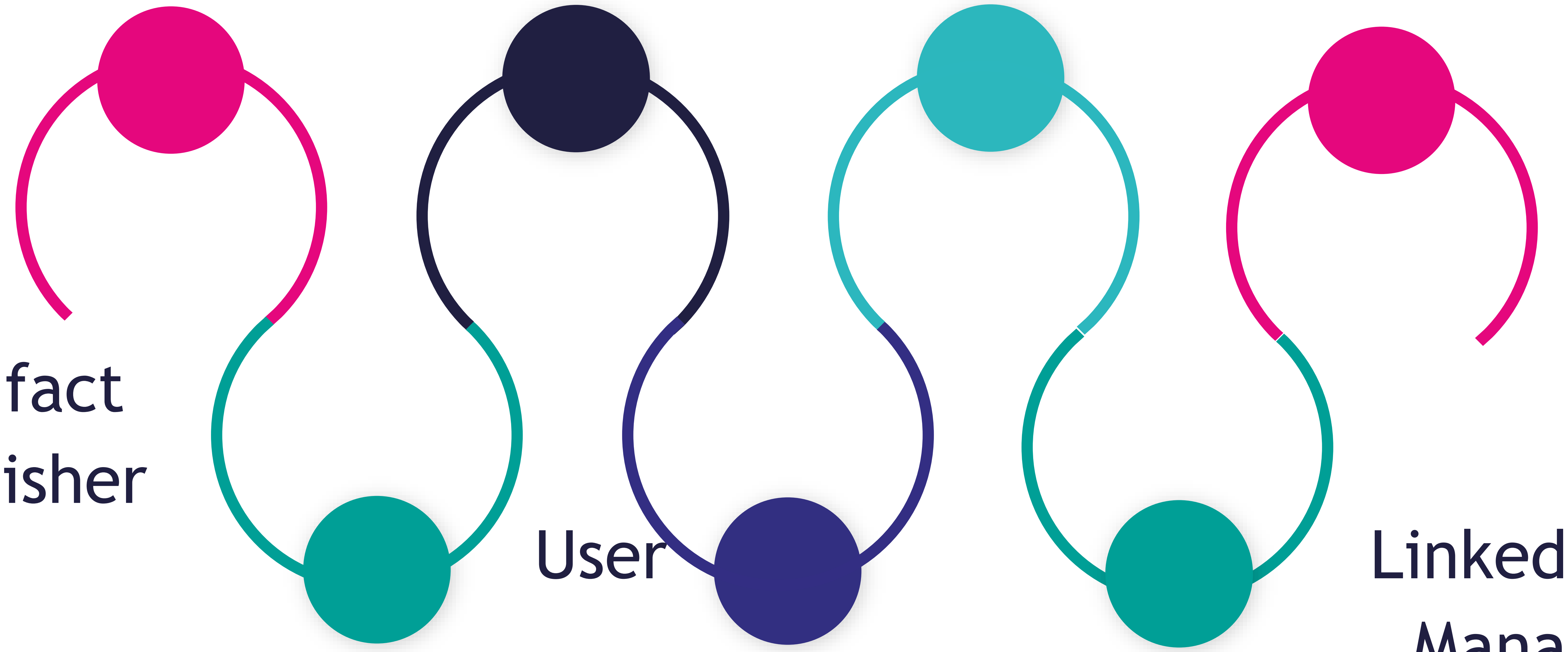
- Can do all actions on SQL scripts
- Can connect to SQL serverless endpoints with SQL db_datareader, db_datawriter, connect, and grant permissions

How many other roles do we have?



Synapse Roles

Non-Administrators



Contributor

Artifact Publisher

Artifact User

User

Compute/ Monitor Operator

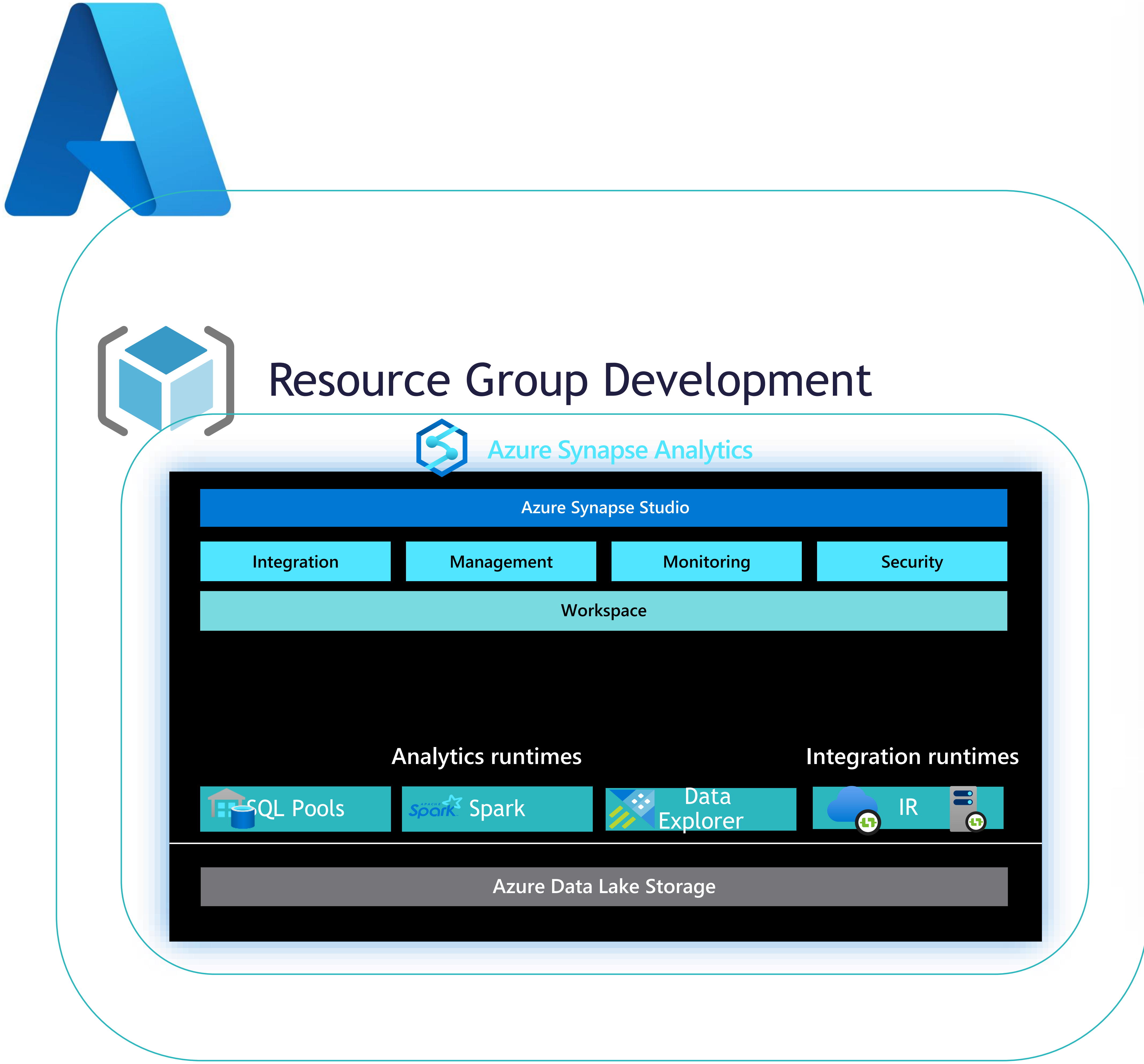
Linked Data Manager

Credential User

Synapse Roles

Workspace

- Synapse Contributor
- Synapse Artifact Publisher
- Synapse Artifact User
- Synapse Compute Operator
- Synapse Monitor Operator
- Synapse Credential User
- Synapse Linked Data Manager
- Synapse User



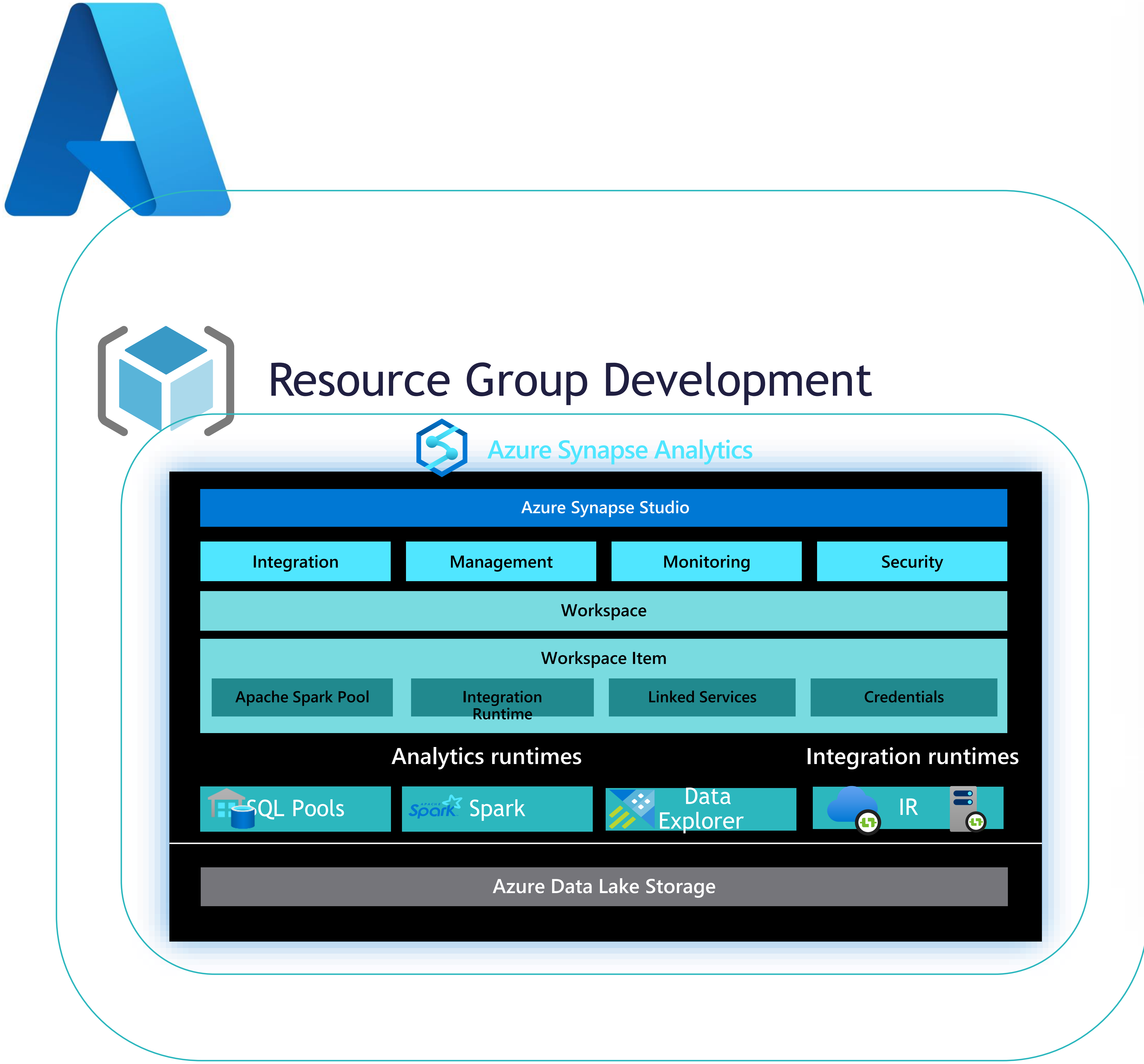
Workspace

	Can list and read Spark pools, Integration runtimes.	Can view Spark pool logs	Can submit and cancel jobs	Can read published artifacts	Can published artifacts	Can view saved notebook and pipeline output	Can view Spark pool logs	Can do all actions on Spark activities	Create Managed Vnet, Linked Service and credentials
User	✓								
Linked Data Manager	✓								✓
Credential User	✓								
Compute Operator	✓								
Artifact User	✓								
Artifact Publisher	✓								
Contributor	✓								

Synapse Roles

Workspace Item

- Linked Service
- Apache Spark Pool
- Integration Runtime
- Credentials



INSPARK

Synapse Roles

Role Assignment

- Role assignment on Workspace or Workspace Item
- Needs to be Synapse Administrator

  Can also be a guest user

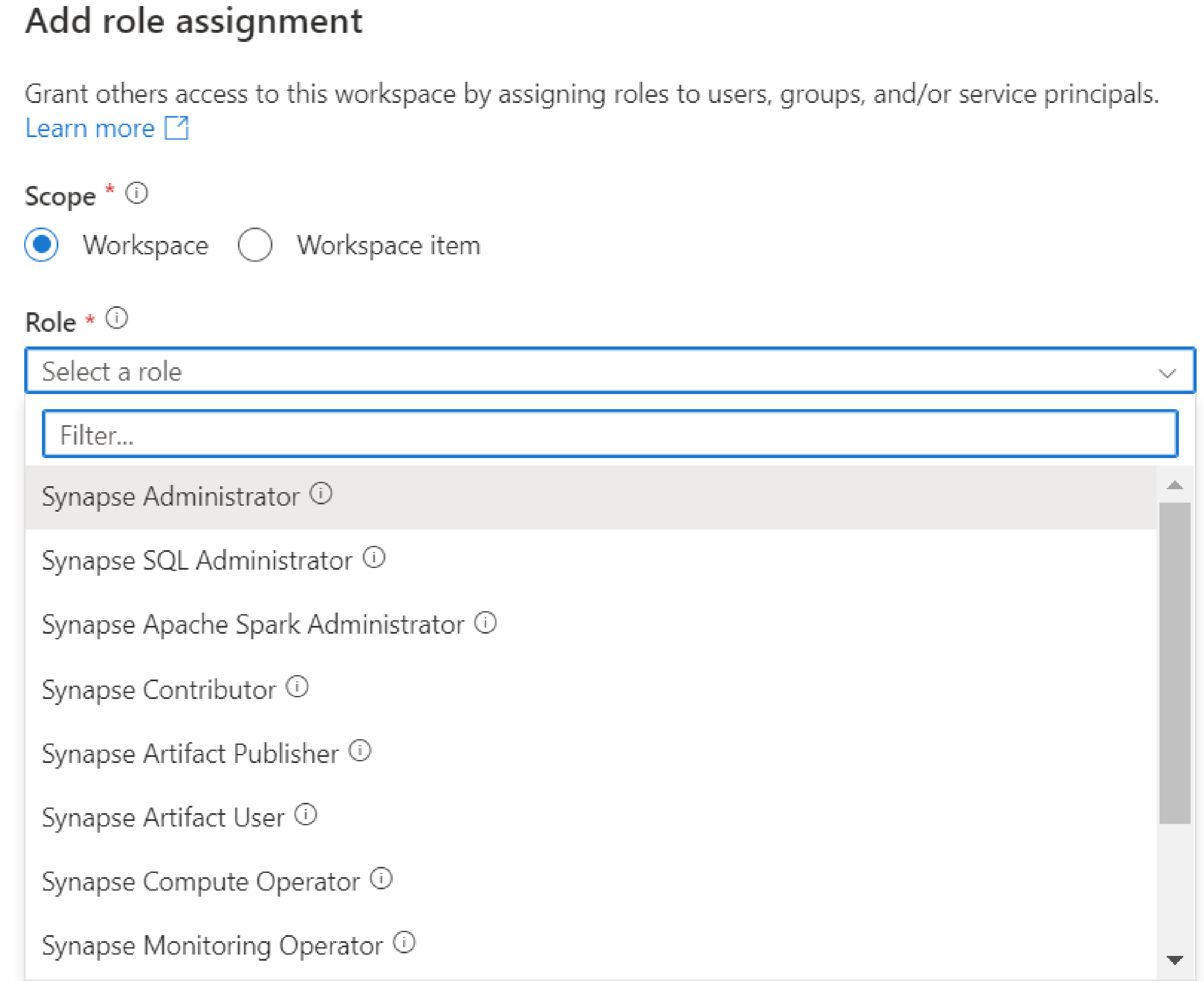
- No Synapse Administrator

  Contributor or Owner on the Workspace

- Advice! => create role assignments based on Security Groups

  Changes in assignments will take up 2-5 minutes

  Changes in SG can take 10-15 minutes



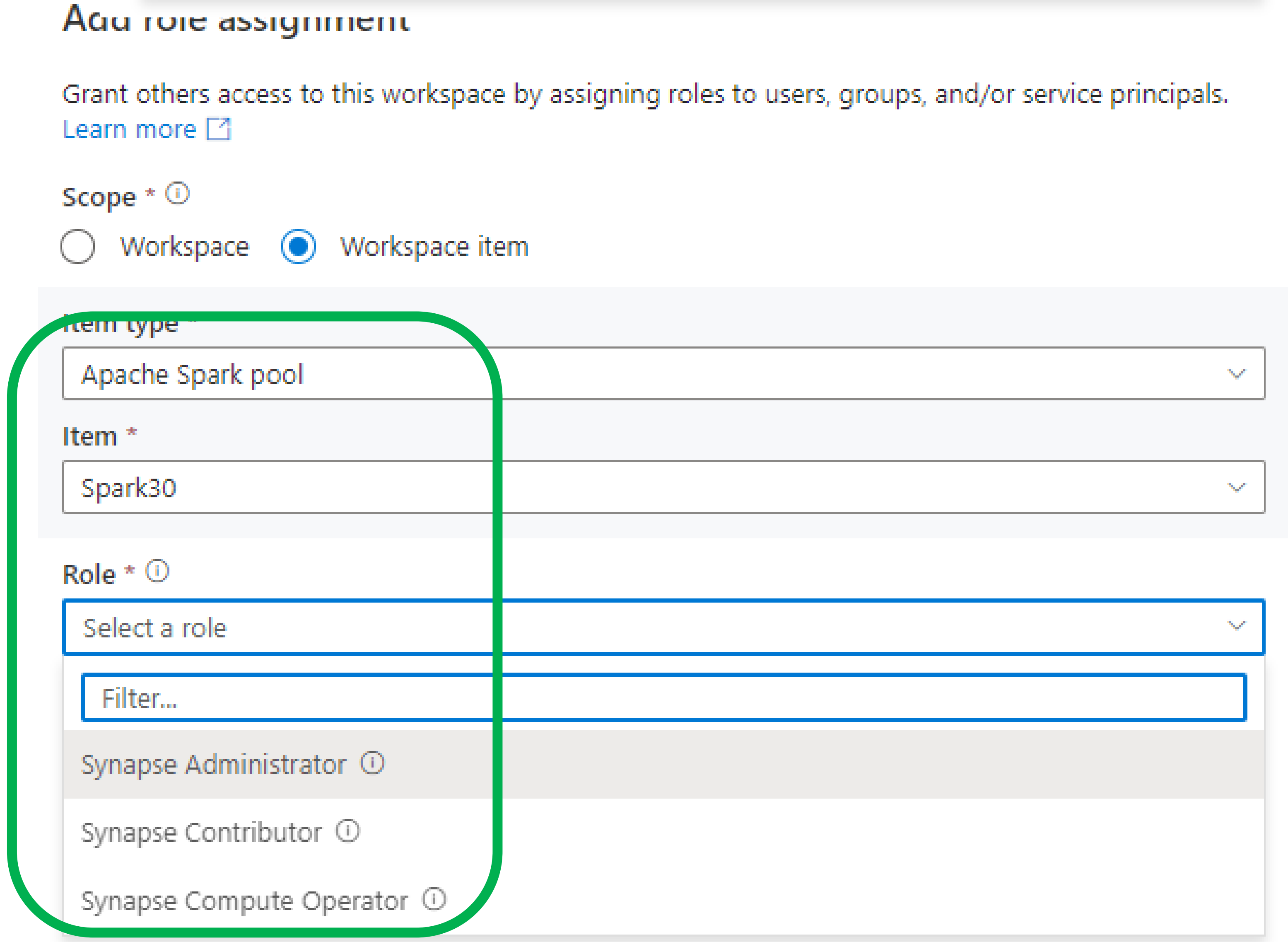
Add role assignment

Grant others access to this workspace by assigning roles to users, groups, and/or service principals.
Learn more

Scope *
● Workspace ○ Workspace item

Role *
Select a role
Filter...

- Synapse Administrator
- Synapse SQL Administrator
- Synapse Apache Spark Administrator
- Synapse Contributor
- Synapse Artifact Publisher
- Synapse Artifact User
- Synapse Compute Operator
- Synapse Monitoring Operator



Add role assignment

Grant others access to this workspace by assigning roles to users, groups, and/or service principals.
Learn more

Scope *
○ Workspace ● Workspace item

Item type
Apache Spark pool

Item *
Spark30

Role *
Select a role
Filter...

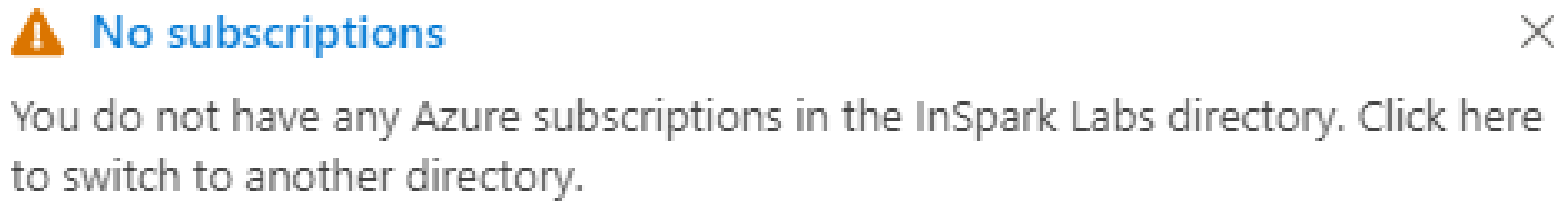
- Synapse Administrator
- Synapse Contributor
- Synapse Compute Operator

Synapse Roles

Tips and Tricks

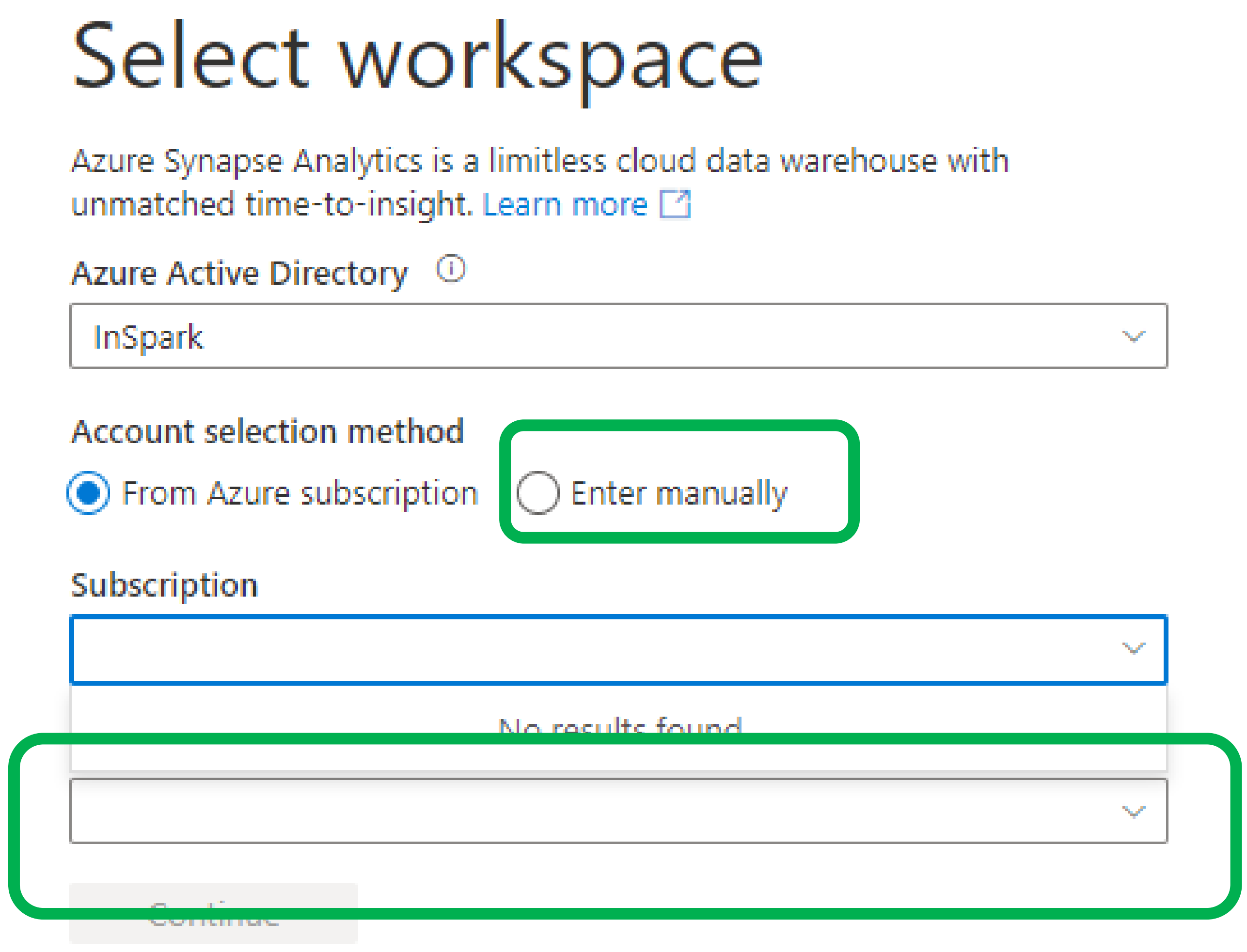
- No access message in Azure Portal

https://web.azuresynapse



⚠ No subscriptions

You do not have any Azure subscriptions in the InSpark Labs directory. Click here to switch to another directory.



Select workspace

Azure Synapse Analytics is a limitless cloud data warehouse with unmatched time-to-insight. Learn more

Azure Active Directory ⓘ

InSpark

Account selection method

● From Azure subscription ○ Enter manually

Subscription

No results found

Continue

Synapse Roles

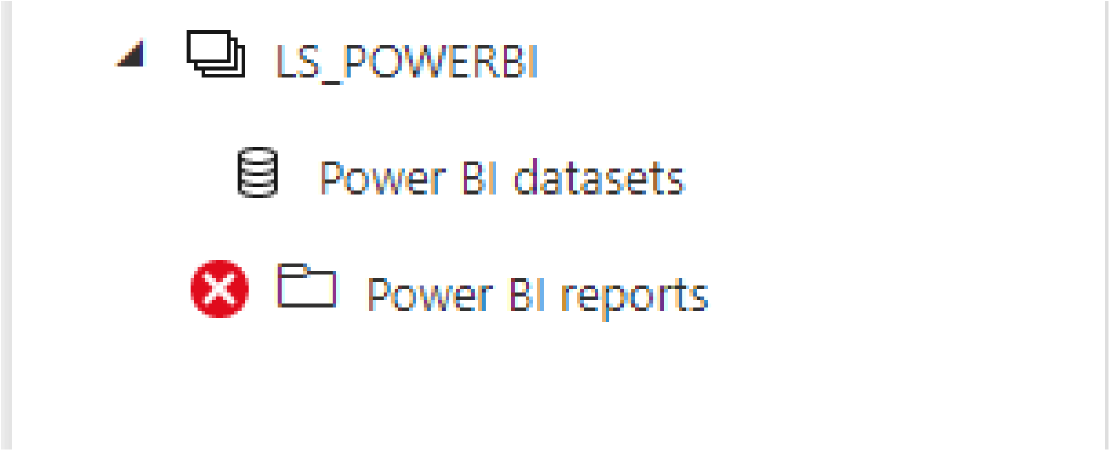
Tips and Tricks

- No access message in Azure Portal

  https://web.azuresynapse

- Power BI

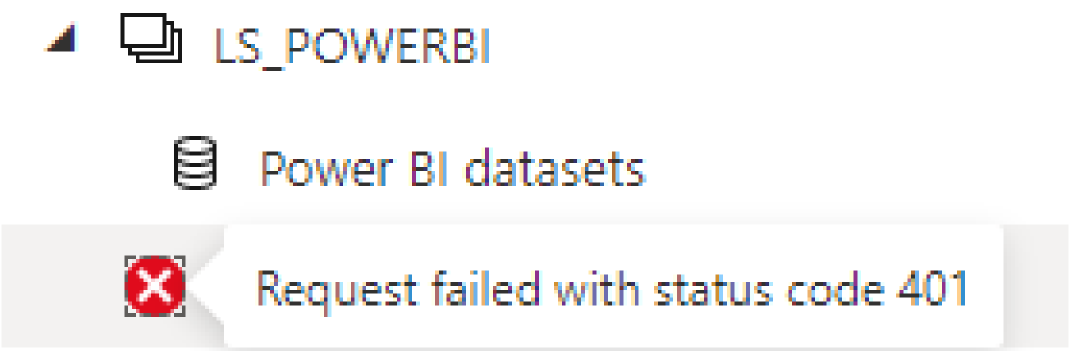
  Access is defined on Power BI workspace level



LS_POWERBI

Power BI datasets

Power BI reports



LS_POWERBI

Power BI datasets

Request failed with status code 401

Synapse Roles

Tips and Tricks

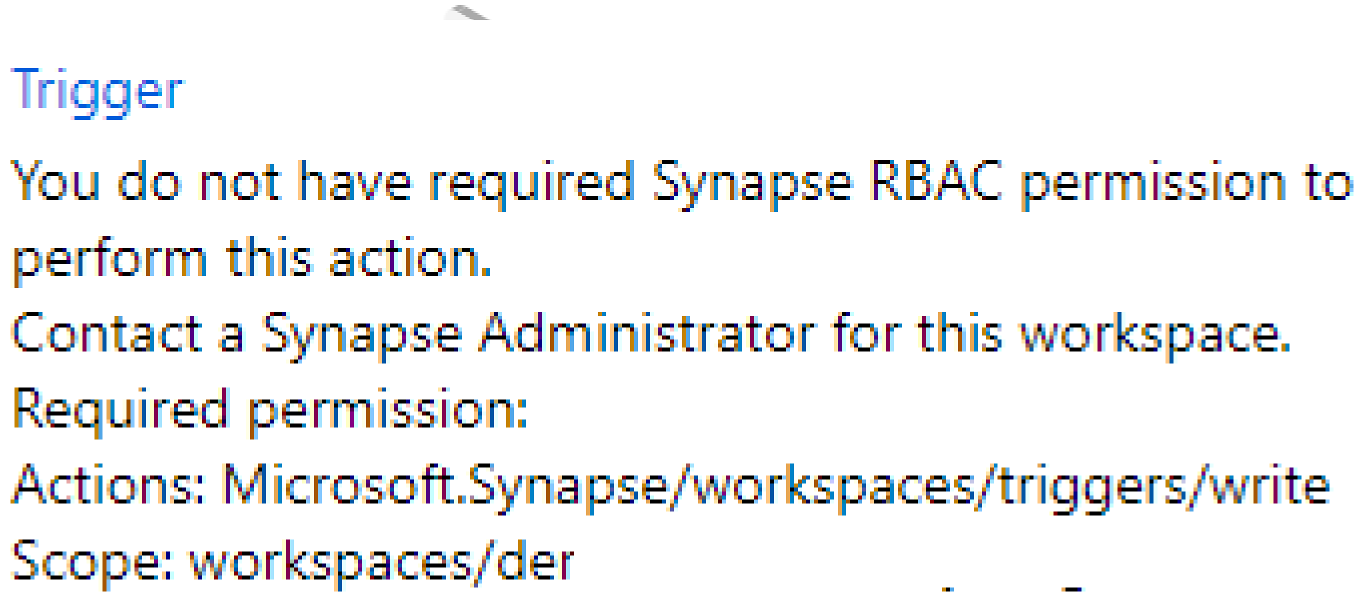
- No access message in Azure Portal

https://web.azuresynapse

- Power BI

Access is defined on Power BI workspace level

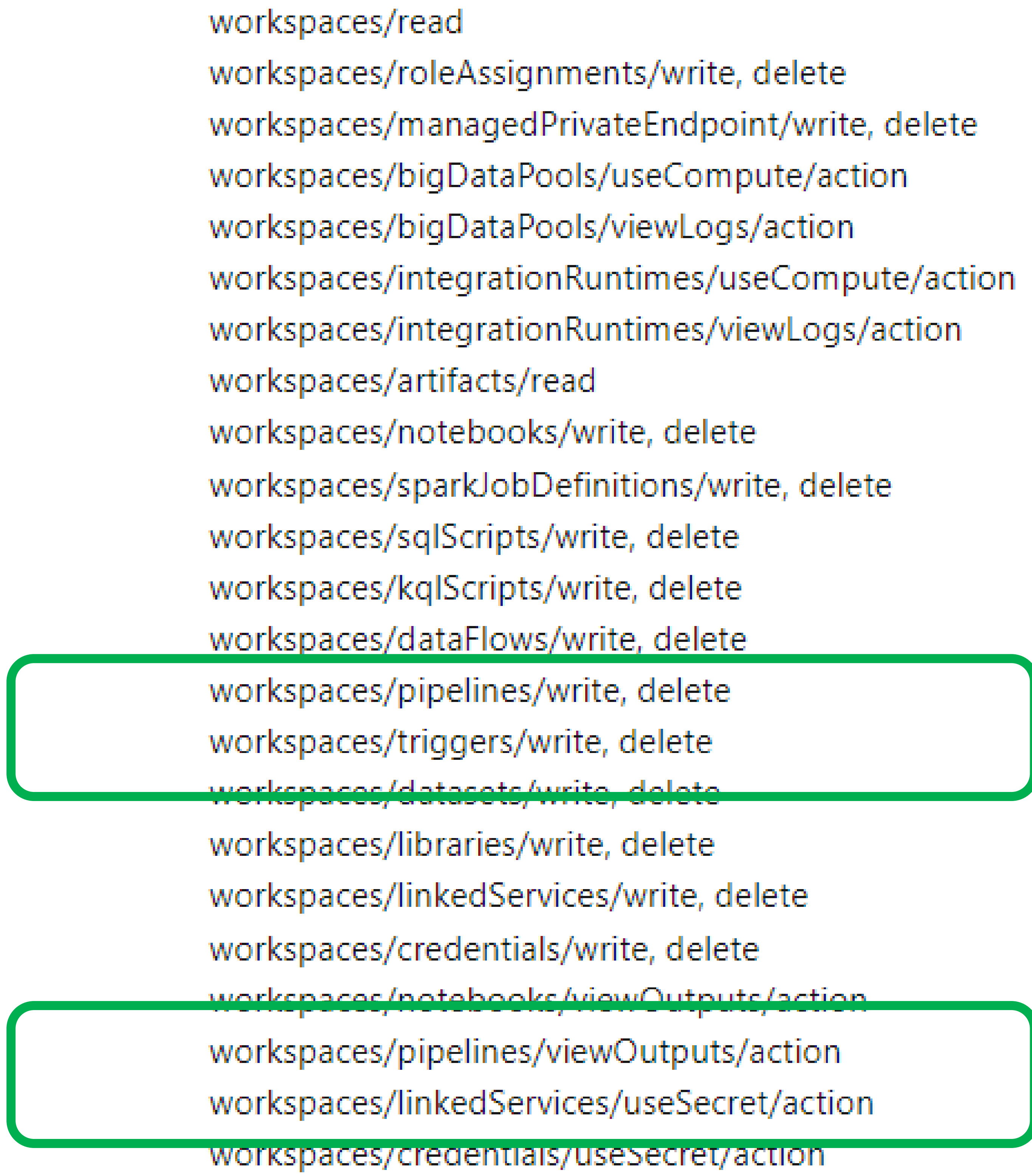
- Publish Error



Trigger

You do not have required Synapse RBAC permission to perform this action.
Contact a Synapse Administrator for this workspace.
Required permission:
Actions: Microsoft.Synapse/workspaces/triggers/write
Scope: workspaces/der

Synapse Administrator



workspaces/read
workspaces/roleAssignments/write, delete
workspaces/managedPrivateEndpoint/write, delete
workspaces/bigDataPools/useCompute/action
workspaces/bigDataPools/viewLogs/action
workspaces/integrationRuntimes/useCompute/action
workspaces/integrationRuntimes/viewLogs/action
workspaces/artifacts/read
workspaces/notebooks/write, delete
workspaces/sparkJobDefinitions/write, delete
workspaces/sqlScripts/write, delete
workspaces/kqlScripts/write, delete
workspaces/dataFlows/write, delete
workspaces/pipelines/write, delete
workspaces/triggers/write, delete
workspaces/datasets/write, delete
workspaces/libraries/write, delete
workspaces/linkedServices/write, delete
workspaces/credentials/write, delete
workspaces/notebooks/viewOutputs/action
workspaces/pipelines/viewOutputs/action
workspaces/linkedServices/useSecret/action
workspaces/credentials/useSecret/action

Synapse Roles

Role actions

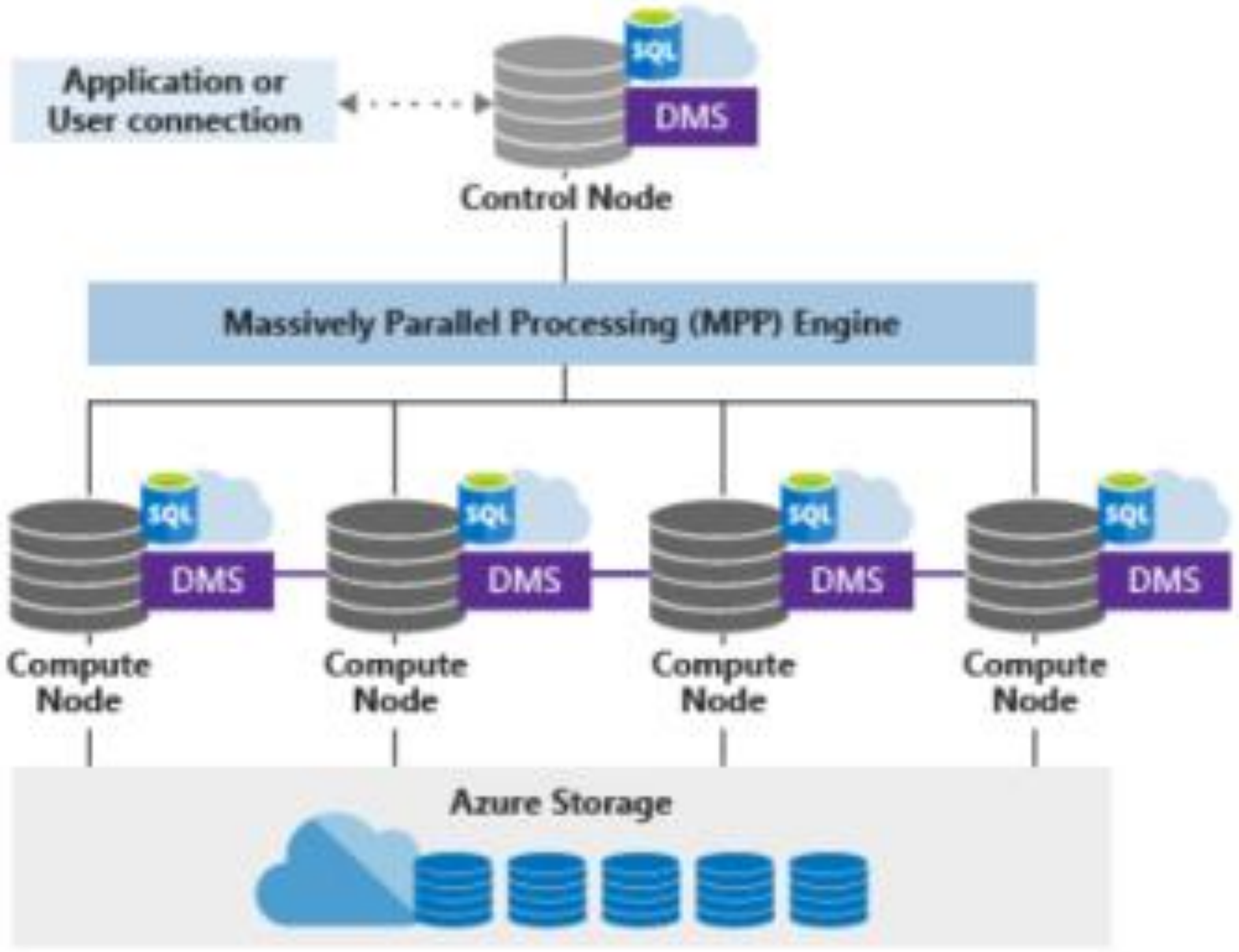
	Administrator	Contributor	Artifact Publisher	Apache Spark Administrator	SQL Administrator	Artifact User	Compute Operator	Credential User	Linked Data Manager	User
workspaces/read	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
workspaces/roleAssignments/write, delete	✓									
workspaces/managedPrivateEndpoint/write, delete	✓								✓	
workspaces/bigDataPools/useCompute/action	✓	✓		✓			✓			
workspaces/bigDataPools/viewLogs/action	✓	✓		✓			✓			
workspaces/integrationRuntimes/useCompute/action	✓	✓					✓			
workspaces/integrationRuntimes/viewLogs/action	✓	✓					✓			
workspaces/artifacts/read	✓	✓	✓	✓	✓	✓				
workspaces/notebooks/write, delete	✓	✓	✓	✓						
workspaces/sparkJobDefinitions/write, delete	✓	✓	✓	✓						
workspaces/sqlScripts/write, delete	✓	✓	✓		✓					
workspaces/kqlScripts/write, delete	✓	✓	✓							
workspaces/dataFlows/write, delete	✓	✓	✓							
workspaces/pipelines/write, delete	✓	✓	✓							
workspaces/triggers/write, delete	✓	✓	✓							
workspaces/datasets/write, delete	✓	✓	✓							
workspaces/libraries/write, delete	✓	✓	✓	✓	✓					
workspaces/linkedServices/write, delete	✓	✓	✓	✓	✓				✓	
workspaces/credentials/write, delete	✓	✓	✓	✓					✓	
workspaces/notebooks/viewOutputs/action	✓	✓	✓	✓		✓				
workspaces/pipelines/viewOutputs/action	✓	✓	✓			✓				
workspaces/linkedServices/useSecret/action	✓							✓		
workspaces/credentials/useSecret/action	✓							✓		

Demo

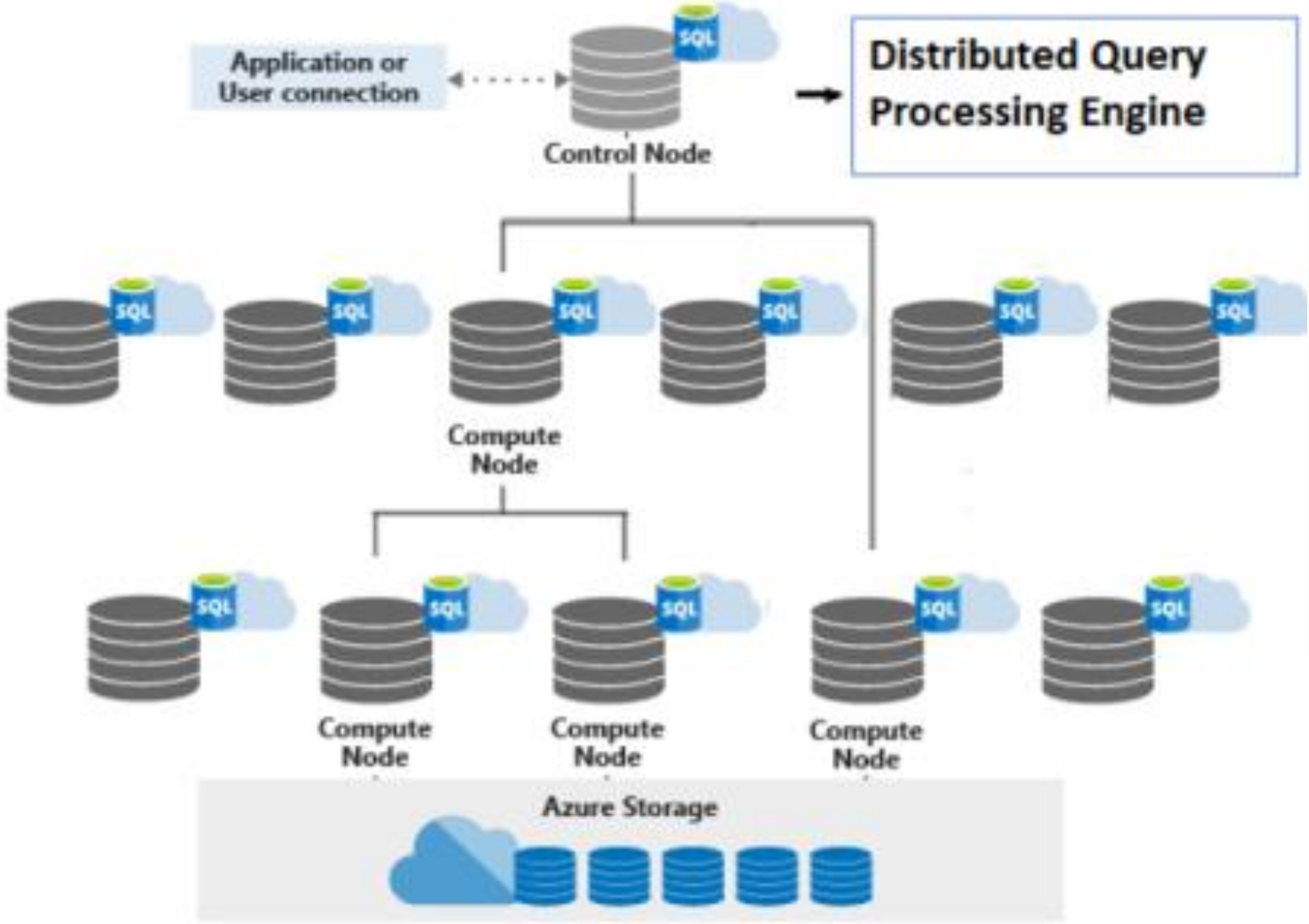
INSPARK

SQL

Dedicated SQL pool



Serverless SQL pool



Serverless SQL Pool

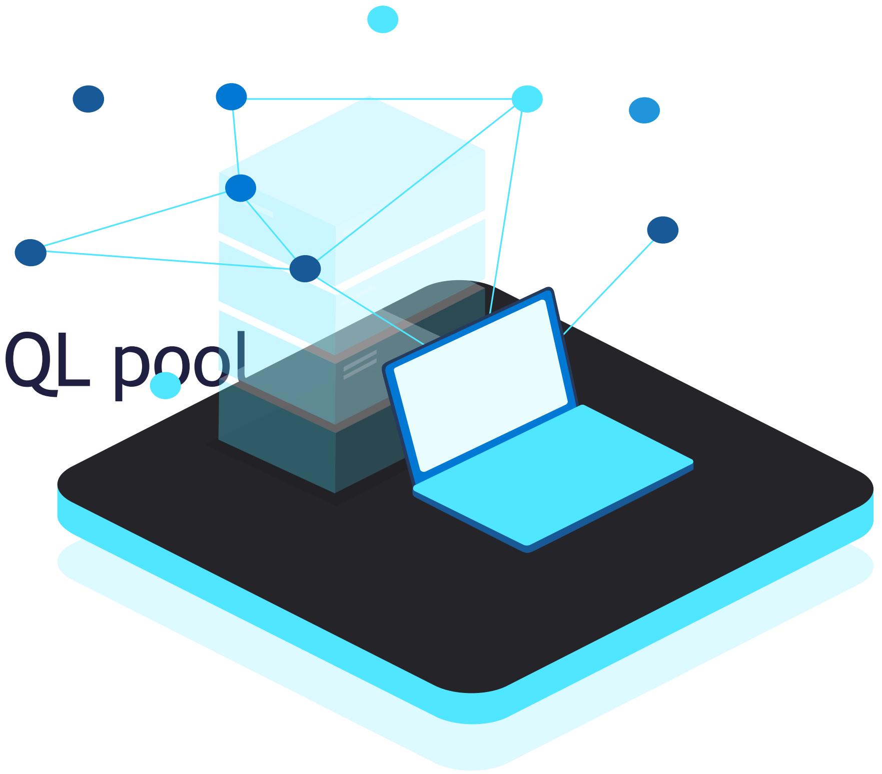
- Synapse Administrator

  db_owner (DBO) permissions on the 'Built-In' serverless SQL pool

- Synapse SQL Administrator

  Can do all actions on SQL scripts

  Can connect to SQL serverless endpoints with SQL db_datareader, db_datawriter, connect, and grant permissions



Serverless

SQL

Dedicated SQL Pool

- Synapse Administrator

  Full access to data in dedicated SQL pools

  Grant access to other users

  Perform configuration and maintenance activities

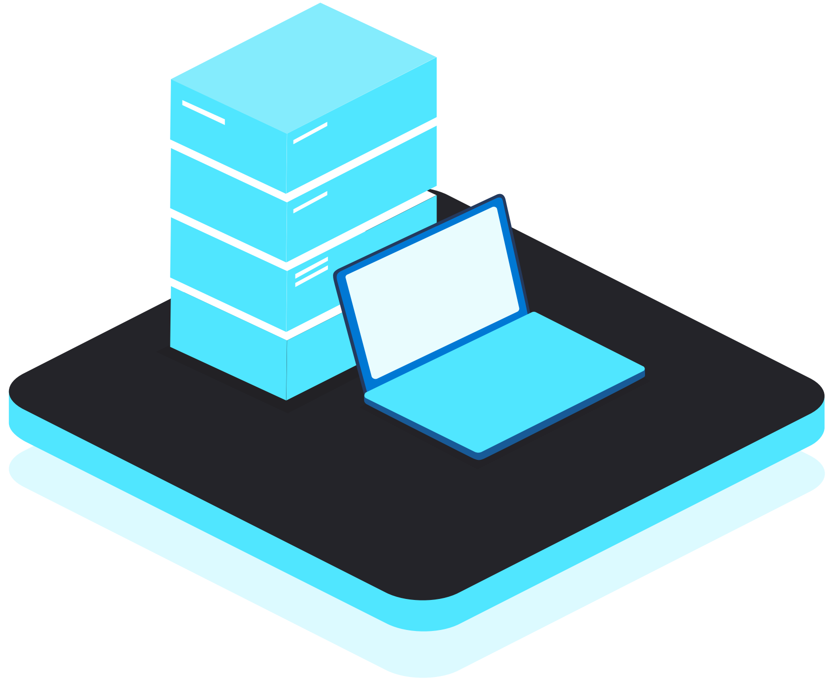
  Can't drop dedicated SQL pools

- Synapse SQL Administrator

  No access by default

- Active Directory Admin

  Full access



Dedicated

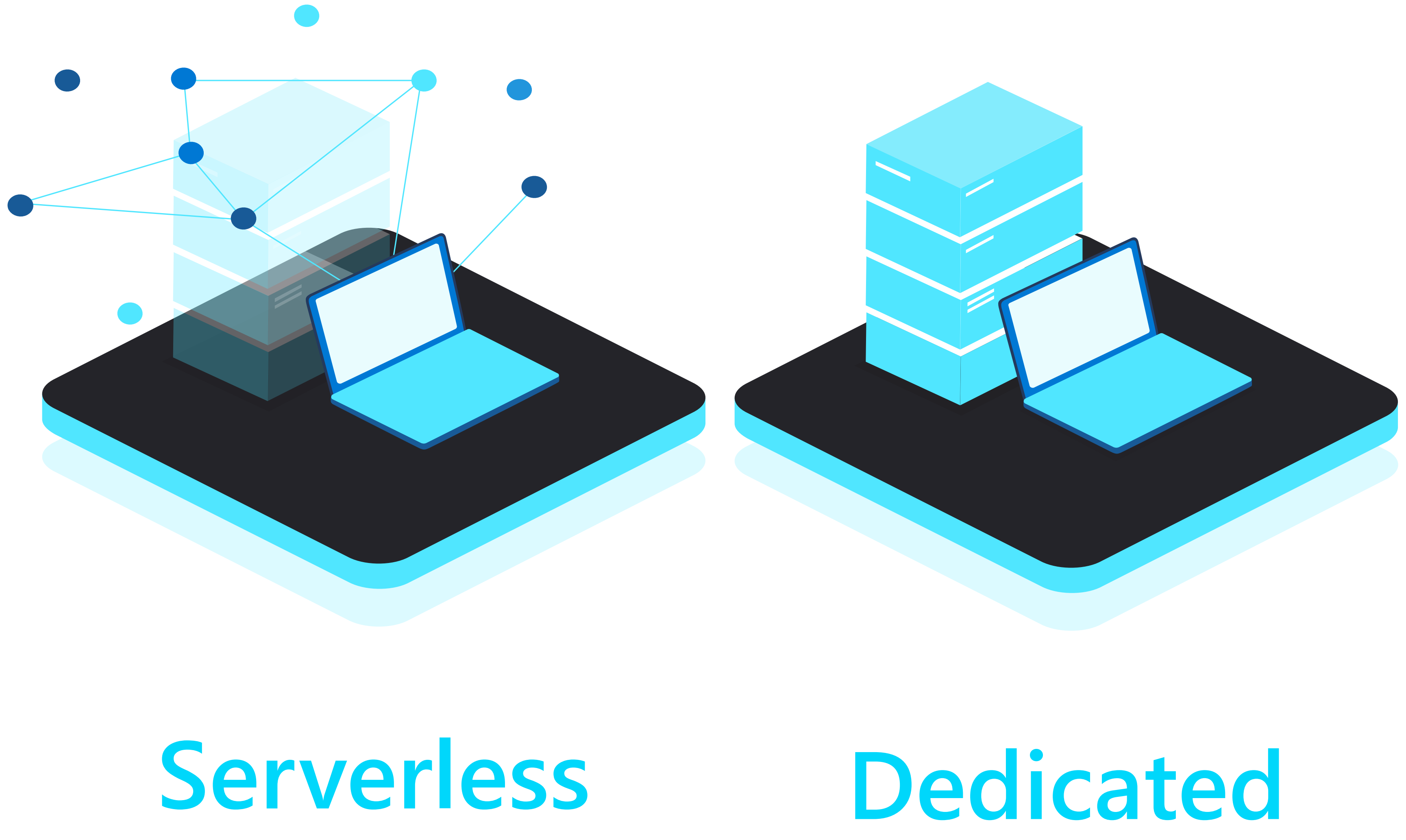
INSPARK

SQL

SQL Pools

Serverless SQL Pool

```
use master
go
CREATE LOGIN [erwin.de.kreuk@demo.com] FROM EXTERNAL PROVIDER;
go

use yourdb -- Use your database name
go
CREATE USER  demouser  FROM LOGIN [erwin.de.kreuk@demo.com];


use yourdb -- Use your database name
go
alter role db_owner Add member demouser
```



Dedicated SQL Pool

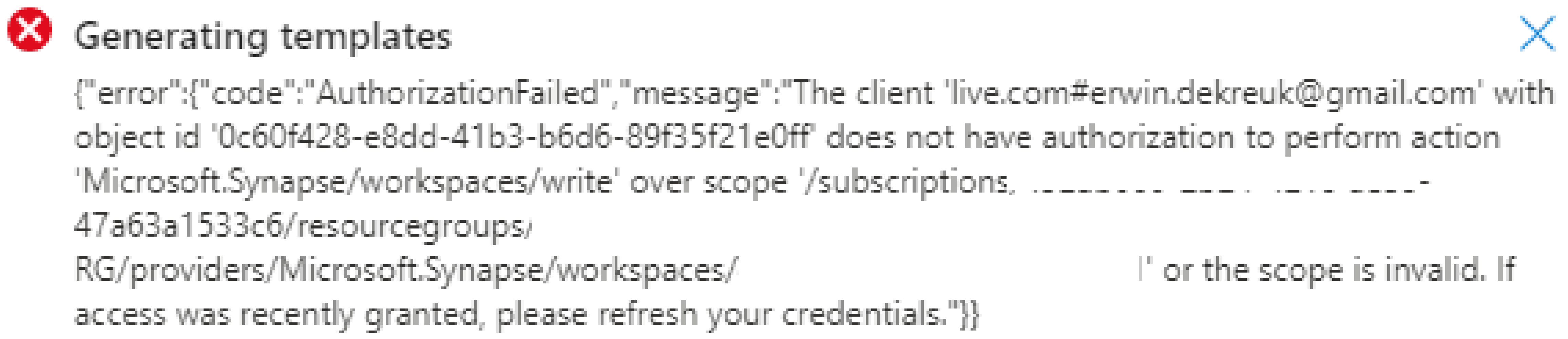
```
--Create user in the database
CREATE USER [erwin.dekreuk@gmail.com] FROM EXTERNAL PROVIDER;


--Grant role to the user in the database
EXEC sp_addrolemember 'db_owner', 'erwin.dekreuk@gmail.com';
```

INSPARK

Demo

GIT Integration

Azure Dev Ops



Generating templates

```
{"error":{"code":"AuthorizationFailed","message":"The client 'live.com#erwin.dekreuk@gmail.com' with
object id '0c60f428-e8dd-41b3-b6d6-89f35f21e0ff' does not have authorization to perform action
'Microsoft.Synapse/workspaces/write' over scope '/subscriptions/[redacted]-
47a63a1533c6/resourcegroups/[redacted]
RG/providers/Microsoft.Synapse/workspaces/[redacted]' or the scope is invalid. If
access was recently granted, please refresh your credentials."}}
```

- Azure Dev Ops

  Basic user settings

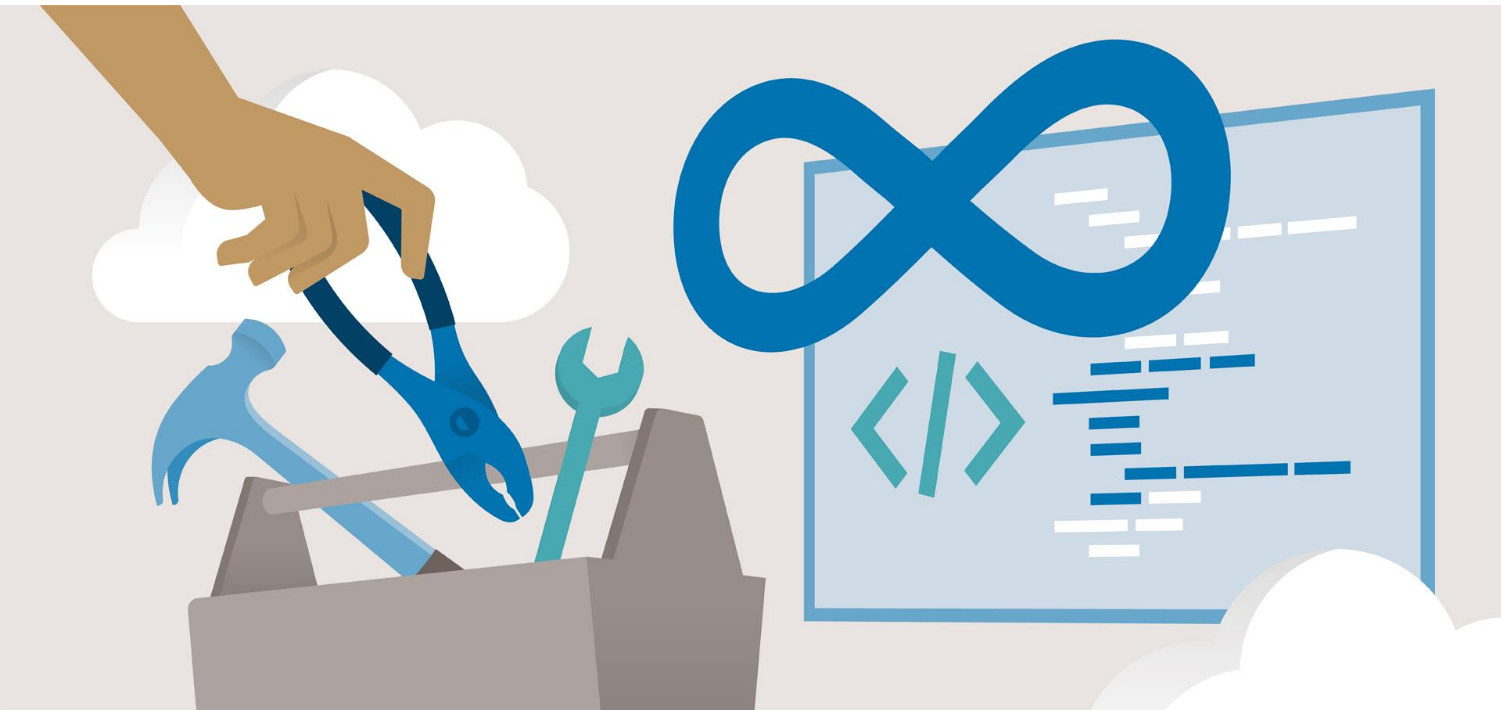
  Azure Artifact Publisher

  Azure Contributor (Azure RBAC) or higher role on the Synapse workspace

- Dev Ops Service Connection

  Azure Contributor (Azure RBAC) or higher role on the Resource Group

  Azure Synapse Administrator

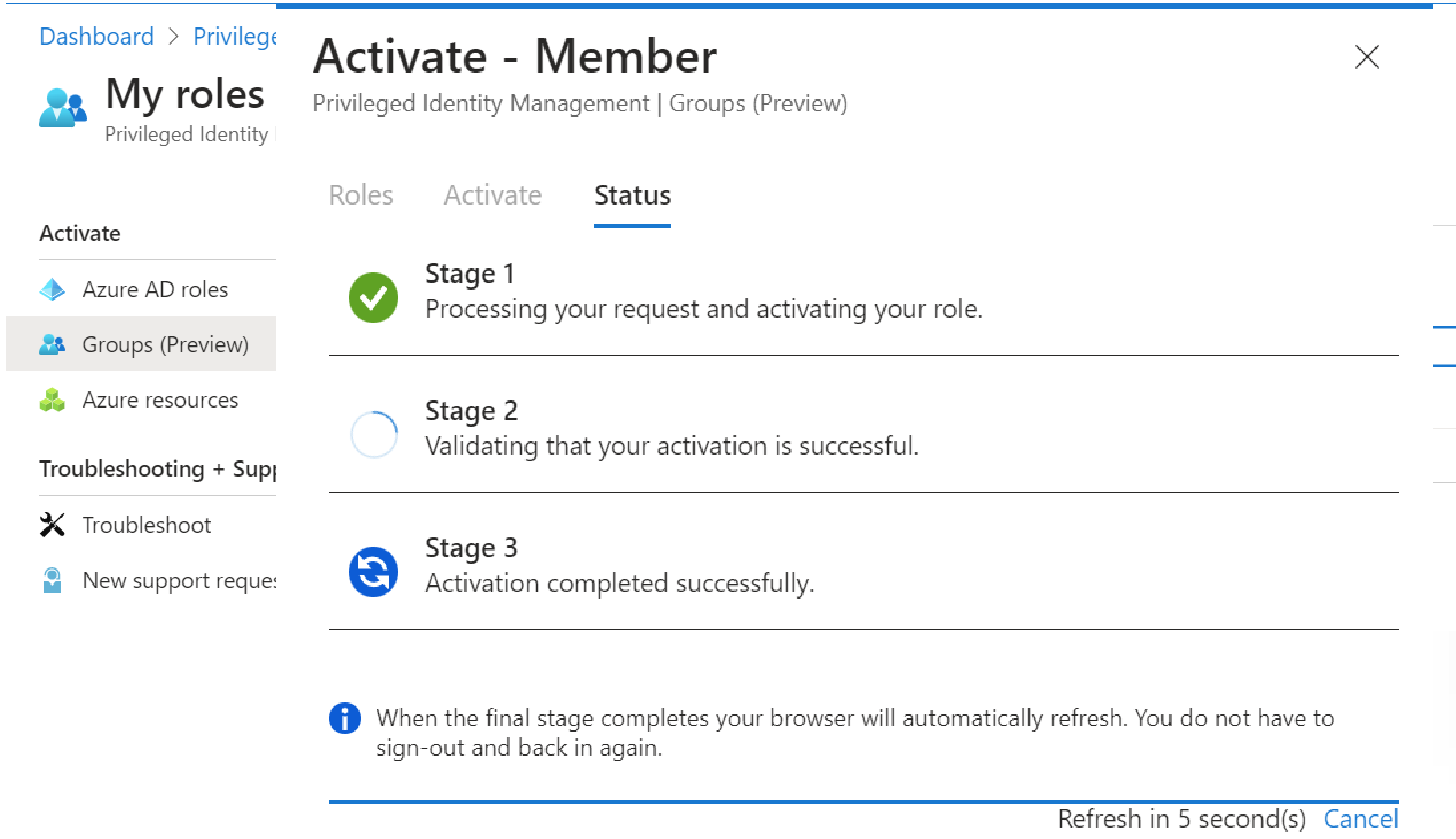


Who is using Privileged Identity Management ?

Advanced Secuirty

Privileged Identity Management (Preview)

- Secure Synapse Administrator role
- More secure
- All Logins are logged
- Possible with approval process
- Specific Time windows



Activate - Member

Privileged Identity Management | Groups (Preview)

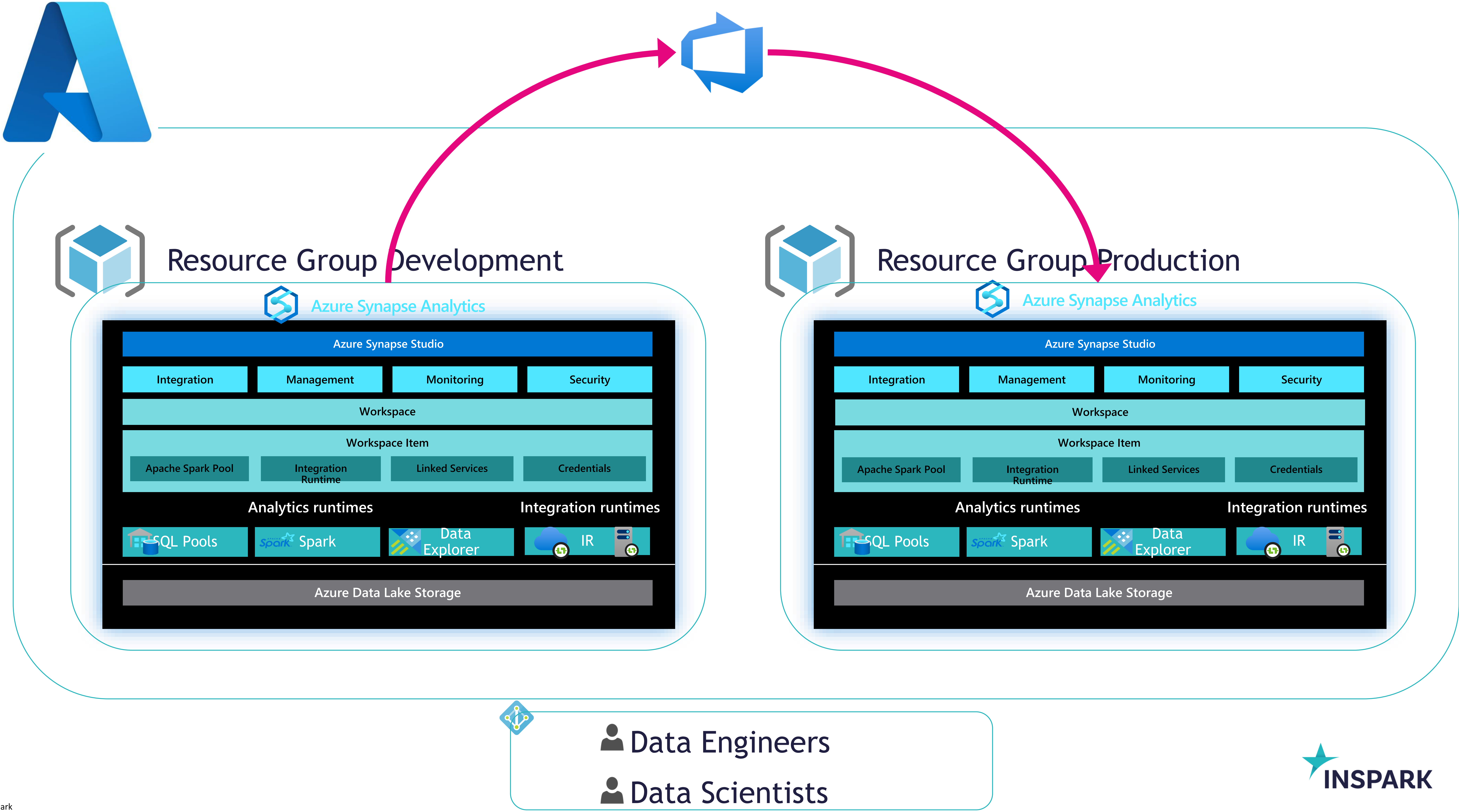
Stage 1
Processing your request and activating your role.

Stage 2
Validating that your activation is successful.

Stage 3
Activation completed successfully.

When the final stage completes your browser will automatically refresh. You do not have to sign-out and back in again.

Refresh in 5 second(s) Cancel



Resource Group Development

Azure Synapse Analytics

Azure Synapse Studio

Integration | Management | Monitoring | Security

Workspace

Workspace Item

Apache Spark Pool | Integration Runtime | Linked Services | Credentials

Analytics runtimes

Integration runtimes

SQL Pools | Spark | Data Explorer | IR

Azure Data Lake Storage

Resource Group Production

Azure Synapse Analytics

Azure Synapse Studio

Integration | Management | Monitoring | Security

Workspace

Workspace Item

Apache Spark Pool | Integration Runtime | Linked Services | Credentials

Analytics runtimes

Integration runtimes

SQL Pools | Spark | Data Explorer | IR

Azure Data Lake Storage

Data Engineers

Data Scientists

INSPARK

Security Groups

- Data Engineers

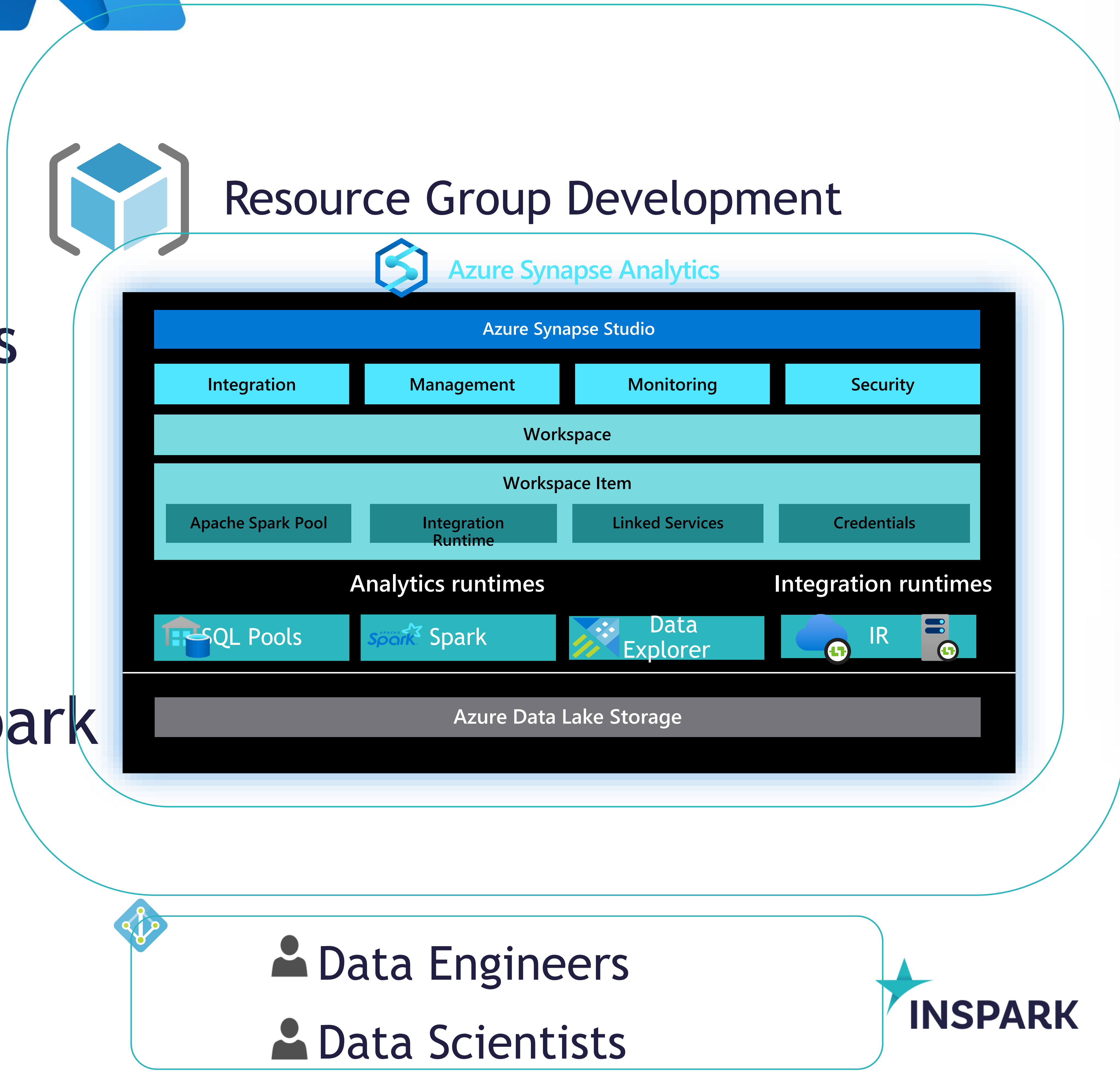
  Needs to access SQL Serverless

  Publish or edit Code

- Data Scientist:

  Needs access to a specified Spark

  Submit Spark Jobs



Resource Group Development

Azure Synapse Analytics

Azure Synapse Studio

Integration | Management | Monitoring | Security

Workspace

Workspace Item

Apache Spark Pool | Integration Runtime | Linked Services | Credentials

Analytics runtimes | Integration runtimes

SQL Pools | Spark | Data Explorer | IR

Azure Data Lake Storage

Data Engineers

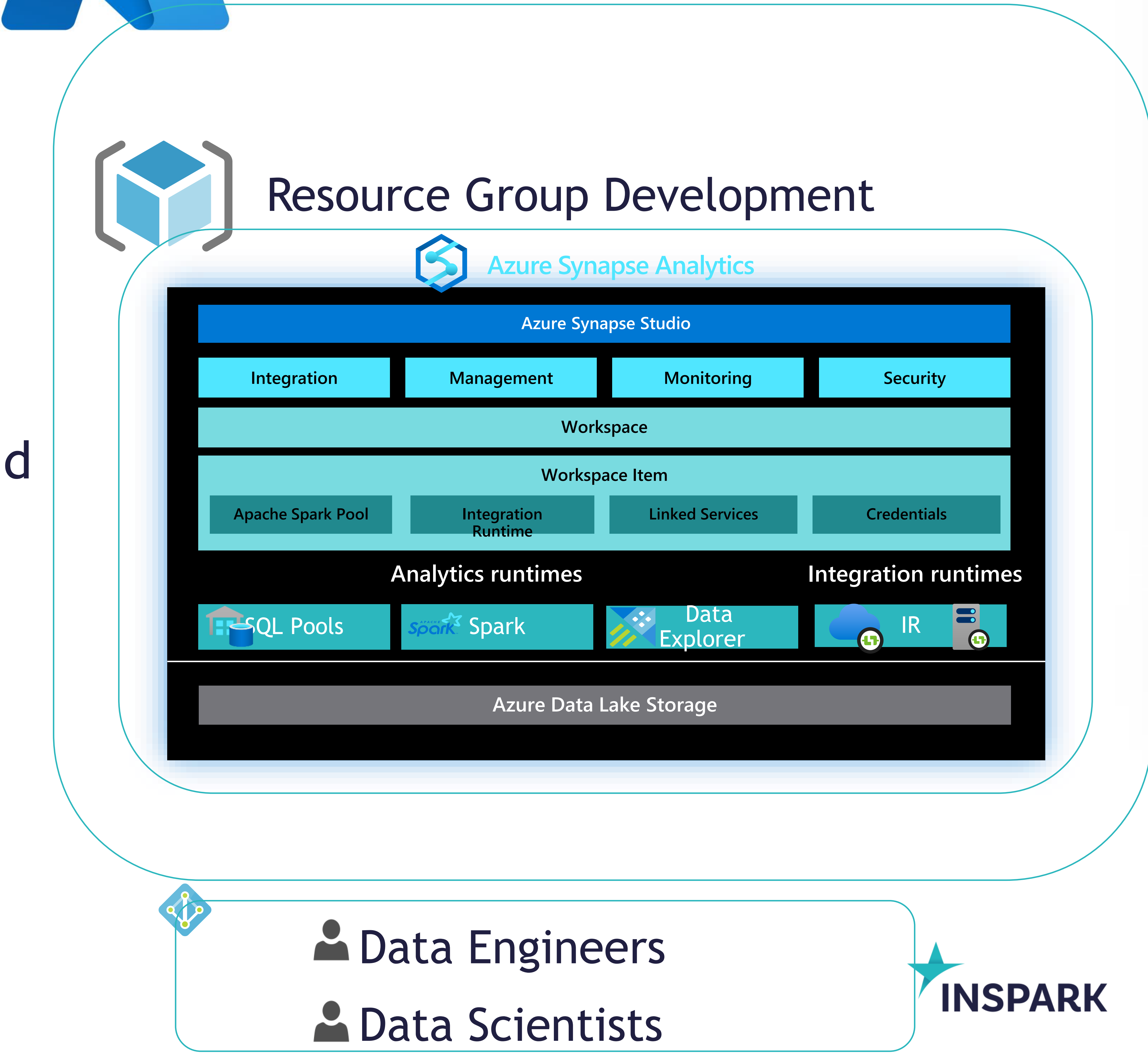
Data Scientists

Demo

Azure Synapse

Recap

- Understanding Access Control in Azure Synapse
- Role-Based Access Control (RBAC)
- Access Control for Data Warehouses and Data Lakes
- Privileged Identity Management (PIM)



Resource Group Development

Azure Synapse Analytics

Azure Synapse Studio

Integration | Management | Monitoring | Security

Workspace

Workspace Item

Apache Spark Pool | Integration Runtime | Linked Services | Credentials

Analytics runtimes

Integration runtimes

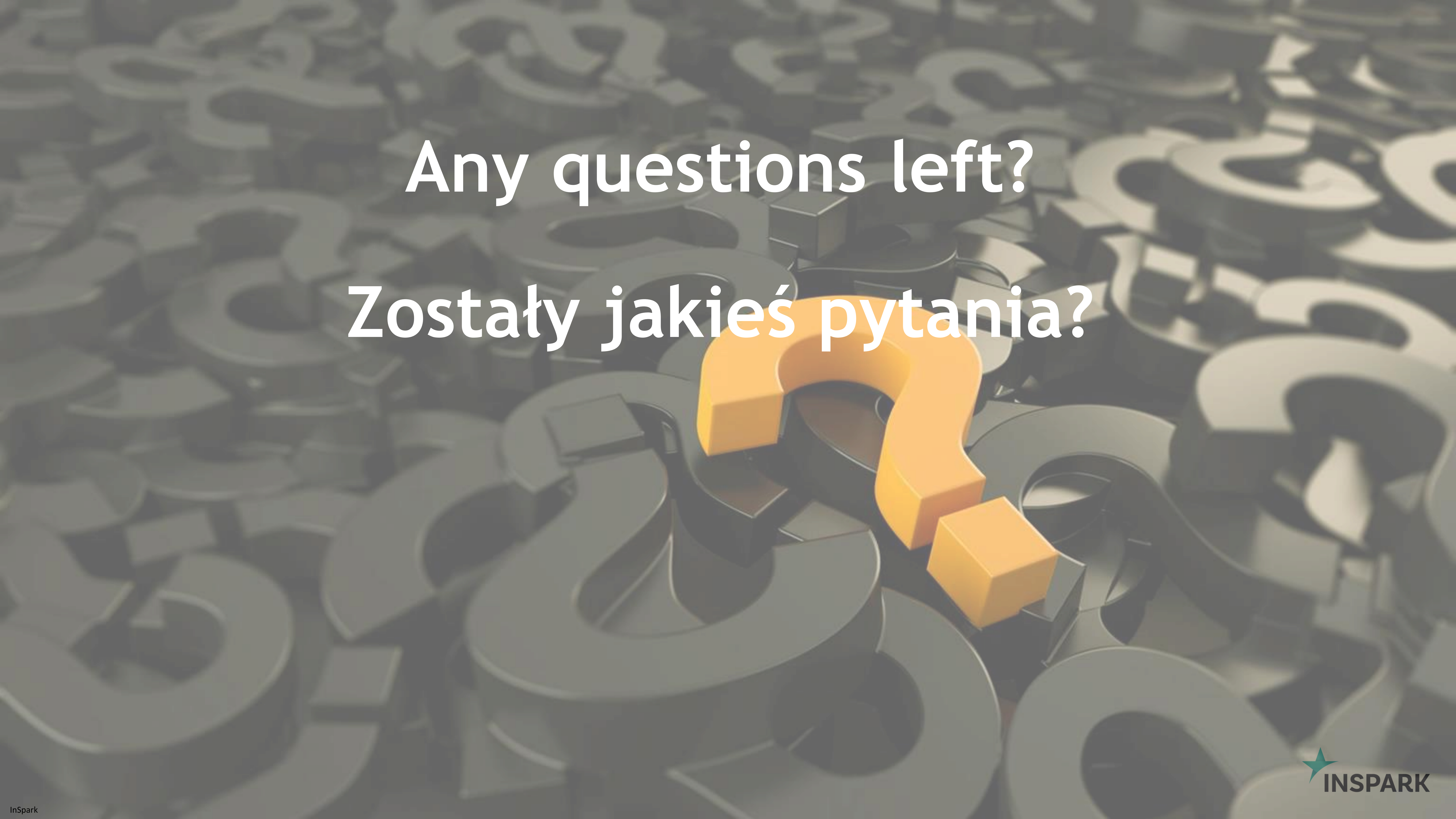
SQL Pools | Spark | Data Explorer | IR

Azure Data Lake Storage

Data Engineers

Data Scientists

INSPARK



Any questions left?

Zostały jakieś pytania?

Thank you for attending!

Erwin de Kreuk
Principal Consultant – Data & AI
InSpark

@ErwinDeKreuk

linkedin.com/in/ErwinDeKreuk

ErwinDeKreuk.com github.com/edkreuk

FEEDBACK in the Whova APP

MVP Microsoft® Most Valuable Professional

INSPARK