July 26, 2022

AZURE COE

Activities newsletter

In this issue:

- CoE Status
- Things to remember
- Key Vault | MS Azure

CoE Status

This month we hosted a Learning Session to allow people compare services between Azure and AWS cloud, we still recruiting people who want to add value through the CoE sharing knowledge or helping in other activities, like this newsletter.

Things to remember: What are Cloud Models?

Private Cloud:
A private cloud is, in some ways, the natural evolution from a corporate datacenter. It's a cloud that's build, controlled, and maintained by a single entity.

Public cloud:
A public cloud is built, controlled, and maintained by a third-party cloud provider. With a public cloud, anyone that wants to purchase cloud services can access and use resources.

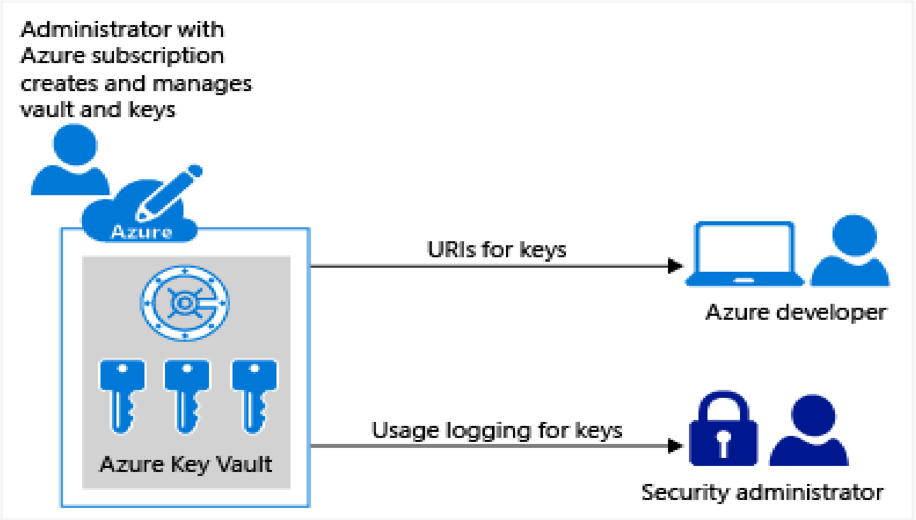
Hybrid cloud:
A hybrid cloud is a computing environment that uses both public and private clouds in an inter-connected environment. A hybrid cloud environment can be used to allow a private cloud to surge for increased, temporary demand by deploying public cloud resources .

"I am not the smartest fellow in the world, but I sure can pick smart colleagues…"

-FRANKLIN D. ROOSVELT

What is Azure Key Vault

Azure Key Vault:
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



Azure Key Vault

July 26, 2022

AZURE COE

Important terms:

Tenant: A tenant is the organization that owns and manages a specific instance of Microsoft cloud services.

Vault Owner: A vault owner can create a key vault and gain full access and control over it. The vault owner can also set up auditing to log who accesses secrets and keys. Administrators can control the key lifecycle. They can roll to a new version of the key, back it up, and do related tasks.

Vault Consumer: A vault consumer can perform actions on the assets inside the key vault when the vault owner grants the consumer access. The available actions depend on the permissions granted.

Managed HSM Administrators: Users who are assigned the Administrator role have complete control over a Managed HSM pool. They can create more role assignments to delegate controlled access to other users.

Managed HSM Crypto Officer/User: Built-in roles that are usually assigned to users or service principals that will perform cryptographic operations using keys in Managed HSM. Crypto User can create new keys, but cannot delete keys.

Managed HSM Crypto Service Encryption User: Built-in role that is usually assigned to a service accounts managed service identity (e.g. Storage account) for encryption of data at rest with customer managed key.

Resource: A resource is a manageable item that's available through Azure. Common examples are virtual machine, storage account, web app, database, and virtual network. There are many more.

Resource Group: A resource group is a container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups, based on what makes the most sense for your organization.

Security Principal: An Azure security principal is a security identity that user-created apps, services, and automation tools use to access specific Azure resources. Think of it as a "user identity" (username and password or certificate) with a specific role, and tightly controlled permissions. A security principal should only need to do specific things, unlike a general user identity. It improves security if you grant it only the minimum permission level that it needs to perform its management tasks. A security principal used with an application or service is specifically called a service principal.

Azure Active Directory: Azure AD is the Active Directory service for a tenant. Each directory has one or more domains. A directory can have many subscriptions associated with it, but only one tenant.

Azure Tenant ID: A tenant ID is a unique way to identify an Azure AD instance within an Azure subscription.

Managed Identities: Azure Key Vault provides a way to securely store credentials and other keys and secrets, but your code needs to authenticate to Key Vault to retrieve them. Using a managed identity makes solving this problem simpler by giving Azure services an automatically managed identity in Azure AD. You can use this identity to authenticate to Key Vault or any service that supports Azure AD authentication, without having any credentials in your code.