greatlearning
Learning for Life

Azure API Management – Build & Deploy APIs

Agenda

- What is Azure API Management?
- Use Cases
- Two sides of API Management
    - Administrative
    - Consumer (Developer)
- Components
- Import APIs and build Mock APIs

Azure API Management

- Build an API gateway for back-end services
- Publish APIs to external developers or customers
- Allows to centrally manage, secure and monitor APIs
- Modify the requests and responses
- Define policies for throttling, token validation etc.
- Make APIs compliant before exposing it to consumers
- Build Mock APIs
- Build products that expose APIs, allowing users to subscribe

Use Cases

- Expose legacy APIs in compliance with to organization standards
- Control access to APIs, and monetize assets
- Quickly onboard clients using built-in developer portal
- Provide consistent interface to customers
- Provide insights into utilization of APIs

Two Sides of API Management

- Administrative
  - Define or import APIs
  - Define policies on request/response of APIs
  - Bundle APIs into products
  - Manage users and subscriptions
  - Monitor API usage
- Consumer (Developer)
  - Subscribe to products
  - Check API documentation
  - Test APIs using interactive console
  - Check their own analytics

Components

- APIs and Operations
- API Gateway
- Policies

- Products
- Users / Groups
- Subscriptions
- Developer Portal

Components

- APIs and Operations
  - Operation is a method that can be invoked
  - APIs are set of operations
  - Each API maps to a back-end service (which is actual implementation)
  - Operation maps to methods implemented by back-end service
- API Gateway
  - Accepts API calls and diverts them to the backends
  - Verifies the request
  - Logs incoming requests
  - Can transform requests and responses

Components

- Policies
  - Set of statements which are executed on the request/response of operation
  - Can be defined without code
  - Changes behavior of an operation

Azure API Management – Consume APIs

Agenda

- Quick Recap
- What is Developer Portal?
- Publish APIs
- Consume APIs

Two Sides of API Management

- Administrative
  - Define or import APIs
  - Define policies on request/response of APIs
  - Bundle APIs into products
  - Manage users and subscriptions
  - Monitor API usage
- Consumer (Developer)
  - Subscribe to products
  - Check API documentation
  - Test APIs using interactive console
  - Check their own analytics

Components

- APIs and Operations
- API Gateway
- Policies

- Products
- Users / Groups
- Subscriptions
- Developer Portal

Components

- Products
  - Collection of APIs
  - Offered to consumers (developers) using Developer Portal
  - Can be Open or Protected
    - Open products can be used without subscription
    - Protected products must be subscribed by developer
    - Protected products can be auto-approved or may require admin approval
- Subscriptions
  - When Developer subscribes to a Product, subscription is created
  - Developer is given subscription keys for a product, to access it

Developer Portal

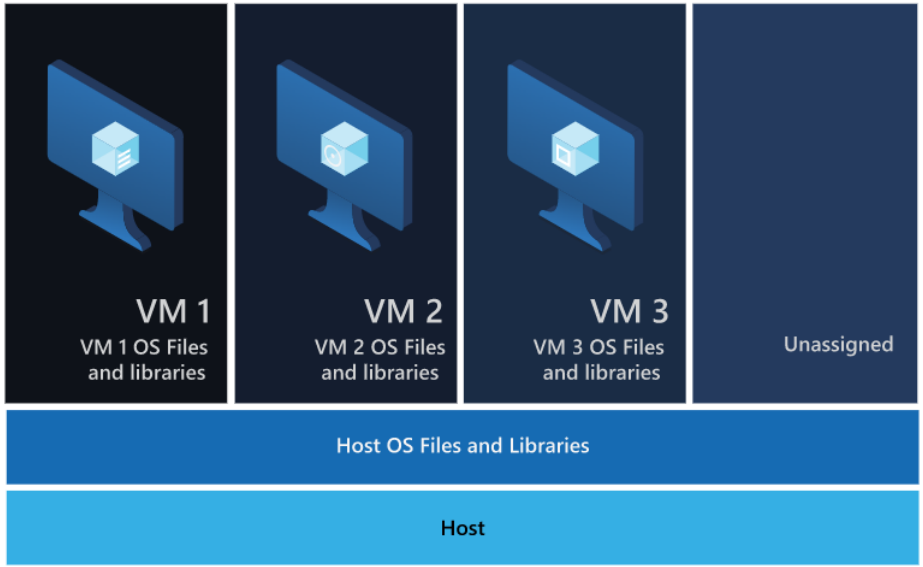
- Automatic setup as part of API Management
- User can…
  - Sign up / sign in to account
  - Subscribe to products
  - Get the keys to access the APIs
  - Interactively test APIs in Developer Portal
  - Access their own analytics

Azure Container Services

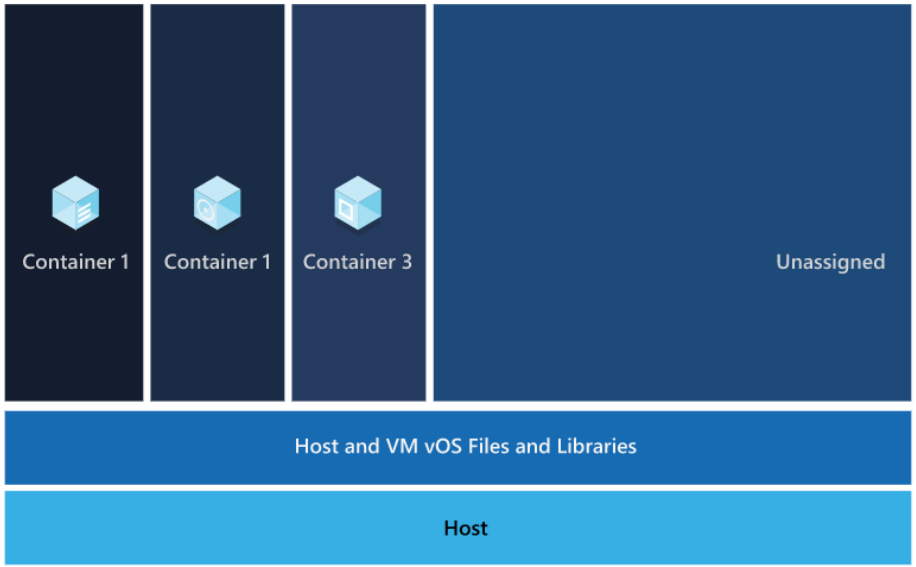
Agenda

- Quick Introduction to Containers
- Azure Container Services
- Store containers images
- Deploy containers

Virtual Machines vs Containers



Virtual Machines



Containers

Source: https://azure.microsoft.com/en-in/overview/what-is-a-container/

Containers

- A standard package of software that includes an Application's code, and all its dependencies – libraries, system files, config files, runtime etc.
- Runs application reliably from one environment to another
- Container Image
  - Packaged software with all its dependencies
- Container Registry
  - Place to store container images
- Container Instance
  - An instance of Container Image is created to run application
- Create images for Windows or Linux

Azure Container Services

- **Azure Container Registry**
  - Place to store images
- **Azure Container Instances**
  - Quick deployment of individual containers in Azure
- **Azure App Services**
  - Deploy containers on App Service Plan (Windows or Linux)
- **Azure Container Groups**
  - Deploy multiple containers on the same host
- **Azure Kubernetes Service**
  - Managed Kubernetes service in Azure
- **Azure Service Fabric**
  - Managed Service Fabric cluster on Azure

Azure Container Instances

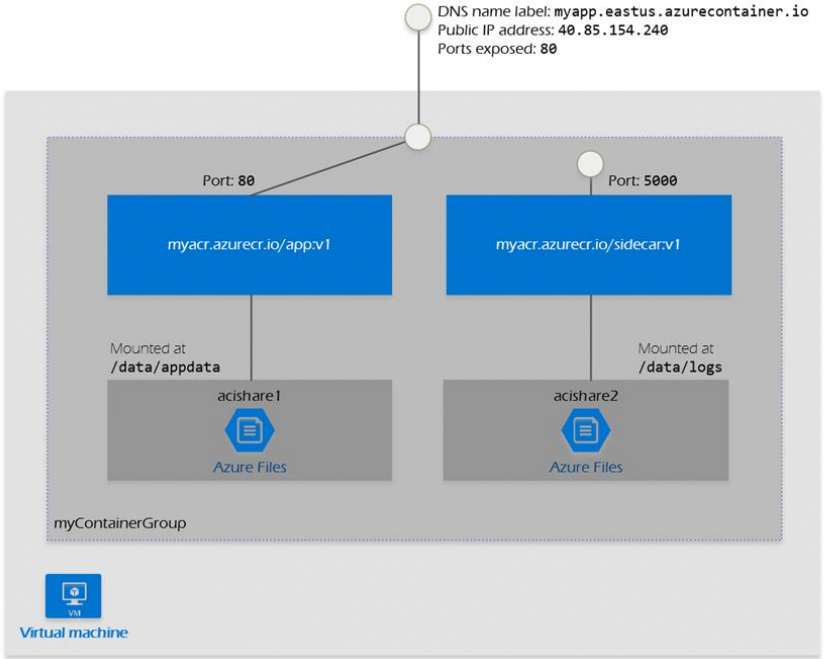
- Allows quick deployment of containers in Azure, without the need for deploying & managing any Virtual Machine
- Specify exact CPU and memory requirements for a container
- Run Windows or Linux containers
- Can run in an isolated manner anywhere in Azure datacenter
- Allows to mount Azure File Share as a storage for containers
- Billed per second

Azure App Services

- Azure PaaS offering providing dedicated infrastructure – App Service Plan
- Can deploy Windows or Linux containers

Azure Container Groups

- Collection of containers that are deployed on the same host machine
- Deploy usir



Source: https://docs.microsoft.com/en-in/azure/container-instances/container-instances-container-groups

greatlearning
Learning for Life

Azure Active Directory

Agenda

- What is Azure Active Directory?
- Feature Walkthrough

Azure Active Directory

- Allows Identity and Access management
- Create users (internal/external), groups, AAD applications etc.
- Setup custom domains
- Use Azure AD to sign in, and access resources
- Protects resources using access management
- Integrated with many enterprise services, like Microsoft 365
- Different licenses are available

Azure Active Directory - Identity

- Create users (internal/external), groups, AAD applications etc.
- Provides **Authentication** capabilities
    - Multi-factor authentication (MFA), self-service password reset (SSPR)
- Create **B2B or B2C Azure AD**
    - B2B – Handle internal users (employees) and external users
    - B2C – Allows users to create & manage accounts, sign-in to applications
- Provides **Identity Protection**
    - Setup user-risk and sign-in risk policies
- **Hybrid identity** setup – Connect on-prem AD with Azure AD

Azure Active Directory - Access

- Setup **Role-based Access Control** (RBAC)
- Setup **Conditional Access** policies
    - For e.g. – Use MFA for management or admin tasks, allow access to only certain locations, block risky sign-ins etc.
- Provides **Privileged Identity Management** (PIM)
    - Enable Just-in-Time access, set approval workflows etc.
- Perform **Access Reviews**
    - Review the granted permissions automatically, ask group owners to periodically confirm access etc.

greatlearning
Learning for Life

Azure AD Connect

Agenda

- What is Hybrid Identity?
- What is Azure AD Connect?
- Authentication Methods

Hybrid Identity

- Organization users needs access to on-premises and cloud resources
- Instead of managing two identities for a user, create a **Hybrid Identity**
- User can sign-in at one location, and access resources anywhere
- Organizations can choose authentication mechanisms, and sign-in locations

Azure AD Connect

- **Azure AD Connect** synchronize identities across on-prem AD & Azure AD
  - Utility that is installed in on-premises environment
  - Synchronize users, groups and other entities
- **Azure AD Connect Health** monitors the connection between on-premises AD and Azure AD to ensure reliability
- Supports different **authentication options**
  - Password hash synchronization
  - Pass-through authentication
  - Active Directory Federation Services (ADFS)

Azure Security Services

Agenda

- Azure Security Services Overview
- Role-based Access Control (RBAC)
- Azure Key Vault
- Service Principal
- Managed Identities

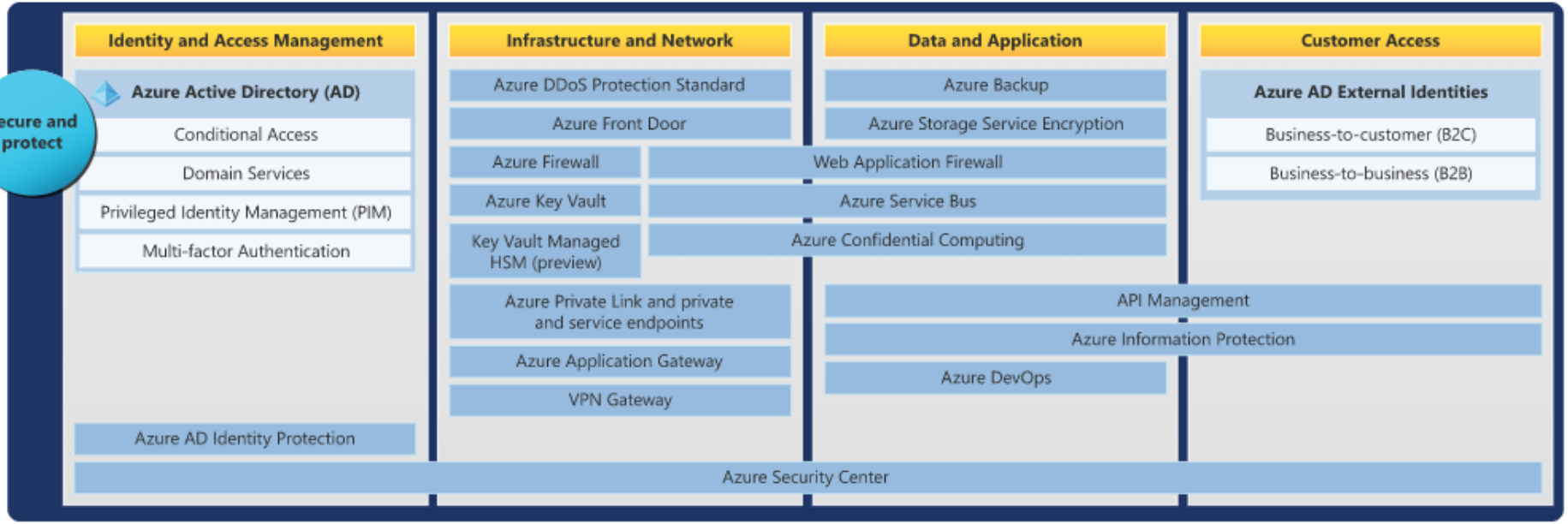
Azure Security Services

- **Role-based Access Control (RBAC)**
  - Assign access to identities using built-in or custom roles
- **Azure Active Directory**
  - Features like MFA, Conditional Access, PIM, Access Reviews etc.
- **Network Security**
  - Network Security Groups, Firewall, DDoS protection, Private Link etc.
- **Application Security**
  - Web Application Firewall (WAF)

Azure Security Services

- **Azure Security Center**
  - Cloud Security Posture Management (CSPM)
  - Cloud Workload Protection Platform (CWPP)
- **Azure Key Vault**
  - Central place to securely store secrets, keys and certificates
- **Managed Identities**
  - Provides an identity to resources

Azure Security Services



Source: https://docs.microsoft.com/en-us/azure/security/fundamentals/end-to-end

greatlearning
Learning for Life

Azure Governance Services

Agenda

- Azure Policies
- Azure Initiatives
- Azure Blueprints

Azure Governance Services

- **Azure Policy**
  - Enforce or audit rules to keep Azure resources compliant
  - Use built-in or custom policies
- **Azure Initiative**
  - Group of Azure Policies that can be applied together
- **Azure Blueprint**
  - Define a set of standards to bring consistency and compliance
  - Can include Policies, Role Assignments, Resource Groups & ARM templates