Azure Key Vault

Agenda

Introduction

Managed Identity

KeyVault Basic Concept

Azure Key Vault Security and Best Practices

Solve problems

Secrets Management

- Securely store and control access to Tokens, Passwords, Certificates, API keys and Other secrets

Key Management

- Create and control the encryption keys used to encrypt your data

Certificate Management

- Provision, manage, and deploy public and private Transport Layer Security/Secure Sockets Layer (TLS/SSL) certificates

Why use Azure Key Vault?

Centralize application secrets

Securely store secrets and keys

Monitor access and use

Simplified administration of application secrets

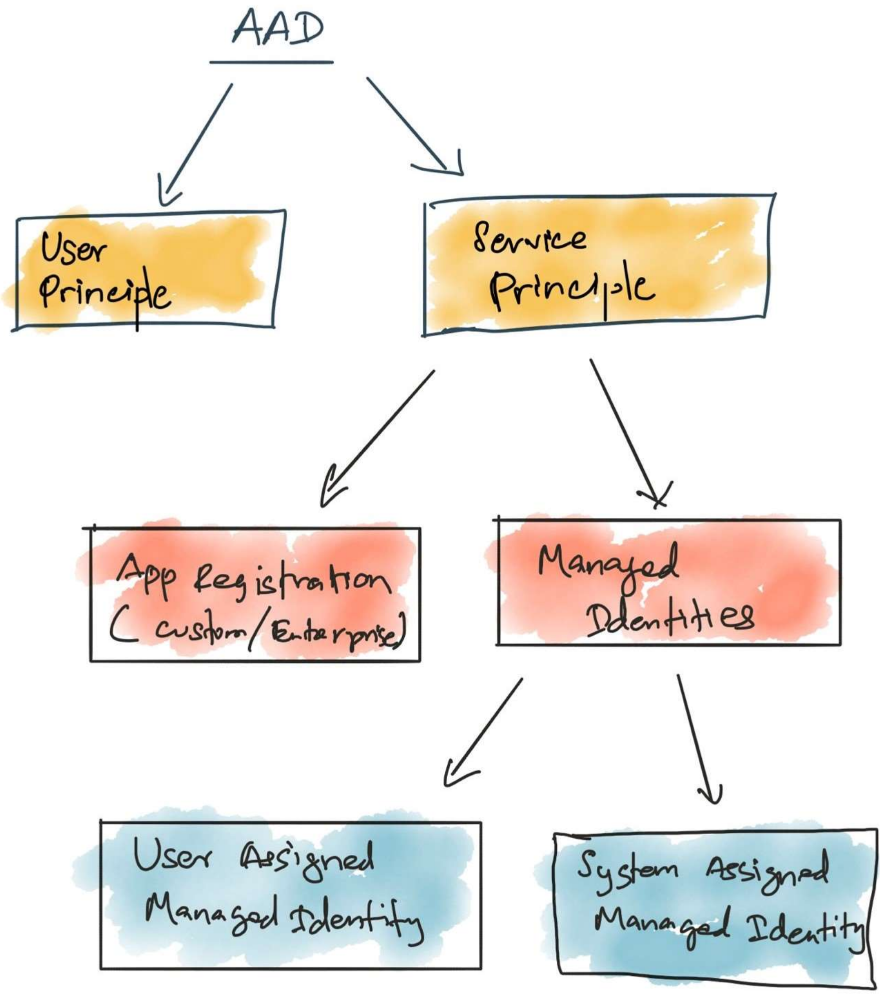
Keys vs Secrets

- Key
  - A Cryptographic key represented as JWK (JSON Web Key).
  - Example: store A .pfx certificate file that contains a pair of public & private keys
- Secret
  - Key Vault accepts any value and stores it as a binary.
  - Example: A password or API key

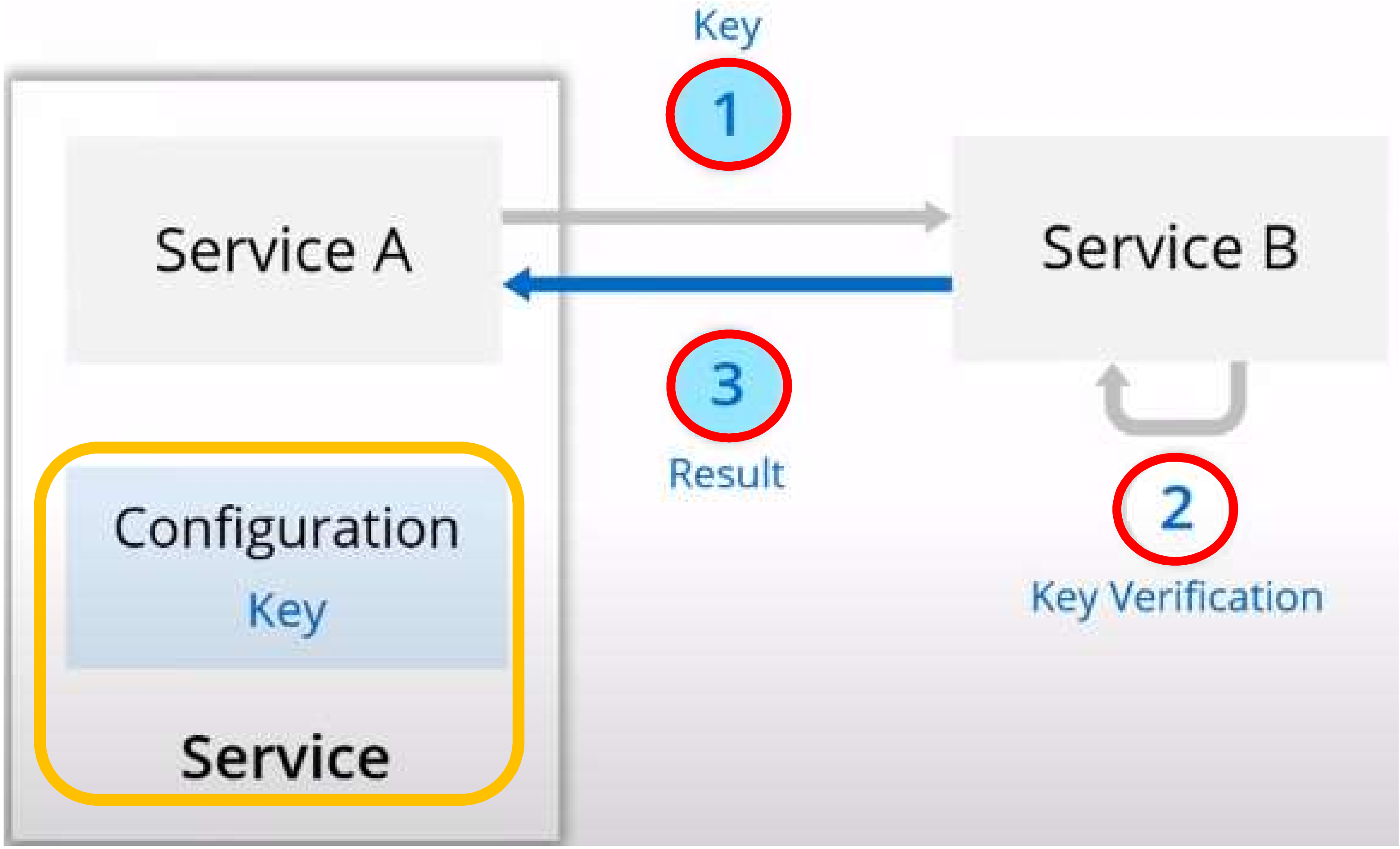
Hands-On: Key Vault

Managed Identity

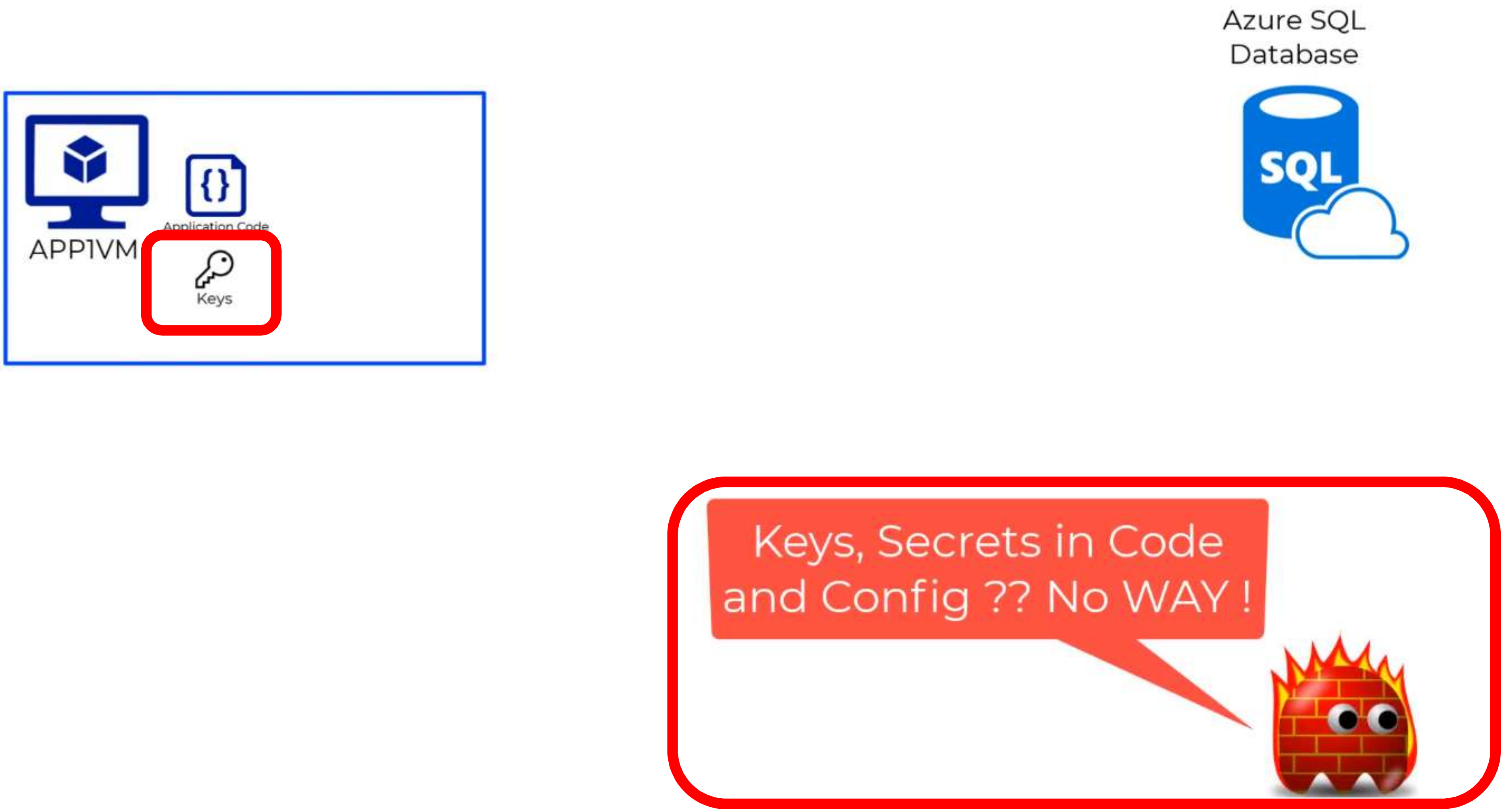
AAD Principle



The Problem


Key
1
Service A
Service B
3
Result
2
Key Verification
Configuration
Key
Service

The Problem



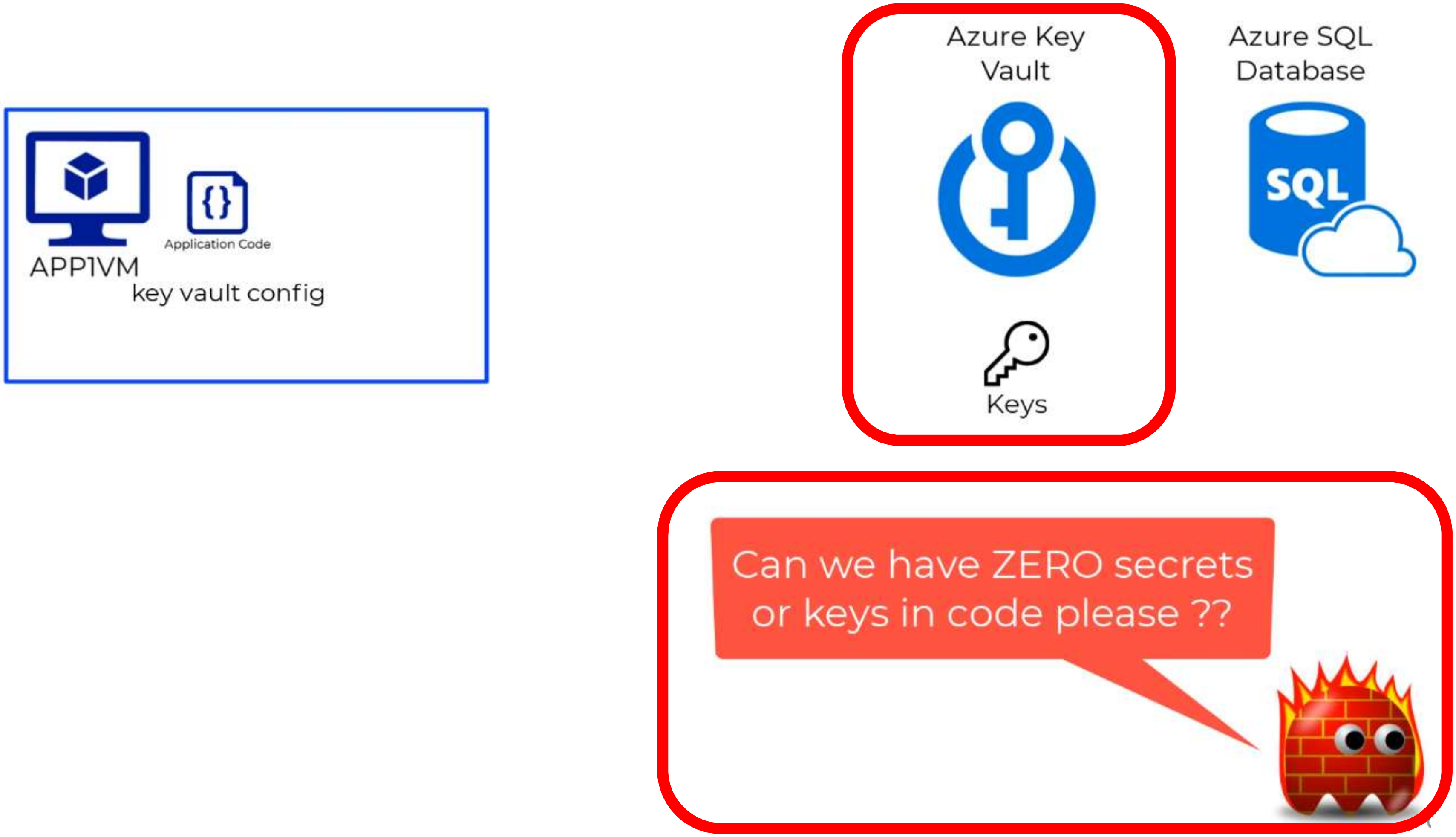
Azure SQL Database

APP1VM

Application Code

Keys

Keys, Secrets in Code and Config ?? No WAY !



APP1VM

Application Code

key vault config

Azure Key Vault

Keys

Azure SQL Database

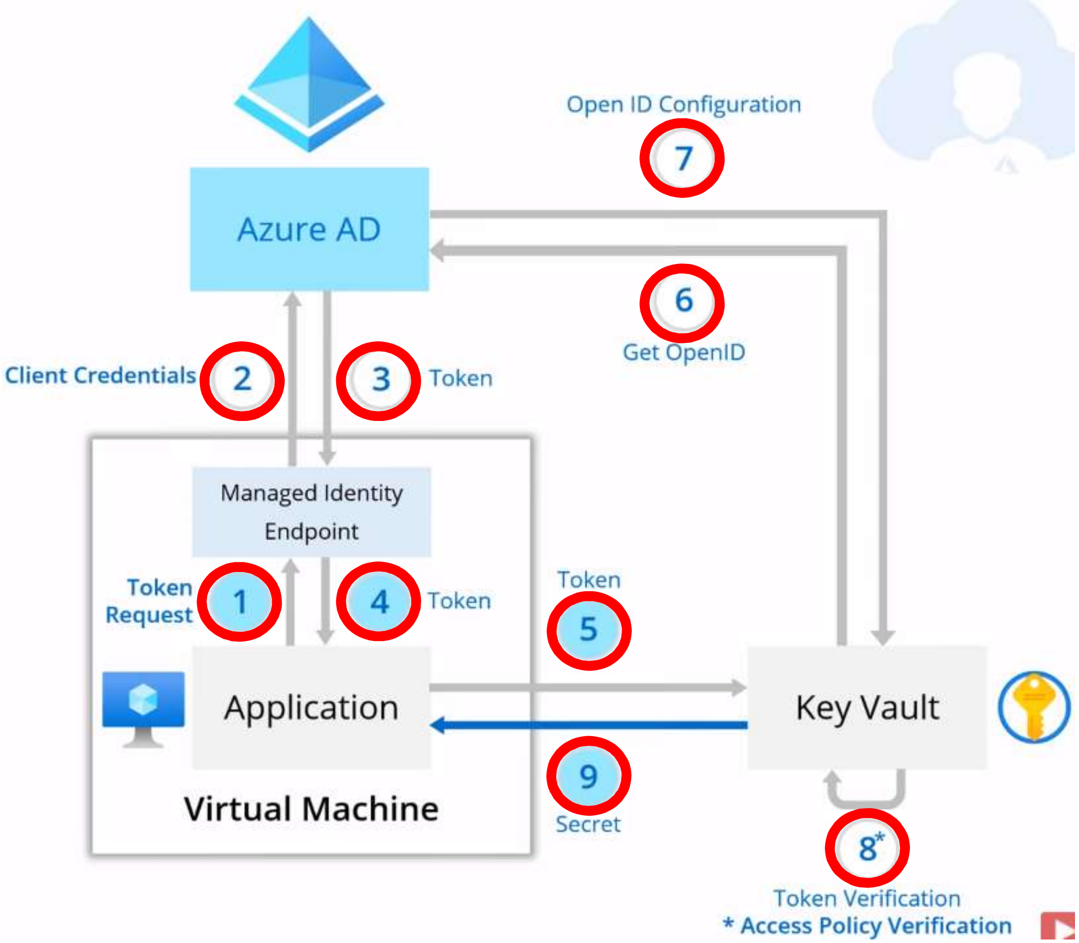
Can we have ZERO secrets or keys in code please ??

Solution: Managed Identities

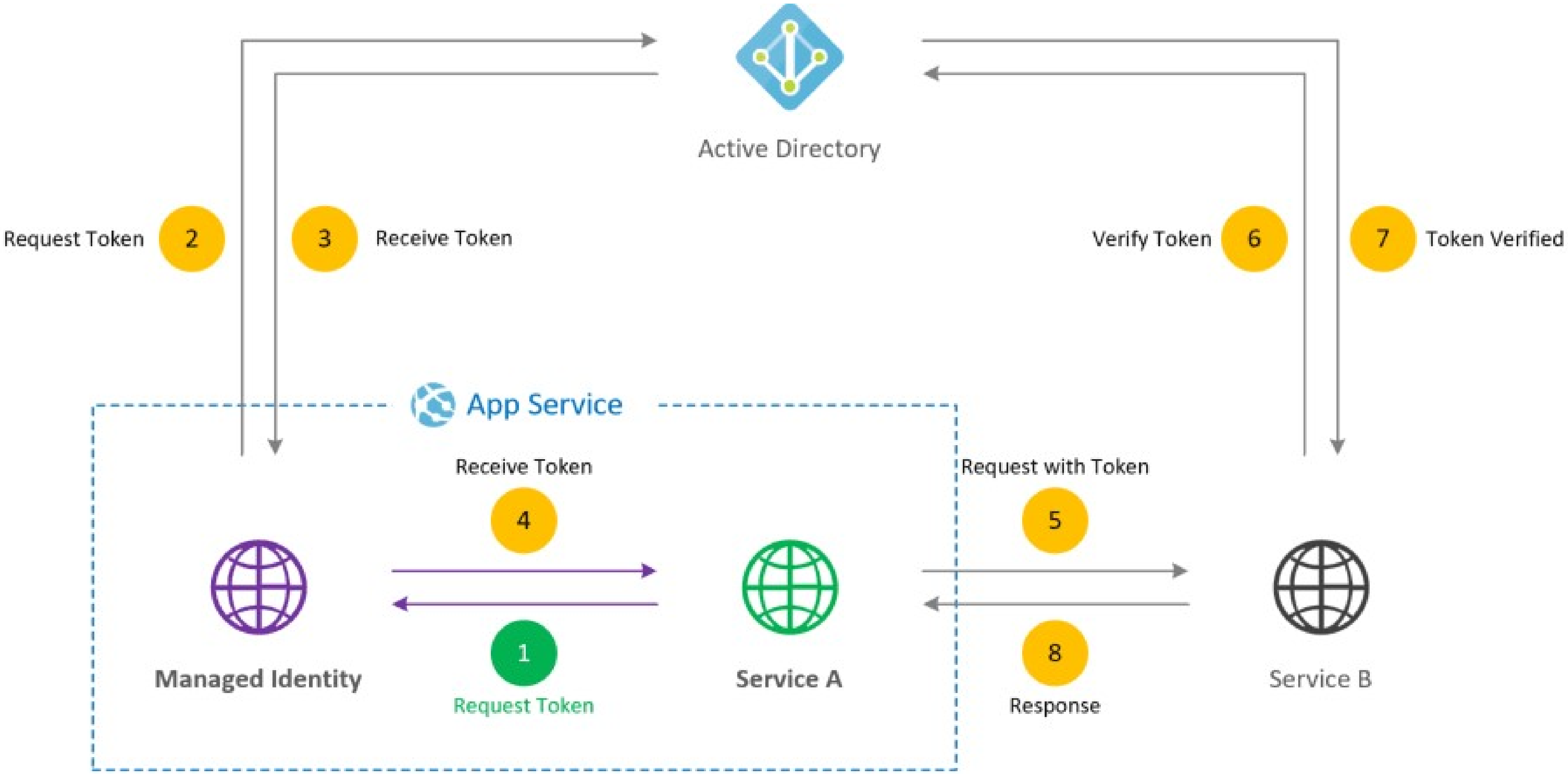
- Characteristics
  - Credentials are moved out of application code
  - Identity created and tied with resource lifecycle
  - Managed Identities are Service Principals of special type
  - Auditable
  - Can be assigned and revoked from individual resources

Managed Identities – Solving Challenges

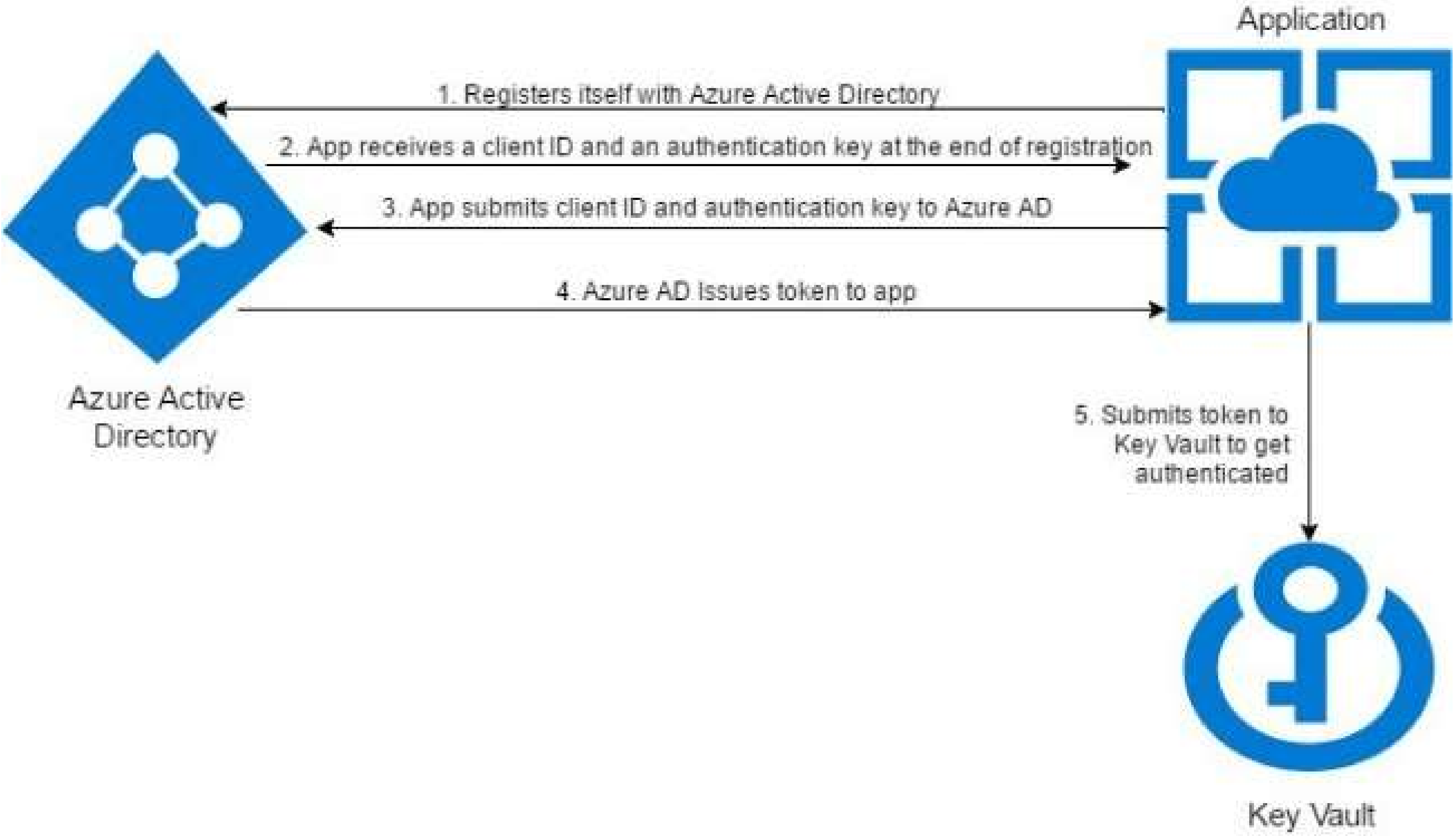
- Internal Endpoint
- No Credentials in the code
- Identity name is the same as resource name
- Identity lifecycle is tied to resource



Managed Identities – Solving Challenges



Managed Identities – Solving Challenges



Application

1. Registers itself with Azure Active Directory

2. App receives a client ID and an authentication key at the end of registration

3. App submits client ID and authentication key to Azure AD

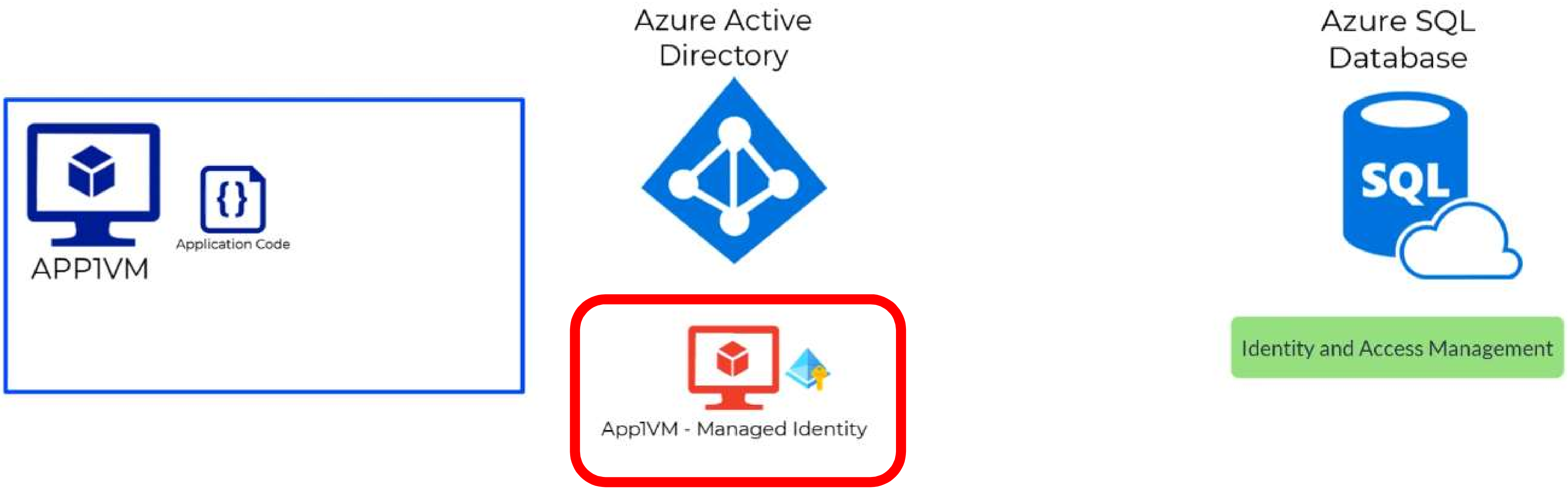
4. Azure AD issues token to app

5. Submits token to Key Vault to get authenticated

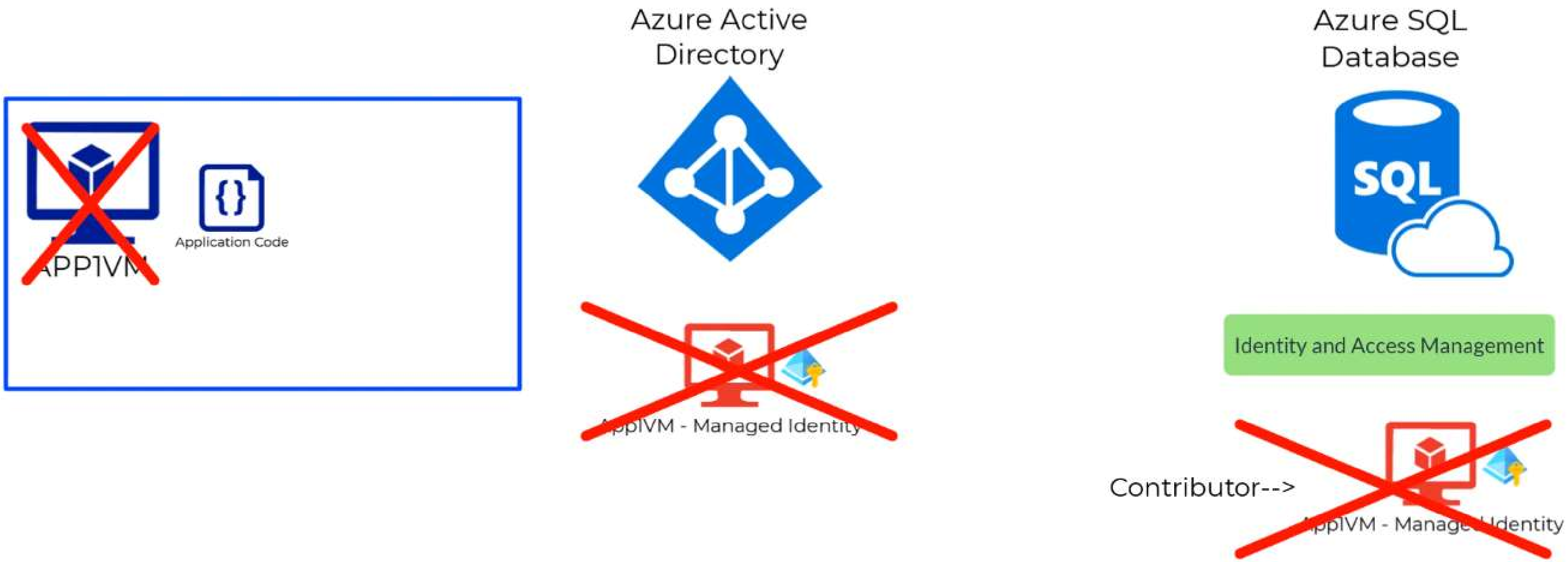
Azure Active Directory

Key Vault

Managed Identities Enabled

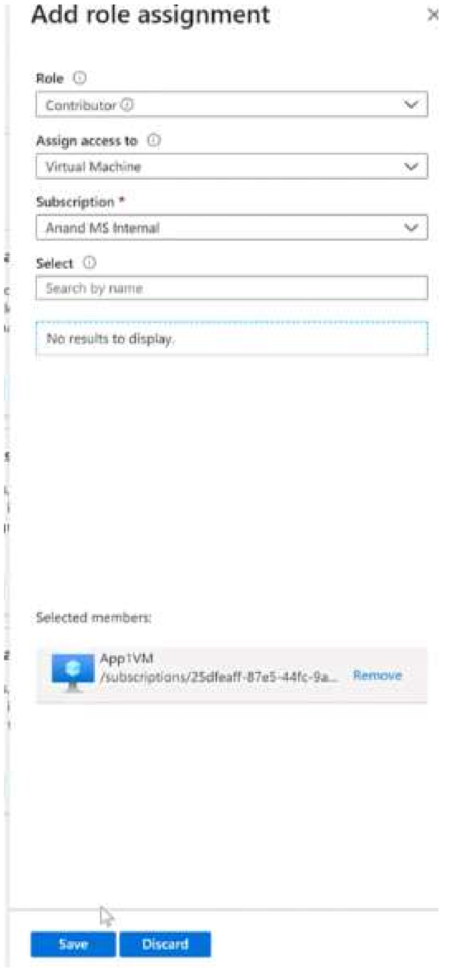


Auto Deleted if VM is Deleted


APP1VM
Application Code
Azure Active Directory
AppIVM - Managed Identity
Azure SQL Database
SQL
Identity and Access Management
Contributor-->
AppIVM - Managed Identity

Hands-On: System Assigned Managed Identity

- Step 1: Create Data Factory
  - Managed Identity for Data Factory is auto created
- Step 2: Grant Access to the Identity
  - Open Target Resource (SQL Server) which is to be access securely
  - Open IAM
  - Grant Permission to Managed Identity
  - Role: Reader
- Now data factory can access SQL Server



Add role assignment

Role: Contributor

Assign access to: Virtual Machine

Subscription *: Anand MS Internal

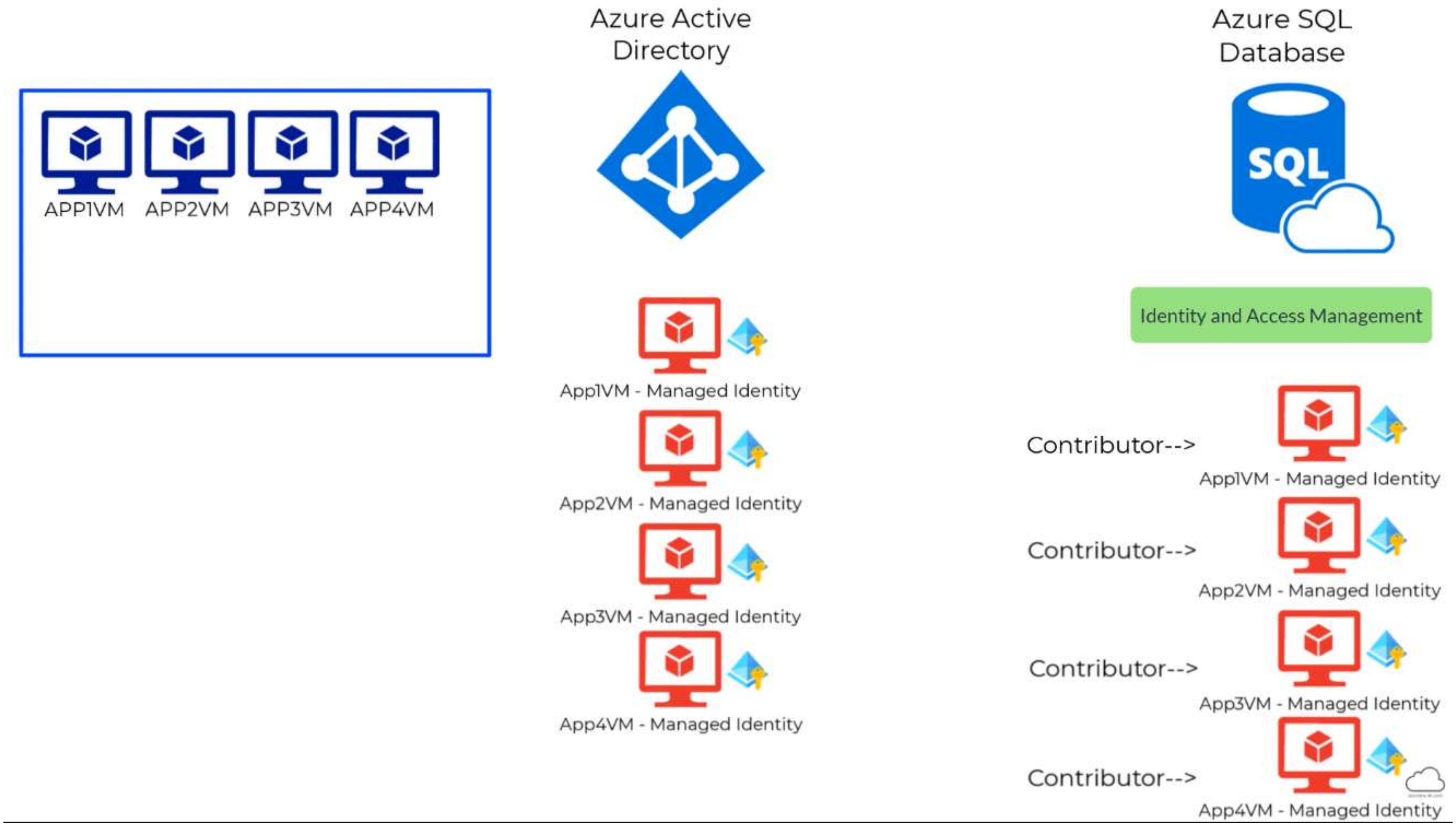
Select: Search by name

No results to display.

Selected members:

App1VM
/subscriptions/25dfeaff-87e5-44fc-9a...

Becomes unmanageable if VMs increases



APP1VM APP2VM APP3VM APP4VM

Azure Active Directory

App1VM - Managed Identity

App2VM - Managed Identity

App3VM - Managed Identity

App4VM - Managed Identity

Azure SQL Database

Identity and Access Management

Contributor--> App1VM - Managed Identity

Contributor--> App2VM - Managed Identity

Contributor--> App3VM - Managed Identity

Contributor--> App4VM - Managed Identity

Azure Key Vault Security and Best Practices

Control Access to your vault

- Lock down access to your subscription, resource group and Key Vaults (RBAC)
- Create Access policies for every vault
- Use least privilege access principal to grant access
- Turn on Firewall and VNET Service Endpoints

Use separate Key Vault

- Use a vault per application per environment

Backup

Use Logging from Monitoring Section

Turn on recovery options

- Turn on Soft Delete.
- Turn on purge protection

Thanks