# AZ-500 4 Secure Data and Applications – completed 2-8-22


COURSE

**Microsoft Azure Security Technologies (AZ-500) Cert Prep: 4 Secure Data and Applications**

LinkedIn Learning · By: Pete Zerger · 2 months ago

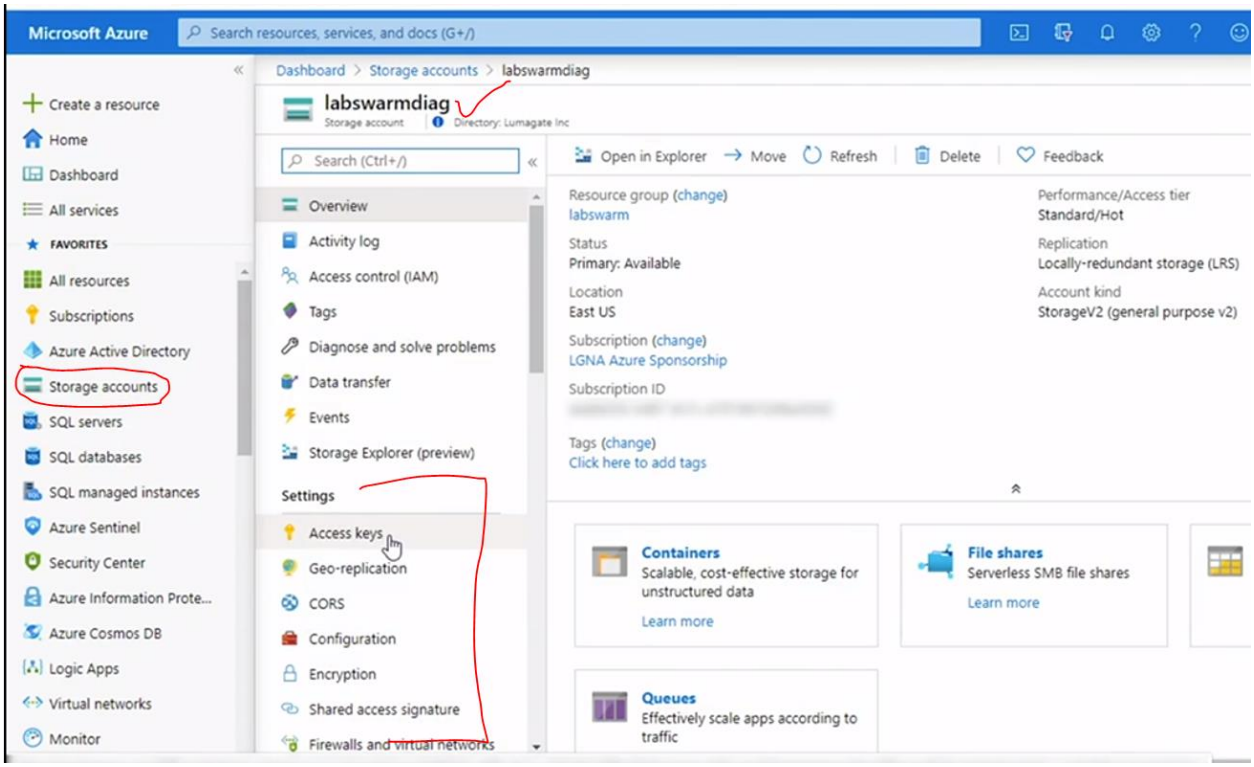
Start your preparations for the "Secure data and applications" domain of the AZ-500 exam.

[Become an Azure Security Engineer (linkedin.com)]

## Table of Contents

# 1. Configure Security for Storage

## 1.1 Configure access control for storage

Dashboard > Storage accounts > labswarmdiag | Access keys

## labswarmdiag | Access keys

Storage account | Directory: Lumagate Inc

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Data transfer
- Events
- Storage Explorer (preview)

Settings

- Access keys
- Geo-replication
- CORS
- Configuration
- Encryption
- Shared access signature
- Firewalls and virtual networks

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 not interrupt access to disks from your virtual machines. Learn more about regenerating storage access keys

Storage account name

labswarmdiag

**key1**

Key

KWSTHcUMAerwDlAJJZJU4WleDvYDO03HbDHL9XT/tg+aWUK2bFYb2zZg3B0qWRXCRWH88pGq9Koh/qnG26pbEw==

Connection string

DefaultEndpointsProtocol=https;AccountName=labswarmdiag;AccountKey=KWSTHcUMAerwDlAJJZJU4WleDvYDO03HbDHL9XT/tg+a...

**key2**

Key

GLlKt4nZNCN/NKZ78rpUvgpsi1NPRcEAkaPfhKdF50Vl4+fu0QMRdDa4wH0vzvhgROO2lOvvrR55ylmoYqASug==

Connection string

DefaultEndpointsProtocol=https;AccountName=labswarmdiag;AccountKey=GLlKt4nZNCN/NKZ78rpUvgpsi1NPRcEAkaPfhKdF50Vl4+fu...

LinkedIn Learning

rch resources, services, and docs (G+/)

Dashboard > Storage accounts > labswarmdiag | Shared access signature

## labswarmdiag | Shared access signature

Storage account | Directory: Lumagate Inc

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Data transfer
- Events
- Storage Explorer (preview)

Settings

- Access keys
- Geo-replication
- CORS
- Configuration
- Encryption
- Shared access signature
- Firewalls and virtual networks

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

03/09/2020 | 4:52:35 PM

End

03/10/2020 | 12:52:35 AM

(UTC-06:00) Central Time (US & Canada)

Allowed IP addresses

for example, 168.1.5.65 or 168.1.5.65-168.1.5.70

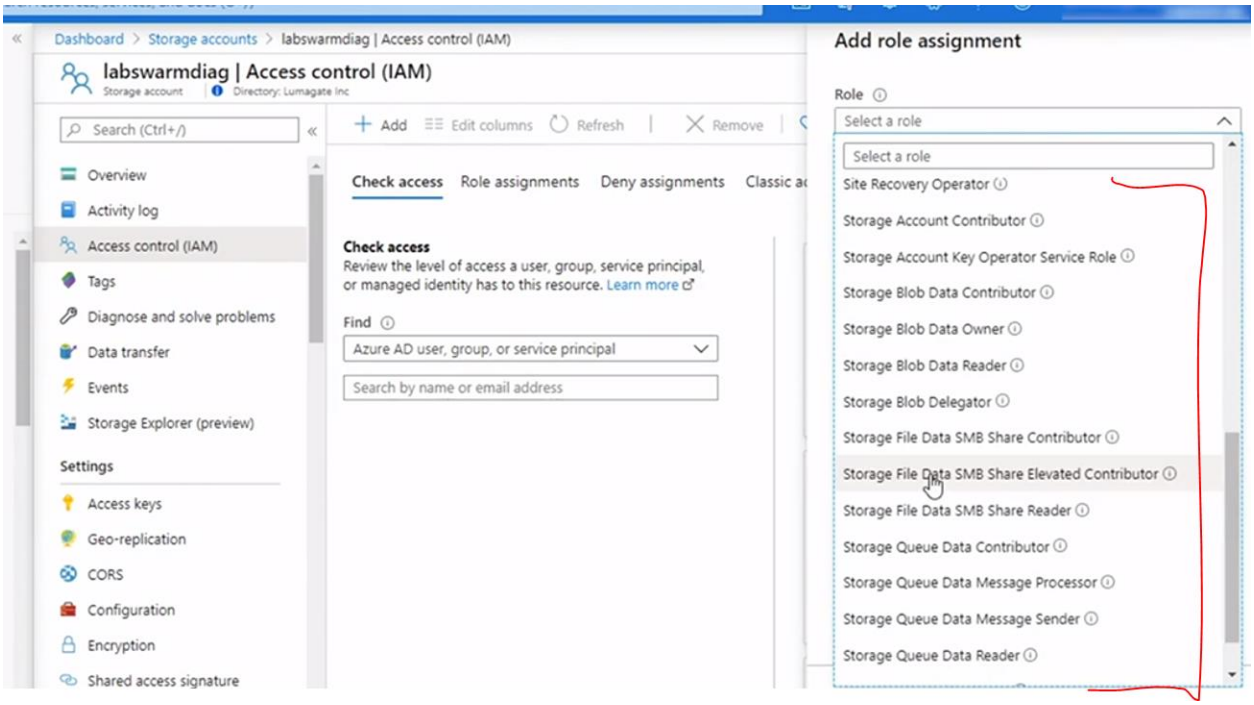
Allowed protocols

◉ HTTPS only ○ HTTPS and HTTP

Signing key

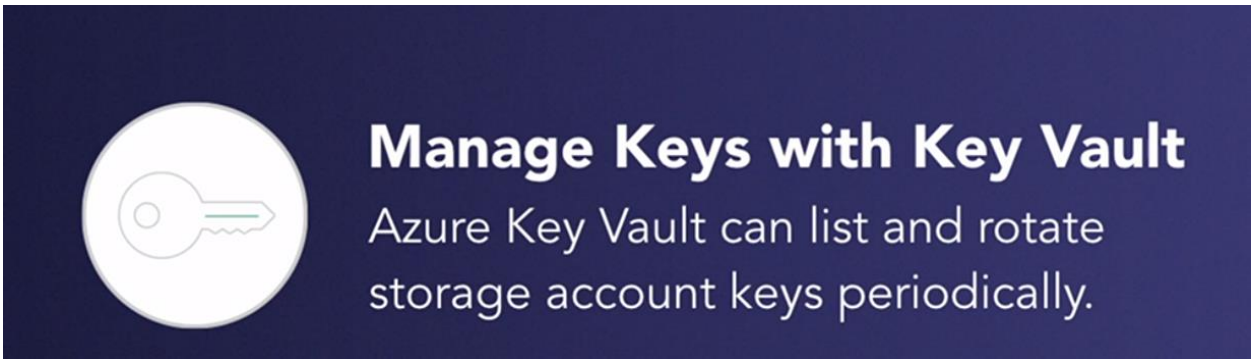
key1

Generate SAS and connection string





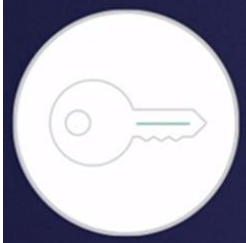
## 1.2 Configure storage account access keys



## Microsoft Guidance on Key Management

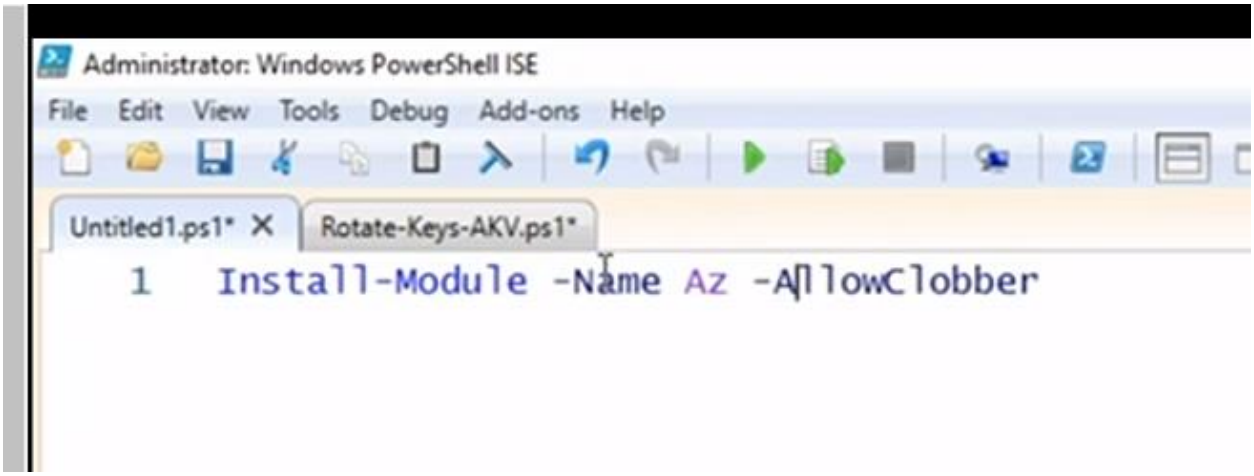
Regenerate keys by using Key Vault only. Don't manually regenerate your storage account keys.

With Azure AD, you can authenticate your client app using an app or user identity. **No storage account credentials are needed.**



## AKV and SAS Tokens

You can also ask Key Vault to generate shared access signature tokens.



Administrator: Windows PowerShell ISE

File Edit View Tools Debug Add-ons Help

Untitled1.ps1* | Rotate-Keys-AKV.ps1*

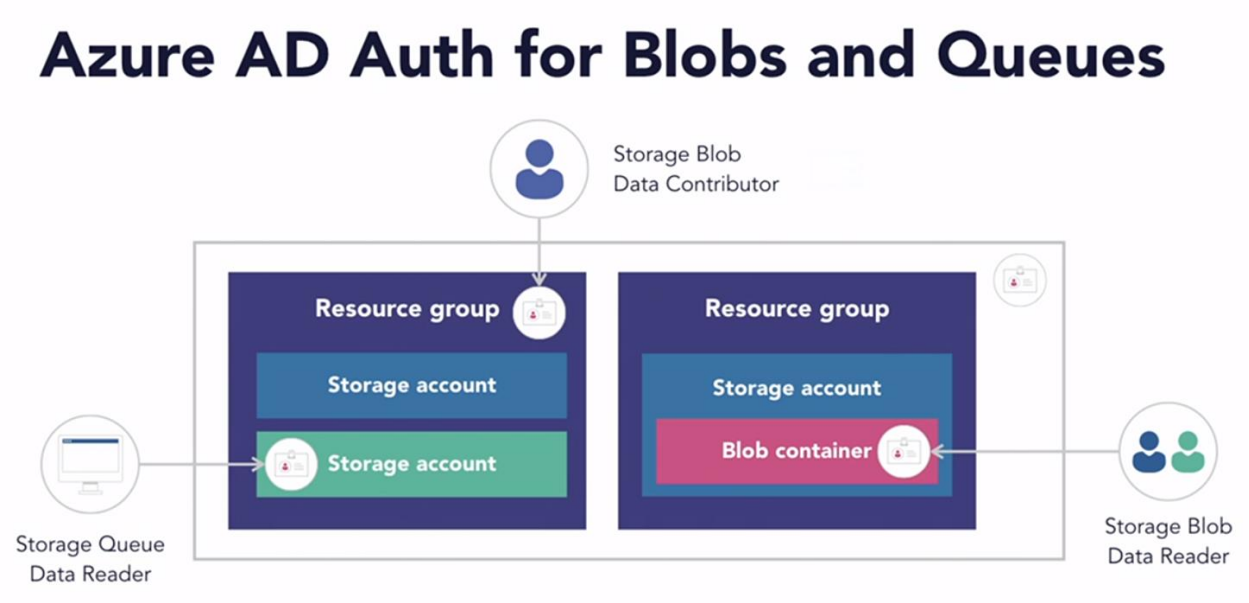
```
# Authenticate to Azure
Connect-AzAccount
Set-AzContext -SubscriptionId [illegible]

# Set variables
$resourceGroupName = "labswarm"
$storageAccountName = "labswarmdiag"
$keyVaultName = "kineteco-akv"
$keyVaultSpAppId = "cfa8b339-82a2-471a-a3c9-0fc0be7a4093"
$storageAccountKey = "key1"

# Get your User Id
$userId = (Get-AzContext).Account.Id

# Get a reference to your Azure storage account
$storageAccount = Get-AzStorageAccount `
-ResourceGroupName $resourceGroupName `
```

Untitled1.ps1* | Rotate-Keys-AKV.ps1*

```
New-AzRoleAssignment -ApplicationId $keyVaultSpAppId `
-RoleDefinitionName 'Storage Account Key Operator Service Role' `
-Scope $storageAccount.Id

# Give your user principal access to all storage account permissions, on your Key Vault instance
Set-AzKeyVaultAccessPolicy -VaultName $keyVaultName -UserPrincipalName $userId `
-PermissionsToStorage get, list, delete, set, update, regeneratekey, getsas, listsas, deletesas, setsas, recover, backup, re

# Enable key regeneration
$regenPeriod = [System.Timespan]::FromDays(3)
Add-AzKeyVaultManagedStorageAccount -VaultName $keyVaultName -AccountName $storageAccountName `
-AccountResourceId $storageAccount.Id -ActiveKeyName $storageAccountKey -RegenerationPeriod $regenPeriod
```

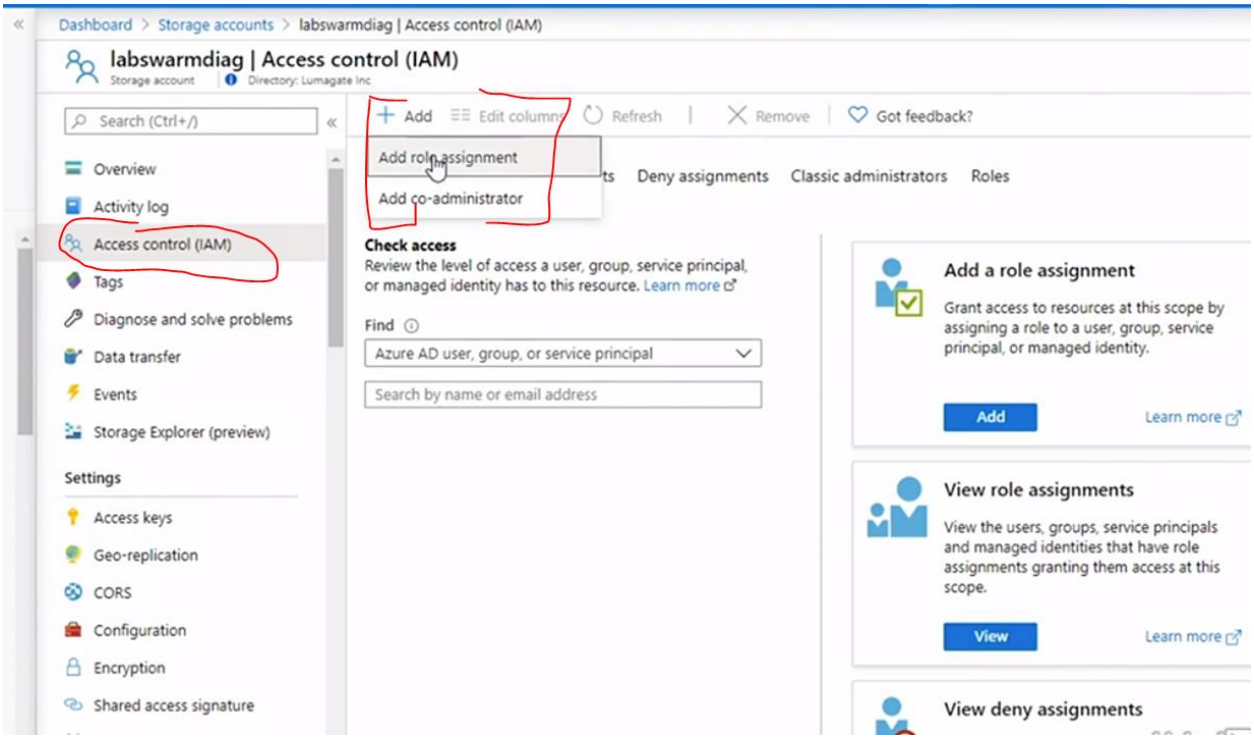
```
PS C:\WINDOWS\system32> $regenPeriod = [System.Timespan]::FromDays(3)
Add-AzKeyVaultManagedStorageAccount -VaultName $keyVaultName -AccountName $storageAccountName `
-AccountResourceId $storageAccount.Id -ActiveKeyName $storageAccountKey -RegenerationPeriod $regenPeriod


Id                  : https://kineteco-akv.vault.azure.net:443/storage/labswarmdiag
Vault Name          : kineteco-akv
AccountName         : labswarmdiag
Account Resource Id : /subscriptions/[illegible]/resourceGroups/labswarm/providers/Microsoft.Storage/s
                      torageAccounts/labswarmdiag
Active Key Name     : key1
Auto Regenerate Key : True
Regeneration Period : 3.00:00:00
Enabled             : True
```

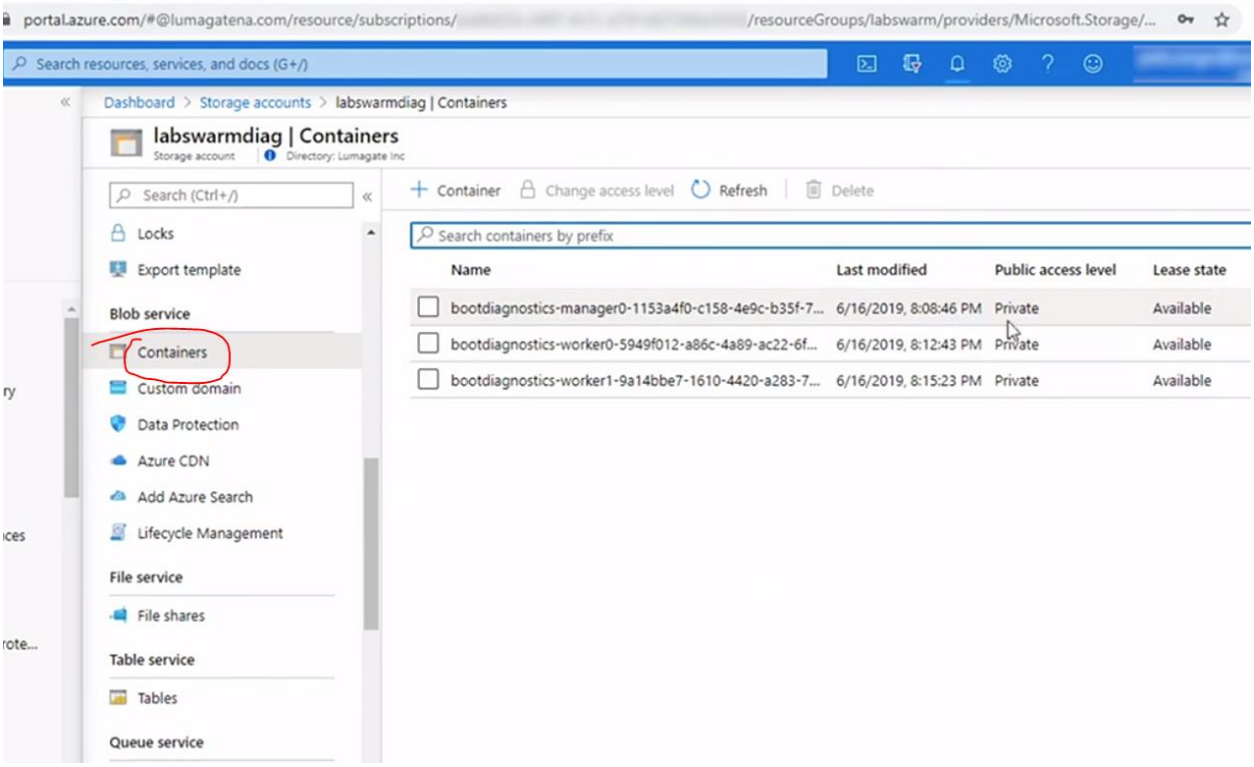
## 1.3 Configure Azure AD authentication for Azure Storage



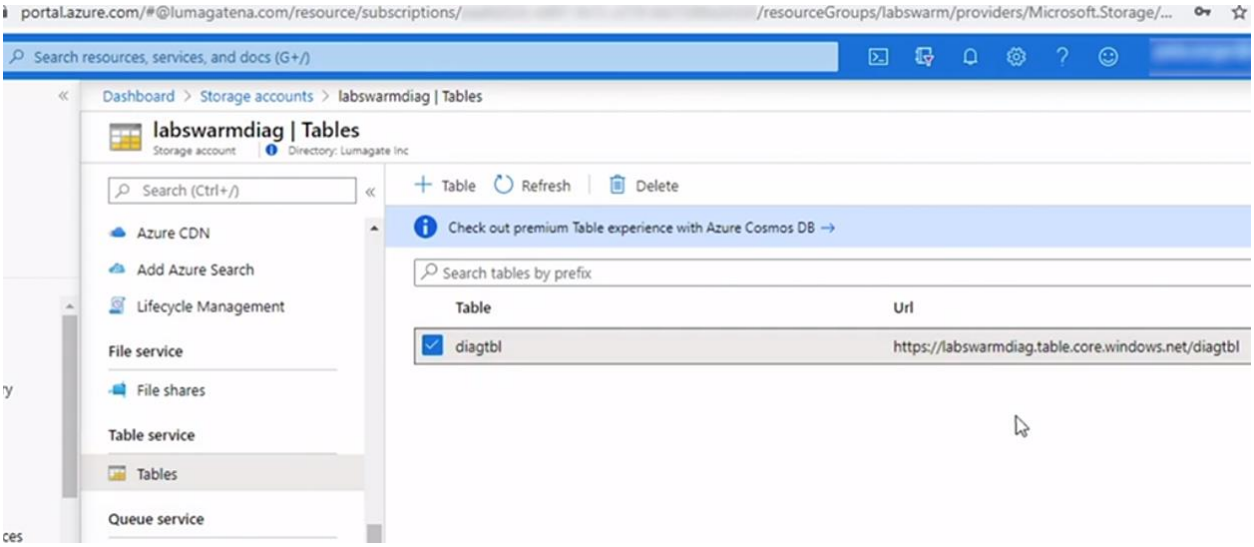

# Azure Storage RBAC Roles

| | | |
|---|---|---|
| Storage Blob Data Contributor | Storage Blob Data Owner | Storage Blob Data Reader |
| Storage Blob Delegator | Storage File Data SMB Share Contributor | Storage File Data SMB Share Elevated Contributor |
| Storage File Data SMB Share Reader | Storage Queue Data Contributor | Storage Queue Data Message Processor |
| Storage Queue Data Message Sender | Storage Queue Data Reader | |



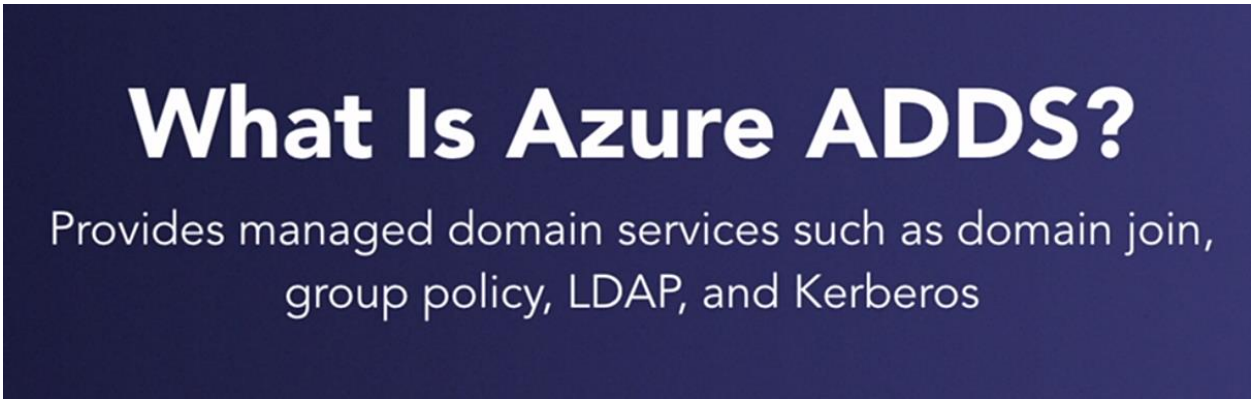



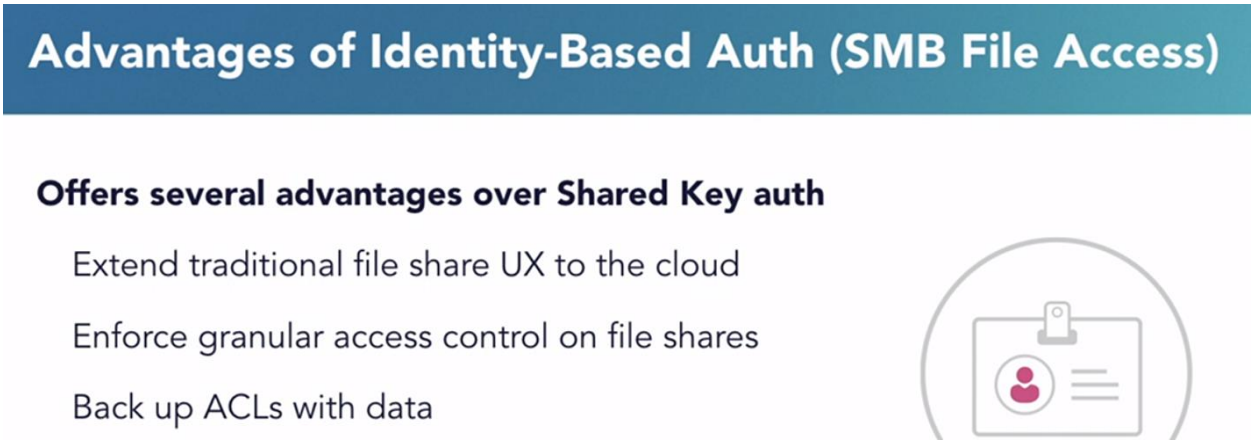

Containers support AD authentication




Tables do not support AD authentication

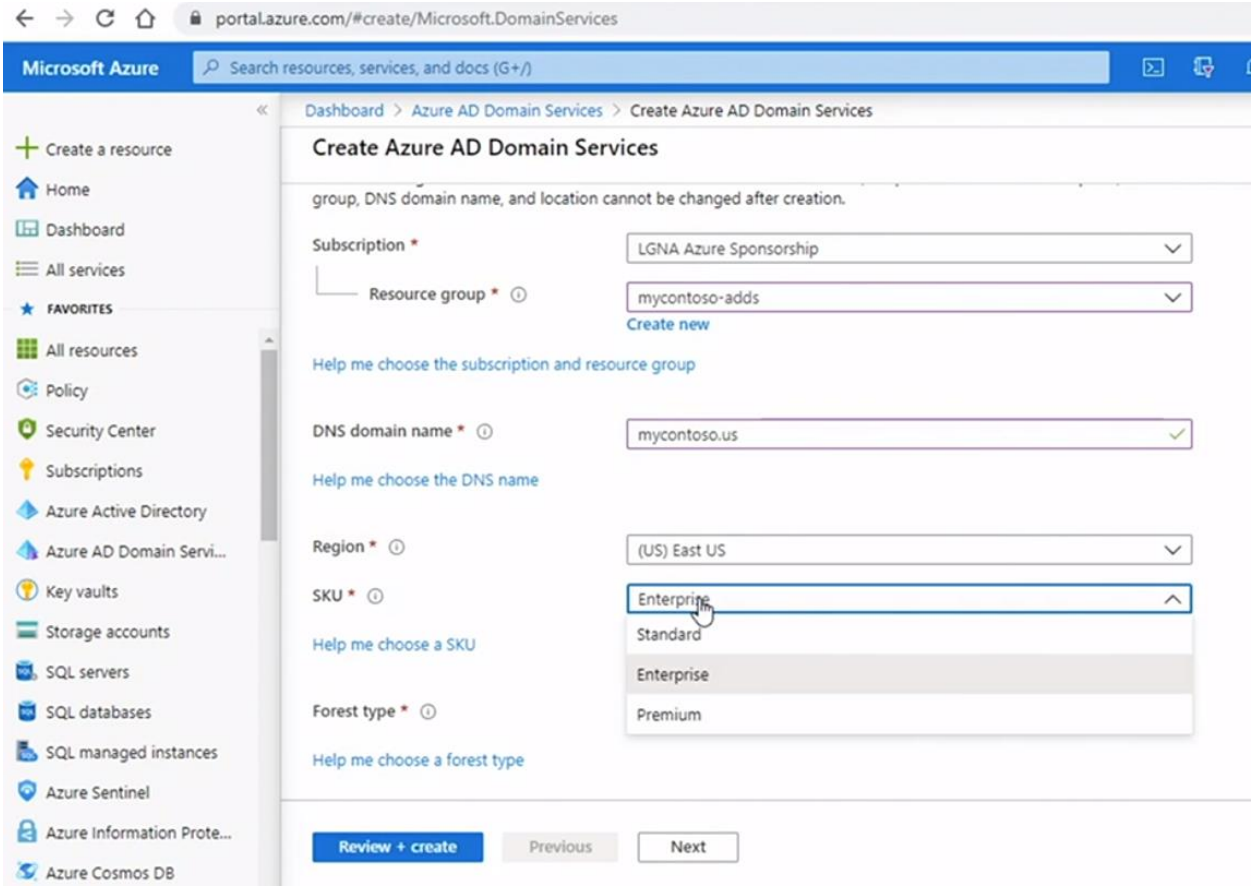
## 1.4 Azure AD Domain Services authentication for Azure Files

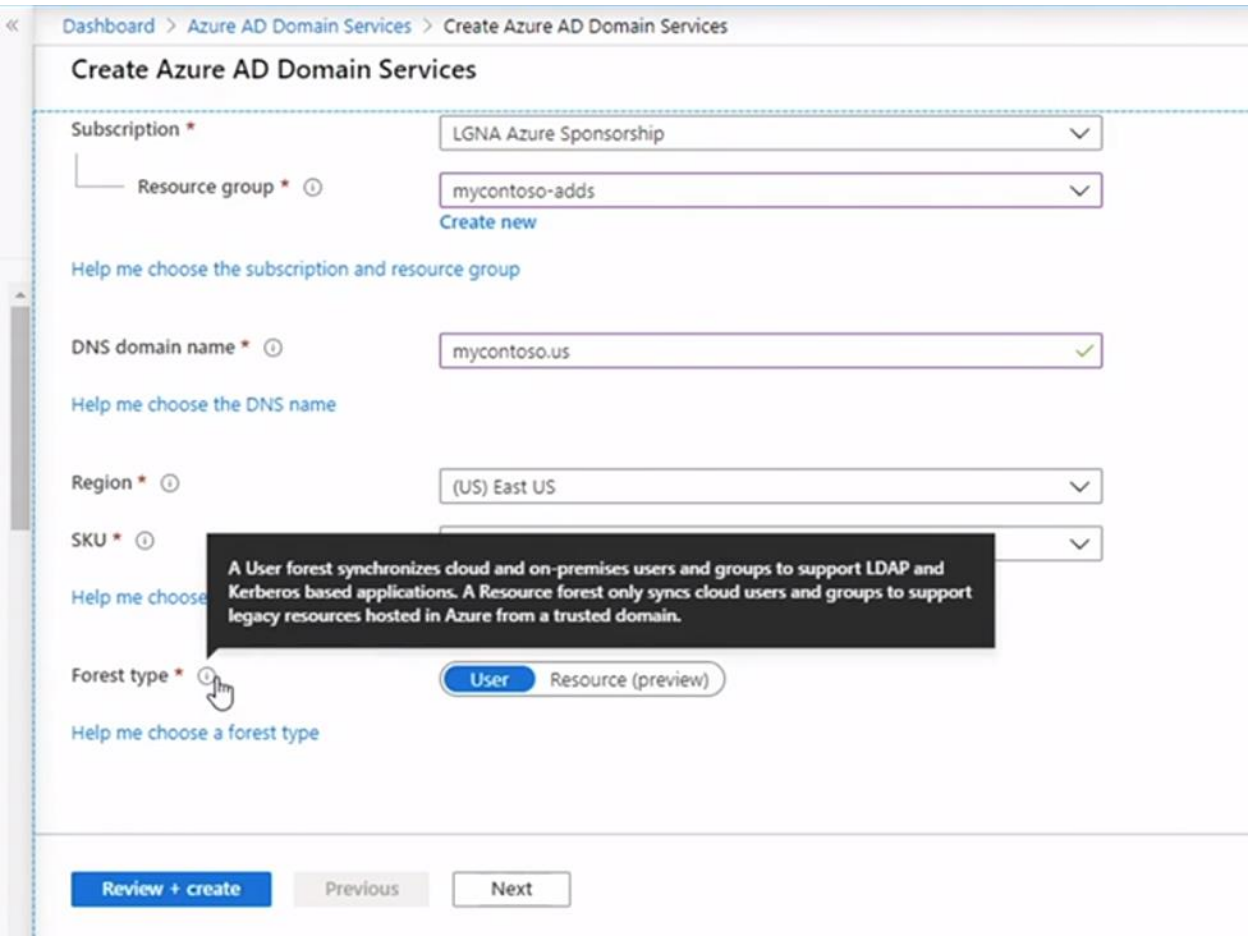


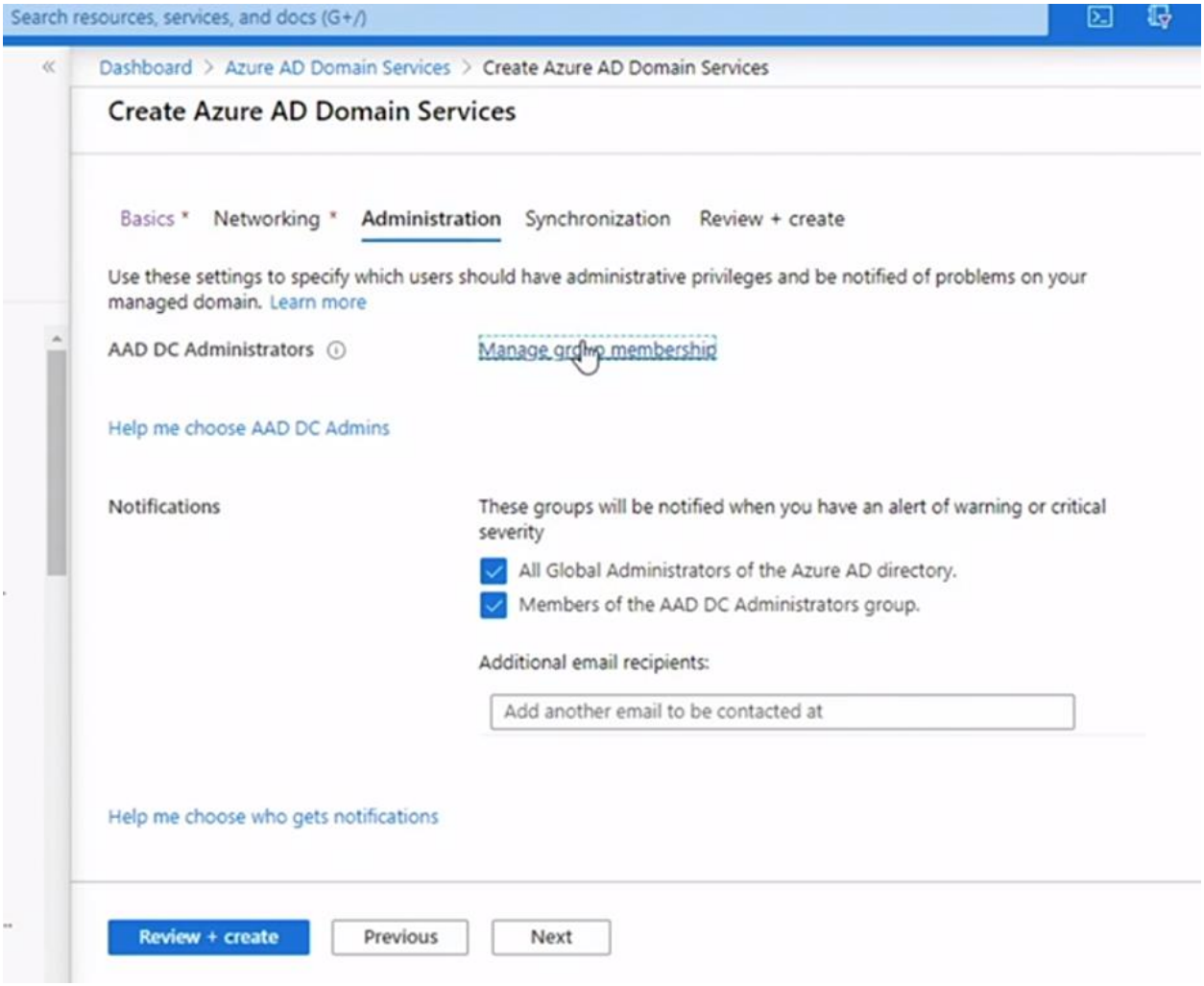



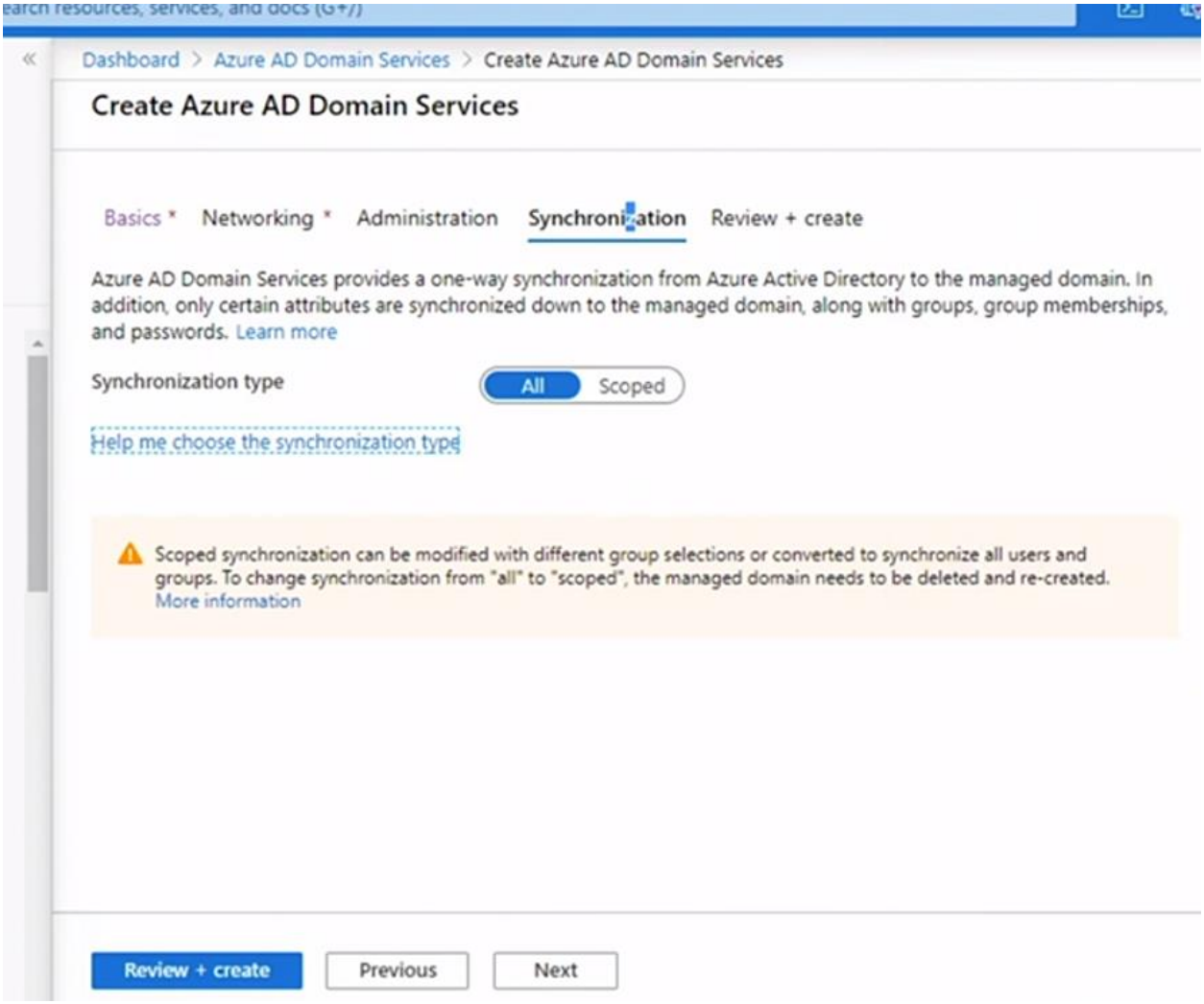
# Prerequisites

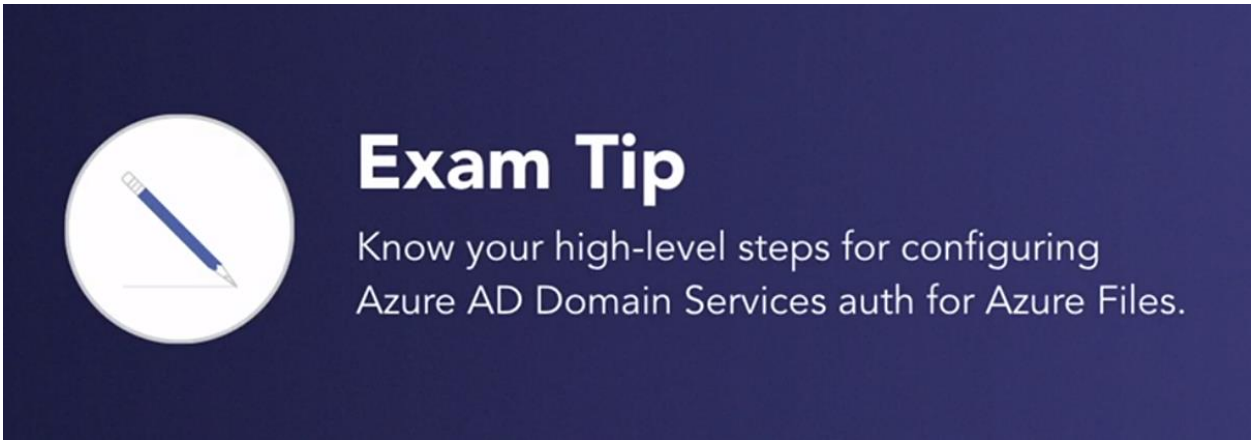
- Select or create an **Azure AD** tenant
- Enable **Azure AD Domain Services** on the tenant
- **Domain join** Azure VMs with AADDS




Dashboard > Azure AD Domain Services > Create Azure AD Domain Services
Create Azure AD Domain Services
Subscription *
LGNA Azure Sponsorship
Resource group *
mycontoso-adds
Create new
Help me choose the subscription and resource group
DNS domain name *
mycontoso.us
Help me choose the DNS name
Region *
(US) East US
SKU *
Help me choose
A User forest synchronizes cloud and on-premises users and groups to support LDAP and Kerberos based applications. A Resource forest only syncs cloud users and groups to support legacy resources hosted in Azure from a trusted domain.
Forest type *
User
Resource (preview)
Help me choose a forest type
Review + create
Previous
Next


Search resources, services, and docs (G+/)
Dashboard > Azure AD Domain Services > Create Azure AD Domain Services
Create Azure AD Domain Services
Basics *
Networking *
Administration
Synchronization
Review + create
Use these settings to specify which users should have administrative privileges and be notified of problems on your managed domain. Learn more
AAD DC Administrators
Manage group membership
Help me choose AAD DC Admins
Notifications
These groups will be notified when you have an alert of warning or critical severity
All Global Administrators of the Azure AD directory.
Members of the AAD DC Administrators group.
Additional email recipients:
Add another email to be contacted at
Help me choose who gets notifications
Review + create
Previous
Next


Dashboard > Azure AD Domain Services > Create Azure AD Domain Services
Create Azure AD Domain Services
Basics * Networking * Administration Synchronization Review + create
Azure AD Domain Services provides a one-way synchronization from Azure Active Directory to the managed domain. In addition, only certain attributes are synchronized down to the managed domain, along with groups, group memberships, and passwords. Learn more
Synchronization type
All Scoped
Help me choose the synchronization type
Scoped synchronization can be modified with different group selections or converted to synchronize all users and groups. To change synchronization from "all" to "scoped", the managed domain needs to be deleted and re-created.
More information
Review + create
Previous
Next


Exam Tip
Know your high-level steps for configuring Azure AD Domain Services auth for Azure Files.

## 1.5 Quiz

Question 1 of 5

You can configure Azure AD authentication for which of the following?

- queues and files
- queues, blobs, and files
- queues, blobs, and tables
- queues and blobs
  Correct
  Only Azure Storage's queues and blobs support Azure AD authentication.

Next question

Question 2 of 5

Microsoft recommends Shared Keys should be rolled automatically using _____.

- Azure Functions
- Logic Apps
- Azure Automation
- Azure Key Vault
  Correct
  Microsoft recommends automating rolling of storage account keys exclusively with Key Vault.

Next question

Question 3 of 5

What key advantage do storage access signatures have over access keys?

- They throttle storage transactions to protect performance.
- They enable permanent administrator-level access.
- They enable programmatic access.
- ✓ They restrict the scope and duration of access.
  Correct
  The key advantage of SAS is the ability to limit the scope and duration of delegated permissions to Azure storage.

Next question

Question 4 of 5

A resource forest in Azure AD Domain Services will sync accounts from on-premises as well as Azure.

- ✓ FALSE
  Correct
  Accounts from resource forests are not synchronized.
- TRUE

Next question

Question 5 of 5

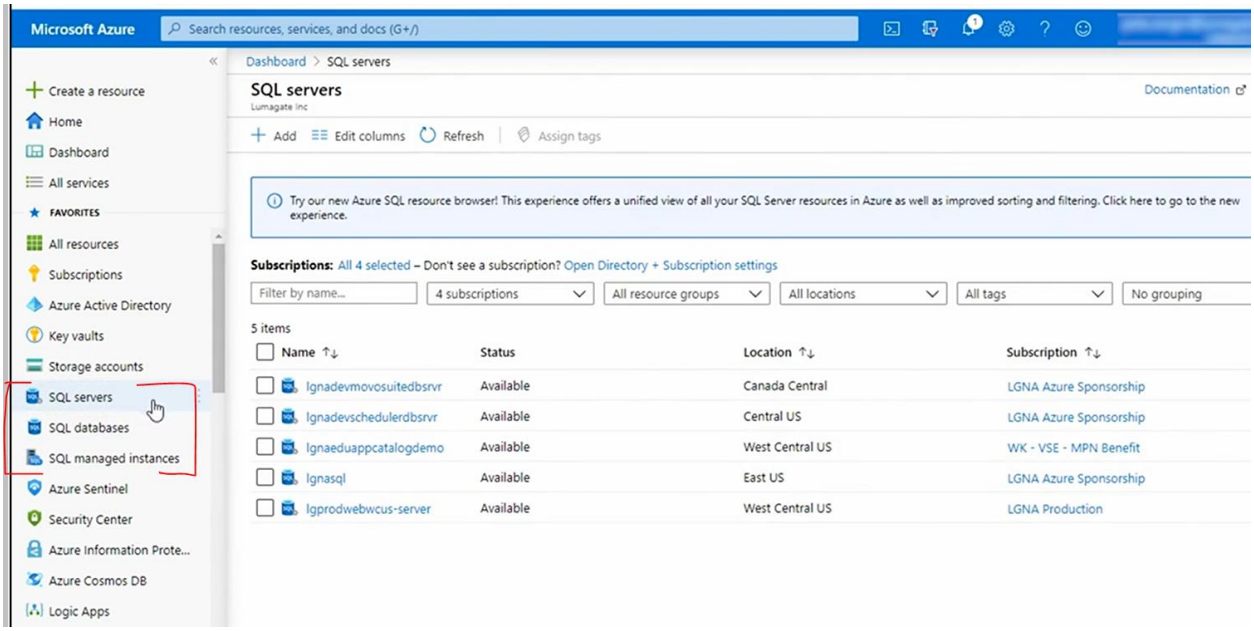
SAS tokens provide root access to an Azure Storage account until the key is revoked or rolled.

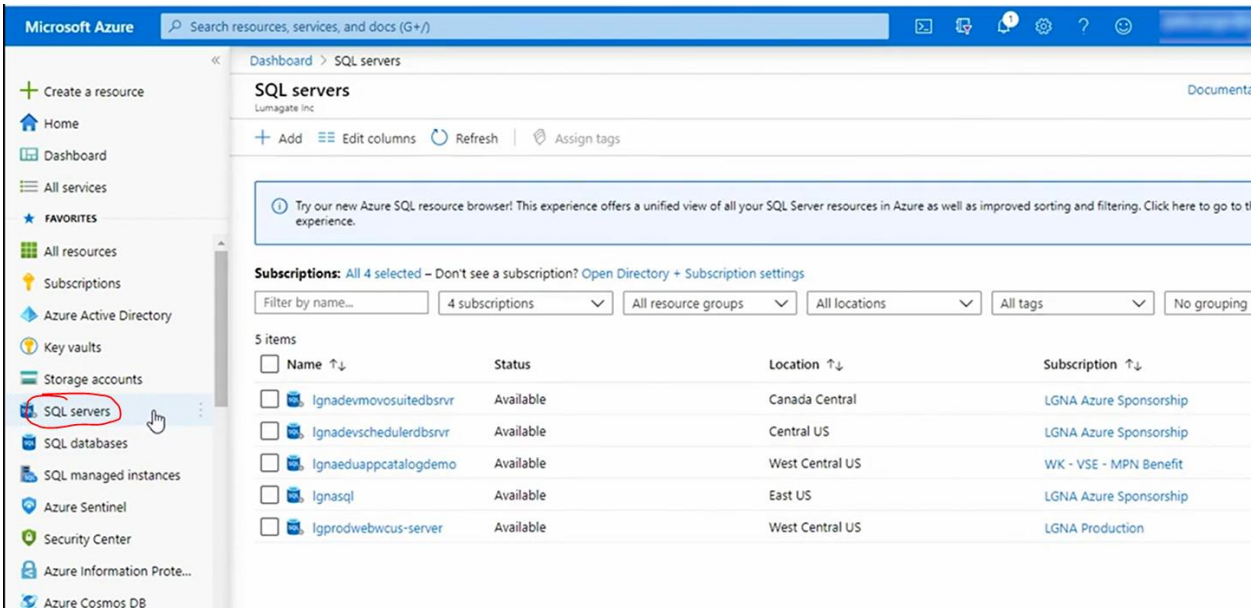
- ✓ FALSE
  Correct
  This describes Shared Keys. SAS tokens are limited to a specific window of time.
- TRUE

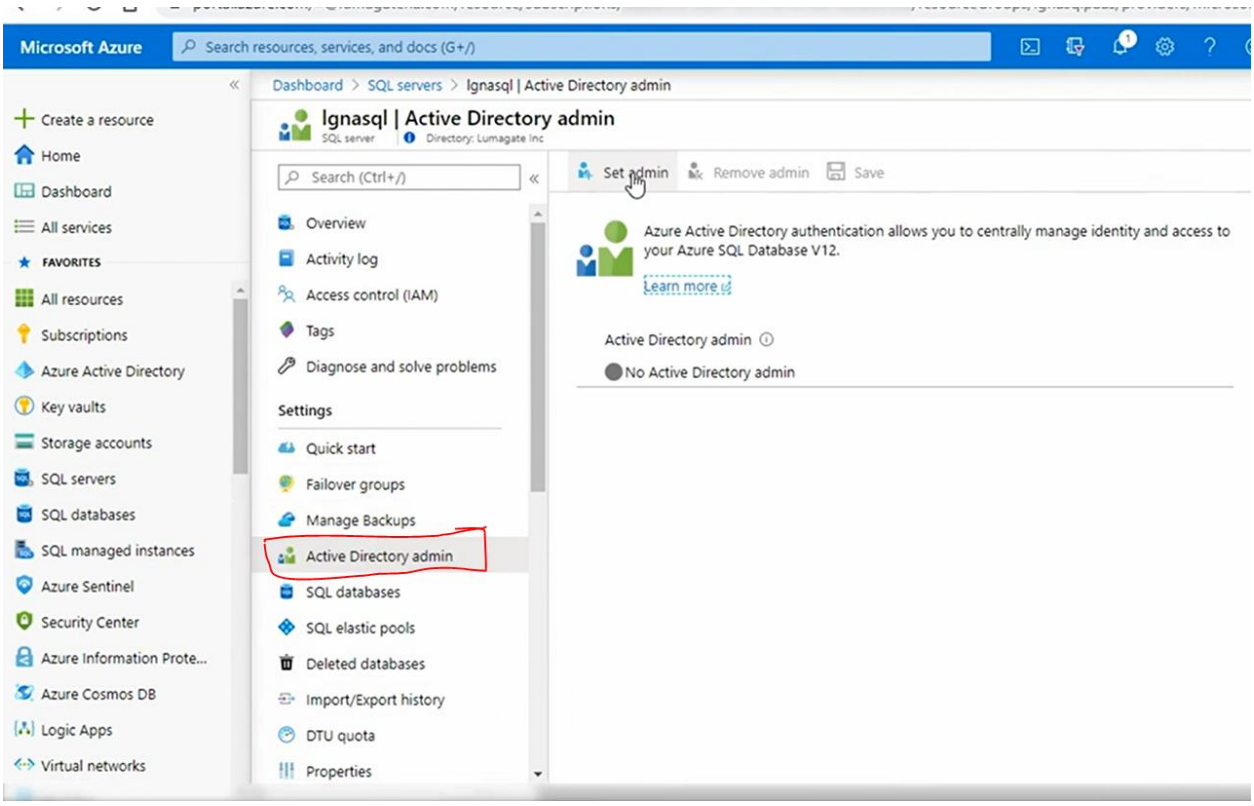
Next

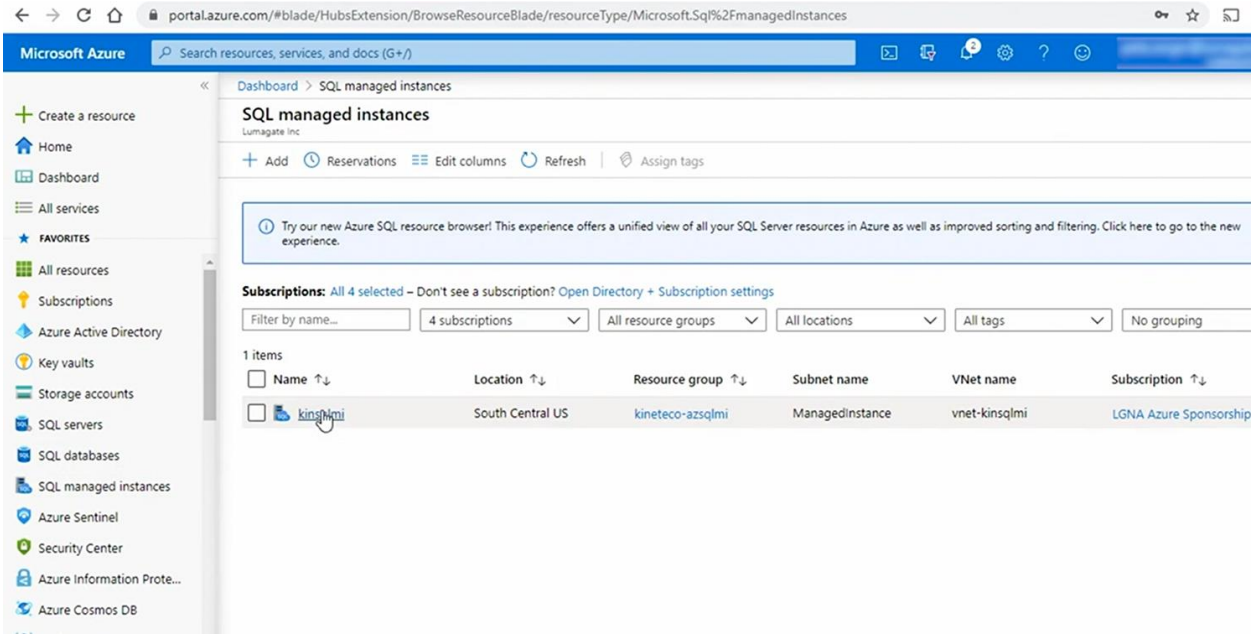
# 2. Configure Security for Databases

## 2.1 Enable database authentication using Azure AD



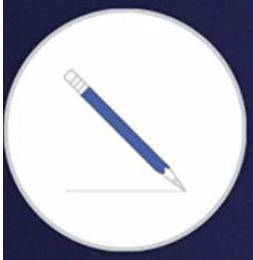




Microsoft Azure
Search resources, services, and docs (G+/)
Dashboard > SQL servers > lgnasql | Active Directory admin
lgnasql | Active Directory admin
SQL server
Directory: Lumagate Inc
Search (Ctrl+/)
Set admin
Remove admin
Save
Azure Active Directory authentication allows you to centrally manage identity and access to your Azure SQL Database V12.
Learn more
Active Directory admin
No Active Directory admin
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Quick start
Failover groups
Manage Backups
Active Directory admin
SQL databases
SQL elastic pools
Deleted databases
Import/Export history
DTU quota
Properties
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Subscriptions
Azure Active Directory
Key vaults
Storage accounts
SQL servers
SQL databases
SQL managed instances
Azure Sentinel
Security Center
Azure Information Prote...
Azure Cosmos DB
Logic Apps
Virtual networks


portal.azure.com/#blade/HubsExtension/BrowseResourceBlade/resourceType/Microsoft.Sql%2FmanagedInstances
Microsoft Azure
Search resources, services, and docs (G+/)
Dashboard > SQL managed instances
SQL managed instances
Lumagate Inc
Add
Reservations
Edit columns
Refresh
Assign tags
Try our new Azure SQL resource browser! This experience offers a unified view of all your SQL Server resources in Azure as well as improved sorting and filtering. Click here to go to the new experience.
Subscriptions: All 4 selected – Don't see a subscription? Open Directory + Subscription settings
Filter by name...
4 subscriptions
All resource groups
All locations
All tags
No grouping
1 items
Name
Location
Resource group
Subnet name
VNet name
Subscription
kinsqlmi
South Central US
kineteco-azsqlmi
ManagedInstance
vnet-kinsqlmi
LGNA Azure Sponsorship
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Subscriptions
Azure Active Directory
Key vaults
Storage accounts
SQL servers
SQL databases
SQL managed instances
Azure Sentinel
Security Center
Azure Information Prote...
Azure Cosmos DB

## AAD Auth with Geo-Replication

The Azure Active Directory administrator must be configured for both the primary and the secondary servers.



## Exam Tip

Remember the details around account type and configuration in geo-replication scenarios.

### 2.2 Enable database auditing

## Azure SQL Database Auditing

**You can use database auditing in Azure SQL to:**

**Retain** an audit trail of selected events

**Report** on DB activity

**Analyze** reports

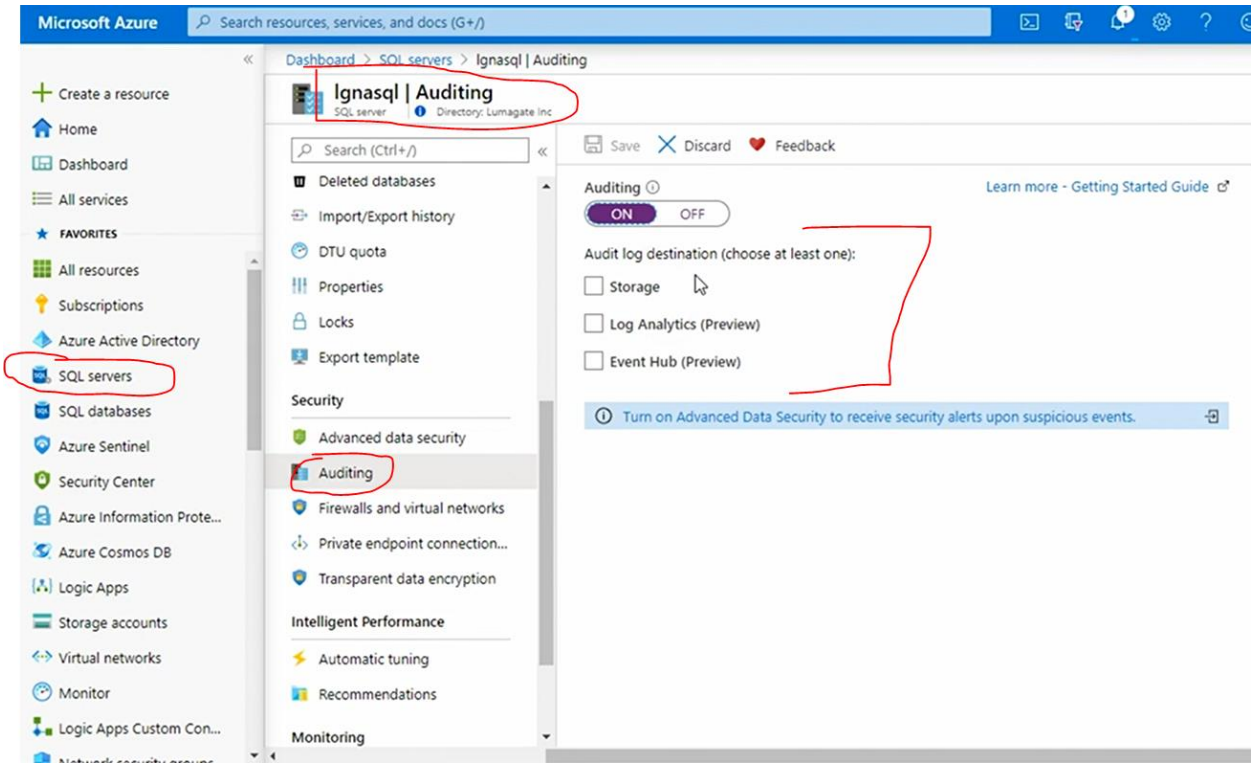
# Server vs. DB-Level Auditing

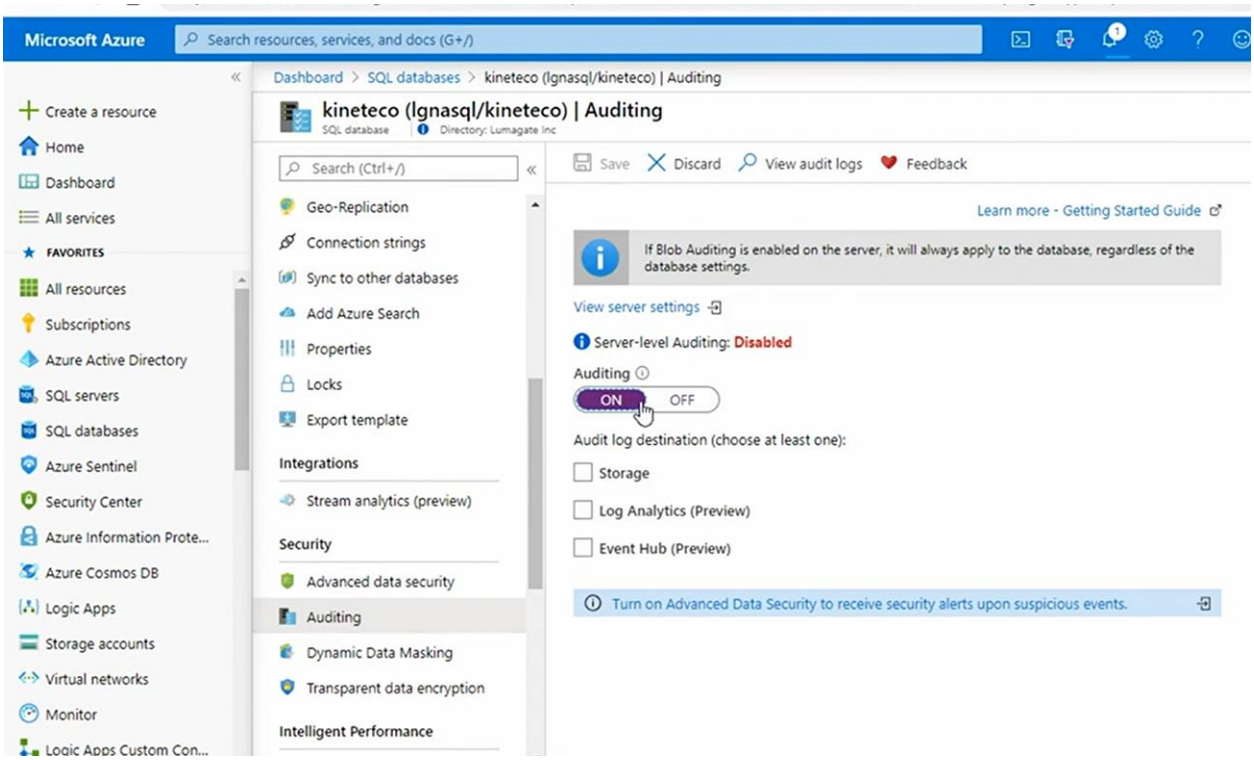
**There are a few behaviors you should be aware of**

**Server policy** applies to *existing* and *new* DBs

If **server blob auditing** is enabled, it *always* applies

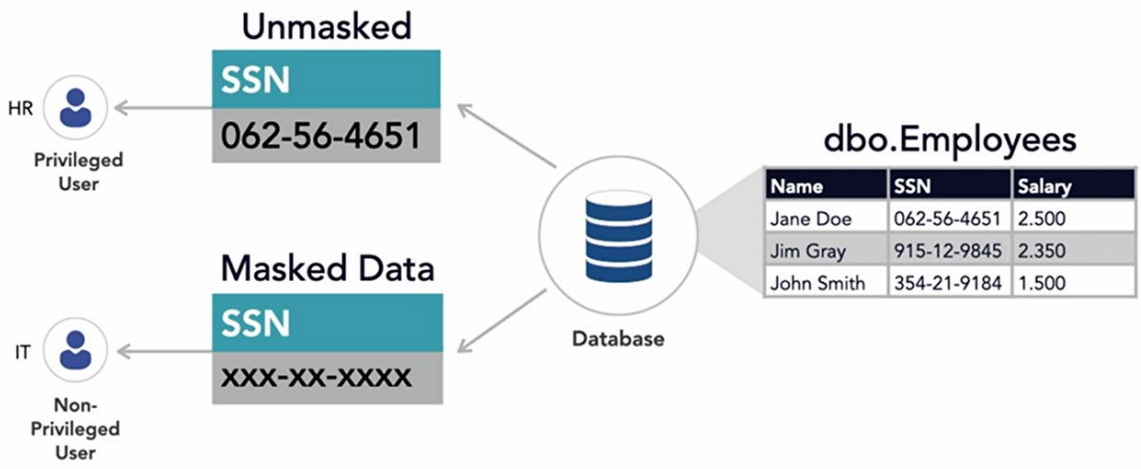
**DB-level settings** do *not* override server-level settings

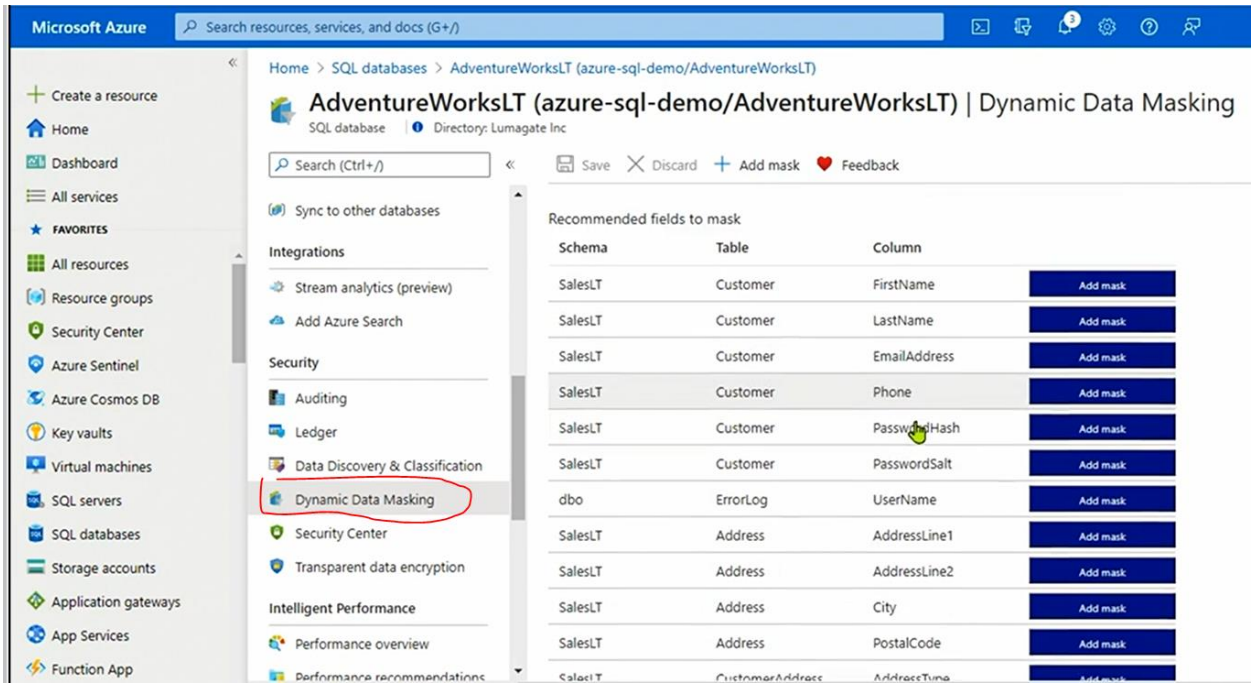



Microsoft Azure
Search resources, services, and docs (G+/)
Dashboard > SQL databases > kineteco (lgnasql/kineteco) | Auditing
kineteco (lgnasql/kineteco) | Auditing
SQL database
Directory: Lumagate Inc
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Subscriptions
Azure Active Directory
SQL servers
SQL databases
Azure Sentinel
Security Center
Azure Information Prote...
Azure Cosmos DB
Logic Apps
Storage accounts
Virtual networks
Monitor
Logic Apps Custom Con...
Search (Ctrl+/)
Geo-Replication
Connection strings
Sync to other databases
Add Azure Search
Properties
Locks
Export template
Integrations
Stream analytics (preview)
Security
Advanced data security
Auditing
Dynamic Data Masking
Transparent data encryption
Intelligent Performance
Save
Discard
View audit logs
Feedback
Learn more - Getting Started Guide
If Blob Auditing is enabled on the server, it will always apply to the database, regardless of the database settings.
View server settings
Server-level Auditing: Disabled
Auditing
ON
OFF
Audit log destination (choose at least one):
Storage
Log Analytics (Preview)
Event Hub (Preview)
Turn on Advanced Data Security to receive security alerts upon suspicious events.


Exam Tip
Know how to configure audit settings and how server vs. database audit settings behave.

# What Is Dynamic Data Masking?



# Dynamic Data Masking Policy

**SQL users excluded from masking**

Users with administrator privileges are *always* excluded from masking

**Masking rules**

A set of rules that define the designated fields to be masked and the masking function that is used

## For SQL Managed Instance

The dynamic data masking feature cannot be set using portal for SQL Managed Instance.

## For the Exam

Know how to configure the dynamic data masking feature and how to control visibility.

## 2.3 Implement database encryption for Azure SQL Database

# Transparent Data Encryption

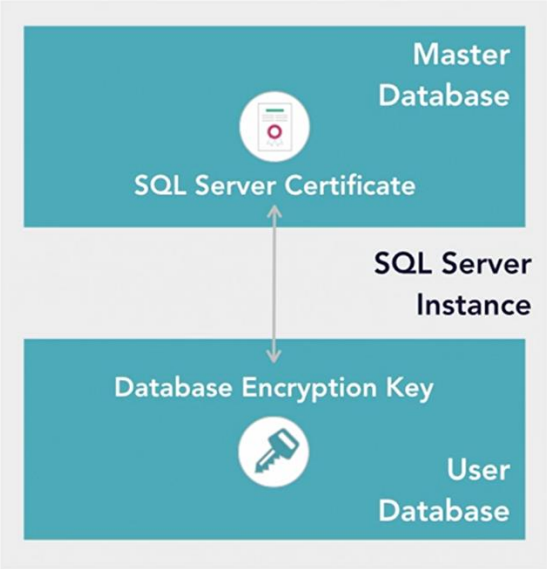
**Performs real-time database encryption and decryption of:**

- Databases
- Associated backups
- Transaction log files

**Without requiring changes to the application**

## TDE Function and Operation

Transparent Data Encryption (TDE) encrypts the storage of an entire database.




**Data encryption key (DEK) is protected by the *TDE protector***

**TDE protector is either a *local certificate* or an *asymmetric key* stored in Key Vault (BYOK)**

**TDE protector is set at the *server level***

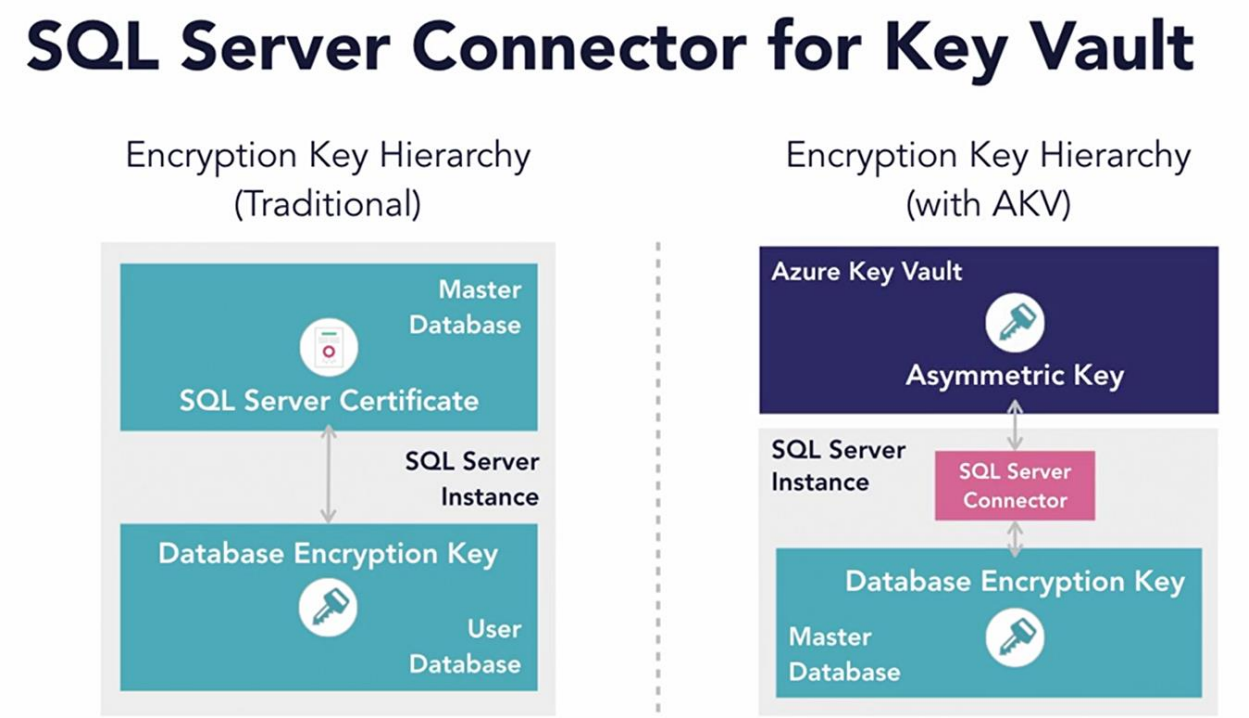
# On Database Startup…

**The encrypted DEK is decrypted.**

And then used for decryption and re-encryption of the **database files**

Performs real-time I/O encryption and decryption of data at **page level**

Each page is **decrypted** when read into memory, and **encrypted** before being written to disk


SQL Server Connector for Key Vault
Encryption Key Hierarchy (Traditional)
Master Database
SQL Server Certificate
SQL Server Instance
Database Encryption Key
User Database
Encryption Key Hierarchy (with AKV)
Azure Key Vault
Asymmetric Key
SQL Server Instance
SQL Server Connector
Database Encryption Key
Master Database


Key Storage in Azure
SQL Server running on an Azure virtual machine can also use an asymmetric key from Azure Key Vault.

# Service-Managed TDE

**By default, the database encryption key is protected by a built-in server certificate.**

Built-in server certificate is **unique for each server**

If two databases are connected to the same server, they **share the same built-in certificate**

## Certificate Rotation

Microsoft automatically rotates these certificates at least every 90 days.

# Bring Your Own Key (BYOK)

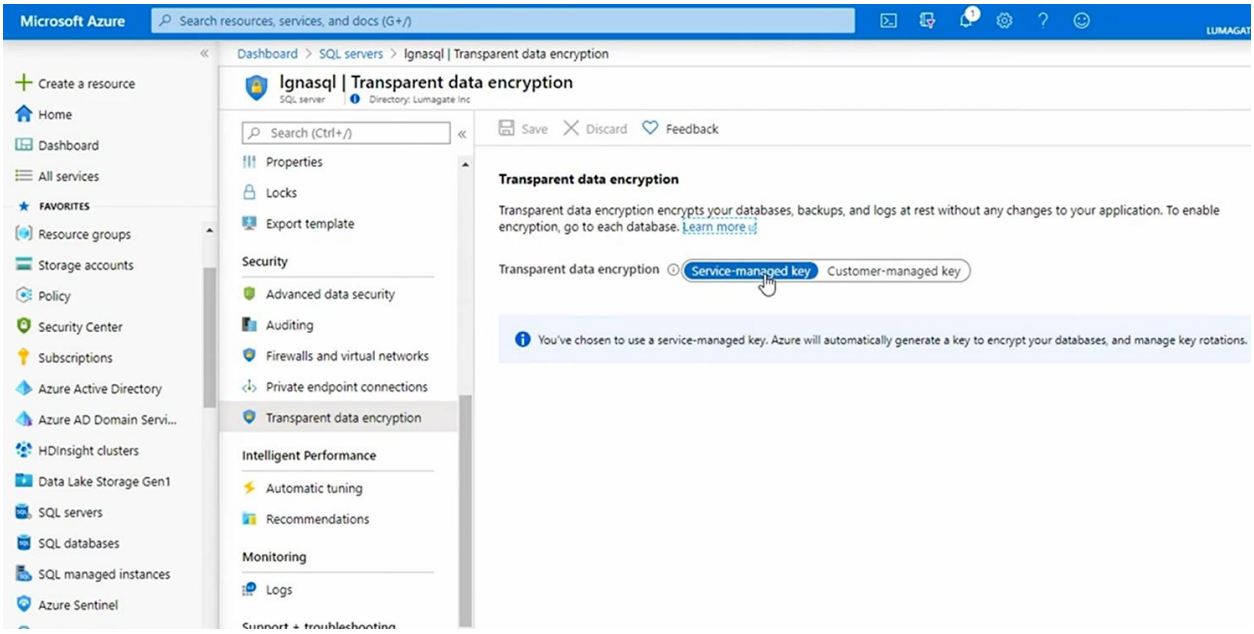
- Allows the user to **take control** over their TDE keys
- Controls **who** can access them and **when** they can access
- AKV is **key management service** with BYOK support for TDE

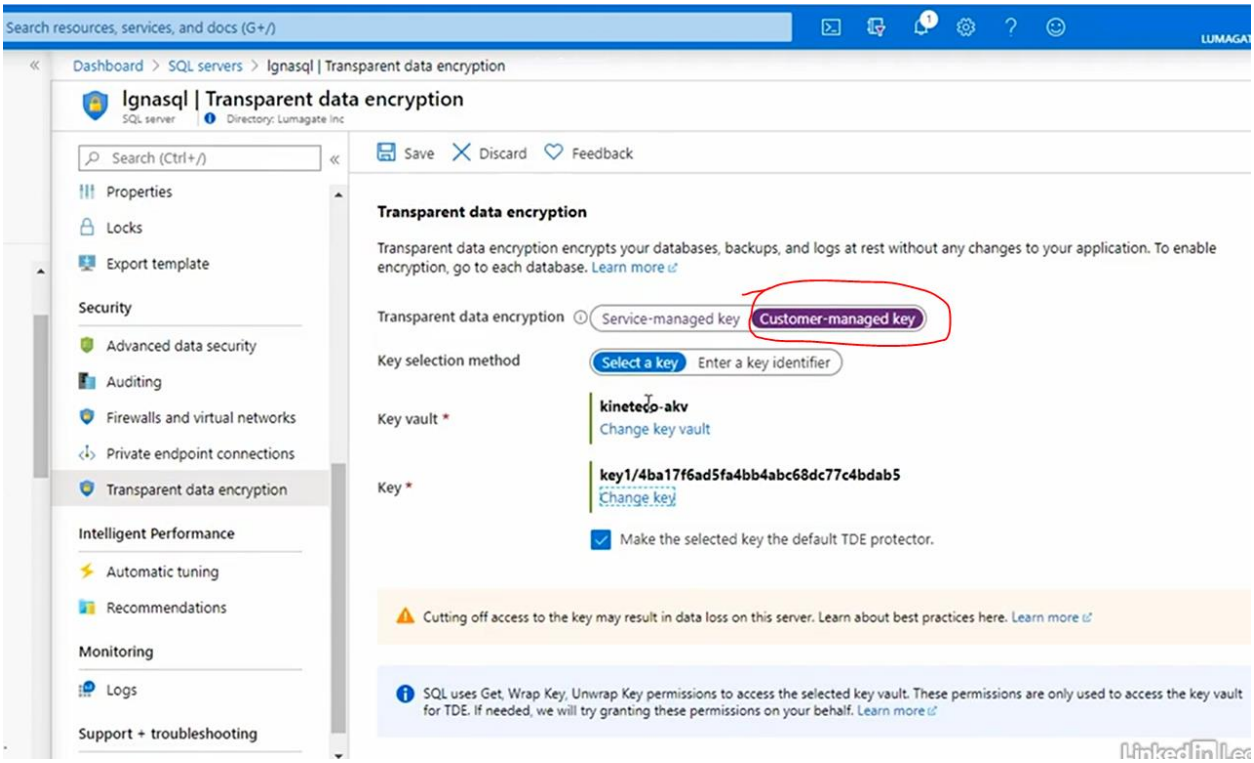
# Key Storage with BYOK

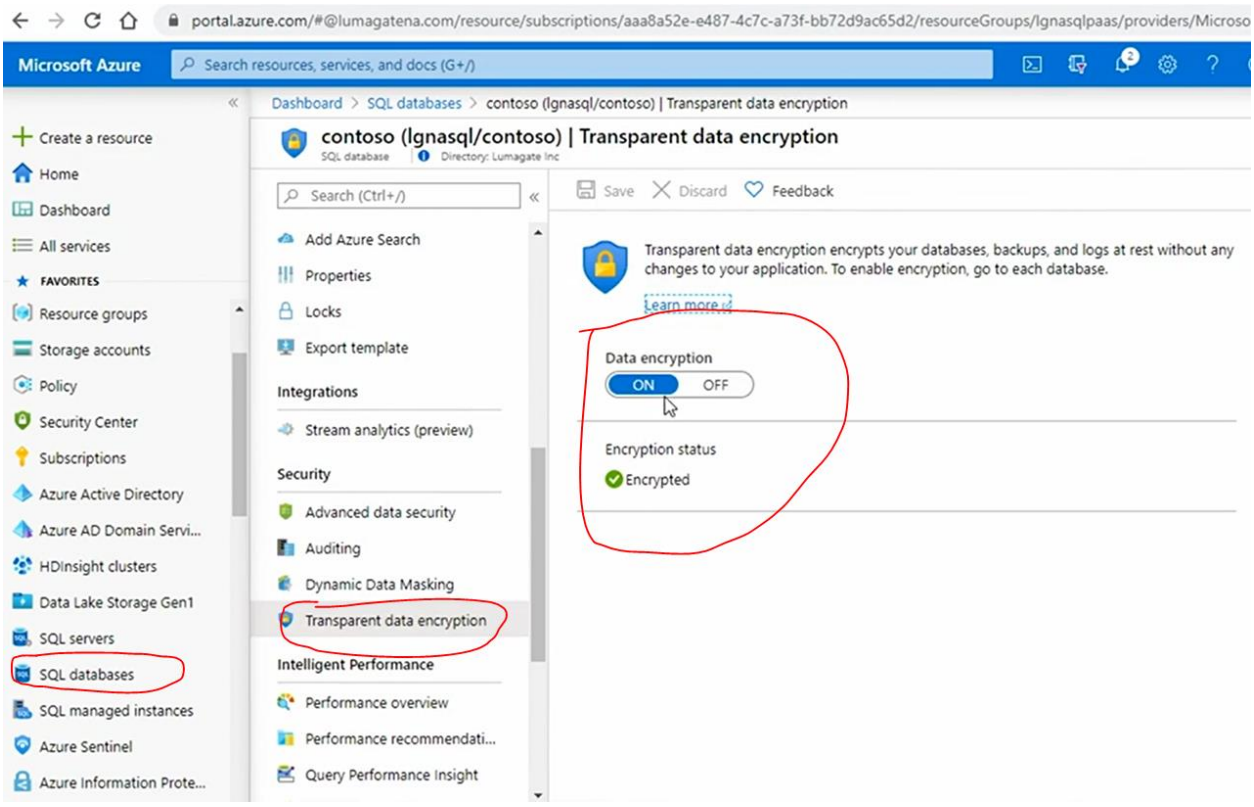
- DEK is protected by an **asymmetric key** stored in AKV
- Asymmetric key **never leaves Key Vault**
- Server sends basic key operation requests **through AKV service**
- Asymmetric key is set at **server level** and inherited by all databases

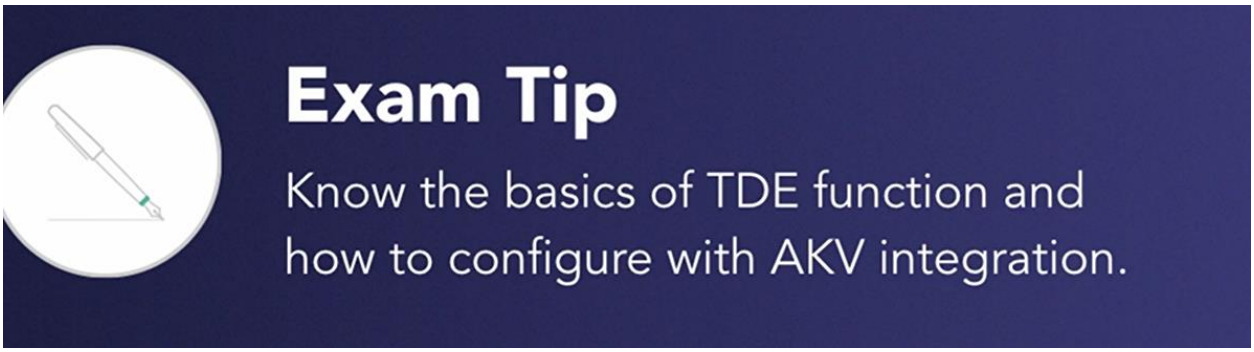
# Configuring TDE

To configure TDE through Azure portal, you must be connected as the **Azure Owner**, **Contributor**, or **SQL Security Manager**.

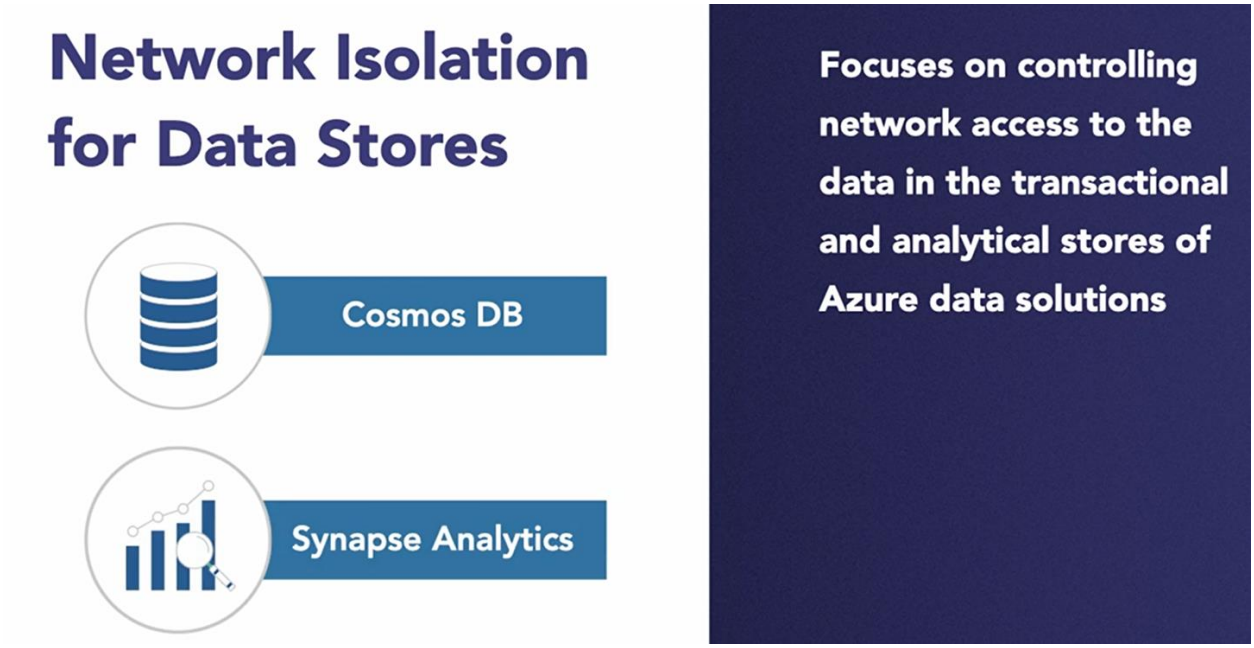


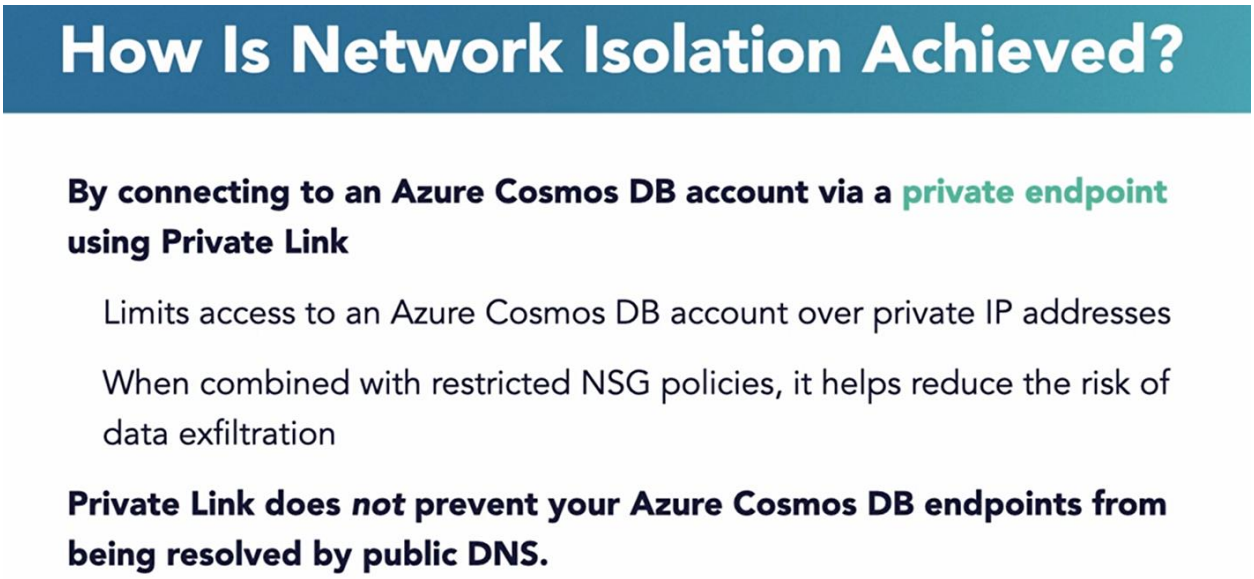

Search resources, services, and docs (G+/)
Dashboard > SQL servers > lgnasql | Transparent data encryption
lgnasql | Transparent data encryption
SQL server
Directory: Lumagate Inc
Search (Ctrl+/)
Properties
Locks
Export template
Security
Advanced data security
Auditing
Firewalls and virtual networks
Private endpoint connections
Transparent data encryption
Intelligent Performance
Automatic tuning
Recommendations
Monitoring
Logs
Support + troubleshooting
Save
Discard
Feedback
Transparent data encryption
Transparent data encryption encrypts your databases, backups, and logs at rest without any changes to your application. To enable encryption, go to each database. Learn more
Transparent data encryption
Service-managed key
Customer-managed key
Key selection method
Select a key
Enter a key identifier
Key vault *
kinetecp-akv
Change key vault
Key *
key1/4ba17f6ad5fa4bb4abc68dc77c4bdab5
Change key
Make the selected key the default TDE protector.
Cutting off access to the key may result in data loss on this server. Learn about best practices here. Learn more
SQL uses Get, Wrap Key, Unwrap Key permissions to access the selected key vault. These permissions are only used to access the key vault for TDE. If needed, we will try granting these permissions on your behalf. Learn more


portal.azure.com/#@lumagatena.com/resource/subscriptions/aaa8a52e-e487-4c7c-a73f-bb72d9ac65d2/resourceGroups/lgnasqlpaas/providers/Microso
Microsoft Azure
Search resources, services, and docs (G+/)
Create a resource
Home
Dashboard
All services
FAVORITES
Resource groups
Storage accounts
Policy
Security Center
Subscriptions
Azure Active Directory
Azure AD Domain Servi...
HDInsight clusters
Data Lake Storage Gen1
SQL servers
SQL databases
SQL managed instances
Azure Sentinel
Azure Information Prote...
Dashboard > SQL databases > contoso (lgnasql/contoso) | Transparent data encryption
contoso (lgnasql/contoso) | Transparent data encryption
SQL database
Directory: Lumagate Inc
Search (Ctrl+/)
Add Azure Search
Properties
Locks
Export template
Integrations
Stream analytics (preview)
Security
Advanced data security
Auditing
Dynamic Data Masking
Transparent data encryption
Intelligent Performance
Performance overview
Performance recommendati...
Query Performance Insight
Save
Discard
Feedback
Transparent data encryption encrypts your databases, backups, and logs at rest without any changes to your application. To enable encryption, go to each database.
Learn more
Data encryption
ON
OFF
Encryption status
Encrypted




## 2.4 Implement network isolation for data solutions



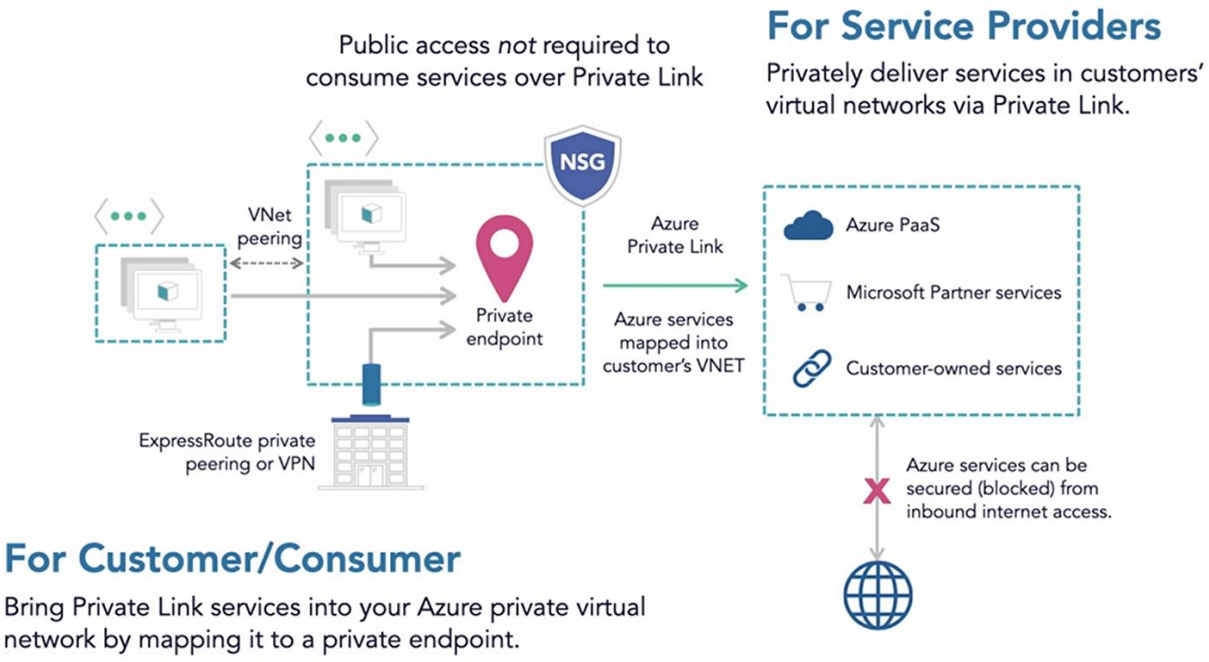
# Access Limits in Network Isolation Scenario

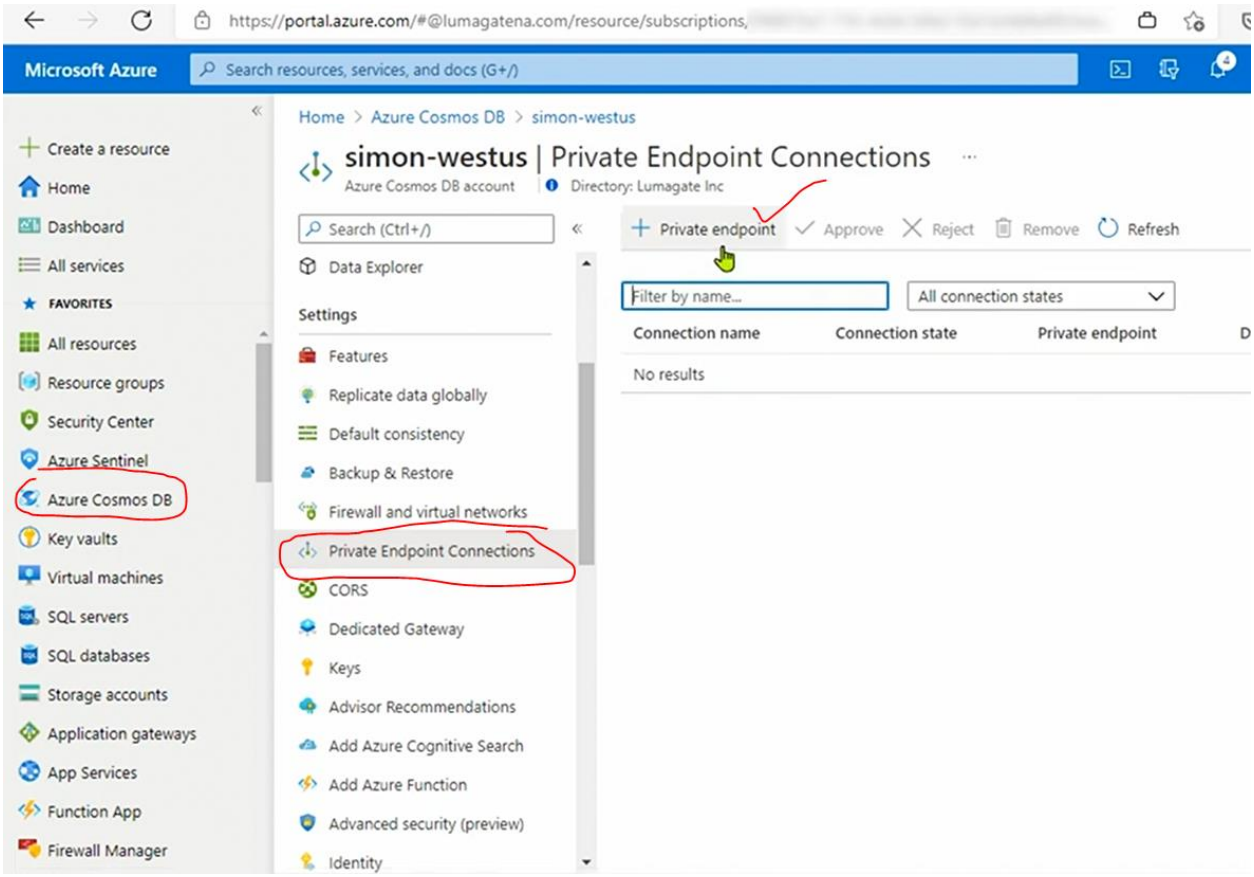
**This configuration enables secure resource access in hybrid cloud scenarios:**

Allows users to access an Azure Cosmos DB account from within the VNet or from any peered virtual network

Mapped resources are accessible on-premises over private peering through VPN or Azure ExpressRoute

**Enables connectivity via automatic or manual approval method using approval workflow**

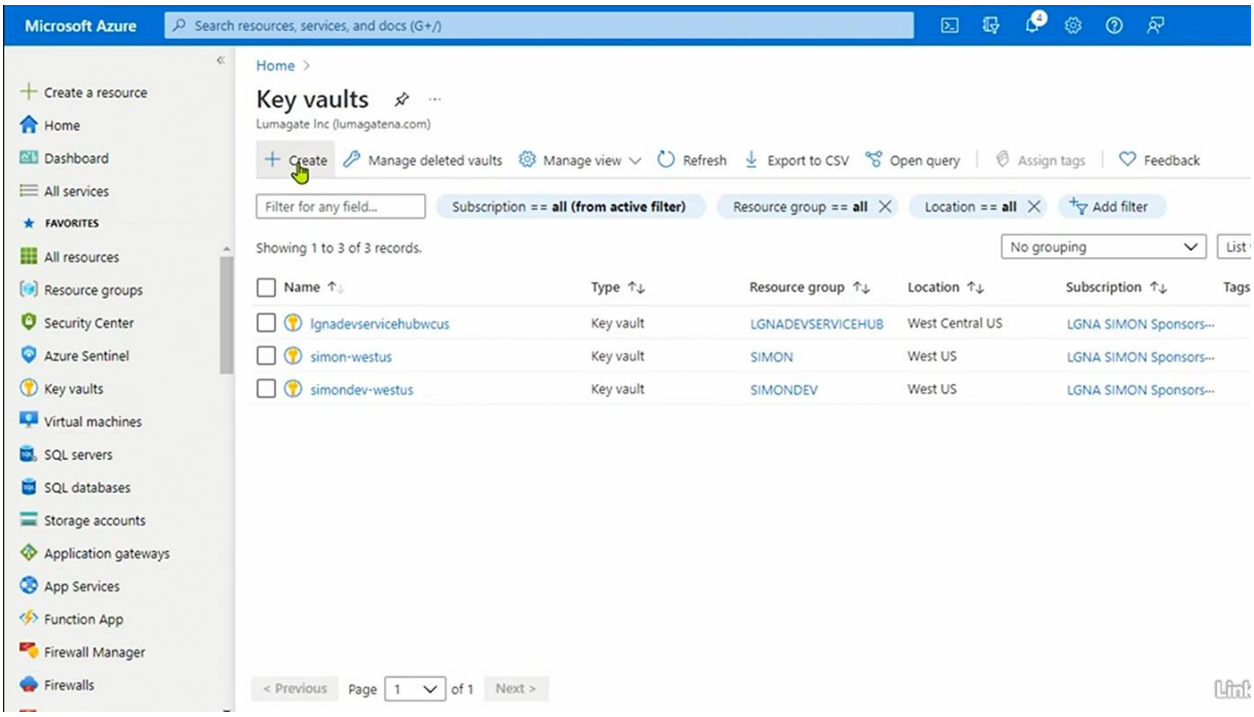


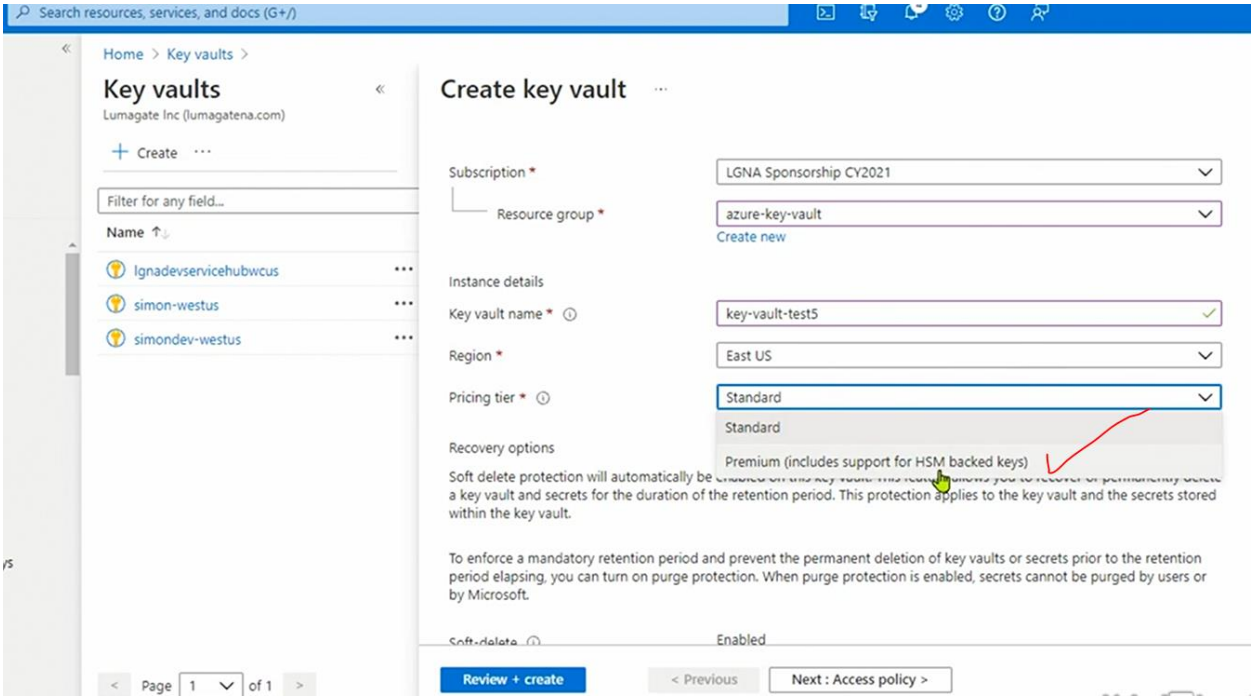

https://portal.azure.com/#@lumagatena.com/resource/subscriptions,
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Azure Cosmos DB > simon-westus
simon-westus | Private Endpoint Connections
Azure Cosmos DB account
Directory: Lumagate Inc
Search (Ctrl+/)
Private endpoint
Approve
Reject
Remove
Refresh
Filter by name...
All connection states
Connection name
Connection state
Private endpoint
No results
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
Security Center
Azure Sentinel
Azure Cosmos DB
Key vaults
Virtual machines
SQL servers
SQL databases
Storage accounts
Application gateways
App Services
Function App
Firewall Manager
Data Explorer
Settings
Features
Replicate data globally
Default consistency
Backup & Restore
Firewall and virtual networks
Private Endpoint Connections
CORS
Dedicated Gateway
Keys
Advisor Recommendations
Add Azure Cognitive Search
Add Azure Function
Advanced security (preview)
Identity

## 2.5 Quiz

# 3. Configure and Manage Key Vault

## 3.1 Create and configure key vault



Home > Key vaults >

## Key vaults

Lumagate Inc (lumagatena.com)

+ Create ···

Filter for any field...

Name

- lgnadevservicehubwcus
- simon-westus
- simondev-westus

## Create key vault

Region * East US

Pricing tier * Premium (includes support for HSM backed keys)

Recovery options

Soft delete protection will automatically be enabled on this key vault. This feature allows you to recover or permanently de
a key vault and secrets for the duration of the retention period. This protection applies to the key vault and the secrets sto
within the key vault.

The ability to turn off soft delete via the Azure Portal has been deprecated. You can create a new key vault with soft delete off for a limited time using CLI / PowerShell / REST API. The ability to create a key vault with soft delete disabled will be fully deprecated by the end of the year.

e permanent deletion of key vaults or secrets prior to the retentior
n purge protection is enabled, secrets cannot be purged by users c

Soft-delete Enabled

Days to retain deleted vaults * 90

Purge protection

- (•) Disable purge protection (allow key vault and objects to be purged during retention period)
- ( ) Enable purge protection (enforce a mandatory retention period for delete vaults and vault objects)

Page 1 of 1

Review + create | < Previous | Next : Access policy >

Home > Key vaults >

## Key vaults

Lumagate Inc (lumagatena.com)

+ Create ···

Filter for any field...

Name

- lgnadevservicehubwcus
- simon-westus
- simondev-westus

## Create key vault

Region * East US

Pricing tier * Premium (includes support for HSM backed keys)

Recovery options

Soft delete protection will automatically be enabled on this key vault. This feature allows you to recover or permanently delete a key vault and secrets for the duration of the retention period. This protection applies to the key vault and the secrets stored within the key vault.

To enforce a mandatory retention period and prevent the permanent deletion of key vaults or secrets prior to the retention period elapsing, you can turn on purge protection. When purge protection is enabled, secrets cannot be purged by users or by Microsoft.

Soft-delete Enabled

Days to retain deleted vaults * 90

Purge protection

- ( ) Disable purge protection (allow key vault and objects to be purged during retention period)
- (•) Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)

Once enabled, this option cannot be disabled

Page 1 of 1

Review + create | < Previous | Next : Access policy >

Remember your options for deploying Azure Key Vault (PowerShell, Azure CLI, Azure portal, etc.)

## 3.2 Configure access to Azure Key Vault

### Key Vault (Management Plane)

**Focuses on operations related to the key vault instance**

**Operations**

- Create and delete vaults
- Update access policies
- Retrieve vault properties

### Key Vault (Management Plane)

**Authentication**

- Azure AD

**Authorization**

- Azure AD RBAC

## Key Vault Contributor Role

Lets you manage key vaults, but does not enable to you access their contents

You can assign permissions at the **Subscription**, **Resource Group**, or **Resource** levels.

## Key Vault (Data Plane)

**Focuses on access to the objects hosted in the key vault**

**Operations**

- View and manage certificates
- View and manage keys
- View and manage secrets

# Key Vault (Data Plane)

**Authentication**

Azure AD

**Authorization**

Azure AD RBAC

Key Vault access policies

Remember that **access policy templates** can help you set only permissions required.

Remember that access policies define access for *object types*, not specific objects.

## Azure Key Vault Authentication Options for Apps

1. **Application-only access:** Application runs as a daemon service or background job
2. **User-only access:** User accesses the Key Vault from any app registered in the tenant
3. **User plus application access:** Application accesses Key Vault on behalf of a signed-in user

## Automation and Programmatic Access

**Know your options for key vault automation**

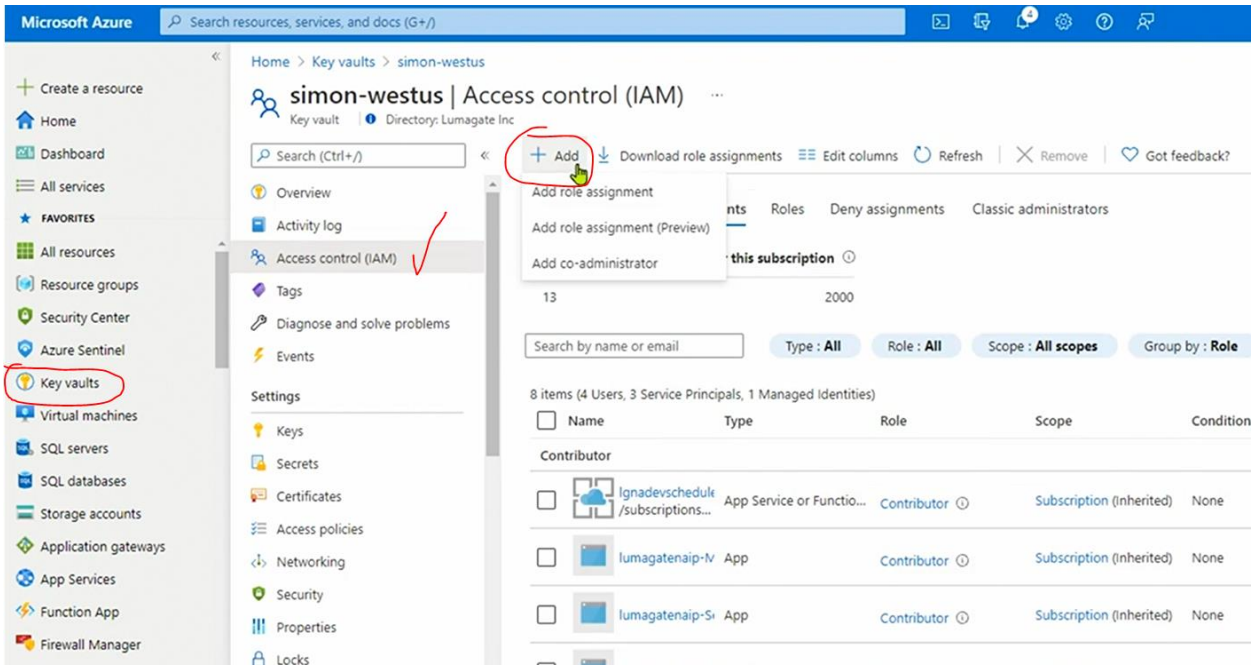
PowerShell

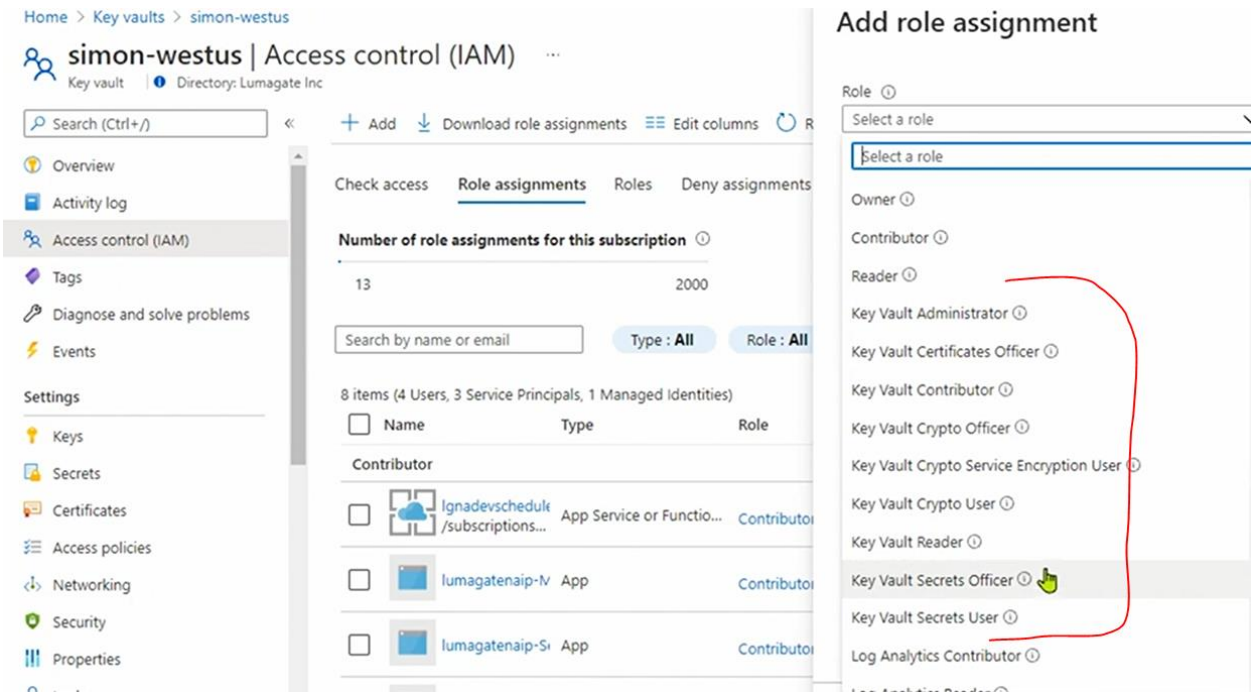
Azure CLI

ARM template

Azure Key Vault REST API

Azure Automation


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Key vaults > simon-westus
simon-westus | Access control (IAM)
Key vault
Directory: Lumagate Inc
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
Security Center
Azure Sentinel
Key vaults
Virtual machines
SQL servers
SQL databases
Storage accounts
Application gateways
App Services
Function App
Firewall Manager
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Events
Settings
Keys
Secrets
Certificates
Access policies
Networking
Security
Properties
Locks
Add
Download role assignments
Edit columns
Refresh
Remove
Got feedback?
Add role assignment
Add role assignment (Preview)
Add co-administrator
Roles
Deny assignments
Classic administrators
this subscription
13
2000
Search by name or email
Type : All
Role : All
Scope : All scopes
Group by : Role
8 items (4 Users, 3 Service Principals, 1 Managed Identities)
Name
Type
Role
Scope
Condition
Contributor
Ignadevschedule /subscriptions...
App Service or Functio...
Contributor
Subscription (Inherited)
None
lumagatenaip-M
App
lumagatenaip-S
App


Home > Key vaults > simon-westus
simon-westus | Access control (IAM)
Key vault
Directory: Lumagate Inc
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Events
Settings
Keys
Secrets
Certificates
Access policies
Networking
Security
Properties
Add
Download role assignments
Edit columns
Check access
Role assignments
Roles
Deny assignments
Number of role assignments for this subscription
13
2000
Search by name or email
Type : All
Role : All
8 items (4 Users, 3 Service Principals, 1 Managed Identities)
Name
Type
Role
Contributor
Ignadevschedule /subscriptions...
App Service or Functio...
lumagatenaip-M
App
lumagatenaip-S
App
Add role assignment
Role
Select a role
Select a role
Owner
Contributor
Reader
Key Vault Administrator
Key Vault Certificates Officer
Key Vault Contributor
Key Vault Crypto Officer
Key Vault Crypto Service Encryption User
Key Vault Crypto User
Key Vault Reader
Key Vault Secrets Officer
Key Vault Secrets User
Log Analytics Contributor

Data Plane

Home > Key vaults > simon-westus

simon-westus | Access policies

Key vault | Directory: Lumagate Inc

Save Discard Refresh

Enable Access to:

- Azure Virtual Machines for deployment
- Azure Resource Manager for template deployment
- Azure Disk Encryption for volume encryption

Permission model: Vault access policy / Azure role-based access control

+ Add Access Policy

Current Access Policies

| Name | Email | Key Permissions | Secret Permissions | Certific |
|---|---|---|---|---|
| APPLICATION | | | | |
| simon-utilities-westus | | 5 selected | Get | 0 sele |
| simon-westus | | 5 selected | Get | 0 sele |

Home > Key vaults > simon-westus

simon-westus | Access policies

Key vault | Directory: Lumagate Inc

Save Discard Refresh

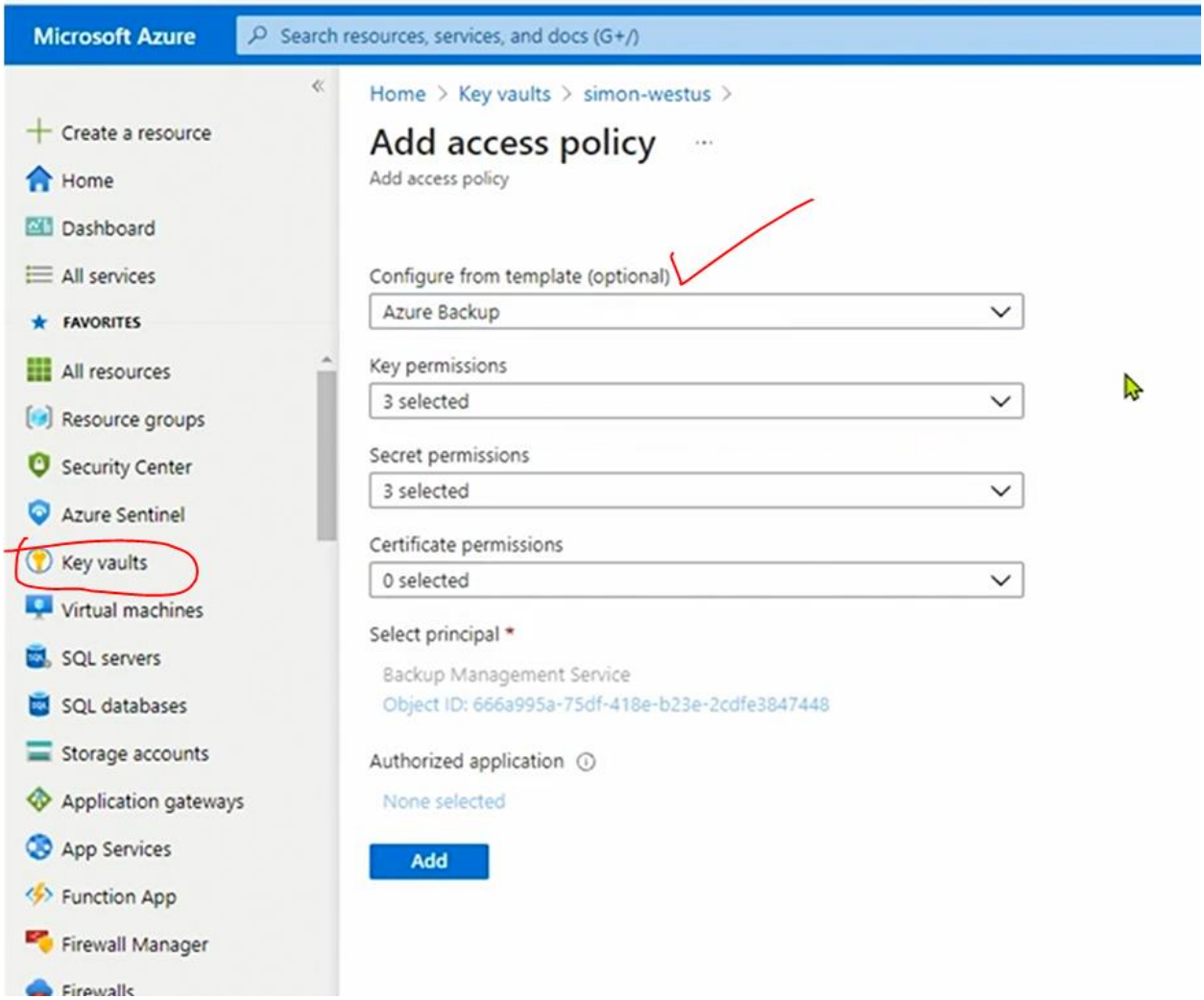
Please click the 'Save' button to commit your changes.

WARNING: You are changing the permission model. This may immediately change users and services that are allowed to access this key vault. You may proceed if this key vault is new, not used in production workloads, or if you are undoing a previous change. Otherwise it's strongly recommended that you perform this action in the beginning of your own planned maintenance event, during which you can test the new configuration and undo if necessary.

Enable Access to:

- Azure Virtual Machines for deployment
- Azure Resource Manager for template deployment
- Azure Disk Encryption for volume encryption

Permission model: Vault access policy / Azure role-based access control




# For the Exam

Knowing the details of Azure Key Vault management and data plane will give you a big advantage on the AZ-500 exam.

## 3.3 Manage certificates, secrets, and keys

### Benefits of Certificate Management with Key Vault

- Central storage of certificates
- Automated renewal of certificates
- Programmatic access to certificates
- Programmatic creation of certificates
- Programmatic renewal of certificates

### Secrets and Keys: What's the Difference?

**Secrets**

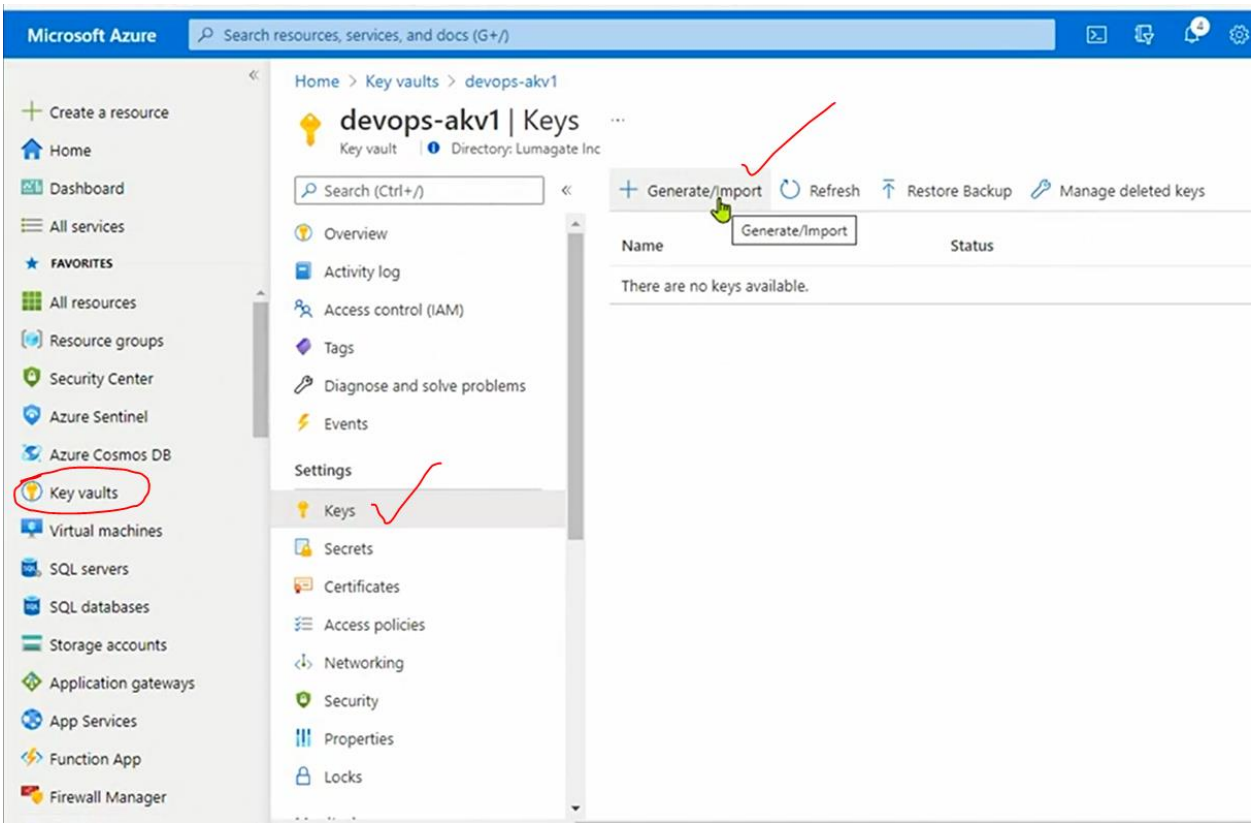
Any sequence of bytes under 10 KB, like connection strings, or passwords for PFX (private key file)

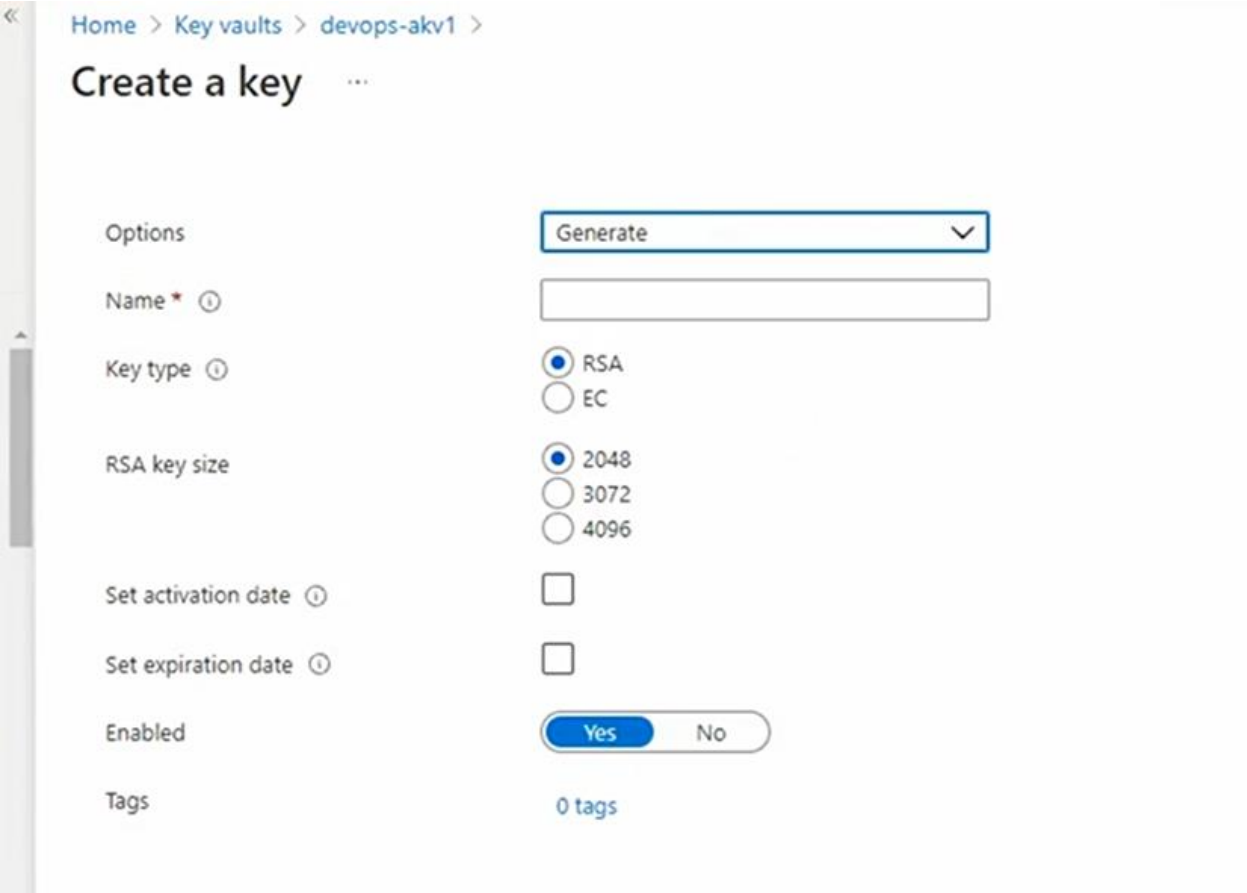
**Keys**

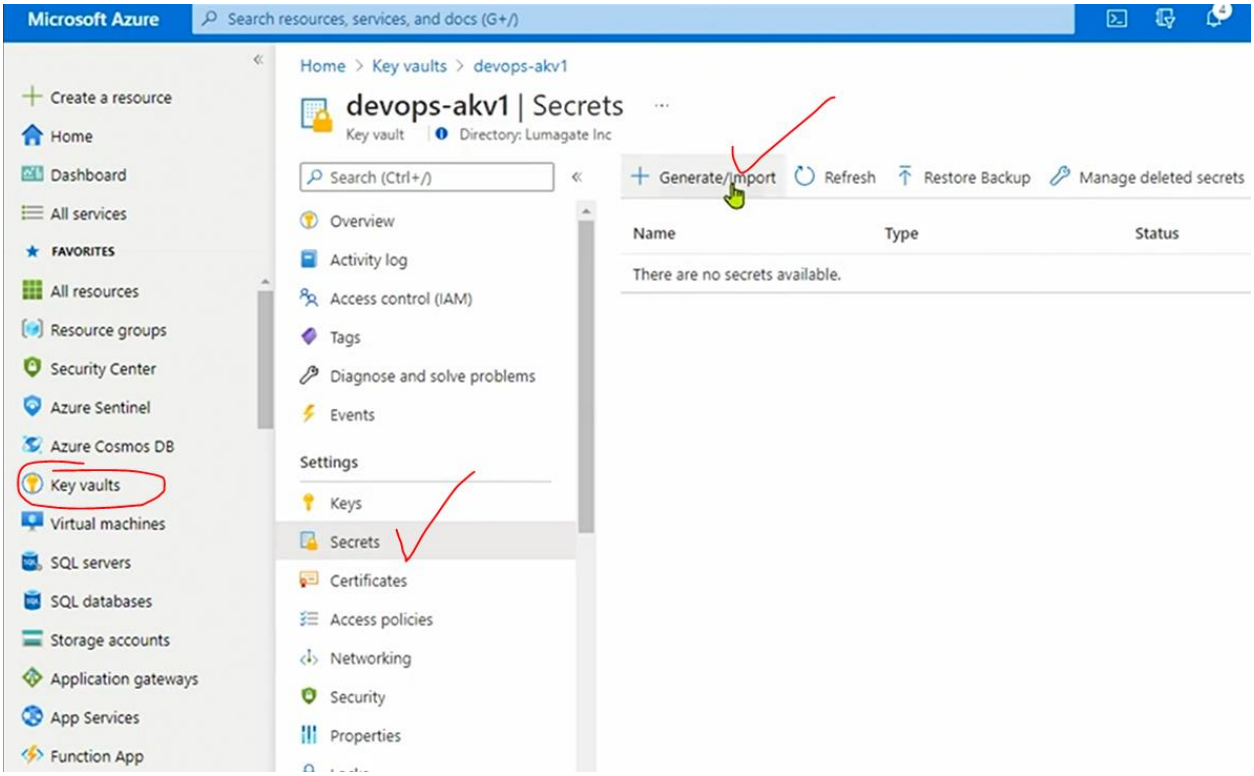
Cryptographic material imported into Key Vault or generated when a service requests the Key Vault to do so

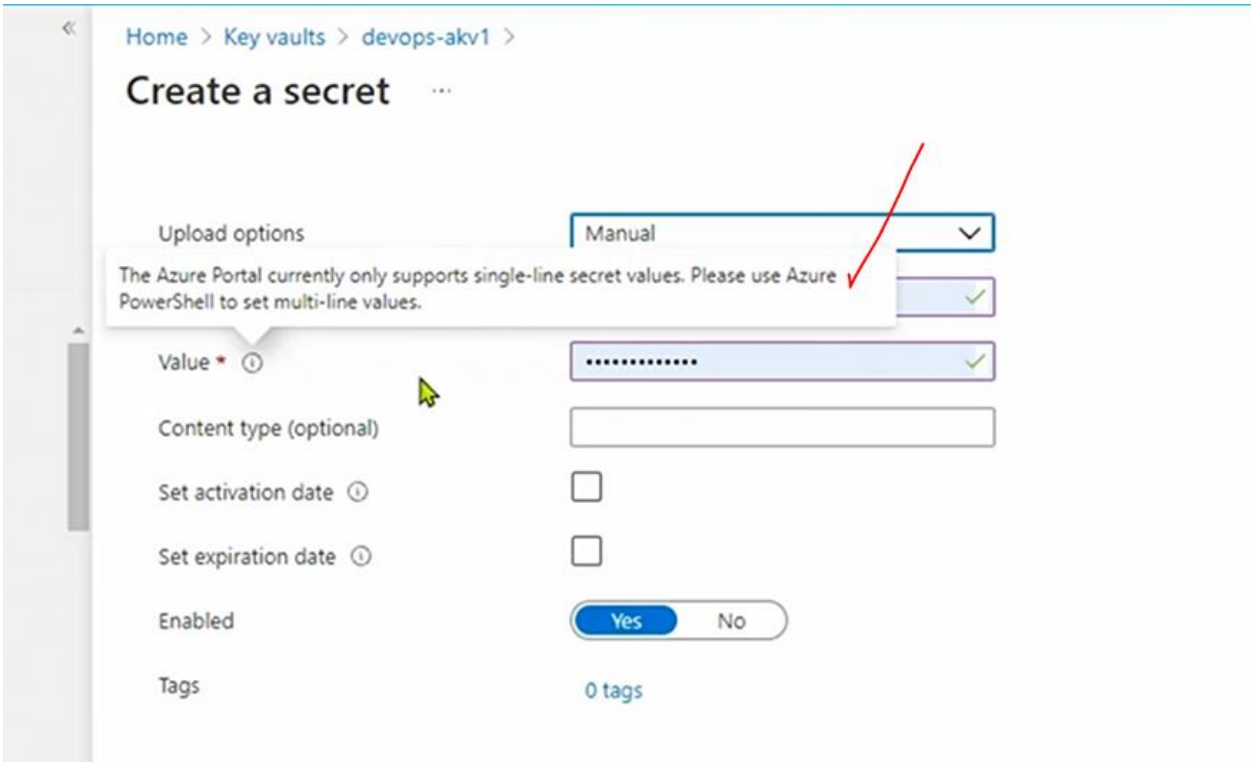
# Steps for Creating Certificates in Key Vault

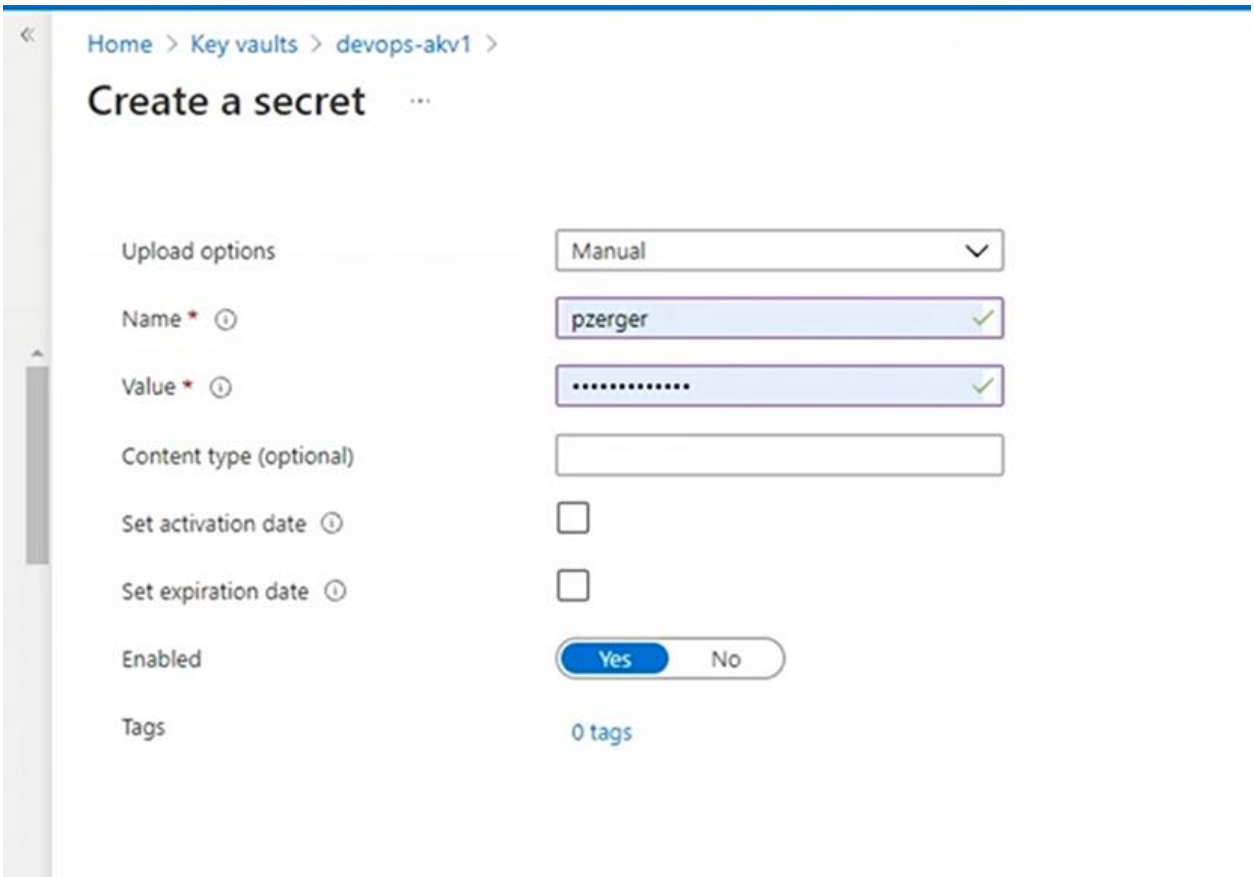
- **Step 1:** Account with CA provider
- **Step 2:** Create CA provider admin account
- **Step 3:** Set certificate issuer resource
- **Step 4:** Certificate Request to CA provider

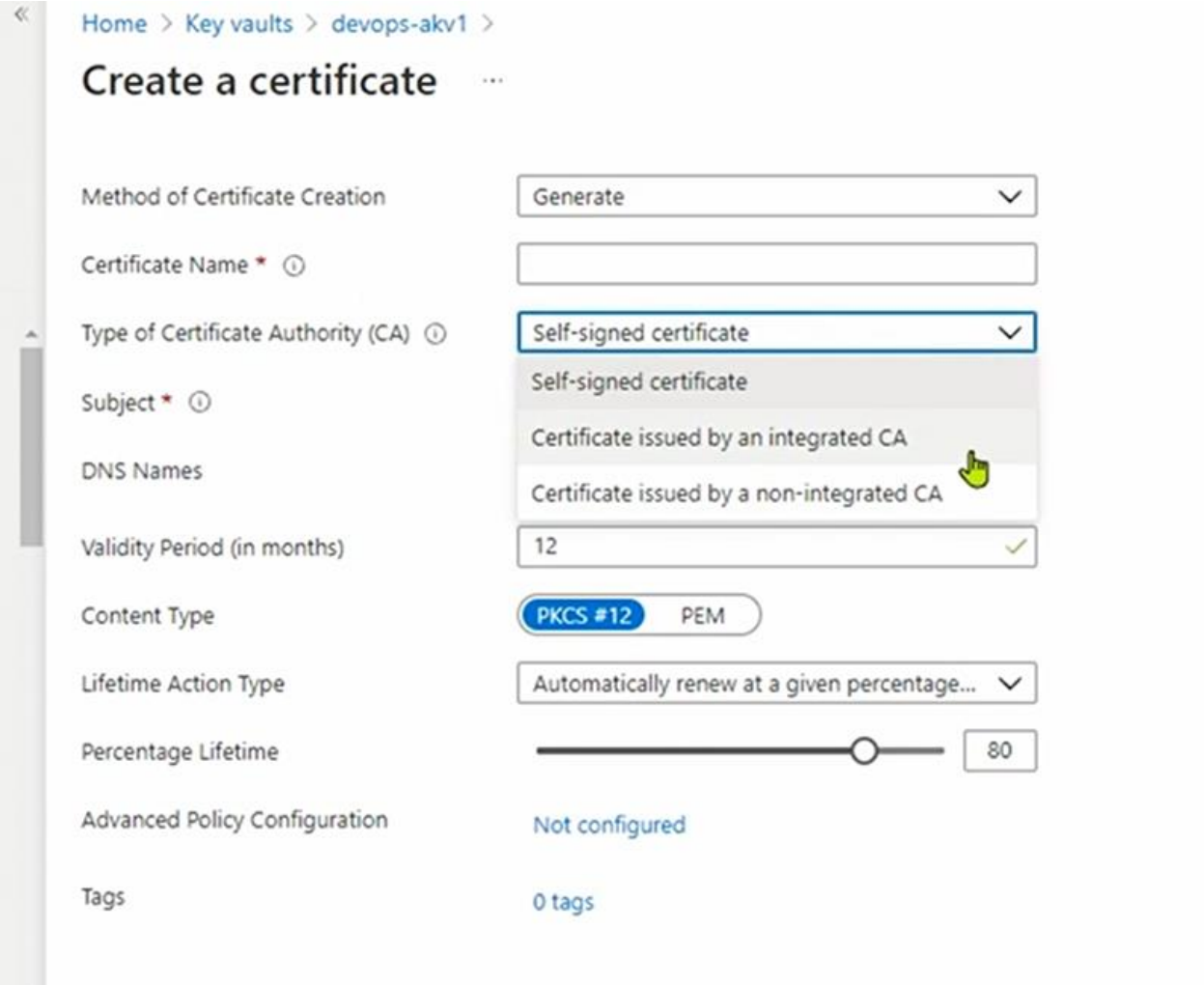



Home > Key vaults > devops-akv1 >
Create a key
Options
Generate
Name *
Key type
RSA
EC
RSA key size
2048
3072
4096
Set activation date
Set expiration date
Enabled
Yes
No
Tags
0 tags


Microsoft Azure
Search resources, services, and docs (G+/)
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
Security Center
Azure Sentinel
Azure Cosmos DB
Key vaults
Virtual machines
SQL servers
SQL databases
Storage accounts
Application gateways
App Services
Function App
Home > Key vaults > devops-akv1
devops-akv1 | Secrets
Key vault
Directory: Lumagate Inc
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Events
Settings
Keys
Secrets
Certificates
Access policies
Networking
Security
Properties
Generate/Import
Refresh
Restore Backup
Manage deleted secrets
Name
Type
Status
There are no secrets available.


Home > Key vaults > devops-akv1 >
Create a secret
Upload options
Manual
The Azure Portal currently only supports single-line secret values. Please use Azure PowerShell to set multi-line values.
Value *
Content type (optional)
Set activation date
Set expiration date
Enabled
Yes
No
Tags
0 tags


Home > Key vaults > devops-akv1 >
Create a secret
Upload options
Manual
Name *
pzerger
Value *
Content type (optional)
Set activation date
Set expiration date
Enabled
Yes
No
Tags
0 tags


Home > Key vaults > devops-akv1 >
Create a certificate
Method of Certificate Creation
Generate
Certificate Name *
Type of Certificate Authority (CA)
Self-signed certificate
Self-signed certificate
Certificate issued by an integrated CA
Certificate issued by a non-integrated CA
Subject *
DNS Names
Validity Period (in months)
12
Content Type
PKCS #12
PEM
Lifetime Action Type
Automatically renew at a given percentage...
Percentage Lifetime
80
Advanced Policy Configuration
Not configured
Tags
0 tags

Home > Key vaults > devops-akv1 >

# Create a certificate

| | |
|---|---|
| Method of Certificate Creation | Generate |
| Certificate Name * | |
| Type of Certificate Authority (CA) | Certificate issued by an integrated CA |
| Certificate Authority (CA) * | Not configured |
| Subject * | For example: "CN=mydomain.com". |
| DNS Names | 0 DNS names |
| Validity Period (in months) | 12 |
| Content Type | PKCS #12 PEM |
| Lifetime Action Type | Automatically renew at a given percentag... |
| Percentage Lifetime | 80 |
| Advanced Policy Configuration | Not configured |
| Tags | 0 tags |

Create

Home > Key vaults > devops-akv1 >

## Certificate Authorities

devops-akv1

+ Add  Refresh

| Name | Provider |
|---|---|
| There are no certificate authorities available. | |

## Create a certificate authority

Name

Provider

DigiCert

DigiCert

GlobalSign

Account Password

Organization ID

## For the Exam

Familiarize yourself with the details of data plane management capabilities in a different Azure Key Vault.

### 3.4 Configure key rotation

## Automated Key Rotation in AKV

- **Step 1**: Store a secret in Azure Key Vault
- **Step 2**: Set up an Azure Automation account
- **Step 3**: Configure the key rotation runbook
- **Step 4**: Configure auditing (optional)

## Solution Components

**Key Rotation**

Key Vault

Azure Automation

PowerShell (runbook)

**Auditing**

Functions

Service Bus

## 3.5 Backup and recovery of certificates, secrets, and keys

# Key Vault Redundancy

### Azure Key Vault Has Multiple Layers of Redundancy

Instance level

- Replicated to another region
- After failover, instance is read only
- Requests are rerouted automatically

Item level

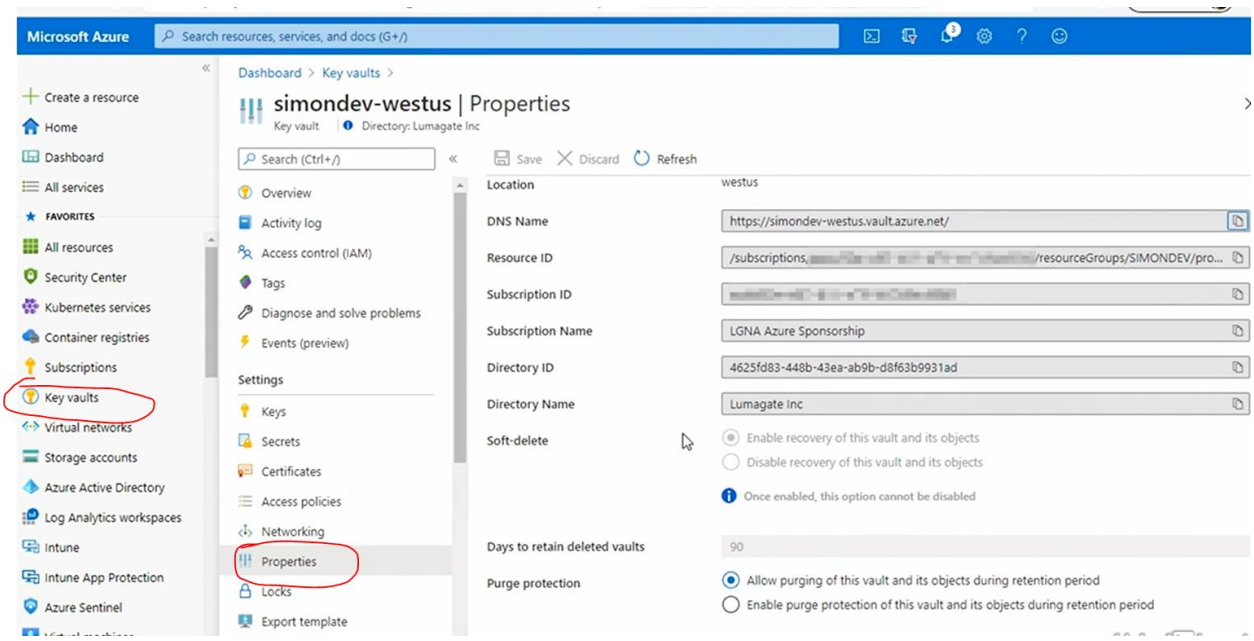
- Soft delete and purge protection
- Backup and restore

# Item-Level Backup and Restore

```
# To create a backup of a specific Key, we can use
Backup-AzureKeyVaultKey -VaultName <Vault-Name> -Name <Key-Name>
```

Result will be a file on the local path
Use `-OutputFile` to control name and path

```
# To restore a specific Key, we can use
Restore-AzureKeyVaultKey -VaultName <Vault-Name> -InputFile <file>
```




## 4.6 Quiz

Question 1 of 5

What Key Vault setting can administrators configure to prevent key vault contents from being deleted before a specified time period?

- Retention period
- Hard delete
- Soft delete
  Incorrect
- Purge protection
  Correct
  Purge protection can be enabled by an administrator, which enforces an administrator-configurable retention period. Soft delete is enabled by default, and cannot be disabled.

Question 2 of 5

Who/what can you grant key vault access to?

- applications
- users
- groups
- all of these answers

  Correct

  You can grant key vault access to an Azure AD user, group, or an application.

Question 3 of 5

What is the narrowest (most restrictive) scope for configuring permissions to an Azure Key Vault instance?

- management group
- resource

  Correct

  Granting permissions on the resource itself ensures permissions are not automatically or unintentionally granted to other Key Vault instances.
- resource group
- subscription

Question 4 of 5

When automating key rotation, Azure Automation runbooks require the use of the AzureRM module with key rotation for Azure Storage.

- TRUE
  This was the correct answer
- FALSE
  Incorrect

Review this video

Question 5 of 5

You can limit operations on a key in Azure Key Vault by configuring the settings under Permitted operations.

- FALSE
  Incorrect
- TRUE
  This was the correct answer

## Certificate

LinkedIn LEARNING

Certificate of Completion

Congratulations, Seolito Rodriguez

**Microsoft Azure Security Technologies (AZ-500) Cert Prep: 4 Secure Data and Applications**

Course completed on Feb 09, 2022 at 03:01AM UTC • 52 min

By continuing to learn, you have expanded your perspective, sharpened your skills, and made yourself even more in demand.

Head of Content Strategy, Learning

LinkedIn Learning
1000 W Maude Ave
Sunnyvale, CA 94085

Certificate Id: AYnMNT9xcWb8OpclsVCac1DgNWhk

# References


[Become an Azure Security Engineer (linkedin.com)]