AZURE

AMJAD NAGORI

CONTENTS

INTRODUCTION (AMJAD NAGORI)

I have 4+ years of experience as **Azure Architect** with total 8+ years of IT Experience. I have extensive experience in Azure from designing the architecture to do the actual implementation of the different kind of environments. I also have good experience in cloud automation by using Azure DevOps, Terraform and Kubernetes.

I am **Microsoft Certified Azure Trainer** (MCT) and have completed my technical certifications into-

Azure Solutions Architect (AZ-300, AZ-301 & AZ-305)

Azure Security Associate (AZ-500)

Azure Networking Engineer (AZ-700)

Azure DevOps Associate (AZ-400)

Azure Administrator (AZ-104)

Azure Fundamental (AZ-900)

Azure Data Fundamentals (DP-900)

Security, Compliance, and Identity Fundamentals (SC-900)

Azure AI Fundamentals (AI-900)

Kubernetes Certified Administrator (CKA)

HashiCorp Terraform Associate

AWS Certified Cloud Practitioner (CLF-C01)

GitLab Associate

To get to know more about me, please visit my LinkedIn profile - https://www.linkedin.com/in/amjad-nagori-55060987/

WHAT IS CLOUD?

OVERVIEW

Cloud computing is the on-demand delivery of IT resources over the Internet with pay-as-you-go pricing. Instead of buying, owning, and maintaining physical data centres and servers, you can access technology services, such as computing power, storage, and databases, on an as-needed basis from a cloud provider like Azure, AWS or GCP.

TOP BENEFITS OF CLOUD COMPUTING

Cost: Cloud computing eliminates the capital expense of buying hardware and software and setting up and running on-site datacentres—the racks of servers, the round-the-clock electricity for power and cooling, the IT experts for managing the infrastructure. It adds up fast.

Global scale: The benefits of cloud computing services include the ability to scale elastically. In cloud speak, that means delivering the right amount of IT resources—for example, more or less computing power, storage, bandwidth—right when it is needed and from the right geographic location.

Performance: The biggest cloud computing services run on a worldwide network of secure datacentres, which are regularly upgraded to the latest generation of fast and efficient computing hardware. This offers several benefits over a single corporate datacentre, including reduced network latency for applications and greater economies of scale.

Security: Many cloud providers offer a broad set of policies, technologies and controls that strengthen your security posture overall, helping protect your data, apps and infrastructure from potential threats.

Speed: Most cloud computing services are provided self service and on demand, so even vast amounts of computing resources can be provisioned in minutes, typically with just a few mouse clicks, giving businesses a lot of flexibility and taking the pressure off capacity planning.

Productivity: On-site datacentres typically require a lot of "racking and stacking"—hardware setup, software patching, and other time-consuming IT management chores. Cloud computing removes the need for many of these tasks, so IT teams can spend time on achieving more important business goals.

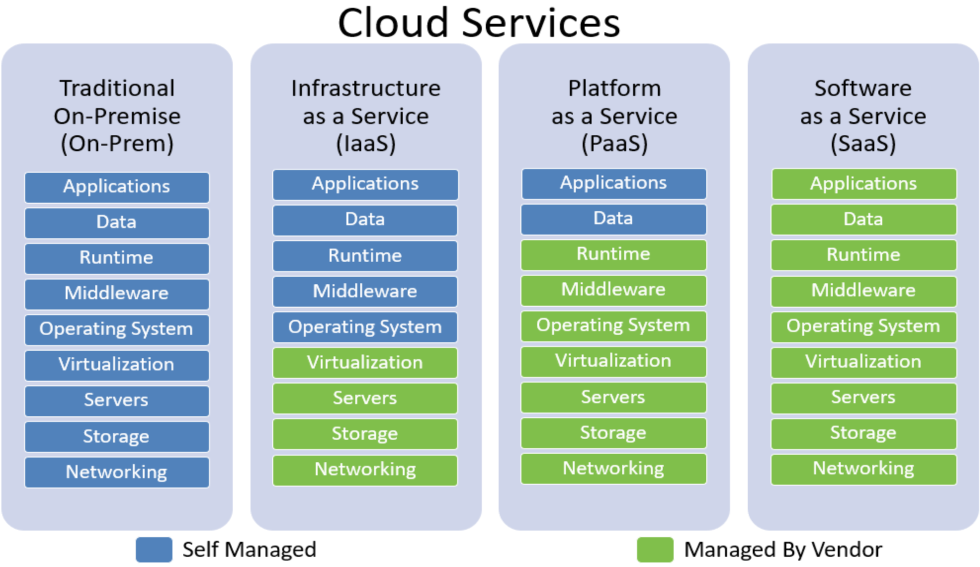
Reliability: Cloud computing makes data backup, disaster recovery and business continuity easier and less expensive because data can be mirrored at multiple redundant sites on the cloud provider's network.

TYPES OF CLOUD COMPUTING

1. Public Cloud
2. Private Cloud
3. Hybrid Cloud

TYPES OF CLOUD SERVICES

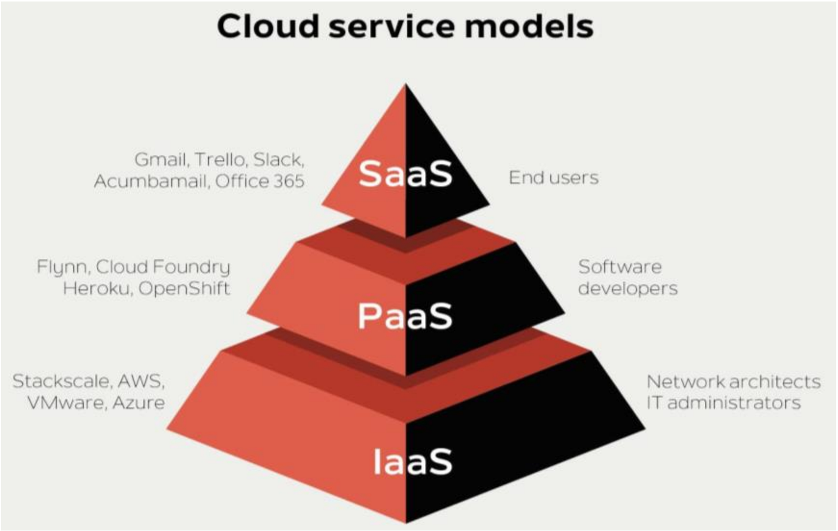
1. IaaS – Infrastructure as a Service
2. PaaS – Platform as a Service
3. SaaS – Software as a Service



Cloud Services

Traditional On-Premise (On-Prem)	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
🟦 Applications	🟦 Applications	🟦 Applications	🟩 Applications
🟦 Data	🟦 Data	🟦 Data	🟩 Data
🟦 Runtime	🟦 Runtime	🟩 Runtime	🟩 Runtime
🟦 Middleware	🟦 Middleware	🟩 Middleware	🟩 Middleware
🟦 Operating System	🟦 Operating System	🟩 Operating System	🟩 Operating System
🟦 Virtualization	🟩 Virtualization	🟩 Virtualization	🟩 Virtualization
🟦 Servers	🟩 Servers	🟩 Servers	🟩 Servers
🟦 Storage	🟩 Storage	🟩 Storage	🟩 Storage
🟦 Networking	🟩 Networking	🟩 Networking	🟩 Networking

🟦 Self Managed 🟩 Managed By Vendor



Cloud service models

Gmail, Trello, Slack, Acumbamail, Office 365
SaaS
End users
Flynn, Cloud Foundry Heroku, OpenShift
PaaS
Software developers
Stackscale, AWS, VMware, Azure
IaaS
Network architects IT administrators

AZURE PORTAL INTRODUCTION

OVERVIEW

The Azure portal is a web-based, unified console that provides an alternative to command-line tools. With the Azure portal, you can manage your Azure subscription using a graphical user interface. You can build, manage, and monitor everything from simple web apps to complex cloud deployments. Create custom dashboards for an organized view of resources. Configure accessibility options for an optimal experience.

AZURE CLOUD SHELL

Azure Cloud Shell is a browser-based shell experience to manage and develop Azure resources. Cloud Shell offers a browser-accessible, pre-configured shell experience for managing Azure resources without the overhead of installing, versioning, and maintaining a machine yourself.

AZURE ACTIVE DIRECTORY

TENANT

A tenant represents an organization in Azure Active Directory. It's a dedicated Azure AD service instance that an organization receives and owns when it signs up for a Microsoft cloud service such as Azure, Microsoft Intune, or Microsoft 365. Each Azure AD tenant is distinct and separate from other Azure AD tenants.

https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-create-new-tenant

LICENSES

1. Azure Active Directory Free
2. Azure Active Directory Premium P1
3. Azure Active Directory Premium P2

https://www.microsoft.com/en-us/security/business/identity-access-management/azure-ad-pricing

USERS

Type of Users –

1. New user
2. Guest user

GUEST USER INVITATION

Overview to send and accept the invitation for Guest Users.

GROUPS

Type of Groups –

1. Security Groups
2. Dynamic Groups
3. O365 Groups

Group Settings –

1. General configurations
2. Expiration
3. Naming Policy

ROLES

Type of Roles –

1. Built-in roles
2. Custom roles

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

ENTERPRISE APPLICATION & APPLICATION REGISTRATION

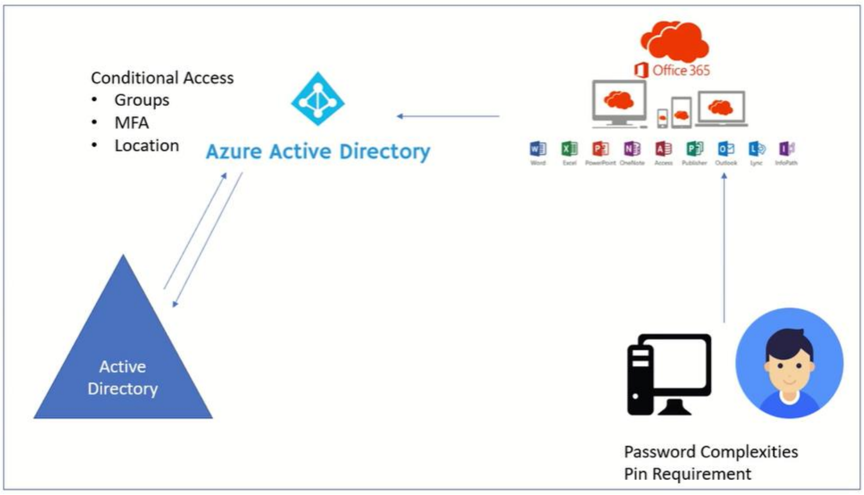
Azure AD is an Identity and Access Management (IAM) system. It provides a single place to store information about digital identities. You can configure your software applications to use Azure AD as the place where user information is stored.

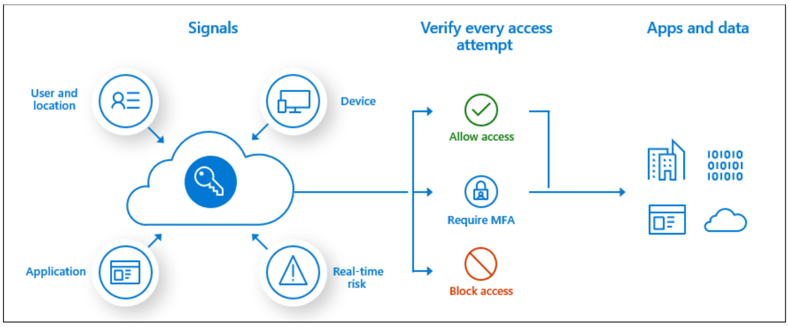
Azure AD must be configured to integrate with an application. In other words, it needs to know what apps are using it for identities. Making Azure AD aware of these apps, and how it should handle them, is known as application management.

CONDITIONAL ACCESS

Conditional Access is the tool used by Azure Active Directory to bring signals together, to make decisions, and enforce organizational policies. Conditional Access is at the heart of the new identity driven control plane.

Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action. Example: A payroll manager wants to access the payroll application and is required to perform multi-factor authentication to access it.





IDENTITY GOVERNANCE (P2 LICENSE REQUIRED)

Types –

1. **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.

2. **Entitlement management (Access Package):**
   Employees in organizations need access to various groups, applications, and sites to perform their job. Managing this access is challenging, as requirements change - new applications are added or users need additional access rights. This scenario gets more complicated when you collaborate with outside organizations - you may not know who in the other organization needs access to your organization's resources, and they won't know what applications, groups, or sites your organization is using.
   Azure AD entitlement management can help you more efficiently manage access to groups, applications, and SharePoint Online sites for internal users, and also for users outside your organization who need access to those resources.

3. **Privileged Identity Management:**
   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. The following video introduces you to important PIM concepts and features.

Features –

- 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

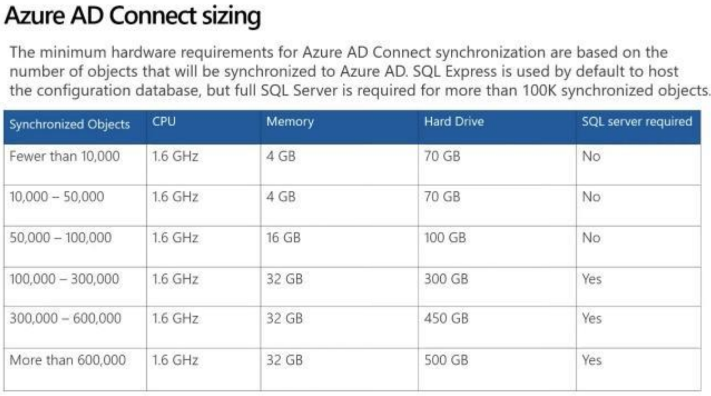
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

AZURE AD CONNECT

Azure AD Connect is the Microsoft tool designed to meet and accomplish your hybrid identity goals. It helps to synchronize your users, passwords and groups from on-premises to Azure AD and vice versa (if password writeback enabled).

Pre-requisites:

- Forest functional level 2003 or higher.
- Writable domain controllers
- Windows Server 2008 or later
- Ports required - 80, 443, 5671 (outbound)
- License – by default its free but required P1 for certain functionality like Password Writeback.
- Recommended server size for Azure AD Connect-



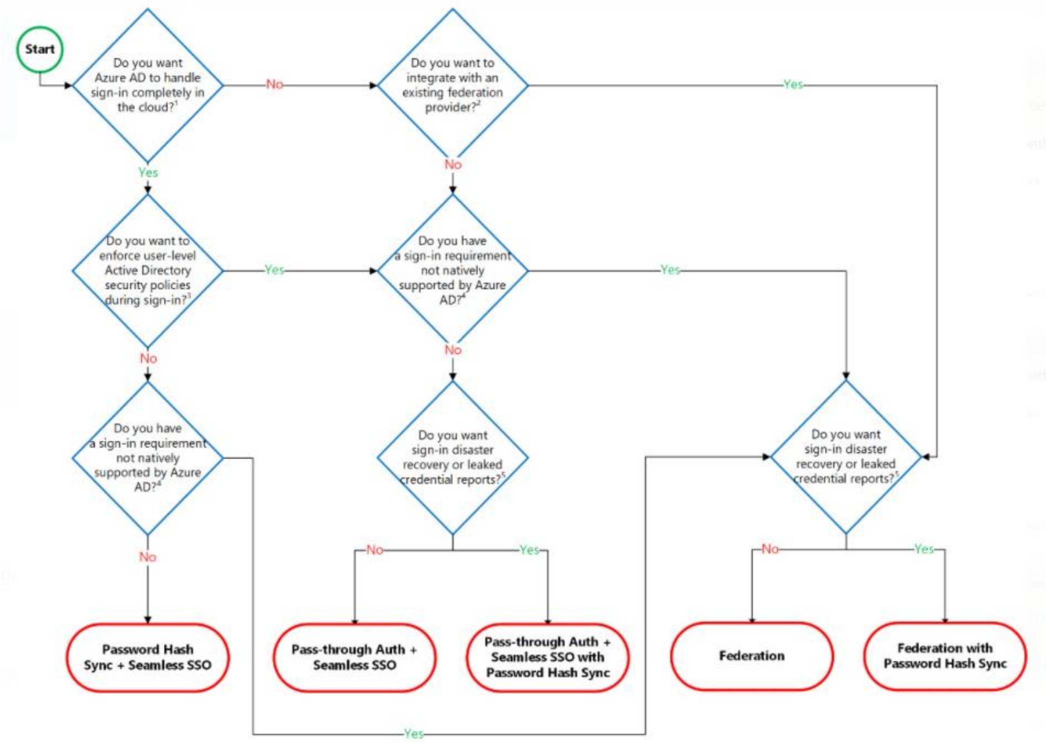
Azure AD Connect sizing

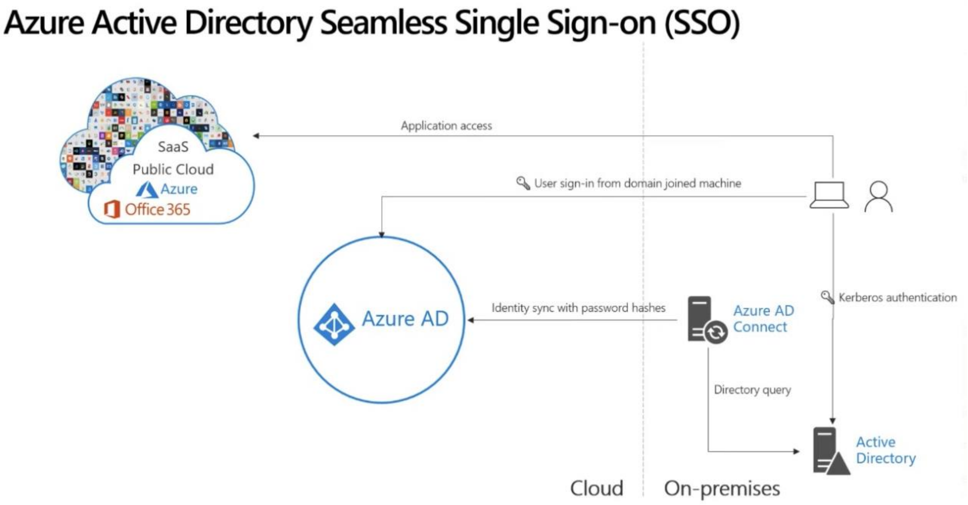
The minimum hardware requirements for Azure AD Connect synchronization are based on the number of objects that will be synchronized to Azure AD. SQL Express is used by default to host the configuration database, but full SQL Server is required for more than 100K synchronized objects.

Synchronized Objects	CPU	Memory	Hard Drive	SQL server required
Fewer than 10,000	1.6 GHz	4 GB	70 GB	No
10,000 – 50,000	1.6 GHz	4 GB	70 GB	No
50,000 – 100,000	1.6 GHz	16 GB	100 GB	No
100,000 – 300,000	1.6 GHz	32 GB	300 GB	Yes
300,000 – 600,000	1.6 GHz	32 GB	450 GB	Yes
More than 600,000	1.6 GHz	32 GB	500 GB	Yes

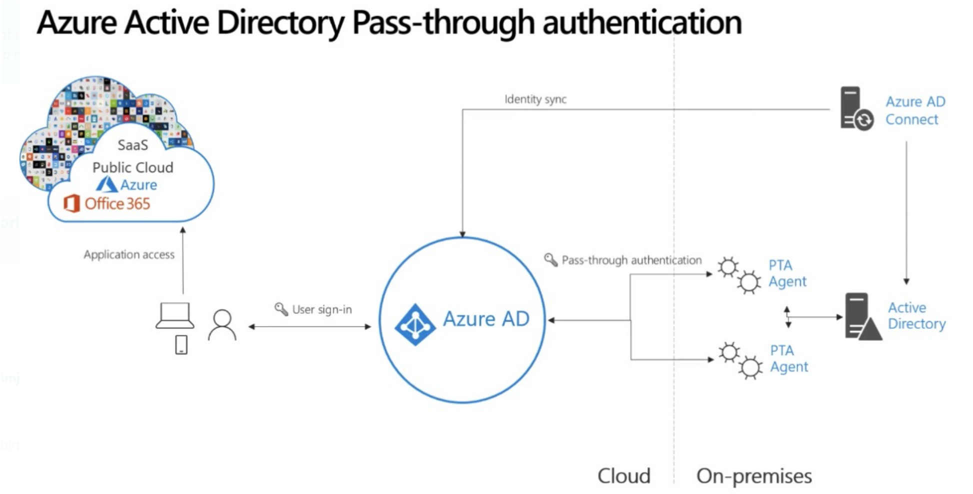
Features-

- **Password hash synchronization**:
  A sign-in method that synchronizes a hash of a users on-premises AD password with Azure AD. It synchronize password from on-premise active directory to Azure AD and storing it on Azure Active Directory, so whenever you are login it verify password from Azure AD itself.
  If you are changing password on on-premises, then it will sync again with Azure AD and schedule for the same is every 2 mins.
  If you are changing any other details like contact number, name or dept then it will synch in every 30 mins, so if you are disabling user on on-premises then it may take up to 30 mins to disable on Azure AD or you can manually do the force synchronization.
  PowerShell command to get status of sync - *Get-ADSyncSchedule*
- **Pass-through authentication**:
  A sign-in method that allows users to use the same password on-premises and in the cloud, but doesn't require the additional infrastructure of a federated environment.
- **Federation integration:**
  Federation is an optional part of Azure AD Connect and can be used to configure a hybrid environment using an on-premises AD FS infrastructure. It also provides AD FS management capabilities such as certificate renewal and additional AD FS server deployments.
- **Password Writeback:**
  Password writeback can be used to synchronize password changes in Azure AD back to your on-premises AD environment. Azure AD Connect provides a secure mechanism to send this password changes back to an existing on-premises directory from Azure.


Start
Do you want Azure AD to handle sign-in completely in the cloud?1
No
Yes
Do you want to integrate with an existing federation provider?2
Yes
No
Do you want to enforce user-level Active Directory security policies during sign-in?3
Yes
No
Do you have a sign-in requirement not natively supported by Azure AD?4
Yes
No
Do you have a sign-in requirement not natively supported by Azure AD?4
No
Yes
Do you want sign-in disaster recovery or leaked credential reports?5
No
Yes
Do you want sign-in disaster recovery or leaked credential reports?5
No
Yes
Password Hash Sync + Seamless SSO
Pass-through Auth + Seamless SSO
Pass-through Auth + Seamless SSO with Password Hash Sync
Federation
Federation with Password Hash Sync

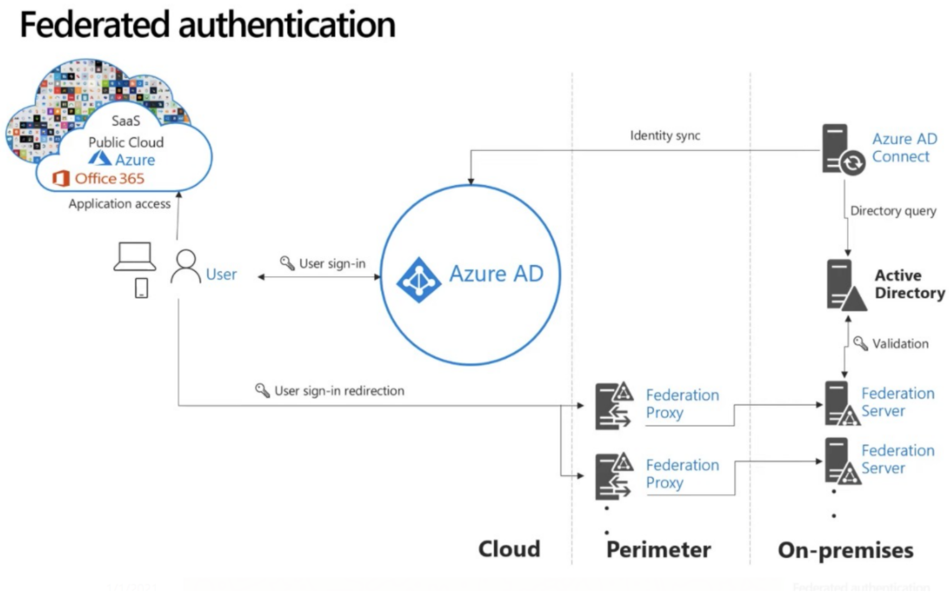


Azure Active Directory Seamless Single Sign-on (SSO)



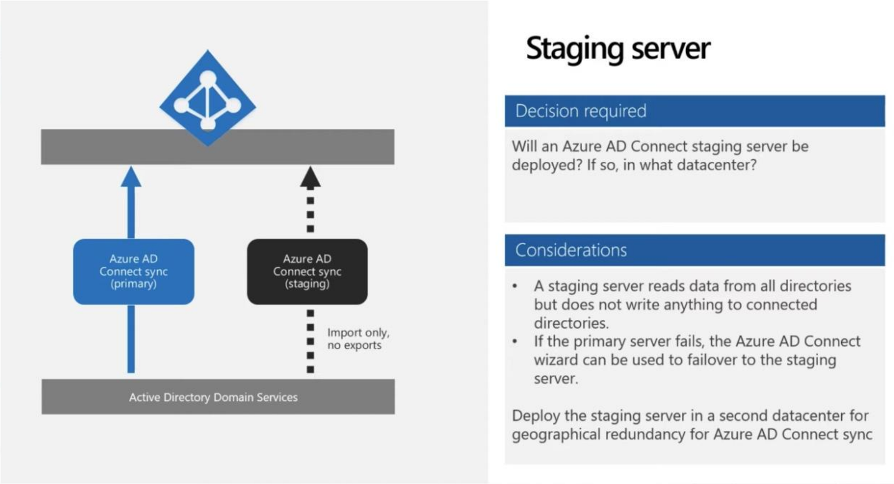
Azure Active Directory Pass-through authentication

On-premises password policy will be application in Pass-through authentication. PTA agent will continuously check and authenticate users whenever we are getting Kerberos authentication request.



Federated authentication

https://docs.microsoft.com/en-gb/azure/active-directory/hybrid/plan-connect-performance-factors


Azure AD Connect sync (primary)
Azure AD Connect sync (staging)
Import only, no exports
Active Directory Domain Services

Staging server

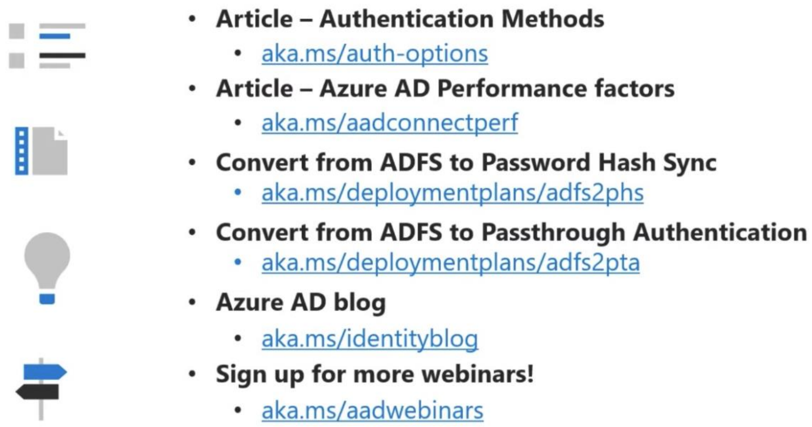
Decision required

Will an Azure AD Connect staging server be deployed? If so, in what datacenter?

Considerations

- A staging server reads data from all directories but does not write anything to connected directories.
- If the primary server fails, the Azure AD Connect wizard can be used to failover to the staging server.

Deploy the staging server in a second datacenter for geographical redundancy for Azure AD Connect sync



- **Article – Authentication Methods**
  - aka.ms/auth-options
- **Article – Azure AD Performance factors**
  - aka.ms/aadconnectperf
- **Convert from ADFS to Password Hash Sync**
  - aka.ms/deploymentplans/adfs2phs
- **Convert from ADFS to Passthrough Authentication**
  - aka.ms/deploymentplans/adfs2pta
- **Azure AD blog**
  - aka.ms/identityblog
- **Sign up for more webinars!**
  - aka.ms/aadwebinars

CUSTOM DOMAIN NAMES

Every new Azure AD tenant comes with an initial domain name, <domainname>.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 usernames that are familiar to your users, such as alain@contoso.com.

PASSWORD RESET

Azure Active Directory (Azure AD) self-service password reset (SSPR) gives users the ability to change or reset their password, with no administrator or help desk involvement. If a user's account is locked or they forget their password, they can follow prompts to unblock themselves and get back to work. This ability reduces help desk calls and loss of productivity when a user can't sign in to their device or an application.

COMPANY BRANDING

Use your organization's logo and custom color schemes to provide a consistent look-and-feel on your Azure Active Directory (Azure AD) sign-in pages. Your sign-in pages appear when users sign in to your organization's web-based apps, such as Microsoft 365, which uses Azure AD as your identity provider.

DEVICES (OVERVIEW)

With the proliferation of devices of all shapes and sizes and the Bring Your Own Device (BYOD) concept, IT professionals are faced with two somewhat opposing goals:

- Allow end users to be productive wherever and whenever
- Protect the organization's assets

To protect these assets, IT staff need to first manage the device identities. IT staff can build on the device identity with tools like Microsoft Intune to ensure standards for security and compliance are met. Azure Active Directory (Azure AD) enables single sign-on to devices, apps, and services from anywhere through these devices.

Types of Azure AD Device Configuration-

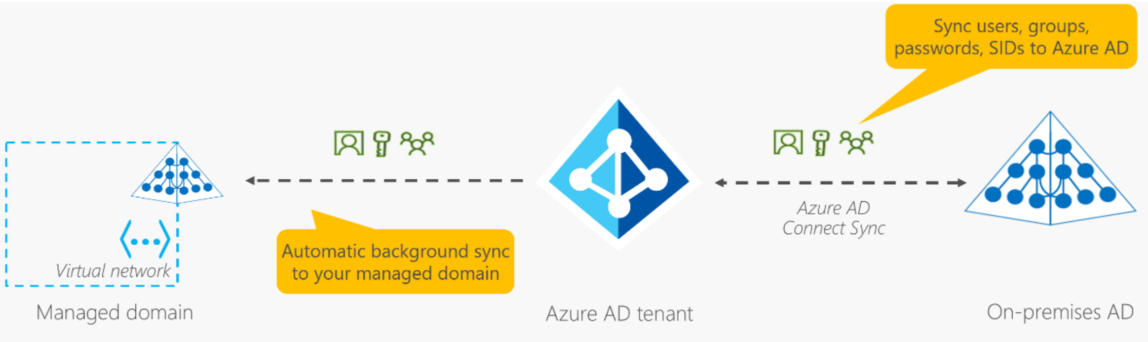
1. **Azure AD Device Registration –** For single user profile registration.
2. **Azure AD Joined Devices –** To join device to Azure AD, we can use Azure AD users to login on machine.
3. **Hybrid Azure AD Joined Devices –** To join devices to on-premises and Azure AD both.

AZURE AD DOMAIN SERVICES (OVERVIEW)

Azure Active Directory Domain Services (AD DS) provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos/NTLM authentication. You use these domain services without the need to deploy, manage, and patch domain controllers (DCs) in the cloud.

An Azure AD DS managed domain lets you run legacy applications in the cloud that can't use modern authentication methods, or where you don't want directory lookups to always go back to an on-premises AD DS environment. You can lift and shift those legacy applications from your on-premises environment into a managed domain, without needing to manage the AD DS environment in the cloud.

Azure AD DS integrates with your existing Azure AD tenant. This integration lets users sign into services and applications connected to the managed domain using their existing credentials. You can also use existing groups and user accounts to secure access to resources. These features provide a smoother lift-and-shift of on-premises resources to Azure.


Sync users, groups, passwords, SIDs to Azure AD
Virtual network
Managed domain
Automatic background sync to your managed domain
Azure AD tenant
Azure AD Connect Sync
On-premises AD

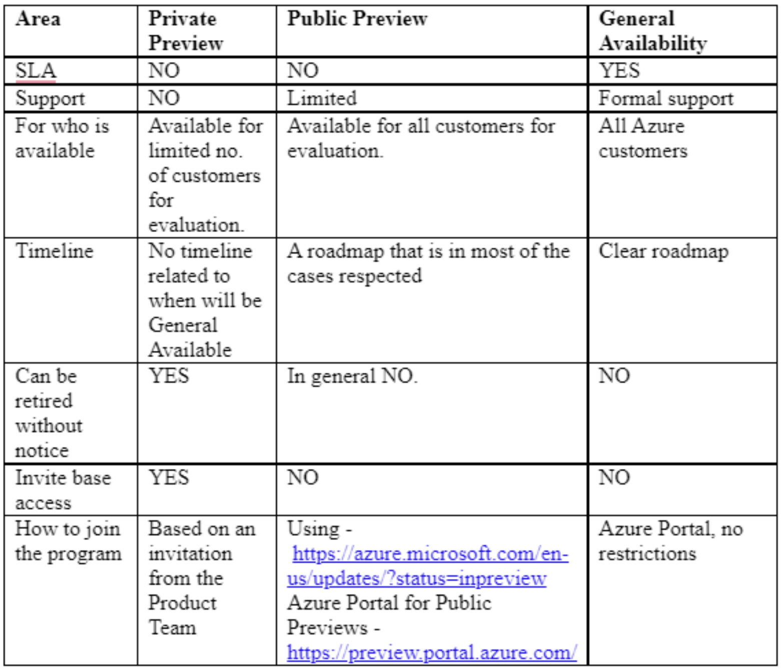
The following features of Azure AD DS simplify deployment and management operations:

- **Integrated with Azure AD:**
  User accounts, group memberships, and credentials are automatically available from your Azure AD tenant. New users, groups, or changes to attributes from your Azure AD tenant or you're on-premises AD DS environment are automatically synchronized to Azure AD DS.
- **Use your corporate credentials/passwords:**
  Passwords for users in Azure AD DS are the same as in your Azure AD tenant. Users can use their corporate credentials to domain-join machines, sign in interactively or over remote desktop, and authenticate against the managed domain.
- **NTLM and Kerberos authentication:**
  With support for NTLM and Kerberos authentication, you can deploy applications that rely on Windows-integrated authentication.
- **High availability:**
  Azure AD DS includes multiple domain controllers, which provide high availability for your managed domain. This high availability guarantees service uptime and resilience to failures.
  In regions that support Azure Availability Zones, these domain controllers are also distributed across zones for additional resiliency.
  Replica sets can also be used to provide geographical disaster recovery for legacy applications if an Azure region goes offline.

AZURE SERVICE LIFECYCLE

OVERVIEW

The service lifecycle defines how every Azure service is released for public use.



Area	Private Preview	Public Preview	General Availability
SLA	NO	NO	YES
Support	NO	Limited	Formal support
For who is available	Available for limited no. of customers for evaluation.	Available for all customers for evaluation.	All Azure customers
Timeline	No timeline related to when will be General Available	A roadmap that is in most of the cases respected	Clear roadmap
Can be retired without notice	YES	In general NO.	NO
Invite base access	YES	NO	NO
How to join the program	Based on an invitation from the Product Team	Using - https://azure.microsoft.com/en-us/updates/?status=inpreview Azure Portal for Public Previews - https://preview.portal.azure.com/	Azure Portal, no restrictions

SUBSCRIPTIONS

OVERVIEW

Azure Subscription is second layer in Azure after first layer of Active Directory. Microsoft generates your consumption bill on each subscription level. You can have multiple subscription in 1 active directory, but you can't connect subscription with more than 1 active directory.

Microsoft offering below plans for subscription-

1. Free Account
2. Pay-as-you-go
3. Enterprise

ROLE BASED ACCESS CONTROL (RBAC) - IAM

1. Check Access
2. Role assignments
3. Roles
4. Deny assignments

SECURITY RECOMMENDATIONS

Azure Security Benchmark is the Microsoft-authored, Azure-specific set of guidelines for security and compliance best practices based on common compliance frameworks.

COST MANAGEMENT

1. Cost analysis
2. Cost alerts
3. Budgets

ADVISOR RECOMMENDATIONS

Advisor is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments. It analyses your resource configuration and usage telemetry and then recommends solutions that can help you improve the cost effectiveness, performance, Reliability (formerly called High availability), and security of your Azure resources.

BILLING

1. Invoices
2. External Services
3. Payment methods
4. Partner information

SETTINGS

1. Resource groups
2. Resources
3. Preview features
4. Usage + quotas
5. Policies
6. My permissions
7. Resource providers
8. Deployments
9. Properties
10. Resource locks
11. Support + troubleshoot

AZURE REGIONS

OVERVIEW

Microsoft Azure services are available globally to drive your cloud operations at an optimal level. You can choose the best region for your needs based on technical and regulatory considerations: service capabilities, data residency, compliance requirements, and latency.

1. Regions
2. Paired Regions

RESOURCE GROUPS

OVERVIEW

Azure Resource Group is logical container (or folder) which contains different kind of resources. We can either bifurcate them on environment type level or tier based.

ACTIVITY LOG

The Activity log is a platform log in Azure that provides insight into subscription-level events. This includes such information as when a resource is modified or when a virtual machine is started. We have same tab on Subscription and all resources level. We can check activity up to last 90 days.

ACCESS CONTROL (IAM)

1. Check Access
2. Role assignments
3. Roles
4. Deny assignments

DEPLOYMENTS

You can examine specific operations in past deployments and see which resources were deployed. This history contains information about any errors. The deployment history for a resource group is limited to 800 deployments.

LOCKS

1. Read-only lock
2. Delete lock

Only Owner or User administrator can enable the lock.

MONITORING

1. Insights (preview)
2. Alerts
3. Metrics
4. Diagnostic settings
5. Logs
6. Advisor recommendations
7. Workbooks
8. Automation
9. Export template

WORKBOOKS

Workbooks provide a flexible canvas for data analysis and the creation of rich visual reports within the Azure portal. They allow you to tap into multiple data sources from across Azure and combine them into unified interactive experiences.

Benefits –

- Query data from multiple sources in Azure
- Visualize data for reporting and analysis.
- Combine multiple elements into a single interactive experience.

AZURE PRICING CALCULATOR

OVERVIEW

Azure Price Calculator is a free cost management tool that can help you estimate your cloud costs for new Azure deployments, or variations of your existing workloads.

https://azure.microsoft.com/en-in/pricing/calculator/

VIRTUAL NETWORK

OVERVIEW

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is like a traditional network that you'd operate in your own data centre but brings with its additional benefits of Azure's infrastructure such as scale, availability, and isolation.

1. Address space
2. Connected devices
3. DDoS Protection
4. Firewall
5. DNS servers

6. Connection Monitor
7. Diagram

SUBNETS

1. Subnet
2. Gateway subnet
3. Manage users

SERVICE ENDPOINTS

Virtual Network (VNet) service endpoint provides secure and direct connectivity to Azure services over an optimized route over the Azure backbone network. Endpoints allow you to secure your critical Azure service resources to only your virtual networks. Service Endpoints enables private IP addresses in the VNet to reach the endpoint of an Azure service without needing a public IP address on the VNet.

SUBNET DELEGATION

Subnet delegation enables you to designate a specific subnet for an Azure PaaS service of your choice that needs to be injected into your virtual network. Subnet delegation provides full control to the customer on managing the integration of Azure services into their virtual networks.

When you delegate a subnet to an Azure service, you allow that service to establish some basic network configuration rules for that subnet, which help the Azure service operate their instances in a stable manner. As a result, the Azure service may establish some pre- or post-deployment conditions, such as:

- deploy the service in a shared versus dedicated subnet.
- add to the service a set of Network Intent Policies post deployment that is required for the service to work properly.

Advantages of subnet delegation

Delegating a subnet to specific services provides the following advantages:

- helps to designate a subnet for one or more Azure services and manage the instances in the subnet as per requirements. For example, the virtual network owner can define the following for a delegated subnet to better manage resources and access as follows:
    - network filtering traffic policies with network security groups.
    - routing policies with user-defined routes.
    - services integration with service endpoints configurations.
- helps injected services to better integrate with the virtual network by defining their pre-conditions of deployments in the form of Network Intent Policies. This ensures any actions that can affect functioning of the injected service can be blocked at PUT.

VIRTUAL NETWORK PEERING

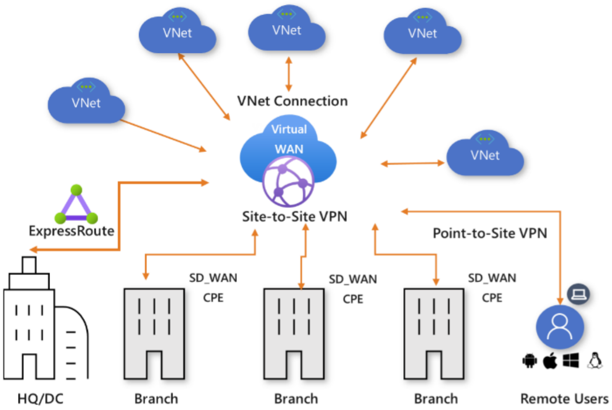
Virtual network peering allows you to establish communication between 2 different Virtual networks whether they are in same region or different, same subscription or different.

VIRTUAL NETWORK HUB

A virtual hub is a Microsoft-managed virtual network that enables connectivity from other resources. When a virtual hub is created from a Virtual WAN in the Azure portal, a virtual hub VNet and gateways (optional) are created as its components.

A secured virtual hub is an Azure Virtual WAN Hub with associated security and routing policies configured by Azure Firewall Manager. Use secured virtual hubs to easily create hub-and-spoke and transitive architectures with native security services for traffic governance and protection.

You can use a secured virtual hub to filter traffic between virtual networks (V2V), virtual networks and branch offices (B2V) and traffic to the Internet (B2I/V2I). A secured virtual hub provides automated routing. There's no need to configure your own UDRs (user defined routes) to route traffic through your firewall.



VIRTUAL MACHINE

SIZE

Type	Sizes	Description
General purpose	B, Dsv3, Dv3, Dasv4, Dav4, DSv2, Dv2, Av2, DC, DCv2, Dv4, Dsv4, Ddv4, Ddsv4, Dv5, Dsv5, Ddv5, Ddsv5, Dasv5, Dadsv5	Balanced CPU-to-memory ratio. Ideal for testing and development, small to medium databases, and low to medium traffic web servers.
Compute optimized	F, Fs, Fsv2, FX	High CPU-to-memory ratio. Good for medium traffic web servers, network appliances, batch processes, and application servers.
Memory optimized	Esv3, Ev3, Easv4, Eav4, Ev4, Esv4, Edv4, Edsv4, Ev5, Esv5, Edv5, Edsv5, Easv5, Eadsv5, Mv2, M, DSv2, Dv2	High memory-to-CPU ratio. Great for relational database servers, medium to large caches, and in-memory analytics.
Storage optimized	Lsv2	High disk throughput and IO ideal for Big Data, SQL, NoSQL databases, data warehousing and large transactional databases.
GPU	NC, NCv2, NCv3, NCasT4_v3, ND, NDv2, NV, NVv3, NVv4, NDasrA100_v4, NDm_A100_v4	Specialized virtual machines targeted for heavy graphic rendering and video editing, as well as model training and inferencing (ND) with deep learning. Available with single or multiple GPUs.
High performance compute	HB, HBv2, HBv3, HC, H	Our fastest and most powerful CPU virtual machines with optional high-throughput network interfaces (RDMA).

DISKS

Types of disks-

1. Managed disk
2. Unmanaged disk
3. Standard HDD
4. Standard SSD
5. Premium SSD
6. Ultra-disk

NETWORK INTERFACE

1. Private IP
2. Public IP
3. Dynamic IP
4. Static IP
5. Primary/Secondary IP

AVAILABILITY SETS

1. Fault Domain
2. Update Domain

AVAILABILITY ZONES

An Availability Zone is a high availability offering that protects your applications and data from datacentre failures. Availability Zones are unique physical locations within an Azure region. Each zone is made up of one or more datacentres equipped with independent power, cooling, and networking. To ensure resiliency, there's a minimum of three separate zones in all enabled regions. The physical separation of Availability Zones within a region protects applications and data from datacentre failures. Zone-redundant services replicate your applications and data across Availability Zones to protect from single-points-of-failure. With Availability Zones, Azure offers industry best 99.99% VM uptime SLA. The full Azure SLA explains the guaranteed availability of Azure as a whole.

CONNECT

1. RDP
2. Jump Server
3. Bastion

EXTENSIONS

Azure virtual machine (VM) extensions are small applications that provide post-deployment configuration and automation tasks on Azure VMs. For example, if a virtual machine requires software installation, anti-virus protection, or to run a script inside of it, a VM extension can be used.

AZURE SPOT INSTANCE

1. **Capacity only:**
   Evict virtual machine when Azure needs the capacity for pay as you go workloads. Your max price is set to the pay as you go rate.
2. **Price or capacity:**
   Choose a max price and Azure will evict your virtual machine when the cost of the instance is greater than your max price or when Azure needs the capacity for pay as you go workloads.

SUPPORT + TROUBLESHOOTING

1. Boot diagnostics
2. Reset password
3. Redeploy + reapply
4. Serial console
5. Connection troubleshoots

AZURE MARKET PLACE

OVERVIEW

The Microsoft Azure Marketplace is an online store that offers applications and services either built on or designed to integrate with Microsoft's Azure public cloud. The products and services sold through the Microsoft Azure Marketplace come from either Microsoft directly or its technology partners.

https://azure.microsoft.com/en-in/marketplace/

AZURE POLICY

OVERVIEW

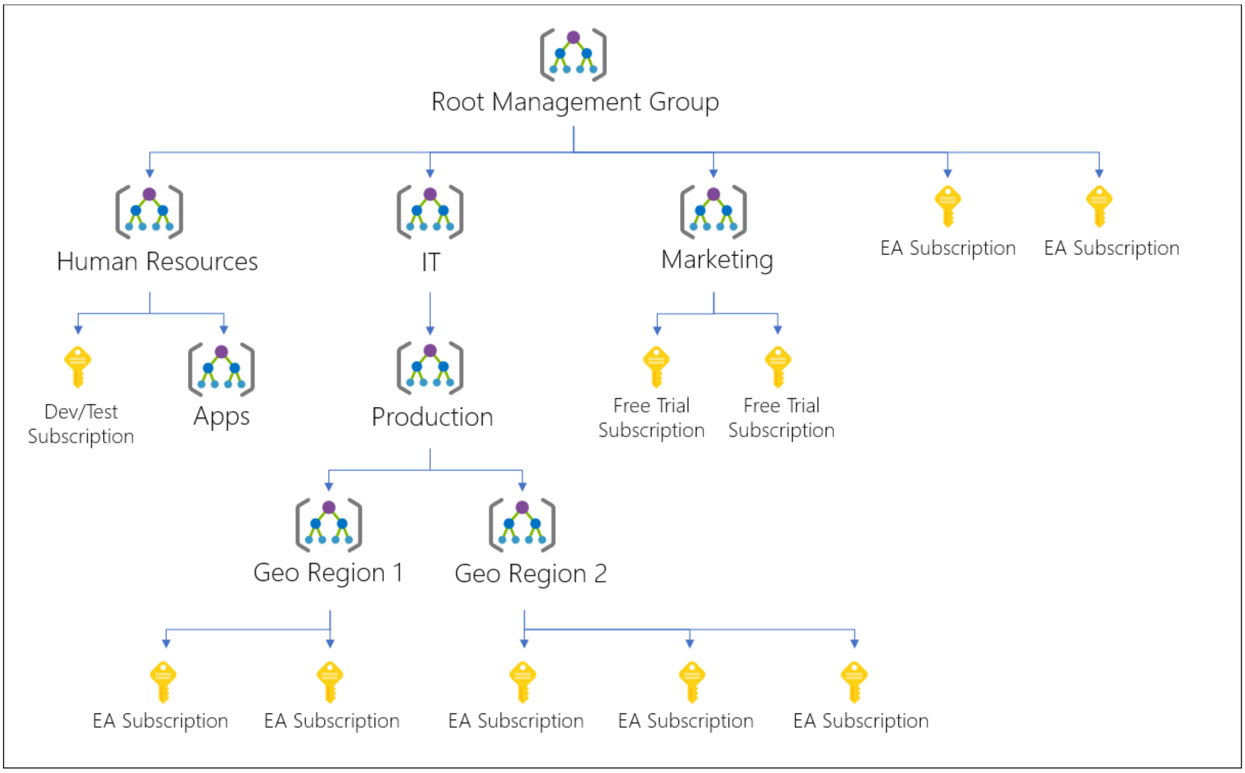
Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity. It also helps to bring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

1. Policy
2. Initiative
3. Definitions
4. Assignments
5. Exemptions

AZURE MANAGEMENT GROUPS

OVERVIEW

If your organization has many subscriptions, you may need a way to efficiently manage access, policies, and compliance for those subscriptions. Azure management groups provide a level of scope above subscriptions. You organize subscriptions into containers called "management groups" and apply your governance conditions to the management groups. All subscriptions within a management group automatically inherit the conditions applied to the management group. Management groups give you enterprise-grade management at a large scale no matter what type of subscriptions you might have. All subscriptions within a single management group must trust the same Azure Active Directory tenant.



NETWORK SECURITY GROUP

OVERVIEW

Network security group can be configured on Network Interface level or Subnet level.

RULES

1. Inbound security rules
2. Outbound security rules

APPLICATION SECURITY GROUP

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.

ROUTE TABLE

OVERVIEW

Create a route table when you need to override Azure's default routing. For example, you can route traffic to a network virtual appliance or to your on-premises network for inspection. A route table contains routes and is associated to one or more subjects.

PUBLIC DNS

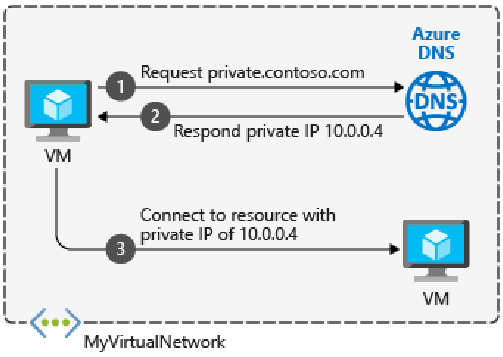
OVERVIEW

Azure DNS is a hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure. By hosting your domains in Azure, you can manage your DNS records by using the same credentials, APIs, tools, and billing as your other Azure services.

PRIVATE DNS

OVERVIEW

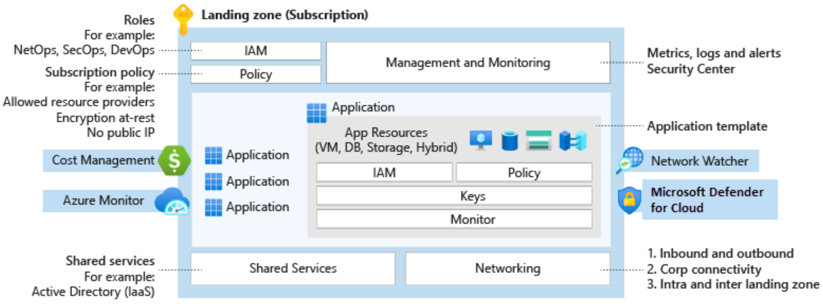
The Domain Name System, or DNS, is responsible for translating (or resolving) a service name to an IP address. Azure DNS is a hosting service for domains and provides naming resolution using the Microsoft Azure infrastructure. Azure DNS not only supports internet-facing DNS domains, but it also supports private DNS zones.


Azure DNS
1 Request private.contoso.com
DNS
2 Respond private IP 10.0.0.4
VM
3 Connect to resource with private IP of 10.0.0.4
VM
MyVirtualNetwork

AZURE LANDING ZONE

OVERVIEW

Azure landing zones are the output of a multi-subscription Azure environment that accounts for **scale, security governance, networking, and identity**. Azure landing zones enable application migration, modernization, and innovation at enterprise-scale in Azure. These zones consider all platform resources that are required to support the customer's application portfolio and don't differentiate between infrastructure as a service or platform as a service.



https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/

AZURE RESERVED INSTANCE

OVERVIEW

Azure Reservations help you save money by committing to one-year or three-year plans for multiple products. Committing allows you to get a discount on the resources you use. Reservations can significantly reduce your resource costs by up to 72% from pay-as-you-go prices. Reservations provide a billing discount and don't affect the runtime state of your resources. After you purchase a reservation, the discount automatically applies to matching resources.

AZURE VM IMAGE

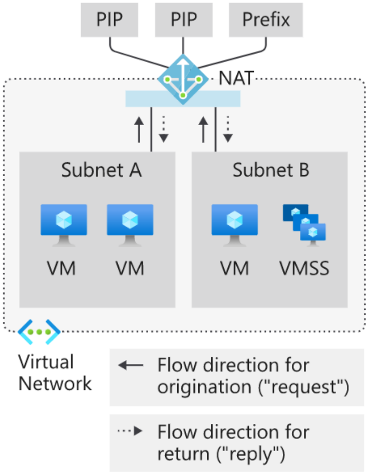
OVERVIEW

A managed image resource can be created from a generalized virtual machine (VM) that is stored as either a managed disk or an unmanaged disk in a storage account. The image can then be used to create multiple VMs. For information on how managed images are billed, see Managed Disks pricing.

NAT GATEWAY

OVERVIEW

NAT gateway provides outbound internet connectivity for one or more subnets of a virtual network. Once NAT gateway is associated to a subnet, NAT provides source network address translation (SNAT) for that subnet. NAT gateway specifies which static IP addresses virtual machines use when creating outbound flows. Static IP addresses come from public IP addresses, public IP prefixes, or both. If a public IP prefix is used, all IP addresses of the entire public IP prefix are consumed by a NAT gateway. A NAT gateway can use a total of up to 16 static IP addresses from either.



PIP
PIP
Prefix
NAT
Subnet A
Subnet B
VM
VM
VM
VMSS
Virtual Network
Flow direction for origination ("request")
Flow direction for return ("reply")

APP SERVICES

OVERVIEW

Azure App Service is an HTTP-based service for hosting web applications, REST APIs, and mobile back ends. You can develop in your favourite language, be it .NET, .NET Core, Java, Ruby, Node.js, PHP, or Python. Applications run and scale with ease on both Windows and Linux-based environments.

PUBLISH TYPE

1. Code
2. Docker Container

SETTINGS

1. App Settings
2. Custom Domains
3. SSL Settings
4. Networking
5. Scale up
6. Scale out
7. Backup
8. Identity

PRIVATE ENDPOINT

OVERVIEW

Azure Private Endpoint is a network interface that connects you privately and securely to a service powered by Azure Private Link. Private Endpoint uses a private IP address from your VNet, effectively bringing the service into your VNet. The service could be an Azure service such as Azure Storage, Azure Cosmos DB, SQL, etc. or your own Private Link Service.

KEY VAULT

OVERVIEW

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 HSM pools. Vaults support storing software and HSM-backed keys, secrets, and certificates. Managed HSM pools only support HSM-backed keys.

TYPES

1. Vault services
2. Hardware Security Module (HSM) Pool

VAULT SERVICES

1. Keys
2. Secrets
3. Certificates

CONFIGURATIONS

1. Access policies
2. Networking

VM & STORAGE ACCOUNT ENCRYPTIONS

Key vault can be used to encrypt OS and Disks of Virtual machines as well as Storage account.

AZURE MANAGED IDENTITIES

OVERVIEW

A common challenge for developers is the management of secrets and credentials used to secure communication between different components making up a solution. Managed identities eliminate the need for developers to manage credentials. Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication. Applications may use the managed identity to obtain Azure AD tokens. For example, an application may use a managed identity to access resources like Azure Key Vault where developers can store credentials in a secure manner or to access storage accounts.

Types of Azure Managed Identities:

1. System-assigned
2. User-assigned

LOAD BALANCER

OVERVIEW

An Azure load balancer is a Layer-4 (TCP, UDP) load balancer that provides high availability by distributing incoming traffic among healthy VMs. To distribute traffic to the VMs, a back-end address pool contains the IP addresses of the virtual (NICs) connected to the load balancer.

SKU

1. Basic
2. Standard

TYPE

1. Internal
2. Public

CONFIGURATIONS

1. Frontend IP Configuration
2. Backend pools
3. Health probs
4. Load balancing rules
5. Outbound rules

INBOUNT NAT RULES

An inbound NAT rule forwards incoming traffic sent to a selected IP address and port combination to a specific virtual machine.

OUTBOUND RULES

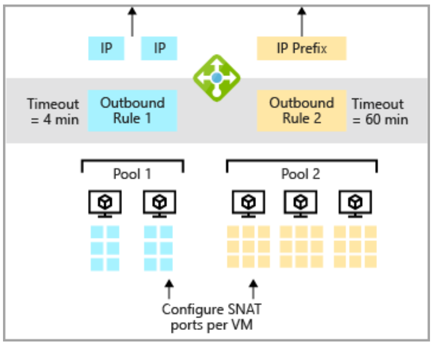
Outbound rules allow you to explicitly define SNAT(source network address translation) for a public standard load balancer. This configuration allows you to use the public IP(s) of your load balancer to provide outbound internet connectivity for your backend instances.

This configuration enables:

- IP masquerading
- Simplifying your allow lists.
- Reduces the number of public IP resources for deployment.

With outbound rules, you have full declarative control over outbound internet connectivity. Outbound rules allow you to scale and tune this ability to your specific needs.

Outbound rules will only be followed if the backend VM doesn't have an instance-level public IP address (ILPIP).



With outbound rules, you can explicitly define outbound SNAT behavior.

Outbound rules allow you to control:

- Which virtual machines are translated to which public IP addresses.
    - Two rules were backend pool A uses IP address A and B, backend pool B uses IP address C and D.
- How outbound SNAT ports are allocated.
    - Backend pool B is the only pool making outbound connections, give all SNAT ports to backend pool B and none to backend pool A.
- Which protocols to provide outbound translation for.
    - Backend pool B needs UDP ports for outbound. Backend pool A needs TCP. Give TCP ports to A and UDP ports to B.
- What duration to use for outbound connection idle timeout (4-120 minutes).
    - If there are long running connections with keepalives, reserve idle ports for long running connections for up to 120 minutes. Assume stale connections are abandoned and release ports in 4 minutes for fresh connections
- Whether to send a TCP Reset on idle timeout.
    - When timing out idle connections, do we send a TCP RST to the client and server so they know the flow is abandoned?

TCP RESET

You can use Standard Load Balancer to create a more predictable application behaviour for your scenarios by enabling TCP Reset on Idle for a given rule. Load Balancer's default behaviour is to silently drop flows when the idle timeout of a flow is reached. Enabling this feature will cause Load Balancer to send bidirectional TCP Resets (TCP RST packet) on idle timeout. This will inform your application endpoints that the connection has timed out and is no longer usable. Endpoints can immediately establish a new connection if needed.

A common practice is to use a TCP keep-alive. This practice keeps the connection active for a longer period. Keep-alive packets ensure the idle timeout value is not reached and the connection is maintained for a long period. The setting works for inbound connections only. To avoid losing the connection, configure the TCP keep-alive with an interval less than the idle timeout setting or increase the idle timeout value. To support these scenarios, support for a configurable idle timeout has been added.

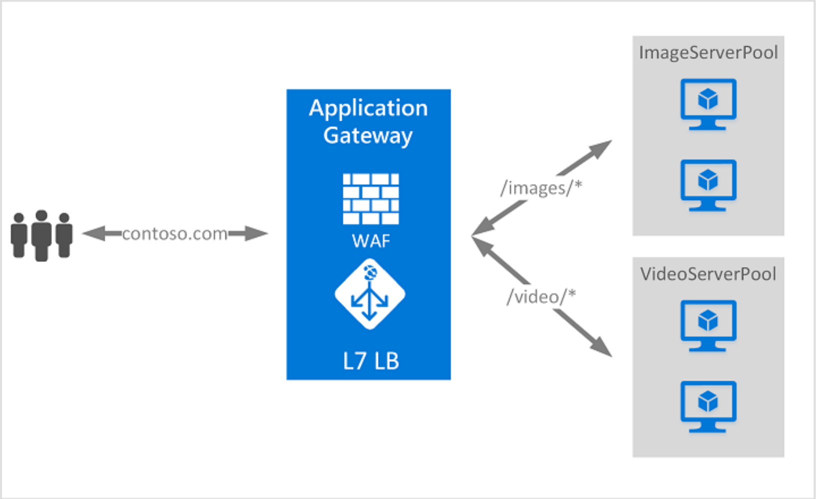
FLOATING IP

Some application scenarios prefer or require the same port to be used by multiple application instances on a single VM in the backend pool. Common examples of port reuse include clustering for high availability, network virtual appliances, and exposing multiple TLS endpoints without re-encryption. If you want to reuse the backend port across multiple rules, you must enable Floating IP in the rule definition.

APPLICATION GATEWAY

OVERVIEW

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 is 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.



TRAFFIC MANAGER

OVERVIEW

Azure Traffic Manager is a DNS-based traffic load balancer. This service allows you to distribute traffic to your public facing applications across the global Azure regions. Traffic Manager also provides your public endpoints with high availability and quick responsiveness.

ROUTING METHODS

1. **Priority:** Select **Priority** routing when you want to have a primary service endpoint for all traffic. You can provide multiple backup endpoints in case the primary or one of the backup endpoints is unavailable.

2. **Weighted:** Select **Weighted** routing when you want to distribute traffic across a set of endpoints based on their weight. Set the weight the same to distribute evenly across all endpoints.

3. **Performance:** Select **Performance** routing when you have endpoints in different geographic locations and you want end users to use the "closest" endpoint for the lowest network latency.

4. **Geographic:** Select **Geographic** routing to direct users to specific endpoints (Azure, External, or Nested) based on where their DNS queries originate from geographically. With this routing method, it enables you to be in compliance with scenarios such as data sovereignty mandates, localization of content & user experience and measuring traffic from different regions.

5. **Multivalue:** Select **MultiValue** for Traffic Manager profiles that can only have IPv4/IPv6 addresses as endpoints. When a query is received for this profile, all healthy endpoints are returned.

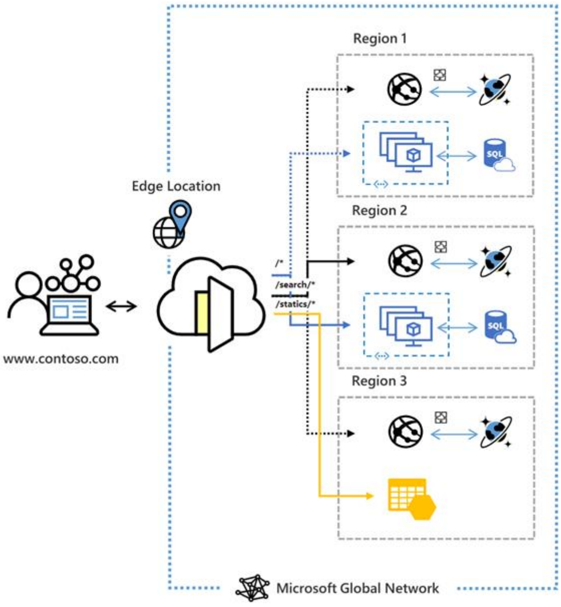
6. **Subnet:** Select **Subnet** traffic-routing method to map sets of end-user IP address ranges to a specific endpoint. When a request is received, the endpoint returned will be the one mapped for that request’s source IP address.

https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods

AZURE FRONT DOOR

OVERVIEW

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.



VIRTUAL MACHINE SCALE SET

OVERVIEW

Azure virtual machine scale sets let you create and manage a group of load balanced VMs. The number of VM instances can automatically increase or decrease in response to demand or a defined schedule. Scale sets provide high availability to your applications, and allow you to centrally manage, configure, and update a large number of VMs. With virtual machine scale sets, you can build large-scale services for areas such as compute, big data, and container workloads.

SCALING POLICY

1. Manual
2. Custom

CONFIGURATIONS

1. **Overprovisioning:**
   With overprovisioning turned on, the scale set actually spins up more VMs than you asked for, then deletes the extra VMs once the requested number of VMs are successfully provisioned. Overprovisioning improves provisioning success rates and reduces deployment time. You are not billed for the extra VMs, and they do not count toward your quota limits.
2. **Instance termination:**
   Opt-in to receive instance termination notifications through the Azure Metadata Service and set a pre-defined delay timeout to the terminate operation.
3. **Application health monitoring:**
   The Application Health extension will probe the application health endpoint and update the status of the application. When the health endpoint is not set up correctly the status of the application will be reported as unhealthy
   a. Enable automatic repairs: Delete unhealthy instances automatically and create new ones with the latest instance model settings.
4. **Spreading Algorithm:**

The spreading algorithm determines how VMs in the scale set are balanced across fault domains. With max spreading, VMs are spread across as many fault domains as possible in each zone. With fixed spreading, VMs are always spread across exactly 5 fault domains. In the case where fewer than 5 fault domains are available, a scale set using "Max spreading" will still complete deployment, while a scale set using "Fixed spreading" will fail to deploy.

AZURE MONITORING

OVERVIEW

Azure Monitor helps you maximize the availability and performance of your applications and services. It delivers a comprehensive solution for collecting, analysing, 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.

INSIGHTS

1. Azure Monitor
2. VM Insight
3. Application Insights
4. Container Insights

VISUALIZE

1. Dashboards
2. Views
3. Workbooks

ANALYZE

1. Metric Analytics
2. Log Analytics Workspace

RESPOND

1. Alerts
2. Actions Groups

STORAGE ACCOUNT

OVERVIEW

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

SKU

1. Standard
2. Premium
    a. **Block blobs:** Best for high transaction rates or low storage latency.
    b. **File shares:** Best for enterprise or high-performance applications that need to scale.
    c. **Page blobs:** Best for random read and write operations.

REDUNDANCY

1. **Locally redundant storage (LRS):** 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.
2. **Zone-redundant storage (ZRS):** 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.
3. **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 the secondary region. Within the secondary region, your data is copied synchronously three times using LRS.
4. **Geo-zone-redundant storage (GZRS):** Copies your data synchronously across three Azure availability zones in the primary region using ZRS. It then copies your data asynchronously to a single physical location in the secondary region. Within the secondary region, your data is copied synchronously three times using LRS.

https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy

SERVICES

1. Blob service
    a. Container
        i. Public access level
        ii. Blobs
        iii. Blob type-page, block & append
        iv. Hot, Cool & Archive tier
        v. Blob versioning
        vi. Snapshot
        vii. Lease
    b. Custom domain
    c. Data protection
    d. Object replication
    e. Azure CDN
    f. Add Azure Search
    g. Lifecycle Management
    h. Blob inventory
2. File service
3. Table service
4. Queue service

AZURE STORAGE EXPLORER

Azure Storage Explorer is an application that helps you to easily access the Azure storage account through any device on any platform, be it Windows, MacOS, or Linux. You can easily connect to your subscription and manipulate your tables, blobs, queues, and files.

AZCOPY

AzCopy is a command-line utility that you can use to copy blobs or files to or from a storage account. This article helps you download AzCopy, connect to your storage account, and then transfer files.

CONFIGURATIONS

1. Access keys
2. Shared access signature (SAS)
3. Encryption
4. Networking

5. Geo-replication

RECOVERY SERVICE VAULTS

OVERVIEW

Azure recovery services vault can be used to take VM backup or replicate them to different region for HA/DR. We can also use Recovery vault to take backup of on-premises servers.

BACKUP

1. Workload running
    a. Azure
    b. Azure Stack
    c. On-Premises
2. Type of backup
    a. Virtual machine
    b. Azure File Share
    c. SQL Server in Azure VM
    d. SAP HANA in Azure VM
3. Backup items
4. Backup policies
5. Backup reports
6. Backup jobs
7. Backup alerts
8. Restore VM
    a. File recovery
    b. New VM restore
    c. Replace existing VM
    d. Restore encrypted VM
9. Geo-redundant backup

REPLICATION

1. Site Recovery
    a. Azure virtual machines
    b. VMware machines to Azure
    c. Hyper-V machines to Azure
2. Replicated items
    a. Planned Failover
    b. Failover
    c. Test Failover
    d. Clean up test failover
    e. Commit
    f. Resynchronization
    g. Change recovery point
    h. Complete migration
    i. Reverse replication
    j. Disable replication
    k. Compute and Network
    l. Disks
    m. Encrypted VM replication
3. Site Recovery infrastructure
    a. Network mapping
    b. Replication policies

    c. Extension updates settings
4. Recovery Plans
5. Site Recovery jobs
6. Site Recovery events

CONFIGURATIONS

1. Backup configuration
    a. LRS & GRS
    b. Cross Region Restore
2. Encryption settings
3. Security settings
4. Security PIN
5. Recovery service agent
6. Backup credentials

AZURE SQL SERVICES

OVERVIEW

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.

TYPE

1. Azure SQL Services (DTU vs Core Based)
2. SQL Managed Instance
3. SQL on Virtual Machine

SETTINGS

1. Configuration
2. Geo Replications
3. Connection strings
4. Sync to other databases
5. Advanced threat protections

AZURE MIGRATE

OVERVIEW

Azure Migrate provides a centralized hub to assess and migrate to Azure on-premises servers, infrastructure, applications, and data. It provides the following:

- **Unified migration platform**: A single portal to start, run, and track your migration to Azure.

- **Range of tools**: A range of tools for assessment and migration. Azure Migrate tools include Azure Migrate: Discovery and assessment and Azure Migrate: Server Migration. Azure Migrate also integrates with other Azure services and tools, and with independent software vendor (ISV) offerings.

https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/

https://azure.microsoft.com/en-in/migration/migration-journey/#how-to-migrate

WINDOWS, LINUX, AND SQL SERVER (VM MIGRATION)

Assess on-premises servers including SQL Server instances and migrate them to Azure virtual machines or Azure VMware Solution (AVS) (Preview).

DATABASES MIGRATION

Assess on-premises databases and migrate them to Azure SQL Database or to SQL Managed Instance.

WEB APPLICATIONS MIGRATION

Assess on-premises web applications and migrate them to Azure App Service by using the Azure App Service Migration Assistant.

VIRTUAL DESKTOP MIGRATION

Assess your on-premises virtual desktop infrastructure (VDI) and migrate it to Windows Virtual Desktop in Azure.

DATA MIGRATION

Migrate large amounts of data to Azure quickly and cost-effectively using Azure Data Box products.

AZURE FIREWALL

OVERVIEW

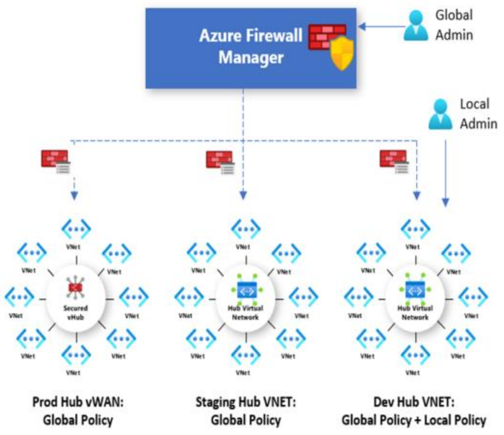
Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It's a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.

TIER

1. Standard
2. Premium

FIREWALL MANAGEMENT

1. Firewall Policy


Azure Firewall Manager
Global Admin
Local Admin
VNet
Secured vHub
Hub Virtual Network
Hub Virtual Network
Prod Hub vWAN: Global Policy
Staging Hub VNET: Global Policy
Dev Hub VNET: Global Policy + Local Policy

2. Firewall Rules

FORCED TUNNELING

When you configure a new Azure Firewall, you can route all Internet-bound traffic to a designated next hop instead of going directly to the Internet. For example, you may have an on-premises edge firewall or other network virtual appliance (NVA) to process network traffic before it's passed to the Internet.

RULES

1. NAT rule collection
2. Network rule collection
3. Application rule collection

THREAT INTELLIGENCE

Threat intelligence-based filtering can be enabled for your firewall to alert and block traffic to/from known malicious IP addresses and domains. The IP addresses and domains are sourced from the Microsoft Threat Intelligence feed, and only highest confidence records are included.

VIRTUAL PRIVATE NETWORK (VPN)

OVERVIEW

Azure VPN Gateway connects your on-premises networks to **Azure** through Site-to-Site **VPNs** in a similar way that you set up and connect to a remote branch office. The connectivity is secure and uses the industry-standard protocols Internet Protocol Security (IPsec) and Internet Key Exchange (IKE).

POINT-TO-SITE VPN

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. This article applies to the Resource Manager deployment model.

SITE-TO-SITE VPN

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.

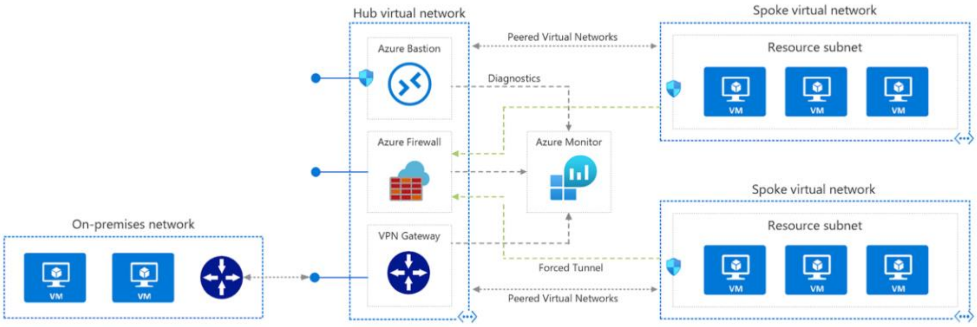
AZURE EXPRESS ROUTE

Use Azure ExpressRoute to create private connections between Azure datacentres and infrastructure on your premises or in a colocation environment. ExpressRoute connections don't go over the public Internet and they offer more reliability, faster speeds and lower latencies than typical Internet connections.

HUB & SPOKE NETWORK TOPOLOGY

OVERVIEW

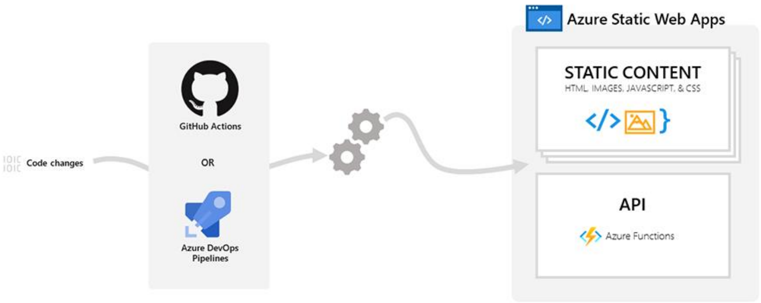
This reference architecture details a hub-spoke topology in Azure. The hub virtual network acts as a central point of connectivity to many spoke virtual networks. The hub can also be used as the connectivity point to your on-premises networks. The spoke virtual networks peer with the hub and can be used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



STATIC WEB APPS

OVERVIEW

Azure Static Web Apps is a service that automatically builds and deploys full stack web apps to Azure from a code repository.



AZURE POWERSHELL (BASIC)

OVERVIEW

Azure PowerShell is a set of cmdlets for managing Azure resources directly from the PowerShell command line. Azure PowerShell is designed to make it easy to learn and get started with, but provides powerful features for automation.

AUTOMATION ACCOUNT

OVERVIEW

Azure Automation delivers a cloud-based automation and configuration service that supports consistent management across your Azure and non-Azure environments. It comprises process automation, configuration management, update management, shared capabilities, and heterogeneous features. Automation gives you complete control during deployment, operations, and decommissioning of workloads and resources.

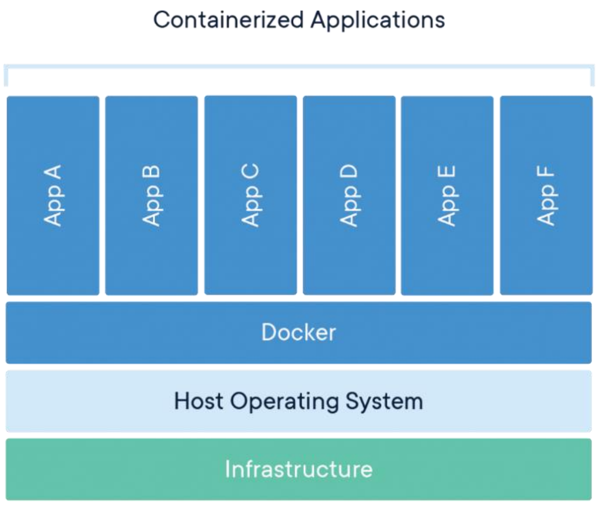
TYPES OF AUTOMATION

1. Process Automation (Automation Runbook)
2. Configuration Management
3. Update Management

CONTAINERIZATION

OVERVIEW

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.



AZURE CONTAINER REGISTRY

OVERVIEW

The Azure container registry is Microsoft's own hosting platform for Docker images. It is a private registry where you can store and manage private docker container images and other related artifacts. These images can then be pulled and run locally or used for container-based deployments to host platforms.

Use Azure container registries with your existing container development and deployment pipelines, or use Azure Container Registry Tasks to build container images in Azure. Build on demand, or fully automate builds with triggers such as source code commits and base image updates.

Managed container registries - Azure Container Registry | Microsoft Docs

AZURE CONTAINER INSTANCE

OVERVIEW

Containers are becoming the preferred way to package, deploy, and manage cloud applications. Azure Container Instances offers the fastest and simplest way to run a container in Azure, without having to manage any virtual machines and without having to adopt a higher-level service.

Azure Container Instances is a great solution for any scenario that can operate in isolated containers, including simple applications, task automation, and build jobs. For scenarios where you need full container orchestration, including service discovery across multiple containers, automatic scaling, and coordinated application upgrades, we recommend Azure Kubernetes Service (AKS).

Serverless containers in Azure - Azure Container Instances | Microsoft Docs

AZURE KUBERNETES SERVICES (OVERVIEW)

OVERVIEW

Azure Kubernetes Service (AKS) simplifies deploying a managed Kubernetes cluster in Azure by offloading the operational overhead to Azure. As a hosted Kubernetes service, Azure handles critical tasks, like health monitoring and maintenance. Since Kubernetes masters are managed by Azure, you only manage and maintain the agent nodes. Thus, AKS is free; you only pay for the agent nodes within your clusters, not for the masters.

Introduction to Azure Kubernetes Service - Azure Kubernetes Service | Microsoft Docs

AZURE COSMOS DB (OVERVIEW)

OVERVIEW

Today's applications are required to be highly responsive and always online. To achieve low latency and high availability, instances of these applications need to be deployed in datacentres that are close to their users. Applications need to respond in real time to large changes in usage at peak hours, store ever increasing volumes of data, and make this data available to users in milliseconds.

Benefits:

1. Guaranteed speed at any scale.
2. Simplified application development.
3. Mission-critical ready.
4. Fully managed and cost-effective.
5. Multi-write support.

https://docs.microsoft.com/en-us/azure/cosmos-db/introduction

API:

1. Core (SQL) API
2. MongoDB
3. Cassandra
4. Gremlin
5. Table

https://docs.microsoft.com/en-us/azure/cosmos-db/choose-api

FUNCTIONS (OVERVIEW)

OVERVIEW

Azure Functions is a serverless solution that allows you to write less code, maintain less infrastructure, and save on costs. Instead of worrying about deploying and maintaining servers, the cloud infrastructure provides all the up-to-date resources needed to keep your applications running.

COMPARE AZURE FUNCTIONS AND AZURE LOGIC APPS

Functions and Logic Apps are Azure services that enable serverless workloads. Azure Functions is a serverless compute service, whereas Azure Logic Apps provides serverless workflows. Both can create complex *orchestrations*. An orchestration is a collection of functions or steps, called *actions* in Logic Apps, that are executed to accomplish a complex task. For example, to process a batch of orders, you might execute many instances of a function in parallel, wait for all instances to finish, and then execute a function that computes a result on the aggregate.

https://docs.microsoft.com/en-in/azure/azure-functions/functions-compare-logic-apps-ms-flow-webjobs

TERRAFORM (BASIC) – BONUS

OVERVIEW

HashiCorp Terraform is an open-source tool for provisioning and managing cloud infrastructure. It codifies infrastructure in configuration files that describe the topology of cloud resources. These resources include virtual machines, storage accounts, and networking interfaces. The Terraform CLI provides a simple mechanism to deploy and version the configuration files to Azure.

Using Terraform with Azure | Microsoft Docs

AZURE DEVOPS CI/CD (BASIC) – BONUS

OVERVIEW

Azure DevOps provides developer services for support teams to plan work, collaborate on code development, and build and deploy applications. Azure DevOps supports a culture and set of processes that bring developers and project managers and contributors together to complete software development. It allows organizations to create and improve products at a faster pace than they can with traditional software development approaches.

Plan, code, collaborate, ship applications - Azure DevOps | Microsoft Docs

RESUME & INTERVIEW PREPARATION

OVERVIEW

In this section we are going to build resume and prepare for interview.

EXAM TIPS AND TRICKS

OVERVIEW

In this section we will go through steps to schedule the exam along with tips and tricks to clear it.

COURSE COMPLETED