1.1. Management - Azure Cloud Shell

Azure Cloud Shell

- Browser-accessible shell for managing Azure resources
  - Can provide Bash or PowerShell
- In background it uses dockerized version of PowerShell / bash
- When you open it for the first time →
  i. It creates a new storage account called `azcloudshell` and some numbers
  ii. It then creates a file share that stores your user information.

1.2. Management - Resources & Costs.

Subscriptions

Resource tagging

- Always tag!
- Tags are additional metadata that can be assigned to resources/resource groups.
  - **!** Child resources do not inherit resource groups tags
  - **!** Max 15 tag name/value pairs.
- E.g. `CostCenter = YHZ`
- Why?
  - Organize
  - Search
  - View
  - Billing & cost managements
- On Portal
  - You can search for Tags and see filtered lists.
  - **!** Resources are tagged **after** resource is created as opposed to PowerShell/CLI.

Resource Tagging and Cost Center Spending Limits

Spending Limits

- Applies to *free trial subscriptions*, *MSDN* and *Visual Studio subscriptions*.
  - If spending limit is exceeded:
    a. Email message is sent

    b. Deployed resources are disabled in next billing cycle.
    c. Databases and storage accounts become read-only
  - Free trials can be upgraded to Pay-as-you-go
- Do not apply to *support plans*, *pay-as-you-go*, *Enterprise Dev/Test*

ARM Consumption API

- Returns usage details
- **!** Supported only in *Enterprise enrollments* and *Web Direct subscriptions*
- Available through CLI and different SDKs.
- Consumption APIs
  - Enterprise customers only: *Price Sheet*, *Budgets*, *Balance*
  - Reserved VMs: *Reservation Summaries API*, *Reservation Details API*, *Reservation recommendations API*
  - Others: *Marketplace charges*, *usage details*

Azure Pricing Calculator

- Estimates monthly costs
- See online

Azure Advisor Cost Recomendations

- Identifies wastage
- E.g. idle VMs, SQL DBs.
  - Can configure automatic shutdown
  - Auto-shutdown option in VM.
- Recommendations about:
  - High availability
  - Security
  - Performance
  - Cost recommendations, e.g.:
    - Virtual machine reserved instances to reduce costs.
    - VM resizing: Scale up / down
    - Remove unprovisioned ExpressRoute circuits.
- Configure rule:
  - E.g. Average CPU Utilization < 5%

Subscription blade

- In *Cost analysis* you can filter by *Tags*.
- Invoices
- **Manage** in Subscription blade
  - Manage payment methods
    - 💡 Adding one allows you to remove subscription limits.
  - Download usage details
  - Transfer/cancel subscription
  - Set-up billing alerts
    - E.g. e-mail if billing total is $150

Optimizing VM costs

- 📝 Use VM Reserved Instances
  - You can create one in *Reservations* blade
- 📝 Set-up auto shutdown in VMs
  - *Auto-shutdown* blade in VM.

Microsoft Azure Resource Providers

- Enables Azure features.
- Many are registered automatically
  - E.g. `Microsoft.Compute` that handles VMs, `Microsoft.Network`, `Microsoft.Sql`, `Microsoft.Storage`
- Some are not registered automatically
  - E.g. `Microsoft.PolicyInsights`, `Microsoft.AzureActiveDirectory`, `Microsoft.AzureStack`, `Microsoft.Botservice`
  - Custom providers can be registered with subscription.
    - Requires the `Contributor` or `Owner` roles.
    - In most cases providers are registered automatically when you deploy resources that uses the providers.
- You can register, unregister, re-register through Subscription → Resource providers in Portal

1.3. Management - Resource Groups

Resource groups

- Logical grouping of resources that shares the same lifecycles.
  - Resource group holds different unique resources.
  - Resource groups can contain resources that reside in different regions.
    - Location of resource group is just the meta data for the resource group.

Tags

- Categorization / organization of resource groups for e.g. billing, management
- E.g. `Dept: IT`
- ❗ Tags are not inherited
- ❗ Max 15 tag name/value pairs.

Locks

- For accidental deletion or accidental changes to resources within a resource group.
- Consists of two locks:
  - `CanNotDelete`
    - Authorized users can still read and modify a resource, but they can't delete the resource.
  - `ReadOnly`
    - Authorized users can read a resource, but they can't delete or update the resource.
    - Same as giving everyone a ***Reader*** role.
- Locks are inherited from resources within the resource group.

IAM

- Access control, RBAC
- Roles are inherited
- ***Role assignment***: Role definition role (role, e.g. Reader) + Person/Scope/Service Principal + Scope

Policies

- Azure entity that controls behaviors within a resource group
  - Allow you to keep compliant with corporate standards and SLAs.
  - Set in a ***scope*** with a ***name*** and ***definition***.

    - Scope: E.g. resource group, subscription.
    - Definition: E.g. "*Allow resource types*"
        - Name, description, Policy (e.g. `azurepolicy.rules.json`), Parameters (e.g. `azurepolicy.parameters.json`)

Events

- Create event subscriptions triggered by the resources group in Event Grid.

Automation Script

- Can be added to library to be redeployed later on.
    - ! All resources cannot be redeployed
    - 💡 Must change the name to avoid duplicates.
- ARM templates for resource groups can also be found on GitHub.
- You can *Add to library*, or click on *Deploy* to deploy directly.

Moving Resources

- You can move resources to another resource group or subscription.
- ! All resources cannot be moved.
- Ways of moving
    - Using CLI: `az resource move --destination-group new-rg --id resourceid`
    - In portal: Overview → Move

Alerts

1. **Target**: What resource and where
2. **Criteria**: What specific action
3. **Details**: Who, when, where, how
4. **Action Group**: Who to inform and how to inform them

Metrics

1. **Resource group**: Where to look at the metric
2. **Resource type**: The type of resource to look at
3. **Available metrics**: What specifics about the metrics

4. **Chart**: Graphic display of the metric

2.1. Governance - Roles

Roles

Role assignments

- Delegated resource administration
- Roles organize related resource permissions together
    - Depends on resource type
        - E.g. different for VM and storage.
- **Scope**
    - Roles are applied to a scope.
    - They're inherited in following order:
        - Management groups
        - Subscription
        - Resource groups
        - Individual resources
- Role can be assigned to:
    - Users
    - Groups
    - Service principal
        - Application
        - System Assigned Managed Identity: App Service, Function App, Virtual Machine, Virtual Machine Scale Set
        - User Assigned Managed Identity

Role types

Built-in roles

- 60+
- Common roles:
    - **Owner**: Manage resources and resource access
    - **Contributor**: Manage resources but not resource access.

- **Reader**: Read-only access
- **Storage Blob Data Reader**: Specific to storage accounts
- **SQL DB Contributor**: Manage, but not access, SQL databases
- **VM Contributor**: Manage, but not access, virtual machines.

Custom roles

- ❗ Built using only PowerShell / CLI or REST API.
  - `New-AzureRmRoleDefinitation -Role $customRole`
- Shows in same drop-down lists with built-in roles
- JSON file looks like this:

```
{
  "Name": "Network Resource Viewer",
  "IsCustom": true,
  "Description": "Allows reading Azure network resources.",
  "Actions": [ "Microsoft.Network/*/read" ],
  "NotActions": [ ],
  "AssignableScopes": [ "/subscriptions/048.." ]
}
```

Classic Administrator Roles

- The account that is used to sign up for Azure is automatically set as both the *Account Administrator* and *Service Administrator*.
  - Roles are properties that can be changed in Subscription blade
- 💡 Azure recommends using RBAC roles
- **Account Administrator** (1 per Azure account)
  - Conceptually, the billing owner of the subscription.
  - The Account Administrator has no access to the Azure portal.
- **Service Administrator** (1 per Azure subscription)
  - By default, for a new subscription, the Account Administrator is also the Service Administrator.
  - The Service Administrator has the equivalent access of a user who is assigned the Owner role at the subscription scope.
  - The Service Administrator has full access to the Azure portal.
- **Co-Administrator** (200 per subscription)
  - The Co-Administrator has the equivalent access of a user who is assigned the Owner role at the subscription scope.

2.2. Governance - Azure AD

Azure AD

Introduction to Active Directory

- Characteristics
  - AD is cloud-based and geo-distributed
    - Your tenant is distributed amongst many servers in Azure.
    - Provides high level of availability and scalability.
  - AD is multi-tenant.
    - You're running a shared platform.
    - Each tenant is segmented off on its own.
    - Provides ability to give permissions from one tenant to another for certain accounts.
  - Identity & Access
    - Can be identity/access provider for Microsoft accounts for e.g. Office 365.
    - In-house & third party developed applications can also leverage this service.
  - Integrates with local AD
  - Provides SSO
    - For third party or in-house applications.
- Global administrator = Root
- Can be managed by Azure Portal, PowerShell/CLI, Microsoft Graph and API
  - Microsoft Graph: API product trying to creating single way of interacting with all Microsoft APIs.

Role Based Access Control

- Roles defines actions that role is capable of doing.
- 🗣 Roles are assigned to users and users only.
- ! Pre-built roles only.
  - No custom roles.
  - You can create custom that are application specific and are outside of the direct administration of Azure AD
- Roles are assigned at tenant level.

- If you need separation of roles, you can create a new tenant and assign roles and permissions on that account.

Custom Domains

- You initially get `tenantname.onmicrosoft.com`
- Custom names must be fully qualified: Not a local name but an online name.
- Ownership must be verified
  - Microsoft gives text records (TXT or MX)
  - You put text record in DNS to get verified
- You can verify multiple domains
- Possible to register subdomains but you register parent domain.
- In Portal: Active Directory → Custom domain names → Add custom domain

Multiple Directories

- **Resource independence**
  - Resource in one directory does not have access to resource in other directory
  - No forests, trusts etc.
- **Administrative independencies**
  - **!** If you're global admin in one directory doesn't mean you have any access in other directory.
- Synchronization independence
  - You can synchronize to specific directory and it does not impact other directories.
- Switch directory
  - In Portal → Active Directory → Overview → Switch directory

Conditional Access

- Can be applied on users, locations, devices, applications.
- Policies allow you to have
  - One application with multiple rules
  - One rule with multiple applications
- **!** Only available in Azure AD Premium
- Condition (if something) → Control (do something)
  - Conditions
    - Users and groups
      - • Groups • User ID • Locations (IP)

        - Cloud apps
        - Device platform and state
            - • Domain Joined • Compliant • Lost or Stolen
        - Locations (IP)
        - Client apps
    - Control: Allow, Deny, MFA
        - Multi-factor authentication
        - Compliant device
        - Approved client app
        - Terms of use
        - Custom and session controls
- Manage in AD - Conditional Access
- Example policy: "Marketing app from US only"
    - Assignments
        - **Users and groups**: All users
        - **Cloud apps**: Marketing app (registered in Azure AD)
        - **Conditions**
            - **Locations**: Include any location but exclude *Contoso location*
                - **Contoso locations** is a **named location**
                    - Set US locations in portal: Active Directory → Conditional Access → Named locations
            - **Client apps**: Apply policy with access from Browser but not from mobile apps and desktop clients.
    - Access controls: Block access

Access Reviews

- Access review is created for an identified reviewer.
    - Duration can be set
    - Usually created by administrators.
    - Reviewers can approve or deny.
- Access review can be a member of programs.
    - A program groups reviews together.
- Managed in Access Reviews (separate view, not included in AD)

Administrative Units

- Container of resources

- Used for
  - Delegating administrative permissions over subsets of users
  - Applying policies to a subset of users
- Useful in organizations with independent (autonomous) divisions
- An administrative unit is a directory object that can be created and populated with resources/users.
- AD Premium feature
- E.g. a central administrator can
  - Create an administrative unit for a particular school (Business school)
  - Populate it with only the Business school users
  - Central administrator can add the Business school IT staff to a scoped role
    - Grants the IT staff of Business school administrative permissions only over the Business school administrative unit

Identity Protection

- Detection
  - Vulnerabilities
    - E.g. MFA not configured, Unmanaged cloud apps, privileged identity management (only grant identity to user for a set period of time).
  - Risk events (e.g. user sign in in from unknown detection)
    - E.g. leaked credentials on internet, anonymous IP addresses (VPNs etc.), suspicious IP addresses, impossible travel (superman event, user logs in from NY and after 5 minutes logs in from Hong Kong), Unknown locations, infected devices.
- Investigations
  - Receive notifications
  - Workflows *(when, who, what happened)*
  - Analysis: How can you apply policies to prevent future events?
- Policies
  - *User risk policy*: E.g. if user risk event is high, allow access but require password change
  - *Sign-in risk*: E.g. if sign-in risk is medium, allow access but require MFA.

Auditing and Monitoring

- Active Directory → Activity
  - Sign-in: See, filter, search log-on statuses
  - Audit logs: See, filter, search activity logs for Azure AD

- Active Directory → Users and groups
  - You can see user sign-in risks
- Active Directory → Azure AD Connect
  - Install Azure AD Connect health from here
  - Shows how health your Azure AD Connections

2.2.1. Governance - Azure AD - Entities

Azure AD Entities

Users

Types of users

- Cloud or Synced (from local AD through AD Connect)
- Member or Guest
  - Members are created within AD directory
  - Guests are invited by administrator or one of other users of Azure AD.

Common settings

- Usual attributes (e.g. department, phone number, contact, email)
- Setup password policy, expiration policy, flag users needing to reset their password

Usage Location

- Location is required if you want to assign license to a user within AD.
- Set usage location
  - In portal: Active Directory → Users → Select User → Profile → Settings
- You can then assign license
  - In Portal: Active Directory → Users → Select User → Licenses
- **User Principal Name**: Combination of a user name + domain.

Create new user

- AD → User → new User

- User name
  - Required, e.g. `test@contoso.onmicrosoft.com`
- Properties: Optional information e.g. first name, last name, job title.

External access

- You can add a user as an External User
- Good for B2B scenarios
  - AD is not required on other business side.

Self-service password reset

- Scenarios
  - Allows users to change their passwords
  - If you cannot log in somehow
  - Helps with account lockout
- Authentication methods
  - Types:
    - Text message/Phone call
    - Secondary email
    - Security questions
  - Administrator requires one or more.
- Manage in portal
  - Steps: Active Directory → Password Reset
  - Configurations
    - **Enable**
      - You can enable for all users or selected users.
      - 💡 Good to first enable for a pilot group to see how it works.
    - **Registration**
      - Require users to register when signin in
        - Prompts user to fill information for authentication methods.
      - After how long user will be prompted to confirm authentication method information
    - **Notifications**
      - Notify users on password resets
      - Notify all admins when other admins reset their password

User settings

- Enterprise applications
  - Users can consent to apps accessing company data on their behalf (yes/no)
    - Yes; users can consent to allow third party and multi-tenant applications to consent on their own behalf.
  - Users can add gallery apps to their Access Panel
    - No; as an administrator you have to manually integrate the applications through Access Panel
- App registrations
  - Users can register applications (yes/no)
    - Yes; non administrations can register applications to be used within the directory, no; only administrators can do it

Groups

- Types of groups
  - **Assigned or Dynamic**
    - **Assigned**: You assign users to groups manually
    - **Dynamic**: You select various attributes to make users member of a group
      - Dynamic query e.g. `department Equals marketing`
  - **Security or Office 365**
    - **Security groups** are for assigning permissions.
- **Owners and members**
  - **Owners**: Can add/remove users from the group.
  - **Members**: cannot manage the group, normal permissions
- **Expiration of groups**
  - Groups can automatically expire.
- You manage in "Azure Directory → Groups"
  - You can assign licenses to a group where each member will get a license.
- Good for performing bulk user updates
- **Self-service group management**
  - **Owners manage groups** instead of administrator that manage the group for the owners.
  - Users can request to join in group with providing some business justification.
  - Audits & alerts
    - Everything is logged
    - You can e.g. trigger alert on frequent activities in a group
- **Company Branding**
  - In portal: Active Directory → Users and groups → Company branding

- Allows you to customize the pages with e.g. banner, sign-in page text, user name hint

Devices

- Enables more management
- Device settings show overview in Portal
  - Intune + MDM offer much more control
- You can add work or school account to integrate

Registration types

Register Device

- Basic registration
- Bring your own device (BYOD) scenario
- For mobile devices and Windows 10
  - Enable/disable and additional management (MDM) for mobile devices like intune.
- Enterprise State Roaming
  - Users synchronizes their user settings and application settings data to the cloud.
  - Supported in Windows 10
  - Enhanced security, management and monitoring.
  - Separation of corporate and consumer data in cloud.

Join Device

- Corporate owned assets that you want to manage
- E.g. Windows 7 or Windows 10
- You get some benefits e.g. single sign on.

Hybrid Join

- You can enable automatic registration for your AD joined computers
- Join device in both local AD and Azure AD
- Grant device user access to apps that need traditional local AD (=on-prem AD) authentication.
- You get service principal for the device
- Actual management is done through Group Policy or System Center Configuration Manager.

    - They're tied in to Azure AD but not part of core AD.
- Relies on AD Connect for synchronization
    - If they're already joined to local AD, they're also registered in Azure AD automatically.
- Configuration
    - Ensure access to external Azure AD URLs.
    - Configure SCP (service connection point) internally.
    - Configure ADFS if required

Manage in Portal

- Active Directory → Devices
- Configurations
    - Users may join devices to Azure AD
    - Additional administrators on Azure AD joined devices
        - Default is none, you can select users
    - Users may register their devices with Azure AD
    - Require Multi-Factor Auth to join devices
    - Maximum number of devices per device
    - Users may sync settings and enterprise app data
        - All, selected, None
    - For more you need PowerShell.

Azure AD Device Settings/Policies

- **Control permissions**
    - Who's allowed to access join devices?
- **Control sync**
    - Enabled/disabled
- **Device management through Intune or other MDM**
- **Conditional access**
    - Whether or not device has access to resources within your organization

Applications

- Azure AD IDaaS (Identity Directory as a Service)
- Application types
    - Third party or internal

    - Pre-integrated or proxies
- Automated user provisioning through SCIM 2.0
    - Use provisioning enables synchronization of user account.
    - SCIM
        - System for cross domain identity management.
        - Defined by IETF
        - Control users, groups and their relations
    - Available on select SaaS apps
- In portal, you can assign access to applications
    - AD → Applications → Select application → Users and groups

2.2.2. Governance - Azure AD - Hybrid Identities

Hybrid Identities

- Hybrid (common) identity = Cloud + On Premises identity
- Connection is done through Azure AD connect

Four Pillars

- **Unified Development and DevOps**
    - A common approach to building applications, and full flexibility to deploy in the cloud or on-premises
- **Integrated management and security**
    - Built-in management and security solutions across full operational lifecycle from cloud to on-premises
- **Common Identity**
    - Enable end-user productivity with single sign on to cloud and on premises applications while protecting corporate data
    - **Single identity**
        - Create and manage a single identity for each user across your hybrid enterprise, keeping users, groups and devices in sync
    - **Single Sign-on**
        - Provide single sign-on access to your application including thousands of pre-integrated SaaS apps
    - **Conditional Access**
        - Protect identities by enforcing risk-based conditional access policies and multi-factor authentication for both on-premises and cloud applications

    - **Remote Access**
        - Provide secure remote access to on-premises web applications through Azure AD **Application Proxy**
    - **Self Service**
        - Self-service password reset and application access requests for directories in the datacenter an the cloud
    - **High Availability**
    - **Collaboration**
        - Enable vendors, contractors and partners to get risk-free access to in-house resources
    - **Consistency**
        - Truly consistent capabilities
- **Consistent Data Platform**
    - Seamlessly distribute data between cloud and on-premises
    - Enrich with analysis and deep learning

Azure AD Connect

- Integrate your on-premises AD or LDAP directory to the cloud
- Establish a single identity for your users to access on-premises and cloud-based resources
- Connect your users to thousands of SaaS applications published through Azure
- Manage in Azure AD Connect → Synchronization Service
- Adjust to business changes after Azure AD Connect is installed.
- Change the service accounts
- Add the **Managers** OU to be included in the synchronization

Preparing for Azure AD Connect

- Create a new user in Azure AD as Global Administrator
- Download Azure AD Connect and install it.
    - You need > Windows Server 2008

Install and configure Azure AD Connect

- Installation settings
    - **Initially**
        - Custom or Express installation
        - Installation location

- Create an express SQL or use an existing SQL instance
- Provide a service account or create a new one
  - Service account for SQL server
- Custom sync groups
  - Fill: Administrators group, operators group, browser group, password reset groups
  - AD Connect groups not domain groups!

- **Then**
  - **How users will sign-in**
    - One of them: *Password synchronization*, *Pass-through authentication*, *Federation with AD FS*
    - *Enable sign on* → Yes, No
  - **Forest and Azure credentials**
    - *Global administration username password*
    - *Select directory type (AD or LDAP)*
      - Then type *Forest name*
    - *Create new AD account* or *use existing AD account*
    - Type *domain username and password*
      - 💡 Recommended to enter Enterprise Admin credentials
  - **Select UPN for sign-in**
    - E.g. `azure-contoso.com`
    - Select user name: e.g. `userPrincipalName`, `treeName`, `unicodePwd`

- **Then**
  - **Choose what domains and OUs get synchronized to the cloud**
    - *Sync all domains* and OUs or *sync selected domains and OUs*
  - **How to uniquely identify users**
    - Identification:
      a. *Users are represented only once across all directories*.
      b. *User identities exist across multiple directories*.
        - Match using: mail attribute, specific attribute, etc.
    - Source anchor (ID)
      . *Let Azure manage the source anchor for me*
      a. *Specific attribute*: objectGUID, pager, objectSid etc.
  - **Filter users and devices by group**
    a. *Synchronize all users and devices*
    b. *Synchronize selected*
  - **Optional features**
    - Exchange hybrid deployment
    - Exchange mail public folders
    - Azure AD app and attribute filtering

        - Password synchronization
        - Password writeback
        - Group writeback
        - Device writeback
        - Directory extension attribute sync.
    - **Enable single sign on**
        - **!** Requires domain administrator account
    - **Choose staging mode or install it**
        - **Staging mode**: Synchronization won't synchronize any data to Azure AD
- **Post installation**
    - Install AzureAD PowerShell module
    - 💡 Then enable Azure AD recycle bin

Metaverse

- What'll be synced in the next synchronization
    - Connectors to and from on-premises Active Directory
    - Connectors to and from Azure Active Directory
- Controls what attributes from what objects from what location are available for synchronization

Hybrid Planning

Sign On

- **Authentication and Authorization**
    - *How do users typically login to their on-premises environment?*
    - *How will users sign-on to the cloud?*
    - *Will you be allowing workers from partner networks access to cl oud and on-premises resources?*
- **Multi Factor Authentication**
    - *Do you currently implement multi-factor authentication?*
    - *What are the key scenarios that you want to enable MFA for?*
    - *Will you use MFA to secure Microsoft Apps?*
    - *Will you use MFA to secure remote access to on-premises apps?*
- **Delegation and Administration**

- *Does your company have more than one user with elevated privilege to manage your identity system?*
- *Does your company need to delegate access to users to manage specific resources?*
- *Does each delegated user need the same access?*

Synchronization

- **Directory synchronization**
  - *Do you have a disaster recovery plan for the synchronization server?*
  - *Where will the synchronization server be located?*
    - E.g. if it's behind a firewall, you'll need to open up some ports
  - *Do you have any other directory on-premises like LDAP or an HR database?*
  - *Does your company use Microsoft Exchange?*
- **Multi Forest synchronization**
  - *Are the UPNs unique in your organization?*
    - More than one forest → You can call people same thing as other people → You won't be able to do that in single Azure AD as they need unique UPNs.
  - *Will the Azure AD Connect server be able to get to each forest?*
  - *Do you have an account with the correct permissions for all forests you want to synchronize with?*
- **Password synchronization**
  - *Do you have restrictions on storing passwords in the cloud?*
  - *Will your employees be able to reset their own passwords?*
  - *What account lockout policy does your company require?

Applications

- **Applications**
  - *Will users be accessing on-premises applications? In the cloud? Or both?*
  - *Are there plans to develop new applications that will use cloud authentications?*
    - If so, then make sure that authentication can use OAuth, certificates e.t.c.
  - *Will cloud users be accessing applications on-premises?*
  - *Will on-premises users be accessing applications in the cloud?*
- **Access Control**
  - *Does your company need to limit access to resources according to some conditions?*
  - *Does your company have any application that needs custom control access to some resources?*

    - *Does your company need to integrate access control capabilities between on-premises and cloud resources?*
    - *Does each user need the same access level?*

Domain Structure

- **Domain Name**
    - *What name will your organization use for your domain in the cloud?*
    - *Does your organization have a custom domain name?*
    - *Is your domain public and easily verifiable via DNS?*
- **Directory Structure**
    - *How many AD forests do you have?*
    - *How many Azure AD directories?*
    - *Will you filter what user accounts are synchronized with the Azure AD?*
    - *Do you have multiple Azure AD Connect servers planned?*
    - *Do you have different directory that users authenticate against?*
- **Federation**
    - *Will you use the Azure Federation or on-premises AD FS?*
        - An option is moving on-premises AD FS to Azure Federation.
    - *More federation services for identities are provided now through Azure*
    - *Does your organization use smart cards for Multi Factor Authentication*

Forest to Azure AD Topology

- **!** Restrictions
    - One to one relation between Azure AD and AD Connect
        - Multiple AD Connect cannot connect to Single azure AD
        - Azure AD Connect cannot connect to multiple Azure AD directories
    - The same user account cannot sync to multiple Azure AD directories
    - Users in one Azure AD cannot appear as contacts in another Azure AD directory
- **Single Forest to Single Azure AD**
    - *Single Forest → Single AD Connect → One Multiple AD*
    - Most common topology
    - 💡 Recommended by Microsoft
    - Expected topology when using Azure AD Connect Express installation
    - Supports multiple domains
- **Single Forest to Multiple Azure AD**
    - *Single Forest → Multiple AD Connects → One Multiple AD*

    - Useful when e.g. some users passwords cannot be written back to the cloud but another department can do it.
    - ! Azure AD Connect sync servers must be configured for mutually exclusive filtering.
    - ! Users in one Azure AD will only be able to see users from their own Azure AD instance.
    - ! A DNS domain can only be registered in a single Azure AD directory.
    - ! Some write-back features not supported with this topology
        - No group / device writeback
- **Multiple Forest to Single Azure AD**
    - *Multiple Forest → One AD Connect → One Azure AD*
    - ! Users must have only one identity across all forests
    - The user authenticates to the forest in which their identity is located.
    - All forests are accessible by Azure AD Connect
    - ! Users have only one mailbox
- **Multiple Forest to Multiple Azure AD**
    - *Multiple Forest → Multiple AD Connects → Multiple Azure ADs*
    - Useful especially if you need isolation for different forests.
    - For each instance of Azure AD, you'll need an installation of Azure AD Connect
    - Users in one Azure AD will only be able to see users from their AAD instance.

Register domain name

- ***Add Azure AD Domain Name***
    - Create directory where organization name is `contoso.local`.
    - Add domain name `azure-contoso.com` and verify through TXT DNS entry.
- ***Add UPN Suffix***
    - On-prem resources has `name@contoso.local` but you'll need `name@azure-contoso.com` to allow e.g. SSO.
    - Flow:
        a. Add `azure-contoso.com` as an alternative UPN Suffix through Active Directory Domains and Trusts
        b. Add `azure-contoso.com` to all user accounts as the preferred UPN suffix.

Single Sign On

- **Password synchronization**
    - A copy of password and usernames is synchronized to the cloud.
- **Pass through authentication**

- You don't store passwords in cloud
- User is authenticated using pass through authentication agent that connects with on-premises AD
- Works seamlessly with Azure Multi-Factor authentication

- **Seamless SSO**
  - Works with Azure AD Join or the desktop is previously joined to your AD domain
  - Requires Azure service endpoints to be added to the client browser's Intranet zone.
    - This way the browser can send the Kerberos ticket to the website.
  - Flow:
    a. Client from a joined device tries to access to a resource in cloud.
    b. Local client goes to AD DC and gets an access token.
    c. Client forwards access token to Azure AD.
       - If MFA is enabled, it'll prompt user.

Making cloud apps available

- Azure AD → Enterprise Applications
- 4 categories
  i. Gallery applications
  ii. Applications you're developing, integrated with Azure AD
  iii. On-premises applications with Azure AD Application Proxy
    - **Azure AD Application Proxy**
      - Allows Azure to reach on-premises resources.
      - Consistent access to private resources without a VPN.
      - Install App Proxy & Connector on-premises
        - **!** Cannot be installed on a server with the Pass Through Authentication connector
        - **!** You need to configure a CNAME on DNS for the particular domain work for it to work.
      - Set-up on Azure
        - Add applications
        - Assign to users
        - Configure SSO
        - Provision just like any SaaS app
      - Flow for Azure user reaching on-premises resource:
        a. Azure AD gives a token to user
        b. User sends that token to Azure App Proxy
        c. Proxy takes UPN and SPN and gives it to connector

d. Connector goes to on-prem AD and gets Kerberos ticket.
e. It forwards it to actual on-prem application, it verifies the ticket and ticket is assigned to the cloud user.

iv. Non-gallery applications

- Manage permission
  - Azure AD → Enterprise Applications → In application → Users and groups
- Configure SSO
  . Configure SSO for the new application
    - Manage permission
      - Azure AD → Enterprise Applications → In application → Single sign-on
    - Sign-on types:
      - Password-based Sign-on
      - Linked Sign-on
      - SAML
        - Provides step by step guide for federation between application and Azure AD manually

i. Click on the new application new in the Azure AD MyApps access panel
   - Access panel is reached at `myapps.microsoft.com`
   - It prompts you to install a browser extension

ii. Install Access Panel Extension

iii. Log into application so that password is stored for SSO

2.3. Governance - Azure Policies.

Microsoft Azure Policies

- Configures what kind of resources can be deployed and managed
- Ensures proper cloud governance by controlling resource deployment and usage.
  - **!** Publishing requires `Microsoft.Authorization/policyassigments/write` permission.
- The assigner is saved as `assignedBy` property.
- Apply to new and existing resources.
  - Resources are scanned hourly for compliance with policies.

Policy types

- **Built-in policies**

    - E.g.: Require SQL Server 12.0, Allowed Storage Account SKU, Allowed Resource Types, Allowed Locations, Allowed Virtual Machine SKUs, Apply tag and its default value, Enforce tag and its value, Not allowed resource types
- **Custom Policies**
    - JSON format
        - Supports logical operations (`or`, `allOf`, `noneOf`) and `if` statements.
    - Used for granular resource control
        - E.g. limit load balancer creation to IT admins.
    - Can be create manually or by copying existing policy from e.g. GitHub.
        - E.g.

```
{
  "policyRule": {
    "if": {
      "not": {
        "field": "location",
        "in": "[parameters('allowedLocations')]"
      }
    },
    "then": {
      "effect": "audit"
    },
    "parameters": {
      "allowedLocations": {
        "type": "Array",
        "metadata": {
          "description": "The list of allowed locations for resources",
          "displayName": "Allowed Locations",
          "strongType": "location"
        }
      }
    }
  }
}
```

Policy parameters

- Passed to policy
- Enable policy reuse
    - Fewer policies are required.
- String or array

Policy Effects

- **`Append`**: Resource policy additions, e.g. tags.
- **`Audit`**: Logging only, generates a warning.
- **`AuditIfNotExists`**: Enables audit if resource does not exists
- **`Deny`**: Denies deployment
  - 💡 Existing non-compliant resources are marked but not deleted.
- **`DeployIfNotExists`**: If resource does not exists, deploy it.

Management Groups

- Organizes multiple subscriptions.
- Up to 6 hierarchical levels.
- Allows to assign policy groups
  - 💡 Subscriptions inherit settings
- Facilitates RBAC
- Subscriptions can be moved to other parts of hierarchy.

Policy exclusions

- Called **exclusion scopes**
- Policies can have exclusions in different scopes
- Scopes can be e.g. resource groups in subscription, or VMs in resource groups.

Policy Initiative Defination

- Groups policies into a single unit.
- Used when a single Azure governance goal consists of multiple checks.
- Can be assigned to resources/groups/subscriptions
- E.g. Security Compliance
  i. Check for endpoint protection
  ii. Check for VM disk encryption

3. Monitoring

Monitoring

Azure Monitor

- Centralized ways of getting insights from application to infrastructure
- You can diagnose, trace and debug issues
- Uses ML to detect anomalies and reveal hidden patterns
- Track how customers interact with the application
- **Components**
  - • Alerts • Metrics • Action groups • Monitoring & reporting • Dashboard • Logs

High level view

- Collects data from
  - • Application • Operating system • Resources • Subscription • Tenant
- Populates stores
  - Metrics & logs
- Perform functions:
  - **Insights**: • Application • Container • VM • Monitoring solutions
  - **Visualize**: • Dashboards • Views • Power BI • Workbooks
  - **Analyze**: • Metrics Explorer • Log Analytics
  - **Respond**: • Alerts • Autoscale
  - **Integrate**: • Event Hubs • Logic Apps • Ingest & Export APIs

Alerts

- Notifies when important conditions are found in the monitoring data
- Flow of alerts
  - Alert Rule
    - Target Resource *(Signal)* → Criteria *(Logic Test)*
    - Action Group *(Actions to do)*
    - Monitor condition *(Alert State)*
- Alert rules have single of each properties:
  - **Target resource**
    - Scope & signals for alerting.
    - E.g. VM
  - **Signal**
    - Emitted by target resource

        - Can be metrics, activity log, application insights and log.
    - **Criteria**
        - Combination of *signal* and *logic* applied on target resources.
        - E.g. less than X CPU usage.
    - **Logic**
        - User-defined logic to verify that signal is within expected range/values.
        - E.g. less than **30%** CPU usage.
    - Alert name
    - Alert description
    - **Severity**
        - Alert once the criteria specified in the alert.
        - Can range from 0 to 4.
    - **Action**
        - Specific action taken when the alert is fired.
- You can alert on:
    - Metric values
    - Log search queries
    - Health of underlying Azure platform
    - More..
- State of alerts:
    - **New**: Created or fired
    - **Acknowledged**: Issue is reviewed.
    - **Closed**: Issue has been resolved.
        - Can be reopened by changing its state.
    - User changes state from New.

Log types

- **Diagnostic Logs**
    - Non-compute resources: Resource metrics
    - Compute resources: Guest OS (e.g. syslog for Linux, event logs for Windows)
    - Azure Monitoring Agents
        - **Azure Diagnostics Extension** (cloud only)
            - Windows Server and Linux
            - useful for basic resource-level monitoring
            - Deployed automatically to VM when you enable it.
            - Boot diagnostics (serial console)
        - **Log Analytics Agent** (hybrid solution)

        - Can collect logs from Azure & on-prem systems to same namespace.
- **Application Logs**
    - Trace event streams
    - Programmed in application itself.
    - Application Insights
        - Instrumentation tool
        - HTTP requests
        - Dependency Calls (to e.g. SQL, external services, background services)
- **Activity Logs**
    - Azure infrastructure logs
    - E.g.
        - Who created VM?
        - Who configured this VNet?
        - Traffic stream from NSG?
    - Can be sent to: Log Analytics, Event Hubs, Azure Storage

NSG (Network Security Group) Flow logging

- Flow logs handled by NSGs.
- Plot using
    - In-built Azure plotting tool **Network Watcher**
    - Power BI

Azure Cost Management

- In portal it can be eached through "Cost analysis" blade of desired scope.
- In "Cost analysis" you can filter by "Tag"s.
- Cost Management shows organizational cost and usage patterns with advanced analytics
- Reports show your internal and external costs for usage and Azure Marketplace charges
- You can automate periodically export of your costs
    - 💡 You can also see daily usage data in Portal: Azure Account Center → Billing history → Current period → Download usage
- Data is consumed by other Azure resources
- Predictive analytics are also available.

Metrics

- Collected one-minute frequency
- Uniquely identified in a namespace.
- 💡 Stored for 93 days
  - Collected in Azure metrics database (time series database)
  - 💡 Copy to Log Analytics for long term storage
- Holds value properties: Time, Type, Resource, Value, Multiple Dimensions
- Value:
  - Health of application: can help to identify route cause.
  - Valuable when combined with other metrics.
- Sources of metrics:
  - **Platform metrics**
    - Each resource provides
    - Visibility into health and performance
  - **Application metrics**
    - Generated by application insights
    - Detect performance issues & track trends
  - **Custom metrics**
    - **!** Must be created in same region as the resource that has the metrics
- Use-cases: • Metrics explorer • Metric Alert Rule • Auto Scale • Route & Stream • Archive • Access

Third party tools

- **ITSM**
  - IT as a Service
  - Helps to design, plan, deliver, operate, and control information technology (IT) services
  - **Azure ITSM Connector**
    - Bi-directional connection layer between and your ITSM tool(s)
    - Use cases:
      - Create ITSM work items based on Azure alerts.
      - Sync ITSM incident/change request data to Azure.
- **SIEM**
  - Security information and event management
  - E.g. Splunk (there's an open source add-on to send to Event Hubs)
    - 💡 You could even use Azure Sentinel as a SIEM tool.

Action groups

- **Name**: Unique identifier
- **Action type**
  - Voice call or SMS
    - ! Up to 10 SMS / voice call actions in an action group.
    - ! No more than 1 SMS / Voice call every 5 minutes.
  - Webhook
    - ! Up to 10 webhook call actions in an action group.
    - It'll retry 2 times: first after 10, then 100 seconds.
  - Logic App
    - ! Up to 10 logic app actions in an action group.
  - Automation runbook
    - ! Up to 10 Runbook actions in an action group.
  - Azure Function
  - ITSM
    - ! Up to 10 ITSM actions in an action group.
  - Email
    - ! Up to 1000 e-mail actions in an action group.
    - ! No more than 100 emails in an hour.
  - Push notification
    - Azure App Push
    - ! Up to 10 Azure app actions in an action group.
- **Details**: corresponding phone number, email address, webhooks URI, or ITSM connection details.

Monitoring and reporting on spend

- Two ways to understand Azure bill to compare usage and costs (invoice):
  i. Using usage file
     - Detailed usage CSV file shows charges & daily usage in billing period
       - Download:
         a. Sign into the Azure account Center as the Account Administrator
         b. Select the subscription for which you want the invoice and usage information
         c. Select billing history → Download usage
       - Select billing history

  ii. Using Azure portal
     - Subscription → Cost analysis → Filter by Timespan
- See estimated costs on Portal: Subscription → Usage and estimated costs

Log Analytics

- Old: OMS, new: Embedded in Azure Monitor as Logs.
- It's a dataware house for telemetry
    - It converts any schema to a table schema that allows you to query.
        - Uses KQL (pipe-based) language to query.
- All monitoring roads lead t o Azure Log Analytics
    - There's always an integration from an logging Azure component to Log Analytics.
- You can download agents in Workspace → Connect
    - Agents do not require VPN
    - **System Center Operations Manager**
        - Can send data to Log Analytics from cloud/on-prem servers.
- **Azure Data Explorer**
    - Query language is used & viewed
- **Alert rule**
    - Based on each query that run on regular intervals, results are evaluated to trigger an alert.
    - **Target**
        - Specific Aure resource
    - **Criteria**
        - Specific logic to trigger an action
        - **Log Alerts**
            - Describes where signal is custom query based on Log Analytics
    - **Action**
        - Call to send a notification
    - Set-up in Log Analytics → Alerts
- **Export**
    - • Excel • PowerBI
- Application Insights data is used in a different partition in Log Analytics.
    - E.g. requests, traces, usages
    - Allows you to cross application queries
- **Function**
    - Queries can be saved as functions to be used within another query.
- Requires log analytics workspace

Create performance baselines

- Baseline
    - Configuration management term

    - Signifies an agreed-upon description of product attributes, per unit time, which serves as a basis for defining change.
    - 💡 It's not only recommended but mandatory for team to develop a baseline.
        - Gather diagnostics for long enough time.
            - Capture all peaks and values over ordinary usage.
            - Enable streams and create baseline
        - Even analyze those and agree upon which performance ranges are acceptable to define SLAs.
        - Helps to isolate problem
- Baselining in Azure
    i. Continuous monitoring
    ii. Normal operational parameters
    iii. Alerts on deviations
    iv. Take proactive corrective actions
- Baselines actions
    - ***Enable diagnostics monitoring and telemetry***, e.g.:
        - Azure IaaS resources
        - Azure App Service apps
    - ***Creating performance baselines***
        - Analyze diagnostics output
        - Plot metrics

4.1. Storage - Azure Storage

Storage

Storage services

- Storage account is top-level account for following services:
    - Blob Storage
    - File Storage
    - Table Storage
    - Queue Storage

Blob Storage

- Object and disk storage

- Blob storage tiers
- Azure Search integration
- Blob Lease for exclusive write access
    - Pass in lease id to API to modify
    - E.g. IaaS VMs lease Page Blob disks to ensure its managed by single VM
- You can create snapshots on blob level and view snapshots.

Azure Data Lake Storage

- Uses blob storage to store data
- Big data analytics
- Analytics interface and APIs
- Blob storage APIs
- Hadoop compatible access to data
- **!** GPv2 Storage accounts only

Blob Types

- **Block Blob**
    - Composed of 100 MB blocks
    - Optimized for efficient upload
    - Insert, replace, delete, blocks
    - **!** Up to 4.77TB max file size
    - **!** 50.000 max blobs
- **Append blob**
    - Can only append blocks
    - Ideal for log and audit files
    - **!** 195GB max file size
- **Page Blob**
    - Optimized for frequent read/write operations
    - Good for VM disks and databases
        - Foundation for IaaS disks
        - Stores VHD files.
        - Underlying storage for Azure SQL
    - **!** Standard (HDD) / Premium (SSD) storage
    - **!** 8 TB max file size
    - **!** Only offered in General Purpose account types

Blob Storage Access Tiers

- Set on blob level.
- Three tiers:
  i. **Hot Tier**: Frequent reads
     - Lower data access costs
     - Higher data storage costs
  ii. **Cool Tier**: Accessed less frequently
     - Higher data access costs
     - Lower data storage costs
     - Optimized for data that's stored 30 days
  iii. **Archive Tier**: Take hours to get data available
     - Highest data access cost
     - Lowest data storage cost
     - Optimized for data that's stored 180 days
     - **!** Only supported for Block Blobs
- Changing storage tiers incurs charges
- **!** Can't change the Storage Tier of a Blob that has snapshots
- **Azure Blob Storage Lifecycle Management Policies**
  - E.g. configure a policy to move a blob directly to the archive storage tier X days after it's uploaded
  - In portal: Storage Account → Blob Service → Lifecycle Management
  - Executed daily

WORM: Write Once Read Many

- Cannot be erased or modify for certain period of time.
- Set on container level
- Enable in portal
  - Access Policy → Add Policy → Time-based retention *(set retention period)* / Legal hold *(attach tags)* → Lock policy

Soft Delete

- Saves deleted for a specified period of time
- In portal: Storage Account → Blob Services → Soft Delete

Static Website Hosting

- When activated it creates `$web` container.
- You need to have default document and error page.
- You can integrate Azure CDN
    - **Azure Content Delivery Network (CDN)**
        - Distributed network of cache servers
        - Provide data to user from closest source
        - Offload traffic from origin servers to CDN
            - Typically static data
        - Pricing tiers are Microsoft, Akami, Verizon (Microsoft partners)
        - Supports • HTTPS • large file download optimization• file compression • geo-filtering
        - Azure CDN Core Analytics is collected and can be exported to blob storage, event hubs, Log Analytics.
    - Azure Storage blob becomes***origin server***.
    - Azure CDN servers become **edge servers**
    - CDN can authenticate to Blob Storage with SAS tokens to be able to read private data.
    - **Caching rules**
        - On blobs you can set CDN caching rules, such as `CacheControl:max-age=86400` in blob properties.
    - Two alternatives to set up:
        a. Create CDN and configure against blob service.
        b. Storage account → Blob service → CDN
- You can have custom domain
- You can have CORS policies

Azure Search

- Integrates with Blob Storage
- You can provide metadata in blobs, they'll be used as fields in search index which helps categorize documents and aid with features like faceted search.
    - You can choose index content, content+metadata or just metadata.
- Searchable blobs can be • PDF • DOC/DOCs • XLS/XLSX • PPT/PPTx • MSG • HTML • XML • ZIP • EML • RTF • TXT • CSV • JSON
- Structure
    - Index, Fields, Documents
- Data Load
    - Push data in yourself

    - Pull data from Azure sources (SQL, Cosmos DB or blob storage)
- Data Access
    - REST API, Simple Query, Lucene, .NET SDK
- Features:
    - **Fuzzy search** handles misspelled words.
    - **Suggestions** from partial input.
    - **Facets** for categories.
    - **Highlighting** search tags for the results.
    - **Tune and rank** search results
    - **Paging**
    - **Geo-spatial search** if index data has latitude and longitude, user can get related data based on proximity
    - **Synonyms**
- Lexical analysis done by **Analyzers**
- You can combine following cognitive skills in pipelines: OCR, language detection, key phrase extraction, NER, sentiment analysis, merger/split/image analysis/shaper.

File Storage

- SMB File Shares
- Attach to Virtual Machines as file shares
- Integrates with Azure File Sync
    - On-prem to Azure sync with caching strategy

Table Storage

- NoSQL Data Store
- Scheme-less design
- Azure Cosmos DB

Queue Storage

- Message based
- For building synchronous applications
- URL format: e.g. `http://storageaccount.blob.core.windows.net`

Account Types

Blob Storage Account

- Supported services: Blob storage
- Supported blob types: Block blobs, append blobs
- Supports blob storage access tiers (hot, cool, archive)

General Purpose V1

- *Supported services*: Blob storage
- ! Does not support blob storage access tiers (hot, cool, archive)
- ! Classic deployment & ARM
- ! Does not support ZRS (Zone Redundant Storage) replication
- Slightly cheaper storage transaction costs, can be converted to V2.

General Purpose V2

- Supports all latest features.
  - Including anything in General Purpose V1 and blob storage access tiers.
- 💡 Recommended choice when creating storage account.
- Lower storage costs than V1
- ! Has a changing soft limit (as of now 500 TB)
  - You can contact Azure support and request higher limits (as of now 5 PB). Same for ingress/egress limits to.

Account Replication

- Impacts SLA
- **Locally Redundant Storage (LRS)**
  - Three copies of data in single data center.
  - Data is spread across multiple hardware racks.
- **Zone Redundant Storage (ZRS)**
  - Three copies of data in different availability zones in same region.
  - ! Only available for GPv2 storage accounts
- **Geo-redundant Storage (GRS)**
  - Three copies of data in two different data centers in two different regions.
  - ! You don't get to choose second region, they're paired regions decided by Microsoft.
  - ! Replication involves a delay.

        - RPO (recovery point objective) is typically lower than 15 minutes.
- **Read-access Geo-redundant Storage (RA-GRS)**
    - Same as GRS, but you get read-only access to data in secondary region.

Azure Storage Explorer

- Cross-platform client application to administer/view storage and Cosmos DB accounts.
    - Can be downloaded with Storage Account → Open in Explorer in Portal.
    - Available in Azure portal as well (preview & simpler)
- Can manage accounts across multiple subscriptions
- Allows you to
    - Run storage emulator in local environment.
    - Manage SAS, CORS, access levels, meta data, files in File Share, stored procedures in Cosmos DB
    - Manage soft delete:
        - Enables recycle bin (retention period) for deleted items.
- Connecting and authentication
    - Admin access with account log-in
    - Limited access with account level SAS

Pricing

- Data storage cost (capacity)
- Data operations
- Outbound data transfer (bandwidth)
- Geo-replication data transfer

Import and export data to Azure

- You can use portal, PowerShell, REST API, Azure CLI, or .NET Storage SDKs.
- You can upload files/folders using Azure Storage Explorer.
- You can use physical drives
    - **!** 64 bit only operating systems: Windows 8+ and Windows Server 2008+
    - Preparing the drive
        - **!** NSTF only.
        - **!** Drives must be encrypted using BitLocker
    - **WAImportExportTool**
        - Azure Import/Export tool

- V1: Blob Storage, Export Jobs, V2: GP v1, GP v2
- Allows you to copy from on-prem.

AzCopy

- You can use **AzCopy** command-line utility tool.
- No limit to # of files in batch
- Pattern filters to select files
- Can continue batch after connection interruption
  - Uses internal journal file to handle it
- Copy newer/older source files.
- Throttle # of concurrent connections
- Modify file name and metadata during upload.
- Generate log file
- Authenticate with storage account key or SAS.

Importing data

- Create import job
  i. Create storage account
  ii. Prepare the drives
    - Connect disk drives to the Windows system via SATA connectors
    - Create a single NTFS volume on each drive
    - Prepare data using `WAImportExportTool`
      - Modify `dataset.csv` to include files/folders
      - Modify `driveset.csv` to include disks & encryption settings
      - Copy access key from storage account

  iii. In Azure → Create import/export job → Import into Azure → Select container RG → Upload JRN (journal) file created from *WAImportExportTool* → Choose import destination to the storage account → Fill return shipping info
  iv. Ship the drives to the Azure data center & update status with tracking number
- Costs
  - Charged: fixed price per device, return shipping costs
  - Free: for the data transfer in Azure
- **!** No SLAs on shipping
  - Estimated: 7-10 days after arrival

Exporting data

1. In portal: Azure → Create Import/Export Job → Choose Export from Azure
2. Select storage account and optionally containers
3. Type shipping info
4. Ship blank drives to Azure
5. Azure encrypts & copies files
    - Provides recovery key for encrypted drive.

Azure Data Box

- Microsoft ships Data Box storage device
    - Each storage device has a maximum usable storage capacity of 80 TB.
- It lets you send terabytes of data into Azure in a quick, inexpensive, and reliable way

4.1.1. Storage - Azure Storage - Security

Azure Storage Account Security

Management vs Data Plane

- Handled with RBAC in Azure AD
    - Can see storage keys: Owner, Contributor & Storage Account,Virtual Machine Contributor, Storage Account Key Operator Service
        - Reader cannot see storage keys

Management Plane

- Administrative tasks e.g.
    - Viewing properties of storage account.
    - Deleting storage account.
    - Assigning roles to other users.
    - Modifying the configuration.

Data Plane

- Requires access to storage account keys.
- On blobs you can set access level to public access.

*Storage Account Keys***

- Provides full access to the storage
- 💡 Best practice: Give all admins and apps same key.
  - Enables you to:
    - Regenerate secondary key.
    - Update apps to use secondary key
    - Regenerate primary key
- Can be managed by Azure Key Vault using Powershell
  - Storage account keys are stored as Key vault secrets.
  - Azure Key Vault syncs keys with storage Account
  - Storage account keys never returned to caller.

Shared Access Signatures (SAS tokens)

- 💡 Better as it follows principle of the least privilege.
- Contains permissions and start & end validity period.
  - Set read and/or write permissions.
  - Grant permissions to access only partition + row key ranges.
  - You can restrict access to IP Address(es)
  - Enforce HTTPS
- Two types:
  - ***Service Level SAS***: Only to a single blob/file/table or queue storage.
  - ***Account Level SAS***: Applies to multiple services
- ❗ It's generated by client and is not tracked by Microsoft.
  - Signature is signed with account key and ensures none of the parameters are tempered.
  - To invalidate, you'll need to regenerate storage account key used to sign SAS.
  - 💡 Better way: **Storage Access Policies**
    - Defined on container level.

        - In portal: Containers → Right click on container → Access policy
    - Permissions + validity period is on server side.
    - Service level SAS only.
    - Easy to revoke by deleting the policy or changing its validity period.

- Example url:

URL part	Description
`https://myacount.blob.core.windows.net/container1/file1.pdf`	URL to endpoint
`?sv=2017-07-29`	Rest API version
`&st=2018-04-30T19%3A19%3A19Z`	Validity start time
`&se=2018-05-01T19%3A19%#A19Z`	Validity end time
`&sr=b`	Type of resource
`&sp=r`	Permissions
`&sip=168.1.5.60-168.1.5.70`	IP Address / range *(optional)*
`&spr=https`	Protocol *(optional)*
`&sig=pk9oGEPqYyu0K4Gutfreq9n0CJqgnjYgkEwcIEL8I0%3D`	Signature

Azure AD authentication with RBAC

- Available for Blob and Queue services.
- Azure AD provides OAuth 2.0 token
- E.g. *Storage Blob Data Contributor*, *Storage Blob Data Reader*, *Storage Queue Data Contributor*, *Storage Queue Data Reader*
- Subscription level (for all Storage Accounts), Resource group level, Storage level or Blob container/queue level.
- For users, groups, applications, managed service identities.
- You register your application in AD (App Registrations)

    - You can then assign roles to your application.
    - Roles can also be assigned to **Managed Service Identity (MSI)**
        - Can set up with Azure VMs, Function Apps, VM Scale Sets
        - Credentials are injected into service instance (e.g. client id and certificate)
        - Code calls local MSI endpoint to authenticate to the resource (e.g. storage)
- Easier management, no need to handle SAS tokens or manage keys.

Encrypt data in transit

- Enforced by enabling **Secure Transfer**
    - Requires HTTPS for REST API
    - Requires SMB 3.0 for Azure file service
- When moving data e.g. between
    - Azure regions
    - On-prem to Azure storage
        - You can use Site-to-Site VPN, Point-to-Site VPN or Azure ExpressRoute.
- The data is moved across internet.
- 💡 Vulnerable to Azure, good to encrypt data.
    - Configuration from outside Storage Account always requires SMB 3.0
    - SMB 2.1 does not have encryption so it's only allowed between different Azure regions.
    - *Secure transfer required* option is disabled by default.
- SAS tokens can specify only HTTPS can be used.
- You can also use **client side encryption**
    - Encrypt data within the application.
    - Double encrypted as Azure storage encrypts data as default.
    - Still good idea to enforce HTTPS
        - HTTPS has built-in integrity checks to avoid network data loss
    - There are SDKS for e.g. C#, JAVA.
    - Can leverage Azure Key vault to generate and/or store keys.

Encrypt data in rest

- Every storage account has encryption enabled by default and cannot be disabled.
- Required for many compliances e.g. privacy.

Storage Service Encryption (SSE)

- Encrypts data before it's written
- Decrypts data before it's read
- Allows you to get encryption without any code
- Applies to Standard and Premium.
- Uses 256 bit AES.
- Keys are managed by Microsoft by default.
- Allows you to use your own encryption keys.
    - ! Blobs and files only.
    - ! Can only enable after the account is created.
    - ! Key vault and storage account must be in same region
        - Can be in different subscriptions

Azure Disk Encryption

- Encrypts data disks (VHD) of VMs.
- Handles both managed & unmanaged disks.
- Windows VMs: BitLocker encryption
- Linux VMs: DM-crypt
- Integrates with Key Vault to manage keys.
    - ! Key Vault must reside in same region and subscription
    - When uploading encrypted VM, you can upload encryption keys to Azure Key Vault first.
        - Good for migrating as you can use same keys as on-premises.

Configure network

- By default, storage accounts are accessible by all networks including internet
- Allows you to create trust boundaries
- Setting up networking/firewall rule
    - ! Denies all traffic by default unless any connection are explicitly opened
- In portal: Settings → Firewalls and Virtual Networks →Select Network
- You can have VNets from the same region as storage account or in a paired region.
- **Firewall** allows you to choose IP addresses that can access VMs
    - E.g. you can set up only ExpressRoute access.
- When you configure Azure Storage firewalls and virtual networks

4.1.2. Storage - Azure Storage - Monitoring

Monitoring

Activity Log Monitoring

- Management logs:
  - Role assignments
  - Regenerating Storage Account keys
  - Changing Storage Account settings
- Not data plane logs e.g. new blob added, they're diagnostic logs

Activitiy Log Events

- Types include: • Administrative events • Service health events • Autoscale events • Recommendations • Security alerts • Alerts
- **!** Stored for 19 days
- Archival possible
  - To Storage Account
  - To Event Hub

Storage Analytics

- Type of diagnostic logs
  - Enabled in Diagnostic settings
- **!** Retention period up to 365 days.
- Contains
  - Details of read, write, and delete operations
  - Reasons for failed requests
- Issues can be found through monitoring or reported by users
- Data includes: • Type of Operation • Success or Failure • Object Key • HTTP Status Code • Start Time • Server and E2E Latency • Authentication Type • IP Address of Caller • Browser Information • Type of Client • Client Operation ID • Server Operation ID
- Write blobs to blocks immediately
  - **!** Can take an hour until available as flush is waited.
  - Search +/- 15 minutes and based on log metadata
- **!** 20 TB limit, independent of Storage Account total limit.

- You can download **Microsoft Message Analyzer** and analyze logs in a good UI instead of text files.

Storage Analytics Metrics

- Enabled as default
- Integrates with Azure monitor
  - **!** Data is stored 30 days.
- Setting up alerts
- Sends
  - **Capacity metrics**
    - For both storage accounts and individual storage services
    - Sent to Azure monitor every hour
    - Values are refreshed daily
  - **Transaction metrics**
    - Successful, failed, errors
    - Ingress/Egress of data
    - Service availability
  - **Performance metrics**: Server latency, E2E (end-to-end) latency
- Metric dimensions: Response type, API calls, authentication type, geotype

Monitoring costs

- **Estimating costs**
  - Azure Pricing Calculator
  - Azure Total Cost of Ownership (TCO) Calculator
    - Calculate the cost savings by migrating from on-premises to Azure
- **End of month bills**
  - Invoice, detailed usage CSV file

Azure Cost Management

- Detailed cost analysis
  - Consumption, cost, performance
  - In portal
    - Open scope (e.g. subscription or resource) → Click on code analysis blade
    - Or go to "Cost Management" → "Cost analysis" and change scope on top
- Resource optimizations
  - Identify underutilized resources

- Budgets, alerts, action groups
  - Compare costs against budget
- Cross-cloud
  - Manage Azure, Amazon and Google cloud resources in one tool.
- In portal can be found
- Replaces **Cloudyn** that was a third party cost management service which was acquired by Microsoft in 2017 and integrated in Azure Cost Management, Cloudyn is deprecated since 2020 but existing users can still user.

Monitoring costs using portal

- In Subscription → Cost Analysis
  - Filter, view consumptions per resource/tags etc.
- Subscription → Invoices
  - Shows invoices
  - **!** It does not show individual resources.
    - To see them go to: Subscription → Manage and download invoices

Monitoring costs using Azure Billing APIs

- **Non-enterprise customers**
  - Azure Resource RateCard API
    - Pricelist across different regions/currencies
  - Azure Resource Usage API
- **Enterprise customers**
  - Balance and Summary API
  - Usage Details API
  - Marketplace Store Charge API
  - Price Sheet API
  - Billing Periods API

4.2. Storage - Azure Files

Azure Files

- 99.9% SLA with availability, redundancy and disaster recovery.
- Typical use cases:
  - Lift and shift

    - Hybrid solutions
    - Born-in-cloud applications that require shared storage are
    - Storage for cross-platform solutions
    - Any workload that currently uses a file server or NAS providing SMB access
- REST compatible
- **SMB**-compatible
    - File protocol over port 445
    - Can be mounted by Linux & windows & macOS compatible
    - Versions
        - **SMB 1**: Limited block sizes, chatty protocol
        - **SMB 2.1** *(Supported by Azure)*
            - No encryption
            - Better network performance than SMB 1.0
            - Group file shares, software shares
            - Supported >Windows 7, > Windows Server 2008
        - **SMB 3** *(Supported by Azure)*
            - Active-active support: Clustering with nodes
            - Transparent failover
            - RDMA support, multi channel > Lower latency
            - Enables usage of SQL and Hyper-V
            - Encryption support
            - Supported > Windows 8, > Windows Server 2012
    - Talks through port 445 and outbound connection
- **Create Azure File Share**
    - Multiple Azure File shares can be created under a storage account
    - Each has a name and optional quota assigned
        - Quota limits the size up to 5120 GB
    - In portal: Storage → Files → File Share
- **File access**
    - Access is via standard SMB client
    - Dialect of SMB is negotiated between the client and Azure Files upon connection
    - Encryption used if outside the Azure region or if required as part of the storage account configuration
    - SMB access utilizes the storage account name *(as user name)* and access key *(as password)*.
    - REST access can utilize SAS tokens

Azure File Snapshots

- Delta snapshot of a file share
- Read-only, you can download your snapshot or mount it.
- Azure Backup can schedule and manage snapshots
- ! 200 snapshots per file share
- If the file share is deleted all snapshots are also deleted

Replication options

- DFS-R (before it was File Replication Service)
- `xcopy`, `robocopy`
- Considerations: locking of files, data consistency, amount of data replicated and maintaining ACLs.

Azure File Sync

- Enables replication from a single Azure Files share to one or more Windows based file servers
  - Windows service are in a synchronization group.
- Utilizes an agent deployed on each Windows Server instance that's then registered with the Storage Sync service then added to a sync group.

Cloud tiering

- Least used data is moved to the cloud
  - Leaves a thumbprint on the server providing transparent access
  - Data is pulled down when access is requested.
- Tiering is based on maintaining a certain percentage of free space.
  - Ensures around 20% is always free in file server.
- Can be disabled
- Is scoped to a file sync namespace.
- ! File must be higher than 64 KB

Quality of Service (QoS)

- Default configuration: Server will consume maximum possible bandwidth for data transfer via the storage sync service.
- Supports network limits to be configured
- For a VM based file server, QoS of the hypervisor can be used.

Considerations

- Avoid actions that'd cause data to be pulled down from the cloud
  - E.g. anti-virus scans, backups on-premises
- ACL (Access Control Lists) are replicated to the cloud but are not enforced when accessed via Azure Files.
  - 🥊 Content should be restored to an IaaS VM file server to enable ACL enforcement.
- Data can be pre-seeded via **Azure Databox** with some caveats
  - Enables pre-seeding instead of full copy over the network.
- Be careful when combining other data replication technologies.

Workflow for replication

1. Deploy a storage account
2. Deploy a **Azure File Share**
3. Deploy **Storage Sync service**
   - Must be in same region as storage account
4. Create a **sync group**
   - Sync group has:
     - Storage account & file share
     - Server endpoints
     - Cloud endpoints
5. Register server
   i. On portal: Sync Service → Registered Service → Download **Azure File Sync Agent**
   ii. Install the service and register the server
6. Add file share into the **sync group** as server endpoint
   - 🥊 You can have only 1 cloud endpoint for the same sync group
   - You can enable/disable cloud tiering
7. Install agent on file server
   - Supported >Windows Server 2012
   - Selected files can be skipped
8. Register server to the *storage sync service* as server endpoint

Scale and Limits

- **15** storage sync services per subscription
- **30** sync groups per storage service
- **1** cloud endpoint and **50** server endpoints per sync group

- **4** TB maximum space
- **100** GB maximum file size
- **64** KB minimum file size to be tiered

Troubleshooting

- Check if TCP 445 is open for outbound traffic.
- In metrics you can monitor for problems.
- On portal
  - In Sync Services → Sync Groups → Group → See health status and action recommendations for problems for cloud and server endpoints
- In Event Viewer you can check FileSync events

4.3. Storage - Azure Backup

Azure Backup

- Backs up to **Recovery Services Vault**
- Online storage entity in Azure used to hold data such as backup copies, recovery points and backup policies.
- Storage account is automatically created an configured
  - Comes with LRS and GRS storage account
    - Configure in Vault → Backup Infrastructure → Backup Configuration
- All backups are listed and globally controlled in *Backup Jobs*
  - You can monitor status and get reports
  - You can filter the jobs
- **Backup policy**
  - Settings
    - Policy type
      - Azure VM
      - Azure File Share
      - SQL Server in Azure VM
    - Backup frequency
    - Retention range: daily, weekly, monthly, yearly
- You can set inbuilt RBAC roles to vault
  - **Backup Operator**
    - Manage backups but cannot remove backup, create vault, give any roles.
  - Others e.g. • Backup Reader • Monitoring Reader

- **Backup Alerts**
  - Vault → Backup Alerts → Configure notifications → Enable e-mail notifications → Choose severities (critical, warning, information) → Select notification (per alert or hourly digest)
- **Enable MFA**
  - Properties → Security settings → Enable
  - **!** Cannot be disabled when enabled once.
- You generate **Security PIN** for critical options and Azure Backup will prompt for the pin (Properties → Security settings)
- When ***creating a VM back-up*** you can enable back-ups and choose a vault and policy.
  - **!** VM must be in same location as recovery vault
- To delete a vault, ensure all backups are stopped, delete backup agents/servers
- **Azure Backup Reports**
  - On portal: Vault → Backup Reports → Diagnostic Settings → Turn on diagnostics
  - You can save reports in you can archive reports in *storage accounts*, *stream to event hubs*, *send to Log Analytics*
  - After you configure a storage account for reports by using a Recovery Services vault, you can connect Azure Backup from Power BI and get a dashboard.

Benefits

- Automatic storage management
- Unlimited scaling
- Application-consistent backup
  - Each and every recovery point it has information for what it needs to go back to recovery point
- Data encryption both in-rest and and in-transit
- Unlimited data transfer
- Long-term retention without any time limit

Pricing

- Pay as you go storage model
- You pay per **Protected Instance**
  - Protected instance is an application server/workload or computer that's been configured to back up to Microsoft Azure

Components

Microsoft Azure IaaS VM Backup

- Features
  - **Policy-driven backup and retention**
    - Scheduled and on-demand backups, multiple recovery points
    - You can hwoever use to backup directly with *Backup Now*
  - **Application-consistent backup**
    - No impact on production environment and no shutdown of VMs
  - **Fabric level backup**
    - Multiple backups, centralized management, detailed tracking
- **!** New VM created by backup won't have backup policy associated with it.
- **Restoring and file-recovery manually**
  - Go to back-up blade for VM.
    - Two alternatives:
      a. Back-up items → Select backup → Restore VM → Select snapshot
      b. VM → Back-up
  - Different alternatives:
    a. **Restore VM**
      - Two alternatives:
        a. Create new VM
        b. Restore disks

    b. **File recovery**
      . Select recovery point
      a. Download script and execute on VM
        - Mounts disks from the selected recovery point
        - 💡 If files are larger than 100 GB, restore whole VM instead

      b. Unmount disks after recovery

Microsoft Azure Backup MARS Agent

- Called also **Recovery Services Agent**
- For backing up on-premises computers to Azure
  - Install back-up agent on local machine
  - Need connectivity to Microsoft Azure
- Same configuration and control
  - Centralized management of all on-premises back-ups
- Secure backup and recovery
  - Protected Instance is registered with Azure
- Flow

i. In recovery services in portal
    a. Back-up
        - Where is your workload running: On-premises
        - What do you want to back-up:
            - • Files and folders • Hyper-V • VMware • Microsoft SQL Server • Sharepoint • Exchange • System State • Bare Metal Recovery
    b. Backup *files and folders* and *system state*
    c. Download **Recovery Services Agent** from link provided
    d. Download credentials to enter in the workstation
    e. Transfer credentials & agents to the workstation

ii. Install the Azure backup client
    - Select a password for encryption

iii. Setup the backup
    - Click on *Schedule Backup* in agent
    - Select files/folders
    - Specify retention settings and policy

iv. Backup and restore file
    - Click on **Backup Now** in agent
    - Click on **Recover Now** in agent

Microsoft Azure Backup Server

- Centralized installation
    - Can be installed on a server in Azure or on-premises
- Free
- Similar functionality as *Data Protection Manager (DPM)*
- Backup a variety of instances
    - Workloads, VMWare and Hyper-V VMs, hosts, files, application workloads and barebone backups
- Flow
    i. Create Backup in Site Recovery Service
        - Go to Vault → Backup
        - Get link for Azure Backup Server
    ii. Install Azure Backup Server
        - Installs SQL server
    iii. Configure Azure Backup Server
        a. Select management
        b. Protection Servers → Register a server

c. Disk Servers → Add a disk for configuration files
d. Create protection group
    - Add servers, workstations and workloads to the group
    - Can back-up to online and/or locally
e. Enable disk for backup data

iv. Recover with Azure Backup Server
    - Select server → Click on Recover Now

5. Compute - Virtual machines (VMs)

Virtual Machines (VMs)

Concepts

- Storage resource provider (SRP)
    - Disks (blob)
    - Storage account
- Compute resource provider (CRP)
    - VMs
- Networking resource provider (NRP)
    - NICs, IP addresses, subnets load balancers..

Common VM Operations

Moving a VM

- Helps for
    - high availability
    - reduce latency for serving from VMs closer to users
- 💡 You can move virtual machines with the managed disks & in Availability Zones across subscriptions and VMs.
    - ❗ Not supported:
        - Virtual Machine Scale Sets.
        - Virtual machines created from Marketplace resources with plans attached
- ❗ To move a virtual machine with a network interface card, you must move all dependent resources.

    - E.g. • virtual network for the network interface card • all other network interface cards for the virtual network • VPN gateways
- Virtual networks (classic) can't be moved.
- Can move across regions using
    - Azure Resource Mover
    - Using Azure Site Recovery by copying the data

Stopping a VM

- **Deallocation**
    - ! If you shut down a VM inside VM, Azure still keeps the resources
        - 💡 Deallocate instead
- **Auto shutdown**
    - VM blade in Portal

Removing a VM*

- Deleting VM doesn't remove dependencies such as NICs, storages, OS/data disks, IP addresses
- 💡 Delete resource group instead, or use taxonomic tags
- PowerShell or CLI allows you to keep OS and/or Data disks

Azure VM Extensions

- Extends VM capabilities
- Requires Azure VM Agent (different for Windows or Linux)
    - Marketplace images already have it
    - For lift & shift, install agent first before uploading to cloud
- **VM Access**
    - Backdoor to reset VM password reset
    - Allows to modify RDP/SSH configurations
- **VM Backup**
    - Allows to back-up VMs and configurations to recovery vault
- **Custom Script**
    - Allows Desired State Configuration (DSC)
        - You can script in Linux (bash), Windows (PowerShell)
        - Puppet, chef etc
- **Microsoft Monitoring Agent**
    - Onboards VM in Log Analytics

Sizing

- Allows vertical scaling, e.g. CPU, RAM and other resources
- ! Resizing requires rebooting VM.
- **Azure Compute Unit (ACU)**
    - Standardization without any hardware details
    - 100 ACU = Small (Standard A1) VM
        - A = Family
        - 1 = Size (versioned)
    - DS_V3 = 160-190 ACU
    - Good for estimating for lift and shift.
    - As you raise ACU, per minute runtime charges increases.
- Types

Type	Sizes	Description
General purpose	B, Dsv3, Dv3, DSv2, Dv2, DS, D, Av2, A0-7	Balanced CPU-to-memory ratio. Ideal for testing and development, small to medium databases, and low medium traffic web servers.
Compute optimized	Fsv2, Fs, F	High CPU-to-memory ratio. Good for medium traffic web servers, network appliances, batch processes, and application servers.
Memory optimized	Esv3, Ev3, M, GS, G, DSv2, DS, Dv2, D	High memory-to-CPU ratio. Great for relational database servers, medium to large caches, and in-memory analytics.
Storage optimized	Ls	High disk throughput and IO. Ideal for Big Data, SQL and NoSQL databases.
GPU	NV, NC, NCv2, NCv3, ND	Specialized virtual machines targeted for heavy graphic rendering and viedo editing, as well as model

Type	Sizes	Description
		training and inferencing (ND) with deep learning. Available with single or multiple GPUs
High performance compute	H, A8-11	Our fastest and most powerful CPU virtual machines with high-throughput network interfaces (RDMA).

Disk Types

- **OS Disk**
  - ! Generation 1. VHD only
    - If you use Generation 2 Hyper-V you need to convert from `.vhdx` to `.vhd`.
  - Registered as SATA drive
  - ! Maximum capacity of 1 TB
- **Data Disk**
  - Dependent # on VM instance size
  - Registered as SCSI disk
  - ! Max capacity 4 TB
- **Temprorary Disk**
  - D: or /dev/sdb1
  - Bound to the hardware host
  - Do not store permanent data!

Storage

Standard vs. Premium Disk Storage

- **Standard Disks**
  - Backed by cost-effective HDDs
  - High availability: several replication options
  - Stored in Azure storage account
  - Standard SSD available for managed disks (dev/test/entry elvel production applications)
  - Standard storage provides maximum IOPS values for each VHD
  - On portal

        - You can see disks in Azure Disks.
        - Azure names managed disks like `dc1_data-disk1`, `dc1_OSDisk` for a VM named `dc`.
        - By clicking on it, you can manage the disk.
            - You can e.g. export, create a snapshot
- **Premium Disks**
    - Backed by high-speed SSDs
    - IOPS values are predictable, expected performance levels
    - Pre-pay for all storage used (fixed sized disk sizes)
        - 🔑 Predictable speed and IOPS
        - P10, 128 GB, 500 IOPs, 50 MB/sec
    - ! Supports only Generation 1 VHD
        - If you use Generation 2 Hyper-V you need to convert from `.vhdx` to `.vhd`.
        - 🔑 Azure Site Recovery migration handles this automatically
        - On portal
            - You can see unmanaged disks in Blob Containers → VHDs → you see VHDs
            - A security problem is that someone by mistake can give public access to the blobs in the storage account.

Managed vs. unmanaged Disk Storage

- **Unmanaged Disks**
    - Original method to store VM VHDS
        - Legacy
    - VHDS are stored as page blobs in an Azure storage account
    - ! Maximum 256 TB of storage per VM
    - ! You need to manage storage account availability
    - ! 20,000 IOPS limit across all VM disks in a standard storage account
    - In storage account they're in Blob Containers → VHDS container.
        - They're leased
            - They a re locked
            - You need to stop & deallocate VMs to delete them
        - You can break lease in Storage Explorer by right clicking
- **Managed Disks**
    - 🔑 Always use
    - Azure manages the disks, you don't have to worry about storage account-level IOPS restrictions.
    - Pre-pay for disk size (no need for SA)

        - S10, 128 GB, 500 IOPS, 60 MB/sec
    - Supports Standard and Premium SSD and Standard HDD
    - ! LRS replication only for Premium managed disks
    - ! You can resize only when they're unattached or owner VM is stopped & deallocated

Costs

- Use Azure Pricing Calculator
- Optimizing costs
    - 💡 Reserved Virtual Instances are the cheapest option.
        - You pay 1 to 3 year term for a particular VM instance size in aspecific region.
    - 💡 Reuse on-prem Microsoft licensens, up to 49% discount
- VM Chooser (`azurevmchooser.kvaes.be`)
    - Open source applications to get recommendations
        a. Give total VCPUs, RAMs etc.
        b. Select a recommended VM
        c. VM optimizer: Choose usage patterns, region etc.

IP addressing

- You always have a private IP and you can optionally have a public IP
- **Public IP addresses**
    - Best practice is to never have a public IP
        - Consider a load balancer to map the private IP.
    - First 5 public IPs are free then it costs
    - You have to NSG with an public IP
    - Public IPv4 addresses can be associated with:
        - VM vNICs, public load balancers, VPN gateways, and application gateways
    - Public IP Address SKUs
        - Basic SKU
            - Open by default
            - Static or dynamic allocation
        - Standard SKU
            - Secure by default (NSG)
            - Static allocation only
            - HA: Availability zone aware, can span to different availability zones
- **DNS Naming**

- For VMs you can configure & use host name
- VM -> Overview -> Configure DNS Name then you can have like `somename.eastus2.cloudapp.azure.com`

Monitoring

Boot Diagnostics

- Periodic screenshots of the console
- Enables serial console
  - You can connect to VM when you can't SSH/RDP for fixing e.g. boot state
  - Requires you to have VM Contributor or higher privileges.
  - No need to open SSH/RDP ports

Guest OS diagnostics

- Requires storage account
- Event logs, performence counters etc.
- Lowest level IaaS monitoring extension
- For more diagnostics:
  - Windows: AzurePerformanceDiagnostics
  - Linux: Linux Diagnostic Extension (LAD) 3.0

Azure Log Analytics

- Enabled by deploying the Microsoft Management Extension
- Onboards VMs into Log Analytics workspace

System Center Operations Manager (SCOM)

- Hybrid cloud approach
- You can track your cloud VMs on on-premises or visa versa

5.1. Compute - Virtual machines (VMs) - High Availability

High Availability

- High Availability = Redundancy
- Layers of availability
  i. Hardware-level availability
     - Handled by Azure
  ii. Server-level availability
     - **Availability Sets**
       - Ensures 99.95% SLA for VMs in availability set
       - Provides server level fault tolerance within a single data center within a single region.
       - Availability sets are containers/racks that's called Fault Domains
       - 2 VMs in same Availability Sets = Azure places those in different availability sets.
       - Update domains are different domains in different availability sets (fault Domains) and your VMs are set in different update domains as well.
         - Protects availability against VM shutdowns because of update failures / hardware shutdowns.
       - **!** Must assign availability set at VM deployment
       - **!** Scaling (resizing) requires stopping all VMs in the availability set.
       - For single VM not in availability set you have 99.9% availability if you use premium storage.
  iii. Datacenter-level
     - **Availability Zones**
       - Allows you to place redundant VMs in different regions.
       - Provides data center level tolerance.
       - Load balancers are availability zone aware on standard SKU
       - **!** You have to use managed disks
  iv. Region-level
     - You need recovery service vault (storage for back-ups/replications)
       - **VM backup**
         - Ad-hoc or scheduled
         - Includes all disks and configurations
       - **Azure Site Recovery**
         - **Failover recovery**
           - 15 minute RPO (recovery point objective)
           - **Azure-to-Azure (A2A) ASR Architecture**
             - Directly available in VM blade

- All storage data, VMs, disks (managed and unmanaged), subnets etc.
  - Prepared and ready to go in another region.
  - In sync
  - ! May require configuration with IP addresses
  - You can failover to it and/or failback
- Configure in VM blade -> Disaster recovery
  - Allows you to configure disaster recovery for single VM
    - For workloads including multiple VMs you should configure it directly from Site Recovery
  - You can choose to automate what happens using Automation runbooks.
  - You can then view recovery status in same blade
    - Replication health
    - Recovery points
      - Crash-consistent:
        - Least preferable
        - As if VM is replicate while it was powered off, no guarantees
      - App-consistent
        - Preferable point to recover
        - Data and OS back
    - Commit -> Finalizes the failover
    - Re-protected -> Creates new recovery environment from old recovery environment (which becomes source environment)
- **Migration to Azure**
  - On-premises to Azure
  - AWS to Azure

Azure Advisor

- Gives recommendation regarding high availability
- E.g.:
    - Add more virtual machines for improved fault tolerance *(medium impact)*
    - Enable VM backup to protect your data from corruption and accidental deletion *(medium impact)*
    - Create an Azure service health alert *(low impact)*

VM Events

- Planned maintenance events
- Unexpected downtime events
- Notification
    - In Azure support webpage, status webpage, twitter account
    - Administrators get e-mail notifications

5.2 Compute - Virtual machines (VMs) - Deployment

Deployment

- Deployment tools
    - • Azure portal • Azure Cloud Shell • Azure PowerShell • Azure CLI • Azure SDKs • ARM templates
- You can create from
    - User images
        - Uses unmanaged disks
    - Marketplace images

Create VM Image

Generalizing VM

- Should be the first step
- Generalization resets server-specific data: Computer name
    - Security identifiers (SIDs)

    - Local administrator/root identity
    - Device driver cache
    - Event logs
- How to generalize
    - On Windows use `sysprep`, "System Preparation Tool"
    - On Linux run `sudo waagent -deprovision+user`
    - Take a VM backup first, because generalization is destructive and permanent

Create VM image from Azure VM

- Managed Disk Concepts
    - Disks
        - No storage account (management) required
        - Pay for pre-allocated storage (P10 =128 GB SSD VHD)
    - Snapshots
        - Read-only full copy of a managed disks
        - You can create new VMs based on snapshots
    - Images
        - Generalized VM disk images
        - Snapshots can be converted into images
- **Flow**
    i. Get an image
        - Get a snapshot image
            a. Go to Disks → Select OS disk → Create snapshot
            b. In snapshot → Click on Export → You will get SAS url → Download VHD
            c. Generalize the image
        - Or capture an image
            - In portal: VM → Overview → Capture
            - **!** Not generalized
            - It appears in images

    ii. Go to Images in portal, select the image, from there click on Deploy and it'll navigate you

VM Connection

- You have different levels of security NSG, host firewall, options to have public IP or not

Just-in-time VM Access

- Allowed by **Azure Defender** (formerly known as **Azure Security Center Standard tier**)
- Locks down all administrator ports as default, when admin requests admin session then session is bounded by time limit and IP address restriction while granting access.
- No need to have management port open all the time
- 💡 Recommended to enable

Deploying Linux Server VM

- Around 40% of workloads in Azure runs on Linux
- Endorsed in Azure: CentOS, CoreOS, Debian, Oracle Linux, Red Hat Enterprise Linux, SUSE Enterprise Linux, openSUSE, Ubuntu
- Connection
    - **Secure Shell (SSH)**
        - A popular client is PuTTy for SSH or you can install *subsystem for Linux* or *git tools* on Windows 10 to get SSH.
    - **Remote Desktop Protocol (RDP)**
        - You can install RDP on Linux.
        - Some do not believe in graphical shell:
            - Presents security vulnerability possible
            - Needlessly consumes CPU
        - Windows team ported RDP into linux.
    - **Serial Console**
        - COM1 serial port connection to VM
        - Low-level access
        - Helpful when e.g. your VM doesn't boot up
- **Authentication**
    i. SSH Public Key
        - You keep private key and share public key with Azure.
    ii. Password
        - You can reset those after deployment in portal: VM → Reset password

Deploying Windows Server VM

- Windows Server 2019, 2016, 2012, 2008, Windows 10 Pro or Enterprise (for e.g. load testing, client-side testing, jump-box)
- **Connect**
    - Remote Desktop Protocol (RDP)

        - Uses TCP 3389
        - You can connect directly from Portal: Overview → Connect
    - WinRM (PowerShell) Remoting
        - TCP 5985, 5986
    - Serial Console
        - Text console into VM
        - Can get to VMs that can't boot

Prepare environment with Azure Policy

- **RBAC vs Azure Policy**
    - RBAC
        - Focuses on user actions at different scopes
        - VM Contributor can manage only VM
        - Built-in custom roles
    - Azure Policy
        - Focuses on resource properties during deployment for already existing resources
        - Uses default allow and explicit deny access system
    - Difference
        - You're not going to be able to create VM unless you have read & write abilities by RBAC
        - Azure Policy in contrast constrains what that RBAC can do when she/he attempts to create VM
- Some built-in Azure Policy definitions are e.g. *`allowed locations`*, *`VM SKU`*, *`ensure MMS extension is deployed`*
- You can create also own policies, or initiatives which are collections of policies.
- Examples
    - Policy definition e.g. allowed locations
    - Parameters e.g. select which regions are allowed

Deploy with ARM templates

- ARM templates are infrastructure as code foundation of automation and DevOps in Azure
- 💡 Visual Studio is a good ARM template editor
    - Visual Studio Code can also be used.
- Different ways to work with templates

i. You can go to Portal → Templates → Usage existing usages or add a new template
ii. In Visual Studio → Cloud → Azure Resource Group → You can select template location (e.g. GitHub) → Select a template
iii. Deploy a VM then in the last step click on "Download template and parameters"

- You can deploy with PowerShell, Cloud Shell, Azure CLI, or directly from Visual Studio
- You can automate deployment actions such as VM access
- Files
  - `azuredeploy.json`
    - Deployment template.
    - Defines resources and property such as `allowedValues`, `defaultValue`
    - You can refactor some values in variables and reuse in the file
    - `copy` element block in deployment script allows you to create e.g. 3 storages.
  - `azuredeploy.parameters.json`
    - Deployment parameters (required for deployment) to deploy `azuredeploy.json`

5.3 Compute - Virtual machines (VMs) - VM Scale Sets (VMMS)

VM Scale Sets (VMSS)

- Group that holds identically configured VMs
- Used for
  - Need to create and manage multiple VMs
    - Centrally create and manage multple VMs (Windows Server or Linux)
  - Need for high availability and app resiliency
    - Horizontal scaling, scaling up and down based on spikes
  - Need for large (1000) scale
    - E.g. Azure Batch uses scale sets under the hood
  - Need for IaaS autoscale
    - Scale out and in based on metrics based autoscale

PaaS Scaling vs IaaS Scaling

- Azure App Service
  - High agility at the expense of administrative power
  - The underlying Hyper-V Vms are almost totally abstracted from you

    - Easy manual, scheduled, or automatic scale out and scale back
- Virtual Machine Scale Set (VMSS)
    - Maximum administrative power at the expense of agility
    - VMSS represents Azure's approach to IaaS horizontal scaling

Deploying a VM Scale Set

- Create virtual machine scale set
    - Availability zone
        - Scale scale sets across one and more availability zones
        - ! All regions do not support availability zone
    - Instance count & instance set
    - Low priority
        - Take advantage of unutilized capacity
            - Compute power that customers/Microsoft is not using
            - Save costs
        - Good for workloads that can handle interruption
            - Stateless workloads
            - VMs in the scale set may be evicted at any time
            - You set eviction policy:
                - Stop / Deallocate
                - Delete
    - Use manage/unmanaged disks
        - ! Managed disks are not supported with availability zones
    - Networking
        - Application Gateway
            - 💡 Useful if your scale sets are web servers
            - ! Do not support RDP
        - Load Balancer
            - Supports RDP
            - You set public IP address name and domain name label (`domain-name.region.cloudapp.azure.com`)
- You can also use ARM template e.g. *Deploy a Windows VM Scale Set with a Custom Script Extension* that deploys VMs, load balancer and a powershell script to be executed after deployment.

Connecting to VMs

- In portal: Choose VM → Settings → Instances you can see all the instances

- To connect to individual instances you need load balancer and NAT (network address translation)
    - You can't RDP/SSH into individual instances directly
    - You can connect to load balancer IPs
        - In portal: Load Balancer → Inbound NAT rules
    - NAT maps different VMs on different ports.

Configuring Autoscale

- ***Manual***: Through Portal/SDK/CLI/PowerShell
- Autoscale
- ***Scheduled***: If you know when the load will be high you can plan for that and scale with time triggers
- ***Metrics***: Use various metrics from various sources to determine when to scale in/out
- Manage in VMSS → Scaling →
    - Enable auto-scaling
    - Select scale-mode
    - **Scale based on metric**
        - Add rule
        - E.g. increase instance count by 1 when CPU percentage above 70%
        - 💡 You should also create scale mode that bring down the scale count
        - Properties
            - Duration: Good to not be confused when scaling out/in, so set a duration to e.g. 10 minutes
            - Cooldown: Waits after scale operation before new scale operation
    - **Scale to specific instance count**
        - Time-based scaling
        - Set start and end date

5.4. Compute - Virtual machines (VMs) - Security

Security

Role based access control

- Provides fine-grained access to resources
- AAA

    - A: Authentication (identity)
    - A: Authorization (abilities)
    - A: Accounting (auditing)
- Higher to lower granularity
    - Management groups → Subscription → Resource group → Resource
- Roles
    - **Reader**: Observers
    - Resource-specific or custom role, **contributor**: Users managing resources
    - **Owner**: Admins
- Custom roles are defined in JSON
- RBAC focuses on user actions at different scopes.
    - By contrast, Azure Policy focuses on resource properties during deployment
        - Policies e.g. *`Allowed virtual machine SKUs`*, *`Enforce automatic OS upgrade with app health checks on VMSS`*
- You can manage in *Access Control (IAM)* blade.

Storage Security

Storage Service Encryption

- Protects data at rest in storage account
- 128-bit AES encryption
- Azure manages encryption keys
    - 💡 You can manage them yourself with Azure Key Vault

Azure Disk Encryption

- BitLocker for Windows Server VMs
- DM-Crypt library for Linux VMs
- Protects OS and data disks
- Azure- or customer- managed disks
- Manage:
    - In VM blade -> Disks -> Add data disk
    - Use PowerShell
        a. Create key vault and vault key
        b. Create security principal (identity in Azure AD) that can take the key from key vault
        c. You run `SetRmVMDiskEncryption` to configure encryption

Network-level security

Network Security Group (NSG)

- Stateful firewalls
- Augmented security rules: Have inbound/outbound rules
- Can be bound to *public addresses*, *load balancers*, *subnets* and *VMs*.
- Traffic streams are identified with 5-tuple hash: Source, destination, port, protocol, IP addresses.
- Source can be service tags
    - In-built e.g. Internet
- Or custom (**Application Security Group** identifiers)
    - Simplifies NSGs
    - Logically groups VMs e.g. by role
        - Association is done through NICs
    - E.g. AppServers, DatabaseServers
    - Flow:
        a. Define ASGs
        b. Include ASGs in NSGs

Host Firewalls

- E.g. Windows Defender Firewall on Windows Server VMs
- 💡 A range that's whitelisted in NSG can be blocked by host firewalls.

Jumpbox Architecture

- Jumpbox is a pivot point VM in a VNet
- Good for auditing every administrative action
    - A shared jumpbox makes it easier to administrate the orchestration
- You can e.g. allow access to public IP and make sure it's locked down to that endpoint.
- Or you can e.g. point to Site-to-Site VPN or point-to-site VPN.

Azure Security Center (ACS)

- Two tiers: Azure Security Center Free Tier, Azure Defender
- See also pricing page

Azure Security Center Free Tier

- Continuous security assessment
- Actionable recommendations
- Prioritized alerts and incidents
- Integrated security solutions
    - E.g. recommends to deploy WAF

Azure Defender

- Just-in-time VM Access
- Threat protection for Azure VMs and non-Azure servers
- Threat protection for PaaS services
- Regulatory compliance dashboard and reports

Just-in-Time (JIT) VM Access

- Allowed by **Azure Defender for servers** (formerly known as **Azure Security Center Standard tier**)
- Normally to access a VM, you need 3389 for RDP protocol, or 22 to SSH for linux, you open those ports 7/24.
    - Not so secure as they're publicly accessible if IP is public.
- JIT locks down inbound administrative port access
- Time-restricted access to specific IP address(es)

5.5. Compute - Virtual machines (VMs) - Backups

Backups

VM Disk Snapshots

- .VHD files (data + os disks in page blobs) are stored aas page blobs.
- Full and incremental point-in-time snapshots
- Faster than performing full back-ups
    - 💡 The difference is that snapshots are deltas
- Supported in

- Managed disks
- Unmanaged disks
  - Use AzCopy command line tool to archive to another storage account
- ❗ Snapshots cannot outlive their sources blob
- If you delete VMs, snapshots become irrelevant
  - 🔔 Consider archiving them
- You can create new VM from a snapshot.
- In Portal -> VM -> Disks -> Select Disk -> Create Snapshot
- In Snaphots -> Find snapshot ->
  - Export:
  - You export with creating SAS URL (time limited)
  - You get direct URL

Azure VM Backup

MARS, Microsoft Agent Recovery Services

- Supports on-prem to cloud
- Supports file/folders but not whole disk back-up

System Center DPM (Data Protection Manager)*

- Supports system image/whole VM back-ups from on-premises to Azure

Azure Backup Server (MABS, Microsoft Azure Backup Server)

- Azure specific version of System Center DPM

Azure Backup

- Azure IaaS VM Backup
- Require recovery services vault
  - Don't need to worry about storage accounts
- Azure Backup service uses VMSnapshot and VMSnapshotLinux extensions
- VSS orchestrates consistent snapshots of OS and data disks.

Consistency levels

- **Application-consistent**
  - 💡 Preferred backup type
  - Data is consistent with time of backup (VSS)
- **File-system consistent**
  - Ensures the VM boots and there is neither corruption nor data loss
  - You may need to take further action to bring data current
- **Crash-consistent**
  - Least preferred backup type
  - Used when you back up a powered down VM

Manage

- VM -> Backup ->
  - Create/select recovery services vault
  - Create back-up policy with backup frequency and retention range
- You can see/start/stop back-ups in Recovery Services vault -> Backup Items
  - You can create policies in Backup Policies blade.
- In back-up/replication jobs blade you can list all jobs

Restore options

- **Create a new VM**
  - Basic VM up and running from a restore point
- **Restore disk**
  - Restores a VM disk which can then be used to create a new VM.
  - Azure Backup provides a template to help you customize and create a VM.
  - Useful if you want to customize the VM, add configuration settings that weren't there at the time of backup, or add settings that must be configured using the template or PowerShell.
- **Replace existing**
  - You can restore a disk, and use it to replace a disk on the existing VM.
  - Supported for unencrypted managed VMs
  - **!** Not supported for unmanaged disks, generalized VMs, or for VMs created using custom images.

Recovery Options

- **Entire VM**

    - OS and data disks
    - Configuration
    - Restore to original or alternate location
    - Quick create option
    - ***Flow***: Recovery Services Vault -> Restore VM -> Restore type: Create VM
- **Individual Disks**
    - Restore to storage account
    - Includes ARM deployment template
    - 💡 Use to control VM restore, gain full control over the VM environment
        - Availability set
        - vNIC
        - IP addresses...
    - ***Flow***
        a. Recovery Services Vault -> Restore VM -> Restore type: disks
        b. Restore VHD(s) to storage account
        c. Create VM configuration
        d. Attach the OS and data disks
- **Files and Folders**
    - Mount OS and data disks as network drives
    - **Azure VM File Recovery**
        - E.g. "We need to retrieve a few log files from 3 months ago. Time is of the essence"
            - If it was a VM back-up, it'd be costly as it takes storage etc.
            - With file recovery you can only recover log folders
        - ***Workflow***
            - Select recovery point
            - Download and run PowerShell script
            - Recover file system
            - Unmount the disks after recovery
        - Manage in Recovery Service Vault -> File Recovery

Azure Site Recovery

- Replication/orchestration engine
- Failover recovery for VMs
- You can use cloud <=> cloud, on-prem <=> cloud, on-prem <=> on-prem
- Provides region level failover
- Physical and virtual (Hyper-V and/or VMware) machines are supported

- Azure as a recovery site
- Migrate to Azure
- Manage in *VM -> Disaster Recovery* or *Recovery Services vault -> Site Recovery* (or *Recovery Services vault -> Disaster Recovery* especially for VMs)
    - Select target region
    - Select target resources (e.g. VNEt, availability set, RG) to new resources or existing
    - You can set storage, replication and extension settings
    - With a **recovery plan** you can set recovery order, inject code in-between VMs
        - You need to do it Recovery services vault
- **Failover/Failback**
    - In VM -> Disaster Recovery ->
        - Select Test failover or Failover
        - Click on "Commit"
        - Re-protect -> Go back to the original location
    - Flow:
        a. Prerequisite check
        b. Failover
        c. Create recovery point
        d. Start the VM
        e. Clean-up resources

6.1. Networking - Virtual Network (VNet)

Virtual Network (VNet)

- Communications and security boundary
    - Provides network isolation and segmentations
    - Enables Azure resources to communicate with each other securely
        - E.g. VMs, storage accounts, App Service apps, Azure SQL database instances
- Uses Azure network backbone
    - Communications are internal by default unless you explicitly make it external
- Name resolution
    - Azure-provided DNS
    - DNS service
- Traffic filtering
    - NSGs

    - Network Virtual Appliances
- ! 50-100 VNets allowed per subscription
- ! A resource can only be created in a virtual network that exists in the same region and subscription as the resource.
- **Why multiple VNets?**
    - Saving money
        - Service chaining: Share a network virtual appliance among several VNets
    - Segmenting workloads
        - NSGs and UDRs give you routing and traffic control
        - E.g. hub and spokes
    - Securing traffic
        - Private connectivity that uses the Microsoft backbone network
- ***Moving a VNet***
    - ! When moving a virtual network, you must also move its dependent resources
        - For VPN Gateways
            - You must move IP addresses, virtual network gateways, and all associated connection resources.
        - 💡 Local network gateways can be in a different resource group.
    - To move a peered virtual network, you must first disable the virtual network peering
    - ! You can't move a virtual network to a different subscription if the virtual network contains a subnet with resource navigation links
        - For example, if an Azure Cache for Redis resource is deployed into a subnet, that subnet has a resource navigation link.

Role of VNet

- You can link app services, storage accounts, VMs
- Provides traffic isolation and segmentation
- Runs on Azure backbone network
- Configure communication with Internet
    - 💡 Ensure only VMs that need public IP addresses get one.
- You need to link VNets together to allow communication
- Control traffic flows into the VNET, within the VNET, and between VNets.
- Have IPv4 address space
    - Uses CIDR block of private RFC 1918 addresses that are not public/internet routable themselves
- VNets are divided into subnets
    - E.g. in multi-tiered application, web-tier, business-tier, data-tier

        - Good for protecting access using NSGs
        - Good for having jumpbox and protecting who can connect to jump-box

VNet Design Best Practices

- Create subnets based on workloads
    - E.g. all of your web front-ends will have similar access requirements, then you can bind NSGs on subnet level.
- Bind NSGs at the subnet level
    - Not good to bind at VNet level for better troubleshooting
- Deploy a network virtual appliance (NVA) and user-defined routes (UDRs) to further customize traffic.
    - **Virtual appliance (NVA)**
        - E.g. enterprise grade firewall appliance, load balancer appliance
        - They exist in Azure marketplace
        - They'll be installed in VNet as a VM
    - **User defined routes (UDRs)**
        - Customize and control routing in a VNet
- Implement site-to-site or point-to-site VPN tunnels with on-premises environment

Deploying a VNet

- You can use ARM templates e.g. from Github.
    - Visual Studio is recommended for editing templates
- During deployment:
    - *Name*: Must be unique
    - *Subnet*: Default gives you one subnet, for more you can use ARM template or PowerShell/CLI
    - *DDoS protection*
        - Microsoft publishes their datacenter public IP address
        - Bad actors run port-scanners on those IP addresses all the time
    - *Service endpoints*
        - Allows you to integrate Azure PaaS services
- After deployment:
    - *Address space*
        - You cannot edit
        - You need to create new and delete old one.
    - *Subnets*

        - You can always add new subnets & deploy gateway subnet that'll be used by an Azure gateway.
    - *DNS server*
        - Default is azure provided
        - You can use custom by additional DNS servers
            - Affect all VMs
            - Still uses Azure DNS when necessary
            - Used when e.g. site-to-site or point-to-site connections, it'll affect all VMs.
    - *Diagram*
        - You can enable network watcher here.
        - You then load in subscription or RG and enable.
        - It shows topology

Network Security Groups (NSG)

- Stateful firewall for inbound and outbound traffic
    - Stateful = 5-tuple hash
        - Source + destination IP and ports
        - Protocol
- Has default rules
- Augmented rules
    - Allow you specify list of IP-addresses
    - No need to create several rules for same list
- **Service tags**
    - Azure defined named IP address endpoints
    - E.g. *Internet*, *VirtualNetwork*, *AzureLoadBalancer*, *AzureTrafficManager*, *Storage*, *SQL*, *AzureCosmosDB*, *AzureKeyVault*.
    - Allows you to use names instead of IP addresses
- **Application Security Groups (ASGs)**
    - Custom (user-defined) logical identifiers
    - You can associate IP ranges and then use it as source/destination in NSGs.
    - E.g. *WebServer*, *WappServers*, *DbServers*
- Can be bound to VNets, subnets or NICs
    - 💡 Bind to subnets
- Security rules
    - Priority: Lower the number, higher the priority of the rules

IP Addressing Best Practices

- If a VM doesn't need a public IP address (PIP), then don't assign one and use an Azure load balancer instead.
- Plan your VNet private address space to avoid overlap.
    - Different from on-premises
    - Different from other VNets in Azure
- Never configure networking from within the VM
    - Do it on Azure instead using Azure abstractions

Network Interfaces

- Assigned to a single subnet.
- Have a public or private IP that's dynamic or static.
- *IP forwarding*
    - E.g. if you have network appliance and you want to give it ability to forwar traffic that's not destined for itself

6.1.1. Networking - Virtual Network (VNet) - Connecting VNets

Connecting VNets

- You don't need to have a Layer 3 router to route traffic from subnet to subnet
- Azure system routes take care of the routing for you automatically

Options

VPN Gateway

- Creates IPsec/IKEv2 tunnel and always-on connection
- Used for connecting VPNs in cloud or hybrid scenario.

Inside Azure

VNet-to-VNet VPN

- Create isolation or administrative boundaries
- Provide cross-region geo-redundancy and replication securely
- No traffic crosses the public internet
- Separate VPN gateways costs while VNet peering is free.
- 💡 Make sure your VNet address spaces do not overlap.
- Troubleshooting
    - Verify connectivity through peering
        - Set up Azure DNS

VNet peering

- ❗ Seamless connection between two Azure VNets.
    - The peered networks appear as one, for connectivity purposes.
    - Name resolution does not flow, requires own DNS zone
- Runs on Azure backbone
- 💡 You can peer across regions and subcriptions
- Peering can overcome misplaced VMs
- Save money with service chaining (e.g. services' communication are chained through a subnet)
- ❗ Peering must be done on both sites
    - VNet1 <=> VNet2 and VNet2 <=> VNet1
- ***Configuration***
    - **Allow forwarded traffic**
        - Am I peering from a hub VNet that'll have IP-forwarder?
        - Allow peers (other VNets) to forward traffic to go through.
    - **Allow gateway transit**
        - Am I hosting a VPN gateway?
    - **Use remote gateways**
        - Is this network use peer's gateway?
        - ❗ VNets must be in same region
- Enables **force tunnelling**
    - E.g. when all Internet traffic must go through on-premises firewall device.
    - You can use *user defined routes* for all outbound traffic to go back through VPN gateway to on-premises.
- ❗ Peerings are not transitive

    - If you peer spoke1 <=> spoke2 and spoke2 <=> spoke3 then spoke1 cannot communicate with spoke3 automatically.
    - Common solution is transiting VNet with **Hub and Spoke topology**.
        - Topology is a segmentation
            - **When to segment with VNets and when with subnets?**
                - Depends on bureaucratic reasons
                - E.g. different VNets when
                    - Different cost centers/groups need management autonomy
                    - You want to completely isolate different workloads
        - Name resolution needs configurations
            - You can't do with Azure provided DNS as all your hosts have then `internal.cloudapp.net`
            - In peering azure provided DNS won't work
- ***Troubleshooting tips***
    - Azure blocks ICMP between Vnets and the Internet
        - ICMP is used for ping
        - Microsoft blocks it because of DDoS attacks.
    - Simplify NSGs as much as possible to reduce troubleshooting friction
    - Azure portal Diagnose and solve problems/Resource health blade is useful
    - Network Watcher and Network Permormance Monitor make troubleshooting much easier
        - **Network Watcher**
            - Shows where's the traffic is captured/denied
            - Suite of tools
                - **Topology**: e.g. VNETs, subnets, VMs, NICs
                - **Variable Packet Capture**: Captures TCP packages at NIC level as wireshark files.
                - **IP Flow Verify**: Troubleshoots NSG
                - **Next hop**: Troubleshoots route tables
                - **Connection troubleshoot**: Why it does not connect?
                - Diagnostics Logging
                - Security Group View
                - NSG Flow Logging
                - VPN Gateway Troubleshooting
                - Network Subscription Limits
                - Role Based Access Control
            - In Portal you can search for Network Watcher and enable it on VMs

- **Network Performance Monitor**
  - E.g. top network health events, ExpressRoute monitor, service endpoint monitor, performance monitor
  - It ties in logs/metrics with Log Analytics.
  - Part of Insights & Analytics Azure management solution.
  - Works with installing Microsoft Monitoring Agent (MMA) in VM.
  - ***Flow***
    a. Deploy Insight & Analytics and then select Network Performance Monitor
    b. Choose VM and click on "Connect", it'll install `MicrosoftMonitoringAgent`

Hybrid Connections

Site-to-site VPN

- Two VPN devices connect to each other.
- ***Flow***
  i. Deploy a ***VPN Gateway*** resource in Azure
     - Requires gateway subnet (or DMZ subnet).
     - Different SKUs: Basic, VpnGw1, VpnGw2, VpnGw3
       - You get more bandwidth, site-to-site and point-to-site points.
       - Don't use basic for production
     - You can see the deployed VPN Gateway in *Connected Devices* in subnet.
  ii. Deploy a ***Local Network Gateway*** as well.
     - For your on-prem gateway device, you need to set up one of the route table configurations:
       - **PolicyBased**
         - Handle route tables manually
         - ❗ Does not work with BGP failover, active-to-active configurations
         - **RouteBased**
           - 💡 Always use if possible
           - Some VPN devices do not support it
           - What's compatible is documented on Microsoft docs.
  iii. Create a connection between two gateways
     - Create local-to-azure in Local Network Gateway
     - Create azure-to-local in VPN Gateway
     - In Shared Key in connection blade, specify a key.

Point-to-site VPN

- Allows access to Azure resources through VPN tunnel from a client agent.
- More portable way
- **Flow**
  i. On Azure deploy VPN gateway
  ii. In Point-to-site configuration blade download VPN client
  iii. Deploy agent (a VPN Client) from VPN gateway
  iv. Install on individual endpoints (e.g. laptops)
- Allows connection outside network perimeter

Express route

- High speed secure connection between on-prem and cloud

Best practices for High Availability

- ***Combine ExpressRoute and VPN***
  - In gateway subnet
    - Deploy ExpressRoute gateway
    - Deploy VPN Gateway
  - Both gateways gives access to front-end tier and a jumpbox in a management subnet
  - If ExpressRoute goes down VPN gateway gets activated
- ***Deploy two VPNs***
  - Requires enabling BGP in gateway link
    - Robust routing
    - Enable active-to-active connection configuration
    - **!** Only allowed RouteBased routing configuration
  - Two VPN gateways on-prem
    - Allows redundant active-to-active connection to single gateway.
    - You have one active and one stand-by gateway

System Routes vs. User-defined Routes

- **Situations**
  - You need to move one VM to another VNet.
    - It requires re-deploying
  - Isolation & segmentations

        - E.g. development / production VNet
    - **Hub & Spoke Topology**
        - *Hub*: VNet have Virtual Network Appliance (e.g. firewall), or gateway
            - You don't want to have *Virtual Network Appliance* as it costs both money and resources.
        - *Spokes*
            - Other VNets (e.g. front-end, back-end)
            - You can force communicates with each other through Hub.
- Internet calls and calls from internet
    - Handled by Azure using system routes
    - You don't need to manipulate them
- If you want to override system routes (e.g. for Hub & Spoke topology)
    - You need User Defined Routing
    - For network appliance you need to configure IP forwarding
        - Enables it to pass on traffic that it's not destined for itself.

6.1.2. Networking - Virtual Network (VNet) - DNS & Name Resolution

DNS & Name Resolution

Azure-provided name resolution

- No configuration required
- All VMs within a VNet can resolve each others' host names
- **!** Limitations
    - Cross-VNet name resolution
    - Issue: No custom DNS suffix
- You can add custom DNS server IP addresses
    - E.g. in hybrid cloud if you want Azure VMs to have IP addresses from on-premises DNS server or vice versa.
    - E.g. stand up own DNS servers in VNet instead.
    - E.g. configure DNS forwarding between one DNS server in one VNet to another DNS server in another VNet

Azure DNS

- Allows VNETs to resolve each others host names.

- **Host your public DNS domain in Azure**
  - Use Azure geo-distributed name servers for high speed name resolution
  - Delegate a domain:
    a. Create a DNS Zone
    b. Copy an Azure DNS name server from the zone
    c. In the registrar's DNS management page, edit the NS records and replace the NS records with the Azure DNS name servers.
- You manage in Portal -> DNS zone
  - Each DNS zone has
    - VNets of associated with it
    - **Record-sets**: IP addresses and host names of VMs
- **Create private DNS zones**
  - Allows you to not route names in public DNS
  - **Linked to VNets**
    - Lets you avoid setting up own DNS infrastructure
  - **Registration VNet**
    - You create private DNS zone and registration VNet
    - Any VMs within that VNet will automatically have their names registered and DNS records created in Azure DNS
  - **Resolution VNet**
    - Allows you to have name resolution across VNets
    - Other VNets will be resolution VNets
    - Allows you to create records (hosts, alias) for VMs and it'll support name resolution across VNets

Hybrid Cloud

- **!**Azure provided DNS won't work with peering.
- A potential solution:
  - On-prem: Configure own DNS server and configure forward queries to Azure.
  - In Azure
    - Connect VNets (peer or VPN)
    - Deploy own DNS servers in VNets and configure forwarding there
  - **!** Too much overhead
- 💡 Use **Azure DNS Private Zones** instead
  - Configure Azure DNS servers specifically for private zones.
  - One network: Registration network
    - Hosts will have their names auto-registered in private zones.
  - Other networks: Resolution networks

- You need to manually create hosts in CNAME/MX records.

- ***Set-up DNS name for peered Virtual Appliance and a VNet in a Hub & Spoke topology***
  - Existing VMs
    - [Host (spoke) VM] in [Host (spoke) VNet]
    - [Hub (virtual appliance, hybrid)] VM in [Hub (virtual appliance, hybrid) VNet]

  b. ***Create & set-up route table***

  a. Create a route table -> Routes -> Add ->
    - *Name*: E.g. *subnet1-nva*
    - *Address prefix*: If destination IP of a packet matches this then it matches the rules. E.g. *192.168.8.0/24*
    - *Next hop type*: Virtual network gateway, virtual network, internet, virtual appliance, none.
      - Choose [Hub (virtual appliance, hybrid) VM]
    - Set next-hop address to IP of [Hub (virtual appliance, hybrid) VM]

  b. Associate route table to related subnets
    - Route-table -> Subnets -> Associate subnet

  c. **Set-up peering**
    - You can ping to VNets as name resolution does not work across VNets
    - Set-up without any *allow forwarded traffic*, *allow gateway transit*, *use remote gateways* configuration
      - [Hub (virtual appliance, hybrid) VNet] <=> [Host (spoke) VNet]

  d. **Create DNS Zone**
    - In portal -> DNS zone -> Add DNS zone
    - Create private DNS zone in VA (hybrid) VNet
    - Create DNS zone
      - Register record set with IP and name of each VM
      - Register two VNets
        - Registration VNET for [Hub (virtual appliance, hybrid) VM]
        - Resolution VNET for [Host (spoke) VM]

6.2. Networking - Load Balancers

Load Balancer Options

- All load balancers are software appliances (software defined networking: SDN)
- 💡 Only Standard (not Basic) SKU allows availability zones in Load balancer

Public Load Balancer

- OSI Layer 4 TCP and UDP
- Internet-facing, has public IP address
- Offers two distribution modes
- ***Set-up public load balancer***
  i. Settings -> Back-end-pools-> Add VMs
  ii. Settings -> Health-probe -> Add health probe
    - E.g. tcp-80-probe (HTTP) probe
    - Set interval -> time between prop events
    - Set unhealth threshold (e.g. 2) before VM is dropped out from the pool
    - Add load balancing port
    - Incoming request from port 80 (*port*) will be passed to TCP passed 80 (*back-end port*)
    - Select backend pool & health-probe
    - Set session persistence
    - Floating IP (direct server return)
      - Use with internal load balancers
      - Use with SQL server always on cluster
      - Used when same back-end port needs to be used across multiple rules in a single Load Balancer.
  iii. Add inbound NAT rule
    - Map TCP 5000 to a VMs RDP port (3389)
    - Map TCP 5000 to a VMs RDP port (3389)

Internal load balancer

- OSI Layer 4 TCP and UDP
- Applies to traffic only within a virtual network
  - No public IP address
- Good for applying load balancing to n-tier application services (database)

Application Gateway

- OSI Layer 7 application
- Application Delivery Controller (ADC) as a service
- SSL offload
- Has Web Application Firewall (WAF)

Traffic Manager

- DNS-level
- Geographical load balancing
- Offers different routing methods