

Dealing with different Roles in Azure Synapse Analytics



We Are InSpark

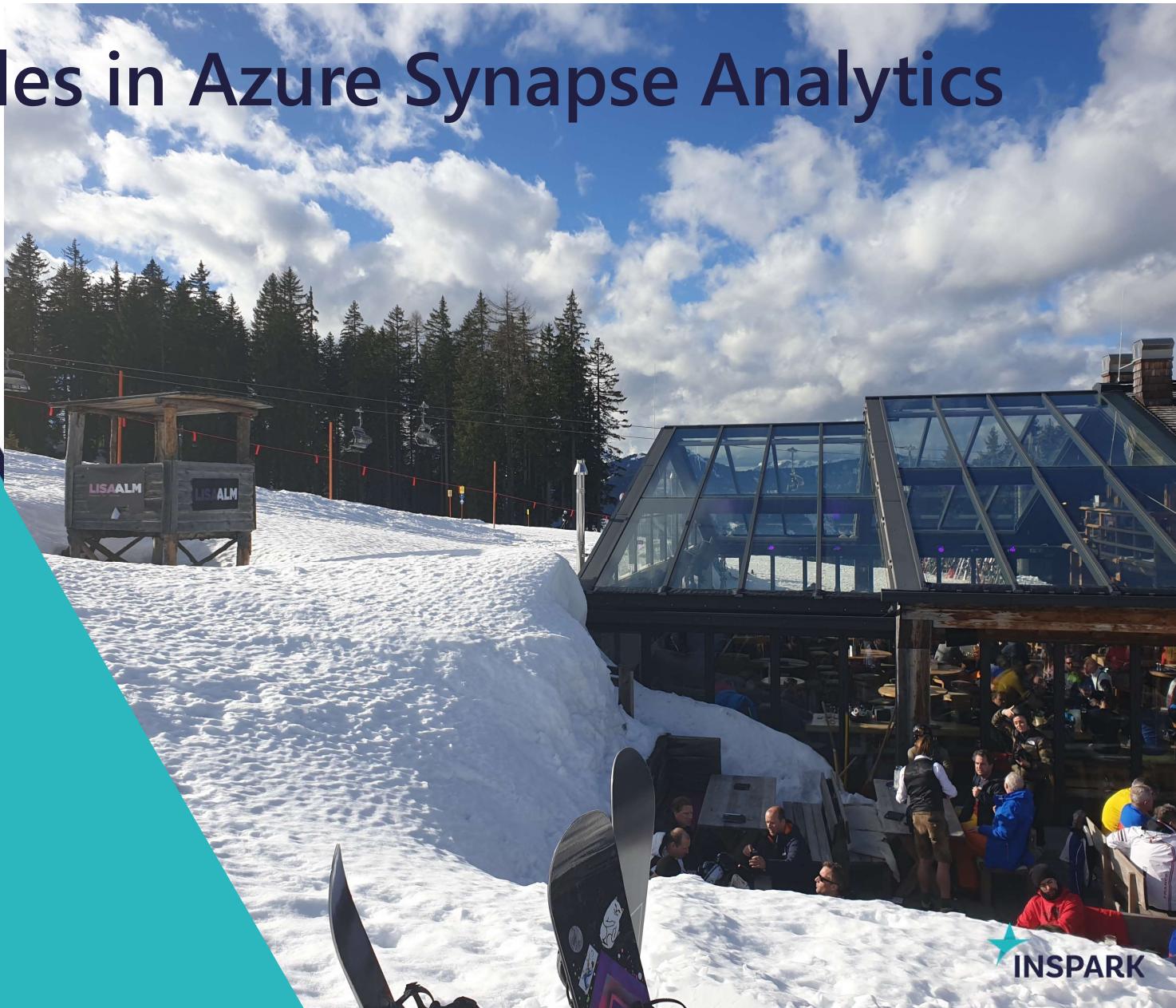
We help organizations
accelerating their digital
transformation with impactful
Microsoft solutions & expertise

Microsoft
Partner

2021 Partner of the Year Finalist
Analytics Award



Roles in Azure Synapse Analytics



Azure Synapse

Access Control

Azure Roles

Synapse Roles

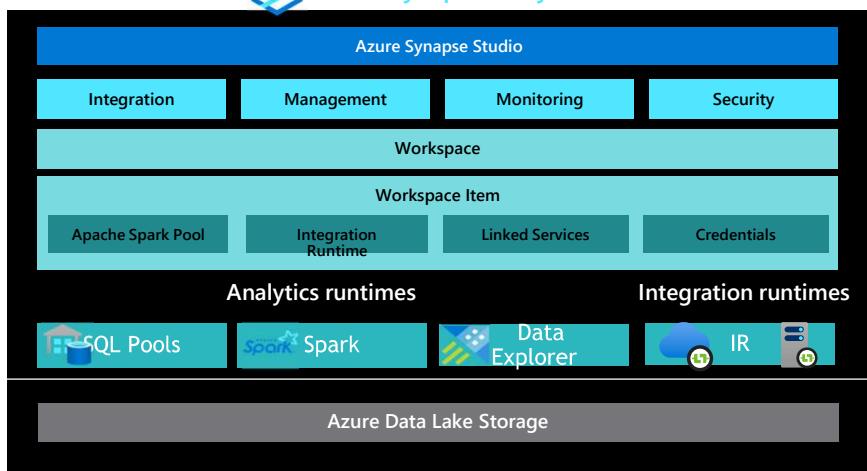
SQL Roles

Git Permissions

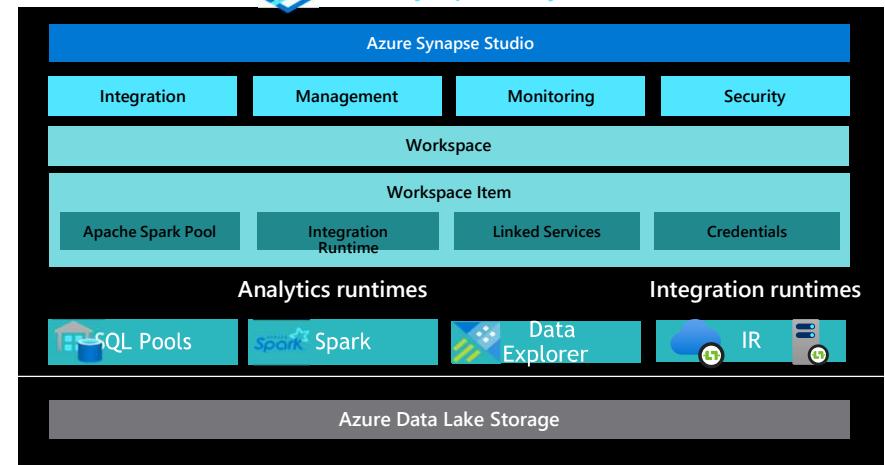




Resource Group Development



Resource Group Production

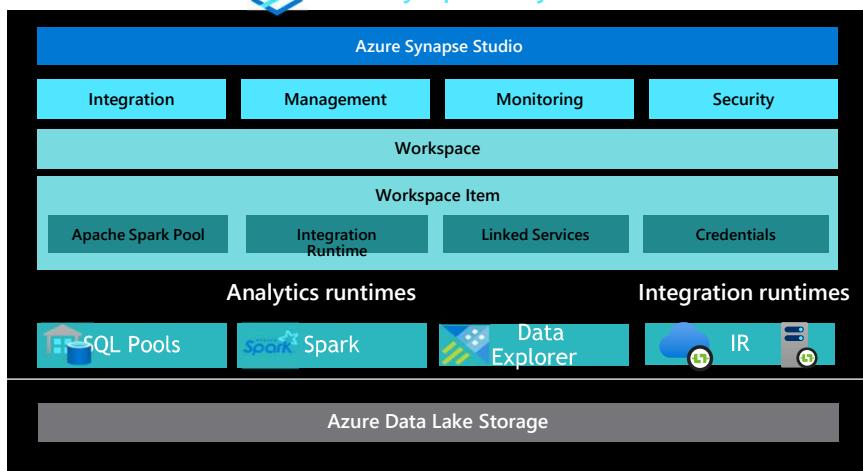


Data Engineers

Data Scientists



Resource Group Development



Azure Roles

Resource Management

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



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 *

Region *

Select Data Lake Storage Gen2 * From subscription Manually via URL

Account name *

File system name *

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

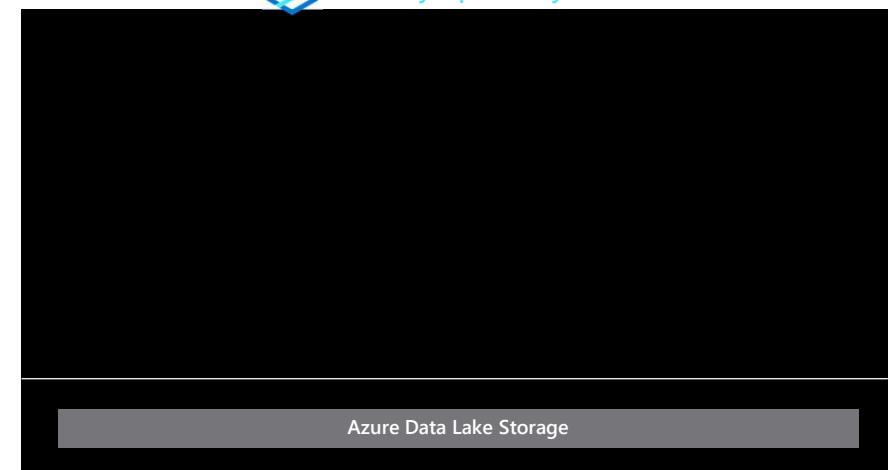
[Learn more](#)



Resource Group Development

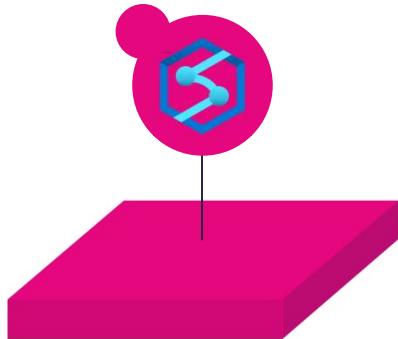


Azure Synapse Analytics

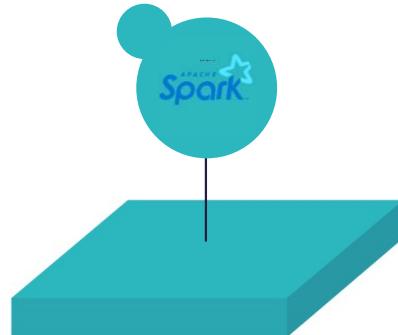


Synapse Roles

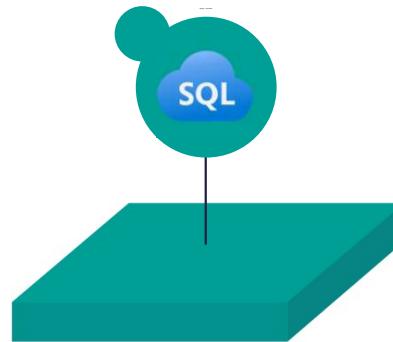
Administrators



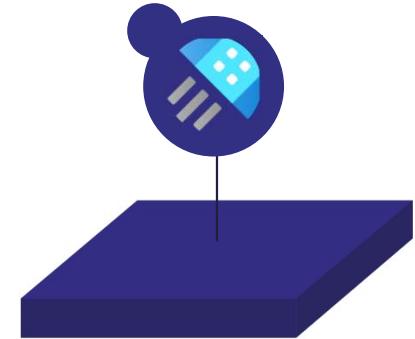
Synapse
Administrator



Synapse
Apache Spark
Administrator



Synapse SQL
Administrator



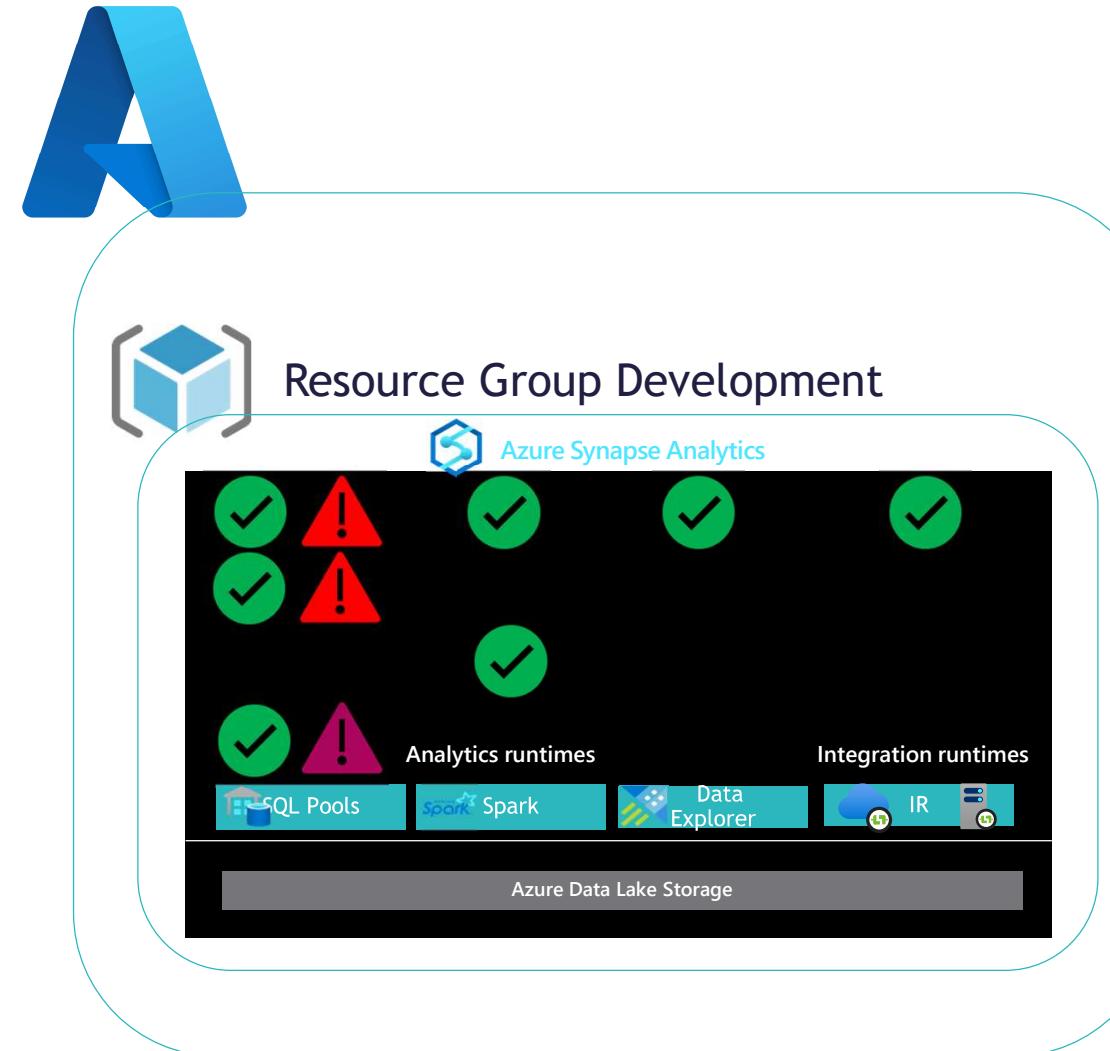
Synapse Data
Explorer
Administrator????

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

Synapse Roles

Synapse Administrator

Activities:

- 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

Activities:

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



Synapse Roles

Synapse SQL Administrator

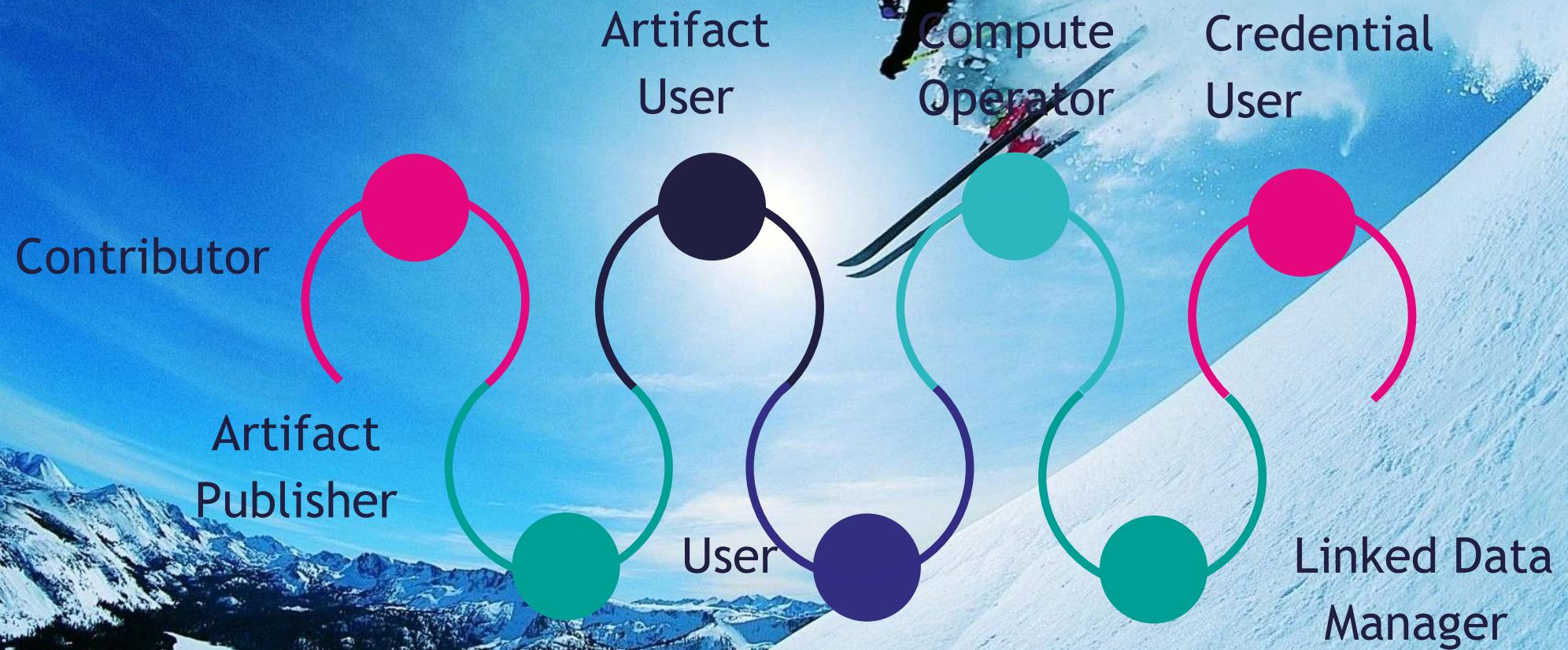
Activities:

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



Synapse Roles

Non-Administrators

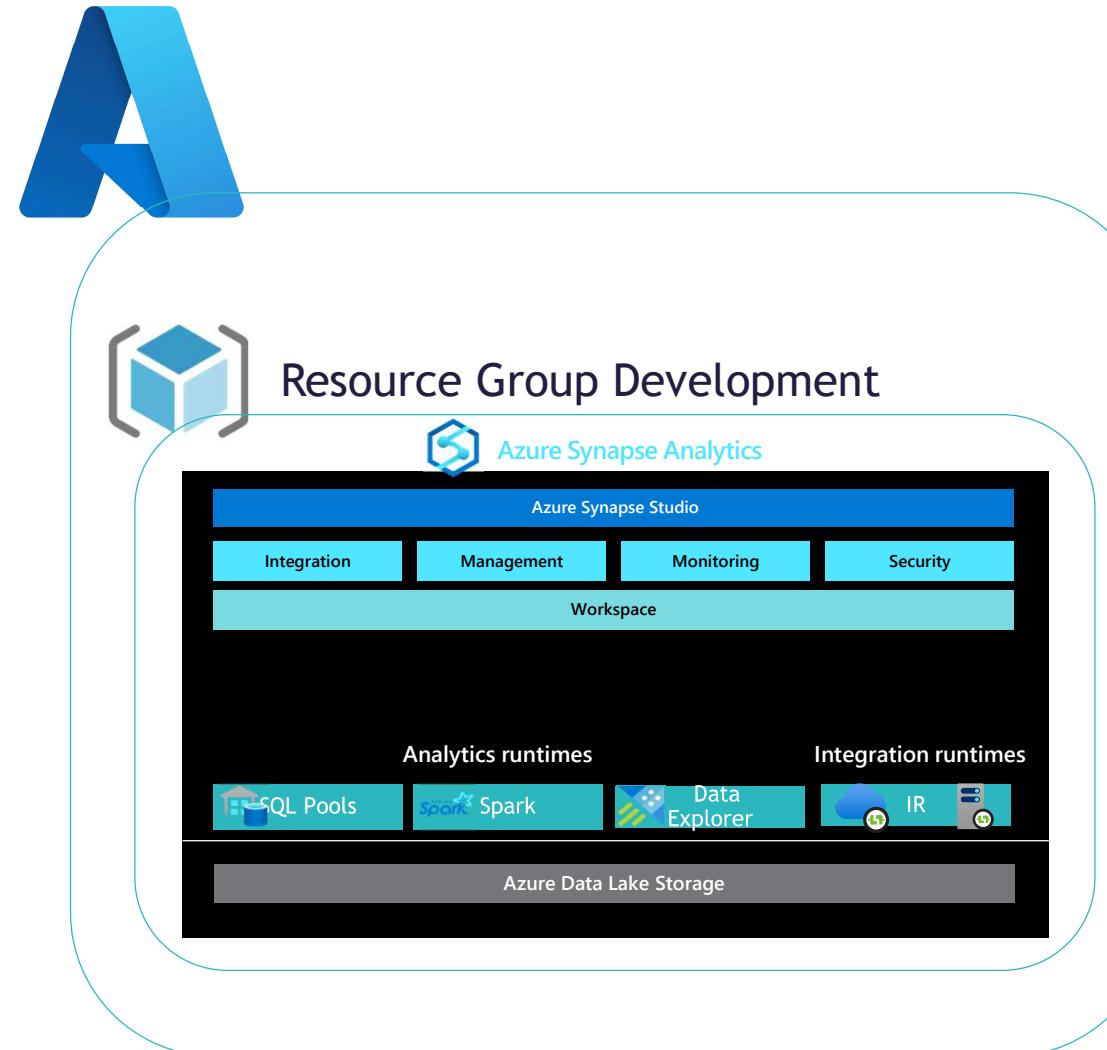


Synapse Roles

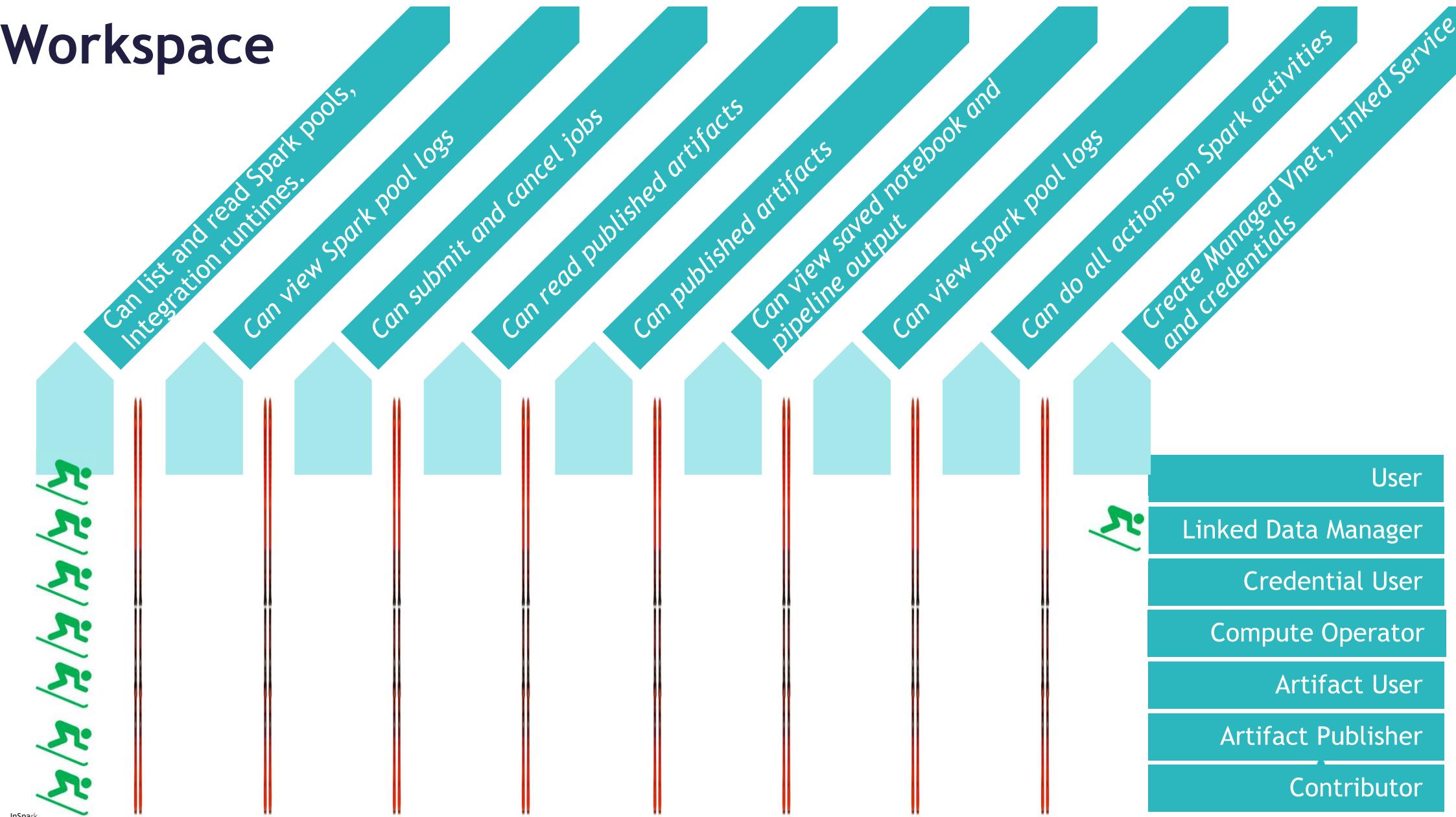
Workspace

Roles:

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



Workspace



Synapse Roles

Workspace Items

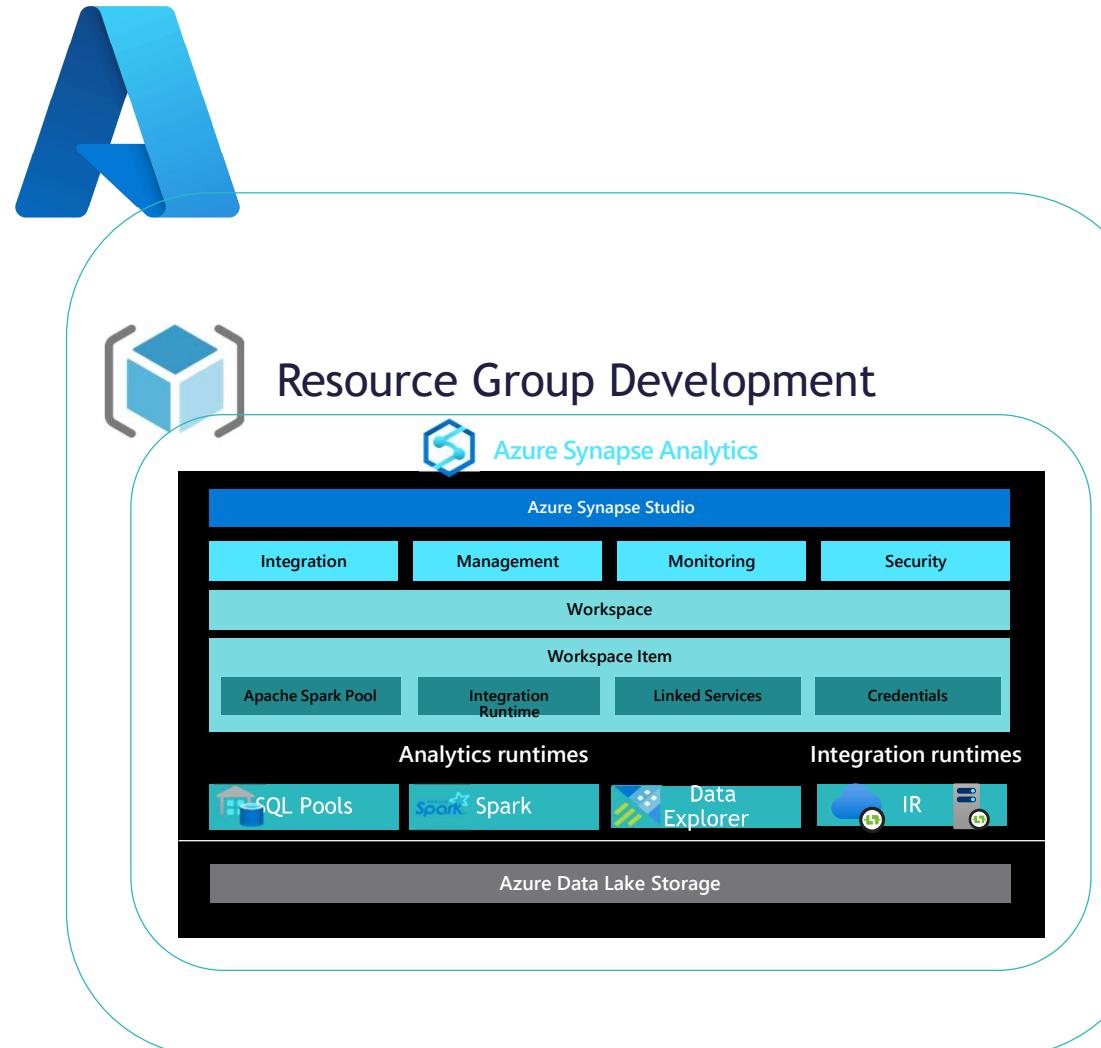


Synapse Roles

Workspace Item

Item:

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



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 * ①

Workspace Workspace item

Role * ①

Select a role

Filter...

Synapse Administrator ①

Synapse SQL Administrator ①

Synapse Apache Spark Administrator ①

Synapse Contributor ①

Synapse Artifact Publisher ①

Synapse Artifact User ①

Synapse Compute Operator ①

Add role assignment

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

Scope * ①

Workspace Workspace item

Item type

Apache Spark pool

Item *

Spark30

Role * ①

Select a role

Filter...

Synapse Administrator ①

Synapse Contributor ①

Synapse Compute Operator ①

Synapse Roles

Tips and Tricks

- ❑ No access message in Azure Portal
- ❑ <https://web.azuresynthesize.net>

⚠️ 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 ①

InSpark

Account selection method

From Azure subscription Enter manually

Subscription

No results found

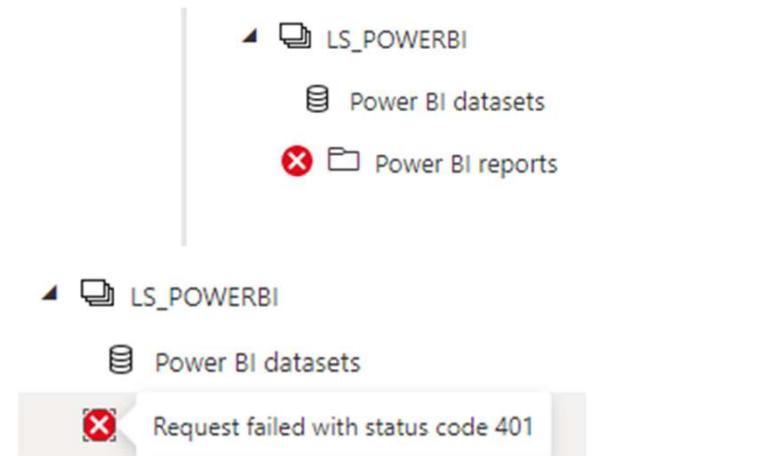
Continue



Synapse Roles

Tips and Tricks

- ❑ No access message in Azure Portal
 - ❑ <https://web.azure-synapse>
- ❑ Power BI
 - ❑ Access is defined on Power BI workspace level



Synapse Roles

Tips and Tricks

- No access message in Azure Portal
 - <https://web.azure-synapse>
- Power BI
 - Access is defined on Power BI workspace level
- Publish Error

Synapse Administrator

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/*

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

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

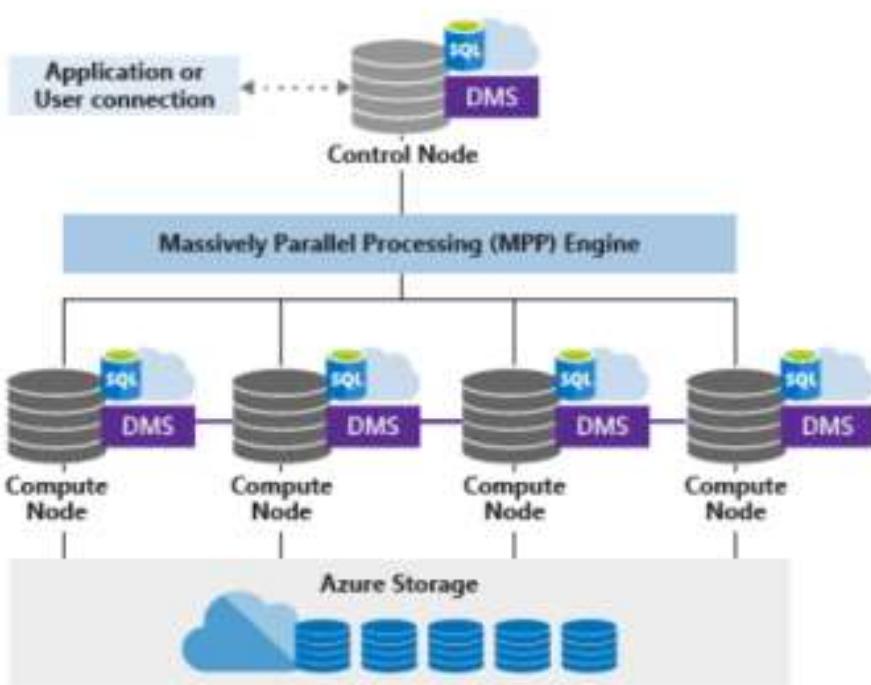
| | Administrator | Contributor | Artifact Publisher | Apache Spark Administrator | SQL Administrator | Artifact User | Compute Operator | Credential User | Linked Data Manager | User |
|-----------------|---------------|-------------|--------------------|----------------------------|-------------------|---------------|------------------|-----------------|---------------------|------|
| workspaces/read | | | | | | | | | | |



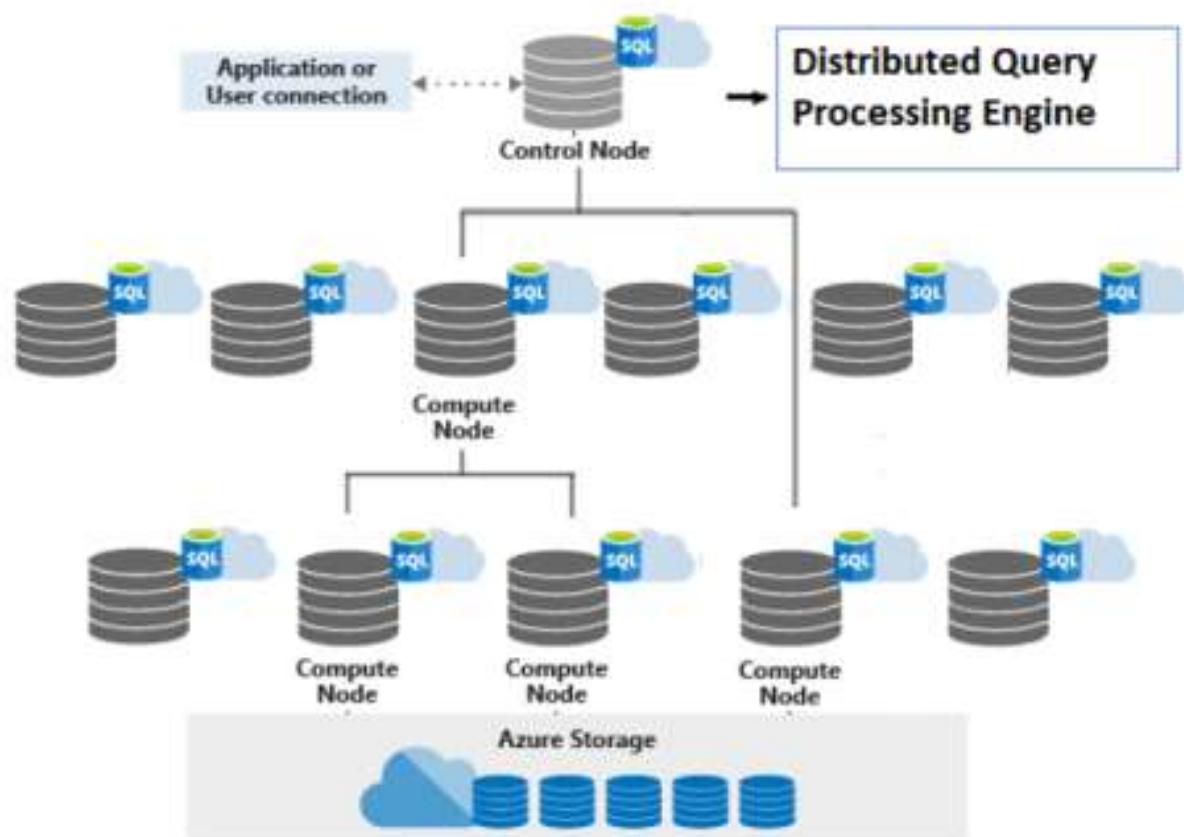
Demo

SQL

Dedicated SQL pool



Serverless SQL pool



IN SPARK

SQL

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



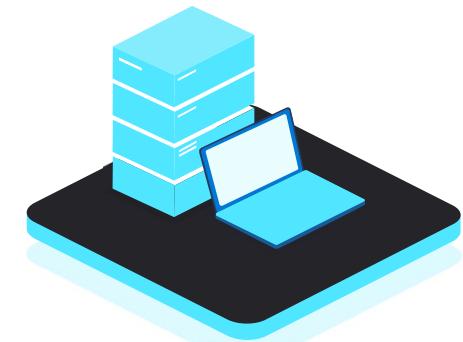
Serverless

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



Dedicated

Synapse SQL Administrator:

- No access by default

Active Directory Admin:

- Full access

SQL

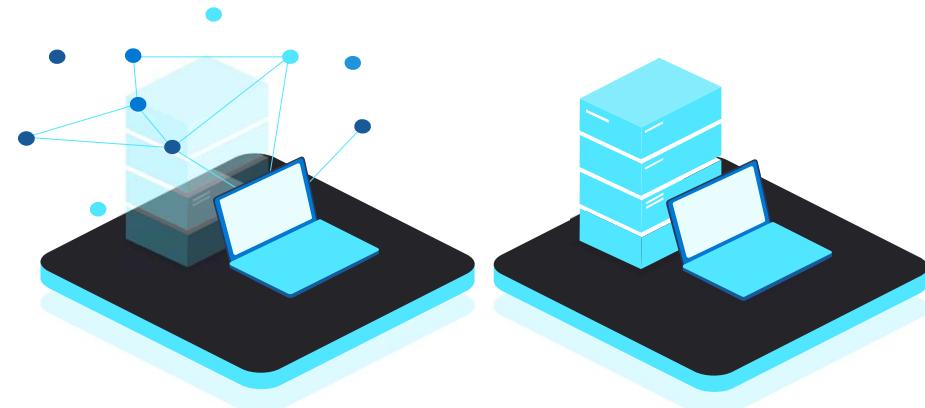
SQL Pools

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
```



Serverless

Dedicated

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';
```



Demo

GIT Integration

Azure Dev Ops

Azure Dev Ops:

- Basic user settings
- Azure Artifact Publisher
- Azure Contributor (Azure RBAC) or higher role on the Synapse workspace

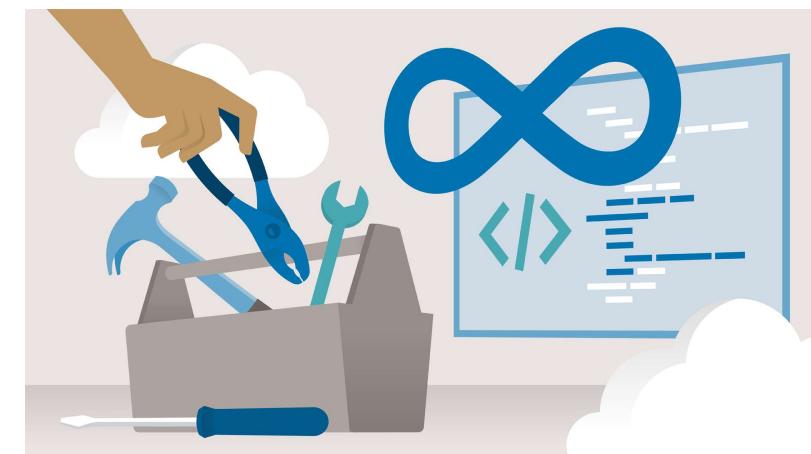
Dev Ops Service Connection:

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

✖ Generating templates

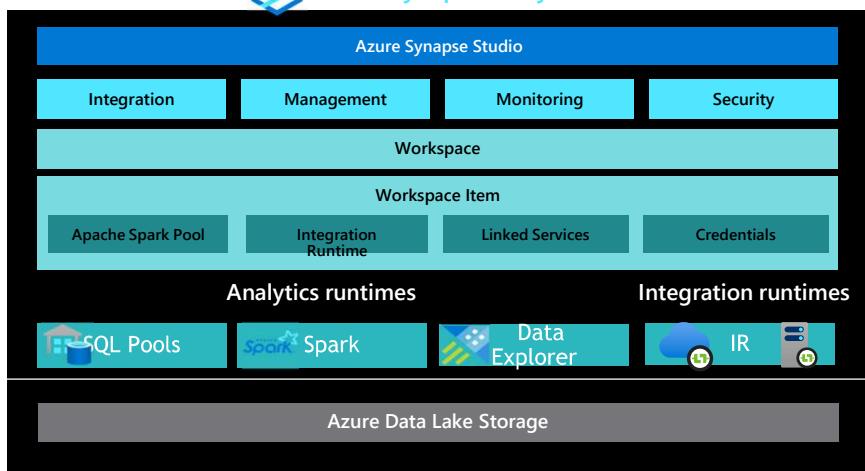
```
{"error":{"code":"AuthorizationFailed","message":"The client 'live.com#erwin.dekreuk@gmail.com' with object id '0c60f428-e8dd-41b3-b6d6-89f35f21e0ff' does not have authorization to perform action 'Microsoft.Synapse/workspaces/write' over scope '/subscriptions, -----, 47a63a1533c6/resourcegroups/RG/providers/Microsoft.Synapse/workspaces/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

! or the scope is invalid. If

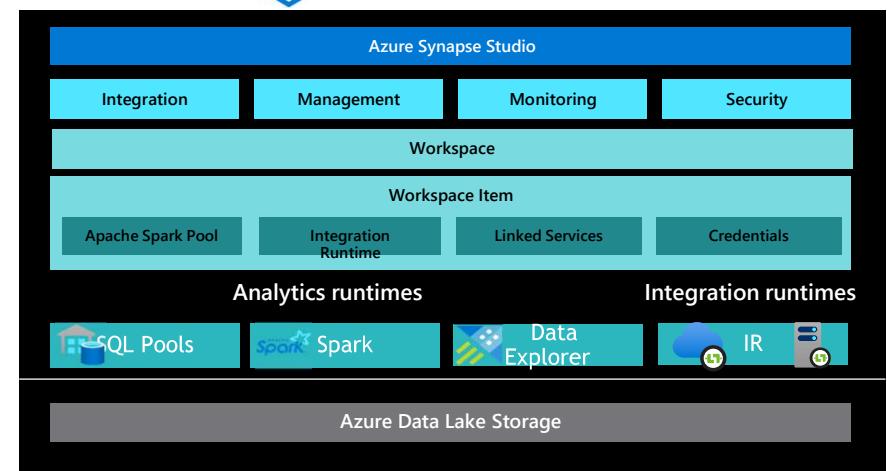




Resource Group Development



Resource Group Production



Data Engineers

Data Scientists



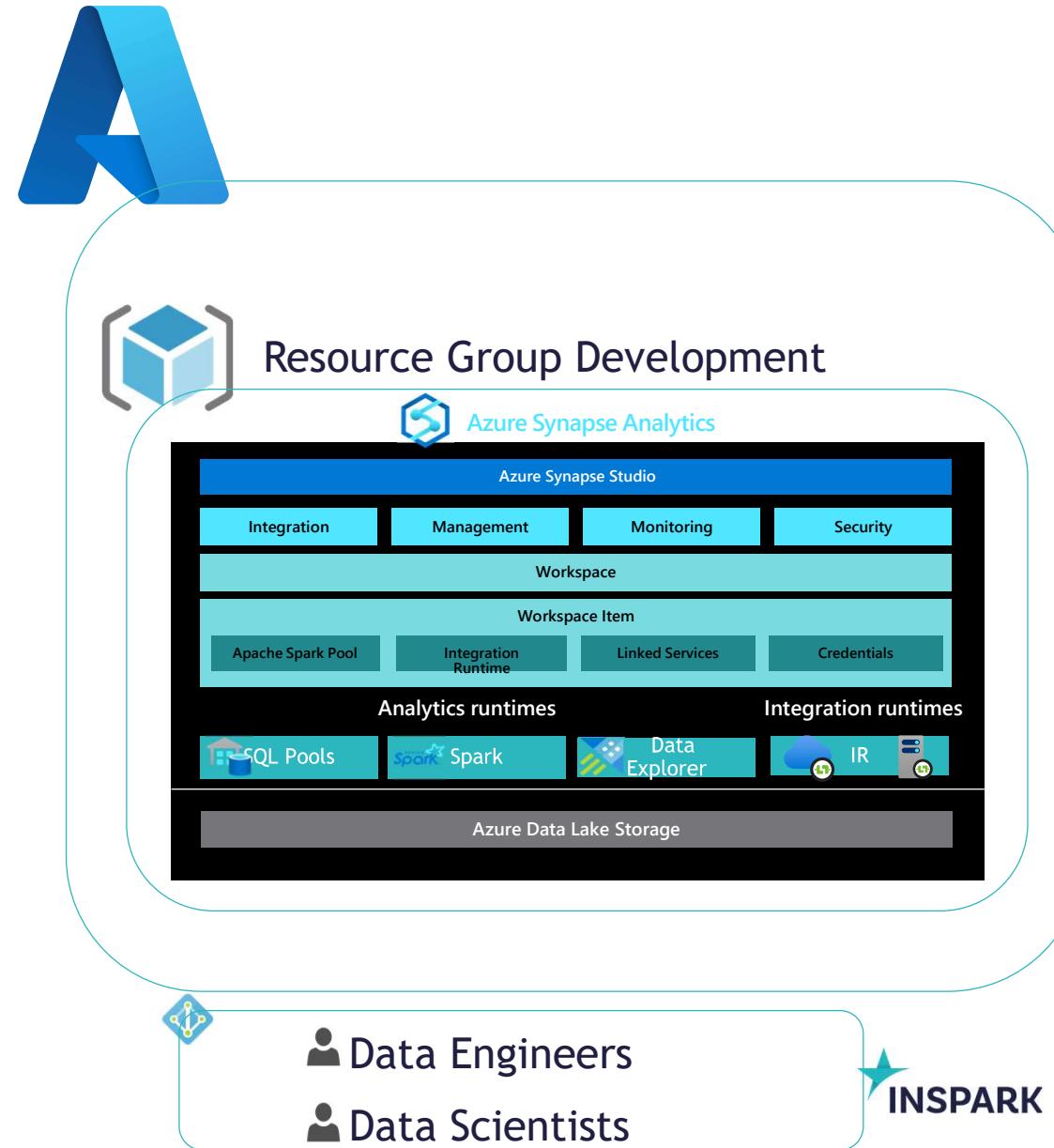
Security Groups

Data Engineers

- Needs to access SQL Serverless
- Publish or edit Code
- Debug pipelines

Data Scientist:

- Needs to access SQL Serverless
- Needs access to a specified Spark Pool
- Publish or edit Code
- Submit Spark Jobs



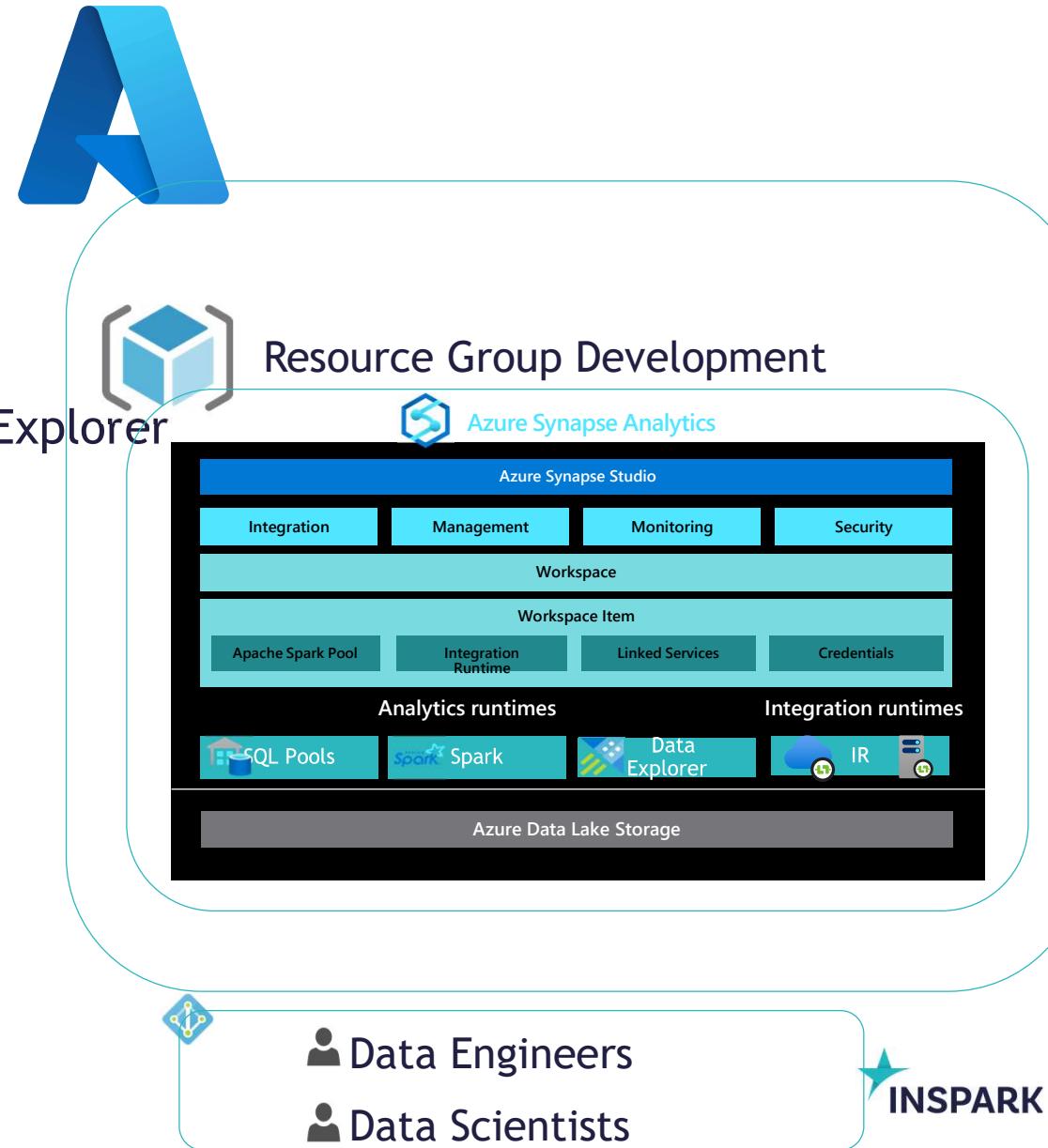


Demo

Azure Synapse

Recap

- Acces to Azure Synapse Studio
- Create SQL Pools/Spark Pools /Data Explorer Pools
- Execute Notebooks
- View and edit code Artifacts
- Debug or Trigger Pipelines
- Monitor
- Publish Code



Questions?



<https://erwindekreuk.com>



@erwindekreuk



<https://www.linkedin.com/in/erwindekreuk/>

Slides will be available on my blog

