

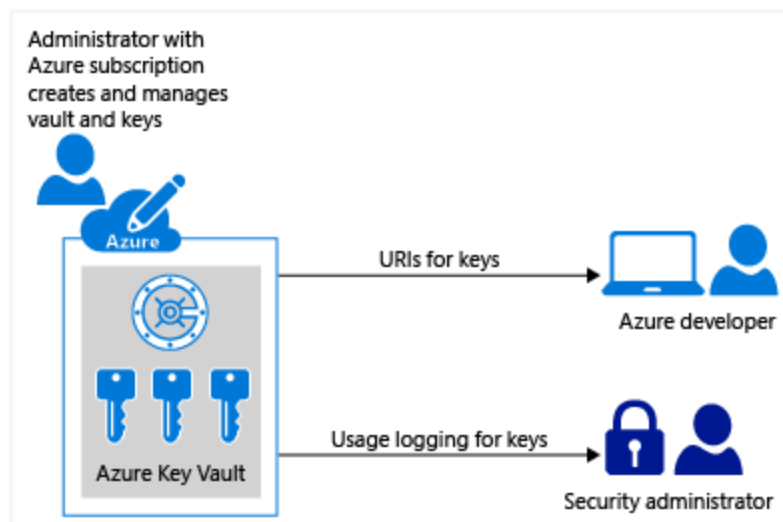


# Stories 13: Azure Key Vault Service

**Azure Key Vault** is a cloud service for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, certificates, or cryptographic keys. Key Vault service supports two types of containers: vaults and managed hardware security module(HSM) pools.

## Hardware Security Module (HSM):

- An HSM is a specialized hardware device designed to securely store and manage cryptographic keys and perform various cryptographic operations.
- Think of it as a highly secure digital safe that protects and manages sensitive information related to encryption.



## 1. Secrets Management:

- Azure Key Vault enables you to store and retrieve sensitive information such as API keys, connection strings, and passwords securely.
- You can manage these secrets centrally, and they can be versioned, so you can keep track of changes over time.

## **2. Key Management:**

- It provides a secure and scalable way to create, import, and control access to cryptographic keys used by cloud applications and services.
- Supports operations like key generation, encryption, decryption, signing, and verification.

## **3. Certificate Management:**

- You can securely store and manage X.509 certificates and their associated private keys.
- Azure Key Vault can automate the renewal of certificates, reducing the manual effort required to maintain certificates.

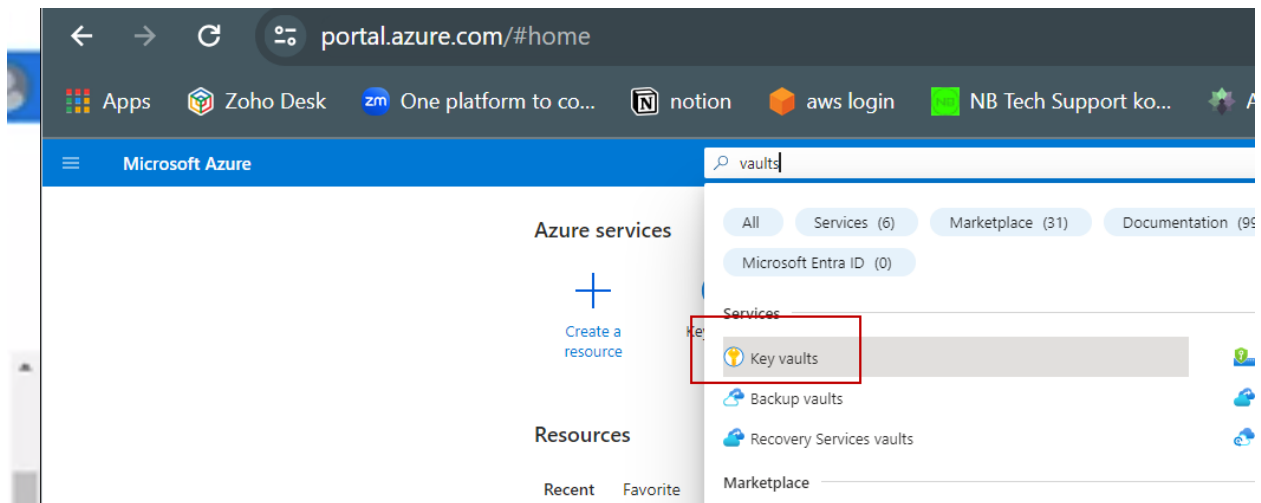
## **4. Access Control:**

- Azure Key Vault integrates with Azure Active Directory (Azure AD) for authentication and authorization.
- Role-Based Access Control (RBAC) is used to control who can perform operations on the key vault and its contents.

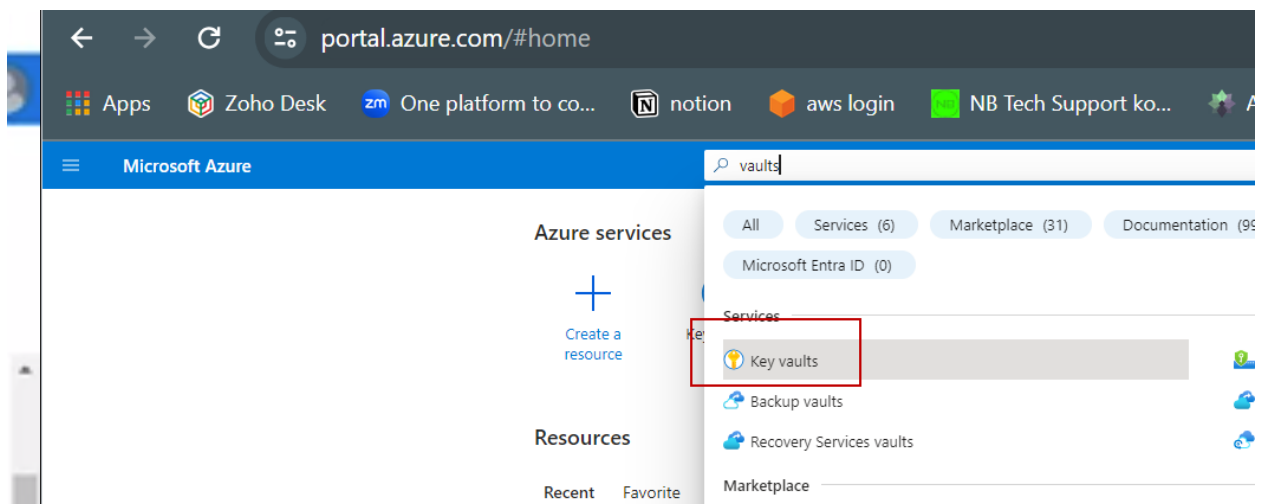
## **5. Audit Logging:**

- Azure Key Vault provides detailed audit logs, allowing you to monitor access and actions performed on the stored secrets, keys, and certificates.

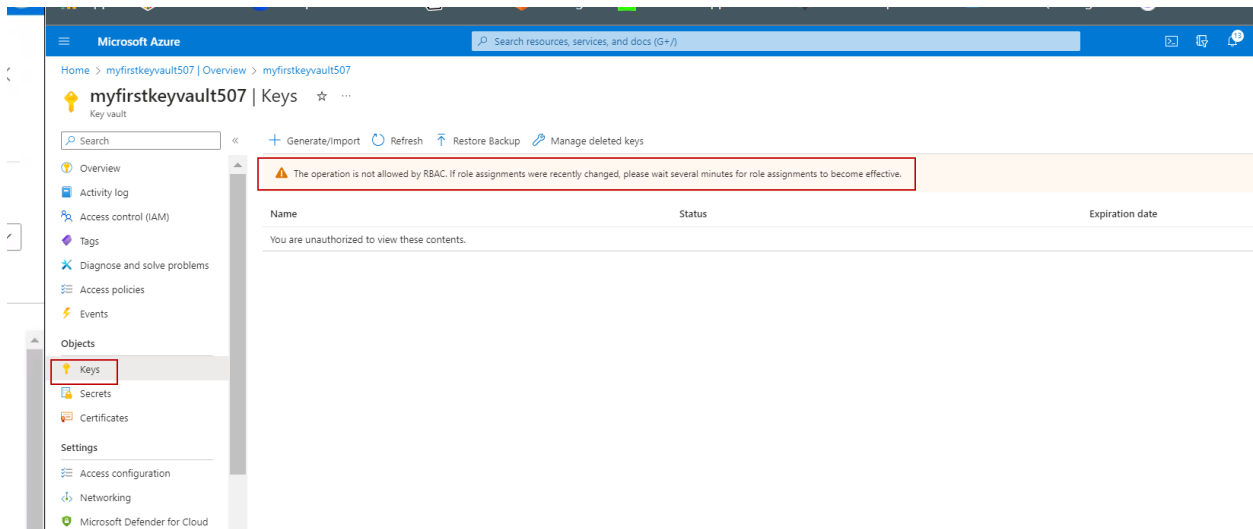
**Lab : Create a Key vault service and assign role to it**



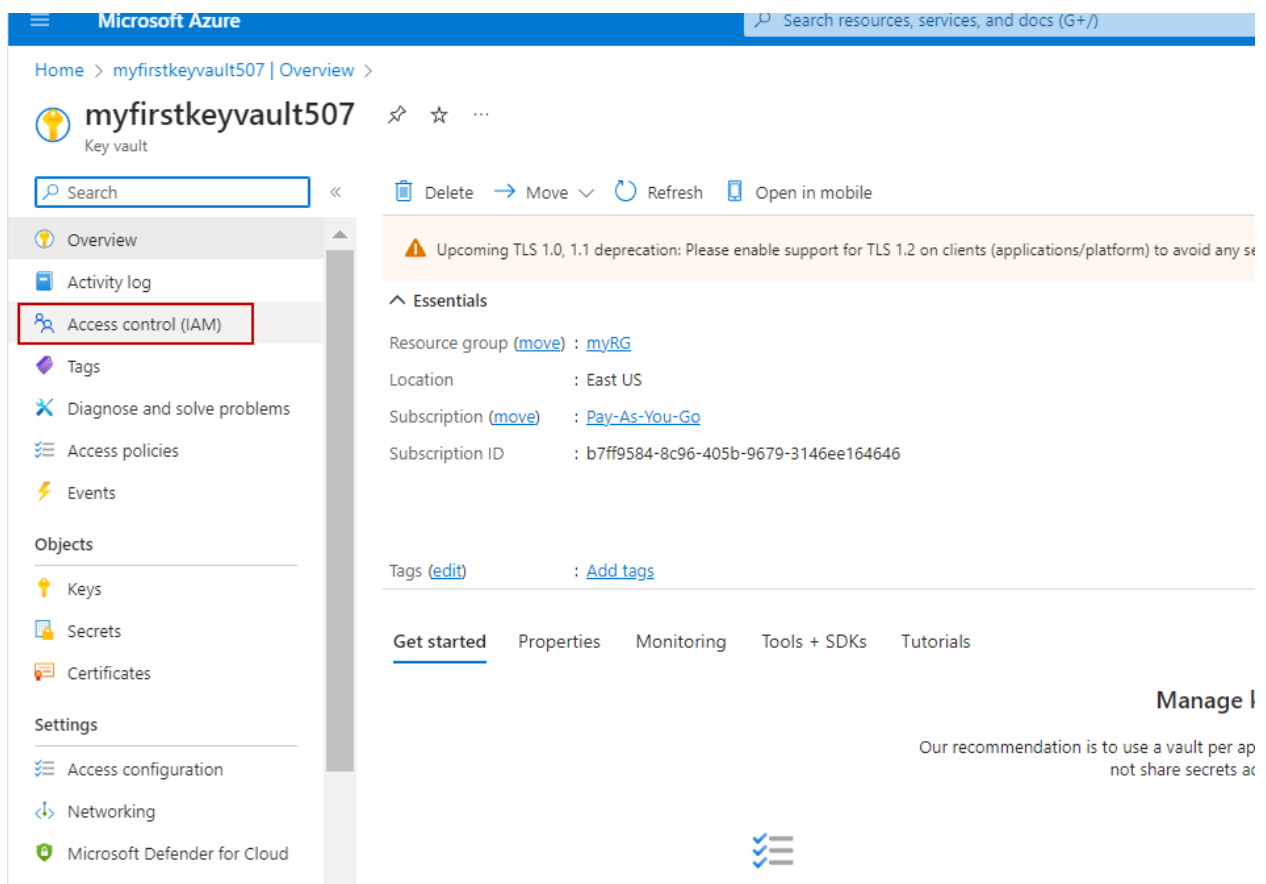
Create a key vault



Goto keys



Assign role now from iam roles



## Assign role

The screenshot shows the Azure portal interface for the 'myfirstkeyvault507' resource. The breadcrumb navigation at the top reads 'Home > myfirstkeyvault507 | Overview > myfirstkeyvault507'. The page title is 'myfirstkeyvault507 | Access control (IAM)'. On the left, a sidebar contains navigation links: Overview, Activity log, Access control (IAM) (selected), Tags, Diagnose and solve problems, Access policies, and Events. The main content area has a top bar with a search box and action buttons: Add, Download role assignments, Edit columns, Refresh, Remove, and Feedback. Below this, a dropdown menu is open, showing 'Add role assignment' (highlighted with a red box), 'Add co-administrator', and 'Add role assignment' (repeated). The 'My access' section includes a 'View my access' button. The 'Check access' section includes a 'Check access' button.

Home > myfirstkeyvault507 | Overview > myfirstkeyvault507

myfirstkeyvault507 | Access control (IAM) ☆ ...

Key vault

Search

« + Add ↓ Download role assignments ≡ Edit columns ↺ Refresh ✕ Remove 🗨 Feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Access policies

Events

Objects

nts Roles Deny assignments Classic administrators

Add role assignment

Add co-administrator

Add role assignment

**My access**

View my level of access to this resource.

[View my access](#)

**Check access**

Review the level of access a user, group, service principal, or managed identity has to this resource. [Learn more](#)

[Check access](#)

## Add role assignment ...

**Role**

Members

Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles.  
Assignment type

**Job function roles**

Privileged administrator roles

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

 Search by role name, description, or ID

Type : All

Category : All

Name ↑↓

Description ↑↓

Reader	View all resources, but does not allow you to make changes to the resources.
App Compliance Automation Administrator	Create, read, download, modify and delete reports and configurations.
App Compliance Automation Reader	Read, download the reports objects and related configurations.
Desktop Virtualization Virtual Machine Contributor	This role is in preview and subject to change. Provides permissions to create and manage virtual machines.
Key Vault Administrator	Perform all data plane operations on a key vault and manage the key vault.
Key Vault Certificate User	Read certificate contents. Only works for key vaults that use the certificate interface.
Key Vault Certificates Officer	Perform any action on the certificates of a key vault, except for deleting a certificate.
Key Vault Contributor	Lets you manage key vaults, but not access to them.
Key Vault Crypto Officer	Perform any action on the keys of a key vault, except for deleting a key.
Key Vault Crypto Service Encryption User	Read metadata of keys and perform wrap/unwrap operations.
Key Vault Crypto Service Release User	Release keys. Only works for key vaults that use the release interface.

Review + assign

Previous

Next

Select role and user

## Add role assignment ...

**Role** **Members** **Review + assign**

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles.  
Assignment type

**Job function roles** Privileged administrator roles

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

 Search by role name, description, or ID

Type : **All**

Category : **All**

Name ↑↓

Description ↑↓

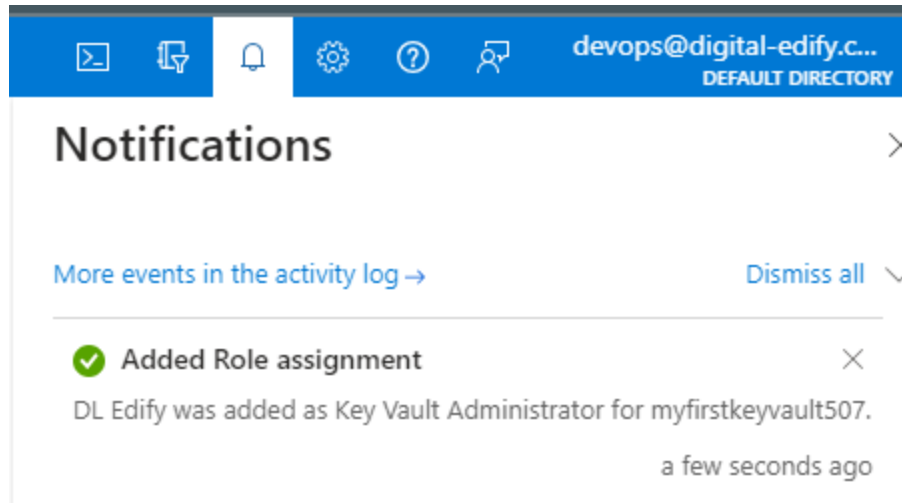
Reader	View all resources, but does not allow you to make c
App Compliance Automation Administrator	Create, read, download, modify and delete reports c
App Compliance Automation Reader	Read, download the reports objects and related oth
Desktop Virtualization Virtual Machine Contributor	This role is in preview and subject to change. Provid
Key Vault Administrator	Perform all data plane operations on a key vault and
Key Vault Certificate User	Read certificate contents. Only works for key vaults 1
Key Vault Certificates Officer	Perform any action on the certificates of a key vault,
Key Vault Contributor	Lets you manage key vaults, but not access to them.
Key Vault Crypto Officer	Perform any action on the keys of a key vault, excep
Key Vault Crypto Service Encryption User	Read metadata of keys and perform wrap/unwrap o
Key Vault Crypto Service Release User	Release keys. Only works for key vaults that use the

**Review + assign**

Previous

Next

### Review and assign





Now view

create a secret and view it





Home > myfirstkeyvault507 | Overview > myfirstkeyvault507 | Secrets > myvmpassword >

 **f06ad07fee954caa6f4309aac5dd7d**  ...

Secret Version

---

Properties

Created	1/24/2024, 10:08:54 AM
Updated	1/24/2024, 10:08:54 AM
Secret Identifier	<a href="https://myfirstkeyvault507.vault.azure.net/secrets/myvmpassword/f06ad07fee954caa6f4309aac5dd7d">https://myfirstkeyvault507.vault.azure.net/secrets/myvmpassword/f06ad07fee954caa6f4309aac5dd7d</a> 
Settings	
Set activation date ⓘ	<input type="checkbox"/>
Set expiration date ⓘ	<input type="checkbox"/>
Enabled	<span>Yes</span> <span>No</span>
Tags	0 tags
Secret	
Content type (optional)	myvmpassword
	<a href="#">Hide Secret Value</a>
Secret value	azureuser 

You can give access to other users as well in organization for our vault service.