Microsoft AZ-500

Azure Security Engineer Associate

Quick Reference Guide

Microsoft Azure Security covers the latest security features provided by Microsoft to identify different threats and protect your Azure cloud using innovative techniques. Cloud computing brings new security challenges, but you can overcome these with Microsoft Azure's shared responsibility model. Azure cloud uses innovative techniques. This guide takes you through the built-in security controls and the multi-layered security features offered by Azure to protect cloud workloads across apps and networks. You'll get to grips with using Azure Security Center for unified security management, building secure application gateways on Azure, protecting the cloud from DDoS attacks, safeguarding with Azure Key Vault, and much more.

Skills Covered

- Manage identity and access (30-35%)
- Implement platform protection (15-20%)
- Manage security operations (25-30%)
- Secure data and applications (20-25%)

Certification Name & Exam Code

Microsoft Certified: Azure Security Engineer Associate

Microsoft Azure Security AZ-500

Prepared By: Deepanshu Sood
Connect At: LinkedIn

Disclaimer

This document is produced by Deepanshu Sood for the sole of purpose of making the quick study notes while studying Microsoft Azure Security Engineer Associate course. All the notes have been in reference to multiple resources available on internet, like: Microsoft Azure website, Alan Rodrigues course notes on Udemy.com, etc. I do not take any responsibility if the topics mentioned in this document turns to be different or updated or changed from Microsoft for Azure. Always refer to Microsoft website for the updated notes.

Intent

The only intention behind creating this document is to do a quick reference check related Azure Security topic. There is no intent or intention to make this document available for any commercial purposes. This document is openly available to use, share, distribute, and share.

Credits

Alan Rodrigues

Microsoft website

Packtpub.com

www.re-mark-able.net

www.k21academy.com

https://msdynamicsworld.com

Contents

Azure Active Directory

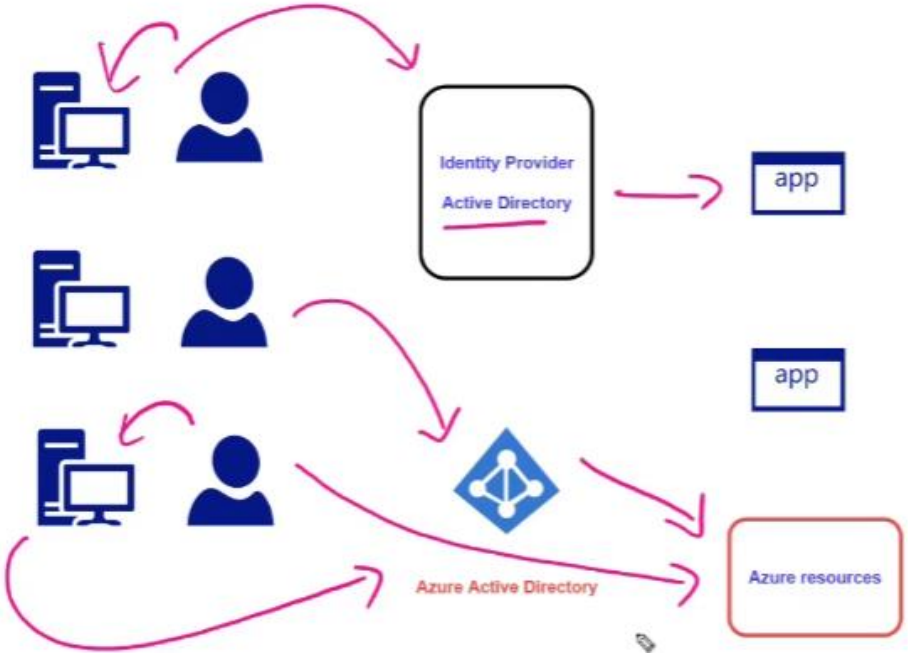
Microsoft Azure Active Directory is a comprehensive identity and access management cloud solution that combines core directory services, application access management and advanced identity protection.

Azure AD is the backbone of the Office 365 system, and it can sync with on-premise Active Directory and provide authentication to other cloud-based systems via OAuth.

Active Directory (AD) helps businesses manage users, groups, and objects within their networks. So, you can assign users to groups, and assign each of those group's access to specific network resources, apps, and devices. This ability to control access at a variety of levels gives businesses the freedom to distribute resources to specific subgroups, which is critical for both resource management as well as compliance and regulation.

Takeaways:

1. Microsoft Azure Active Directory (AAD) is a cloud-based identity and access management service
2. This allows users to sign-in and access resources in the Azure portal, Microsoft Office 365, and other SaaS application as well
3. There are many features available on Azure AD in addition to just adding users and groups
4. You can also define applications that would need access to resources in Azure
5. There are also different pricing models available for Azure Active Directory



Azure AD – Custom Domain

Every new Azure AD tenant comes with an initial domain name, <domain name>. onmicrosoft.com. You can't change or delete the initial domain name, but you can add your organization's names. Adding custom domain names helps you to create user names that are familiar to your users, such as alain@contoso.com.

You can add up to 5000 managed custom domain names.

Pre-requisites – You should own a domain name

Steps to add custom domain names:

1. Choose Azure AD
2. Select "Custom Domain Names"
3. Click "add custom domain" and enter domain name
4. Now enter the domain records to validate your domain

5. Click “Verify”

Azure AD – Pricing & Licensing

Azure Active Directory comes in four editions:

1. Free
2. Office 365
3. Premium P1
4. Premium P2

Features of all the editions:
https://www.agileit.com/news/understanding-azure-active-directory-licensing-free-basic-p1-p2/

1. The **Free edition** is included with a subscription of a commercial online service, e.g., Azure, Dynamics 365, Intune and Power Platform.
2. **Office 365** subscriptions include the Free edition, but Office 365 E1, E3, E5, F1 and F3 subscriptions also include the features listed under the Office 365 apps column.
3. **Premium P1** edition adds feature-rich enterprise-level identity management capabilities and enables hybrid users to seamlessly access on-premises and cloud capabilities. This edition includes everything you need for information worker and identity administrators in hybrid environments across application access, self-service identity and access management (IAM) and security in the cloud.
4. **Premium P2** includes every feature of all other Azure Active Directory edition enhanced with advanced identity protection and privileged identity management capabilities.

Important Notes:

1. The user who will be purchasing the licenses of Azure Active Directory has to be a part of custom domain
2. You can’t have a user that’s a part of default directory for purchasing licenses
3. You have to assign the role of “Billing Administrator” to the user who will be buying the licenses
4. It is very important to make ensure that you define the usage location to the users, if you don’t assign the usage location then you will not be able to assign the license on to the user

How to check your current Licensing:

1. Open Default Active Directory
2. Go to “Licenses”
3. Go to “All Products”
4. There you will see your current licensing

Azure AD – Dynamic Groups

Dynamic groups basically make use of rules that evaluate the attributes of users and then they can be added on to a group. You can create dynamic group for both for your users and for your devices as well.

Important Notes:

1. You need to have Azure AD Premium licenses to implement Dynamic Groups for each unique user that is a member of one or more dynamic groups
2. There is no license is required for devices that are members of a dynamic device groups
3. You can’t have one dynamic group for both users and devices together, they have to separate

How to create Dynamic Groups:

1. Go to Active Directory
2. Go to “Groups”
3. Click on “New Group”
4. In “Membership Type”, select “Dynamic User” or “Dynamic Device”

5. And make a rule or add a custom dynamic query

Azure AD – Roles Vs RBAC

Azure AD administrator roles are used to manage Azure AD resources in a directory. **Azure AD Roles** – Here you define your users, your groups, your applications, your service principles. These users can authenticate onto Azure and then they could access resources that are part of your Azure subscription.

Azure AD roles, you can assign the roles on to your users and these permissions are normally given to manage the various aspects of Azure AD.

RBAC roles are used to manage access to Azure resource, like VM's, and storage accounts.

Role-based Access Control – Is meant to authorize a user to use resources in Azure. Role-based access control can be given at the management group level, at the subscription level, at the resource group level or at the resource level.

https://cloudacademy.com/course/managing-azure-ad-user-roles/azure-rbac-roles-and-azure-ad-administrator-roles/

Azure AD – Relationship b/w AD Tenant and Subscription

What is a Tenant?

A tenant is the organization that owns and manages a specific instance of Microsoft cloud services. It's most often used in a inexact manner to refer to the set of Azure AD and Office 365 services for an organization.

What is Subscription?

The primary purpose of a subscription is to provide a common billing paradigm for use of Azure services. A subscription might have one or more tenants, directories, and domains associated with it.

Relationship b/w Tenant and Subscription

Azure tenant is a directory, subscription is an object that represents a "folder" that you can put resources in. Subscriptions are tied to tenants. so, 1 tenant can have many subscriptions, but not vice versa.

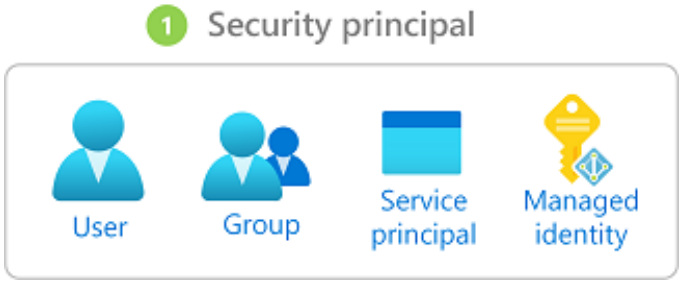
https://itconnect.uw.edu/wares/msinf/aad/new-aad-tenant/

Azure AD – RBAC

Azure role-based access control (Azure RBAC) is a system that provides fine-grained access management of Azure resources. Using Azure RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs. Azure RBAC is an authorization system built on Azure Resource Manager.

You can assign roles using the Azure portal, Azure CLI, Azure PowerShell, Azure SDKs, or REST APIs.

You can assign a role to a **user**, **group**, **service principal**, or **managed identity**. This is also called a *security principal*.



- **User** - An individual who has a profile in Azure Active Directory. You can also assign roles to users in other tenants.
- **Group** - A set of users created in Azure Active Directory. When you assign a role to a group, all users within that group have that role.
- **Service principal** - A security identity used by applications or services to access specific Azure resources. You can think of it as a user identity (username and password or certificate) for an application.
- **Managed identity** - An identity in Azure Active Directory that is automatically managed by Azure. You typically use managed identities when developing cloud applications to manage the credentials for authenticating to Azure services.

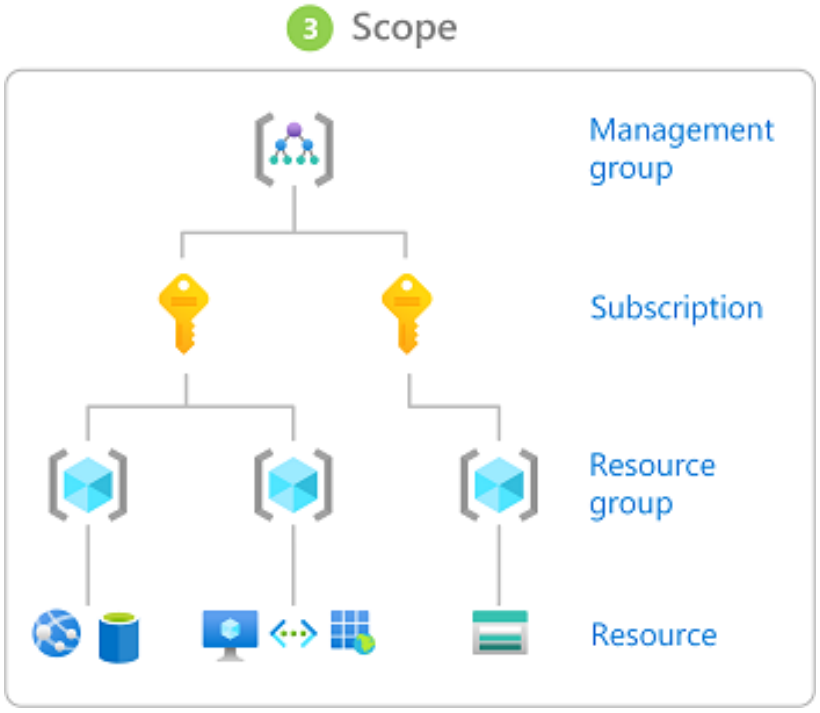
You can apply the roles at 4 different levels:

- Management Group
- Subscription
- Resource Group
- Resource

Each level of hierarchy makes the scope more specific. You can assign roles at any of these levels of scope. The level you select determines how widely the role is applied. Lower levels inherit role permissions from higher levels.

https://docs.microsoft.com/en-us/azure/role-based-access-control/overview

https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles



Azure AD – Built-In Roles

In Azure Active Directory (Azure AD), if another administrator or non-administrator needs to manage Azure AD resources, you assign them an Azure AD role that provides the permissions they need. If you can assign roles to allow adding or changing users, resetting user passwords, managing user licenses, or managing domain names to another user.

https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

How to assign role to a user:

1. Go to Users
2. Select the user onto which you want to assign a role
3. Go Under “Assigned Roles”
4. Click on “Add Assignments”
5. Choose “**Assignment Type**” as “Active”
6. Choose the role which you want to assign

There are two types of “Assignment Type”:

1. **Eligible assignments** require the member of the role to perform an action to use the role. Actions might include performing a multi-factor authentication (MFA) check, providing a business justification, or requesting approval from designated approvers.
2. **Active assignments** don't require the member to perform any action to use the role. Members assigned as active have the privileges assigned to the role at all times.

Azure Active Directory (Azure AD) **Privileged Identity Management** (PIM) can help you manage the eligibility and activation of assignments to privileged access groups in Azure AD. You can assign eligibility to members or owners of the group.

Azure AD – Password Administrator Role

Users with this role have limited ability to manage passwords. This role does not grant the ability to manage service requests or monitor service health. Whether a Password Administrator can reset a user's password depends on the role the user is assigned.

https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#password-reset-permissions

Azure AD – Group Owners

Azure Active Directory (AAD) groups are owned and managed by group owners. Group owners can be users or service principals, and are able to manage the group including membership.

- Only existing group owners or group-managing administrators can assign group owners.
- Group owners aren't required to be members of the group
- It is recommended for every group to have at least one owner
- When a group has no owner, group-managing administrators are still able to manage the group
- Once owners are assigned to a group, the last owner of the group cannot be removed. Please make sure to select another owner before removing the last owner from the group

How to add an owner to a group:

1. Select **"Active Directory"**
2. Select **"Groups"**
3. Choose the **right group** on to which you want to add a group owner
4. In the **Group** > Go to "**Owners"**
5. Click on **"Add owners"**
6. And add the right "**user**" and **"Select"**

Azure AD – Inviting Guest Users

In Azure, you can invite anyone to collaborate with your organization by adding them to your directory as a guest user. Then you can either send an invitation email that contains a redemption link or send a direct link to an app you want to share. Guest users can sign in with their own work, school, or social identities.

You'll add a new guest user to your Azure AD directory via the Azure portal, send an invitation, and see what the guest user's invitation redemption process looks like.

Pre-requisites

1. A role that allows you to create users in your tenant directory, like the Global Administrator role or any of the limited administrator directory roles such as guest inviter or user administrator
2. A valid email account that you can add to your tenant directory, and that you can use to receive the test invitation email

Azure AD – Restore Deleted Users & Groups

In Azure Active Directory, you can restore a user which has been deleted.

- When you delete a user in Azure Active Directory, you have a 30-day window in you can restore the user
- After the 30-day window, the user is permanently deleted, and you will never be able to restore the user. Even MS support wouldn't be able to help you out with this
- Required permissions when it comes to roles to restore the deleted users
  - Global Administrator
  - User Administrator
  - Partner Tier 1 & Tier 2 Support
- You can only restore Office 365 groups

Permanently Delete a User

You can permanently delete a user from your organization without waiting the 30 days for automatic deletion. A permanently deleted user can't be restored by you, another administrator, nor by Microsoft customer support.

How to restore a User:

1. Open Azure Active Directory
2. Select **"Users"**

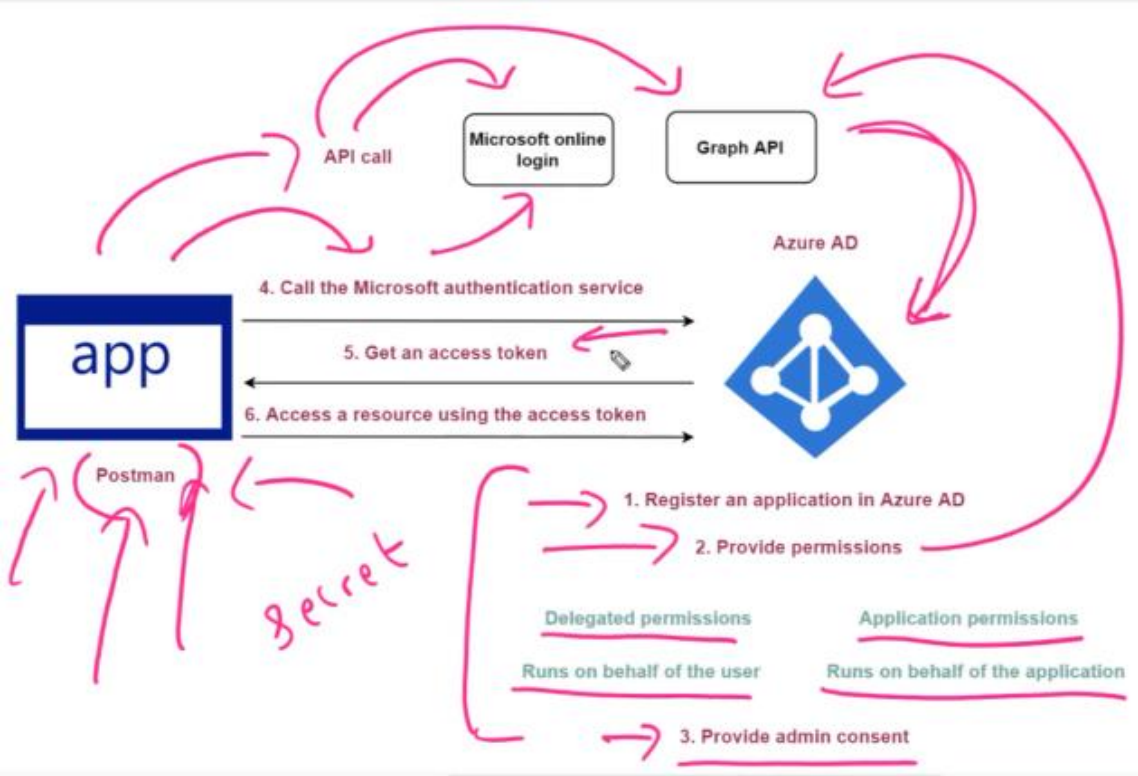
3. Select **"Deleted Users"**
4. **Select the user** you want to restore, and click on **"Restore User"**

Azure AD – Application Registration

If your application wants to fetch user information from Active Directory, below is the way which you do that securely

1. Register your application in Active Directory
2. When the registration happens, AD do two things
   - Application Object
   - Service Principle
3. The service principle is attached to that application object and that service principle is then used to invoke or work with other Azure services
4. There are permissions that's get attached onto that service principle and since that service principle is attached to that application object which in turn gets attached to your application
5. Your application can now via Azure AD go ahead and securely access resources that are part of your Azure subscription

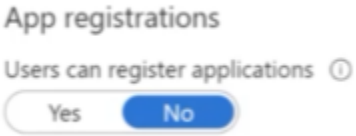
https://www.re-mark-able.net/understanding-azure-active-directory-application-registrations/



Azure AD – Managing Applications in AD

Application-Level Permissions

- By-default all users can create applications in Azure AD
- When a user creates an application in Azure AD, they can manage all aspects of the application
- You can restrict this setting and ensure that by default no one can go ahead and create an application



- You can then assign owners to applications. This way they will be able to manage aspects of an application

- You can then assign users the role of **Application Developer**. This will give the user the ability to create application registrations
- Users with the Application Developer role are added as owners when they create applications in Azure AD
- This role grants permission to consent on one's own behalf when the users can consent to app accessing company data on their behalf setting is set to No
- The **Application Developer** role can't manage enterprise applications
- There is the **Application Administration** role for this
- Users in this role can create and manage all aspects of enterprise applications, application registrations, or enterprise applications
- Here the users assigned to the role are not added as owners when creating new application registrations or enterprise applications
- **Cloud Application Administration** – Similar to Application Administration, but here they can not manage the application proxy feature

Assignment of Owner to an Application

You can delegate the administration of the application object on to a user in Azure AD, so that users should have the ability to go out and change aspect about the authentication or go ahead and generate certificates or secrets for this application so that you can, so in this case you can assign an owner onto an application.

Azure AD – Sign-In & Audit Logs

The Azure Active Directory portal gives you access to three activity logs:

1. **Sign-ins Log** – Information about sign-ins and how your resources are used by your users
2. **Audit Logs** – Information about changes applied to your tenants such as users and group management
3. **Provisioning Logs** – Activities performed by the provisioning service, such as creation of a group in ServiceNow or user imported from Workday

Who can access sign-ins logs:

- A global administrator
- A user in one of the following roles:
  - Security administrator
  - Security reader
  - Global reader
  - Report reader
- You can always **access your own sign-ins** history using this link: https://mysignins.microsoft.com

How to access sign-ins logs:

1. Go to **Active Directory**
2. Go to **"Monitoring**" section
3. Click on **"Sign-ins"**
4. You can see all the **"sign-ins**" logs
5. Second option in **"Monitoring"** section you can see **"Audit Logs"**

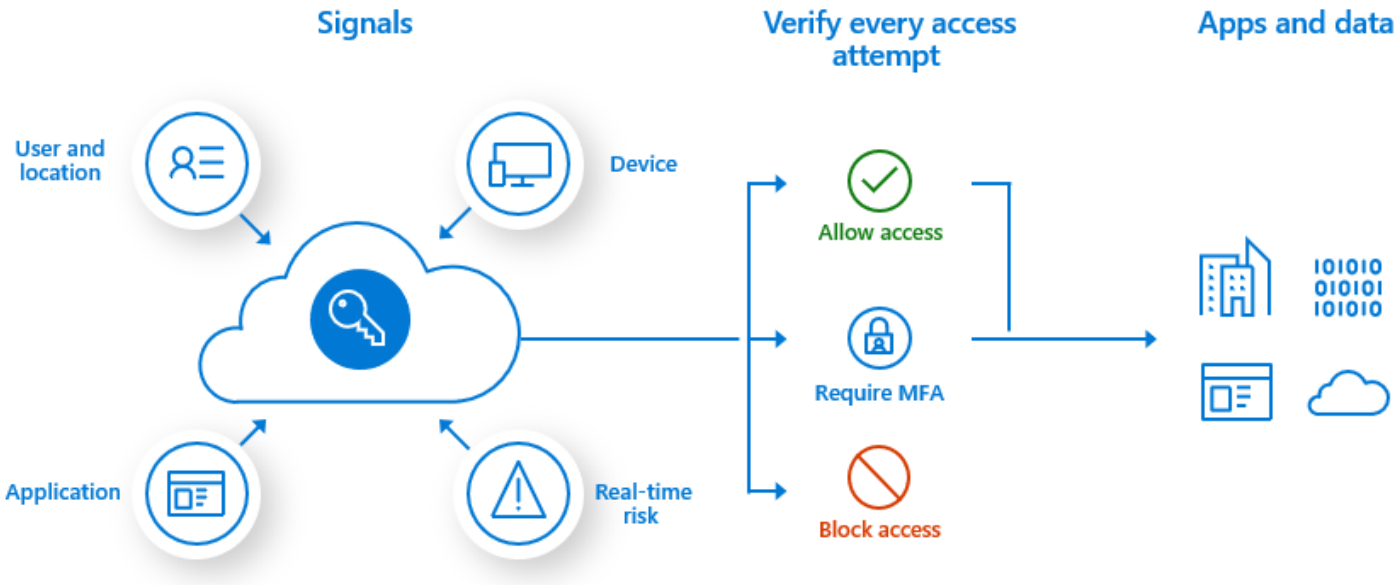
Note: You can get directly get to the sign-in logs using this link:
https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/SignIns

Azure AD – Multi-Factor Authentication

Multi-factor authentication is a process where a user is prompted during the sign-in process for an additional form of identification, such as to enter a code on their cellphone or to provide a fingerprint scan

Azure AD Multi-Factor Authentication works by requiring two or more of the following authentication methods:

- Something you know, typically a password
- Something you have, such as a trusted device that is not easily duplicated, like a phone or hardware key
- Something you are - biometrics like a fingerprint or face scan



Available Verification Methods

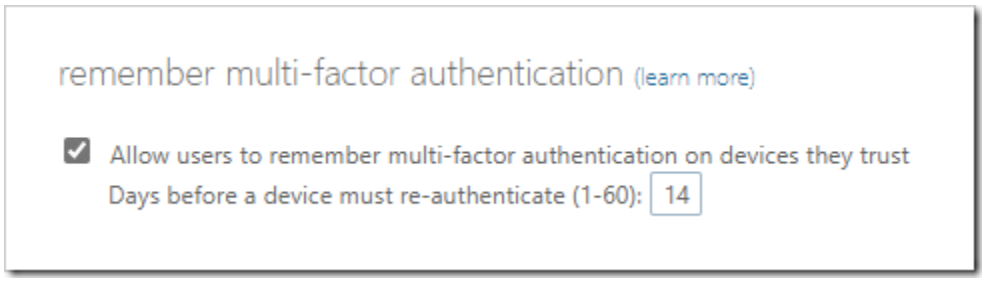
- Microsoft Authenticator app
- OATH Hardware token (preview)
- OATH Software token
- SMS
- Voice call

How to Enable Multi-Factor Authentication

- Browse to **Azure Active Directory** > **Security** > **Identity Protection** > **MFA registration policy**
- Under **Assignments**
- **Users** – Choose **All users** or **Select individuals** and groups if limiting your rollout.
- Optionally you can choose to exclude users from the policy.
- **Enforce Policy - On**
- **Save**

Trusted Devices

You can enable this option to trust the device from which you're connecting to not validate you always for the next 14-days



Trusted IP's

The **Trusted IPs** feature of Azure AD Multi-Factor Authentication **bypasses multi-factor authentication** prompts for users who **sign in from a defined IP address range**. You **can set trusted IP ranges for your on-premises environmen**ts so when users are

in one of those locations, there's no Azure AD Multi-Factor Authentication prompt. The Trusted IPs feature of Azure AD Multi-Factor Authentication requires Azure AD Premium P1 edition.

You can skip MFA from an entire subnet if you want to.

Azure AD – Conditional Access

Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action.

Azure Active Directory (AD) Conditional Access provides added security by allowing access to your applications across cloud and on-premises only from trusted and compliant devices. It is a policy-based approach. You can configure a Conditional Access policy with the required conditions to apply the access controls. Conditions can be device type, users' attributes, operating systems, client application accessed over web or cloud apps, network login location, sign-in risks, and so forth.

A Conditional Access policy works only when modern authentication (ADAL-based) is used with Office 365 resources. You cannot apply a Conditional Access policy to on-premises applications, such as local SharePoint or Exchange.

Using Conditional Access policies, you can accomplish the following requirements:

- Restricting access to protected applications only from managed and trusted devices: corporate devices and BYOD
- Restricting access only from compliant devices with appropriate security profile
- Securing the enterprise data outside the network boundary
- Managing devices:
  - Visibility of the number of devices accessing the application
  - Visibility of the security strength of devices accessing the application
  - Assigning and revoking devices
  - Defining a group of users or devices and applying policies

Azure AD – Identity Protection

This is a service that can be used to detect any identity-based risks

Identity Protection is a tool that allows organizations to accomplish three tasks:

1. Automate the detection and remediation of identity-based risks
2. Investigate risks with the identities
3. Export risk detection data to your SIEM

Risk Detection Types:

- Anonymous IP address use
- Atypical travel
- Malware linked IP address
- Unfamiliar sign-in properties
- Leaked credentials
- Password spray

Remediation:

The risk signals can trigger remediation efforts such as requiring users to:

- Perform Azure AD Multi-factor Authentication
- Reset their passwords
- Blocking the user until an administrator takes an action

Risk Investigation and Detections:

There are three key reports that administrators use for investigations in Identity Protection:

- Risky users
- Risky sign-ins
- Risk detections

Risk Levels:

Identity Protection categorizes risk into three tiers:

- Low
- Medium
- High

Azure AD – Access Reviews

Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access.

Access Reviews feature is available in **Identity Governance** service

Licensing Requirements

This feature requires an Azure AD Premium P2 License

Your directory needs at least as many Azure AD Premium P2 licenses as the number of employees who will be performing the following tasks:

- Member users who are assigned as reviewers
- Member users who perform a self-review
- Member users as group owners who perform an access review
- Member users as application owners who perform an access review

Where to create review:

Access rights of users	Reviewers can be	Review created in	Reviewer experience
Security group members Office group members	Specified reviewers Group owners Self-review	Azure AD access reviews Azure AD groups	Access panel
Assigned to a connected app	Specified reviewers Self-review	Azure AD access reviews Azure AD enterprise apps (in preview)	Access panel
Azure AD role	Specified reviewers Self-review	Azure AD PIM	Azure portal
Azure resource role	Specified reviewers Self-review	Azure AD PIM	Azure portal

Azure AD – Privileged Identity Management (PIM)

A Privileged Identity Management (PIM) is a service in Azure Active Directory (Azure AD) that enables you to manage, control, and monitor access to important resources in your organization. These resources include resources in Azure AD, Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune. This service is used to control the access permissions for your users.

To this feature, you should have **Azure AD Premium P2 license**

Here are some of the **key features of Privileged Identity Management**:

- Provide **just-in-time** privileged access to Azure AD and Azure resources
- Assign **time-bound** access to resources using start and end dates
- Require **approval** to activate privileged roles
- Enforce **multi-factor authentication** to activate any role
- **Use justification** to understand why users activate
- **Get notifications** when privileged roles are activated
- **Conduct access reviews** to ensure users still need roles
- **Download audit history** for internal or external audit
- Prevents removal of the **last active Global Administrator** role assignment

Azure AD – Connect

Azure AD Connect is the Microsoft tool designed to meet and accomplish your hybrid identity goals. It lets you connect your on-premises Active Directory to Azure Active Directory. You can sync all your on-prem AD users, groups, devices, etc. with Azure AD.

Important Notes:

1. The Azure AD Connect synchronization service is used to synchronize identity data between your on-premises environment and Azure AD
2. There are two components for this service:
   - **Azure AD Connect Sync Component** (also called Sync Engine) – This is installed on the Windows machine on on-premises environment.
   - **Azure AD Connect Sync Service** – This service runs in Azure AD
3. To use Azure AD Connect, you need to have the following pre-requisites in place
   - An Azure AD tenant
   - You need to add and verify your domain in Azure AD
   - Use the IdFix tool to identify errors such as a duplicate and formatting problems in your on-premises directory

IdFix can be used to identify any errors in your on-premises environment when it comes to definition of users and groups. It could then go ahead and rectify those errors before the synchronization can occur of the identities from your on-premises environment onto Azure AD. The Azure AD

4. The Azure AD Connect sync component must be installed on Windows Server 2012 Standard or better. The server must have the full GUI installed. The server must be domain joined. This component must not be installed on the domain controller.

Few more important notes:

1. If you create or define a user in Azure AD, the user will not be reflected in on-premises Active Directory. The Azure AD Connect service is meant to sync identities from on-premises Active Directory to Azure AD, not the other way around
2. If you change your user's password in Azure AD, will the password get synchronized back to Active Directory. This will only happen if you enable another feature known as **Password Write Back**

Configuration Requirements

1. During the configuration of the Azure AD Connect sync component, you need to use an
   - Azure AD Global Administrator account for the Azure AD tenant. The account should be a school or organization account and cannot be a Microsoft account
   - An Enterprise Administrator account for the on-premises Active Directory
2. The Azure AD Connect server needs DSN resolution for both intranet and internet. The DNS server must be able to resolve names both to your on-premises Active Directory and the Azure AD endpoints
3. The Azure AD Connect sync component requires a SQL Server database for storing identity data. By default, the installation of Azure AD Connect will install SQL Server 2012 Express LocalDB

Synchronization Techniques

There are two types of synchronization techniques:

1. **Password Hash Synchronization**

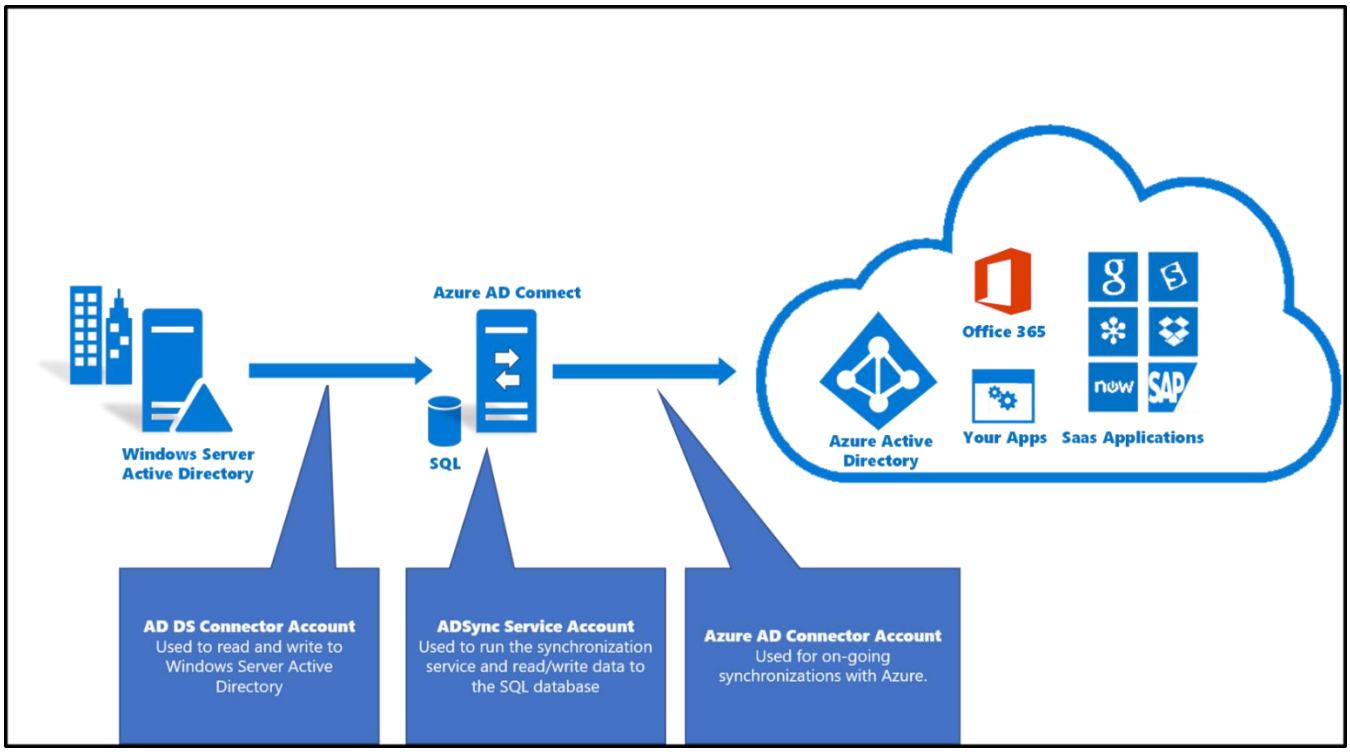
Here the Azure AD Connect synchronizes a hash, of the hash, of a user's password from an on-premises Active Directory instance to cloud-based Azure AD instance

Advantage:

- The advantage is that you only need to maintain one password for both authentication in your on-premises environments and in the cloud
- If you change a user's password in the on-premises Active Directory setup, the password will be synched onto Azure AD

2. **Pass-through Authentication**

This is kind of similar to password hash synchronization, but here the user's passwords are directly validated against the on-premises Active Directory. This allows organization to enforce their on-premises Active Directory security and password policies



Azure AD – Passwordless Authentication

Passwordless authentication methods are more convenient because the password is removed and replaced with something you have; plus, something you are or something you know. Microsoft global Azure and Azure Government offer the following three passwordless authentication options that integrate with Azure Active Directory (Azure AD):

- Windows Hello for Business
- Microsoft Authenticator app
- FIDO2 security keys

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless

Azure – Transferring Ownership of Subscriptions

Few notes:

1. You can transfer billing ownership of an Azure subscription onto another account

2. When you transfer billing ownership to the other account, the administrators of the new account have permissions for the billing tasks
3. They would be able change the payment method, view charges and cancel the subscription
4. You can also transfer a subscription to another Azure account when you transfer the billing ownership
5. Here the resources along with your subscription will be moved to the new account
6. But the users, groups or service principals who has role-based access will lose access to the resources

Azure – Virtual Machine Security

An Azure virtual machine gives you the flexibility of virtualization without having to buy and maintain the physical hardware that runs the virtual machine. You can build and deploy your applications with the assurance that your data is protected and safe in highly secure datacenters.

With Azure, you can build security-enhanced, compliant solutions that:

- Protect your virtual machines from viruses and malware
- Encrypt your sensitive data
- Secure network traffic
- Identify and detect threats
- Meet compliance requirements

Using Role-Based Access Control

1. Control who has access to your virtual machine
2. Control who can stop or start the virtual machine
3. Control who can change the properties of the virtual machine

Protect Against Malware

1. Install an anti-malware solution that can help identify and remove viruses
2. You can use Microsoft Antimalware solution
3. You can also use other vendor-based solutions, like McAfee, Symantec, etc.

Update Management for Virtual Machines

1. You manage the updates for your virtual machines
2. Always deploy the latest security updates
3. If you are deploying a new virtual machine, always use the latest image which has all the latest security updates

Azure Security Center

1. This tool can give you several recommendations on how to improve the security posture of your virtual machines
2. It can also actively monitor for any threats to your virtual machines
3. You can use features such as Just-in-time VM access to give access to your virtual machines

Azure Disk Encryption

1. Encrypt the disks on your virtual machine using Azure Disk Encryption
2. This can be used to encrypt both Windows and Linux based virtual machines

Use Network Security Groups

1. Ensure to restrict inbound and outbound traffic via Network Security Rules
2. Continuously review the rules you have in place

Virtual Machine Backup

1. Natively manage your entire backup estate from a central console using Backup Centre
2. Automatically onboard and configure Azure Backup on production virtual machines (VMs) using Azure Automanage

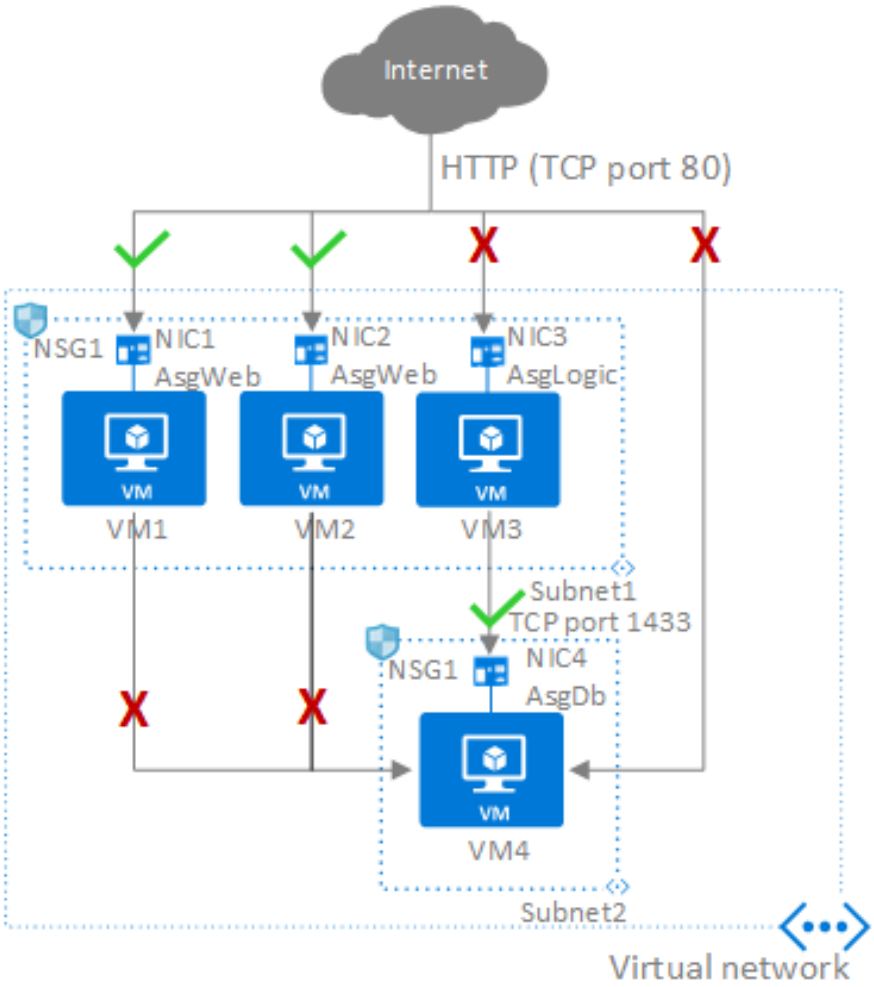
3. Use APIs, PowerShell and Azure CLI to automate Backup policy and security configurations

Azure Site Recovery

1. Simplifies your BCDR strategy
2. It provides flexible replication
3. Supports failover and recovery
4. Eliminates secondary datacenters
5. Integrates with existing BCDR technologies

Azure – Application Security Groups

An Azure Application security groups enable you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups. You can reuse your security policy at scale without manual maintenance of explicit IP addresses. The platform handles the complexity of explicit IP addresses and multiple rule sets, allowing you to focus on your business logic.



In the previous picture, NIC1 and NIC2 are members of the AsgWeb application security group. NIC3 is a member of the AsgLogic application security group. NIC4 is a member of the AsgDb application security group. Though each network interface in this example is a member of only one network security group, a network interface can be a member of multiple application security groups, up to the Azure limits. None of the network interfaces have an associated network security group. NSG1 is associated to both subnets and contains the following rules:

Allow-HTTP-Inbound-Internet – This rule is needed to allow traffic from the internet to the web servers. Because inbound traffic from the internet is denied by the **DenyAllInbound** default security rule, no additional rule is needed for the *AsgLogic* or *AsgDb* application security groups.

ALLOW-HTTP-INBOUND-INTERNET

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
100	Internet	*	AsgWeb	80	TCP	Allow

Deny-Database-All – Because the **AllowVNetInBound** default security rule allows all communication between resources in the same virtual network, this rule is needed to deny traffic from all resources.

DENY-DATABASE-ALL

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
120	*	*	AsgDb	1433	Any	Deny

Allow-Database-BusinessLogic – This rule allows traffic from the *AsgLogic* application security group to the *AsgDb* application security group. The priority for this rule is higher than the priority for the *Deny-Database-All* rule. As a result, this rule is processed before the *Deny-Database-All* rule, so traffic from the *AsgLogic* application security group is allowed, whereas all other traffic is blocked.

ALLOW-DATABASE-BUSINESSLOGIC

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
110	AsgLogic	*	AsgDb	1433	TCP	Allow

The rules that specify an application security group as the source or destination are only applied to the network interfaces that are members of the application security group. If the network interface is not a member of an application security group, the rule is not applied to the network interface, even though the network security group is associated to the subnet.

Application security groups have the following constraints:

- There are limits to the number of application security groups you can have in a subscription, as well as other limits related to application security groups.
- All network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in. For example, if the first network interface assigned to an application security group named AsgWeb is in the virtual network named VNet1, then all subsequent network interfaces assigned to ASGWeb must exist in VNet1. You cannot add network interfaces from different virtual networks to the same application security group.
- If you specify an application security group as the source and destination in a security rule, the network interfaces in both application security groups must exist in the same virtual network. For example, if AsgLogic contained network interfaces from VNet1, and AsgDb contained network interfaces from VNet2, you could not assign AsgLogic as the source and AsgDb as the destination in a rule. All network interfaces for both the source and destination application security groups need to exist in the same virtual network.

What's ASG?

Application Security Groups helps to manage the security of Virtual Machines by grouping them according the applications that runs on them. It is a feature that allows the application-centric use of Network Security Groups. This approach allows for the grouping of Virtual Machines logically, irrespective of their IP address or subnet assignment within a Virtual Network.

ASGs are used within a NSG to apply a network security rule to a specific workload or group of VMs — defined by ASG worked as being the “network object” & explicit IP addresses are added to this object. This provides the capability to group VMs into associated groups or workloads, simplifying the NSG rule definition process. Another great use of this is for scalability, creating the virtual machine and assigning the newly created virtual machine to its ASG will provide it with all the NSG rules in place for that specific ASG — zero distribution to your service!

ASG Key Points

- Azure Security Groups allow us to define fine-grained network security policies based on workloads, centralized on applications, instead of explicit IP addresses.
- ASGs provide the capability of grouping the VMs with monikers and secure our applications by filtering traffic.
- By implementing granular security traffic controls, we can improve isolation of workloads and can protect them individually.
- If a breach occurs, this method limits the potential impact of lateral exploration of our networks from hackers.
- The security definition is simplified when using the ASGs.
- We can define application groups by providing a moniker descriptive name that fits our architecture.
- We can use it the way we want i.e. for applications, systems, environments, workload types, tiers or even any kind of roles.
- We can define a single collection of rules using ASGs and NSGs. We just have to apply a single NSG to our entire virtual network on all subnets.
- This way by defining a single NSG gives us the full visibility on all traffic policies and a single place for management. Hence, it reduces the tedious job.

Benefits of using ASGs:

- We can scale at our own pace. While deploying the VMs, we can make them members of the appropriate ASGs.
- If the VM is running more than one workload, we can simply assign multiple ASGs.
- The access is always granted based on workloads.
- We don’t have to worry about security definition ever again.
- The most important point to be noted is that we can implement a zero-trust model. Meaning, we can limit access to the application flows that are explicitly permitted.
- ASGs introduce the ability to deploy multiple applications within the same subnet and also isolate traffic based on ASGs.
- With the use of Azure Security Groups, you can reduce the number of Network Security Groups in our subscription.
- In some cases, it gets so helpful that you can use a single NSG for multiple subnets of your virtual network.

For more information, refer: https://medium.com/awesome-azure/azure-application-security-group-asg-1e5e2e5321c3
https://azure.microsoft.com/en-in/blog/applicationsecuritygroups/
https://blog.kloud.com.au/2017/11/21/azure-application-security-groups/

Azure – Front Door

An Azure Front Door is a global, scalable entry-point that uses the Microsoft global edge network to create fast, secure, and widely scalable web applications. With Front Door, you can transform your global consumer and enterprise applications into robust, high-performing personalized modern applications with contents that reach a global audience through Azure.

Azure Front Door is an Application Delivery Network (ADN) as a service, offering various layer 7 load-balancing capabilities for your applications. It provides dynamic site acceleration (DSA) along with global load balancing with near real-time failover. It is a highly available and scalable service, which is fully managed by Azure.

Azure Front Door is a secure cloud CDN service that helps cyber security teams accelerate content delivery while protecting apps, APIs, and websites from cyber threats. It combines intelligent threat protection and modern CDN technology in a tightly integrated service that's easy to set up, deploy, and manage.

Azure Front Door Standard/Premium is a fast, reliable, and secure modern cloud CDN that uses the Microsoft global edge network and integrates with intelligent threat protection. It combines the capabilities of Azure Front Door, Azure Content Delivery Network (CDN) standard, and Azure Web Application Firewall (WAF) into a single secure cloud CDN platform.

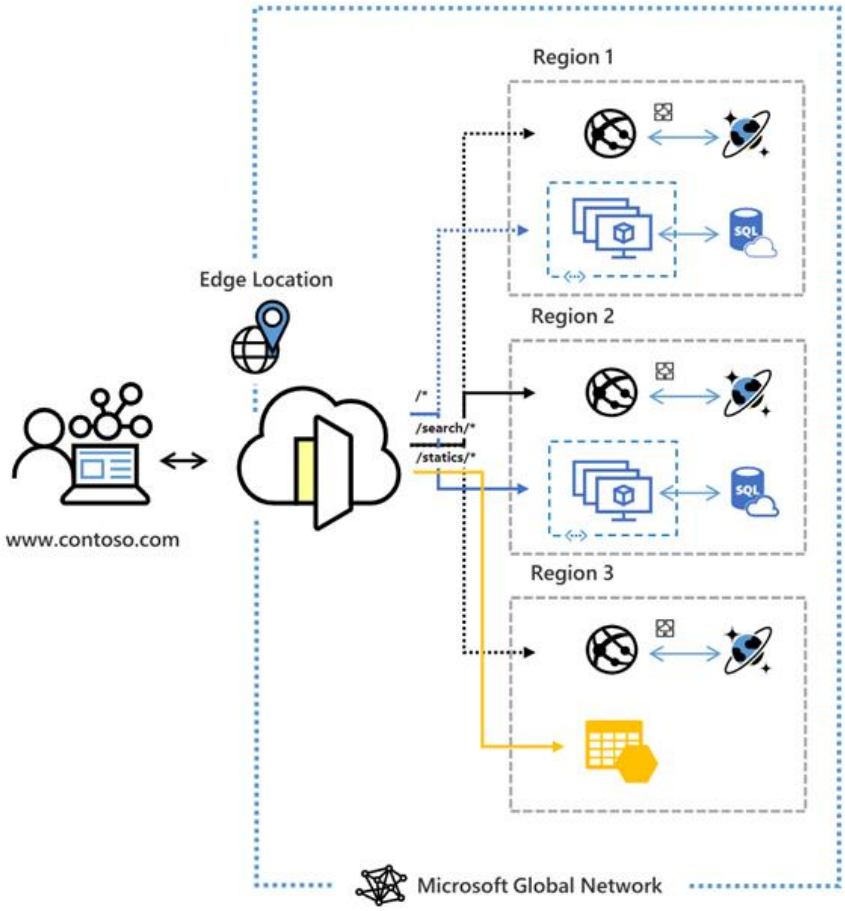
With Azure Front Door Standard/Premium, you can transform your global consumer and enterprise applications into secure and high-performing personalized modern applications with contents that reach a global audience at the network edge close to the user. It also enables your application to scale out without warm-up while benefitting from the global HTTP load balancing with instant failover.

A brief about working:

The underlying technology in Azure Front Door has been in place inside of Microsoft for the past five years where it has enabled scaling and protection for many popular Microsoft services, including Office 365, Bing, Xbox, LinkedIn and Microsoft Teams. Microsoft provided a public preview of the technology back in September 2018, and is now available to all customers.

For organizations that have web applications with global reach, the performance of these applications can be impacted by the proximity of the consumer. In order to provide a better, and more consistent experience, organizations may leverage Content Delivery Networks (CDNs) which have several distribution points and deliver content to consumers faster due to proximity and optimized connections.

Azure Front Door takes advantage of the anycast protocol, which goes beyond providing traditional CDN capabilities by also providing advanced security capabilities, including preventing Distributed Denial of Service (DDoS) attacks.



Important Notes:

1. This is a routing service that helps accelerate your application performance by routing based on performance of your endpoints
2. This service works at Layer 7 or http/https

3. This service will route your client request to the fastest and most available application backend
4. An application backend is any Internet facing service that could be hosted inside or outside of Azure

Features:

1. **URL-based Routing**
   - Here you can route traffic to your backend servers based on the URL paths of the request
   - If you have a web application hosted via your domain URL of http://cloudlearninghub.com , you could direct request for http://cloudlearninghub.com/images* to one set of servers and other requests for http://cloudlearninghub.com/videos* to another set of servers
2. **Multi-site hosting**
   - Here you can configure more than one website on the same Front Door configuration
3. **Session Affinity**
   - Here you can keep a user session attached to the same application backend
4. **SSL Termination**
   - Here SSL connections can be terminated at the Front Door itself rather than being processed by the backend servers
5. **Web Application Firewall**
   - You can use this feature to help protect your web application from internet-based attacks
6. Accelerated application performance by using split TCP-based anycast protocol
7. Intelligent health probe monitoring and load balancing among origins
8. Define your own custom domain with flexible domain validation
9. Application security with integrated Web Application Firewall (WAF)
10. SSL offload and integrated certificate management
11. Secure your origins with Private Link
12. Customizable traffic routing and optimizations via Rule Set
13. Built-in reports with all-in-one dashboard for both Front Door and security patterns
14. Real-time monitoring and alerts that integrate with Azure Monitoring
15. Logging for each Front Door request and failed health probes
16. Native support of end-to-end IPv6 connectivity and HTTP/2 protocol

Pricing

Azure Front Door has two SKU's:

- Standard
- Premium

https://docs.microsoft.com/en-us/azure/frontdoor/standard-premium/tier-comparison

Azure – Application Gateway

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. Traditional load balancers operate at the transport layer (OSI layer 4 - TCP and UDP) and route traffic based on source IP address and port, to a destination IP address and port.

Application Gateway can make routing decisions based on additional attributes of an HTTP request, for example URI path or host headers. For example, you can route traffic based on the incoming URL. So, if /images are in the incoming URL, you can route traffic to a specific set of servers (known as a pool) configured for images. If /video is in the URL, that traffic is routed to another pool that's optimized for videos.

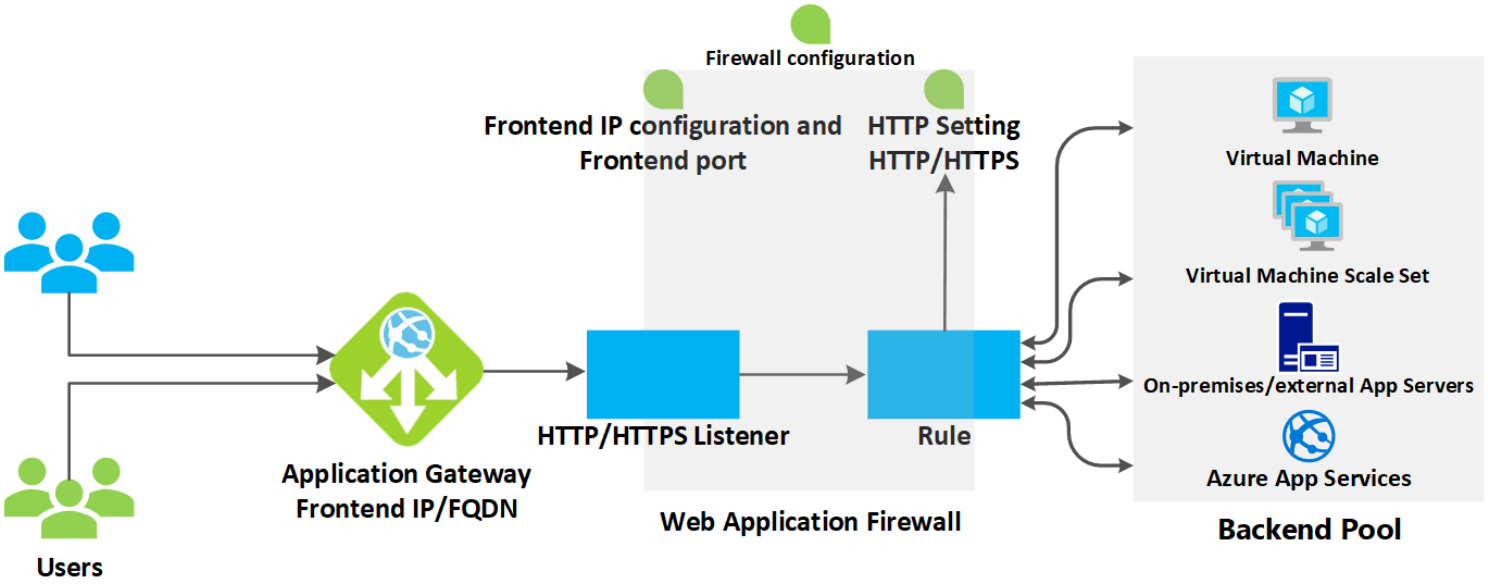
This type of routing is known as application layer (OSI layer 7) load balancing. Azure Application Gateway can do URL-based routing and more.

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications.

Features of Azure Application Gateway

https://docs.microsoft.com/en-us/azure/application-gateway/features

- Secure Sockets Layer (SSL/TLS) termination
- Autoscaling
- Zone redundancy
- Static VIP
- Web Application Firewall
- Ingress Controller for AKS
- URL-based routing
- Multiple-site hosting
- Redirection
- Session affinity
- WebSocket and HTTP/2 traffic
- Connection draining
- Custom error pages
- Rewrite HTTP headers and URL
- Sizing



Important Notes:

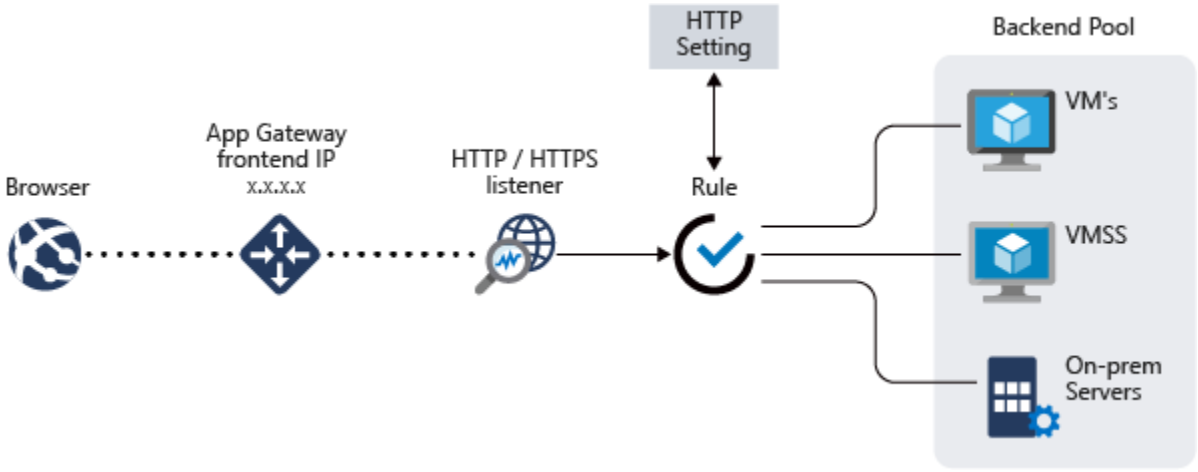
1. This service is a web traffic load balancer that is used to distribute traffic to web applications
2. The web applications can reside on Virtual Machines, Virtual Machine Scale sets, or even on on-premises servers
3. The application gateway is an OSI Layer 7 load balancer
4. You can also enable Autoscaling for your Application Gateway resource
5. This allows the Application Gateway to scale up or scale down based on the traffic load patterns
6. You can also enable the Web Application Firewall feature for the Application Gateway resource
7. You can also enable session affinity which allows a user session to directed to the same server for processing. If the state of the user session is stored on the server, then this can be a useful feature.

Different Components of the Application Gateway

1. **Frontend IP address** – Users will hit the Application Gateway via the Frontend IP address
2. **Listener** – This is a logical entity that checks for incoming connection requests. There can be multiple listeners attached to an application gateway.
   There are two types of listeners:
   - **Basic** – In this the listener listens to single domain site

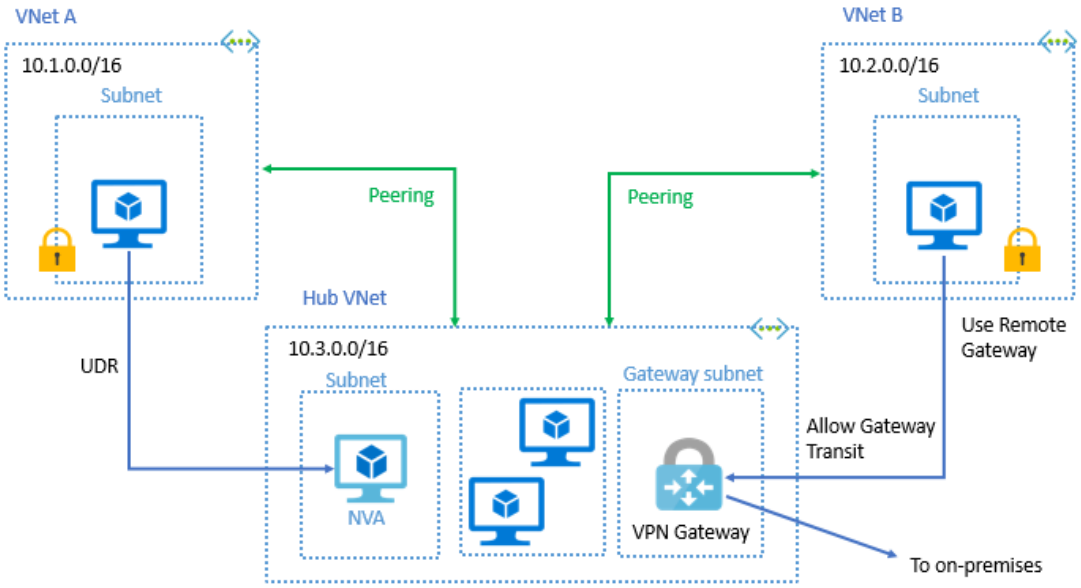
- **Multi-site** – In this the listeners maps to multiple domain site

3. **Routing Rules** – This is used to route the traffic from the listener to the backend pool
   There are two types of routing rules:
   - **Basic** – In this all the requests are routed to backend pool directly
   - Path-based – In this request are routed to the backend pool based on the URL in the request
4. **Backend Pools** – These can be Network Interface Cards, Virtual Machine Scale Sets, Public or Private IP addresses, FQDN or backends such as App Service
5. **Health Probes** – This defines how the application gateway will monitor the health of the resources in the backend pool



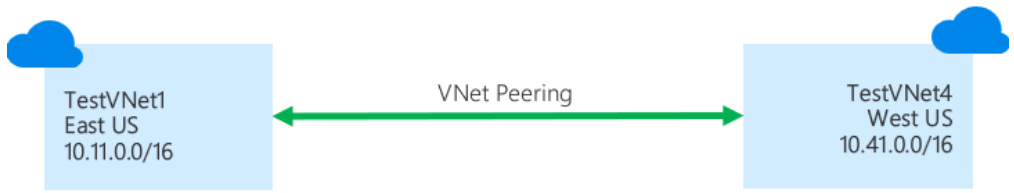
Azure – Virtual Network Peering

Virtual network peering enables you to seamlessly connect two or more Virtual Networks in Azure. The virtual networks appear as one for connectivity purposes. The traffic between virtual machines in peered virtual networks uses the Microsoft backbone infrastructure. Like traffic between virtual machines in the same network, traffic is routed through Microsoft's private network only.



Azure supports the following types of peering:

- **Virtual network peering** – Connect virtual networks within the same Azure region
- **Global virtual network peering** – Connecting virtual networks across Azure regions



Benefits of Virtual Network Peering

- Network traffic of peered Virtual networks become private.
- Virtual network peering in Azure allows transferring data across Azure deployment models, subscriptions, and other regions.
- No downtime issues in global Azure virtual network peering.
- It configures the connection with high bandwidth Low latency in the VNet region.
- Global VNet peering has erased the need for VNet to VNet peering Azure configuration. It disabled the use of VPN encryption, public internet, or any gateways.
- This is a very cost-effective and Time-saving process that controlling the backup, traffic, sharing from different regions

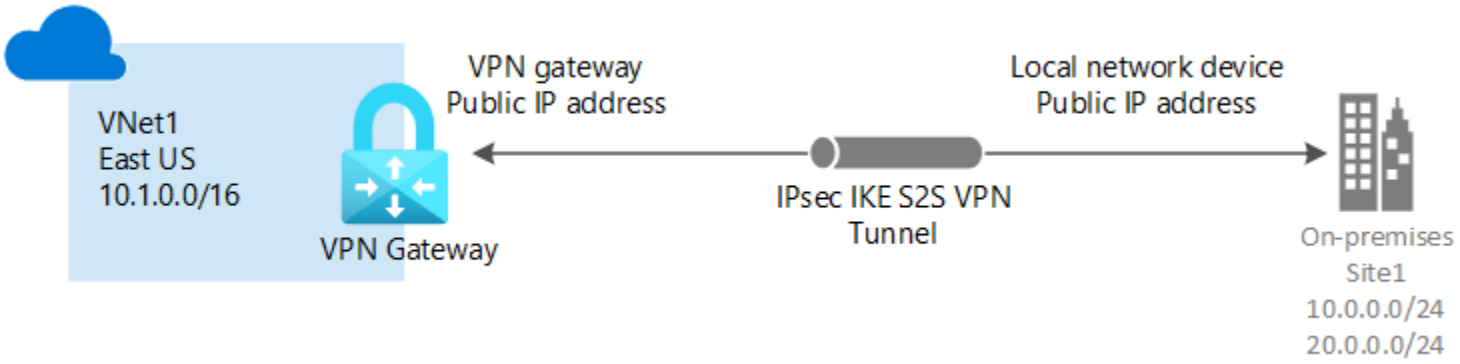
Azure – Point to Site VPN Connectivity

A Point-to-Site (P2S) VPN gateway connection lets you create a secure connection to your virtual network from an individual client computer. A P2S connection is established by starting it from the client computer. This solution is useful for telecommuters who want to connect to Azure VNets from a remote location, such as from home or a conference. P2S VPN is also a useful solution to use instead of S2S VPN when you have only a few clients that need to connect to a VNet.

Protocol Used by P2S

Point-to-site VPN can use one of the following protocols:

- **OpenVPN® Protocol**, an SSL/TLS based VPN protocol. A TLS VPN solution can penetrate firewalls, since most firewalls open TCP port 443 outbound, which TLS uses. OpenVPN can be used to connect from Android, iOS (versions 11.0 and above), Windows, Linux, and Mac devices (macOS versions 10.13 and above)
- **Secure Socket Tunneling Protocol (SSTP)**, a proprietary TLS-based VPN protocol. A TLS VPN solution can penetrate firewalls, since most firewalls open TCP port 443 outbound, which TLS uses. SSTP is only supported on Windows devices. Azure supports all versions of Windows that have SSTP and support TLS 1.2 (Windows 8.1 and later)
- **IKEv2 VPN**, a standards-based IPsec VPN solution. IKEv2 VPN can be used to connect from Mac devices (macOS versions 10.11 and above)



Client Configuration Requirements

Users use the native VPN clients on Windows and Mac devices for P2S. Azure provides a VPN client configuration zip file that contains settings required by these native clients to connect to Azure.

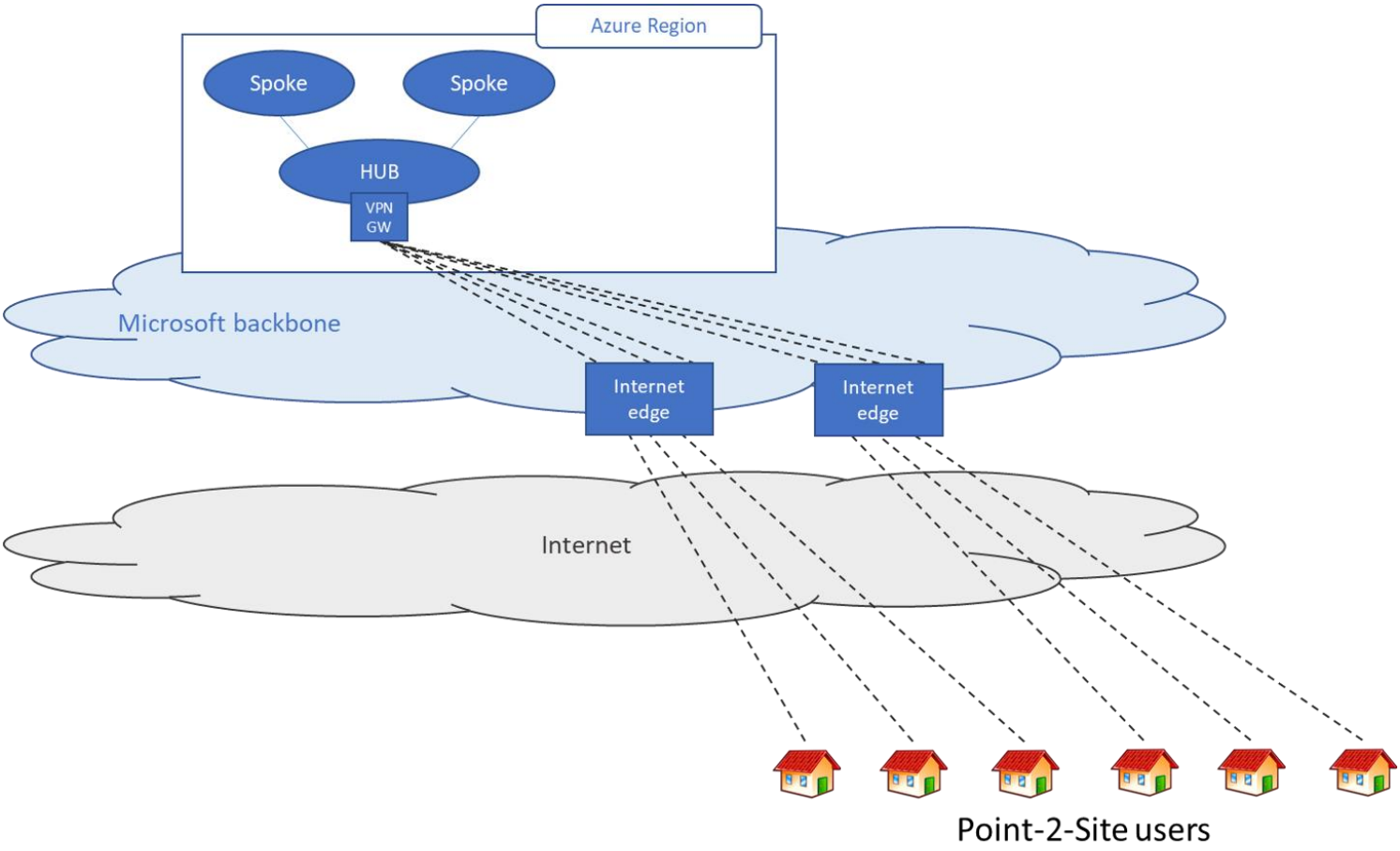
- For Windows devices, the VPN client configuration consists of an installer package that users install on their devices
- For Mac devices, it consists of the mobileconfig file that users install on their devices

The zip file also provides the values of some of the important settings on the Azure side that you can use to create your own profile for these devices. Some of the values include the VPN gateway address, configured tunnel types, routes, and the root certificate for gateway validation.

Scenarios

1. **Users need access to resources in Azure only**

In this scenario, the remote users only need to access to resources that are in Azure

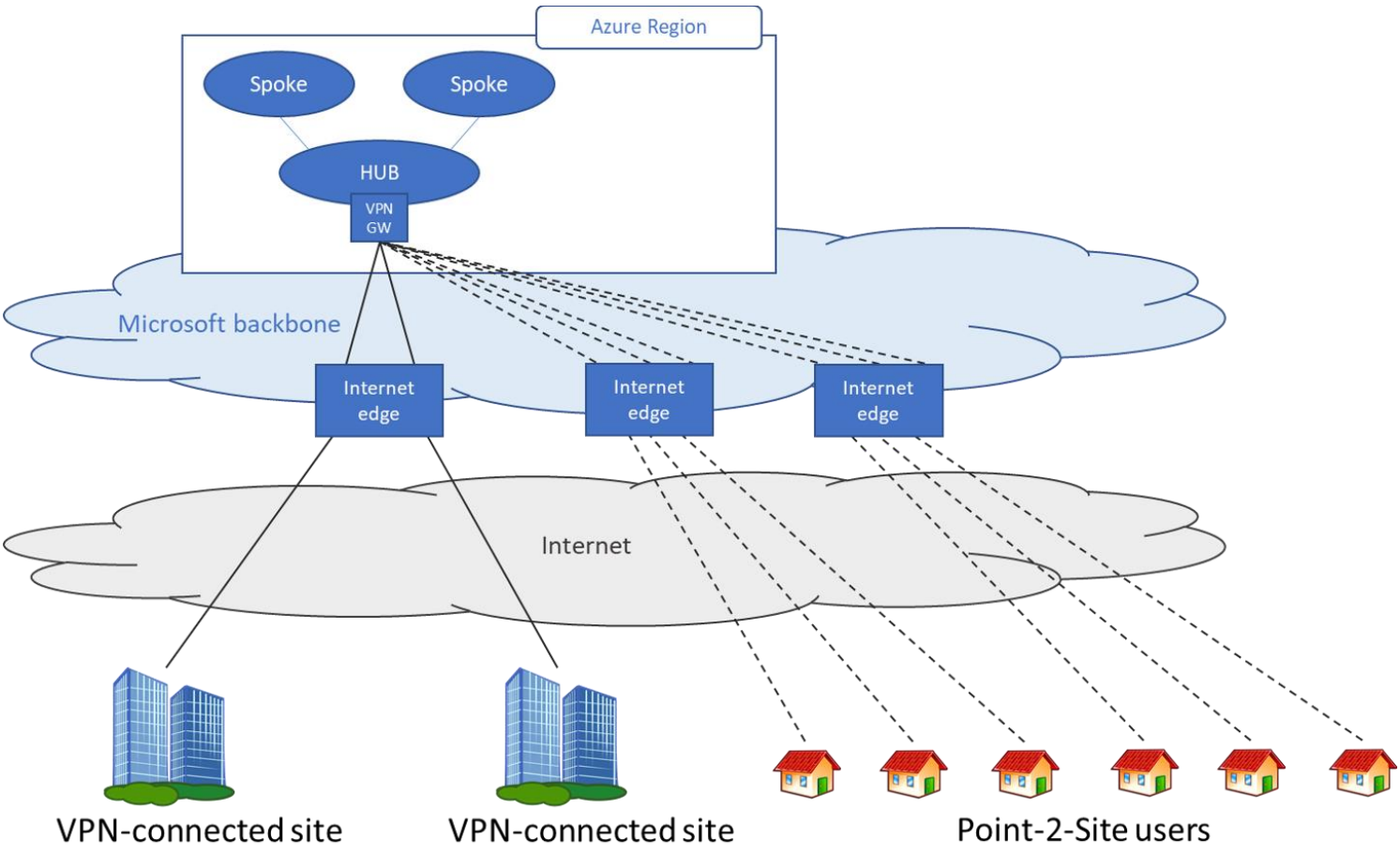


At a high level, the following steps are needed to enable users to connect to Azure resources securely:

1. Create a virtual network gateway (if one does not exist)
2. Configure point-to-site VPN on the gateway
   - For certificate authentication, follow this link
   - For OpenVPN, follow this link
   - For Azure AD authentication, follow this link
   - For troubleshooting point-to-site connections, follow this link
3. Download and distribute the VPN client configuration
4. Distribute the certificates (if certificate authentication is selected) to the clients
5. Connect to Azure VPN

2. **Users need access to resources in Azure and/or on-premises resources**

In this scenario, the remote users need to access to resources that are in Azure and in the on-premises data centers



At a high level, the following steps are needed to enable users to connect to Azure resources securely:

1. Create a virtual network gateway (if one does not exist)
2. Configure point-to-site VPN on the gateway (see Scenario 1)
3. Configure a site-to-site tunnel on the Azure virtual network gateway with BGP enabled
4. Configure the on-premises device to connect to Azure virtual network gateway
5. Download the point-to-site profile from the Azure portal and distribute to clients

How to setup Point-to-Site VPN Connection

So, what it goes into establishing a point to site VPN connection

On Azure Side

1. As part of your virtual network, you have to create a “Gateway Subnet”. This Gateway Subnet will be used as a gateway between your workstation and a virtual network
2. Once the “Gateway Subnet” is created, you have to create “Virtual Network Gateway”, it is a separate resource available in Azure
3. You can only create the Virtual Network Gateway and attach it your virtual network, if you have the gateway subnet in place
4. Once the “Virtual Network Gateway” is ready then you can go ahead and configure a **Point to Site VPN connection**

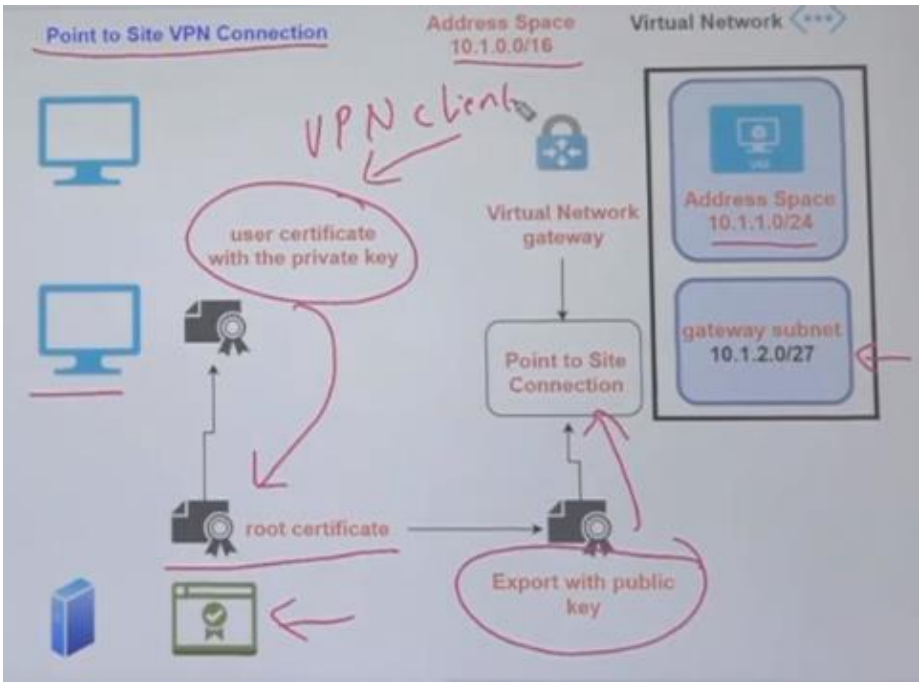
On workstation/on-premises Side

1. In order to go ahead and connect securely using the Point to site VPN connection, you have to go ahead and have certificates in place
2. You could go ahead and create your own self signed certificate, or your company might already have a private certificate provider

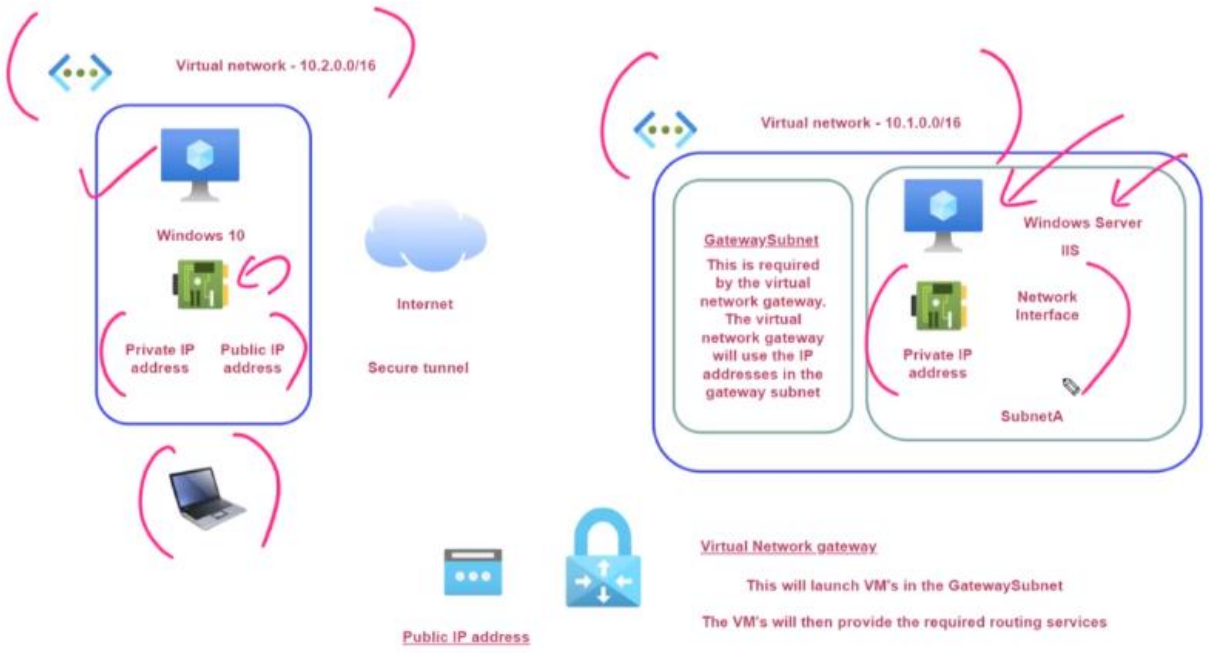
3. Your private certificate provider could go ahead and generate a root certificate, this generation of certificate on the certificate provider can be done by you itself on their portal
4. Once you have the root certificate, you have to go ahead and export the certificate with the Public Key and then upload it to the Point to Site connection
5. On Azure end, Azure has to authenticate the connection based on the certificate
6. Now you want to ensure a workstation can connect using the Point to site connection on the client/workstation machine you have to have a “user certificate” with a “private key” in place that user certificate is generated from the root certificate

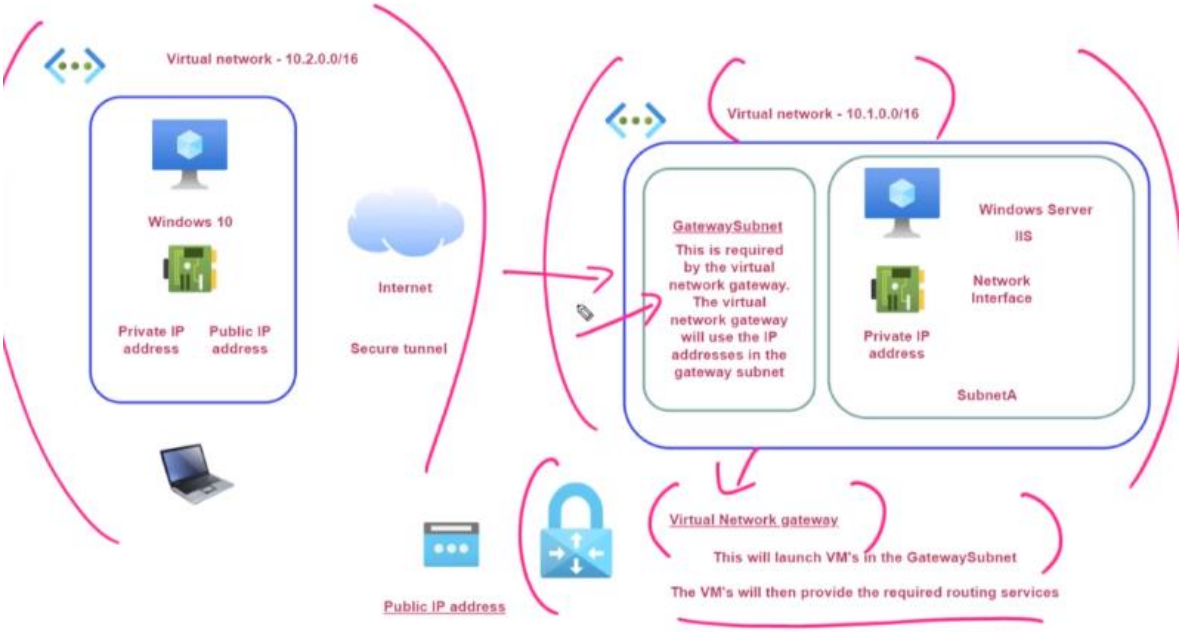
Now from Azure you can download the VPN client and then the VPN client can be used to establish a point to site connection

Now if you want another workstation to also establish a point to site connection make sure the VPN client is also on that workstation and ensure that the same user certificate is also available on the client workstation



Point to Site VPN Connection – Lab/Simulation





The virtual network gateway has to have a Public IP address, because the traffic from the client workstation when it establishes a point to site VPN connection.

The traffic from workstation will flow from the internet then will hit the public IP address of the virtual network gateway, and the virtual network gateway will route the traffic via gateway subnet on to your Azure virtual network resources.

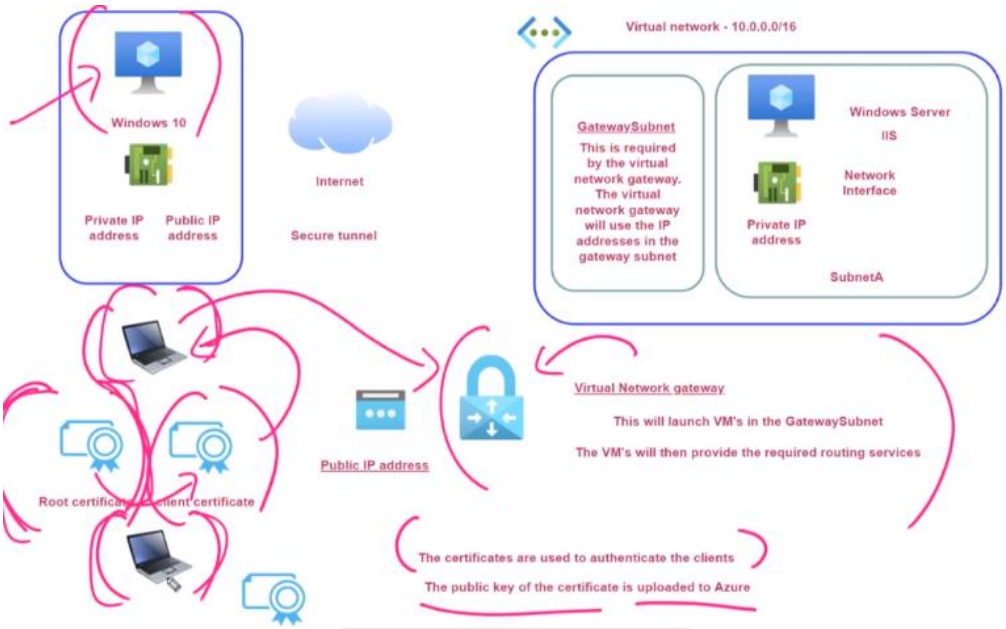
The virtual network gateway takes about 30-45 minutes to get functional ready after creation of it.

VPN Gateway Type

There are multiple options to choose which version/kind of VPN to select in Virtual Network Gateway, and generations as well. Versions are different with pricing and offering the speed of the VPN.

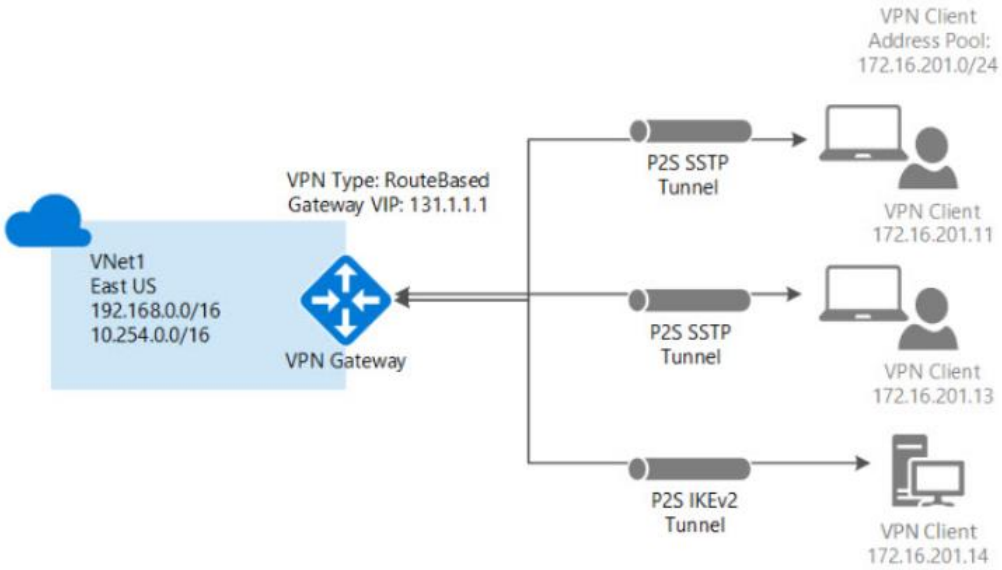
If there are so many workstations who are trying to connect to virtual machines once at a time, then you need a higher version of VPN to support many connections and bandwidth at a time, the lowest version of VPN gateway type is BASIC.

The simulation example:



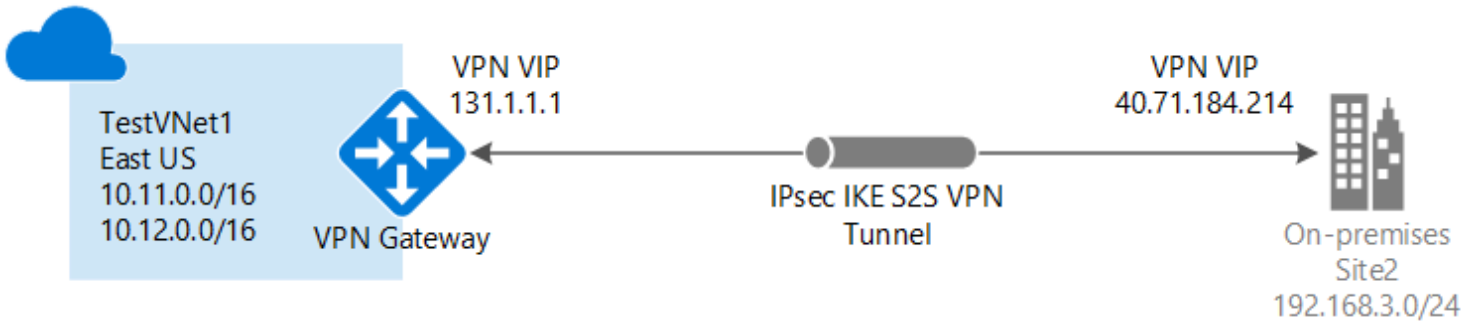
A Point-to-Site VPN connection is used to establish a secure connection between multiple client machines an Azure virtual network via the Internet.

Below is a diagram from the Microsoft documentation on a sample scenario:



Azure – Site to Site VPN Connectivity

A Site-to-Site VPN gateway connection is used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. This type of connection requires a VPN device located on-premises that has an externally facing public IP address assigned to it.



Requirements

1. Verify that you want to work in the classic deployment model
2. Verify that you have an external facing public IPv4 address for your VPN device
3. Make sure you have a compatible VPN device and someone who is able to configure it

Steps to Perform

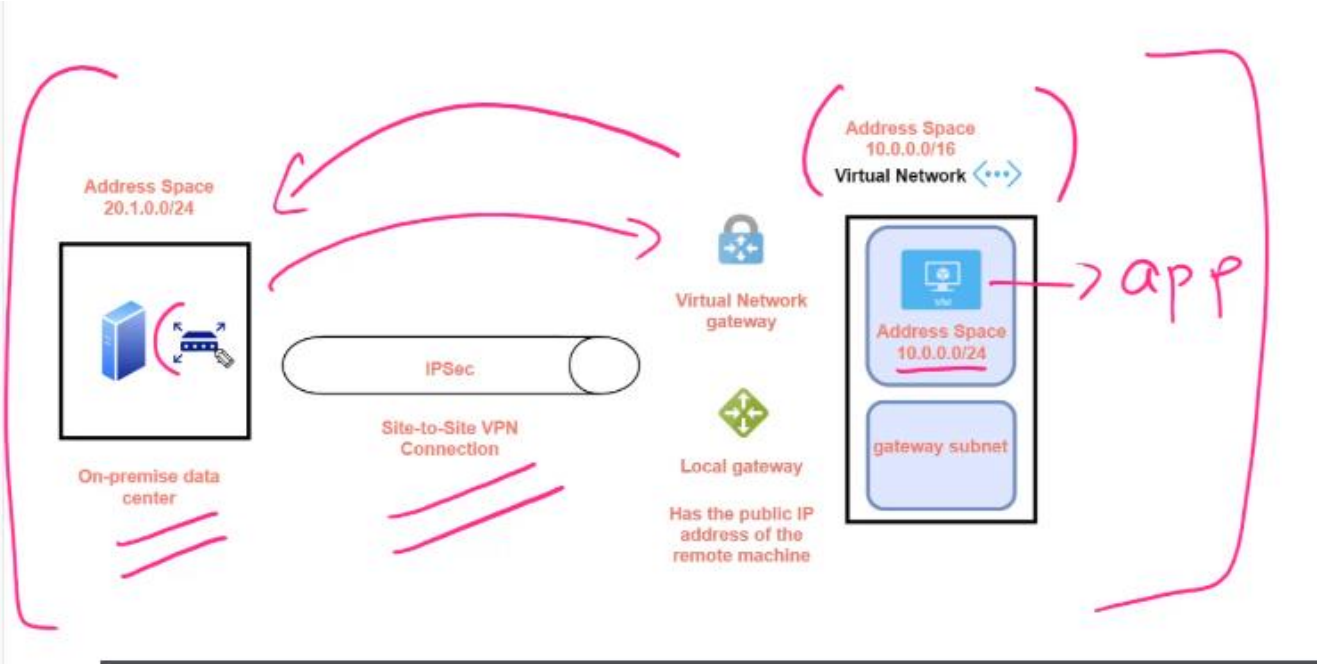
1. Create a virtual network
2. Create a VPN gateway
3. Create a local network gateway
4. Create a VPN connection
5. Verify the connection
6. Connect to a virtual machine

Azure VPN gateways provide cross-premises connectivity between customer premises and Azure. In Azure environment if you want to connect your virtual machine to your on-premises data center. So instead of exposing public IP address for the Azure

virtual machine and allow your employees in the company to access the applications running on the virtual machines via their public IP address.

You can have a connection between your on-premises data center and the Azure virtual network, in such a way that the communications happen via the private IP address of the virtual network, it's a more secure way to accessing your VM's.

So, connecting your entire data center onto the Azure virtual network is to go out and create a Site-to-Site VPN connection.



On the Azure end, you need to have the below configurations and services:

1. Gateway subnet
2. Local gateway
3. Virtual network gateway
4. Then site-to-site VPN connection will be established

Gateway subnet – This is required by the virtual network gateway

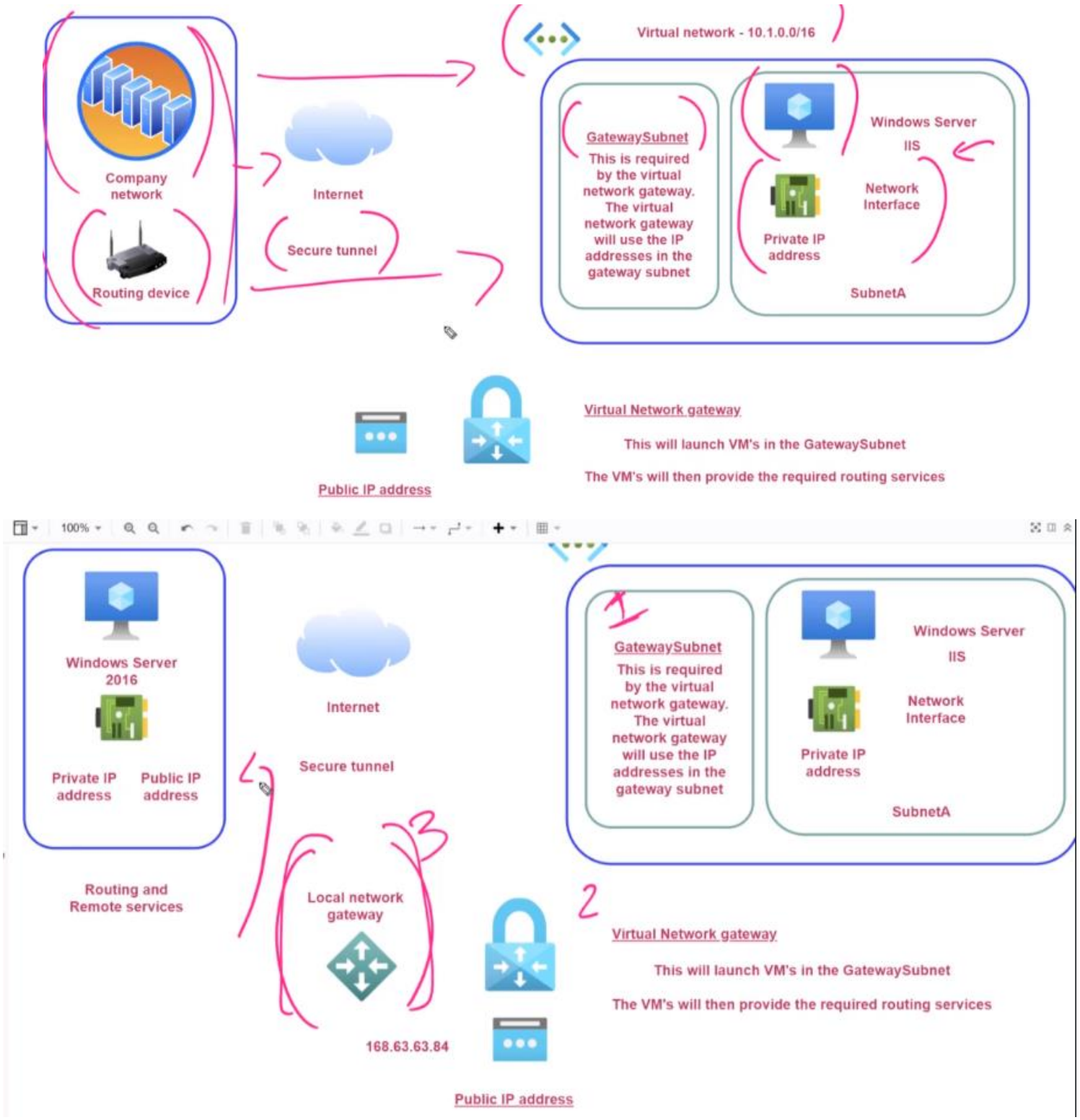
Virtual Network gateway – This will use the IP address in the gateway subnet.

On the On-premises data center, you need to have below requirements:

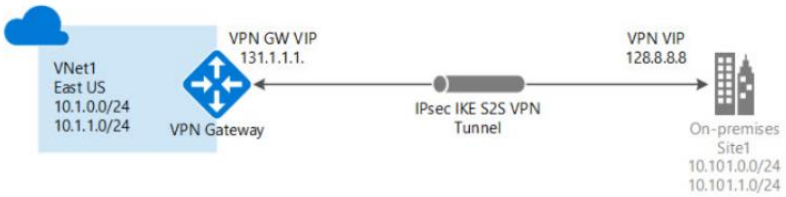
1. A routing device – it could be a physical device, like Cisco router.
2. A software-based routing solution can also work.

The routing device should have a capability of routing the traffic from the company network onto the virtual network in Azure.

A Site-to-Site VPN connection is used to establish a secure connection between an on-premises network and an Azure network via the Internet.



Below is a diagram from the Microsoft documentation on a sample scenario.



On the on-premises side, you need to have a VPN device that can route traffic via the Internet onto the VPN gateway in Azure. The VPN device can be a hardware device like a Cisco router or a software device (e.g Windows Server 2016 running Routing and Remote services). The VPN device needs to have a publicly routable IP address.

The subnets in your on-premises network must not overlap with the subnets in your Azure virtual network

The Site-to-Site VPN connection uses an IPSec tunnel to encrypt the traffic.

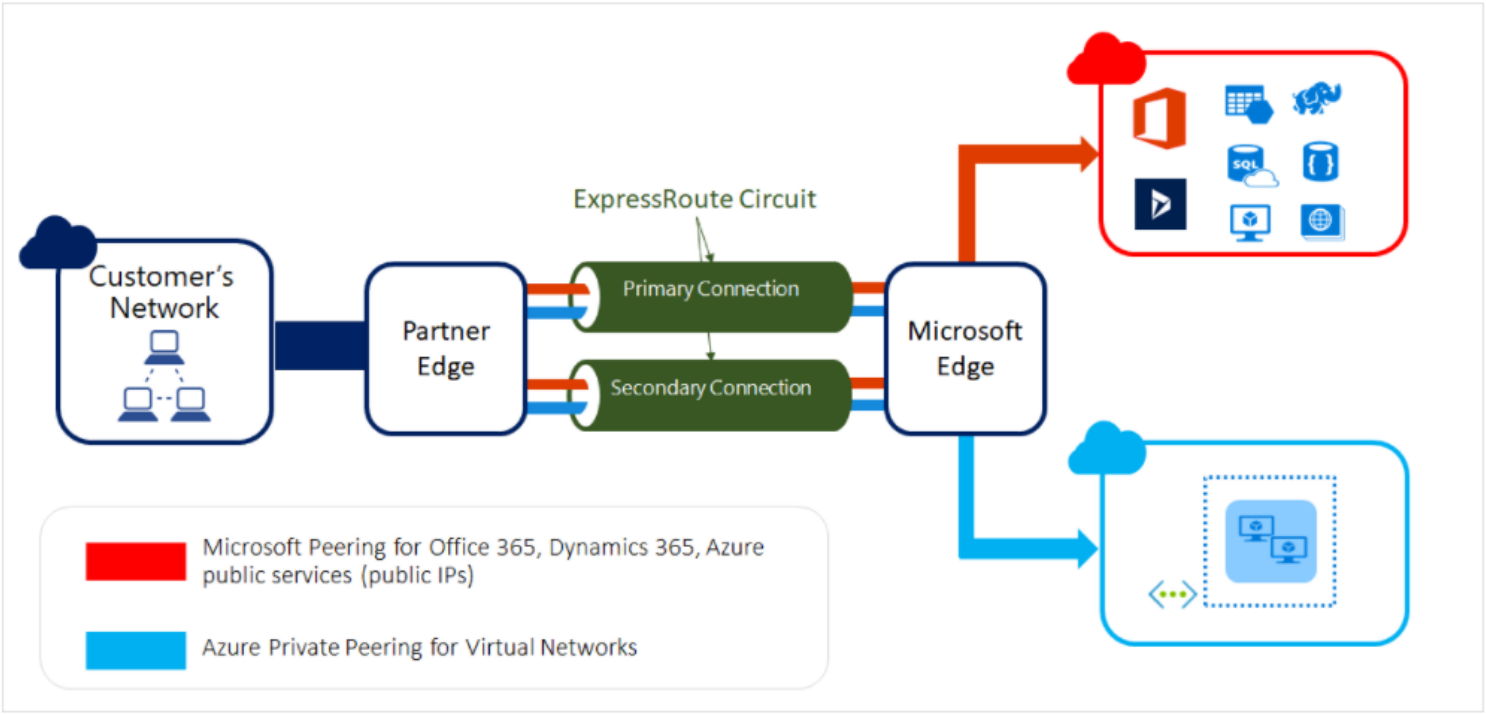
The VPN gateway resource you create in Azure is used to route encrypted traffic between your on-premises data center and your Azure virtual network.

There are different SKU's for the Azure VPN gateway service. Each SKU has a different pricing and attributes associated with it - Reference - https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings

Azure ExpressRoute

ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection with the help of a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure and Microsoft 365.

Connectivity can be from an any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a colocation facility. ExpressRoute connections don't go over the public Internet. This allows ExpressRoute connections to offer more reliability, faster speeds, consistent latencies, and higher security than typical connections over the Internet. For information on how to connect your network to Microsoft using ExpressRoute.



My notes:

This is one of the services that allows you to connect your on-premises data center onto your Azure virtual network. In my making a dedicated connection, you can use Azure ExpressRoute circuit.

When you connect your customer network onto let's say an Azure virtual network using express route all the traffic flows via the entire Microsoft backbone network. This makes it much faster when it comes to the data transfer between the customer network and Azure virtual network.

You can also connect your customer network onto PaaS services such as Azure storage account, Azure SQL database and even MS Office 365.

In this case your connection is not going over the internet.

In Azure ExpressRoute, you create something known as Express Route Circuit, in that circuit you create something known as peering connections onto either private services such as Azure virtual network or onto public services such as Azure storage account, Azure SQL or MS Office 365.

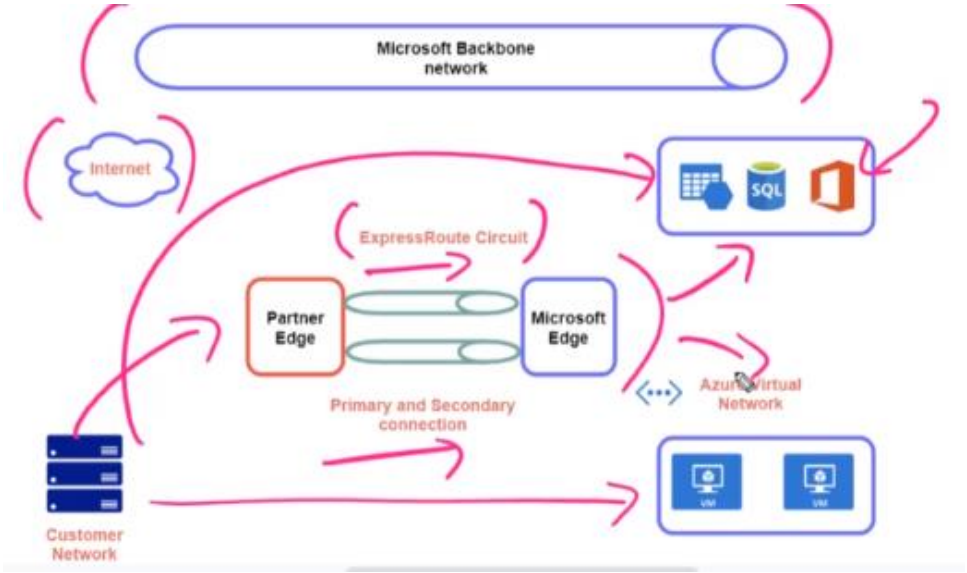
When you want to set up an Azure ExpressRoute circuit, you can create either a dedicated connection or you can create a connection via the third-party provider.

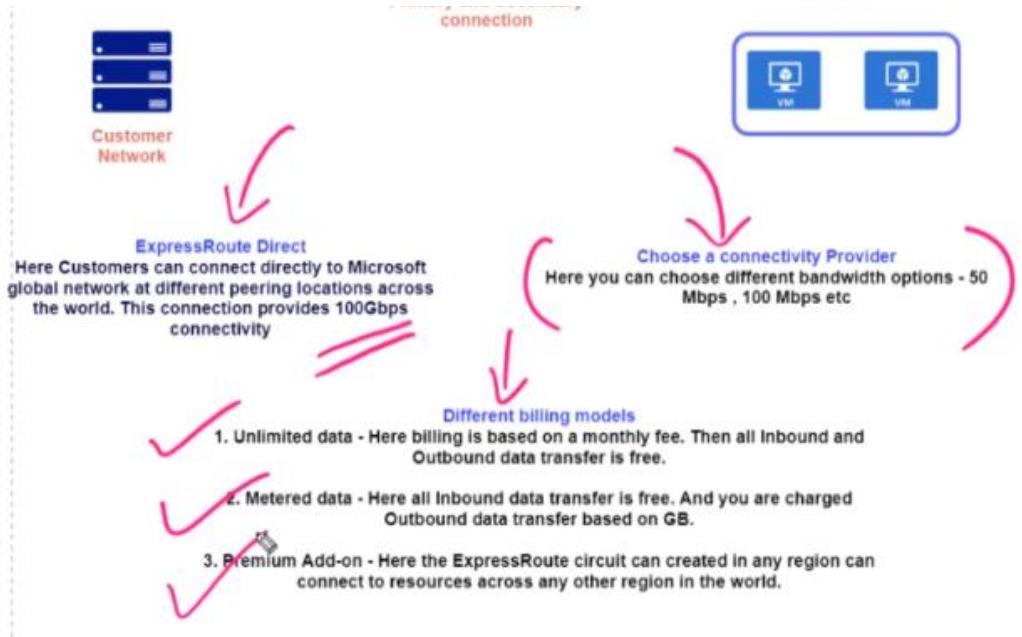
ExpressRoute are used by large organizations that need to have the dedicated line. This is for those organizations that want to have a large bandwidth pipe between their customer network and Azure.

Your connection can flow through internet service provider or a third-party provider, it's a actually knows as a partner edge. You then have connections on to Microsoft Edge.

So, when you create an ExpressRoute circuit connection, there are two connections in place, a primary and a secondary connection. This is used for high availability.

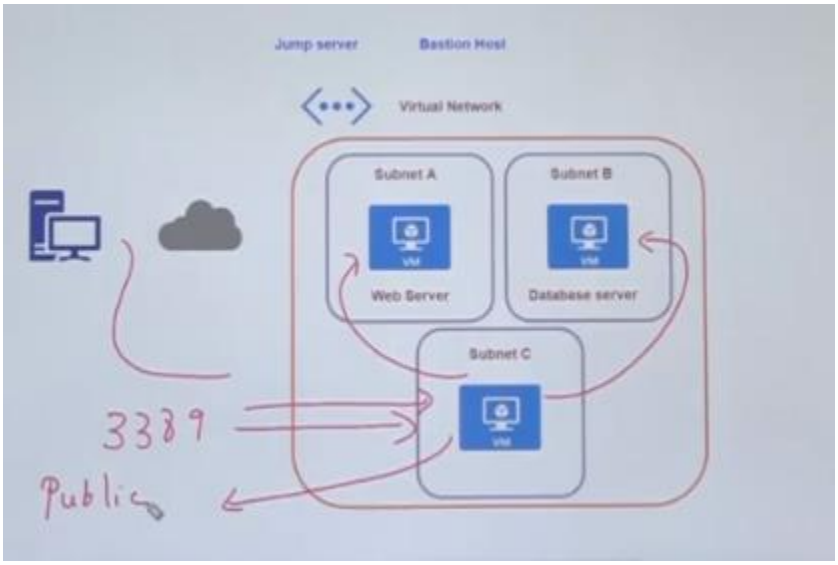
This connects on to Microsoft Edge network, we then have connections on to Azure services.





Azure – Jump Server & Bastion Host

When we create a virtual machine in the Azure cloud. This virtual machine is on the virtual network on the Azure cloud. This VM is called Jumpbox also named as Jump server. Then, by using this VM, we can connect to the other Azure VM's using dynamic IP. Jump box prevents all Azure VM's to expose to the public.



Azure Bastion Service

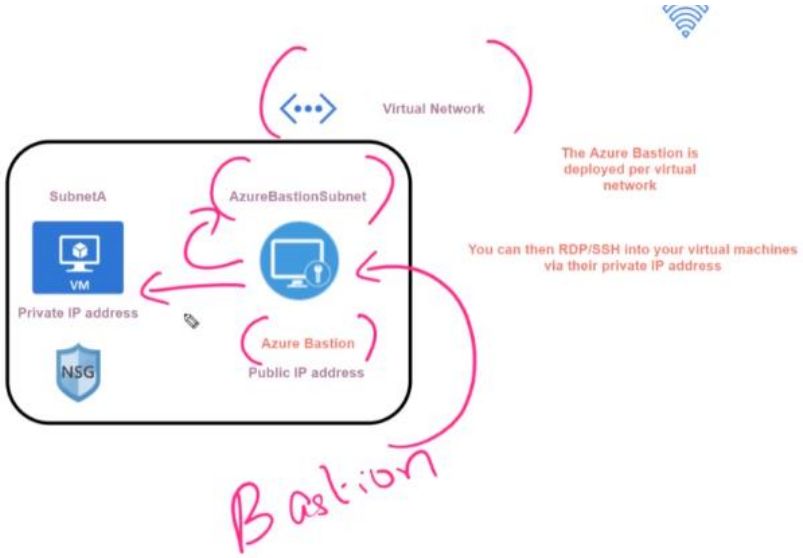
Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines do not need a public IP address, agent, or special client software.

Bastion provides secure RDP and SSH connectivity to all of the VMs in the virtual network in which it is provisioned. Using Azure Bastion protects your virtual machines from exposing RDP/SSH ports to the outside world, while still providing secure access using RDP/SSH.

Note:

In order to go ahead and launch the Azure Bastion host in your virtual network, you need to have a subnet known as BastionSubnet.

We are going to go ahead and connect via the bastion host on the public address onto our VM, but this is going to be seamlessly with the help of Bastion service.



Azure – DDoS Protection

A DDoS attack attempts to exhaust an application's resources, making the application unavailable to legitimate users. DDoS attacks can be targeted at any endpoint that is publicly reachable through the internet. Every property in Azure is protected by Azure's infrastructure DDoS (Basic) Protection at no additional cost. The scale and capacity of the globally deployed Azure network provides defense against common network-layer attacks through always-on traffic monitoring and real-time mitigation. DDoS Protection Basic requires no user configuration or application changes. DDoS Protection Basic helps protect all Azure services, including PaaS services like Azure DNS.

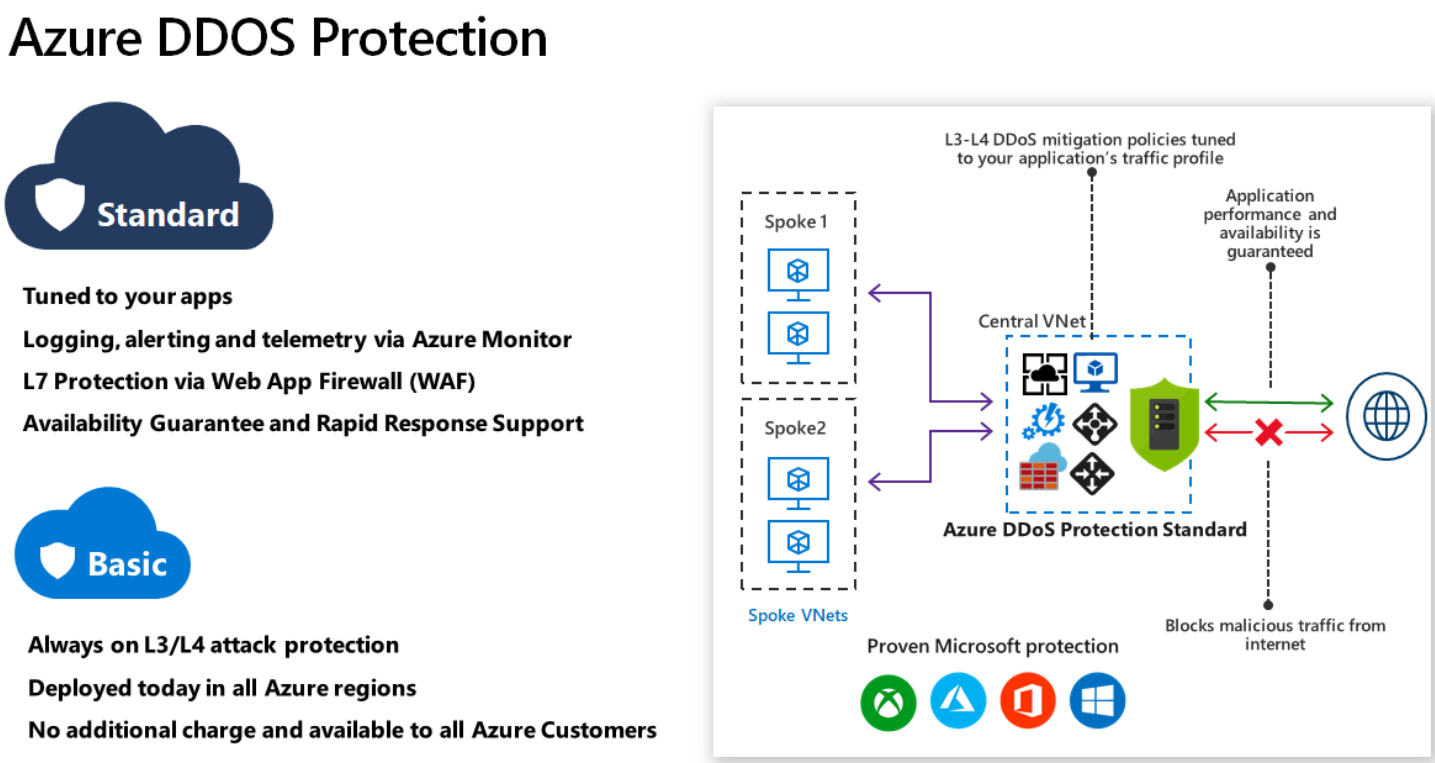
https://docs.microsoft.com/en-us/azure/ddos-protection/ddos-protection-reference-architectures

DDoS Protection Tiers

There are two tiers of Azure DDoS Protection services:

1. DDoS Protection Basic
2. DDoS Protection Standard

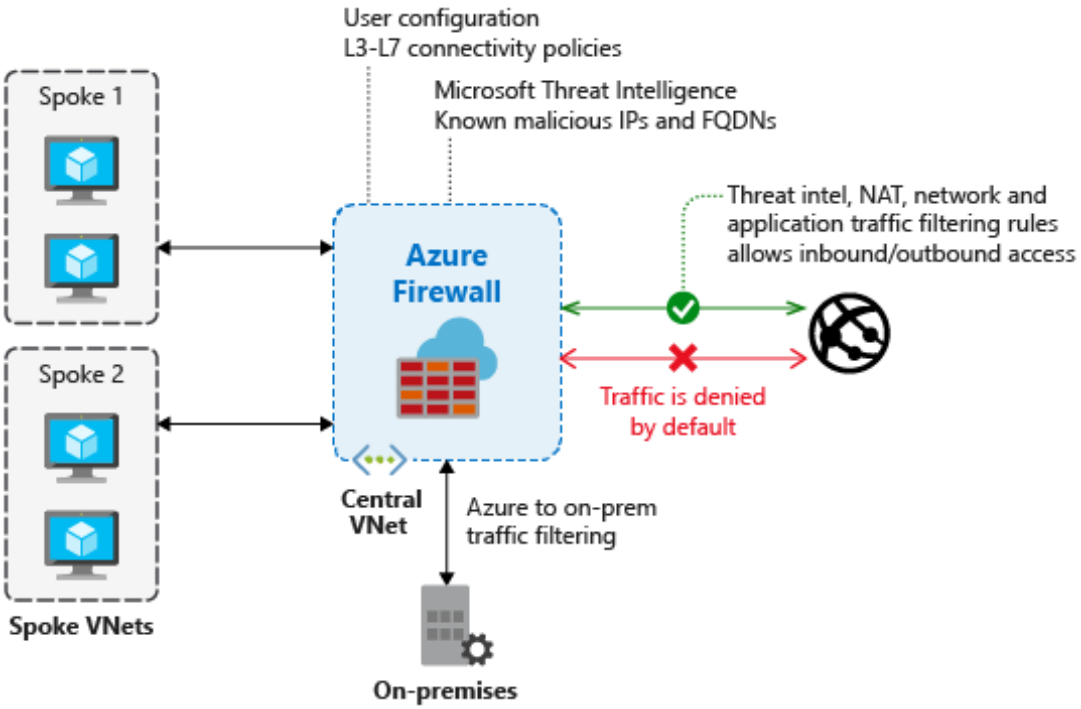
Under a tenant, a single DDoS protection plan can be used across multiple subscriptions, so there is no need to create more than one DDoS protection plan.

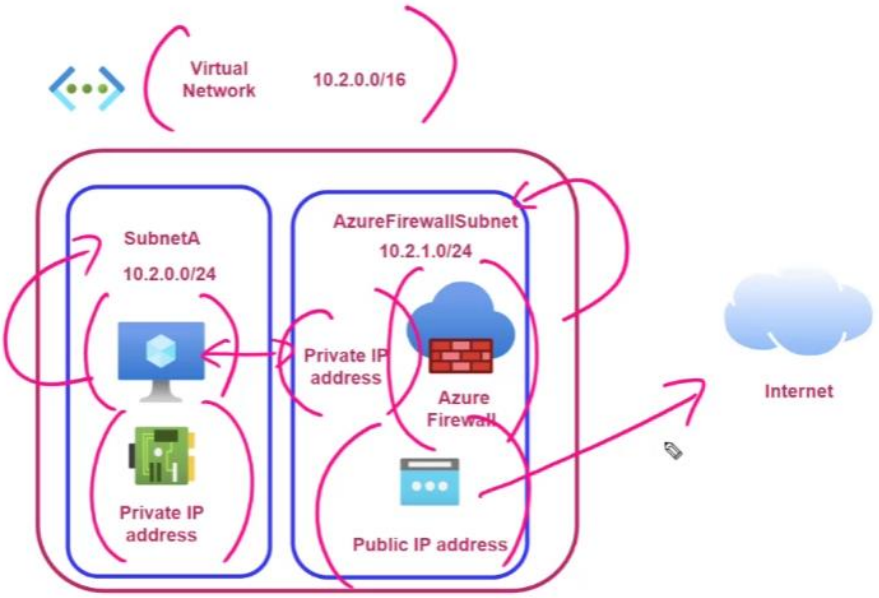


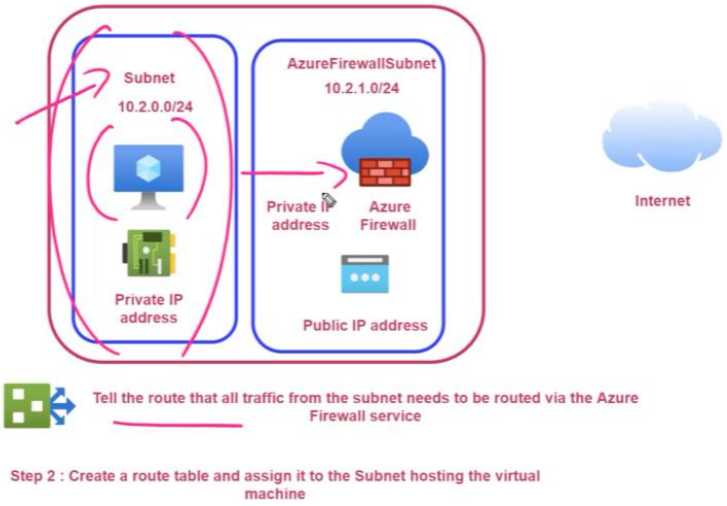
Azure – Firewall

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It's a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.

You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network. The service is fully integrated with Azure Monitor for logging and analytics.







Controlling outbound network access is an important part of an overall network security plan. For example, you may want to limit access to web sites. Or, you may want to limit the outbound IP addresses and ports that can be accessed.

One way you can control outbound network access from an Azure subnet is with Azure Firewall. With Azure Firewall, you can configure:

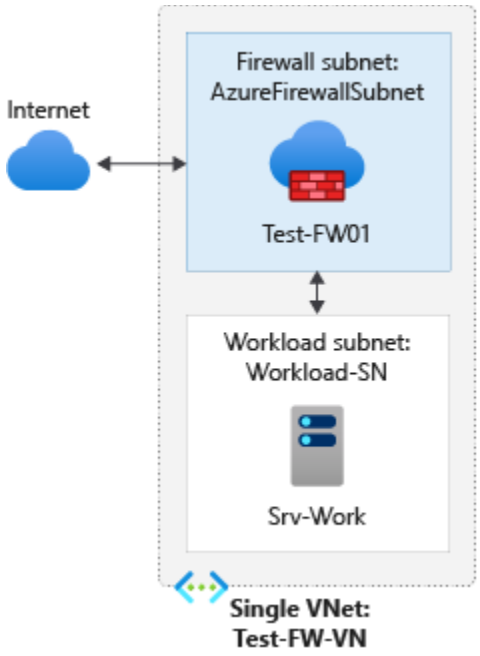
- Application rules that define fully qualified domain names (FQDNs) that can be accessed from a subnet
- Network rules that define source address, protocol, destination port, and destination address

Network traffic is subjected to the configured firewall rules when you route your network traffic to the firewall as the subnet default gateway.

You create a simplified single VNet with two subnets for easy deployment.

For production deployments, a hub and spoke model is recommended, where the firewall is in its own VNet. The workload servers are in peered VNets in the same region with one or more subnets.

- **AzureFirewallSubnet** – The firewall is in this subnet
- **Workload-SN** – The workload server is in this subnet. This subnet's network traffic goes through the firewall



Demo Setup:

1. Set up a test network environment
2. Deploy a firewall
3. Create a default route
4. Configure an application rule to allow access to www.google.com
5. Configure a network rule to allow access to external DNS servers
6. Configure a NAT rule to allow a remote desktop to the test server
7. Test the firewall

Firewall Configuration

The firewall will be in the subnet, and the subnet name must be **AzureFirewallSubnet ***

https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal

Azure – Anti-Malware Extension

Microsoft Antimalware for Azure is a free real-time protection that helps identify and remove viruses, spyware, and other malicious software. It generates alerts when known malicious or unwanted software tries to install itself or run on your Azure systems.

The solution is built on the same antimalware platform as Microsoft Security Essentials [MSE], Microsoft Forefront Endpoint Protection, Microsoft System Center Endpoint Protection, Microsoft Intune, and Microsoft Defender.

Microsoft Antimalware for Azure is a single-agent solution for applications and tenant environments, designed to run in the background without human intervention. Protection may be deployed based on the needs of application workloads, with either basic secure-by-default or advanced custom configuration, including antimalware monitoring.

- Microsoft Antimalware can also be deployed using Azure Security Center
- To enable this feature on Virtual Machines, you have to install an extension
- On Windows Server 2016, Windows Defender is the built-in Antimalware
- If you apply the Antimalware Extension on Windows Server 2016 machines, it will apply any option configuration policies used by Windows Defender

Core Features:

1. Real-time protection
2. Scheduled scanning
3. Signature updates
4. Antimalware Engine updates
5. Antimalware Platform updates
6. Active Protection
7. Samples Reporting
8. Exclusions: Path, Extension Type, Processes
9. Antimalware Event Collection

Extension Support & Non-Support

Microsoft Antimalware is supported on:

1. Windows Server 2008 R2
2. Windows Server 2012
3. Windows Server 2012 R2

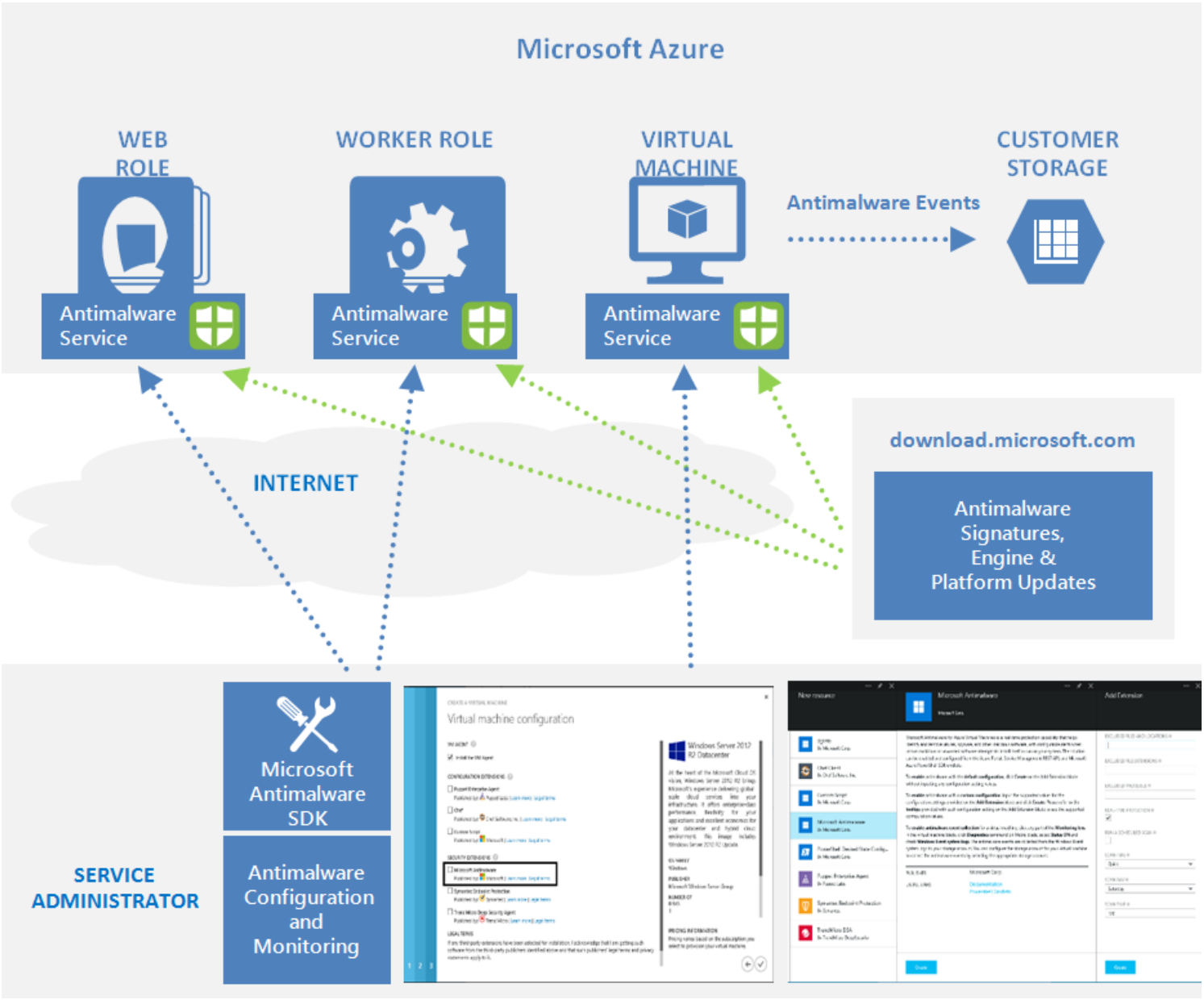
Microsoft Antimalware is not supported on:

1. Windows Server 2008
2. Linux OS

Deployment Methods

The Azure service administrator can enable Antimalware for Azure with a default or custom configuration for your Virtual Machines and Cloud Services using the following options

- Virtual Machines – In the Azure portal, under Security Extensions
- Virtual Machines – Using the Visual Studio virtual machines configuration in Server Explorer
- Virtual Machines and Cloud Services – Using the Antimalware classic deployment model
- Virtual Machines and Cloud Services – Using Antimalware PowerShell cmdlets



Azure – Hub & Spoke Architecture

The hub virtual network acts as a central point of connectivity to many spoke virtual networks. The hub can also be used as the connectivity point to your on-premises networks. The spoke virtual networks peer with the hub and can be used to isolate workloads.

This hub-spoke architecture provides an alternate solution to the reference architectures hub-spoke network topology in Azure and implement a secure hybrid network.

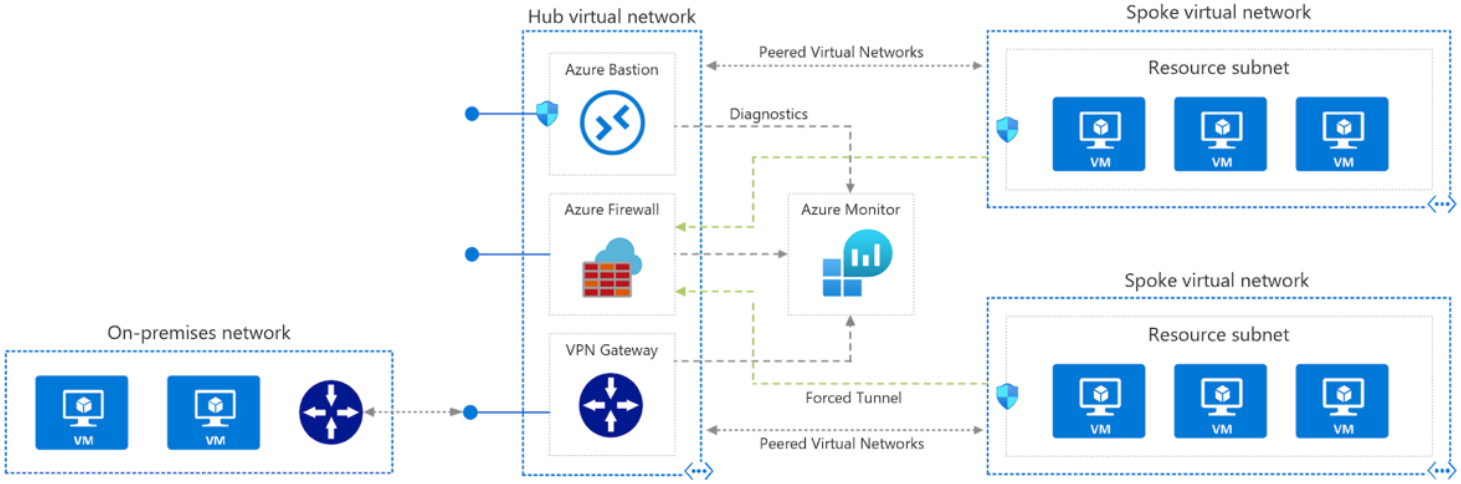
The hub is a virtual network in Azure that acts as a central point of connectivity to your on-premises network. The spokes are virtual networks that peer with the hub and can be used to isolate workloads. Traffic flows between the on-premises data center(s) and the hub through an ExpressRoute or VPN gateway connection. The main differentiator of this approach is the use of Azure Virtual WAN (VWAN) to replace hubs as a managed service.

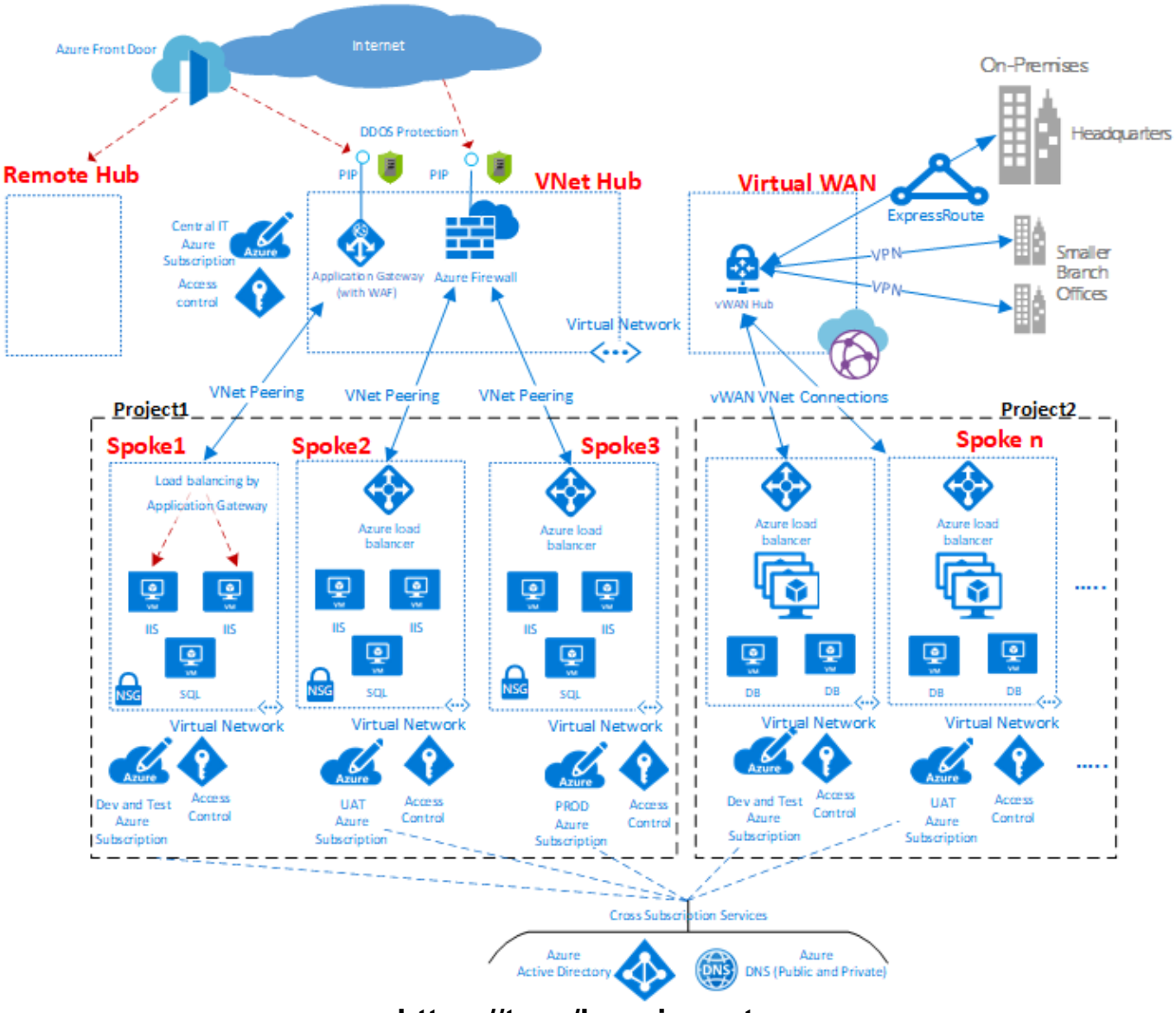
The benefits of using a hub and spoke configuration include cost savings, overcoming subscription limits, and workload isolation.

This reference architecture details a hub-spoke topology in Azure.

Hub and **spoke** is a networking model for efficiently managing common communication or security requirements. It also helps avoid Azure subscription limitations. This model addresses the following concerns:

- **Saving on costs and efficient management:** Centralizing services that can be shared by multiple workloads, such as network virtual appliances (NVAs) and DNS servers, in a single location allows IT to minimize redundant resources and management effort.
- **Overcoming subscription limits:** large cloud-based workloads might require using more resources than are allowed in a single Azure subscription. Peering workload virtual networks from different subscriptions to a central hub can overcome these limits. For more information, see Azure subscription limits.
- **A separation of concerns:** You can deploy individual workloads between central IT teams and workload teams.





Important Notes:

- When you create this route table, you have to ensure to disable the virtual network gateway propagation, just because you have Site-to-Site VPN connection in place.
- So, if you have Site-to-Site VPN connection between your on-premises network and the hub network which is hosting your Azure Firewall then make sure to disabled the virtual network gateway propagation.
- Also, you need to create another Route Table, which basically assigns to a gateway subnet. This points to the firewall IP address has the next hop for the spoke networks. So, this is to ensure if the traffic is flowing from Site-to-Site VPN on to the on-premises network, then the traffic would flow via the Azure Firewall instance.

The Architecture

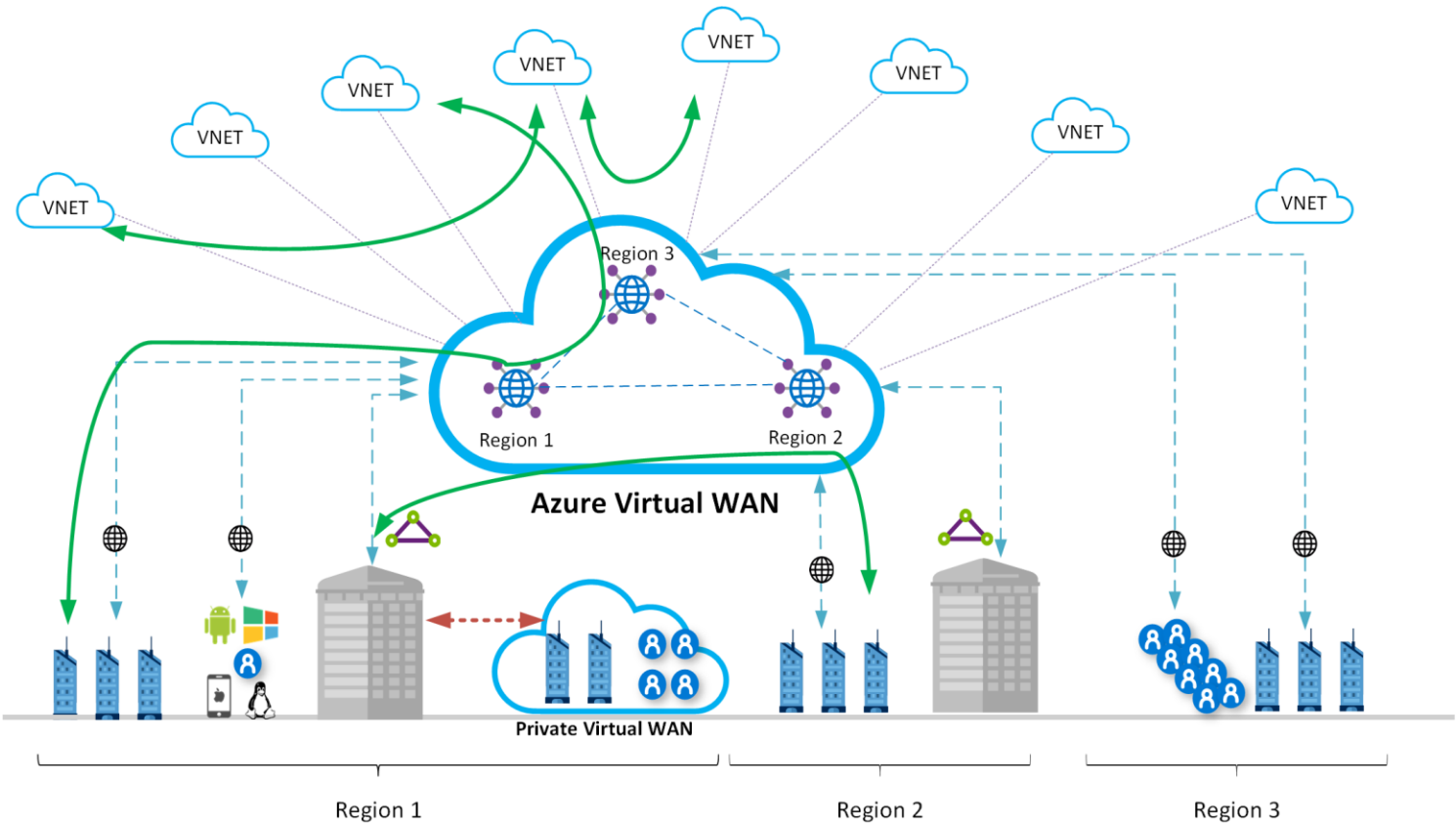
The architecture consists of the following components:

1. **Hub Virtual Network**
   The hub virtual network is the central point of connectivity to your on-premises network. It's a place to host services that can be consumed by the different workloads hosted in the spoke virtual networks
2. **Spoke Virtual Networks**
   Spoke virtual networks are used to isolate workloads in their own virtual networks, managed separately from other spokes. Each workload might include multiple tiers, with multiple subnets connected through Azure load balancers
3. **Virtual Network Peering**
   Two virtual networks can be connected using a **peering connection**. Peering connections are non-transitive, low latency connections between virtual networks. Once peered, the virtual networks exchange traffic by using the Azure Backbone without the need for a router
4. **Bastion Host**
   Azure Bastion Host lets you securely connect to a virtual machine using your browser and the Azure portal. An Azure Bastion host is deployed inside an Azure Virtual Network and can access virtual machines in the VNet, or Virtual Machines in peered VNets
5. **Azure Firewall**
   Azure Firewall is a managed firewall as a service. The firewall instance is placed in its own subnet
6. **VPN Virtual Network Gateway or ExpressRoute Gateway**
   The virtual network gateway enables the virtual network to connect to the VPN device, or ExpressRoute circuit, used for connectivity with your on-premises network
7. **VPN Device**
   A device or service that provides external connectivity to the on-premises network. The VPN device may be a hardware device or a software solution such as the Routing and Remote Access Service (RRAS) in Windows Server 2012

Advantages

This diagram illustrates a few of the advantages that this architecture can provide:

- A full meshed hubs among Azure Virtual Networks
- Branch to Azure connectivity
- Branch to Branch connectivity
- Mixed use of VPN and Express Route
- Mixed use of user VPN to the site
- VNET to VNET connectivity



Azure – Log Analytics Workspace

A Log Analytics workspace is a unique environment for Azure Monitoring log data. Each workspace has its own data repository and configuration, and data sources and solutions are configured to store their data in a particular workspace.

Log Analytics Workspace Insights (preview) provides comprehensive monitoring of your workspaces through a unified view of your workspace usage, performance, health, agent, queries, and change log.

Log Analytics is a tool in the Azure portal to edit and run log queries from data collected by Azure Monitor Logs and interactively analyze their results. You can use Log Analytics queries to retrieve records that match particular criteria, identify trends, analyze patterns, and provide a variety of insights into your data.

You require a Log Analytics workspace if you intend on collecting data from the following sources:

- Azure resources in your subscription
- On-premises computers monitored by System Center Operations Manager
- Device collections from Configuration Manager
- Diagnostics or log data from Azure Storage

Azure – Update Management

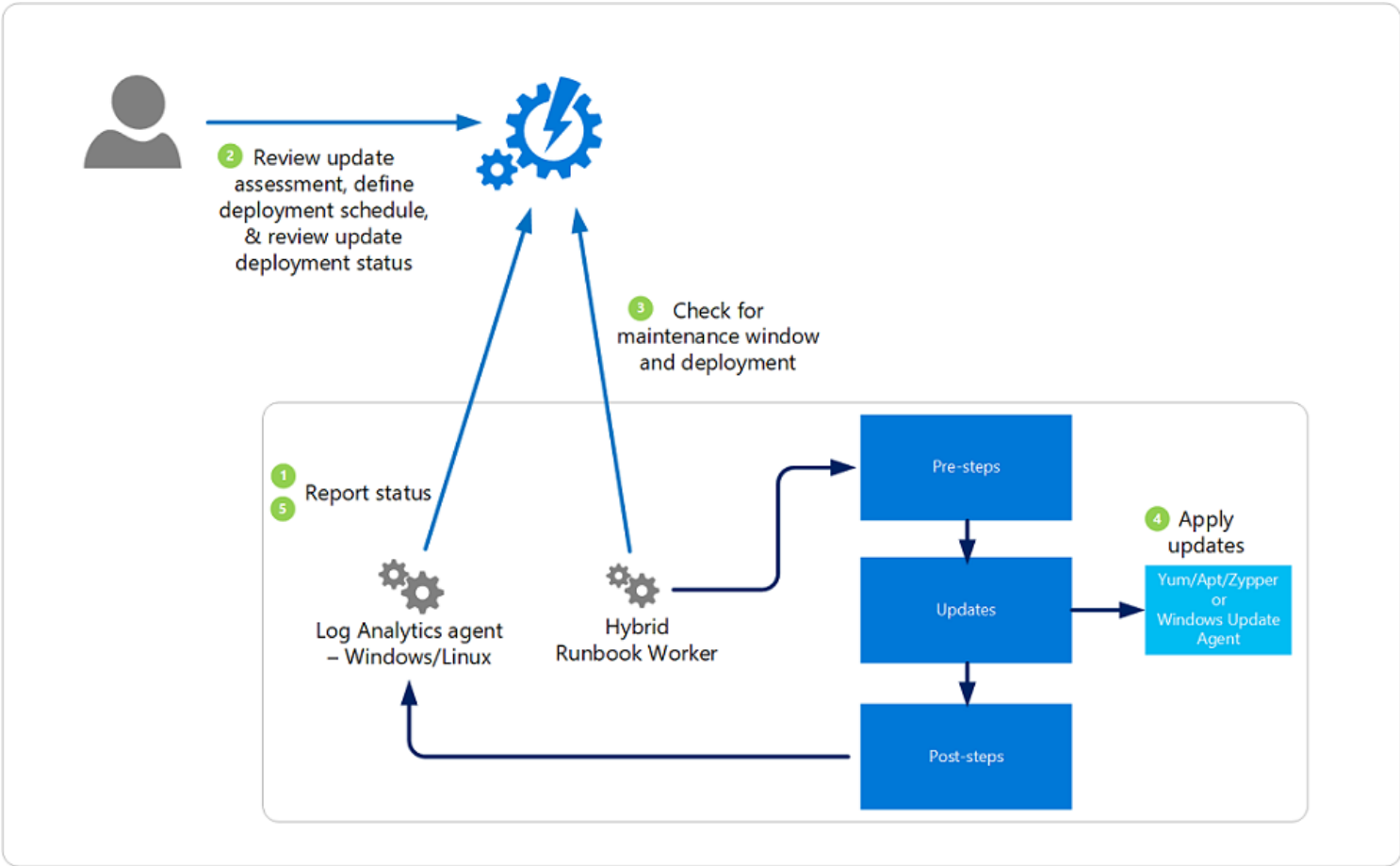
You can use Update Management in Azure Automation to manage operating system updates for your Windows and Linux virtual machines in Azure, physical or VMs in on-premises environments, and in other cloud environments. You can quickly assess the status of available updates and manage the process of installing required updates for your machines reporting to Update Management.

Microsoft offers other capabilities to help you manage updates for your Azure VMs or Azure virtual machine scale sets that you should consider as part of your overall update management strategy.

Update Management integrates with Azure Monitor Logs to store update assessments and update deployment results as log data, from assigned Azure and non-Azure machines. To collect this data, the Automation Account and Log Analytics workspace are linked together, and the Log Analytics agent for Windows and Linux is required on the machine and configured to report

to this workspace. Update Management supports collecting information about system updates from agents in a System Center Operations Manager management group connected to the workspace.

The following diagram illustrates how Update Management assesses and applies security updates to all connected Windows Server and Linux servers.



Note:

Having a machine registered for Update Management in more than one Log Analytics workspace (also referred to as multihoming) isn't supported.

Important Notes:

1. The Update Management solution in Azure can be used to manage the updates and patches for your Windows & Linux virtual machines
2. With this solution you can
   - Onboard virtual machines
   - See the status of available updates
   - Schedule the installation of required updates
   - Review the deployment results
3. For enabling updates, you need to have an **Azure Automate Account** and a **Log Analytics Workspace**

What is an Azure Automation Account?

This is a service that helps provide cloud-based automation and a configuration service for both Azure and non-Azure environments.

There are different capabilities within Azure Automation Account:

1. **Process Automation** – Here you can orchestrate processes using graphical runbooks, PowerShell, and Python runbooks
2. **Configuration Management** – Here you can collect inventory, track changes, and configure the desired state for Virtual Machines
3. **Update Management** – You can also assess the compliance of Virtual Machines and also schedule the installation of updates on Virtual Machines

The Architecture

The architecture consists of the following components:

1. **Log Analytics Workspace** – A Log Analytics workspace is a data repository for log data that's collected from resources that run in Azure, on-premises, or in another cloud provider
2. **Automation Hybrid Worker solution** – Create Hybrid Runbooks Workers to run Azure Automation runbooks on your Azure and non-Azure computers
3. **Automation Account** – This is a cloud service that automates configuration and management across your Azure and non-Azure environments
4. **Hybrid Runbook Worker Group** – It's a group of Hybrid Runbook Workers used for high availability
5. **Runbook** – This is a collection of one or more linked activities that together automate a process or operation
6. **On-premises Computers & VM's** – These are on-premises computers and VM's with Windows or Linux operating systems that reside on-premises
7. **Azure VM's** – Azure VM's include Windows or Linux VM's that hosted in Azure

Update Management

Update Management is a configuration component of Automation. Windows and Linux computers, both in Azure and on-premises, send assessment information about missing updates to the Log Analytics workspace. Azure Automation then uses that information to create a schedule for automatic deployment of the missing updates.

The following steps highlight the actual implementation:

1. Create a Log Analytics workspace
2. Create an Automation account
3. Link the Automation account with the Log Analytics workspace
4. Enable Update Management for Azure VMs
5. Enable Update Management for non-Azure VMs

How to work on and create Update Management

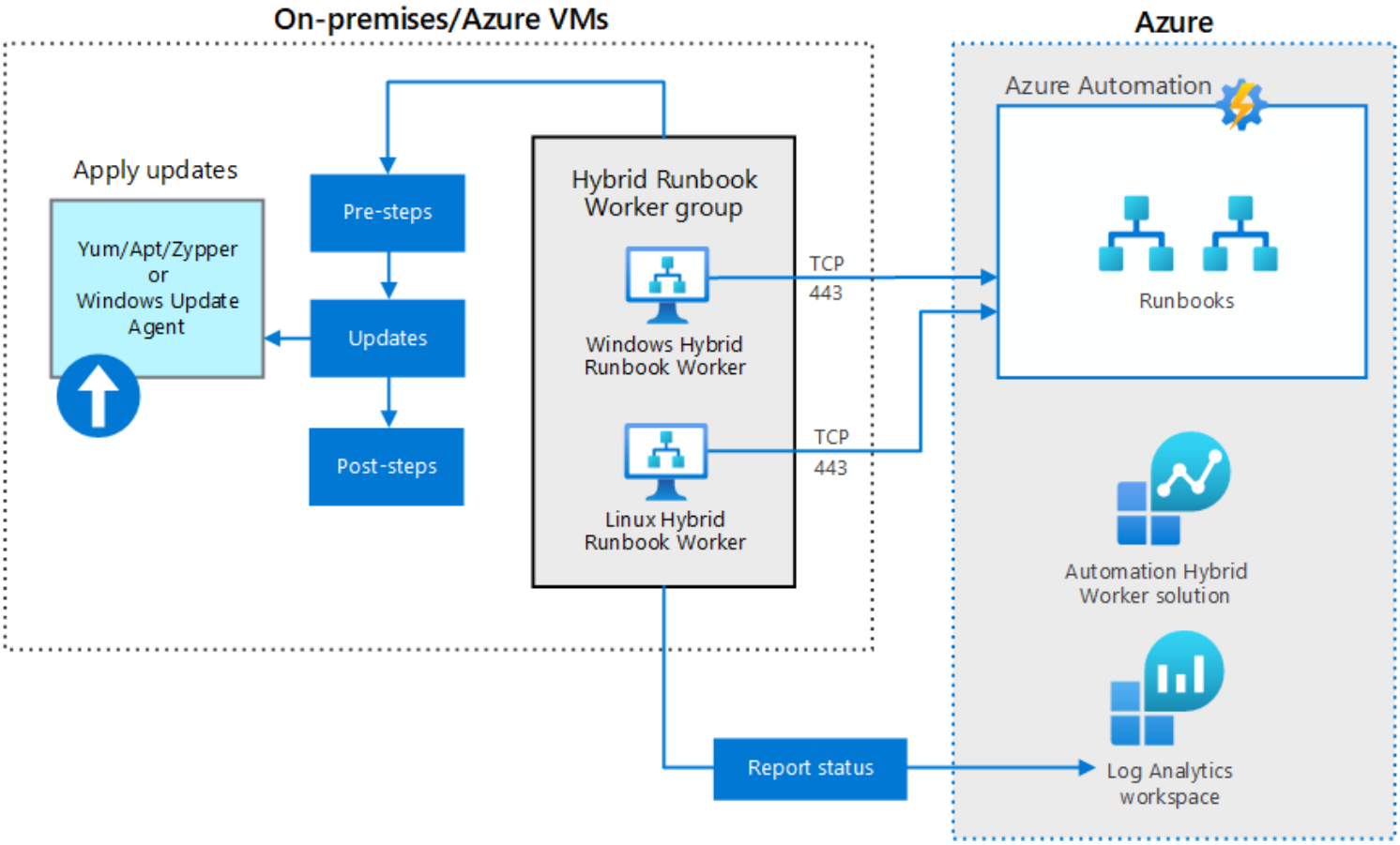
https://docs.microsoft.com/en-us/azure/architecture/hybrid/azure-update-mgmt

Before you deploy software updates to your machines, review the update compliance assessment results for enabled machines. For each software update, its compliance state is recorded and then after the evaluation is complete, it is collected and forwarded in bulk to Azure Monitor logs.

On a Windows machine, the compliance scan is run every 12 hours by default, and is initiated within 15 minutes of the Log Analytics agent for Windows is restarted. The assessment data is then forwarded to the workspace and refreshes the Updates table. Before and after update installation, an update compliance scan is performed to identify missing updates, but the results are not used to update the assessment data in the table.

For a Linux machine, the compliance scan is performed every hour by default. If the Log Analytics agent for Linux is restarted, a compliance scan is initiated within 15 minutes.

The compliance results are presented in Update Management for each machine assessed. It can take up to 30 minutes for the dashboard to display updated data from a new machine enabled for management.

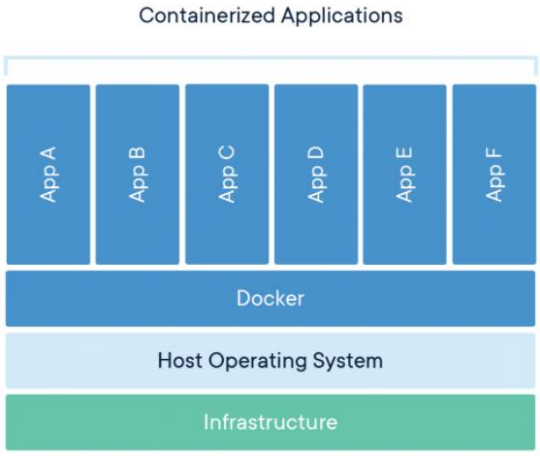


Azure – Containers & Dockers & Kubernetes

What are Containers?

A container is a standard unit of software that packages up code and all its dependencies so the application runs quickly and reliably from one computing environment to another. A Docker container image is a lightweight, standalone, executable package of software that includes everything needed to run an application: code, runtime, system tools, system libraries and settings.

Container images become containers at runtime and in the case of Docker containers - images become containers when they run on Docker Engine. Available for both Linux and Windows-based applications, containerized software will always run the same, regardless of the infrastructure. Containers isolate software from its environment and ensure that it works uniformly despite differences for instance between development and staging.



What is Azure Container?

Azure Container Instances is a service that enables a developer to deploy containers on the Microsoft Azure public cloud without having to provision or manage any underlying infrastructure.

The service which supports both Linux and Windows containers eliminates the need for a developer to provision virtual machines, or implement a container orchestration platform, such as Kubernetes, to deploy and run containers. Instead, with Azure Container Instances (ACI), an organization can spin up a new container via the Azure portal or command-line interface (CLI), and Microsoft automatically provisions and scales the underlying compute resources. ACI also supports standard Docker images a developer can pull from a container registry, such as Docker Hub or Azure Container Registry.

There are three sources to pull the images, from where you can select the docker image

- Quickstart images
- Azure Container Registry
- Docker Hub or other registry

Container Groups

- This is nothing but a collection of containers
- These containers get scheduled on the same host machine
- They share the same lifecycle, resources, local network, and storage volumes
- The deployment can be done via Resource Manager template or a YAML file
- These container groups can also go out and use Azure file share when it comes to the storage of the underlying data for the container itself. So, the container wants to go out and actually mount volumes for storage.

What is Kubernetes?

- This is an open-source platform that is used to managing containerized workloads
- Kubernetes is able to provide a DNS name to your container
- If there is a high load on your containers, Kubernetes can load balance and distribute network traffic
- Kubernetes can also restart containers that fail
- It can be used to replace or kill containers
- It also helps to store and manage sensitive information such as passwords, OAuth tokens, and SSH Keys

What is Azure Kubernetes?

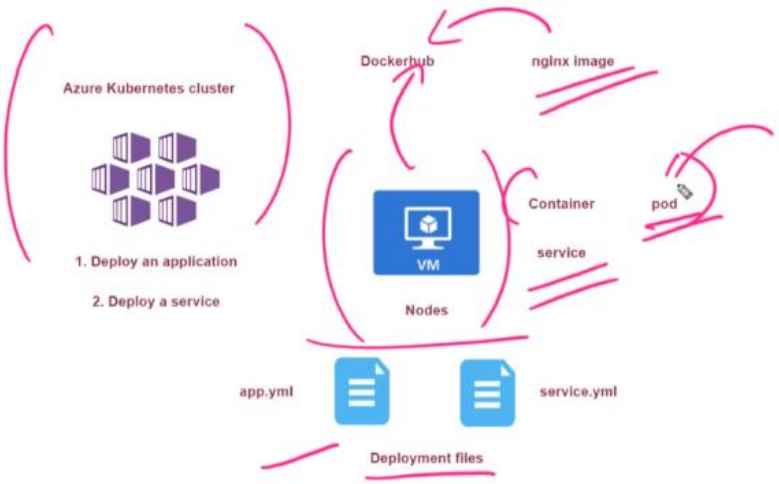
Deploy and manage containerized applications more easily with a fully managed Kubernetes service. Azure Kubernetes Service (AKS) offers serverless Kubernetes, an integrated continuous integration and continuous delivery (CI/CD) experience and enterprise-grade security and governance. Unite your development and operations teams on a single platform to rapidly build, deliver and scale applications with confidence.

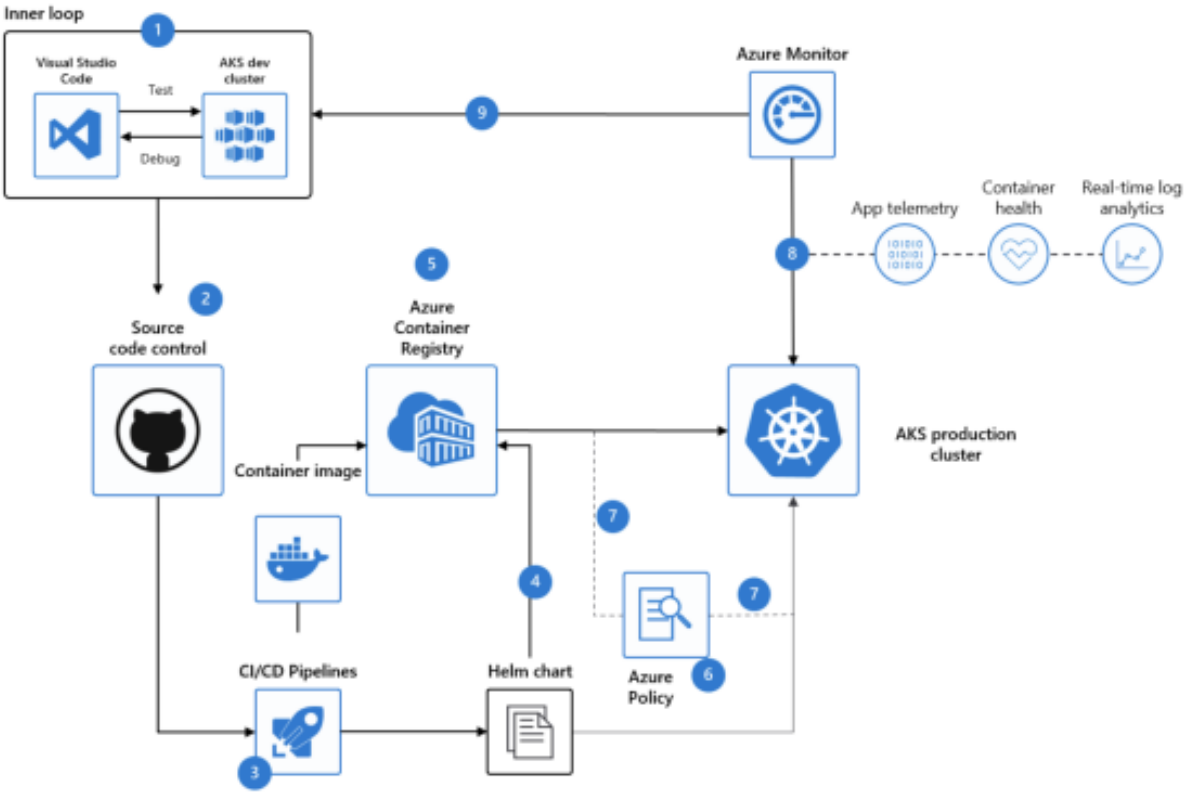
- Fully managed Kubernetes service on Azure
- Makes it easy to deploy and manage containerized applications
- It helps to remove the burden of managing the underlying infrastructure for the Kubernetes deployment

You can deploy a simple container onto the cluster by app.yaml file. The deployment file is going to go ahead and deploy a pod onto a cluster, that is basically a container. It's used for deploying the pods or containers.

So, the service.yaml file will go out and use a load balancer and it allows to go ahead and actually access that nginx container via a public IP address. It is used for deploying the services.

- It's a fully managed Kubernetes service on Azure
- Makes it easy to deploy and manage containerized applications
- It helps to remove the burden of managing the underlying infrastructure for the Kubernetes deployment



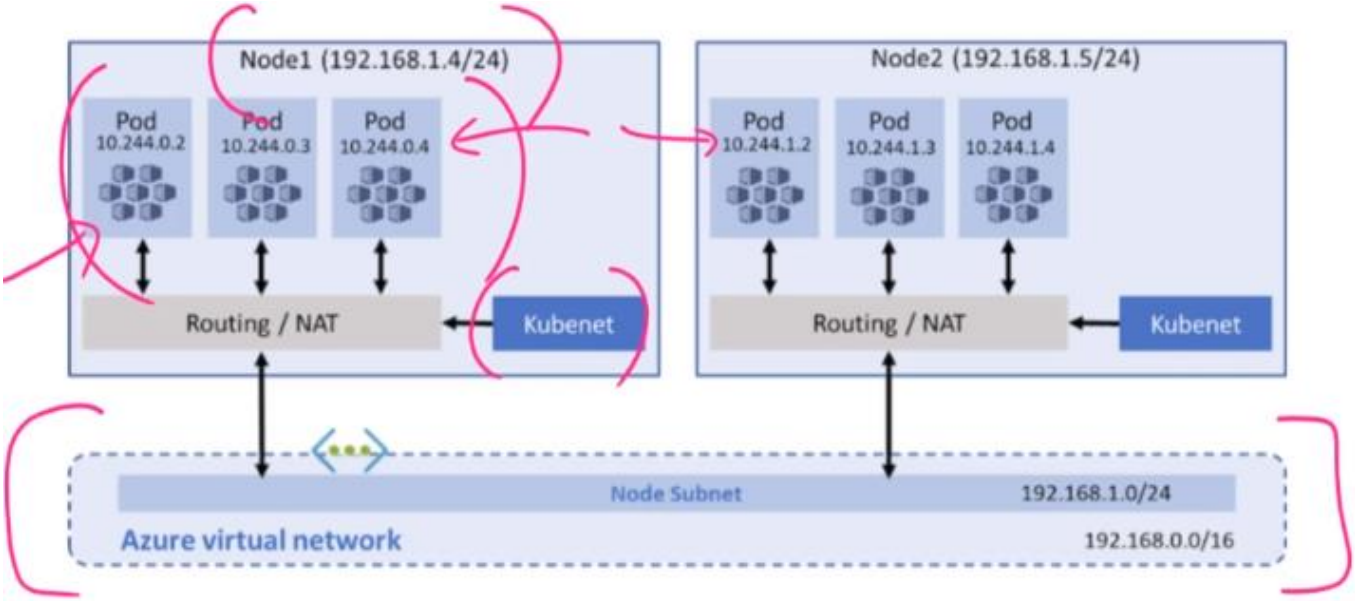


Kubernetes Networking

In Azure Kubernetes when you go ahead and deploy your containers so they are deployed onto individual pods, and these pods would reside on the nodes, so the nodes basically are your compute infrastructure that is required for hosting the pods, which in turns holds your containers.

Now these pods also go ahead and receive an IP address, and this allows for inter-communications between the pods itself.

Now when it comes to the IP addresses that can be assigned onto the pods, so there are two ways that can be achieved.



https://docs.microsoft.com/en-us/azure/aks/configure-kubenet

Nodes receive an IP address from the Azure virtual network

Pods receive an IP address from a logically different address space to the Azure virtual network subnet

Network Address translation is then used

Azure Container Networking Interface

1. Kubenet

When you use Kubenet:

- Nodes receive an IP address from the Azure underlying network or Azure virtual network
- Then the pods actually receive an IP address that are logically different addresses spaces to that of the Azure virtual network
- So over here, network address translation (NAT) is then use to go ahead and translate the address from Azure virtual network onto the addresses that are assigned onto the individual pods

2. Azure Container Network Interface

- Every pod gets an IP address from the subnet directly and can be accessed directly as well, but this could go and lead onto IP address exhaustion, so the IP addresses in your subnet may not be enough to go out and cover all the pods on the different nodes

---

https://docs.microsoft.com/en-us/azure/aks/configure-kubenet

Nodes receive an IP address from the Azure virtual network

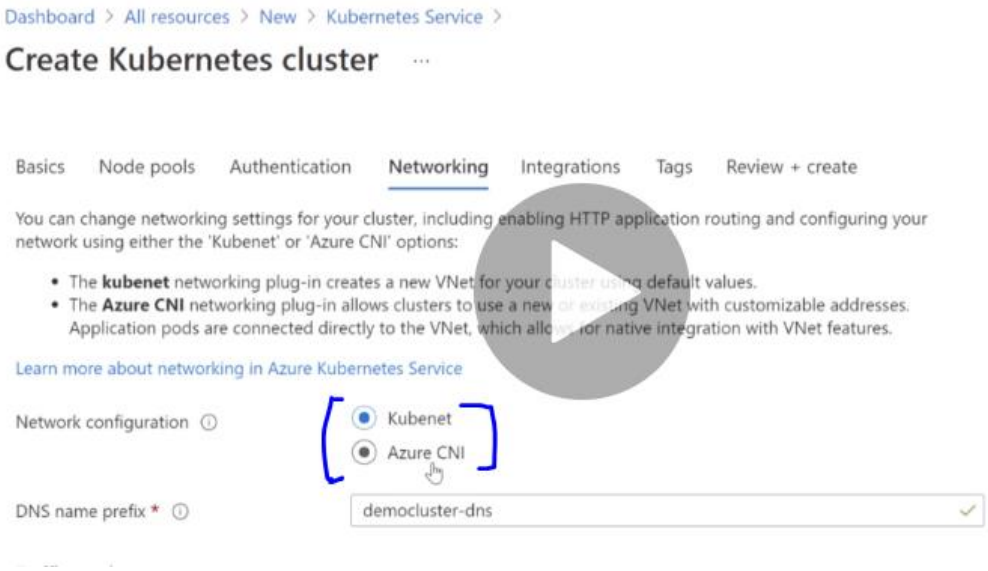
Pods receive an IP address from a logically different address space to the Azure virtual network subnet

Network Address translation is then used

Azure Container Networking Interface

Every pod gets an IP address from the subnet and can be accesed directly

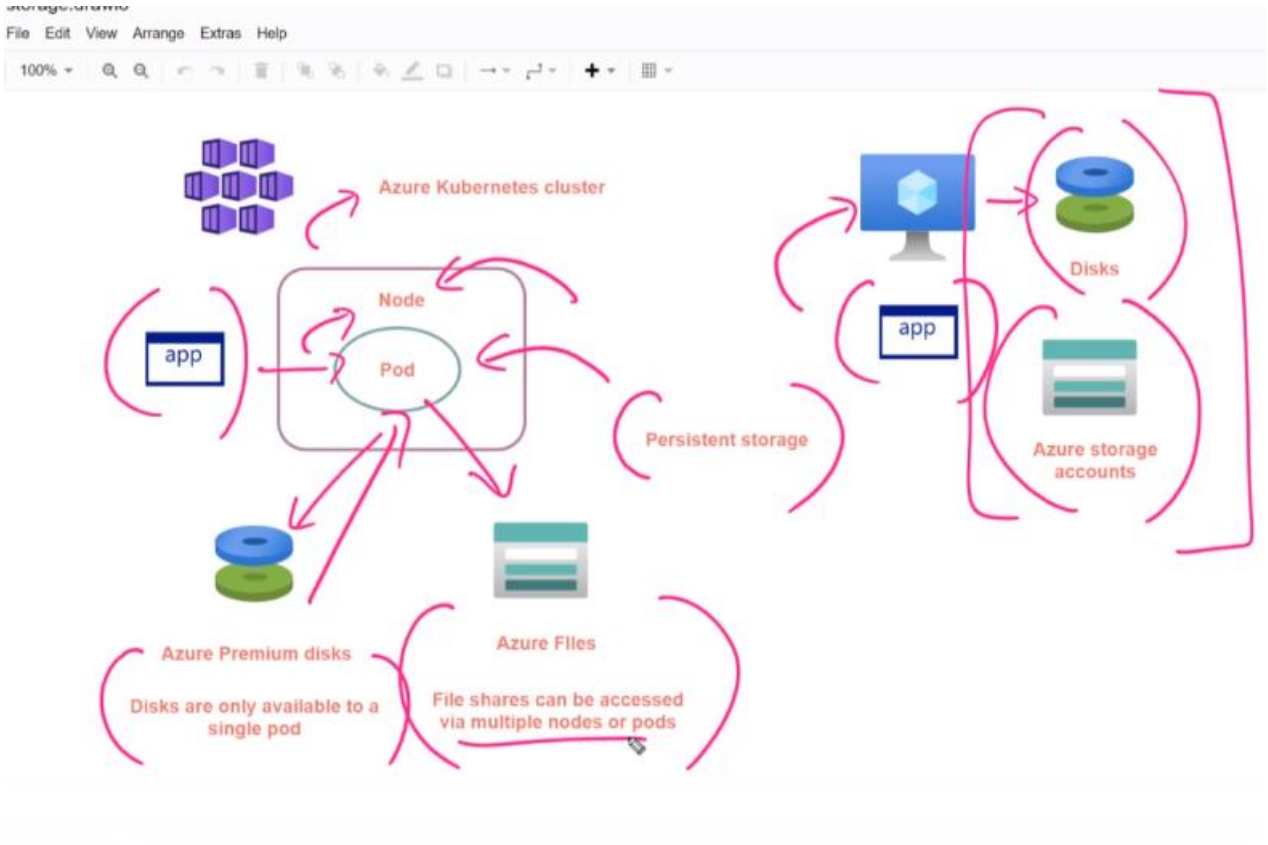
This could also lead to an IP address exhaustion



Azure Kubernetes Storage

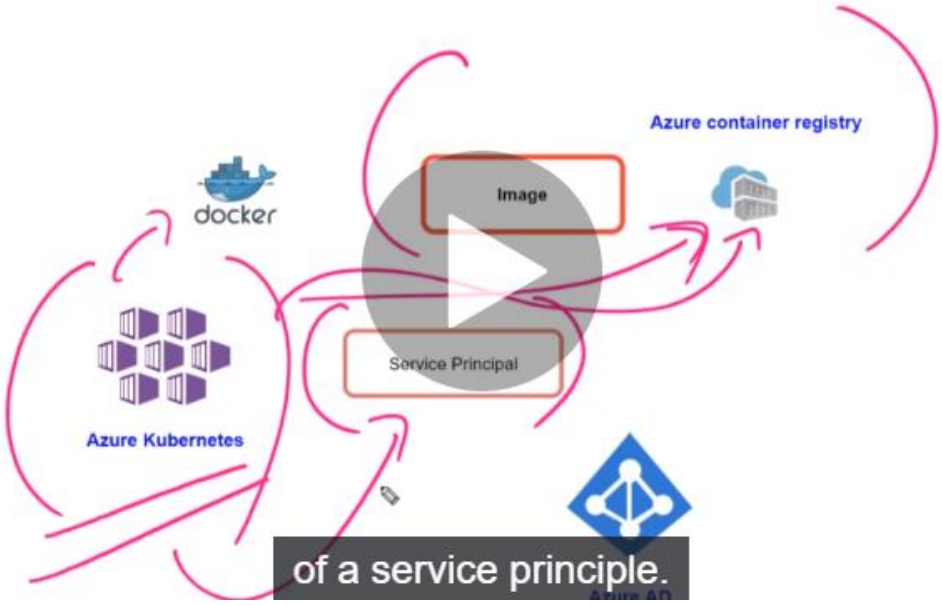
When you deploy your Kubernetes cluster, make sure that it is not a part of any availability zone.

1. **Azure Disks**
   Use Azure Disks to create a Kubernetes DataDisk resource. Disks can use:
- Azure Premium storage, backed by high-performance SSDs, or
- Azure Standard storage, backed by regular HDDs.
2. **Azure Files**
   Use Azure Files to mount an SMB 3.0 share backed by an Azure Storage account to pods. Files let you share data across multiple nodes and pods and can use:
- Azure Premium storage, backed by high-performance SSDs, or
- Azure Standard storage backed by regular HDDs.



Azure Container Registry

Azure Container registry allows you to build, store, and manage container images and artifacts in a private registry for all types of container deployments

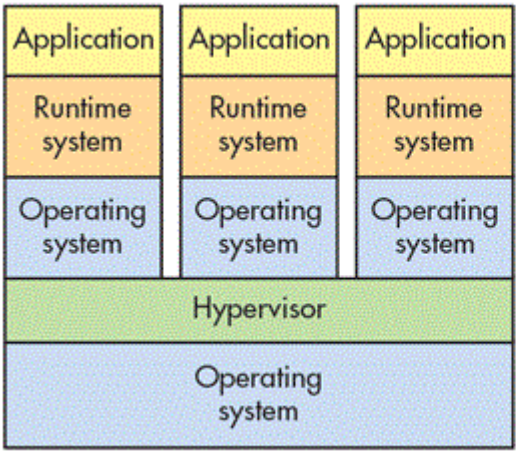


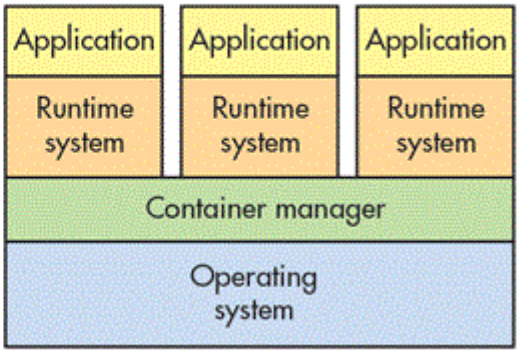
Difference b/w Containers & VM's

In traditional virtualization, a hypervisor virtualizes physical hardware. The result is that each virtual machine contains a guest OS, a virtual copy of the hardware that the OS requires to run and an application and its associated libraries and dependencies. VMs with different operating systems can be run on the same physical server. For example, a VMware VM can run next to a Linux VM, which runs next to a Microsoft VM, etc.

Instead of virtualizing the underlying hardware, containers virtualize the operating system (typically Linux or Windows) so each individual container contains only the application and its libraries and dependencies. Containers are small, fast, and portable because, unlike a virtual machine, containers do not need to include a guest OS in every instance and can, instead, simply leverage the features and resources of the host OS.

Just like virtual machines, containers allow developers to improve CPU and memory utilization of physical machines. Containers go even further, however, because they also enable microservice architectures, where application components can be deployed and scaled more granularly. This is an attractive alternative to having to scale up an entire monolithic application because a single component is struggling with load.





Azure – Monitor

Azure Monitor helps you maximize the availability and performance of your applications and services. It delivers a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments. This information helps you understand how your applications are performing and proactively identify issues affecting them and the resources they depend on.

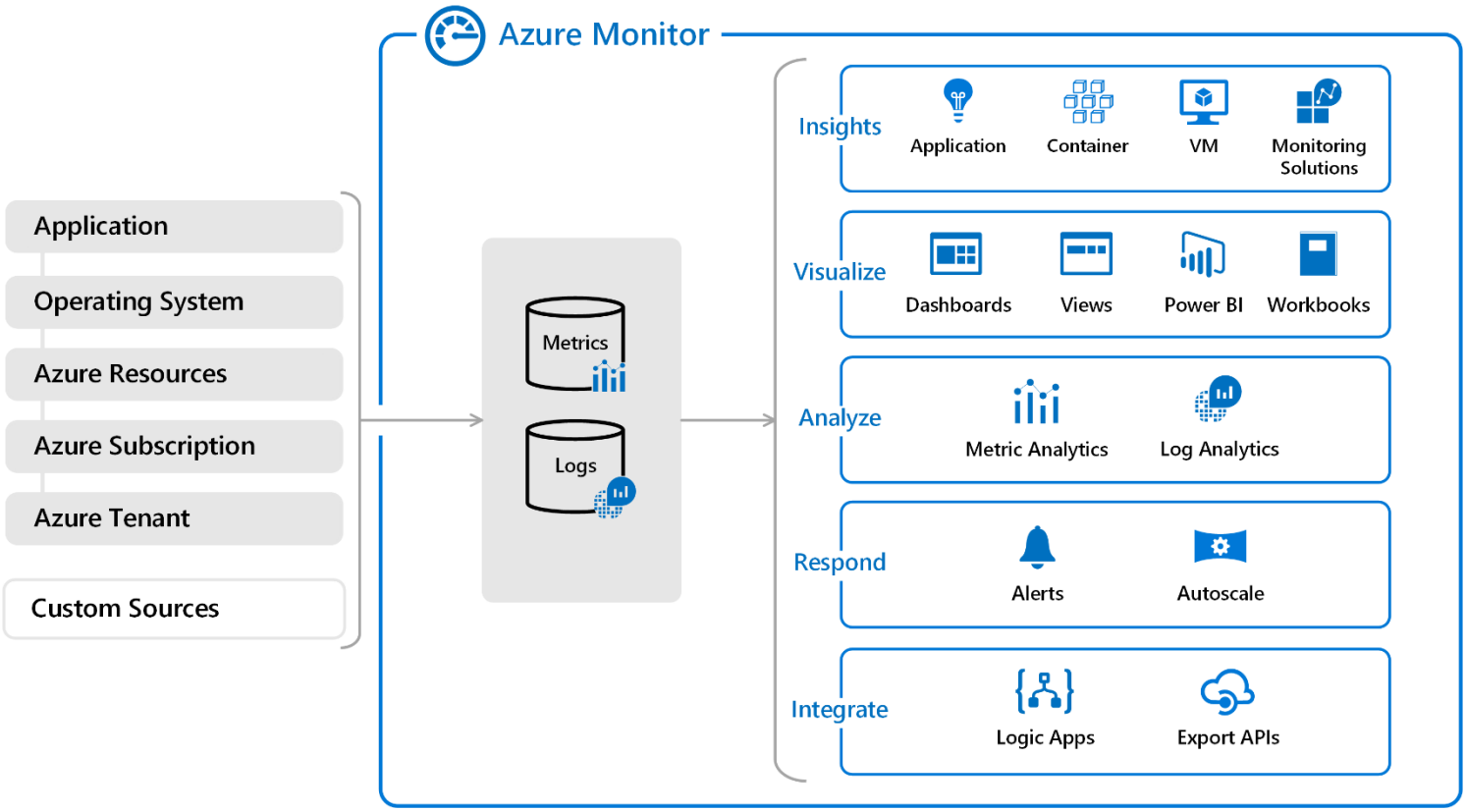
Just a few examples of what you can do with Azure Monitor include:

- Detect and diagnose issues across applications and dependencies with Application Insights
- Correlate infrastructure issues with VM insights and Container insights
- Drill into your monitoring data with Log Analytics for troubleshooting and deep diagnostics
- Support operations at scale with smart alerts and automated actions
- Create visualizations with Azure dashboards and workbooks
- Collect data from monitored resources using Azure Monitor Metrics

What does Azure Monitor collect?

Azure Monitor can collect data from a variety of sources. This ranges from your application, any operating system and services it relies on, down to the platform itself. Azure Monitor collects data from each of the following tiers:

- **Application monitoring data**: Data about the performance and functionality of the code you have written, regardless of its platform
- **Guest OS monitoring data**: Data about the operating system on which your application is running. This could be running in Azure, another cloud, or on-premises
- **Azure resource monitoring data**: Data about the operation of an Azure resource
- **Azure subscription monitoring data**: Data about the operation and management of an Azure subscription, as well as data about the health and operation of Azure itself
- **Azure tenant monitoring data**: Data about the operation of tenant-level Azure services, such as Azure Active Directory



Azure – VM Diagnostics Logs

Azure Diagnostics extension is an agent in Azure Monitor that collects monitoring data from the guest operating system of Azure compute resources including virtual machines.

The primary scenarios addressed by the diagnostics extension are:

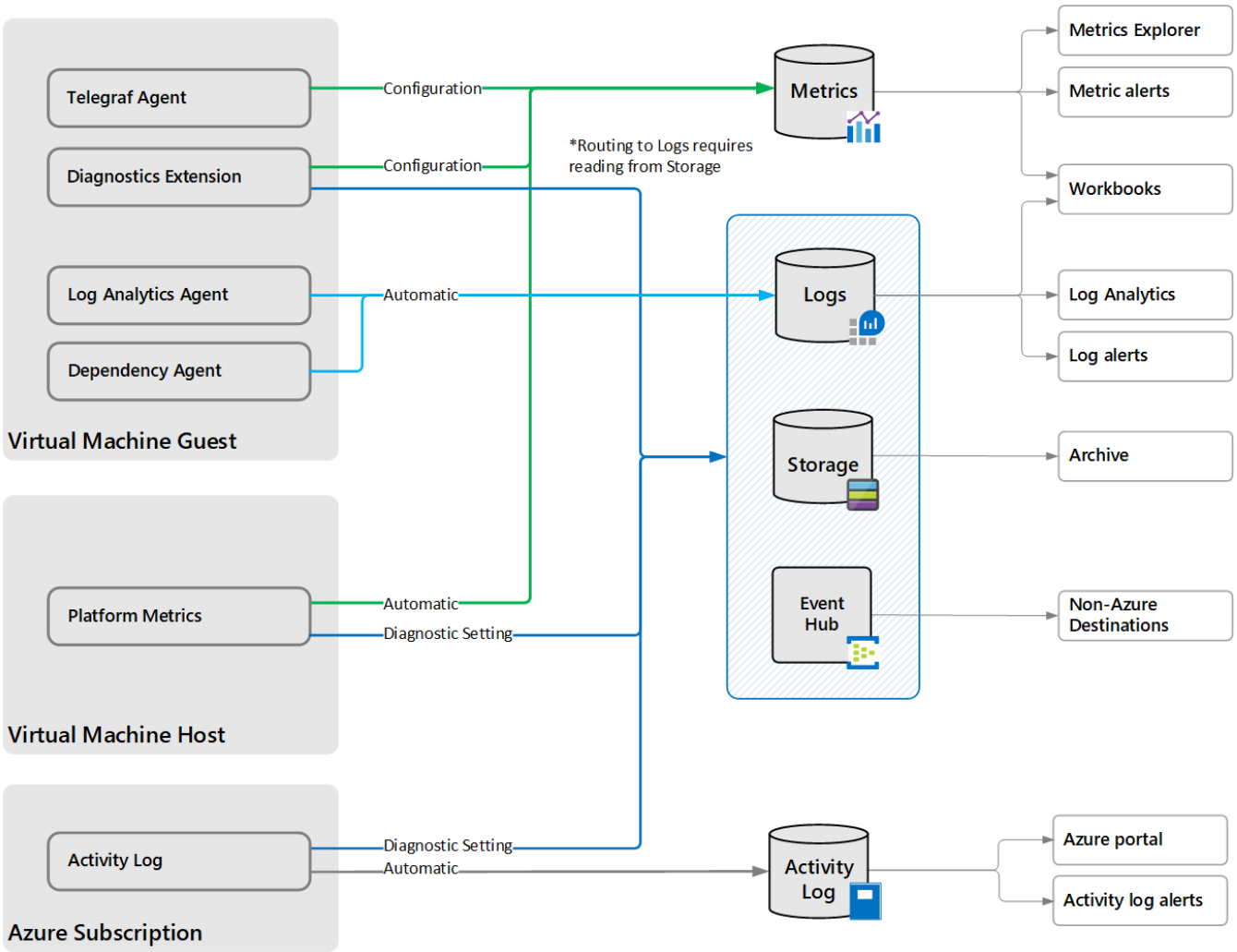
- Collect guest metrics into Azure Monitor Metrics
- Send guest logs and metrics to Azure storage for archiving
- Send guest logs and metrics to Azure event hubs to send outside of Azure

Azure Monitor Agent

The Azure Monitor Agent is meant to replace the Log Analytics agent, Agent Diagnostics extension and Telegraf agent for both Windows & Linux machines. It can send data to both Azure Monitor Logs and Azure Monitor Metrics and use Data Collection Rules (DCR) which provide a more scalable method of configuring data collection and destination for each agent.

Monitoring Azure resources with Azure Monitor describes the monitoring data generated by Azure resources and how you can use the features of Azure Monitor to analyze and alert on this data. You can collect and act on the same monitoring data from Azure virtual machines with the following differences:

- Platform metrics are collected automatically for virtual machines but only for the virtual machine host. You need an agent to collect performance data from the guest operating system
- Virtual machines don't generate resource logs which provide insight into operations that were performed within an Azure resource. You use an agent to collect log data from the guest operating system
- You can create diagnostic settings for a virtual machine to send platform metrics to other destinations such as storage and event hubs, but you can't configure these diagnostic settings in the Azure portal



Comparison to Log Analytics Agent

The Log Analytics agent in Azure Monitor can also be used to collect monitoring data from the guest operating system of virtual machines. You may choose to use either or both depending on your requirements. See Overview of the Azure Monitor agents for a detailed comparison of the Azure Monitor agents.

The key differences to consider are:

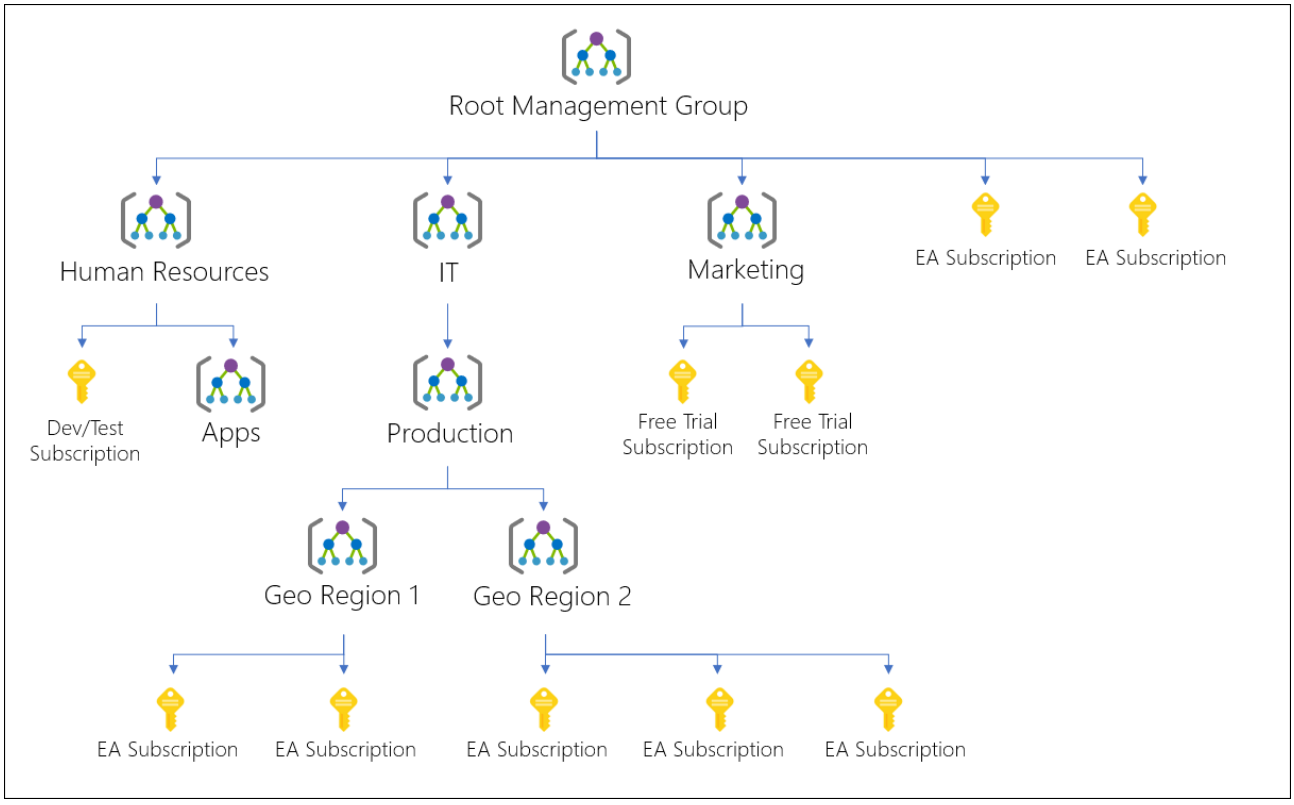
- Azure Diagnostics Extension can be used only with Azure virtual machines. The Log Analytics agent can be used with virtual machines in Azure, other clouds, and on-premises
- Azure Diagnostics extension sends data to Azure Storage, Azure Monitor Metrics (Windows only) and Event Hubs. The Log Analytics agent collects data to Azure Monitor Logs
- The Log Analytics agent is required for solutions, VM insights, and other services such as Azure Security Center

Azure – Management Group & Subscriptions

Azure management groups provide a way for an organization to control and manage access, compliance, and policies for their subscription within their tenant. These containers provide scope above subscriptions, allowing a level of inheritance applied to that management group or any parent group. This allows a single mechanism to leverage RBAC (role-based access control) to your subscriptions rather than assigning them individually.

Management Groups Facts:

- A subscription can belong to one management group
- Management groups can only be six levels deep
- You are allowed 10,000 management groups in a single tenant
- There is a single top-level root management group that cannot be deleted
- New subscriptions are automatically placed under the root
- Any user access assigned to a management group is applied to all resources and child management groups



Root Management Group Facts:

- By default, the root management group's display name is Tenant root group. The ID is the Azure Active Directory ID
- To change the display name, your account must be assigned the Owner or Contributor role on the root management group. See Change the name of a management group to update the name of a management group
- The root management group can't be moved or deleted, unlike other management groups
- All subscriptions and management groups fold up to the one root management group within the directory
- All resources in the directory fold up to the root management group for global management
- New subscriptions are automatically defaulted to the root management group when created
- All Azure customers can see the root management group, but not all customers have access to manage that root management group
  - Everyone who has access to a subscription can see the context of where that subscription is in the hierarchy
  - No one is given default access to the root management group. Azure AD Global Administrators are the only users that can elevate themselves to gain access. Once they have access to the root management group, the global administrators can assign any Azure role to other users to manage it
- In SDK, the root management group, or 'Tenant Root', operates as a management group

Azure – Resource Locks

As an administrator, you can lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. The lock overrides any permissions the user might have.

Types of Locks

You can set the lock level to **CanNotDelete** or **ReadOnly**:

1. **CanNotDelete** – means authorized users can still read and modify a resource, but they can't delete the resource
2. **ReadOnly** – means authorized users can read a resource, but they can't delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role

Microsoft recommends locking all of your storage accounts with an Azure Resource Manager lock to prevent accidental or malicious deletion of the storage account. There are two types of Azure Resource Manager resource locks:

1. A **CannotDelete** lock prevents users from deleting a storage account, but permits reading and modifying its configuration
2. A **ReadOnly** lock prevents users from deleting a storage account or modifying its configuration, but permits reading the configuration

Who can Apply Locks?

To create or delete management locks, you must have access to Microsoft.Authorization/* or Microsoft.Authorization/locks/* actions. Of the built-in roles, only Owner and User Access Administrator are granted those actions.

Azure – Policy

Azure Policy is a service in Azure which allows you create polices which enforce and control the properties of a resource. When these policies are used, they enforce different rules and effects over your resources, so those resources stay compliant with your IT governance standards.

Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity. It also helps to bring your resources to compliance through bulk remediation for existing resources and automatic remediation for new resources.

Common use cases for Azure Policy include implementing governance for resource consistency, regulatory compliance, security, cost, and management. Policy definitions for these common use cases are already available in your Azure environment as built-ins to help you get started.

To summarize, Azure policy is basically 3 components; policy definition, assignment and parameters:

- **Policy Definition** – is the conditions which you want controlled. There are build-in definitions such as controlling what type of resources can be deployed to enforcing the use of tags on all resources
- **Policy Assignment** – is the scope of what the policy definition can take effect around. Scope of assignment can be assigned to an individual, resources, resource group or management group. Policy assignments are inherited by all child resources
- Policy **parameters** are used by reducing the number of policy definitions you must create. Parameters would be used to define which type of VM SKU's to deploy or defining a specific location

Azure Policy vs Azure RBAC

There are a few key differences between Azure Policy and Azure role-based access control (Azure RBAC). Azure Policy evaluates state by examining properties on resources that are represented in Resource Manager and properties of some Resource Providers. Azure Policy doesn't restrict actions (also called operations). Azure Policy ensures that resource state is compliant to your business rules without concern for who made the change or who has permission to make a change. Some Azure Policy resources, such as policy definitions, initiative definitions, and assignments, are visible to all users. This design enables transparency to all users and services for what policy rules are set in their environment.

Azure RBAC focuses on managing user actions at different scopes. If control of an action is required, then Azure RBAC is the correct tool to use. Even if an individual has access to perform an action, if the result is a non-compliant resource, Azure Policy still blocks the create or update.

The combination of Azure RBAC and Azure Policy provides full scope control in Azure

What is an Azure Initiative?

An Azure initiative is a collection of Azure policy definitions that are grouped together towards a specific goal or purpose in mind. Azure initiatives simplify management of your policies by grouping a set of policies together as one single item. For example, you could use the PCI-DSS built-in initiative which has all the policy definitions that are centered around meeting PCI-DSS compliance.

Azure – Blueprints

An Azure Blueprint is a package for creating specific sets of standards and requirements that govern the implementation of Azure services, security, and design. Such packages are reusable so that consistency and compliance among resources can be maintained.

A policy included in a blueprint offers the ability to create the correct pattern or design when the blueprint is assigned. Additionally, a policy inclusion ensures that only approved changes can be made to the resources or environment to which the blueprint was assigned. This ensures ongoing compliance with the blueprint.

Azure Blueprints are made up of artifacts. Resources supported as artifacts include resource groups, resource manager templates, policy assignments, and role assignments. Resource Groups allow an administrator to organize resources and to structure them as needed. They also serve as scope limiters for policy assignment artifacts, role assignment artifacts, and Azure Resource Manager templates.

Blueprint Resources

As mentioned previously, Azure Blueprints are made up of artifacts. Resources supported as artifacts include resource groups, resource manager templates, policy assignments, and role assignments.

Azure Resource Group Templates are useful when designing complex environments, such as those managed with Azure Automation State Configuration. Leveraging templates makes standardization of such environments far easier than building them individually.

Resource Groups allow an administrator to organize resources and to structure them as needed. They also serve as scope limiters for policy assignment artifacts, role assignment artifacts, and Azure Resource Manager templates.

Policy Assignments provide a means for applying policy to a subscription to which a blueprint is assigned. That said, the policy must be within the scope of the blueprint containing the policy. Parameters defined with a policy are assigned during blueprint creation or during blueprint assignment.

Role Assignments provide a means for adding existing users or groups to a built-in role. This is done to ensure the correct people have the proper access to Azure resources. Role assignments are often defined for an entire subscription, but they can also be scoped to a specific resource group that's included in the blueprint.

Lifecycle of an Azure Blueprint

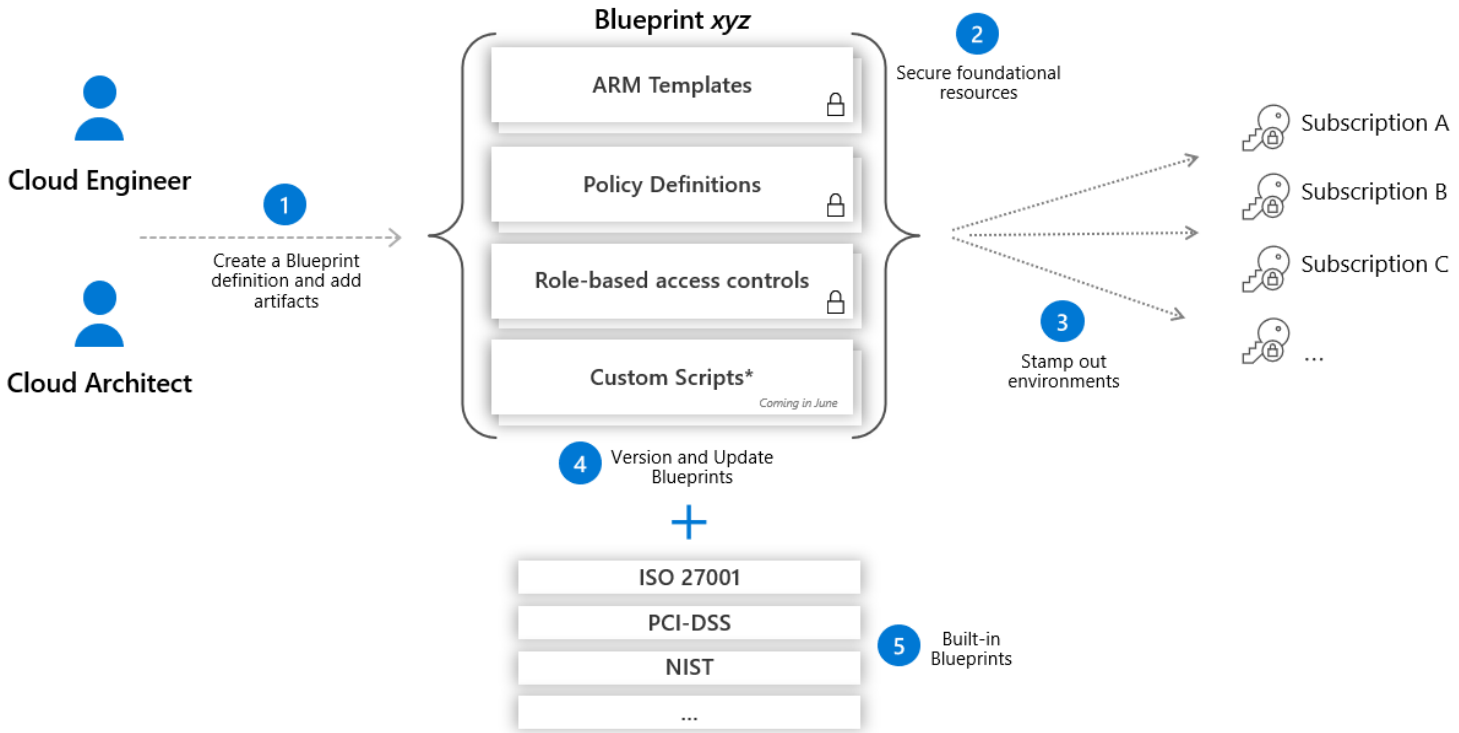
Like many resources within Azure, a blueprint in Azure Blueprints has a typical and natural lifecycle. They're created, deployed, and finally deleted when no longer needed or relevant. Azure Blueprints supports standard lifecycle operations.

To fully understand a blueprint and the stages, we'll cover standard lifecycle:

1. Created and editing a blueprint
2. Publishing the blueprint
3. Creating and editing a new version of the blueprint
4. Publishing a new version of the blueprint
5. Deleting a specific version of the blueprint
6. Deleting the blueprint

The lifecycle of an Azure Blueprint begins with the creation of the blueprint and then the publishing of the blueprint. New versions of the blueprint are then created and published as needed. The lifecycle of an Azure Blueprint ends with deletion of specific versions of the blueprint, and then of the blueprint itself.

While Azure Blueprints are like Resource Manager Templates and Azure Policies, the blueprints differ because they are "living and breathing", so to speak. As such, they retain their relationships to the resources they have been assigned to and can be tracked and audited. This is not possible with templates and policies.



Resource Locks in Azure Blueprint

Resource locks allows you to lock resources and prevent the users from changing them.

Resources locks are deployed by Azure Blueprints are only applied to resources deployed by the blueprint assignment. Existing resources, such as those in resource groups that already exist, don't have locks added to them.

Resources created by artifacts in a blueprint assignment have four states:

- Not Locked
- Read Only
- Cannot Edit / Delete
- Cannot Delete

1. **Don't Lock**

Not Locked – Resources aren't protected by Azure Blueprints. This state is also used for resources added to a Read Only or Do Not Delete resource group artifact from outside a blueprint assignment

2. **Read Only (Resource Group)**

Cannot Edit / Delete – The resource group is read only and tags on the resource group can't be modified. Not Locked resources can be added, moved, changed, or deleted from this resource group

3. **Read Only (Non-Resource Group)**

Read Only – The resource group can't be altered in any way. No changes and it can't be deleted

4. **Do Not Delete**

Cannot Delete – The resources can be altered, but can't be deleted. Not Locked resources can be added, moved, changed, or deleted from this resource group

Azure – Security Center

Azure Security Center helps you prevent, detect, and respond to threats with increased visibility into and control over the security of your resources. It provides integrated security monitoring and policy management across your subscriptions, helps detect threats that might otherwise go unnoticed, and works with a broad ecosystem of security solutions.

Security Center uses the Log Analytics agent to collect and store data.

More detailed definition

Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud - whether they're in Azure or not - as well as on premises.

Keeping your resources safe is a joint effort between your cloud provider, Azure, and you, the customer. You have to make sure your workloads are secure as you move to the cloud, and at the same time, when you move to IaaS (infrastructure as a service) there is more customer responsibility than there was in PaaS (platform as a service), and SaaS (software as a service). Azure Security Center provides you the tools needed to harden your network, secure your services and make sure you're on top of your security posture.

Azure Security Center addresses the three most urgent security challenges:

- Rapidly changing workloads
- Increasingly sophisticated attacks
- Security skills are in short supply

Security Center provides you with the tools to:

- Strengthen security posture
- Protect against threats

- Get secure faster

Architecture

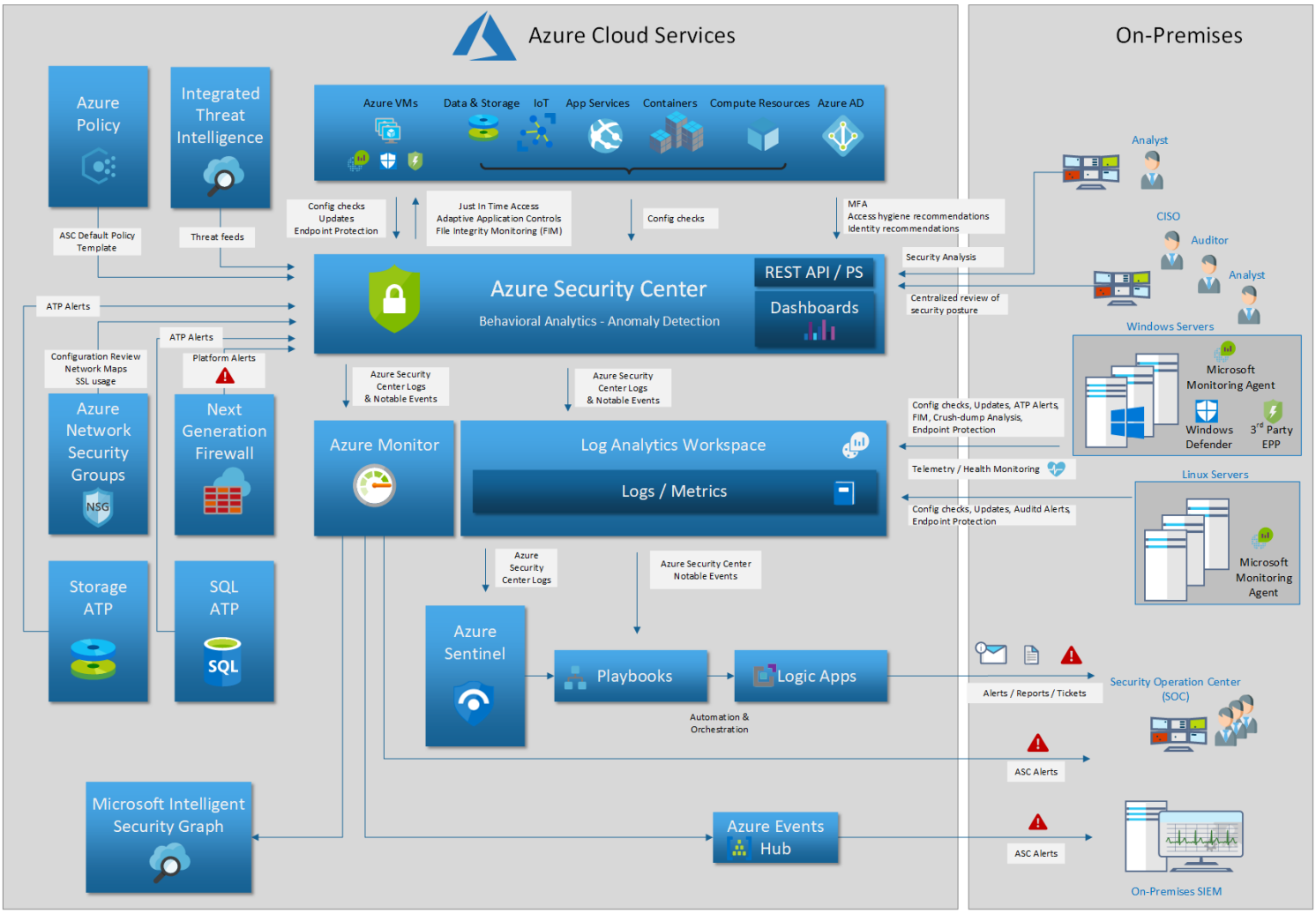
Security Center is natively part of Azure, PaaS services in Azure - including Service Fabric, SQL Database, SQL Managed Instance, and storage accounts - are monitored and protected by Security Center without necessitating any deployment.

In addition, Security Center protects non-Azure servers and virtual machines in the cloud or on premises, for both Windows and Linux servers, by installing the Log Analytics agent on them. Azure virtual machines are auto provisioned in Security Center.

The events collected from the agents and from Azure are correlated in the security analytics engine to provide you tailored recommendations (hardening tasks), that you should follow to make sure your workloads are secure, and security alerts. You should investigate such alerts as soon as possible to make sure malicious attacks aren't taking place on your workloads.

When you enable Security Center, the security policy built-in to Security Center is reflected in Azure Policy as a built-in initiative under the Security Center category. The built-in initiative is automatically assigned to all Security Center registered subscriptions (regardless of whether or not they have Azure Defender enabled). The built-in initiative contains only Audit policies.

Diagram link https://www.managedsentinel.com/azure-security-center/



Azure Security Center Components - July 2019 © Marius Mocanu, Adrian Grigorof
High Definition available at http://www.managedsentinel.com

Managed Sentinel

Security Center Agents

Azure Security Center collects data from your resources using the relevant agent or extensions for that resource and the type of data collection you have enabled.

Security Center collects data from your Azure virtual machines (VMs), virtual machine scale sets, IaaS containers, and non-Azure (including on-premises) machines to monitor for security vulnerabilities and threats.

Data collection is required to provide visibility into missing updates, misconfigured OS security settings, endpoint protection status, and health and threat protection. Data collection is only needed for compute resources such as VMs, virtual machine scale sets, IaaS containers, and non-Azure computers.

You can benefit from Azure Security Center even if you don't provision agents. However, you'll have limited security and the capabilities listed above aren't supported.

https://techcommunity.microsoft.com/t5/azure-security-center/azure-security-center-monitoring-agent-deployment-options/ba-p/817520

Types of Agents:

1. Direct Agents
2. Log Analytics Agent extension

Direct Agents

The direct agent is a standalone installation. This installation is an MSI\EXE file hence, organizations can leverage a deployment tool such as System Center Configuration Manager or other scripted way to deploy it.

To extend visibility and security center capabilities, we can install the agent on computers running outside of Azure, including resources running on-premises and in other clouds.

Log Analytics Agent Extension

The extension installs the Log Analytics agent on Azure virtual machines and enrolls virtual machines into an existing Log Analytics workspace.

Types of features Security Center offers:

1. Security Recommendations
2. Azure Security Alerts
3. Vulnerability Assessments
4. Azure Defender
5. Just-in-Time
6. Network Map
7. Adaptive Application Control
8. Continuous Assessments

https://docs.microsoft.com/en-us/azure/security-center/security-center-services?tabs=features-windows

Security Recommendations in Security Center

Azure Security Center analyzes the security state of your Azure resources. When potential security vulnerabilities are identified, recommendations are created. The recommendations guide you through the process of configuring the needed control. Examples are:

- Provisioning of anti-malware to help identify and remove malicious software
- Network security groups and rules to control traffic to virtual machines
- Provisioning of a web application firewall to help defend against attacks targeting your web applications
- Deploying missing system updates
- Addressing OS configurations that do not match the recommended baselines

Security Alerts

Azure Security Center automatically collects, analyzes, and fuses log data from your Azure resources, the network, and partner solutions like antimalware and firewalls. When threats are detected, a security alert is created. Examples include detection of:

- Compromised virtual machines communicating with known malicious IP addresses
- Advanced malware detected using Windows error reporting
- Brute force attacks against virtual machines
- Security alerts from integrated partner security solutions such as Anti-Malware or Web Application Firewalls

Alerts are the notifications that Security Center generates when it detects threats on your resources. Security Center prioritizes and lists the alerts, along with the information needed for you to quickly investigate the problem. Security Center also provides detailed steps to help you remediate attacks. Alerts data is retained for 90 days.

A **security incident** is a collection of related alerts, instead of listing each alert individually. Security Center uses Cloud smart alert correlation to correlate different alerts and low fidelity signals into security incidents.

Using incidents, Security Center provides you with a single view of an attack campaign and all of the related alerts. This view enables you to quickly understand what actions the attacker took, and what resources were affected.

Alerts Level Classifications

- **High** – There is a high probability that your resource is compromised
- **Medium** – This is probably a suspicious activity might indicate that a resource is compromised
- **Low** – This might be a benign positive or a blocked attacked
- **Informational** – An incident appears on their own to be only informational

Regulatory Compliance

Azure Security Center continually compares the configuration of your resources with requirements in industry standards, regulations, and benchmarks. The regulatory compliance dashboard provides insights into your compliance posture based on how you're meeting specific compliance requirements.

Industry standards, regulatory standards, and benchmarks are represented in Security Center's regulatory compliance dashboard. Each standard is an initiative defined in Azure Policy.

The regulatory compliance dashboard provides insight into your compliance posture for a set of supported standards and regulations, based on continuous assessments of your Azure environment.

The assessments performed by Azure Security Center analyze risk factors in your hybrid cloud environment in accordance with security best practices. These assessments are mapped to selective compliance controls from a supported set of standards. In the regulatory compliance dashboard, you get a single view of the status of all assessments within your environment, in the context of a particular standard or regulation. As you act on the recommendations and reduce risk factors in your environment, you can see your compliance posture improve.

All the compliance which Microsoft Azure provides

https://docs.microsoft.com/en-us/azure/compliance/

Prerequisites

- Azure Defender must be enabled
- You must be signed in with an account that has reader access to the policy compliance data (**Security Reader** is sufficient). The role of **Global Reader** for the subscription will work. At a minimum, you'll need to have **Resource Policy Contributor** and **Security Admin** roles assigned

Network Map

Azure Security Center continuously analyzes the security state of your Azure resources for network security best practices. When Security Center identifies potential security vulnerabilities, it creates recommendations that guide you through the

process of configuring the needed controls to harden and protect your resources.

The Networking features of Security Center include:

- Network map (requires Azure Defender)
- Adaptive network hardening (requires Azure Defender)
- Networking security recommendations

The default view of the topology map displays:

- Subscriptions you selected in Azure. The map supports multiple subscriptions.
- VMs, subnets, and VNets of the Resource Manager resource type (Classic Azure resources are not supported)
- Peered VNets
- Only resources that have network recommendations with a high or medium severity
- Internet facing resources
- The map is optimized for the subscriptions you selected in Azure. If you modify your selection, the map is recalculated and re-optimized based on your new settings

Vulnerability Assessments

Vulnerability management is a critical part of an organization's security and compliance strategy. Security flaws are constantly being discovered and fixed by vendors, making it hard for organizations to keep up with security patches. Meanwhile, missing security updates are easy targets for attackers and can compromise the security of the entire network.

Traditional network-based scanners are available in the Azure Marketplace and successfully used by customers for vulnerability assessment. Nevertheless, many Azure customers are looking for continuous agent-based solutions for the following reasons:

- Cloud environments tend to be more dynamic. Virtual Machines (VMs) are being spun up and down frequently, making it more difficult for a scheduled scan to cover all assets
- Network based scanners require a user account on target virtual machines in order to provide full insight. In many cases, however, customers lack the ability to centrally manage such accounts in the cloud
- When resources are spread across different virtual networks, multiple network-based scanners are required to get access to all virtual machines

Security Center regularly checks your connected machines to ensure they're running vulnerability assessment tools.

When a machine is found that doesn't have vulnerability assessment solution deployed, Security Center generates the following security recommendation:

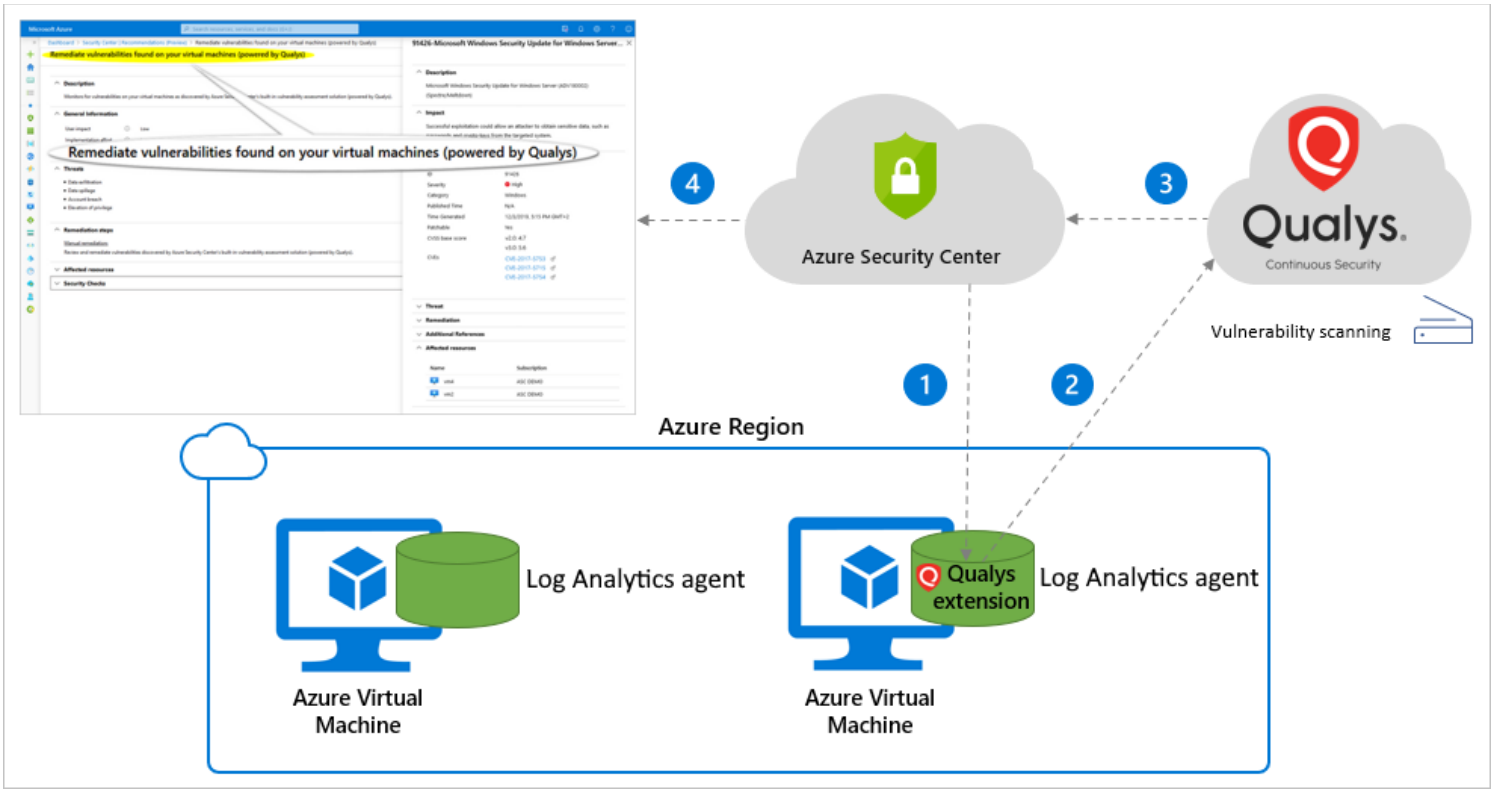
A vulnerability assessment solution should be enabled on your virtual machines

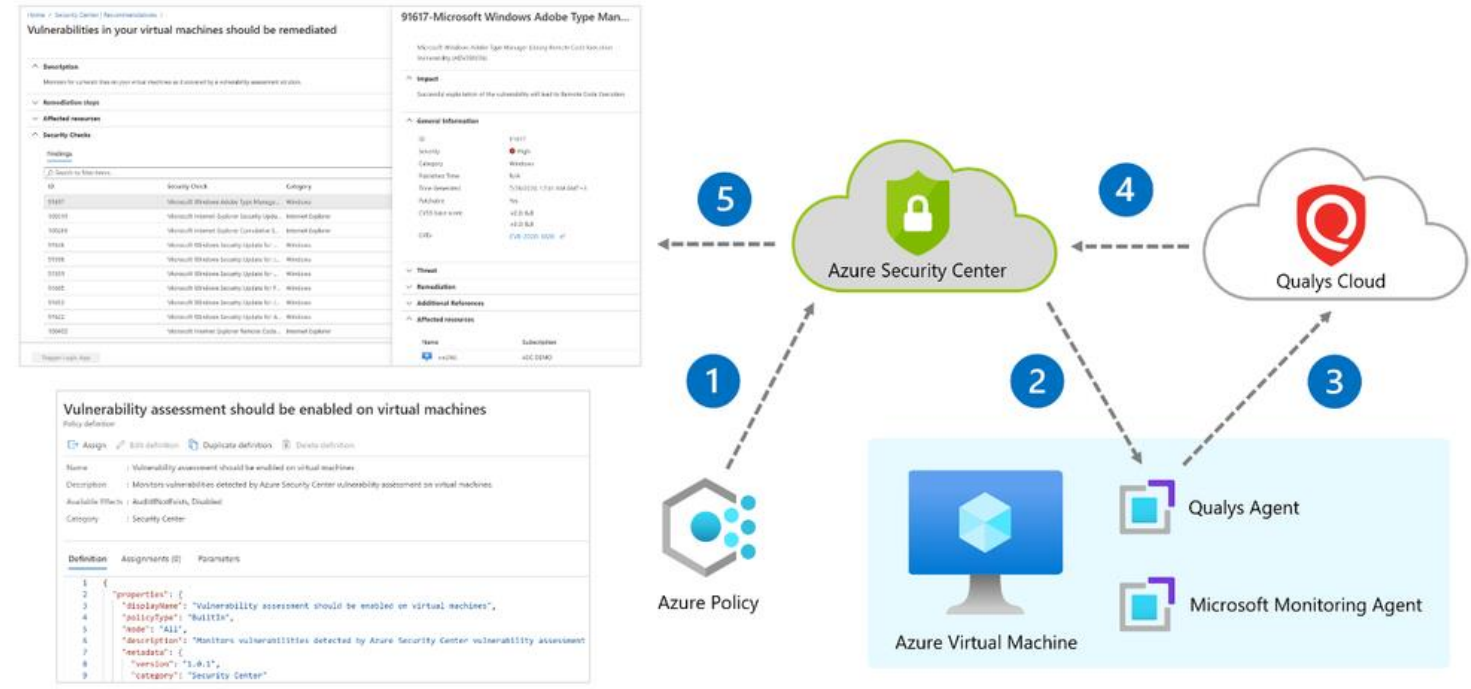
The vulnerability scanner included with Azure Security Center is powered by Qualys. Qualys' scanner is one of the leading tools for real-time identification of vulnerabilities. It's only available with Azure Defender for servers. You don't need a Qualys license or even a Qualys account - everything's handled seamlessly inside Security Center.

How the integration works

The vulnerability scanner extension works as follows:

1. **Deploy** – Azure Security Center monitors your machines and provides recommendations to deploy the Qualys extension on your selected machines
2. **Gather Information** – The extension collects artifacts and sends them for analysis in the Qualys cloud service in the defined region
3. **Analyze** – Qualys' cloud service conducts the vulnerability assessment and sends tis findings to Security Center
4. **Report** – The findings are available in Security Center





After the scanning and reporting, your machines will appear in one or more of the following groups:

- **Healthy** resources – Security Center has detected a vulnerability assessment solution running on these machines
- **Unhealthy** resources – A vulnerability scanner extension can be deployed to these machines
- **Not Applicable** resources – These machines can't have a vulnerability scanner extension deployed

Findings are categorized by severity:

- High = Critical + Urgent
- High = Serious + Medium
- Low = All the reset

Just-In-Time (JIT) Virtual Machine (VM) Access

Lock down inbound traffic to your Azure Virtual Machines with Azure Security Center's just-in-time (JIT) virtual machine (VM) access feature. This reduces exposure to attacks while providing easy access when you need to connect to a VM.

With Just-in-Time VM access, you can define what VM and what ports can be opened and controlled and for how long. The Just-in-Time access locks down and limits the ports of Azure virtual machines in order to overcome malicious attacks on the virtual machine, therefore only providing access to a port for a limited amount of time. Basically, you block all inbound traffic at the network level.

When Just-In-Time access is enabled, every user's request for access will be routed through Azure RBAC, and access will be granted only to users with the right credentials. Once a request is approved, the Security Center automatically configures the NSGs to allow inbound traffic to these ports – only for the requested amount of time, after which it restores the NSGs to their previous states.

The just-in-time option is available only for the standard security center tier and is only applicable for VMs deployed via Azure resource manager.

Continuous Assessments

Security Center continuously discovers new resources that are being deployed across your workloads and assesses whether they are configured according to security best practices, if not, they're flagged and you get a prioritized list of recommendations for what you need to fix in order to protect your machines. This list of recommendations is enabled and supported by Azure Security Benchmark, the Microsoft-authored, Azure-specific set of guidelines for security and compliance best practices based on common compliance frameworks. This widely respected benchmark builds on the controls from the Center for Internet Security (CIS) and the National Institute of Standards and Technology (NIST) with a focus on cloud-centric security.

Workflow Automation

Security Center workflow automation allows you to create a trigger and from that trigger, initiate an action. These workflows are created at the subscription level, and you are able to have multiple workflows to cover multiple triggers. This feature can trigger Logic Apps on security alerts, recommendations, and changes to regulatory compliance.

The logic app designer supports these Security Center triggers:

- When an Azure Security Center Recommendation is created or triggered
- When an Azure Security Center Alert is created or triggered
- When a Security Center regulatory compliance assessment is created or triggered

Adaptive Application Controls

It's one of the advanced protections that is included in the Azure Security Center that falls under the **Cloud Workload Protection Platform** (CWPP) for threat detection and response, which is something you must consider for your Windows and Linux systems whether they are running on Azure, on-premises or in other cloud environments.

Adaptive application controls are an intelligent and automated solution for defining allow lists of known-safe applications for your machines.

Often, organizations have collections of machines that routinely run the same processes. Security Center uses machine learning to analyze the applications running on your machines and create a list of the known-safe software. Allow lists are based on your specific Azure workloads, and you can further customize the recommendations using the instructions below.

When you've enabled and configured adaptive application controls, you'll get security alerts if any application runs other than the ones you've defined as safe.

Benefits of Adaptive Application Controls

By defining lists of known-safe applications, and generating alerts when anything else is executed, you can achieve multiple oversight and compliance goals:

- Identify potential malware, even any that might be missed by antimalware solutions
- Improve compliance with local security policies that dictate the use of only licensed software
- Identify outdated or unsupported versions of applications
- Identify software that's banned by your organization but is nevertheless running on your machines
- Increase oversight of apps that access sensitive data

Azure Defender

Azure Security Center's features cover the two broad pillars of cloud security:

- **Cloud security posture management (CSPM)** – Security Center is available for free to all Azure users. The free experience includes CSPM features such as secure score, detection of security misconfigurations in your Azure machines, asset inventory, and more. Use these CSPM features to strengthen your hybrid cloud posture and track compliance with the built-in policies.
- **Cloud workload protection (CWP)** – Security Center's integrated cloud workload protection platform (CWPP), Azure Defender, brings advanced, intelligent, protection of your Azure and hybrid resources and workloads. Enabling Azure Defender brings a range of additional security features as described on this page. In addition to the built-in policies, when you've enabled any Azure Defender plan, you can add custom policies and initiatives. You can add regulatory standards - such as NIST and Azure CIS - as well as the Azure Security Benchmark for a truly customized view of your compliance.

Azure Defender provides security alerts and advanced threat protection for virtual machines, SQL databases, containers, web applications, your network, and more.

As well as defending your Azure environment, you can add Azure Defender capabilities to your hybrid cloud environment:

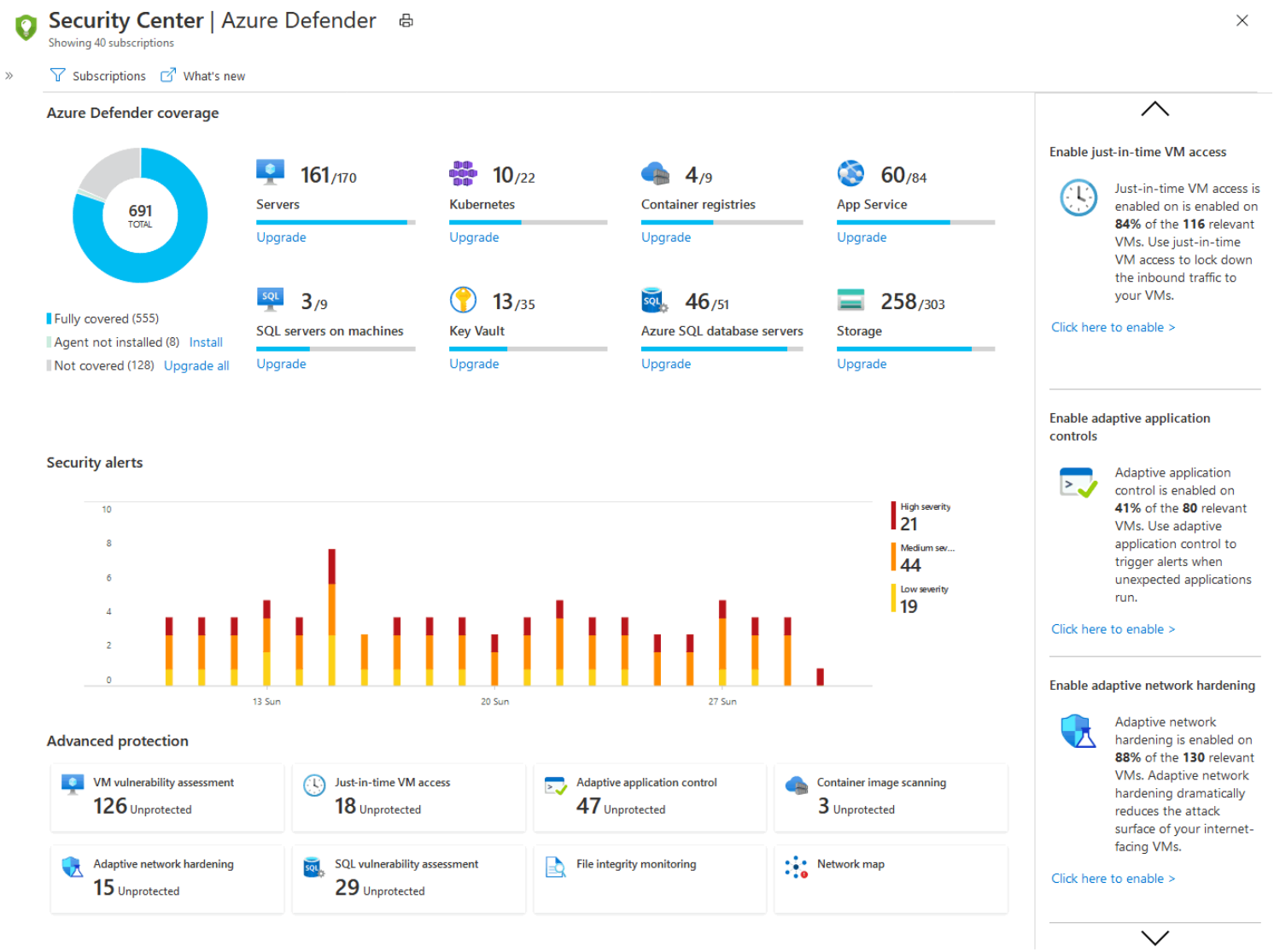
- Protect your non-Azure servers
- Protect your virtual machines in other clouds (such as AWS and GCP)

You'll get customized threat intelligence and prioritized alerts according to your specific environment so that you can focus on what matters the most.

To extend protection to virtual machines and SQL databases that are in other clouds or on-premises, deploy Azure Arc and enable Azure Defender. Azure Arc for servers is a free service, but services that are used on Arc enabled servers, for example Azure Defender, will be charged as per the pricing for that service.

Azure Security Center provides unified security management and threat protection across your hybrid and multi-cloud workloads. While the free features offer limited security for your Azure resources only, enabling Azure Defender extends these capabilities to on-premises and other clouds. Azure Defender helps you find and fix security vulnerabilities, apply access and application controls to block malicious activity, detect threats using analytics and intelligence, and respond quickly when under attack. You can try Azure Defender at no cost.

The Azure Defender dashboard in Security Center provides visibility and control of the CWP features for your environment:



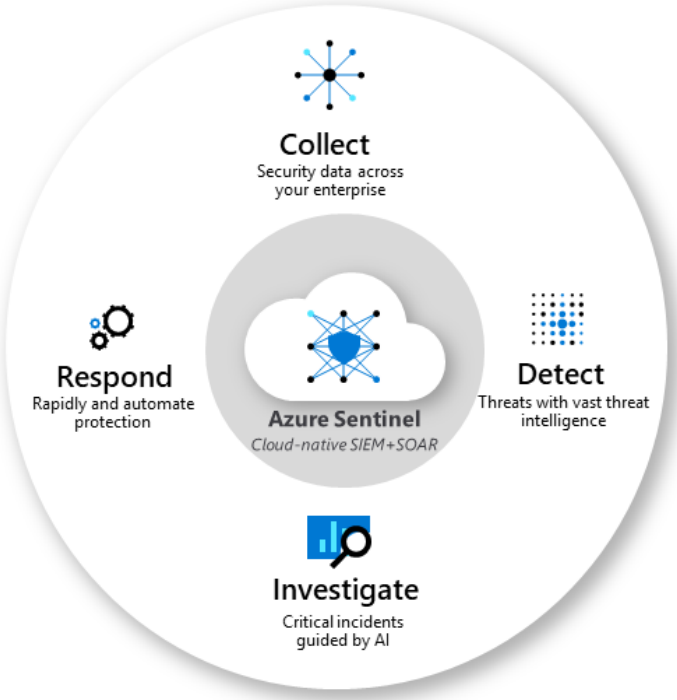
Azure – Sentinel

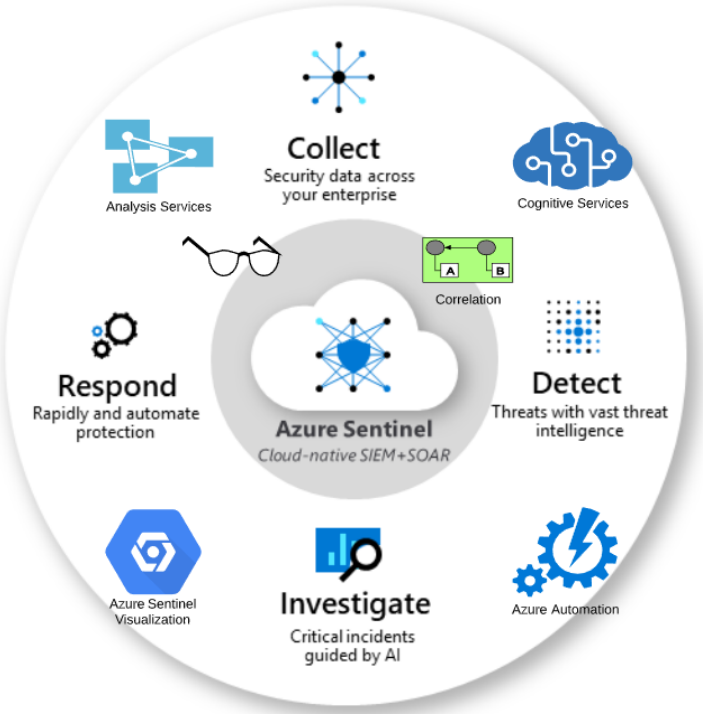
Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Azure Sentinel is your birds-eye view across the enterprise alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution times frames.

- **Collect data at cloud scale** – across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.
- **Detect previously undetected threats** – and minimize false positives using Microsoft's analytics and unparalleled threat intelligence
- **Investigate threats with artificial intelligence** – and hunt for suspicious activities at scale, tapping into years of cyber security work at Microsoft
- **Respond to incidents rapidly** – with built-in orchestration and automation of common tasks

Azure Sentinel comes with a number of connectors for Microsoft solutions, available out of the box and providing real-time integration, including Microsoft 365 Defender (formerly Microsoft Threat Protection) solutions, and Microsoft 365 sources, including Office 365, Azure AD, Microsoft Defender for Identity (formerly Azure ATP), and Microsoft Cloud App Security, and more. In addition, there are built-in connectors to the broader security ecosystem for non-Microsoft solutions. You can also use common event format, Syslog or REST-API to connect your data sources with Azure Sentinel as well.





Microsoft Sentinel Solution Overview

Data Collection and Aggregation

Microsoft Azure Sentinel seamlessly integrates with a variety of native and 3rd party data sources, granting security teams the ability to collect and analyze massive amounts of network data across deployments, users, applications, and devices each second. Azure Sentinel automatically correlates abnormal event data and create a case for immediate analysis and response.

- Collects user, application, server, and device data on-premise or in the cloud
- Built-in connectors for simplified onboarding of popular security tools
- Real-time solution integration
- Extensive architecture to support custom collectors

Security Orchestration and Automation

Microsoft Azure Sentinel can be used to automate everyday security tasks, such as event alerts, threat responses, and process workflows to streamline company security efforts from end to end. In-house teams can choose to create their workbooks or leverage existing workbooks to create highly-efficient, automated security processes for detecting and mitigating network threats.

- Pre-built and customizable playbooks
- Integrates with over 200 data connectors
- Setup automated threat responses
- Integration with Azure Logic Apps to automate workflows

Alert Visibility and Analytics

Microsoft Azure Sentinel gives security teams live insight into network traffic through a variety of rich user displays and interactive dashboards. From there, analysts can attend to high-priority alerts with relevant context into the location of the activity, the type of threat detected, a timeline of events, and several other useful data points the team may need to mitigate the threat successfully.

- Instant visualization and analysis of network data
- Pre-built and customizable dashboards

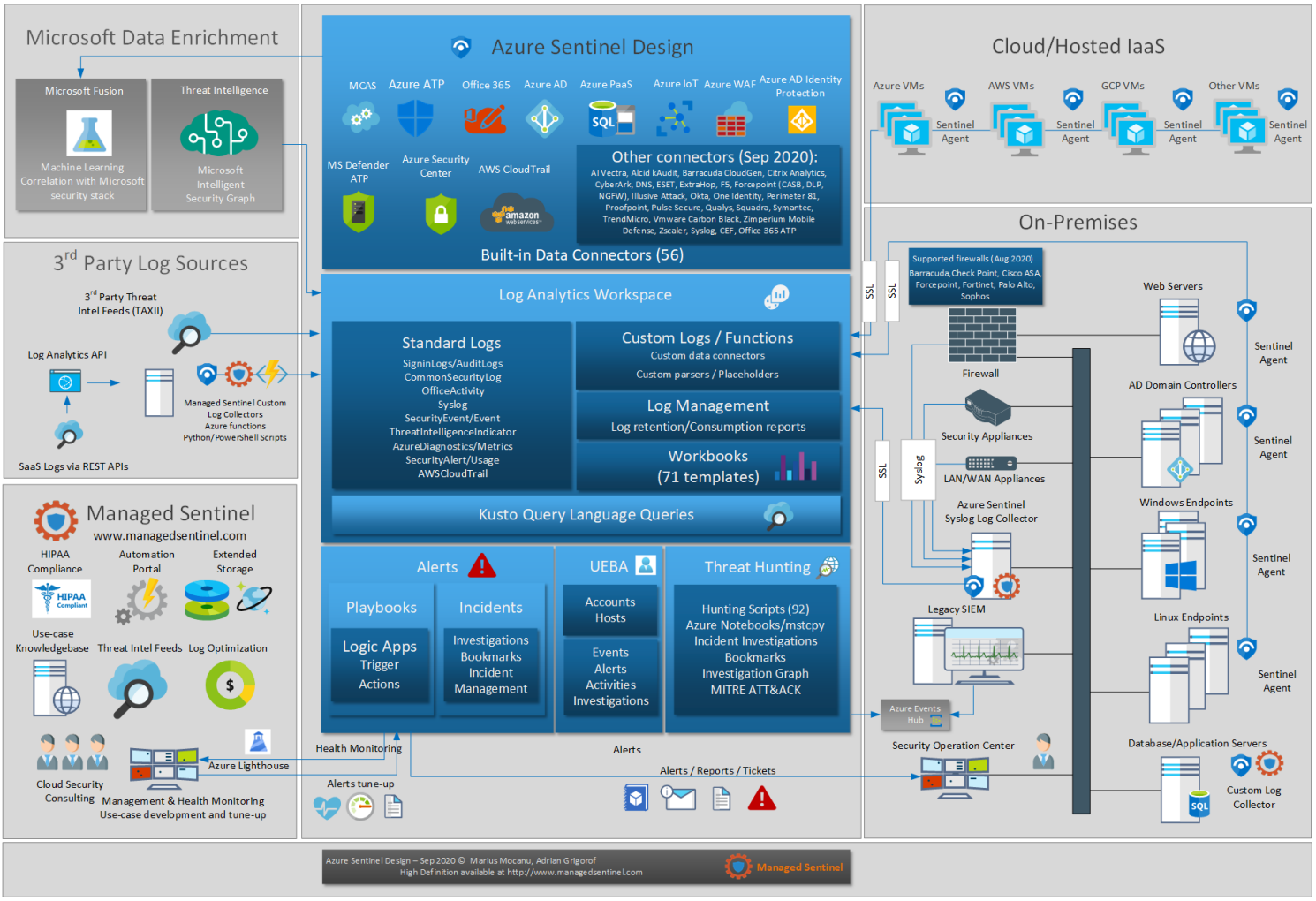
- Event log and query analytics
- Graph-powered machine learning
- Integration with Azure Advanced Threat Protection

Threat Hunting

For organizations that prefer to maintain a human layer to their threat hunting efforts, Microsoft Azure Sentinel gives security teams a set of intelligent search and query tools their analysts can use to unearth threats and catch other suspicious behavior that may have passed under the radar.

- Built-in queries to get threat hunters familiar with tables and query language
- Create your bookmarks to revisit suspicious findings
- Create threat hunting playbooks (SOPs) to document investigation steps
- Query storage data
- Access to community resources

https://www.managedsentinel.com/azure-sentinel-design/



Summary:

1. This is a cloud service that provides a solution for SIEM (Security Information and Event Management) and SOAR (Security Orchestration Automation Response)
2. This provides a solution that helps in the following
3. Collection of data – Here you can collect data across all users, devices, applications, and your infrastructure. The infrastructure could be located on-premises and on the cloud
4. It helps to detect undetected threats

5. It helps to hunt for suspicious activities at scale
6. It helps to respond to incident rapidly

Difference between Azure Security Center & Sentinel

https://techcommunity.microsoft.com/t5/itops-talk-blog/what-s-the-difference-between-azure-security-center-azure/ba-p/2155188

https://www.taliun.com/difference-between-microsoft-azure-security-center-and-azure-sentinel

Azure Security Center vs. Azure Sentinel

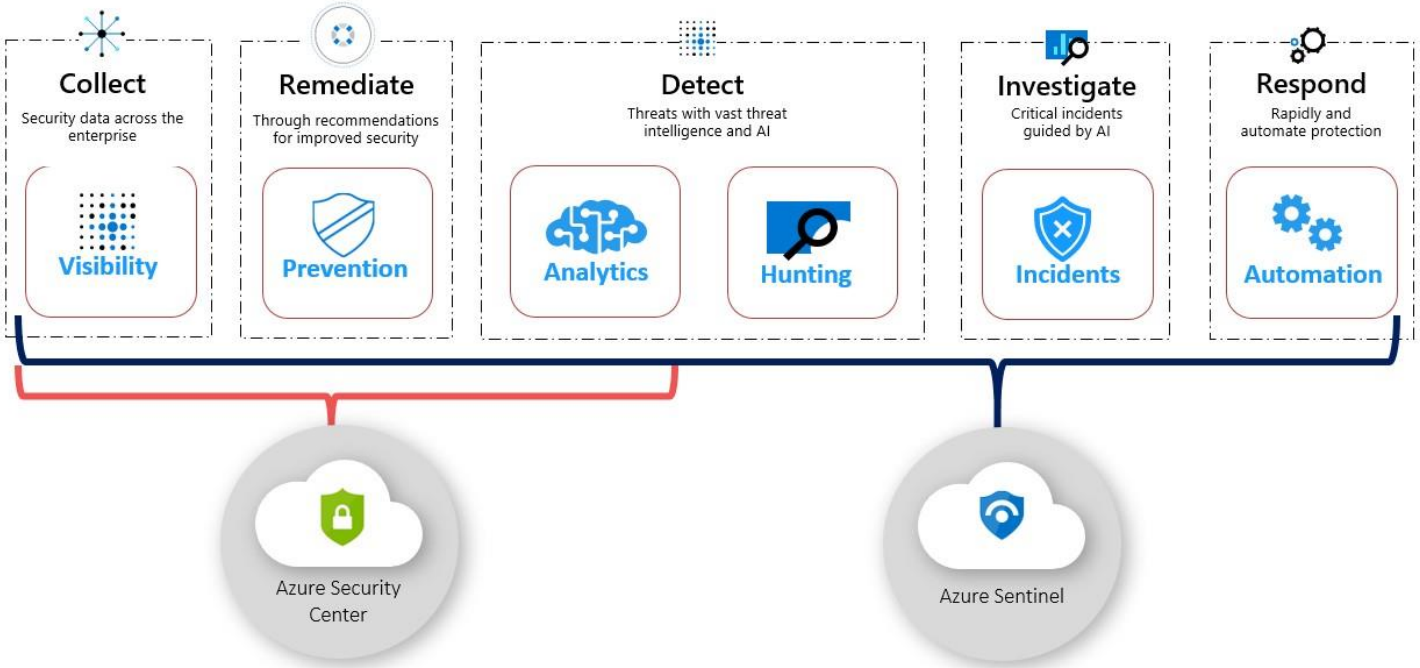
Azure Security Center is a security management framework offered by Microsoft to Azure clients. It helps the Azure infrastructure by giving visibility and authority over the security of Azure sources such as Virtual Machines, Cloud Services, Azure Virtual Networks, and Blob Storage.

Whereas, Azure Sentinel is a cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution provided by Microsoft to assist clients with a birds-eye view across a certain project.

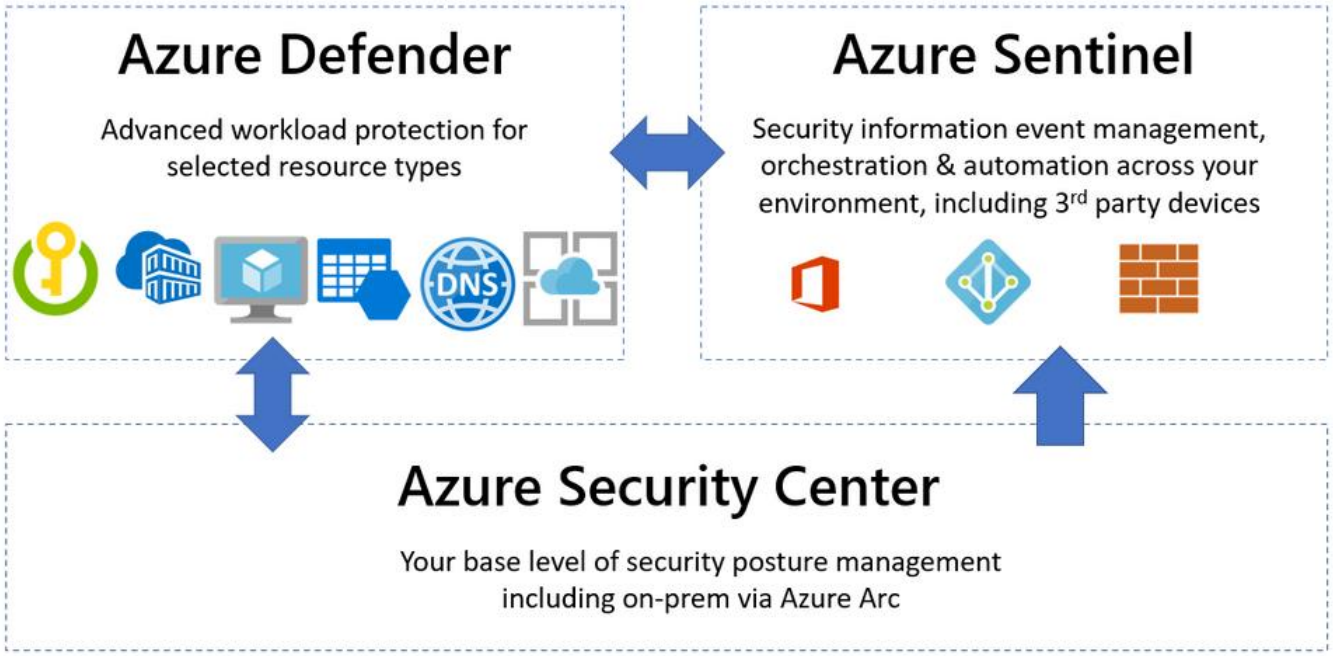
	Azure Security Center	Azure Sentinel
Description	Unified infrastructure security management system	Intelligent security analytics and threat intelligence service.
Category	Cloud Security Posture Management (CSPM) / Cloud Workload Protection Platform (CWPP)	Security Information Event Management (SIEM) / Security Orchestration Automated Response (SOAR)
Function	Provides security alerts, scores, vulnerability assessment, recommendations, and security posture management.	Provides alert detection, threat visibility, proactive hunting, and threat response.
Features	• Microsoft Defender ATP Integration • Network map • Virtual Machine Behavioral Analytics • Adaptive network hardening • Regulatory Compliance dashboard & reports • Missing OS patches assessment • Security misconfigurations assessment • Endpoint protection assessment • Disk encryption assessment • Third-party vulnerability assessment • Network security assessment	• Custom analytics rules • Multiple Workspace View • Azure Monitor Workbooks Integration • Security playbook • Investigation Graph • Hunting search and query tools
Provides Security Recommendation?	Yes	No
Threat Response Management	Manual	Automated
Integration	You may use the Azure Security Center to provide Azure Sentinel with more information to identify, investigate, and remediate threats.	

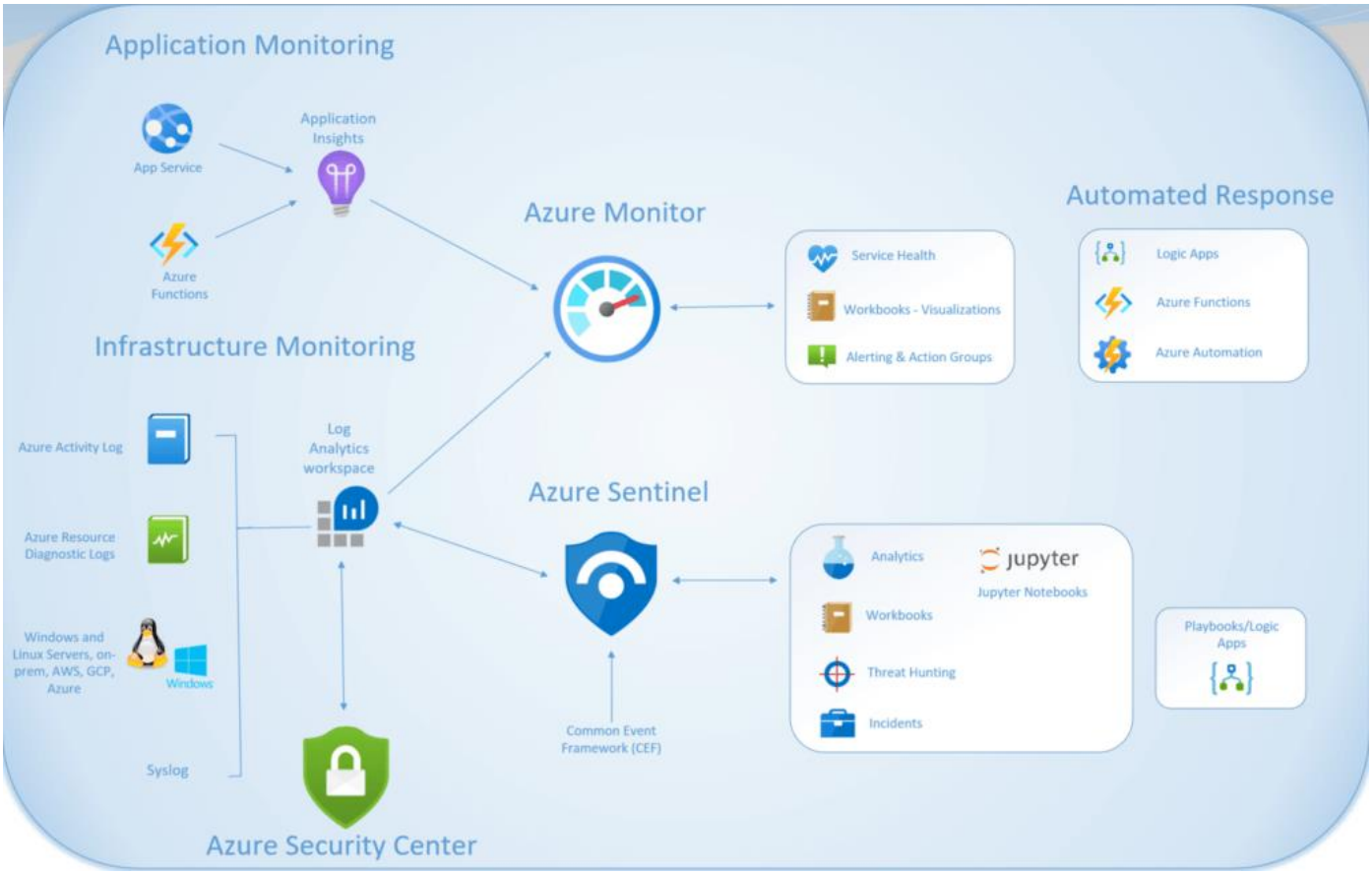
The **Azure Security Center** uses a built-in Azure Policy initiative in audit-only mode (the Azure Security Benchmark) as well as Azure Monitor logs and other Azure security solutions like Microsoft Cloud App Security.

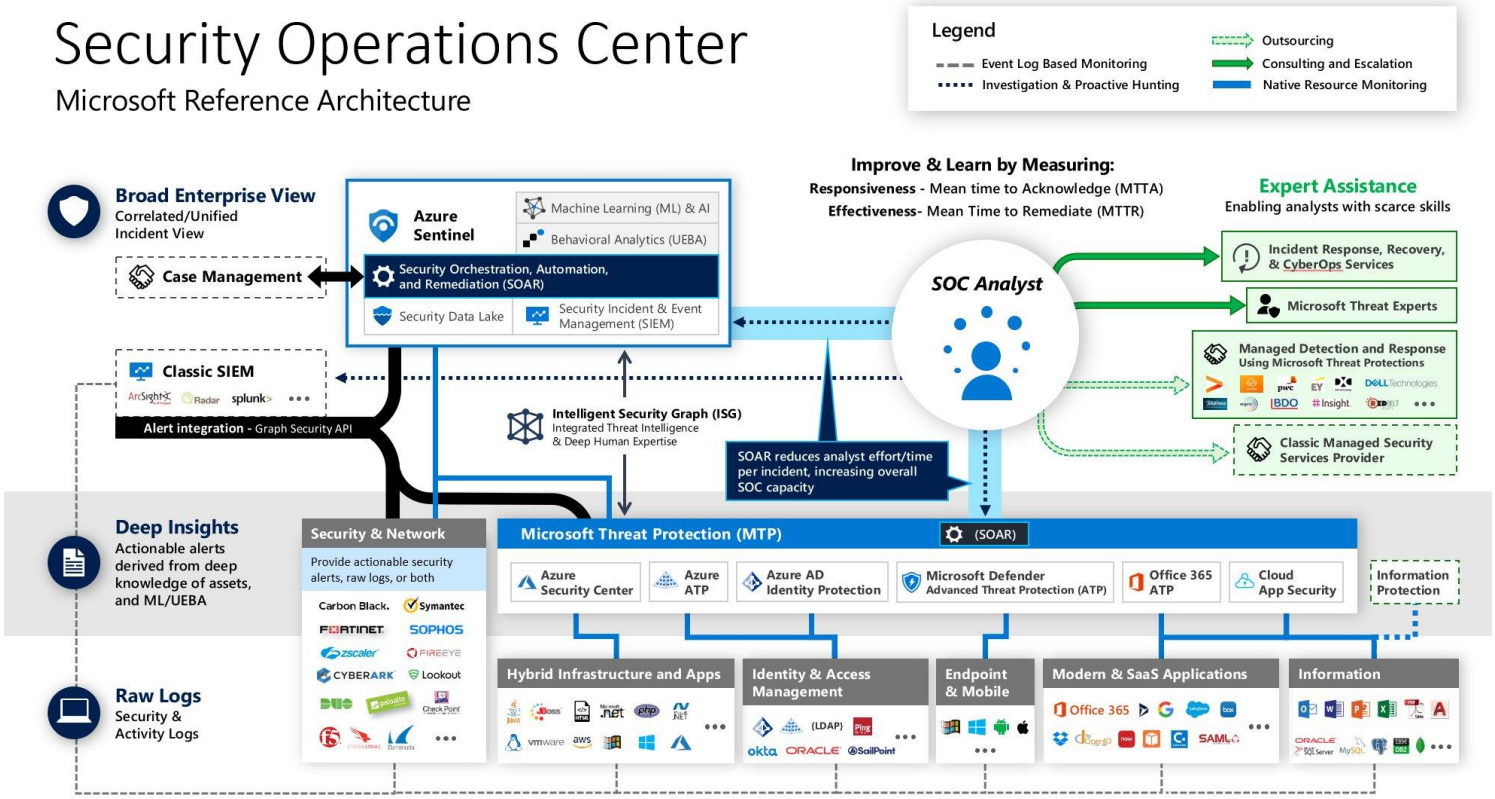
Azure Sentinel helps you to bring in the big picture of what's happening across your environment and connect the dots that might be related to the same security incident. While I've mentioned Azure and on-premises workloads so far, there's often more to your IT footprint than that - Microsoft 365, Azure Active Directory, Amazon Web Services - CloudTrail, Citrix Analytics, VMWare Carbon Black Cloud Endpoint, and third-party firewalls and proxies, just to name a few examples.



How Sentinel Works







Notes:

- If you're going in and only using as your security center that has its own logic and its workspace, you can't use the same workspace as your sentinel house.

- Well, and once you have gone ahead and enable, as your sentinel on a workspace, you can't move the workspace onto another resource group or onto another subscription.

Detection of Threats – Sentinel

1. Azure Sentinel can start detecting for threats once data is being collected
2. There are many in-built templates available to detect different types of threats from different sources
3. There are different rule types:
   - **Scheduled** – These are based on built-in queries that are written by Microsoft security experts
     Here you can change the query logic to suit your needs
   - **Fusion** – This uses advanced multistage attack detection techniques with the use of machine learning algorithms
     These rule types are not customizable

Azure – Key Vault Service

Azure Key Vault is a cloud service for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, certificates, or cryptographic keys. Key Vault service supports two types of containers: vaults and managed hardware security module (HSM) pools. Vaults support storing software and HSM-backed keys, secrets, and certificates.

You can securely store keys, passwords, certificates, and other secrets. Azure key vaults can be created and managed through the Azure portal.

Azure Key Vault Helps Solve Problem

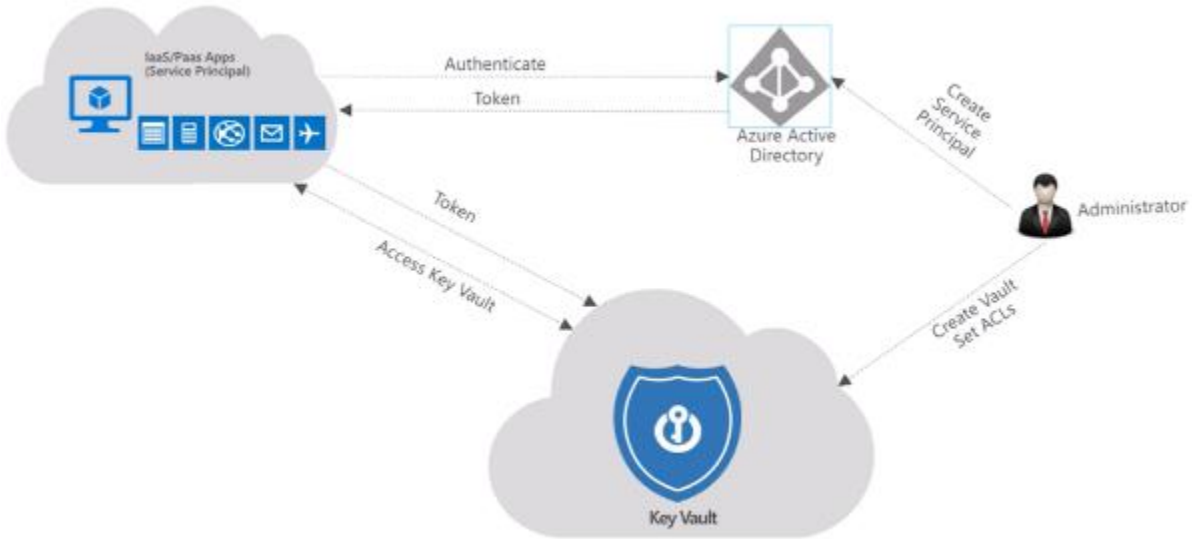
Azure Key Vault helps solve the following problems:

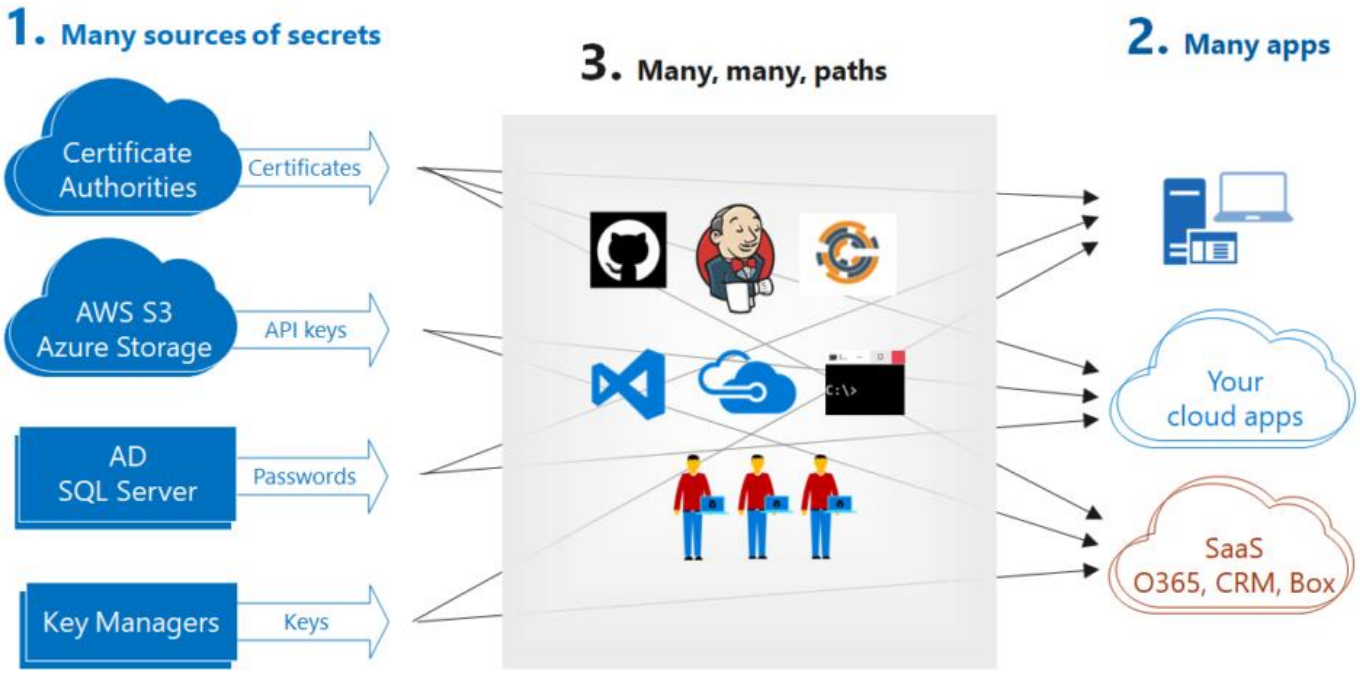
- **Secrets Management** – Azure Key Vault can be used to Securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets
- **Key Management** – Azure Key Vault can also be used as a Key Management solution. Azure Key Vault makes it easy to create and control the encryption keys used to encrypt your data
- **Certificate Management** – Azure Key Vault is also a service that lets you easily enroll, manage, and deploy public and private Transport Layer Security/Security Sockets Layer (TLS/SSL) certificates for use with Azure and internal connected resources

Azure Key Vault Service Tiers

Azure Key Vault has two service tiers:

- **Standard Tier** – which encrypts with a software key
- **Premium Tier** – which includes hardware security modules (HSM) protected keys





Here are other important terms:

- **Tenant** – A tenant is the organization that owns and manages a specific instance of Microsoft cloud services. It's most often used to refer to the set of Azure and Microsoft 365 services for an organization
- **Vault owner** – A vault owner can create a key vault and gain full access and control over it. The vault owner can also set up auditing to log who accesses secrets and keys. Administrators can control the key lifecycle. They can roll to a new version of the key, back it up, and do related tasks
- **Vault consumer** – A vault consumer can perform actions on the assets inside the key vault when the vault owner grants the consumer access. The available actions depend on the permissions granted
- **Managed HSM Administrators** – Users who are assigned the Administrator role have complete control over a Managed HSM pool. They can create more role assignments to delegate-controlled access to other users
- **Managed HSM Crypto Officer/User** – Built-in roles that are usually assigned to users or service principals that will perform cryptographic operations using keys in Managed HSM. Crypto User can create new keys, but cannot delete keys
- **Managed HSM Crypto Service Encryption User** – Built-in role that is usually assigned to a service accounts managed service identity (e.g., Storage account) for encryption of data at rest with customer managed key
- **Resource** – A resource is a manageable item that's available through Azure. Common examples are virtual machine, storage account, web app, database, and virtual network. There are many more
- **Resource group** – A resource group is a container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups, based on what makes the most sense for your organization
- **Security principal** – An Azure security principal is a security identity that user-created apps, services, and automation tools use to access specific Azure resources. Think of it as a "user identity" (username and password or certificate) with a specific role, and tightly controlled permissions. A security principal should only need to do specific things, unlike a general user identity. It improves security if you grant it only the minimum permission level that it needs to perform its management tasks. A security principal used with an application or service is specifically called a service principal
- **Azure Active Directory (Azure AD)** - Azure AD is the Active Directory service for a tenant. Each directory has one or more domains. A directory can have many subscriptions associated with it, but only one tenant
- **Azure tenant ID** – A tenant ID is a unique way to identify an Azure AD instance within an Azure subscription

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

Key Vault's Soft-Delete

Key Vault soft-delete feature allows recovery of the deleted vaults and deleted key objects (for e.g., keys, secrets, certificates), known as soft-delete.

When soft-delete is enabled, resources marked as deleted resources are retained for a specified period (90 days by default). The service further provides a mechanism for recovering the deleted object, essentially undoing the deletion.

When creating a new key vault, soft-delete is on by default. You can create a key vault without soft-delete through the Azure CLI or Azure PowerShell. Once soft-delete is enabled on a key vault it cannot be disabled

The default retention period is 90 days but, during key vault creation, it is possible to set the retention policy interval to a value from 7 to 90 days through the Azure portal. The purge protection retention policy uses the same interval. Once set, the retention policy interval cannot be changed.

Turn on soft-delete for an existing key vault

1. Sign in to the Azure portal
2. Search for your key vault
3. Select Properties under Settings
4. Under Soft-Delete, select the Enable recovery of this vault and its objects option
5. Set the retention period for soft-delete
6. Select Save

Purge Protection

Purge protection is an optional Key Vault behavior and is not enabled by default. Purge protection can only be enabled once soft-delete is enabled. It can be turned on via CLI or PowerShell.

When purge protection is on, a vault or an object in the deleted state cannot be purged until the retention period has passed. Soft-deleted vaults and objects can still be recovered, ensuring that the retention policy will be followed.

The default retention period is 90 days, but it is possible to set the retention policy interval to a value from 7 to 90 days through the Azure portal. Once the retention policy interval is set and saved it cannot be changed for that vault.

Vault Access Policy vs RBAC

The **vault access policy** model is an existing authorization system built in Key Vault to provide access to keys, secrets, and certificates. You can control access by assigning individual permissions to security principals (user, group, service principal, managed identity) at Kay Vault scope.

Azure Role-based Access Control (RBAC) is an authorization system built on Azure Resource Manager (ARM) that provides fine-grained access management of Azure resources. With Azure RBAC you can control access to resources by creating role assignments, which consist of three elements;

- A security principal
- A role definition
- A scope

The Azure RBAC model provides the ability to set permissions on different scope levels: management group, subscription, resource group, or individual resources. Azure RBAC for key vault also provides the ability to have separate permissions on individual keys, secrets, and certificates.

Azure Key Vault – Backup

A backup is intended to provide you with an offline copy of all your secrets in the unlikely event that you lose access to your key vault. Azure Key Vault automatically provides features to help you maintain availability and prevent data loss. Back up secrets only if you have a critical business justification. Backing up secrets in your key vault may introduce operational challenges such as maintaining multiple sets of logs, permissions, and backups when secrets expire or rotate.

Important Notes:

1. With an Azure Key Vault service, you can individually backup your secrets, keys, and certificates
2. You can create an offline copy of all of the secrets that you store in the key vault
3. If you want to protect against accidental or malicious deletion of secrets, then use the soft-delete and purge protection feature
4. You can't backup the entire key vault in one operation. You can only backup individual secrets at a time
5. When you download a backup of a secret, key, or a certificate, the downloaded blob will be an encrypted blob
6. To perform a restore, you can choose a key vault which is in the same Azure subscription and same Azure geography

Prerequisites

To back up a key vault object, you must have:

- Contributor-level or higher permissions on an Azure subscription.
- A primary key vault that contains the secrets you want to back up.
- A secondary key vault where secrets will be restored

Azure – Managed Service Identity

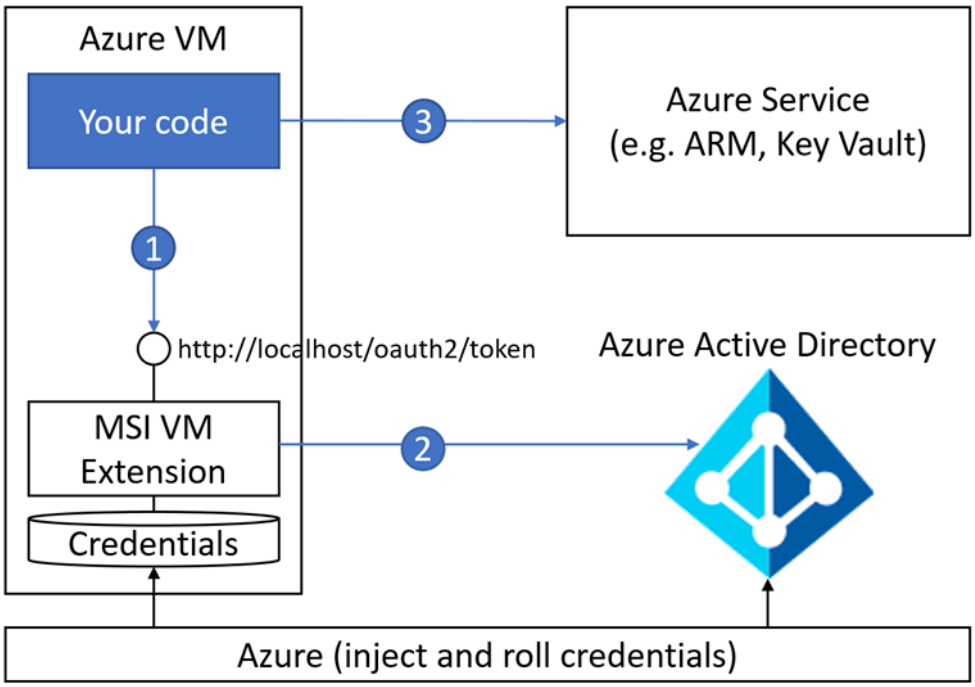
Your code needs credentials to authenticate to cloud services, but you want to limit the visibility of those credentials as much as possible. Ideally, they never appear on a developer's workstation or get checked-in to source control. Azure Key Vault can store credentials securely so they aren't in your code, but to retrieve them you need to authenticate to Azure Key Vault. To authenticate to Key Vault, you need a credential. Through the magic of Azure and Azure AD, MSI provides a "bootstrap identity" that makes it much simpler to get things started.

When you enable MSI for an Azure service such as Virtual Machines, App Service, or Functions, Azure creates a Service Principal for the instance of the service in Azure AD, and injects the credentials (client ID and certificate) for the Service Principal into the instance of the service. Next,

1. Your code calls a local MSI endpoint to get an access token
2. MSI uses the locally injected credentials to get an access token from Azure AD
3. Your code uses this access token to authenticate to an Azure service

And that's it! The access token can be used directly with a service that supports Azure AD authentication, such as Azure Resource Manager. If you need to authenticate to a service that doesn't natively support Azure AD, you can use the token to authenticate to Key Vault and retrieve credentials from there. Azure and Azure AD take care of rolling the Service Principal's credentials. Your code and your developers will never see or manage them.

Managed Service Identity is a feature of Azure AD Free, which comes with every Azure subscription. There is no additional charge for using Managed Service Identity.



Types of Managed Identity

There are two types of managed identities:

1. A system-assigned managed identity is enabled directly on an Azure service instance. When the identity is enabled, Azure creates an identity for the instance in the Azure AD tenant that's trusted by the subscription of the instance. After the identity is created, the credentials are provisioned onto the instance. The lifecycle of a system-assigned identity is directly tied to the Azure service instance that it's enabled on. If the instance is deleted, Azure automatically cleans up the credentials and the identity in Azure AD.
2. A user-assigned managed identity is created as a standalone Azure resource. Through a create process, Azure creates an identity in the Azure AD tenant that's trusted by the subscription in use. After the identity is created, the identity can be assigned to one or more Azure service instances. The lifecycle of a user-assigned identity is managed separately from the lifecycle of the Azure service instances to which it's assigned.

Internally, managed identities are service principals of a special type, which are locked to only be used with Azure resources. When the managed identity is deleted, the corresponding service principal is automatically removed.

Your code can use a managed identity to request access tokens for services that support Azure AD authentication. Azure takes care of rolling the credentials that are used by the service instance.

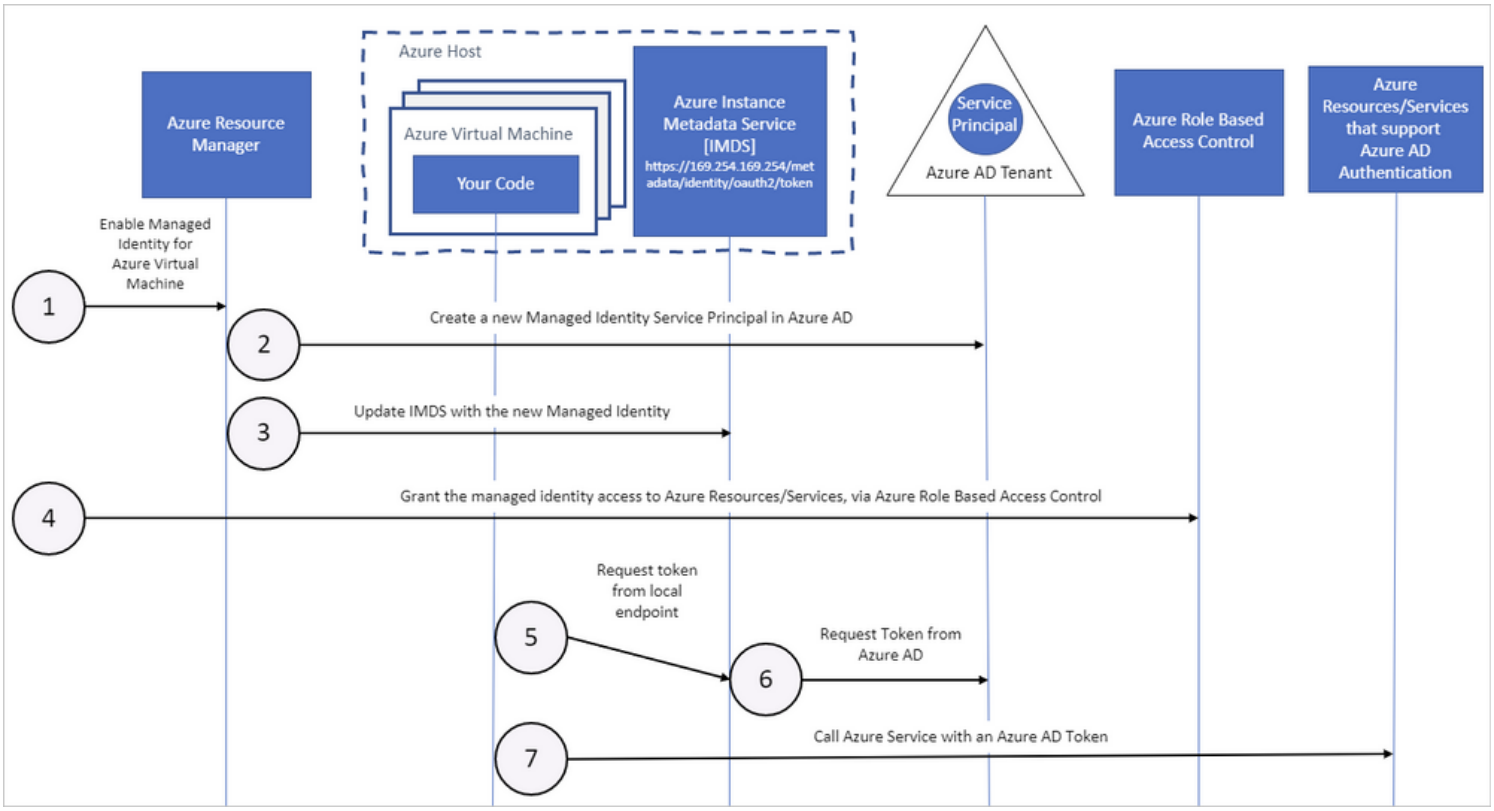
The following diagram shows how managed service identities work with Azure virtual machines (VMs):

How a system-assigned managed identity works with an Azure VM

1. Azure Resource Manager receives a request to enable the system-assigned managed identity on a VM
2. Azure Resource Manager creates a service principal in Azure AD for the identity of the VM. The service principal is created in the Azure AD tenant that's trusted by the subscription
3. Azure Resource Manager configures the identity on the VM by updating the Azure Instance Metadata Service identity endpoint with the service principal client ID and certificate
4. After the VM has an identity, use the service principal information to grant the VM access to Azure resources. To call Azure Resource Manager, use role-based access control (RBAC) in Azure AD to assign the appropriate role to the VM service principal. To call Key Vault, grant your code access to the specific secret or key in Key Vault
5. Your code that's running on the VM can request a token from the Azure Instance Metadata service endpoint, accessible only from within the VM: http://169.254.169.254/metadata/identity/oauth2/token

- The resource parameter specifies the service to which the token is sent. To authenticate to Azure Resource Manager, use resource=https://management.azure.com/
- API version parameter specifies the IMDS version, use api-version=2018-02-01 or greater

6. A call is made to Azure AD to request an access token (as specified in step 5) by using the client ID and certificate configured in step 3. Azure AD returns a JSON Web Token (JWT) access token
7. Your code sends the access token on a call to a service that supports Azure AD authentication.



There are three ways you can use the managed identity:

1. To call the Azure resource manager, use role-based access control (RBAC) in Azure AD to assign the appropriate role to the service principal
2. To call the Key Vault, grant your code access to the specific secret or key in Key Vault
3. Use the IMDS service to request an access token, The request is made to http://169.254.169.254/metadata/identity/oauth2/token. This request is made using the client ID and certificate of the service principal, and you get your usual JWT token that you can use to do your usual Azure AD authentication

As you can see, managed identities can be used to work with nearly every conceivable scenario. There's lots of flexibility. Not to mention that more and more Azure services are adding support for managed identities. One of my favorites is Azure functions v2 runtime that now supports managed identity.

Azure – Encryption for Managed Disks

There are three types of encryptions available for your managed disks:

1. Azure Disk Encryption
2. Server-Side Encryption
3. Encryption at host

https://terenceluk.blogspot.com/2021/05/azure-server-side-encryption-sse-and.html

Summary of all the Three Data Encryptions

1. **Azure Disk Encryption**

It helps protect and safeguard your data to meet your organizational security and compliance commitments. ADE provides volume encryption for the OS and data disks of Azure virtual machines (VM) through the use of feature DM-Crypt of Linux or the BitLocker feature of Windows. ADE is integrated with Azure Key Vault to help you control and manage the disk encryption keys and secrets.

2. **Server-Side Encryption**

It's also referred to as encryption at rest or Azure Storage Encryption, which automatically encrypts data stored on Azure managed disks (OS and data disks) which persisting it to the cloud.

3. **Encryption at host**

It ensures that data stored on the VM host is encrypted at rest and flows encrypted to the Storage service. Disks with encryption at host enabled data flows into Azure storage.

Detailed Explanation about all three Disk Encryptions

Azure Disk Encryption (ADE)

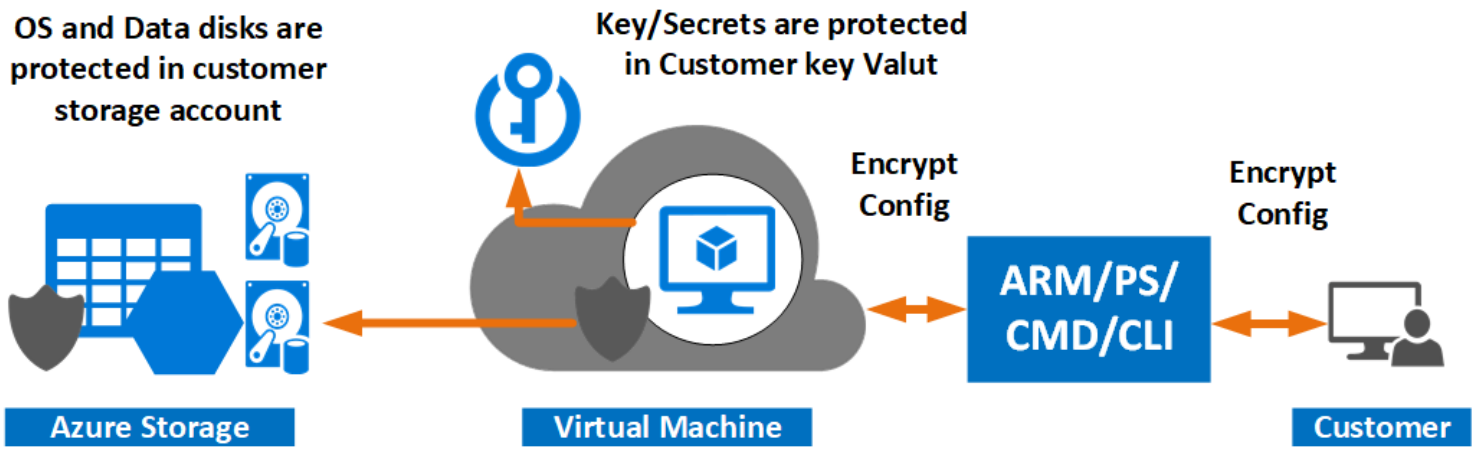
Azure Disk Encryption (ADE) is a capability that helps you encrypt your Windows and Linux IaaS virtual machine disks. Azure Disk Encryption leverages the industry standard BitLocker feature of Windows and the DM-Crypt feature of Linux to provide volume encryption for the OS and the data disks. The solution is integrated with Azure Key Vault to help you control and manage the disk-encryption keys and secrets in your key vault subscription. The solution also ensures that all data on the virtual machine disks are encrypted at rest in your Azure storage.

- Azure disk encryption for Windows and Linux IaaS VMs is now in General Availability in all Azure public regions and AzureGov regions for Standard VMs and VMs with premium storage.
- There is no charge for encrypting VM disks with Azure Disk Encryption, but there are charges associated with the use of Azure Key Vault
- Azure Disk Encryption GA supports Azure Resource Manager (ARM) templates, Azure PowerShell, and Azure CLI. The different user experiences give you flexibility. You have three different options for enabling disk encryption for your VM's
- You can encrypt both boot and data volumes, but you can't encrypt the data without first encrypting the OS volume
- Azure Disk Encryption (ADE) provides end-to-end encryption for the OS disk, data disks, and the temporary disk with a customer-managed key
- If your requirements include encrypting all of the above and end-to-end encryption, use Azure Disk Encryption (AED)
- If your requirements include encrypting only data at rest with customer-managed key, then use Server-side encryption with customer-managed keys. You cannot encrypt a disk with both Azure Disk Encryption and Storage server-side encryption with customer managed keys
- If you are using a scenario called out in unsupported scenarios for Windows, consider Server-side encryption with customer-managed keys
- If your organization's policy allows you to encrypt content at rest with an Azure-managed key, then no action is needed - the content is encrypted by default. For managed disks, the content inside storage is encrypted by default with Server-side encryption with platform-managed key. The key is managed by the Azure Storage service
- Azure Backup provides a mechanism to backup and restore encrypted VM's within the same subscription and region. For instructions, please see backup and restore encrypted virtual machines with Azure Backup. Restoring an encrypted VM to a different region is not currently supported
- Azure Disk Encryption is also available for VMs with premium storage. Azure Disk Encryption is not available on Generation 2 VMs. For more exceptions, see Azure Disk Encryption: Unsupported scenarios. Azure Disk Encryption is not available on VM images without temp disks (Dv4, Dsv4, Ev4, and Esv4)

Azure Disk Encryption in Running Virtual Machines

We can have encrypted enhanced virtual machine (VM) security and compliance, virtual disks in Azure. Disks are encrypted using cryptographic keys that are secured in an Azure Key Vault. Cryptographic keys are stored in Azure key vault using

software protection, or you can import or generate your keys in Hardware Security Modules (HSMs) certified to FIPS 140-2 level 2 standards. Cryptographic keys are used to encrypt and decrypt virtual disks attached to your VM. An Azure Active Directory service principle provides a secure mechanism for issuing these cryptographic keys as VMs are powered on or off.



Server-Side Encryption

Most Azure managed disks are encrypted with Azure Storage encryption, which uses server-side encryption (SSE) to protect your data and to help you meet your organizational security and compliance commitments. Azure Storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud. Disks with encryption at host enabled, however, are not encrypted through Azure Storage. For disks with encryption at host enabled, the server hosting your VM provides the encryption for your data, and that encrypted data flows into Azure Storage.

Data in Azure managed disks is encrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant. For more information about the cryptographic modules underlying Azure managed disks, see Cryptography API: Next Generation.

Azure Storage encryption does not impact the performance of managed disks and there is no additional cost.

Encryption at Host

When you enable encryption at host, data stored on the VM host is encrypted at rest and flows encrypted to the Storage service. For conceptual information on encryption at host, and other managed disk encryption types, see: Encryption at host - End-to-end encryption for your VM data.

Temporary disks and ephemeral OS disks are encrypted at rest with platform-managed keys when you enable end-to-end encryption. The OS and data disk caches are encrypted at rest with either customer-managed or platform-managed keys, depending on what you select as the disk encryption type. For example, if a disk is encrypted with customer-managed keys, then the cache for the disk is encrypted with customer-managed keys, and if a disk is encrypted with platform-managed keys then the cache for the disk is encrypted with platform-managed keys.

Restrictions

- Doesn't support ultra-disks
- Cannot be enabled if Azure Disk Encryption (guest-VM encryption using bitlocker/DM-Crypt) is enabled on your VMs/virtual machine scale sets
- Azure Disk Encryption cannot be enabled on disks that have encryption at host enabled
- The encryption can be enabled on existing virtual machine scale set. However, only new VMs created after enabling the encryption are automatically encrypted
- Existing VMs must be deallocated and reallocated in order to be encrypted
- Supports ephemeral OS disks but only with platform-managed keys

Azure – SQL Database

Azure SQL Database is a fully managed platform as a service (PaaS) database engine that handles most of the database management functions such as upgrading, patching, backups, and monitoring without user involvement. Azure SQL Database is always running on the latest stable version of the SQL Server database engine and patched OS with 99.99% availability. PaaS capabilities that are built into Azure SQL Database enable you to focus on the domain-specific database administration and optimization activities that are critical for your business.

With Azure SQL Database, you can create a highly available and high-performance data storage layer for the applications and solutions in Azure. SQL Database can be the right choice for a variety of modern cloud applications because it enables you to process both relational data and non-relational structures, such as graphs, JSON, spatial, and XML.

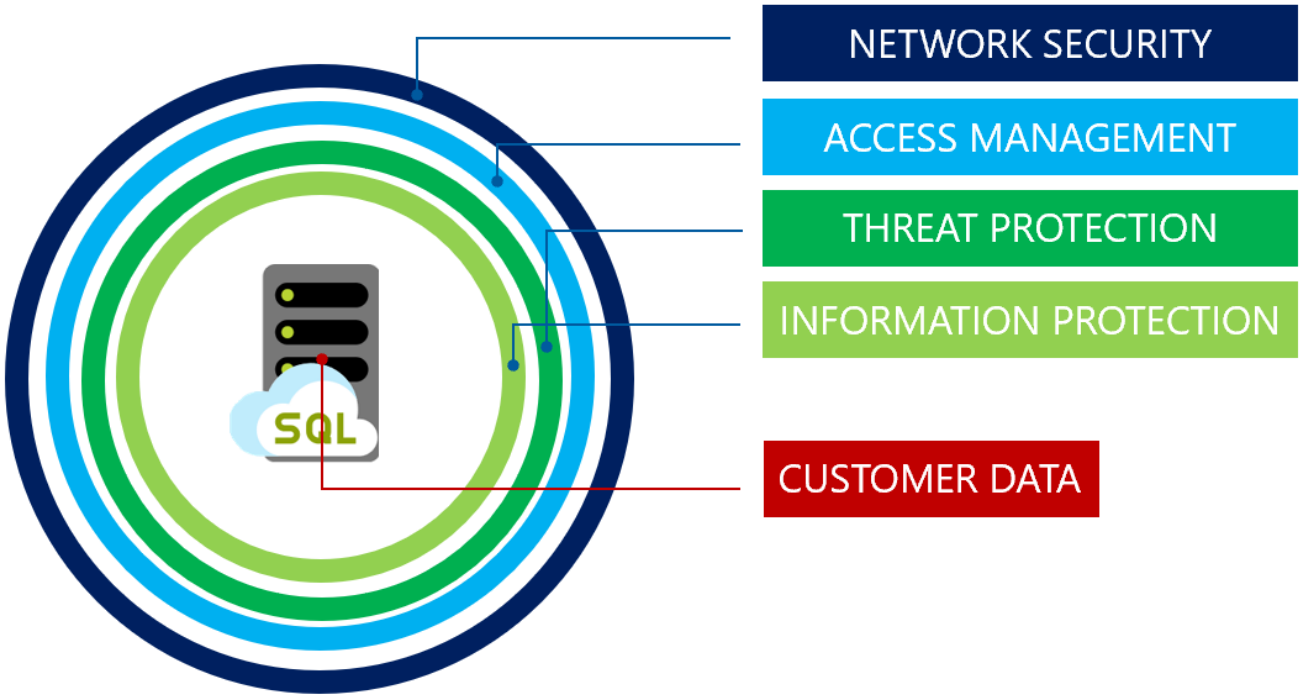
Azure SQL Database is based on the latest stable version of the Microsoft SQL Server database engine. You can use advanced query processing features, such as high-performance in-memory technologies and intelligent query processing. In fact, the newest capabilities of SQL Server are released first to SQL Database, and then to SQL Server itself. You get the newest SQL Server capabilities with no overhead for patching or upgrading, tested across millions of databases.

SQL Database enables you to easily define and scale performance within two different purchasing models: a vCore-based purchasing model and a DTU-based purchasing model. SQL Database is a fully managed service that has built-in high availability, backups, and other common maintenance operations. Microsoft handles all patching and updating of the SQL and operating system code. You don't have to manage the underlying infrastructure.

Azure SQL Database Server – Security Practices

When using Azure SQL Database, there are several areas in which you should focus your security efforts:

- Ensure you meet data privacy standards and regulatory compliance requirements
- Restrict access to your databases and harden security permissions
- Monitor changes across your database to ensure data integrity and privacy
- Detect and respond to potential threats



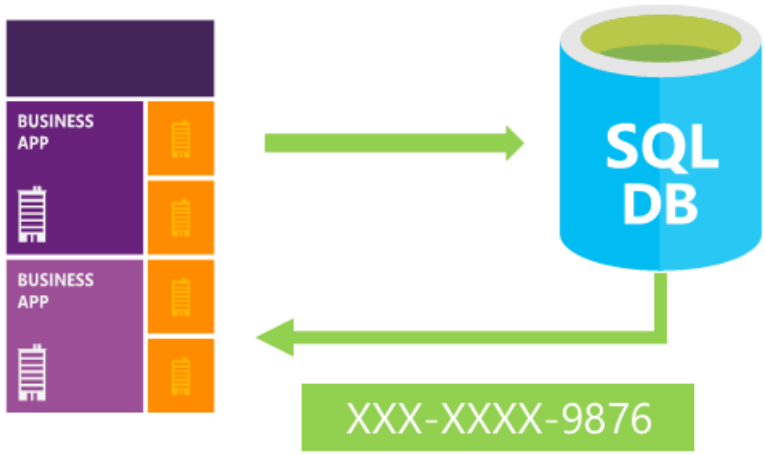
https://ballardchalmers.com/2020/03/09/azure-sql-database-security-features/

Encryption Features

1. You can encrypt multiple columns located in different tables
2. You can encrypt multiple columns located in the same table
3. You can just encrypt one specific column
4. There are two types of encryptions
   Deterministic Encryption – Here the same encrypted value is generated for any given plain text value. This is less secure. But it allows for point lookups, equality joins, grouping and indexing on encrypted columns
   Randomized Encryption – This is the most secure encryption method. But it prevents the searching, grouping, indexing and joining on encrypted columns.
5. We can enable the Always Encrypted feature using SQL Server Management Studio
6. There are 2 keys that get created when the Always Encrypted feature is enable for a database
   Column Master Key – This is an encryption key that needs to be stored in an external data store. Here you can store the key in a Windows certificate store or in the Azure Key Vault service
   Column Encryption Key – This is generated from the column master key and is used to encrypt the actual column
7. The user who is implementing the Always Encrypted feature needs to have the following permissions for keys – create, get, list, sign, verify, wrapKey, unwrapKey

Dynamic Data Masking

Dynamic data masking limits sensitive data exposure by masking it to non-privileged users. Dynamic data masking automatically discovers potentially sensitive data in Azure SQL Database and SQL Managed Instance and provides actionable recommendations to mask these fields, with minimal impact to the application layer. It works by obfuscating the sensitive data in the result set of a query over designated database fields, while the data in the database is not changed.



Auditing

1. You can enable auditing for an Azure SQL database and also for Azure Synapse Analytics
2. This feature can be used to track database events and write them to an audit log
3. The logs can be stored in an Azure Storage account, Log Analytics workspace or the Azure Event Hubs
4. This helps in regulatory compliance. It helps to gain insights on any anomalies when it comes to database activities
5. Auditing can be enabled at the database or server level
6. If it is applied at the server level, then it will be applied to all of the database that reside on the server

Data Discovery and Classification

Data discovery and classification provides basic capabilities built into Azure SQL Database and SQL Managed Instance for discovering, classifying and labelling the sensitive data in your databases. Discovery and classifying your utmost sensitive data can play a pivotal role in your organizational Information Protection stature. It can serve as infrastructure for:

- Various security scenarios, such as monitoring (auditing) and alerting on anomalous access to sensitive data

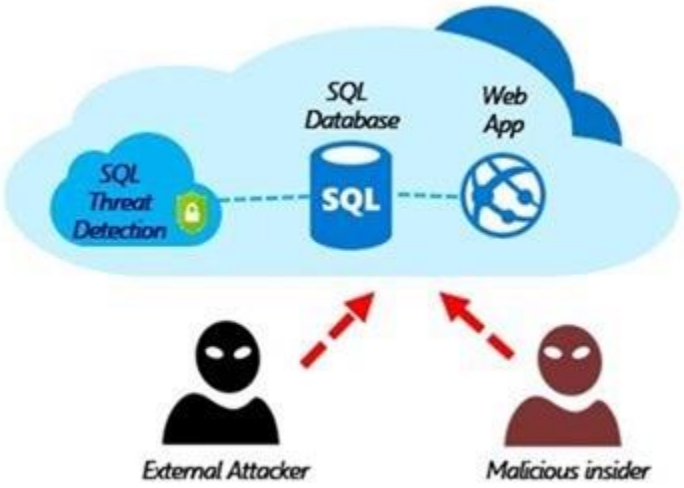
- Controlling access to, and hardening the security of, databases containing highly sensitive data
- Helping meet data privacy standards and regulatory compliance requirements

Vulnerability Assessment

Vulnerability assessment is an easy to configure service that can discover, track, and help remediate potential database vulnerabilities with the goal to proactively improve overall database security. Vulnerability assessment (VA) is part of the Azure Defender for SQL offering, which is a unified package for advanced SQL security capabilities. Vulnerability assessment can be accessed and managed via the central Azure Defender for SQL portal.

Advanced Threat Protection

Advanced Threat Protection is analyzing your logs to detect unusual behavior and potentially harmful attempts to access or exploit databases. Alerts are created for suspicious activities such as SQL injection, potential data infiltration, and brute force attacks or for anomalies in access patterns to catch privilege escalations and breached credentials use. Alerts are viewed from the Azure Security Center, where the details of the suspicious activities are provided and recommendations for further investigation given along with actions to mitigate the threat. Advanced Threat Protection can be enabled per server for an additional fee.



Azure – Storage Account

The Azure Storage platform is Microsoft's cloud storage solution for modern data storage scenarios. Core storage services offer a massively scalable object store for data objects, disk storage for Azure virtual machines (VM's). a file systems service for the cloud, a messaging store for reliable messaging, and a NoSQL store. The services are:

- **Durable and highly available** – Redundancy ensures that your data is safe in the event of transient hardware failures. You can also opt to replicate data across datacenters or geographical regions for additional protection from local catastrophe or natural disaster. Data replicated in this way remains highly available in the event of an unexpected outage
- **Secure** – All data written to an Azure storage account is encrypted by the service. Azure Storage provides you with fine-grained control over who has access to your data
- **Scalable** – Azure Storage is designed to be massively scalable to meet the data storage and performance needs of today's applications
- **Managed** – Azure handles hardware maintenance, updates, and critical issues for you
- **Accessible** – Data in Azure Storage is accessible from anywhere in the world over HTTP or HTTPS. Microsoft provides client libraries for Azure Storage in a variety of languages, including .NET, Java, Node.js, Python, PHP, Ruby, Go, and others, as well as a mature REST API. Azure Storage supports scripting in Azure PowerShell or Azure CLI. And the Azure portal and Azure Storage Explorer offer easy visual solutions for working with your data

Core Storage Services

The Azure Storage platform includes the following data services:

- Azure Blobs – A massively scalable object store for text and binary data. Also includes support for big data analytics through Data Lake Storage Gen2
- Azure Files – Managed file shares for cloud or on-premises deployments
- Azure Queues – A messaging store for reliable messaging between application components
- Azure Tables – A NoSQL store for schemaless storage of structured data
- Azure Disks – Block-level storage volumes for Azure VMs

Blob storage

Azure Blob storage is Microsoft's object storage solution for the cloud. Blob storage is optimized for storing massive amounts of unstructured data, such as text or binary data

Blob storage is ideal for:

Serving images or documents directly to a browser

- Storing files for distributed access
- Streaming video and audio
- Storing data for backup and restore, disaster recovery, and archiving
- Storing data for analysis by an on-premises or Azure-hosted service

Objects in Blob storage can be accessed from anywhere in the world via HTTP or HTTPS. Users or client applications can access blobs via URLs, the Azure Storage REST API, Azure PowerShell, Azure CLI, or an Azure Storage client library. The storage client libraries are available for multiple languages, including .NET, Java, Node.js, Python, PHP, and Ruby.

Azure Files

Azure Files enables you to set up highly available network file shares that can be accessed by using the standard Server Message Block (SMB) protocol. That means that multiple VMs can share the same files with both read and write access. You can also read the files using the REST interface or the storage client libraries.

One thing that distinguishes Azure Files from files on a corporate file share is that you can access the files from anywhere in the world using a URL that points to the file and includes a shared access signature (SAS) token. You can generate SAS tokens; they allow specific access to a private asset for a specific amount of time.

File shares can be used for many common scenarios:

- Many on-premises applications use file shares. This feature makes it easier to migrate those applications that share data to Azure. If you mount the file share to the same drive letter that the on-premises application uses, the part of your application that accesses the file share should work with minimal, if any, changes
- Configuration files can be stored on a file share and accessed from multiple VMs. Tools and utilities used by multiple developers in a group can be stored on a file share, ensuring that everybody can find them, and that they use the same version
- Resource logs, metrics, and crash dumps are just three examples of data that can be written to a file share and processed or analyzed later

Queue Storage

The Azure Queue service is used to store and retrieve messages. Queue messages can be up to 64 KB in size, and a queue can contain millions of messages. Queues are generally used to store lists of messages to be processed asynchronously.

For example, say you want your customers to be able to upload pictures, and you want to create thumbnails for each picture. You could have your customer wait for you to create the thumbnails while uploading the pictures. An alternative would be to use a queue. When the customer finishes their upload, write a message to the queue. Then have an Azure Function retrieve

the message from the queue and create the thumbnails. Each of the parts of this processing can be scaled separately, giving you more control when tuning it for your usage.

Table Storage

Azure Table storage is now part of Azure Cosmos DB. To see Azure Table storage documentation, see the Azure Table Storage Overview. In addition to the existing Azure Table storage service, there is a new Azure Cosmos DB Table API offering that provides throughput-optimized tables, global distribution, and automatic secondary indexes. To learn more and try out the new premium experience, see Azure Cosmos DB Table API.

Disk Storage

An Azure managed disk is a virtual hard disk (VHD). You can think of it like a physical disk in an on-premises server but, virtualized. Azure-managed disks are stored as page blobs, which are a random IO storage object in Azure. We call a managed disk 'managed' because it is an abstraction over page blobs, blob containers, and Azure storage accounts. With managed disks, all you have to do is provision the disk, and Azure takes care of the rest.

An Azure storage account contains all of your Azure Storage data objects: blobs, file shares, queues, tables, and disks. The storage account provides a unique namespace for your Azure Storage data that's accessible from anywhere in the world over HTTP or HTTPS. Data in your storage account is durable and highly available, secure, and massively scalable.

Storage Data Objects:

- Blobs
- File shares
- Queues
- Tables
- Disks

Azure Storage Explorer

Microsoft Azure Storage Explorer is a standalone app that makes it easy to work with Azure Storage data on Windows, macOS, and Linux. It is a useful GUI tool for inspecting and altering the data in your Windows Azure Storage projects including the logs of your cloud-hosted applications.

All 3 types of cloud storage can be viewed and edited: blobs, queues, and tables.

Access Storage Account Access

There are three ways you give access onto storage account, below are those:

- Access Keys
- Shared Access Signatures
- Azure Active Directory (User defined roles by RBAC)

Storage Account access keys – gives you full authorization over all of the services that are part of your storage account

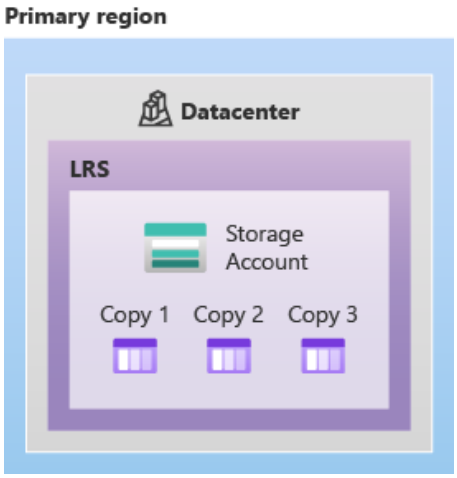
Azure Storage Redundancy / Replication

Azure Storage always stores multiple copies of your data so that it is protected from planned and unplanned events, including transient hardware failures, network or power outages, and massive natural disasters. Redundancy ensures that your storage account meets its availability and durability targets even in the face of failures.

1. **Locally redundant storage (LRS)**

It copies your data synchronously three times within a single physical location in the primary region. LRS is the least expensive replication option but is not recommended for applications requiring high availability or durability.

Note: In LRS case, the data is getting stored on 3 different storage devices within the same data center, so your data remains in the same data center, and do not gets shared into any other zones or geo location.



2. **Zone-redundant storage (ZRS)**

It copies your data synchronously across three Azure availability zones in the primary region. For applications requiring high availability, Microsoft recommends using ZRS in the primary region, and also replicating to a secondary region.

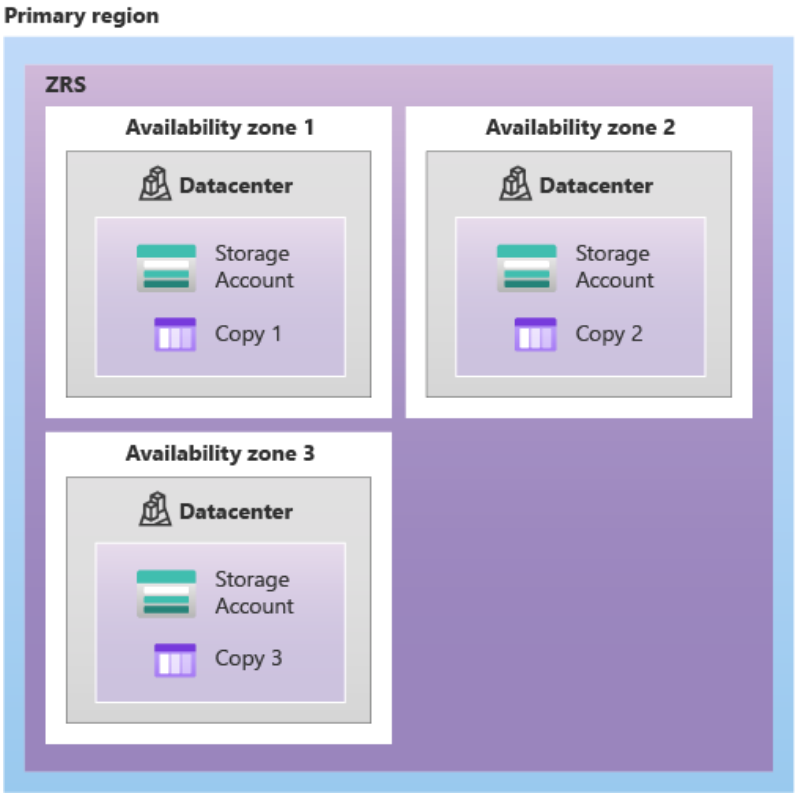
Zone Redundant Storage (ZRS) helps you to protect against data center level failure.

Notes:

In one geo location, there are 3 three availability zones.

Each availability zone is a separate physical location with independent power, cooling, and networking. And each zone is a collection of multiple data centers

In this case the file or data will be copied in another data center in another availability zone, to avoid data center failures



3. **Geo-redundant storage (GRS)**

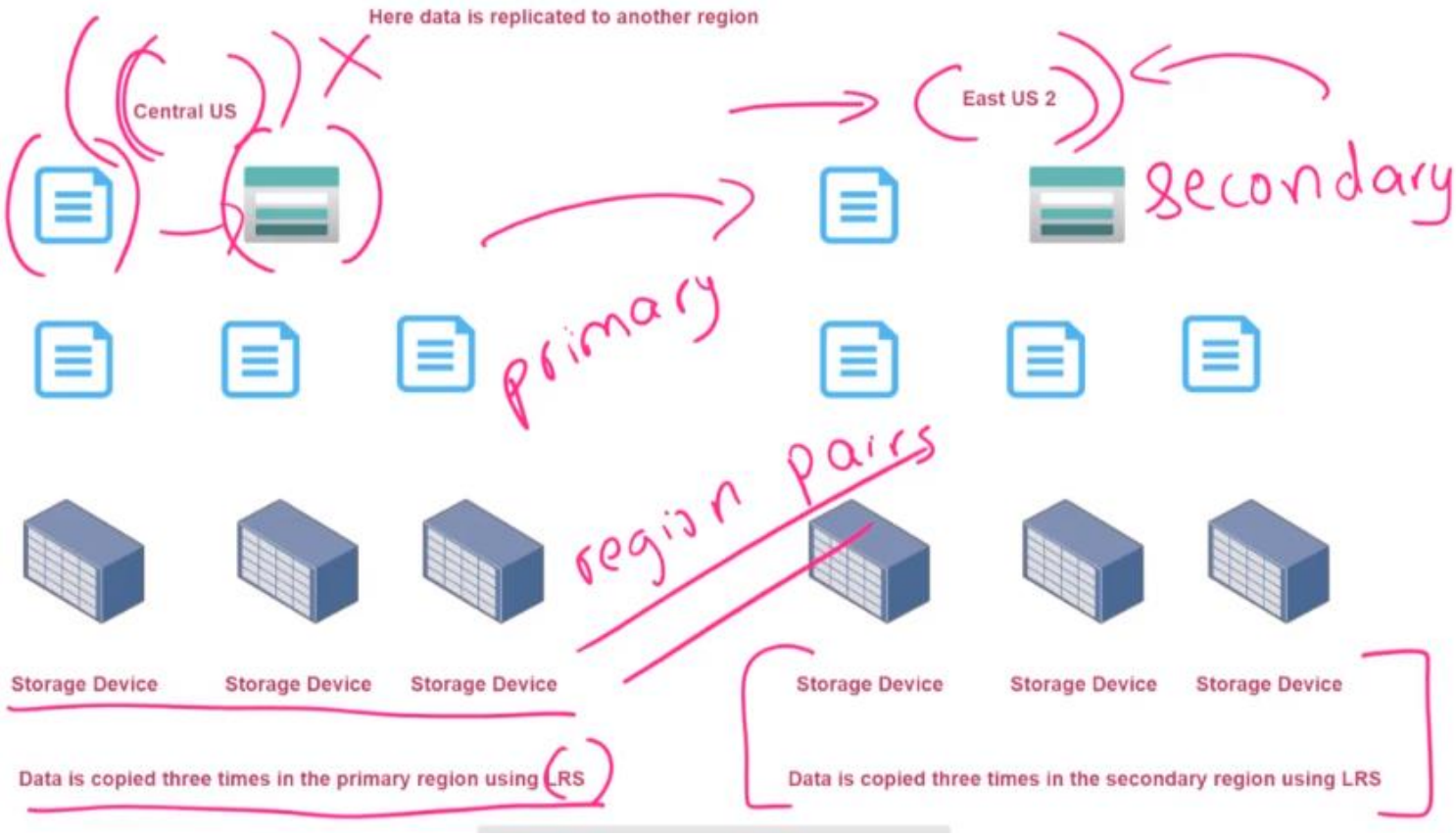
Geo-redundant storage (GRS) copies your data synchronously three times within a single physical location in the primary region using LRS. It then copies your data asynchronously to a single physical location in a secondary region that is hundreds of miles away from the primary region. GRS offers durability for Azure Storage data objects of at least 99.99999999999999% (16 9's) over a given year.

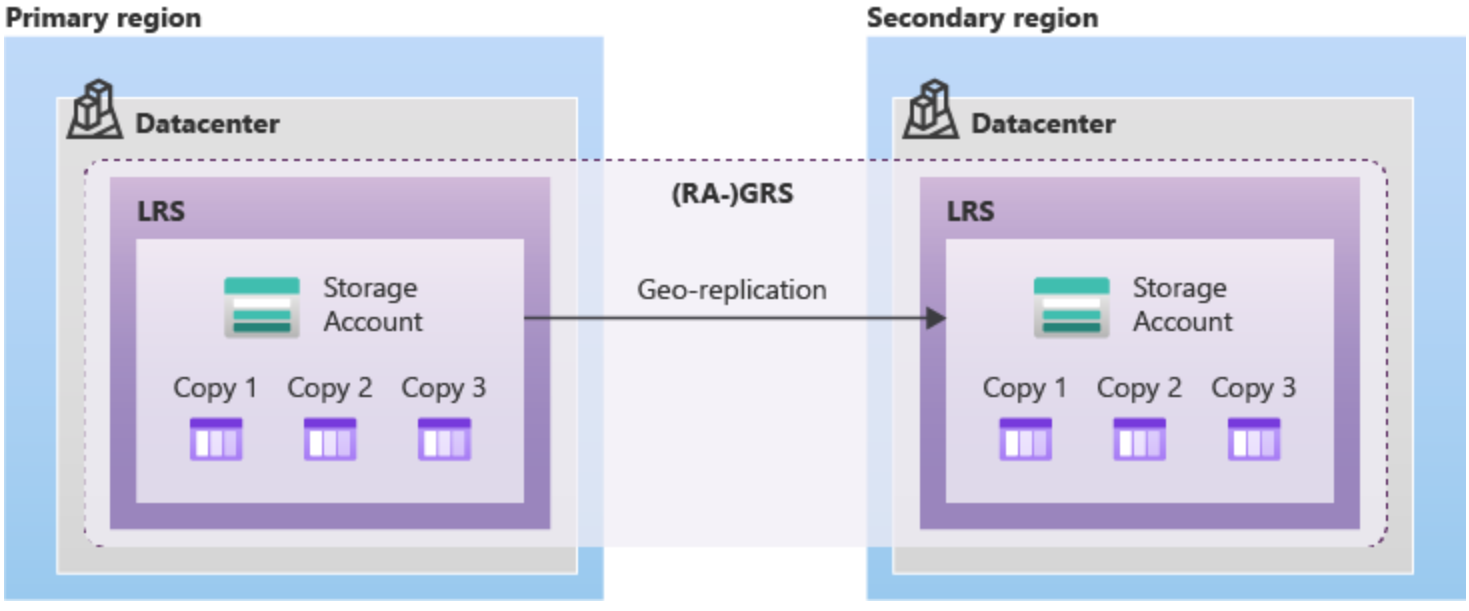
Notes:

In GRS case, your data will be replicated on to a different region altogether.

In this scenario Local redundancy storage will also work, and the data will be stored locally on three devices within a data center.

In this case, if entire zone, like Central US goes down, your data will be available in East US 2.





4. **Read-access Zone Redundant Storage**

Read-access zone redundant storage is similar to zone redundant storage, but in this scenario, you would be able to access your data in both the regions at the same time, like: US-East 1 & Central US.

Use Case: So, if your application needs access onto objects in both of the regions, you can choose Read-access zone redundant storage.

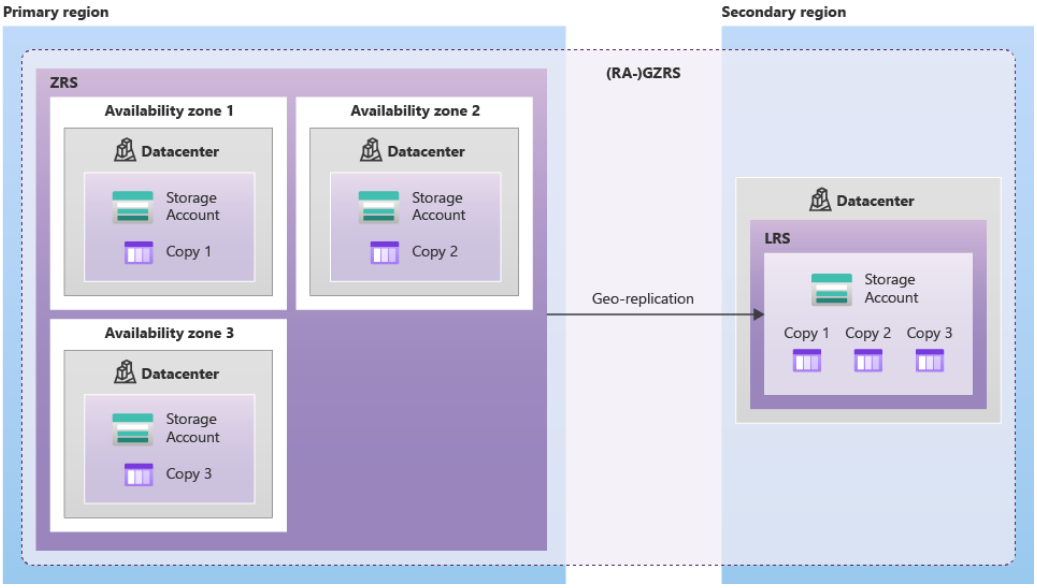
5. **Geo-zone-redundant storage**

Geo-zone-redundant storage (GZRS) combines the high availability provided by redundancy across availability zones with protection from regional outages provided by geo-replication. Data in a GZRS storage account is copied across three Azure availability zones in the primary region and is also replicated to a secondary geographic region for protection from regional disasters. Microsoft recommends using GZRS for applications requiring maximum consistency, durability, and availability, excellent performance, and resilience for disaster recovery.

With a GZRS storage account, you can continue to read and write data if an availability zone becomes unavailable or is unrecoverable. Additionally, your data is also durable in the case of a complete regional outage or a disaster in which the primary region isn't recoverable. GZRS is designed to provide at least 99.99999999999999% (16 9's) durability of objects over a given year.

Only general-purpose v2 storage accounts support GZRS and RA-GZRS.

Read-Access Geo-Zone-Redundant Storage (RA-GZRS) is also there.



Azure Storage – Access Tiers

There are three access tiers in Azure storage.

1. **Hot Access Tier** – This is used for data that is accessed frequently
2. **Cool Access Tier** – This is used for data that is accessed infrequently and stored for at least 30 days
3. **Archive Access Tier** – This is used for data that is rarely accessed and stored for at least 180 days
   Archive can be only enabled on individual Blob level. Hot & Cool can be enabled for any kind of storage, like Blob, files, tables

How to access Archive files

1. You have to rehydrate the file to access the file
2. To rehydrate the file, you have to change the access tier of the file to either Hot or Cool to access the file
3. It takes time to rehydrate and access that object

Rehydration Process

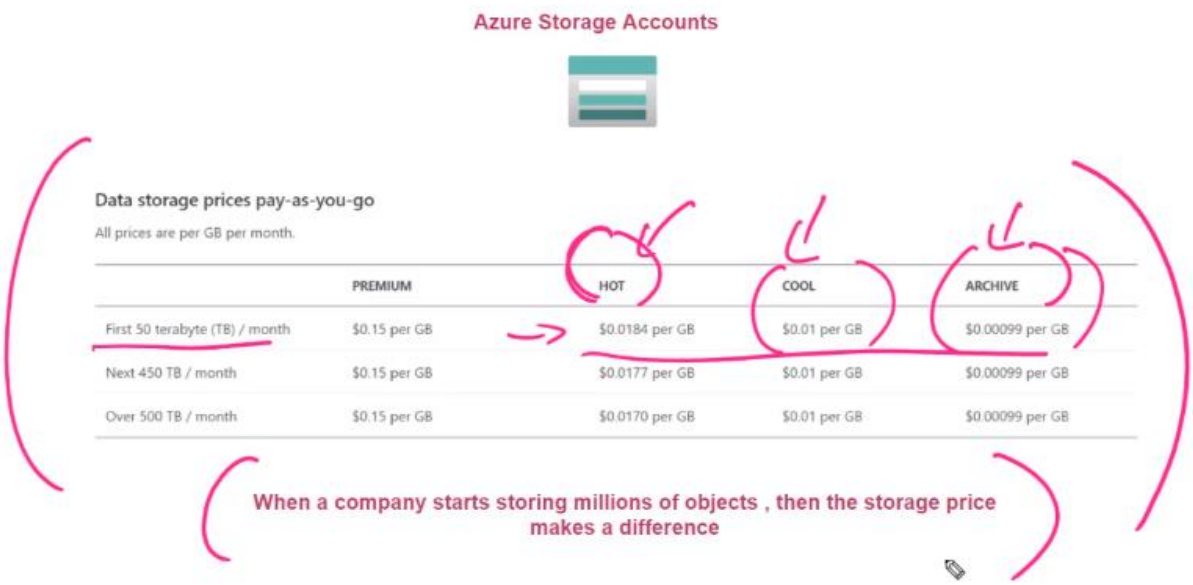
There are two options

1. **Standard Priority**

The request is processed in the order received and can take up to 15 hours. After this time only you could access the file

2. **High Priority**

The request is prioritized and could finish in under 1 hour for objects under 10 GB in size



Azure Block Blob Storage

Premium Performance for Block Blob Storage

Block blobs are optimized for uploading large amounts of data efficiently. Block blobs are composed of blocks, each of which is identified by a block ID.

1. Block blobs are basically your objects such as videos and images
2. You can create a **BlockBlobStorage** account of the Premium performance kind
3. Here the data will be stored on solid state drive (SSD). This will give you faster access to your data when compared to let's say using the Blob service in General Purpose v2 storage accounts
4. If you have applications like Artificial Intelligence or Machine Learning applications that require rapid responses to change in data, you can consider this type of storage account

Premium Performance for block blob

› Reference - https://azure.microsoft.com/en-us/pricing/details/storage/blobs/

Data storage prices pay-as-you-go

All prices are per GB per month.

	PREMIUM	HOT	COOL	ARCHIVE
First 50 terabyte (TB) / month	$0.15 per GB	$0.0184 per GB	$0.01 per GB	$0.00099 per GB
Next 450 TB / month	$0.15 per GB	$0.0177 per GB	$0.01 per GB	$0.00099 per GB
Over 500 TB / month	$0.15 per GB	$0.0170 per GB	$0.01 per GB	$0.00099 per GB

Premium Performance for page Blob

1. Page blobs are basically used for storing disk files for your virtual machines
2. You can choose Premium SSD to get the best performance for your page Blob
3. This will increase the storage performance for your underlying virtual machines
4. With Azure Management Disks, you can also choose Premium SSD's
5. You can use un-managed disks, where in you manage the disks for your virtual machines
6. You can choose General Purpose V2 or General Purpose V1 storage accounts of the Premium Performance to store page blobs

Azure Storage Account – Change Replication

1. If you want to migrate the storage account from LRS to ZRS in the primary region, then you need to perform either a manual migration or live migration
- For a manual migration, you basically create another storage account with the ZRS replication type, and then you copy the data from the source onto the destination
- Now during the manual migration, you might need to ensure that no new objects are being added on to your primary storage accounts because you need to go out and migrate everything at a particular point in time once a migration is complete
- If you have an application that has been using that storage account that you need to go out and switch onto a new storage account, so there might be a downtime for your application during a manual migration.
2. You can also request Microsoft to perform a live migration. This ensures that you have no application downtime during the migration process. Here you can access the data as the migration is processing
3. To migrate from LRS to GZRS or RA-GZRS, first switch to GRS or RA-GRS and then request a live migration
4. To migrate from GRS or RA-GRS to ZRS, first switch to LRS, then request a live migration

Azure Storage Account – Lifecycle Management Policies

Azure Blob Storage lifecycle management offers a rich, rule-based policy for GPv2 and blob storage accounts. Use the policy to transition your data to the appropriate access tiers or expire at the end of the data's lifecycle. The lifecycle management feature is available in all Azure regions for general purpose v2 (GPv2) accounts, blob storage accounts, premium block blobs storage accounts, and Azure Data Lake Storage Gen2 accounts.

Azure Storage Account – Object Replication

Object replication asynchronously copies block blobs between a source storage account and a destination account.

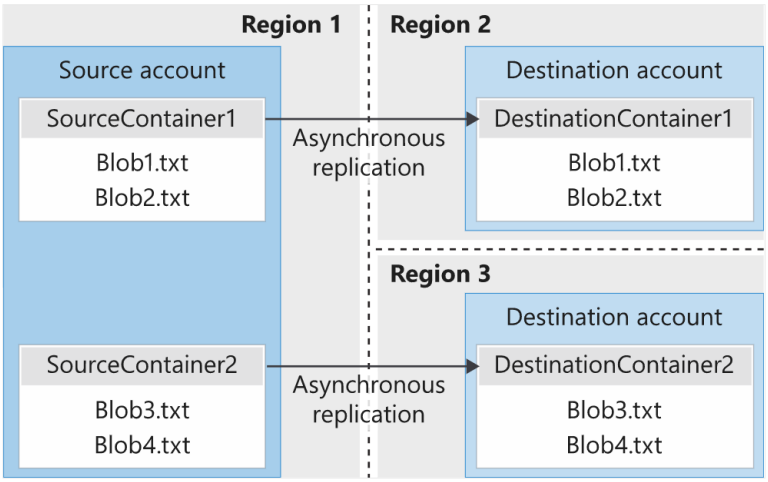
Some benefits and use cases:

- Minimizing latency
- Increase efficiency for compute workloads
- Optimizing data distribution
- Optimizing costs

Notes:

- Object replication works if the blobs are either in the Hot/Cool access tier
- Object replication will fail if the objects are in the archive access tier

The following diagram shows how object replication replicates block blobs from a source storage account in one region to destination accounts in two different regions.



Azure – File Share

Azure Files offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) protocol or Network File System (NFS) protocol. Azure file shares can be mounted concurrently by cloud or on-premises deployments. Azure Files SMB file shares are accessible from Windows, Linux, and macOS clients.

Azure Files NFS file shares are accessible from Linux or macOS clients. Additionally, Azure Files SMB file shares can be cached on Windows Servers with Azure File Sync for fast access near where the data is being used.

Key benefits of Azure File Share

1. **Shared access**

Azure file shares support the industry standard SMB and NFS protocols. Being able to share a file system across multiple machines, applications/instances is a significant advantage with Azure Files for applications that need shareability

2. **Fully managed**

Azure file shares can be created without the need to manage hardware or an OS. This means you don't have to deal with patching the server OS with critical security upgrades or replacing faulty hard disks

3. **Scripting and tooling**

PowerShell cmdlets and Azure CLI can be used to create, mount, and manage Azure file shares as part of the administration of Azure applications. You can create and manage Azure file shares using Azure portal and Azure Storage Explorer

4. **Resiliency**

Azure Files has been built from the ground up to be always available. Replacing on-premises file shares with Azure Files means you no longer have to wake up to deal with local power outages or network issues

5. **Familiar programmability**

Applications running in Azure can access data in the share via file system I/O APIs. Developers can therefore leverage their existing code and skills to migrate existing applications. In addition to System IO APIs, you can use Azure Storage Client Libraries or the Azure Storage REST API

Transferring Data to Azure Storage Accounts

Azure Import/Export Service

- This can be used to securely import large amounts of data to the Azure Blob and Azure File service
- Here you can actually store the data that you want to transfer on your own drives, or you can use disk drives provided by Microsoft
- You can ship the drives to an Azure datacenter
- The data on the drives will be imported to Azure Blob or Azure File storage
- You can also use the service to export data from Azure Blobs

What are general steps involved

1. First you decide the storage account that you're going to import data into
2. What is the type of service you want – Azure Blob or Azure File Share
3. Then, finally you have your disk drives in place on which you're going to have your data
4. Now on your disk drives you need to get your data in a ready state that needs to be imported onto Azure Storage Account. For that you have to download a tool, that's freely available.
5. WAImportExportTool to copy data onto disk drives . The Disk Drives needs to be encrypted with BitLocker
6. You then need to create an import job in Azure. Here you need to associate the job with an Azure storage account. You also need to upload the drive journal files to the job
7. You also need to mention the return address (while physically mailing the drives onto the Azure Datacenters)
8. Then ship the drives to the Azure datacenters

AzCopy Tool

Another tool which is available for transferring data is AzCopy Tool

- This is a command utility that you can use to copy blobs or files to or from a storage account
- This tool works on Windows, Linux, and MacOS

Azure Data Box

This is similar to the Azure Import/Export service, but here the device itself sent to you for storing the data, which is a Microsoft provided appliance

Data Box – 100 TB

Data Box Disk – 8 TB

Data Box Heavy – 1 PB

Azure Data Factory

- This is a cloud service that can be used to perform ETL (Extract-Transform-Load), ELT (Extract-Load-Transform) and data integration projects
- In the Azure Data Factory service, you can author various types of activities

Key Components:

- Data Set

This is the source of your data. It can be an on-premises file server, SQL database server, Azure SQL database server. You define a linked service that is used to connect to the data source.

- Activity

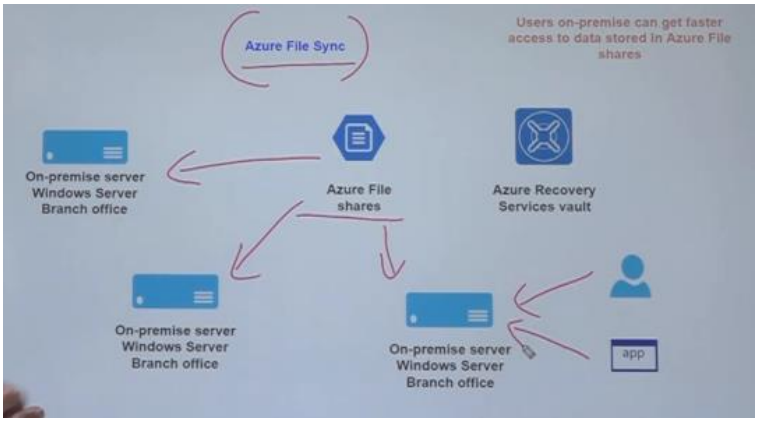
You then define the activity. Examples of activities is ingesting data, cleaning data

- All of these activities then run as part of a pipeline

Azure File Sync

Azure File Sync is a service that allows you to cache several Azure file shares on an on-premises Windows Server or cloud VM.
You can use the Azure File Sync service to seek files from your file share onto your on-premises servers. You could use the file share service to actually sync the files from Azure File Share onto multiple servers in your on-premises locations.

Example:
You have multiple branch offices, and you want the file shares to be available locally so they could be accessed faster.



Azure – Backup Service

The Azure Backup service provides simple, secure, and cost-effective solutions to back up your data and recover it from the Microsoft Azure cloud

1. It is a service to take backup of your Azure virtual machines. You can restore the virtual machine using the Azure backup service.
2. There are recovery points being created every time the backup happens, like today recovery point, tmrw recovery point, last week recovery point, etc.
3. When you choose recovery point, you can decide what kind of data you want to recover, like:
   a. Individual Files – you can choose particular files which you want to recover
   b. VM Recovery – you can recover whole VM and create a duplicate VM
   c. Disk Recovery – you can recover a whole disk and save it separately
4. When you are recovering data, at no point in time you are actually connected to the virtual machine, whose data got backed up. The VM will be running separately without any impact on it.
5. At the time of creation of virtual machine, you can select if you want to enable backup for the virtual machine and select and configure the backup policy as well
6. There are two major separate services which are a part of Azure Backup service:
   d. Azure Recovery Services Vault
   e. Backup Policy
7. When you take backup, the backup data is being stored in "Azure Recovery Services Vault". It is a separate resource in
   Azure
a. Azure Recovery Services Vault
8. The "Azure Recovery Services Vault" should be in the same region as the Azure virtual machine
9. During the first backup, all the data from the underlying disk will be taken as backup onto "Recovery Services Vault"
10. The next backup will be subsequent in nature, and only the changes or new data will be backed up

b. Backup Policy

11. Backup policy is to configure to schedule the backup process
12. You can mention the retention period of the backup data as well

Few more points:

- During the first backup, an extension gets installed on the virtual machine
- The type of extension depends upon the type of virtual machine operating system, like for Windows or for Linux
- This extension is used to take a snapshot of the disk attached to the virtual machine
- For Windows based VM's, the backup service works with the "Windows Volume Shadow Copy Service" that can be used to take an application consistent snapshot of the virtual machine
- For Linux based VM's, the service takes a file-consistent backup

Types of Snapshots are:

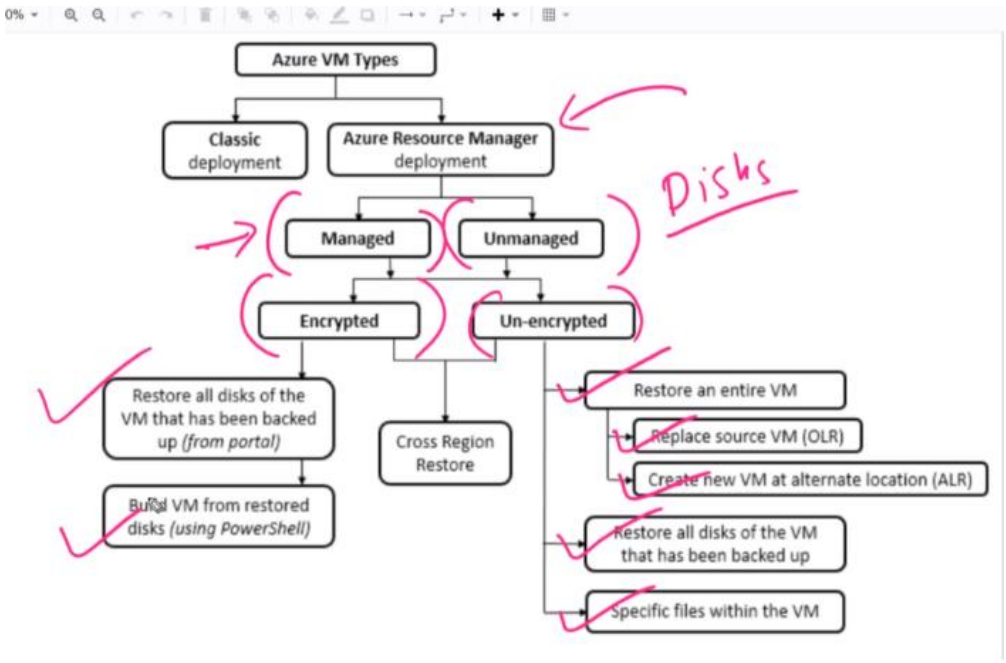
- Application Consistent
  It captures the memory content, pending I/O operations
  It ensures that whatever is the state of the application at that point in time when the backup is being taken is consistent when a restore is taken from the particular backup
- File System Consistent
  It takes a snapshot of all the files at the same time
- Crash Consistent
  This happens when the virtual machine shuts down at the time of backup process

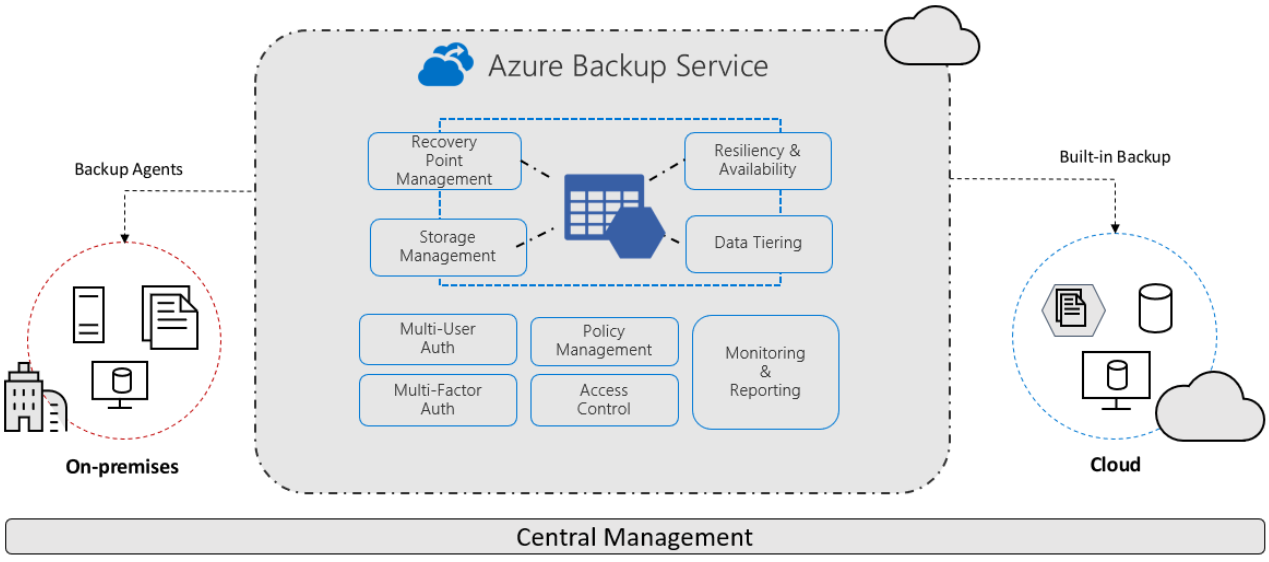
Instant Recovery Feature

Snapshots taken as a part of the backup job are stored along with the disk and are available for recovery instantly. Once the snapshot phase is done, users can go ahead and use the local snapshot to restore if the patch goes bad.

The instant recovery feature basically goes out and takes a snapshot of the VM itself and stores it locally within the virtual machine itself.

Restore Options





Restore individual files:

The particular drive gets created on your local machine, and from that you can take the files.

The *.exe file will be created, which will run on PowerShell on local system to make new drives on your host from the restore point

Once the activity done, you can unmount those drive on the Azure portal itself

Soft Delete

Soft delete protects backup data from accidental deletes

Soft delete is a feature which keeps your backup files for 14 days.

Even if you stop the backup of a VM, still the backup of a particular VM would be available for 14 days in the recovery services vault

Soft delete option has to be disabled to delete the saved backups in the recovery services vault

Steps:

1. Stop the backup of the VM
2. Go to > Recovery Services Vault > Properties > Security Settings > Soft Delete > disable soft delete
3. Even if you stop and delete the backup data, you still won't be able to delete the recovery services vault for 14 days
4. Then delete the backup of all the VM's
5. Then delete the recovery services vault, without disable of soft delete, you wouldn't had been able to delete the recovery services vault.

MARS Agent / Azure Backup Agent / Azure Recovery Services Agent

This agent helps you to take backup of particular services/files/folders of on-premises host as well.

You have to register your on-prem machine with Azure Recovery Services vault by using a MARS agent.

You can also use the 1st on-prem machine backup and restore it onto 2nd on-prem/VM machine as well.

Azure to Azure Site Recovery

This service recovers every resource which you choose to a new Azure location, in case of a primary site goes down.

This requires a Cache storage for keeping all the recovery in it, and once you do a failover, then everything will be copied from Cache storage, and will be restored to a new Azure site.

Azure Security – Interview Questions

Below are the interview questions which could be asked during the interviews, these are just the questions which I have mentioned, I didn't write the answers because this guide will help you find those answers.

1. Define Azure Security Center?
2. How does Azure Security Center help in improving the overall security infrastructure?
3. Difference between Azure Policies and Azure Blueprint?
4. Define encryption of data at rest?
5. What is Break-fix issues in Azure?
6. Name of the services that used to manage resources in Azure?
7. What is three tier architectures in Azure, and how that can be protected?
8. How do you connect on-premises applications to cloud services?
9. What should be strategy for application migration to the cloud?
10. What is the use of Azure CloudFront?
11. What is "EUCALYPTUS" stands for?

12. How many applications can be hosted on Azure WebApp?
13. How many layers are involved in PaaS architecture?
14. State the Azure encryption models?
15. What is conditional access in Azure, state some examples of it?