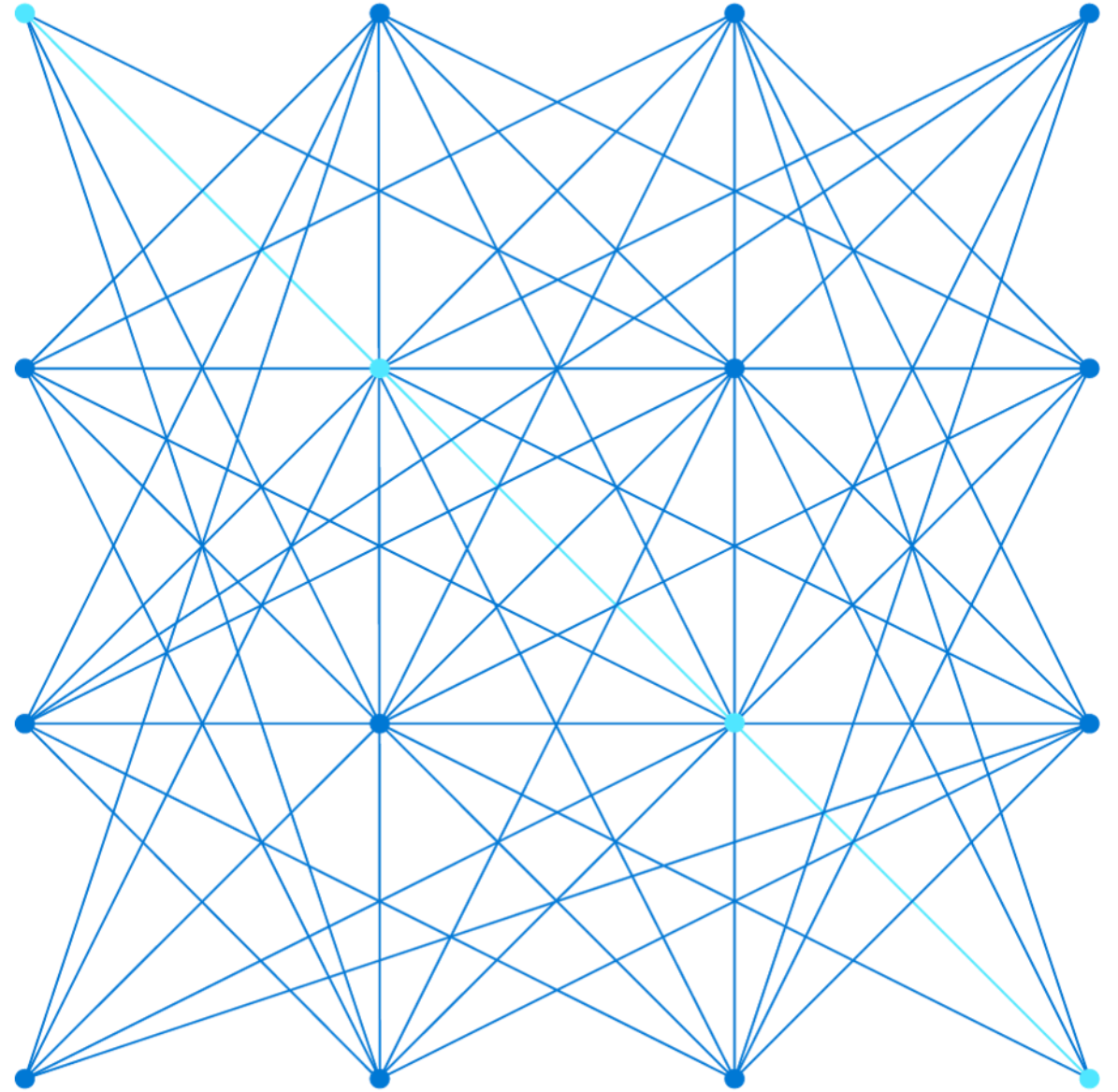
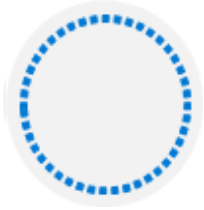


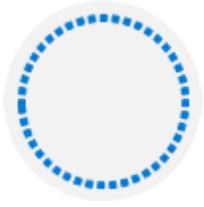
DP-203T00: End-to-end security with Azure Synapse Analytics



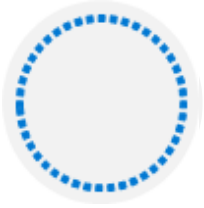
Agenda



Lesson 01: Secure a data warehouse in Azure Synapse Analytics



Lesson 02: Configure and manage secrets in Azure Key Vault

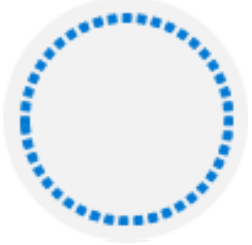


Lesson 03: Implement compliance controls for sensitive data

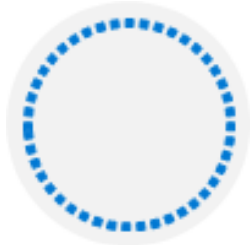
Lesson 01: Secure a data warehouse in Azure Synapse Analytics



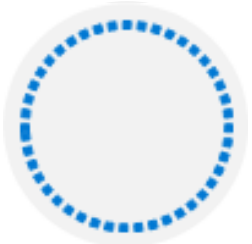
Secure a data warehouse in Azure Synapse Analytics



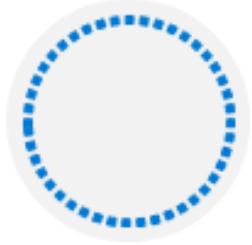
Network security



Identity and access management



Managing sensitive data



Encryption capabilities built into Azure

Network security

Securing your network from attacks and unauthorized access is an important part of any architecture

Internet protection	Firewalls	DDoS protection	Network security groups
Assess the resources that are internet-facing, and to only allow inbound and outbound communication where necessary. Make sure you identify all resources that are allowing inbound network traffic of any type	To provide inbound protection at the perimeter, there are several choices: <ul style="list-style-type: none">• Azure Firewall• Azure Application Gateway• Azure Storage Firewall	The Azure DDoS Protection service protects your Azure applications by scrubbing traffic at the Azure network edge before it can impact your service's availability	Network Security Groups allow you to filter network traffic to and from Azure resources in an Azure virtual network. An NSG can contain multiple inbound and outbound security rules

Identity and access

Authentication

This is the process of establishing the identity of a person or service looking to access a resource. Azure Active Directory is a cloud-based identity service that provide this capability

Authorization

This is the process of establishing what level of access an authenticated person or service has. It specifies what data they're allowed to access and what they can do with it. Azure Active Directory also provides this capability

Azure Active Directory features

Single sign-on

Enables users to remember only one ID and one password to access multiple applications

Apps & device management

You can manage your cloud and on-premises apps and devices and the access to your organizations resources

Identity services

Manage Business to business (B2B) identity services and Business-to-Customer (B2C) identity services

Lesson 01: Configure and manage secrets in Azure Key Vault



Configure and manage secrets in Azure Key Vault

Azure Key Vault protects

1. Secrets
2. Keys
3. Certificates

Data Engineers are typically concerned with accessing the data contained in Key Vault to apply to linked services

The screenshot displays the 'New linked service' configuration interface. At the top, a header reads 'New linked service'. Below it, a light blue information bar states: 'Choose a name for your linked service. This name cannot be updated later.' The form includes several fields: 'Name *' (a text input field), 'Description' (a larger text area), and 'Connect via integration runtime *' (a dropdown menu currently showing 'AutoResolveIntegrationRuntime'). A red rectangular box highlights the 'AKV linked service' section. Within this box, there are two tabs: 'Connection string' (selected) and 'Azure Key Vault'. Below the tabs, the 'AKV linked service *' dropdown is shown with a selection icon. An 'Edit connection' link is present. The 'Secret name *' field is a text input. The 'Secret version' field has a dropdown menu with the text 'Use the latest version if left blank'. Below the highlighted section, there is an 'Annotations' section with a '+ New' button, and two expandable sections: 'Parameters' and 'Advanced'.

Lesson 01: Implement compliance controls for sensitive data



Managing sensitive data

Column level security

```
GRANT SELECT ON wwi_security.Sale([ProductID], [Analyst], [Product], [CampaignName],[Quantity], [Region], [State], [City], [RevenueTarget]) TO DataAnalystMiami;
```

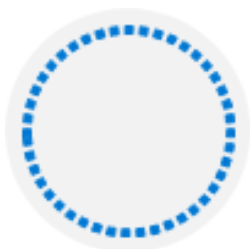
Row level security

```
CREATE FUNCTION wwi_security.fn_securitypredicate(@Analyst AS sysname) RETURNS TABLE WITH SCHEMABINDING AS RETURN SELECT 1 AS fn_securitypredicate_result WHERE @Analyst = USER_NAME() OR USER_NAME() = 'CEO' GO
```

```
CREATE SECURITY POLICY SalesFilter ADD FILTER PREDICATE wwi_security.fn_securitypredicate(Analyst) ON wwi_security.Sale WITH (STATE = ON);
```

```
GRANT SELECT ON wwi_security.Sale TO CEO, DataAnalystMiami, DataAnalystSanDiego;
```

Implement compliance controls for sensitive data



Dynamic data masking

Masking rules

MASK NAME	MASK FUNCTION
You haven't created any masking rules.	

SQL users excluded from masking (administrators are always excluded) ⓘ

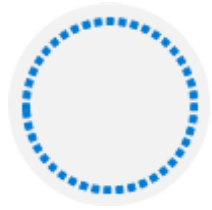
SQL users excluded from masking (administrators are always excluded) ✓

Recommended fields to mask

SCHEMA	TABLE	COLUMN	
SalesLT	Address	AddressID	Add mask
SalesLT	Address	AddressLine1	Add mask
SalesLT	Address	AddressLine2	Add mask
SalesLT	Customer	FirstName	Add mask
SalesLT	Customer	LastName	Add mask

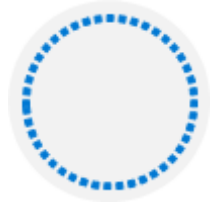
Load more

Review questions



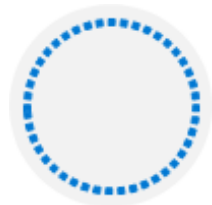
Q01 – Which TCP ports should be configured on your network and computer to allow Azure Synapse Studio to work?

A01 – TCP Port 80, 443 and 1443



Q02 – Which Azure Key Vault object stores storage account key information?

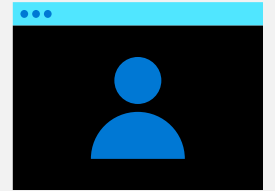
A02 – Secrets



Q03 – Encrypted communication is turned on automatically when connecting to Azure Synapse Analytics. True or False?

A03 – True

Lab: Run interactive queries using Azure Synapse Analytics serverless SQL pools



Lab overview

In this lab, students will learn how to secure a Synapse Analytics workspace and its supporting infrastructure. The student will observe the SQL Active Directory Admin, manage IP firewall rules, manage secrets with Azure Key Vault and access those secrets through a Key Vault linked service and pipeline activities. The student will understand how to implement column-level security, row-level security, and dynamic data masking when using dedicated SQL pools.

Lab objectives

After completing this lab, you will be able to:

Securing Azure Synapse Analytics supporting infrastructure

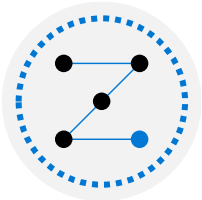
Securing the Azure Synapse Analytics workspace and managed services

Securing Azure Synapse Analytics workspace data

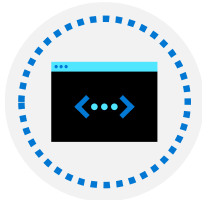
Lab review



Question 1 – Where do you set the SQL Active directory admin account?



Question 2 – Which UDP port should be open to use Azure Synapse Studio?



Question 3 – Which Azure Key Vault permission are required for your Azure Synapse workspace to access the values for secrets that it stores?



Question 4 – How can you set Transparent Data Encryption in Azure Synapse Analytics?

Module summary

In this module, you have learned about:

Secure a data warehouse in Azure Synapse Analytics

Configure and manage secrets in Azure Key Vault

Implement compliance controls for sensitive data

Next steps

After the course, consider visiting [[Azure security baseline for Synapse Analytics](#)]. The Azure Security Benchmark provides recommendations on how you can secure your cloud solutions on Azure.

