



DP-200T01: Securing Azure Data Platforms



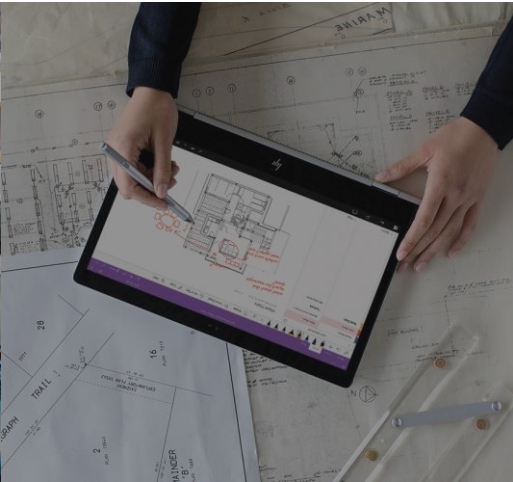
Agenda

- L01 - An introduction to security
- L02 - Key security components
- L03- Securing Storage Accounts and Data Lake Storage
- L04 - Securing data stores
- L05 - Securing streaming data



Lesson 01

An Introduction to Security

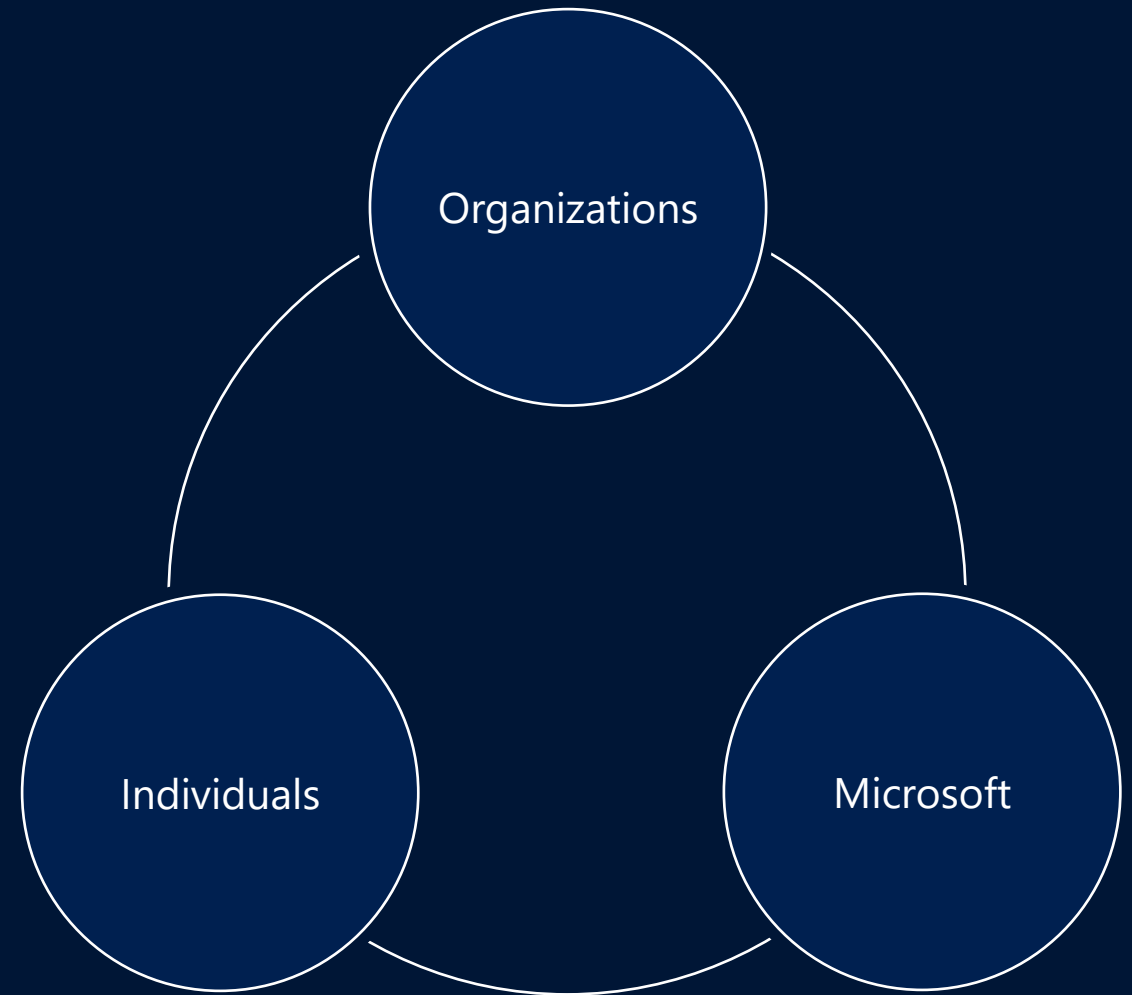


Lesson Objectives

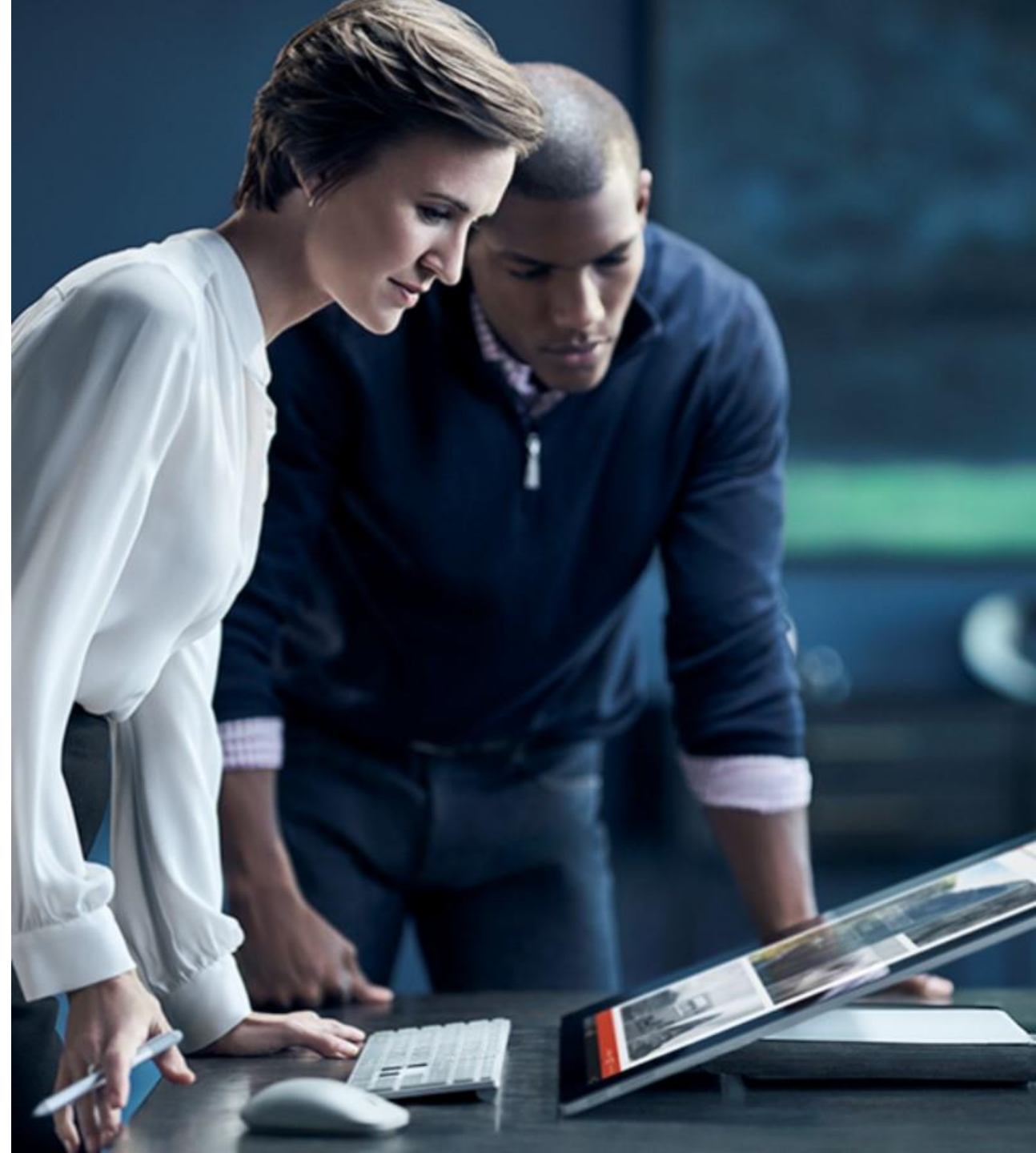
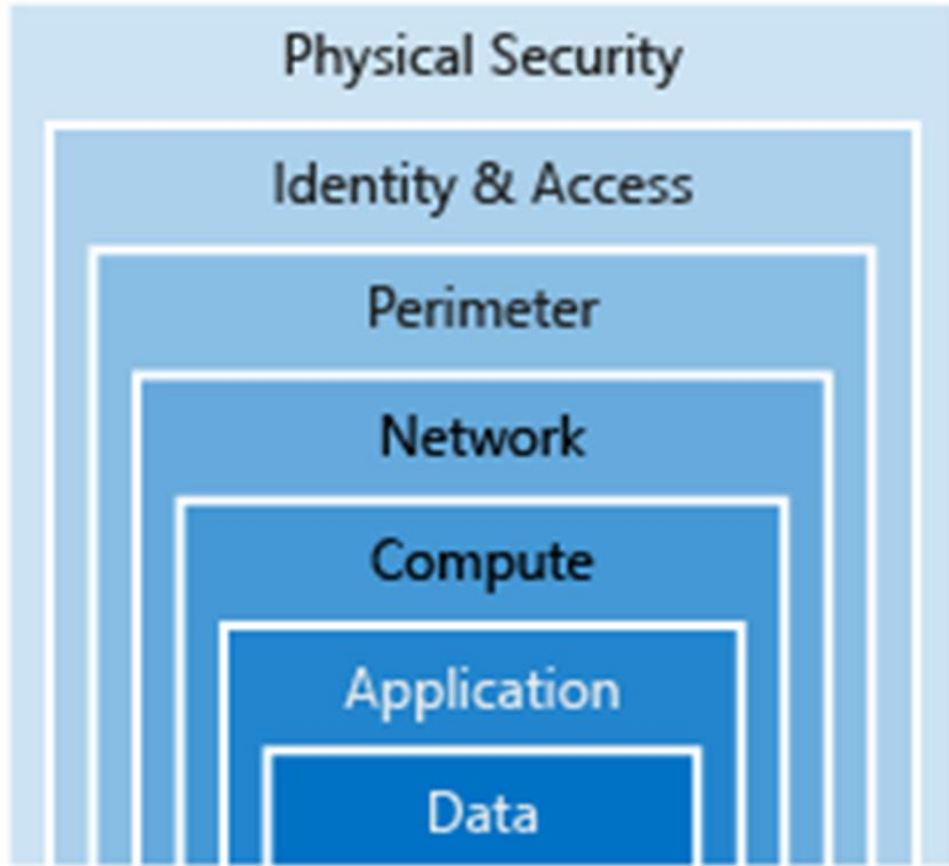
- Shared Security Responsibility
- A layered approach to security
- The Azure Security Center
- Azure Government



Shared Security Responsibility



A Layered Approach to Security.



Azure Security Center



Microsoft Azure

Overview Solutions **Products** Documentation Pricing Training Marketplace Partners

Azure Security Center

Gain unmatched hybrid security management and threat protection

[Turn on Security Center >](#)

Not yet subscribed to Azure? [Start free >](#)

Pricing > Documentation > Updates > Training >

Turn on protection you need

Microsoft uses a wide variety of physical, infrastructure, and additional actions you need to take to help safeguard your your security posture and protect against threats.

Use for incident response

You can use Security Center during the detection, assessment, and diagnosis of security at various stages.

Use to enhance security.

Reduce the chances of a significant security event by configuring a security policy, and then implementing the recommendations provided by Azure Security Center.

Azure Government

**Modernize
Government
Services**

**Provide a
platform of
agility**

**Advanced
Government
Mission**

**Physically
separate from
Azure**

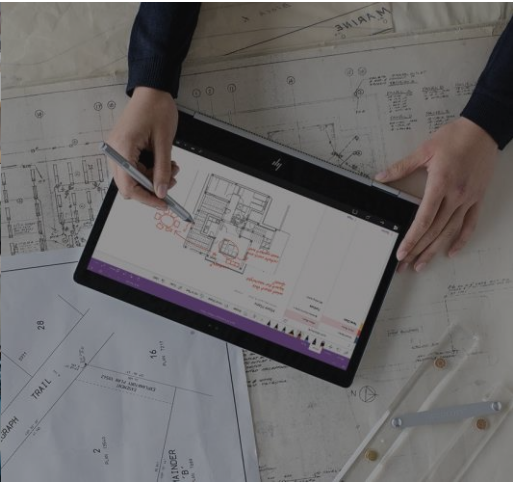
Review Questions

- Q01 – Cloud security is a shared responsibility between you and your cloud provider. Which category of cloud services requires the greatest security effort on your part?
- A01 – Infrastructure as a service (IaaS)
- Q02 – Which one of the following is a key difference between global Azure and Azure Government?
- A02 – Azure Government is a physically separate instance of Azure.



Lesson 02

Key Security Components



Lesson Objectives

- Network security
- Identity and access management
- Encryption capabilities built into Azure
- Azure Threat Protection

Network Security

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

Internet Protection

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.

Firewalls

To provide inbound protection at the perimeter, there are several choices:

- Azure Firewall
- Azure Application Gateway
- Azure Storage Firewall

DDoS Protection

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

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.

Encryption

Encryption at rest

Data at rest is the data that has been stored on a physical medium. This could be data stored on the disk of a server, data stored in a database, or data stored in a storage account.

Encryption in transit

Data in transit is the data actively moving from one location to another, such as across the internet or through a private network. Secure transfer can be handled by several different layers.

Encryption on Azure.

Raw Encryption

Enables the encryption of:

- Azure Storage
- V.M. Disks
- Disk Encryption

Database Encryption

Enables the encryption of databases using:

- Transparent Data Encryption

Encrypting Secrets

Azure Key Vault is a centralized cloud service for storing your application secrets.

Azure Threat Protection

The screenshot displays the Azure Advanced Threat Protection (ATP) interface, specifically the 'Timeline' view for the 'contoso-corp' environment. The interface features a dark header bar with the title 'Azure Advanced Threat Protection | contoso-corp | Timeline', a search icon, a document icon, and the Microsoft logo. The main content area is a vertical timeline of security events, each with a timestamp, a title, a description, and an 'OPEN' button. The events are as follows:

- 4:04 PM Today**: **Honeytoken activity** (Updated). The following activities were performed by **Bob Minion**:
 - Logged in to 2 computers via **Contoso-DC**.
 - Authenticated from 2 computers using Kerberos when accessing 5 resources against **Contoso-DC**.
 - Authenticated from **ITARGOET-T4705** using NTLM against corporate resources via **Contoso-DC**.Started at 3:08 PM Jan 22, 2018.
- 3:23 PM Jan 22, 2018**: **Remote execution attempt detected**. The following remote execution attempts were performed on **Contoso-DC** from **ALICE-DESKTOP**:
 - Attempted remote execution of one or more WMI methods by **AdminUser**.
- 3:06 PM Jan 22, 2018**: **Suspicious service creation**. **AdminUser** created 10 services in order to execute potentially malicious commands on **Contoso-DC**.
- 3:03 PM Jan 22, 2018**: **Brute force attack using LDAP simple bind**. 200 password guess attempts were made on 2 accounts from **ALICE-DESKTOP**. 2 account passwords were successfully guessed.
- 2:59 PM Jan 22, 2018**: **Reconnaissance using account enumeration**. Suspicious account enumeration activity using Kerberos protocol, originating from **ALICE-DESKTOP**, was detected. The attacker performed a total of 101 guess attempts for account names. 2 guess attempts matched existing account names in Active Directory.
- 12:38 PM Jan 21, 2018**: **Malicious replication of directory services**. Malicious replication requests were attempted by **Alice Liddel**, from **ALICE-DESKTOP** against **Contoso-DC**.
- 11:59 AM Jan 21, 2018**: **Reconnaissance using DNS**. Suspicious DNS activity was observed, originating from **ALICE-DESKTOP** (which is not a DNS server) against **Contoso-DC**.

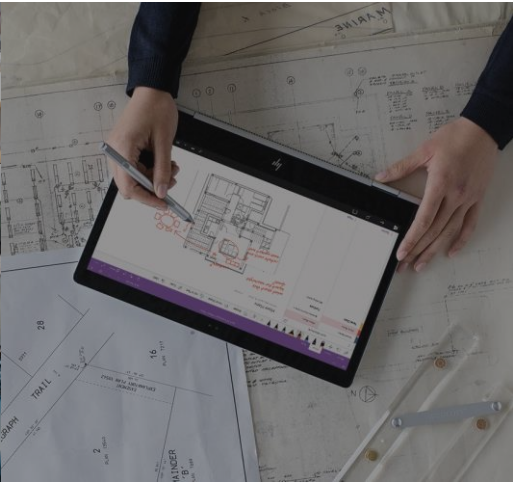
Review Questions

- Q01 - Which of these is the *strongest* way to protect sensitive customer data?
- A01 – Encrypt data both as it sits in your database and as it travels over the network
- Q02 - You want to store certificates in Azure to centrally manage them for your services. Which Azure service should you use?
- A02 – Azure Key Vault



Lesson 03

Securing Storage Accounts and Data Lake Storage



Lesson Objectives

- Storage Account security features
- Explore the authentication options available to access data
 - Storage Account Key
 - Shared Access Signature
- Control network access to the data
- Managing encryption
- Azure Data Lake Storage Gen II security features

Storage Account Security Features

**Encryption at
Rest**


**Encryption in
Transit**

**Role Based
Access Control**

**Auditing
Access**

Storage Account Keys

Home > [Resource groups](#) > [cto_rg](#) > ctoazureblob - Access keys

 **ctoazureblob - Access keys**
Storage account

Search (Ctrl+ /)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Events

Storage Explorer (preview)

Settings

Access keys

Geo-replication

CORS

Configuration

Encryption

Shared access signature


Use access keys to authenticate your applications when making requests to this Azure storage account. Store your access keys securely - for example, using Azure Key Vault - and don't share them. We recommend regenerating your access keys regularly. You are provided two access keys so that you can maintain connections using one key while regenerating the other.

When you regenerate your access keys, you must update any Azure resources and applications that access this storage account to use the new keys. This action will interrupt access to disks from your virtual machines. [Learn more](#)

Storage account name

ctoazureblob

key1




Key

eU7[REDACTED]Cg==

Connection string

Defa[REDACTED]9YrQ...

key2



Key

NW0[REDACTED]A/pUgB5w==

Connection string

Defa[REDACTED]Ns6...

Shared Access Signatures

Home > Resource groups > cto_rg > ctoazureblob - Shared access signature

ctoazureblob - Shared access signature

Storage account

Search (Ctrl+)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Events

Storage Explorer (preview)

Settings

Access keys

Geo-replication

CORS

Configuration

Encryption

Shared access signature

Firewalls and virtual networks

Advanced Threat Protection

Static website

Properties

Locks

Export template

Blob service

A shared access signature (SAS) is a URI that grants restricted access rights to Azure Storage resources. You can provide a shared access signature to clients who should not be trusted with your storage account key but whom you wish to delegate access to certain storage account resources. By distributing a shared access signature URI to these clients, you grant them access to a resource for a specified period of time.

An account-level SAS can delegate access to multiple storage services (i.e. blob, file, queue, table). Note that stored access policies are currently not supported for an account-level SAS.

[Learn more](#)

Allowed services ⓘ

☒ Blob ☒ File ☒ Queue ☒ Table

Allowed resource types ⓘ

☒ Service ☒ Container ☒ Object

Allowed permissions ⓘ

☒ Read ☒ Write ☒ Delete ☒ List ☒ Add ☒ Create ☒ Update ☒ Process

Start and expiry date/time ⓘ

Start

2019-03-29

11:59:33

End

2019-03-29

19:59:33

(UTC+00:00) --- Current Time Zone ---

Allowed IP addresses ⓘ

for example, 168.1.5.65 or 168.1.5.65-168.1.5.70

Allowed protocols ⓘ

☒ HTTPS only ☐ HTTPS and HTTP

Signing key ⓘ


key1

Generate SAS and connection string

Control network access to data

Firewalls and virtual networks

 Save  Discard  Refresh


 Firewall settings allowing access to storage services will remain in effect for up to a minute after saving updated settings restricting access.

Allow access from
☐ All networks ☒ Selected networks

Configure network security for your storage accounts. [Learn more.](#)


Virtual networks
Secure your storage account with virtual networks. [+ Add existing virtual network](#) [+ Add new virtual network](#)

VIRTUAL NETWORK	SUBNET	ADDRESS RANGE	ENDPOINT STATUS	RESOURCE GROUP	SUBSCRIPTION
No network selected.					

Firewall
Add IP ranges to allow access from the internet or your on-premises networks. [Learn more.](#)
☐ Add your client IP address ('86.184.235.180') 

ADDRESS RANGE

IP address or CIDR

Exceptions
☒ Allow trusted Microsoft services to access this storage account 
☐ Allow read access to storage logging from any network
☐ Allow read access to storage metrics from any network

Managing Encryption

Databases stores information that is sensitive, such as physical addresses, email addresses, and phone numbers. The following can be used to protect this data:

Transport Layer Security (TLS)

Azure SQL Database and Data Warehouse enforces Transport Layer Security (TLS) encryption at all times for all connections, which ensures all data is encrypted "in transit" between the database and the client.

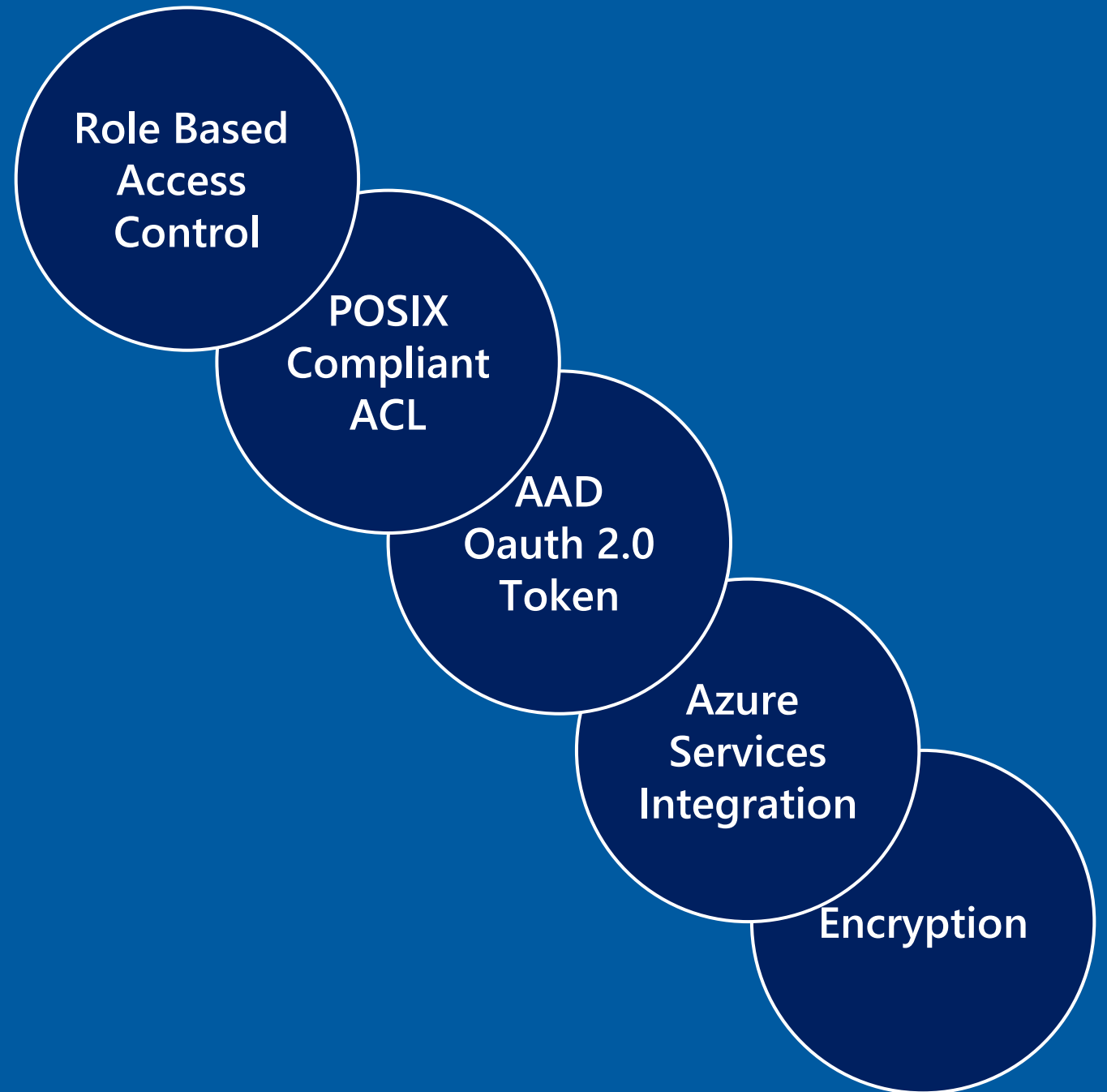
Transparent data encryption

Both Azure Data Warehouse and SQL Database protects your data at rest using transparent data encryption (TDE). TDE performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application.

Application encryption

Data in transit is a method to prevent man-in-the-middle attacks. To encrypt data in transit, specify **Encrypt=true** in the connection string in your client applications

Azure Data Lake Storage Gen2 Security Features



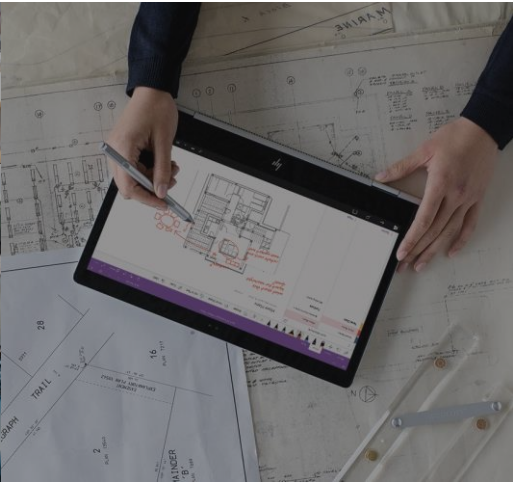
Review Questions

- Q01 – Mike is working as a consultant developing an application for a national Realtor company. They store thousands of images of houses in an Azure BLOB storage account. The web application Mike is developing needs to have access these images. How can Mike provide secure access for the third-party web application?
- A01 – Use a Shared Access Signature to give the web application access.
- Q02 – Mike wants to gain insights should any unusual activity be occurring with his storage account with minimal configuration. What can Mike use to achieve this?
- A02 – Automatic Threat Detection



Lesson 04

Securing Data Stores



Lesson Objectives

- Control network access to your data stores using firewall rules
- Control user access to your data stores using authentication and authorization
- Dynamic Data Masking
- Audit and monitor your Azure SQL Database for access violations

Control network access to your data stores using firewall rules

There are a number of ways you can control access to your Azure SQL Database or Data Warehouse over the network.

Server-level firewall rules

These rules enable clients to access your **entire Azure SQL server**, that is, all the databases within the same logical server.

Database level firewall rules

These rules allow access to an individual database on a logical server and are stored in the database itself. For database-level rules, only **IP address rules** can be configured.

Control user access to your data stores using authentication and authorization

Authentication

SQL Database and Azure Synapse Analytics supports two types of authentication: SQL authentication and Azure Active Directory authentication.

Authorization

Authorization is controlled by permissions granted directly to the user account and/or database role memberships. A database role is used to group permissions together to ease administration

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](#)

Auditing and Monitoring



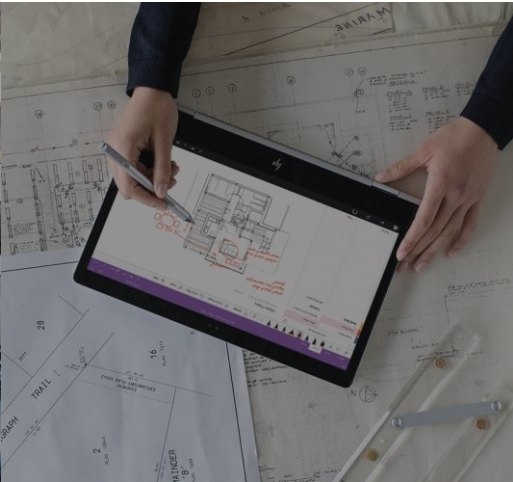
Review Questions

- Q01 – Which of the following is the most efficient way to secure a database to allow only access from a VNet while restricting access from the internet?
- A01 – A server-level virtual network rule
- Q02 – A mask has been applied to a column in the database that holds a user's email address, laura@contoso.com. From the list of options, what would the mask display for a database administrator account?
- A02 – laura@contoso.com
- Q03 – Encrypted communication is turned on automatically when connecting to an Azure SQL Database or Azure SQL Data Warehouse. True or False?
- A03 – True



Lesson 05

Securing Streaming Data



Lesson Objectives

- Understand Stream Analytic security
- Understand Event Hub security

Stream Analytics Security

Data in transit

Azure Stream Analytics encrypts all incoming and outgoing communications and supports Transport Layer Security v 1.2

Data at rest

Stream Analytics doesn't store the incoming data since all processing is done in-memory. Therefore, consider setting security for services such as Event Hubs or Internet of Things Hubs, or for data stores such as Cosmos DB.

Event Hub Security

Authentication

Authentication makes use of Shared Access Signatures and Event Publishers to ensure that only applications or devices with valid credentials are only allowed to send data to an Event Hub. Each client is assigned a token

Token Management

Once the tokens have been created, each client is provisioned with its own unique token. If a token is stolen by an attacker, the attacker can impersonate the client whose token has been stolen. Blacklisting a client renders that client unusable.

Review Questions

- Q01 – You need to set the encryption for the data stored in Stream Analytics. What should you do?
- A01 – It cannot be done
- Q02 – Authentication for an Event hub is defined with a combination of an Event Publisher and which other component?
- A02 - Shared Access Signature

Lab: Securing Azure Data Platforms



Lab overview

The students will be able to describe and document the different approaches to security that can be taken to provide defense in depth. This will involve the student documenting the security that has been set up so far in the course. It will also enable the students to identify any gaps in security that may exists for AdventureWorks.

Lab objectives

After completing this lab, you will be able to:

1. An Introduction to Security
2. Key security components
3. Securing Storage Accounts and Data Lake Storage
4. Securing Data Stores
5. Securing Streaming Data

Lab scenario

As a senior data engineer within AdventureWorks, you are responsible for ensuring that your data estate is secured. You are performing a security check of your current infrastructure to ensure that you have diligently placed security where it is required. This check should be a holistic check of all the services and data that you have created so far, and an identification of any gaps that there may be in the configuration of the security.

You have also been asked to tighten up the security of the SQL Database and have been asked to setup auditing against the database so that you can monitor access to the database. Furthermore, you have learned that the Manage permission for your event hub is not restrictive enough, and you want to remove this permission.

At the end of this lab, you will have:

1. An Introduction to Security
2. Key security components
3. Securing Storage Accounts and Data Lake Storage
4. Securing Data Stores
5. Securing Streaming Data

Lab review

- Exercise 1 – Do you perform regular holistic security audits with other IT professionals in your organization?
- Exercise 2 – Where you aware of the Azure Security Center?
- Exercise 3 – Would you have a need to use Shared Access Signatures?
- Exercise 4 – Would anyone in the room use Dynamic Data Masking?
Can you provide an example
- Exercise 5 – What is a Shared Access Policy?

Module Summary >

In this module, you have learned about:

- An introduction to security
- key security components
- Securing Storage Accounts and Data Lake Storage
- Securing Data Stores
- Securing Streaming Data

Next steps >

After the course, consider visiting [the Microsoft Learn website](#) to learn more about Role Based Access Permissions

