Caltech | Center for Technology & Management Education

Post Graduate Program in Cloud Computing

Powered by simplilearn

Caltech | Center for Technology & Management Education

PG CC - Microsoft Azure Architect Technologies: AZ:303

Powerd by simplilearn

Manage Security for Applications

Learning Objectives

By the end of this lesson, you will be able to:

- Implement and configure Key Vault
- Implement and configure Managed Identities
- Register and manage applications in Azure AD

A Day in the Life of an Azure Architect

You are working for an organization that is looking for some security solutions available in azure to access the resources.

You have been asked to advise a solution that can be used to access Azure resources through applications, hosted services, and automated tools. The solution must be assigned a certain role that will limit this access, providing the control over which resources can be accessed and to what degree.

Additionally, the organization is looking for a solution to store sensitive data such as passwords that a user uses to access an application.

To achieve all the above along with some additional features, we will be learning a few concepts in this lesson that will help you find a solution for the given scenario.

Implement and Configure Key Vault

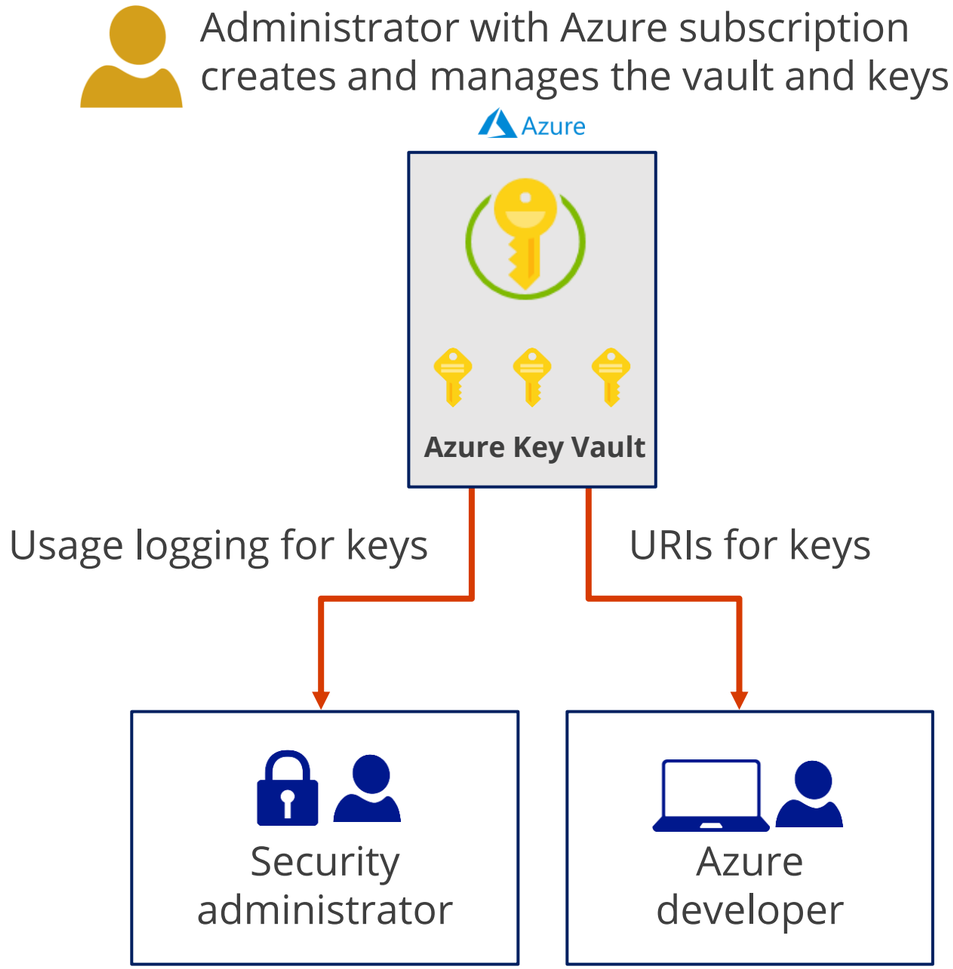
Azure Key Vault

Azure key vault is a centralized cloud service to store sensitive data such as encryption keys, certificates, and server-side tokens.

Azure Key Vault

Key Vault Offerings

- Storing secrets
- Managing stored secrets
- Managing keys
- Managing certificates



Benefits of Azure Key Vault

These are the benefits of Azure key vault:

- Centralize application secrets
- Securely store secrets and keys
- Monitor access and use
- Simplified administration of application secrets
- Integrate with other Azure services

Keys

A keys are the central actor in the Azure Key Vault service.

- A key is a cryptographic asset used for specific purpose

  For instance, A key used for SQL Server TDE
- Applications never have direct access to keys
- Keys can be single instanced (only one key exists)
- Keys can be versioned (mix of primary and secondary keys)

Keys

There are two types of keys in Key Vault:

Hardware Protected Keys	Uses Hardware security modules (HSMs) that provide a hardened, tamper-resistant environment for cryptographic processing, and key generation
Software Protected Keys	Uses software-based Rivest–Shamir–Adleman (RSA) and Elliptic curve cryptography (ECC) algorithms

Secrets

Secrets are small (less than 10K) data blobs protected by Hardware security modules generated key that is with the Key Vault.

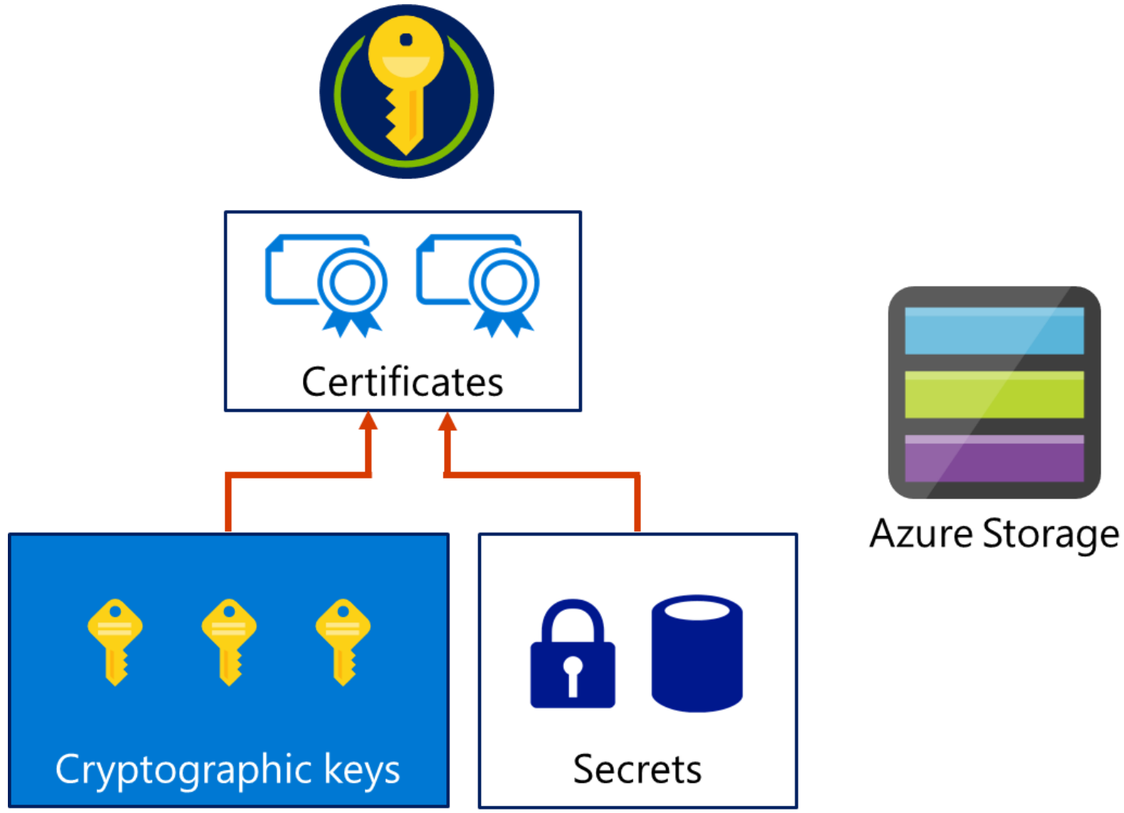


image source: https://docs.microsoft.com/en-in/

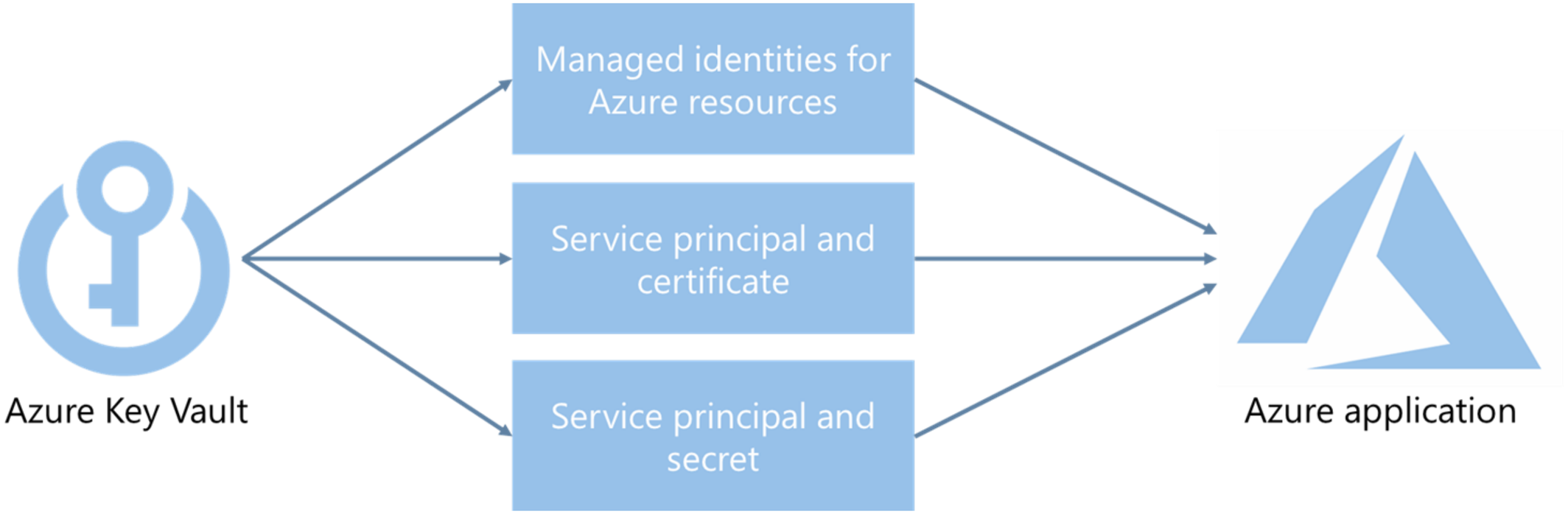
Types of Secrets

Secret Types	Description
Cryptographic keys	Key Vault supports multiple key types and algorithms and uses hardware security modules (HSMs) for high-value keys.
Secrets	Key Vault provides secure storage of secrets, such as passwords and database connection strings.
Certificates	Key Vault supports certificates, which are built on top of keys and secrets, and add an automated renewal feature.
Azure Storage	Key Vault can manage the keys of an Azure Storage account. Internally, Key Vault can list (sync) keys with an Azure Storage Account and regenerate (rotate) the keys periodically.

Key Vault: Terminologies

- Vault Owner
- Vault Consumer
- Service Principal
- Azure Active Directory
- Azure Tenant ID
- Managed Identities

Key Vault Authentication



Key Vault: Best Practices

Grant access for a specific scope

Control what users have access to

Store certificates in the key vault

Ensure that the deleted key vault or key vault objects can be recovered

Managed Identity

Azure Managed Identity

It provides identity for application to connect with resources that support Azure AD authentication.

Benefits

- Combines Azure AD authentication and Azure RBAC
- Eliminates the need for rotating credentials or certificates

Azure Managed Identity Terminologies

Client ID	A unique ID linked to the Azure AD application and service principal. It is created when a user provisions an identity.
Azure Instance Metadata Service	A REST API that's enabled when Azure Resource Manager provisions a VM. The endpoint is accessible only from within the VM.
Object ID	The service principal object of the managed identity.

Types of Managed Identity

User-assigned managed identity

- It is created as a standalone azure resource.
- When a user-assigned identity is provisioned
- Azure creates a service principal just as it does for a system-assigned identity.

System-assigned managed identity

- It is enabled on an azure service instance, such as a VM.
- When a user enables the identity, azure creates a service principal through Azure Resource Manager.

Managed Identity for Azure Resources

It manages the credentials to authenticate cloud services, when building cloud applications:

Keeps credentials out of code

Uses a local MSI endpoint to get access tokens from Azure AD

Manages the identity in Azure AD for Azure resources automatically

Offers direct authentication with services or retrieval of credentials from Azure Key Vault

Workflow of Managed Identity

The following diagram shows the internal workflow of Managed Identity:

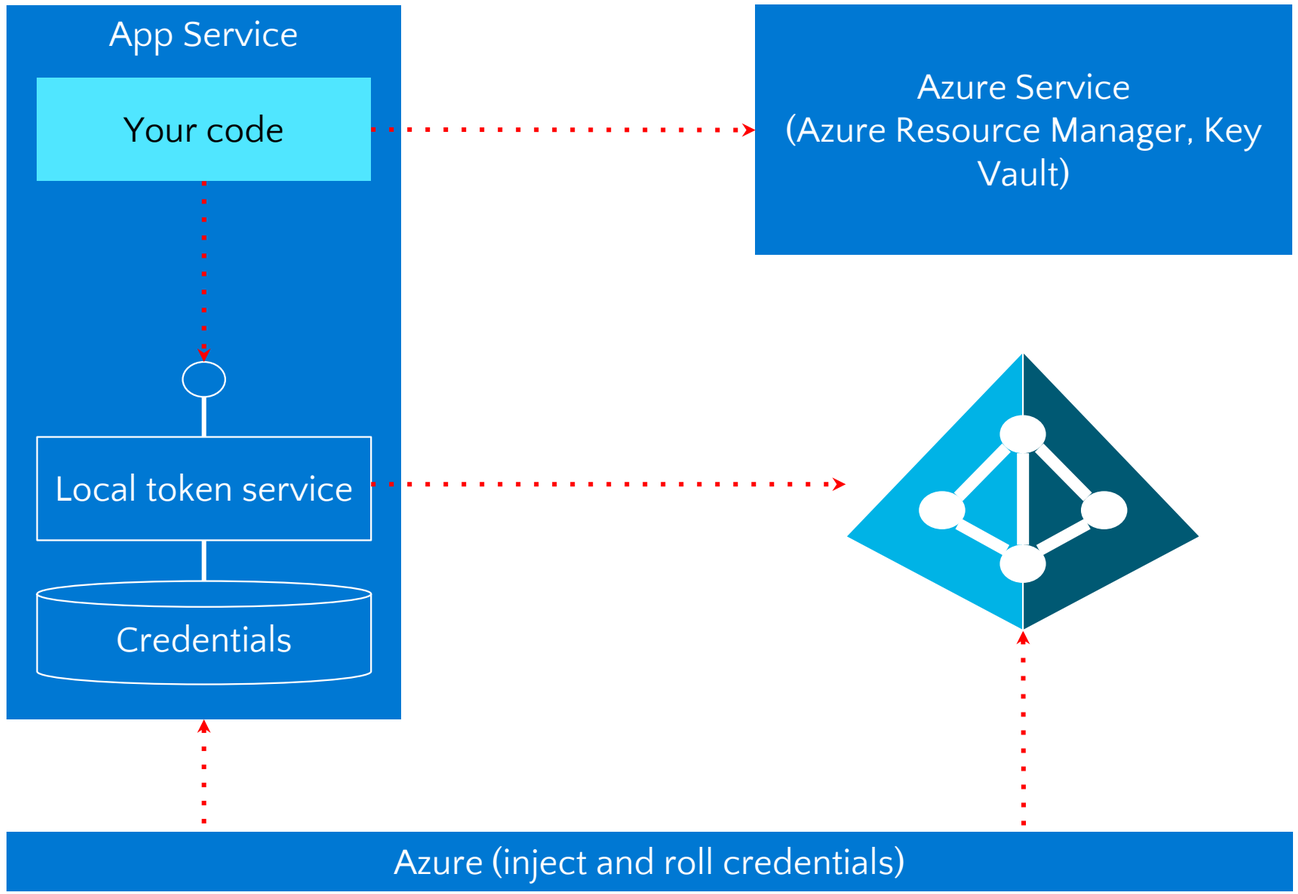
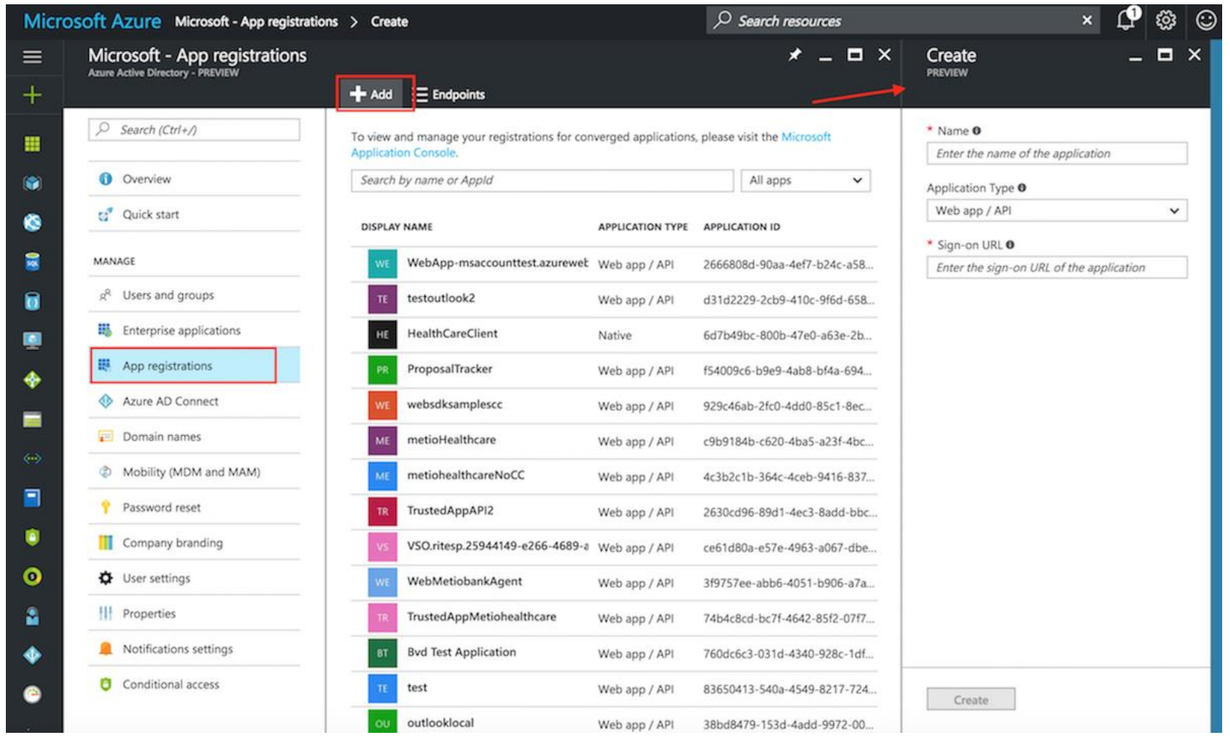


image source: https://docs.microsoft.com/en-in/

App Registration

Registering an application provides authentication and authorization services for the application and its users.



An application can be registered under Azure Active Directory

Assisted Practice

Create a Service Principal

Duration: 10 Min.

Problem Statement:

You're given a project to construct a service principle that you can use to access Azure resources through applications, hosted services, and automated tools. The roles granted to the service principal will limit this access, providing you control over which resources can be accessed and at what degree.

Assisted Practice: Guidelines

Steps to create a service principal are:

1. Login to your Azure portal
2. Select Azure Active Directory
3. Select App registrations under manage
4. Fill in the required details
5. Azure AD application and service principal is created

Assisted Practice

Azure Key Vault

Duration: Min

Problem Statement:

You've been assigned the task of creating an Azure key vault to store keys, passwords, certifications, and other sensitive information.

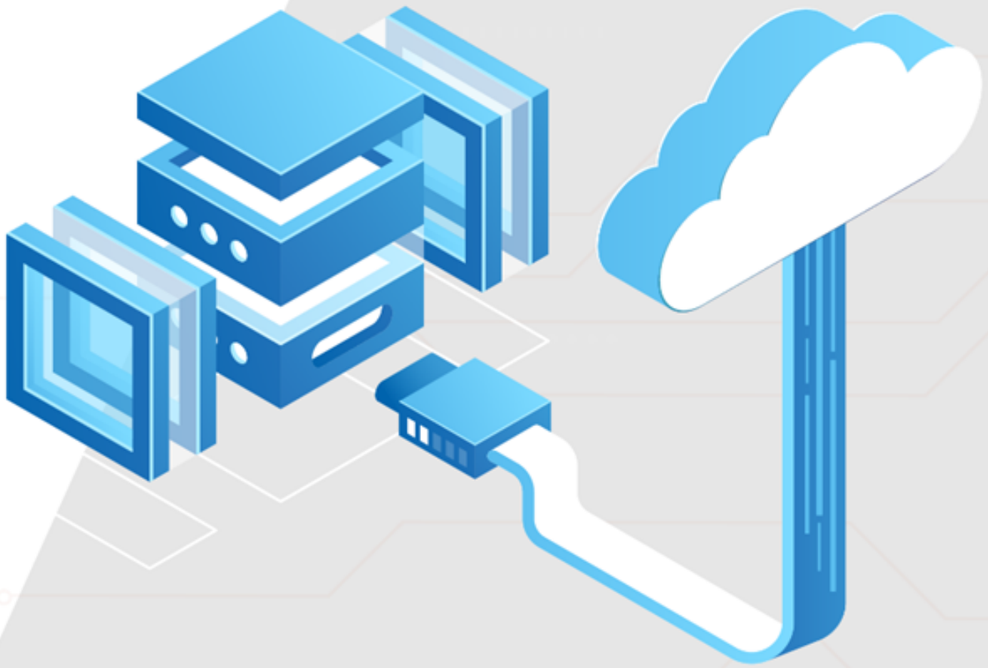
Assisted Practice: Guidelines

Steps to create an Azure key vault are:

1. Login to your Azure portal
2. Search and select key vault
3. Select create on key vault page
4. Provide the details and create Azure key vault

Key Takeaways

- Azure Key Vault is a centralized cloud service for storing application secrets.
- A key is a cryptographic asset which is used for a specific purpose.
- Azure Managed Identity provides identity for an application to connect with the resources that support Azure AD authentication.



Thank you