2022

Exam AZ-305: Azure Solutions Architect Expert Certification Short Notes

EXAM PREP

AKSHAY TONDAK

Notes:

Single sign-on (SSO) allows your users to access an application without authenticating multiple times. It allows the single authentication to occur in the cloud, against Azure Active Directory, and allows the service or Connector to impersonate the user to complete any additional authentication challenges from the application.

How to configure single sign on?

To configure SSO, first make sure that your application is configured for Pre-Authentication through Azure Active Directory. To do this configuration, go to **Azure Active Directory** -> **Enterprise Applications** -> **All Applications** -> Your application **-> Application Proxy**. On this page, you see the "Pre-Authentication" field, and make sure that is set to "Azure Active Directory.

What are 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.

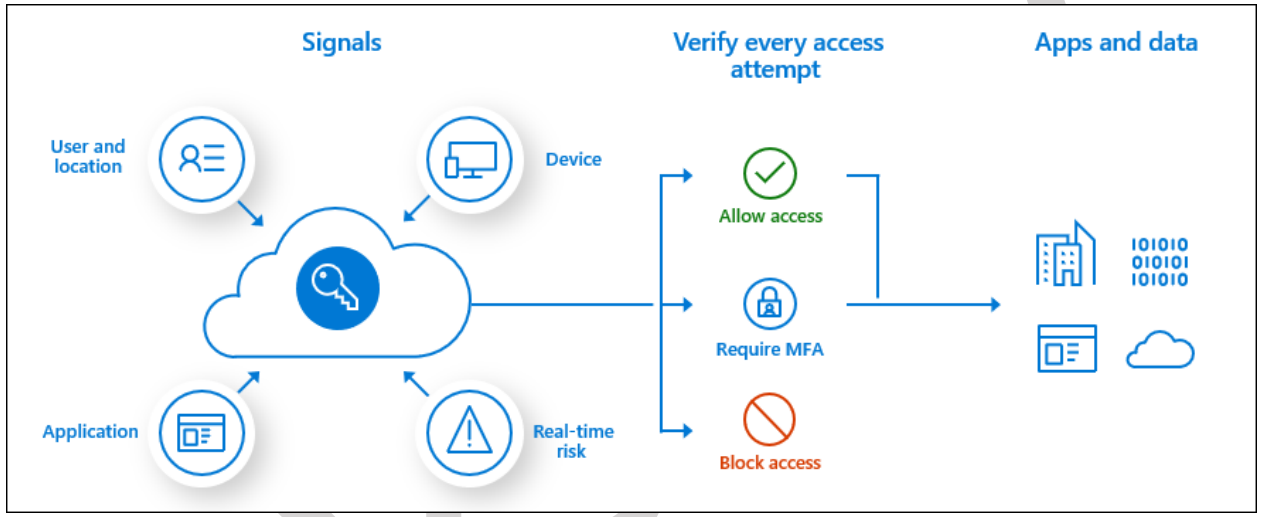
What is Conditional Access?

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

Administrators are faced with two primary goals:

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

Use Conditional Access policies to apply the right access controls when needed to keep your organization secure.



Source: Microsoft

Application management

If you develop your own business application, you can register it with Azure AD to take advantage of the security features that the tenant provides. You can register your application in App Registrations, or you can register it using the Create your own application link when adding a new application in Enterprise applications. Consider how authentication is implemented in your application for integration with Azure AD.

Access Azure Data Lake Storage

When you enable Azure Data Lake Storage credential passthrough for your cluster, commands that you run on that cluster can read and write data in Azure Data Lake Storage without requiring you to configure service principal credentials for access to storage.

High concurrency clusters can be shared by multiple users. They support only Python and SQL with Azure Data Lake Storage credential passthrough.

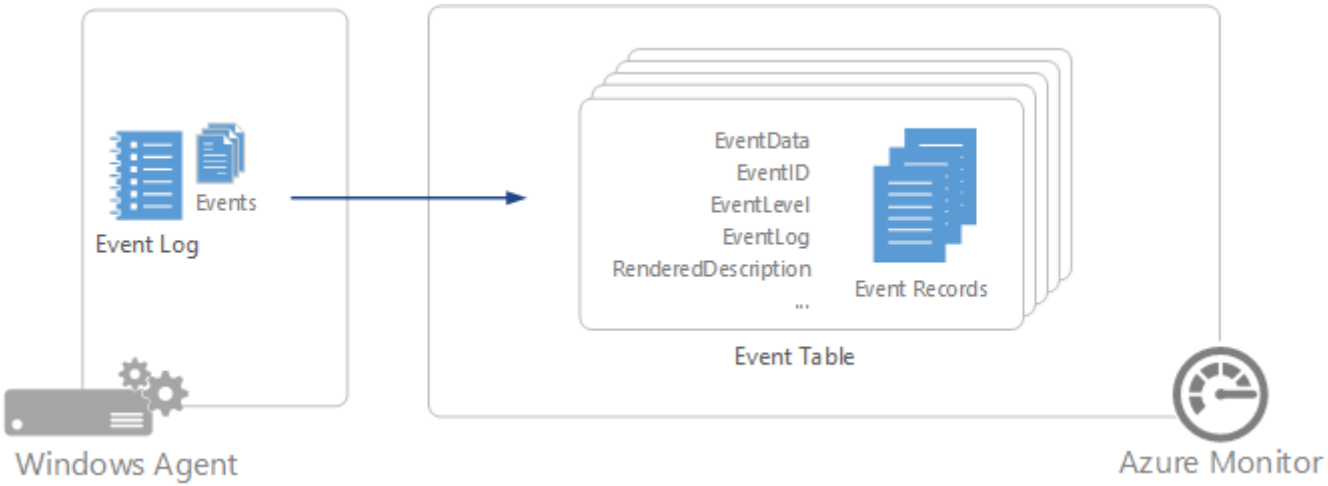
IP flow verify

IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen, IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.

An instance of Network Watcher needs to be created in all regions that you plan to run IP flow verify. Network Watcher is a regional service and can only be ran against resources in the same region. The instance used does not affect the results of IP flow verify, as any route associated with the NIC or subnet is still be returned.

Collect Windows event log data sources

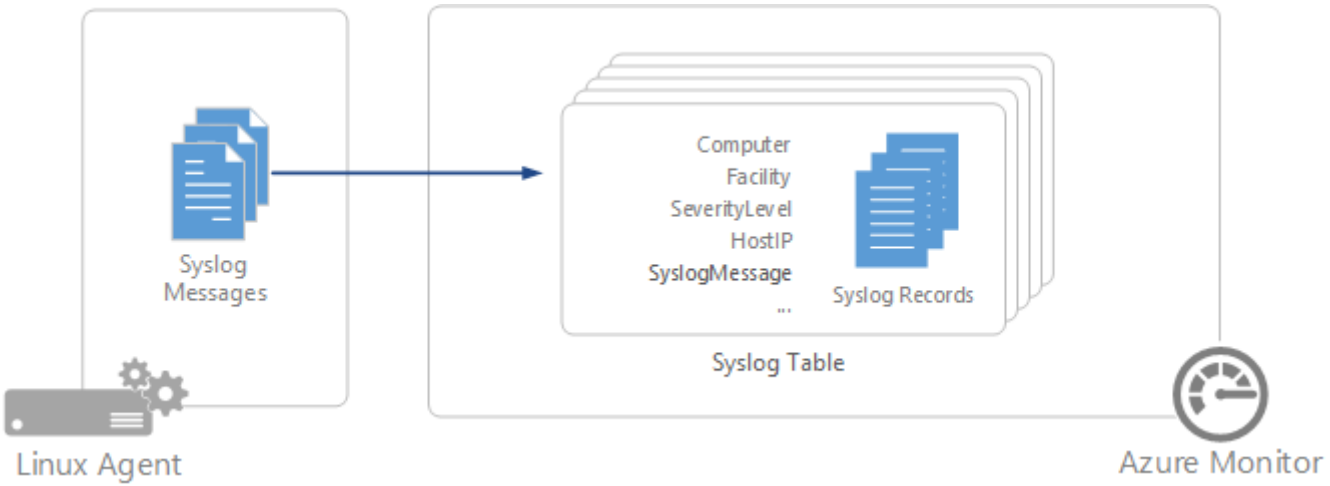
Windows Event logs are one of the most common data sources for Log Analytics agents on Windows virtual machines since many applications write to the Windows event log. You can collect events from standard logs such as System and Application in addition to specifying any custom logs created by applications you need to monitor.



Source: Microsoft

Collect Syslog data sources

Syslog is an event logging protocol that is common to Linux. Applications will send messages that may be stored on the local machine or delivered to a Syslog collector. When the Log Analytics agent for Linux is installed, it configures the local Syslog daemon to forward messages to the agent. The agent then sends the message to Azure Monitor where a corresponding record is created.



Source: Microsoft

Azure Policy

Azure Policy uses a JSON format to form the logic the evaluation uses to determine whether a resource is compliant or not. Definitions include metadata and the policy rule. The defined rule can use functions, parameters, logical operators, conditions, and property aliases to match exactly the scenario you want. The policy rule determines which resources in the scope of the assignment get evaluated.

An assignment is a policy definition or initiative that has been assigned to take place within a specific scope. This scope could range from a management group to an individual resource. The term scope refers to all the resources, resource groups, subscriptions, or management groups that the definition is assigned to. Assignments are inherited by all child resources. This design means that a definition applied to a resource group is also applied to resources in that resource group.

Azure AD Application Proxy

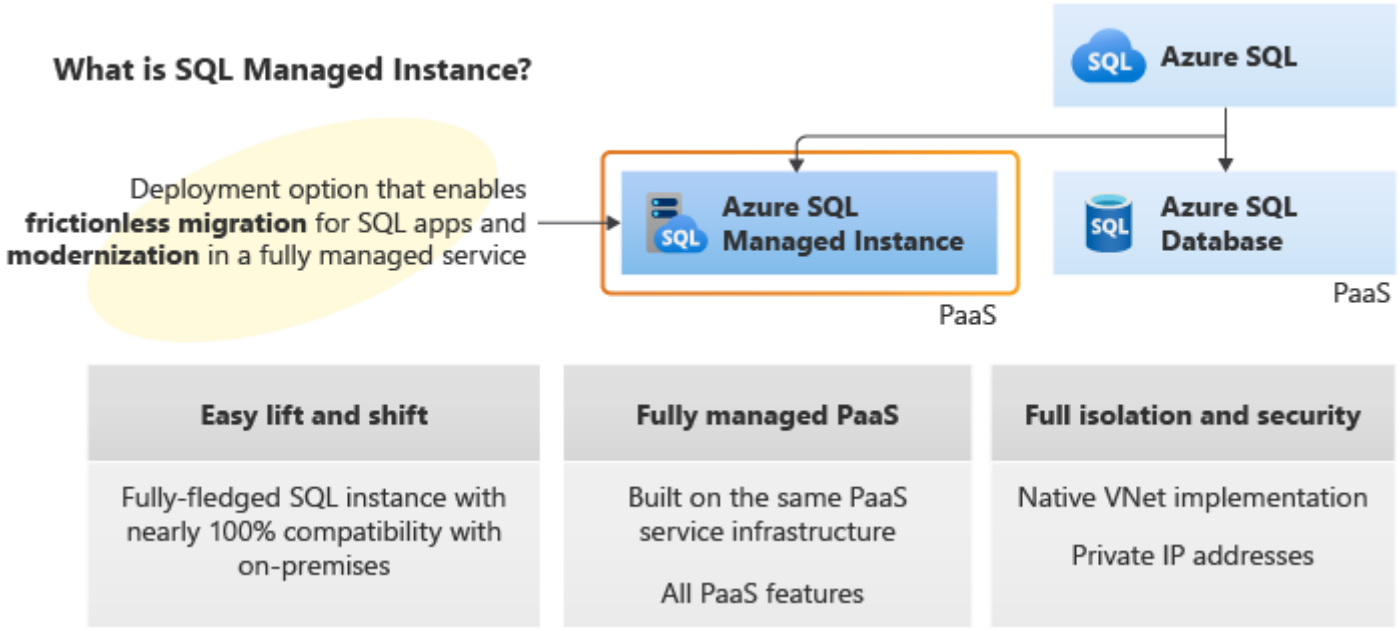
Azure Active Directory's Application Proxy provides secure remote access to on-premises web applications. After a single sign-on to Azure AD, users can access both cloud and on-premises applications through an external URL or an internal application portal. For example, Application Proxy can provide remote access and single sign-on to Remote Desktop, SharePoint, Teams, Tableau, Qlik, and line of business (LOB) applications.

Azure 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. You can view the Activity log in the Azure portal or retrieve entries with PowerShell and CLI.

Azure SQL Managed Instance

SQL Managed Instance allows existing SQL Server customers to lift and shift their on-premises applications to the cloud with minimal application and database changes. At the same time, SQL Managed Instance preserves all PaaS capabilities (automatic patching and version updates, automated backups, high availability) that drastically reduce management overhead and TCO.



Source: Microsoft

Azure Import/Export service

Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter. This service can also be used to transfer data from Azure Blob storage to disk drives and ship to your on-premises sites. Data from one or more disk drives can be imported either to Azure Blob storage or Azure Files.

Supply your own disk drives and transfer data with the Azure Import/Export service. You can also use disk drives supplied by Microsoft.

[Akshay Tondak | LinkedIn]

Azure Service Bus

Azure Service Bus supports a set of cloud-based, message-oriented middleware technologies including reliable message queuing and durable publish/subscribe messaging.

A queue allows processing of a message by a single consumer. In contrast to queues, topics and subscriptions provide a one-to-many form of communication in a publish and subscribe pattern. It's useful for scaling to large numbers of recipients.

Data Lifecycle

Lifecycle management policies are supported for block blobs and append blobs in general-purpose v2, premium block blob, and Blob Storage accounts. Lifecycle management does not affect system containers such as the $logs or $web containers.

Real-time analytics

Time series data is often very high volume, especially in IoT scenarios. Storing, indexing, querying, analysing, and visualizing time series data can be challenging.

Time Series Insights performs the roles of stream processing, data store, and analytics and reporting. It accepts streaming data from either IoT Hub or Event Hubs and stores, processes, analyses, and displays the data in near real time. It does not pre-aggregate the data but stores the raw events.

Auditing limitations

- Premium storage is currently not supported.
- Hierarchical namespace for Azure Data Lake Storage Gen2 storage account is currently not supported.
- Enabling auditing on a paused Azure Synapse is not supported. To enable auditing, resume Azure Synapse.
- Auditing for Azure Synapse SQL pools supports default audit action groups only.

Azure Recovery Services

Site Recovery helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. When an outage occurs at your primary site, you fail over to secondary location, and access apps from there. After the primary location is running again, you can fail back to it.

The Azure Backup service keeps your data safe and recoverable.

What is Traffic Manager?

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.

Traffic Manager uses DNS to direct the client requests to the appropriate service endpoint based on a traffic-routing method. Traffic manager also provides health monitoring for every endpoint. The endpoint can be any Internet-facing service hosted inside or outside of Azure. Traffic Manager provides a range of traffic-routing methods and endpoint monitoring options to suit different application needs and automatic failover models. Traffic Manager is resilient to failure, including the failure of an entire Azure region.

Storage tiers

Azure Files offers four different tiers of storage, premium, transaction optimized, hot, and cool to allow you to tailor your shares to the performance and price requirements of your scenario:

Premium: Premium file shares are backed by solid-state drives (SSDs) and provide consistent high performance and low latency, within single-digit milliseconds for most IO operations, for IO-intensive workloads. Premium file shares are suitable for a wide

variety of workloads like databases, web site hosting, and development environments. Premium file shares can be used with both Server Message Block (SMB) and Network File System (NFS) protocols.

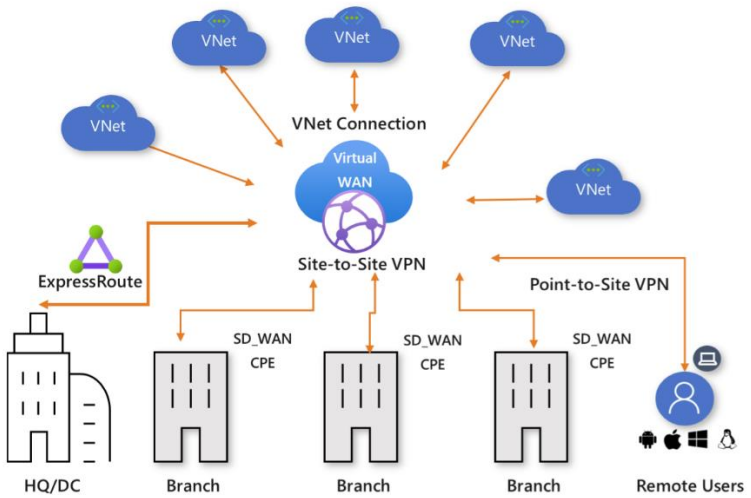
Transaction optimized: Transaction optimized file shares enable transaction heavy workloads that don't need the latency offered by premium file shares. Transaction optimized file shares are offered on the standard storage hardware backed by hard disk drives (HDDs). Transaction optimized has historically been called "standard", however this refers to the storage media type rather than the tier itself (the hot and cool are also "standard" tiers, because they are on standard storage hardware).

Hot: Hot file shares offer storage optimized for general purpose file sharing scenarios such as team shares. Hot file shares are offered on the standard storage hardware backed by HDDs.

Cool: Cool file shares offer cost-efficient storage optimized for online archive storage scenarios. Cool file shares are offered on the standard storage hardware backed by HDDs.

What is Azure Virtual WAN?

Azure Virtual WAN is a networking service that brings many networking, security, and routing functionalities together to provide a single operational interface.



Source: Microsoft

There are two types of virtual WANs: Basic and Standard. The following table shows the available configurations for each type.

BASIC AND STANDARD VIRTUAL WANS

Virtual WAN type	Hub type	Available configurations
Basic	Basic	Site-to-site VPN only
Standard	Standard	ExpressRoute
		User VPN (P2S)
		VPN (site-to-site)
		Inter-hub and VNet-to-VNet transiting through the virtual hub
		Azure Firewall
		NVA in a virtual WAN

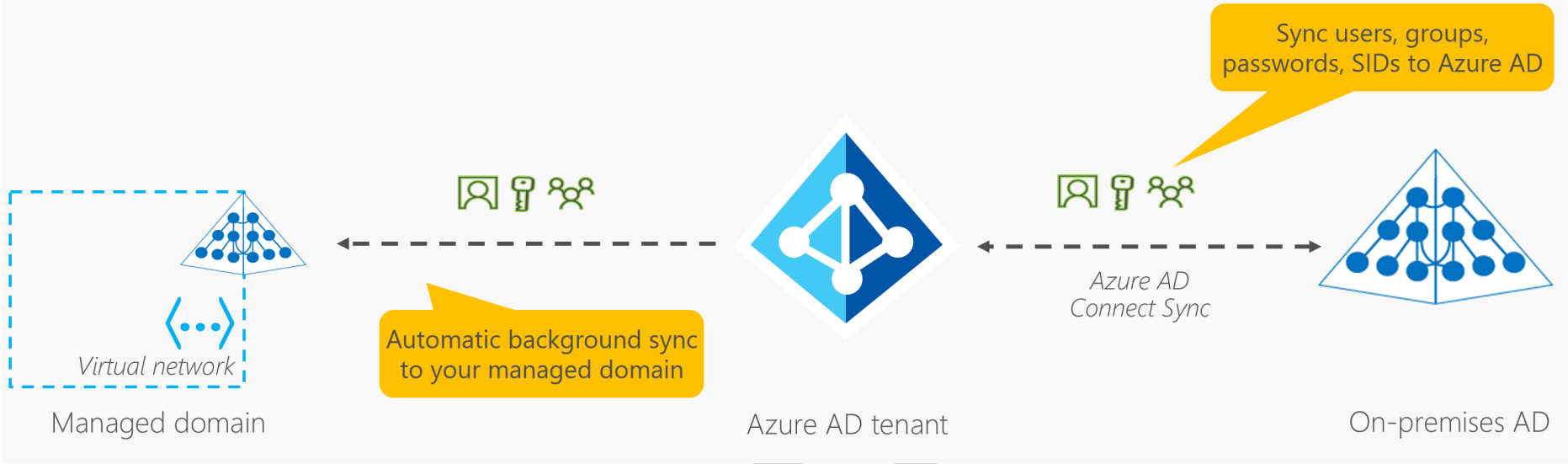
Create and run your own code from workflows

When you want to run code that performs a specific job in your logic app workflow, you can create a function by using Azure Functions. This service helps you create Node.js, C#, and F# functions so you don't have to build a complete app or infrastructure to run code. You can also call logic app workflows from inside an Azure function. Azure Functions provides serverless computing in the cloud and is useful for performing certain tasks.

What is Azure Active Directory Domain Services?

Azure Active Directory Domain Services (Azure 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.



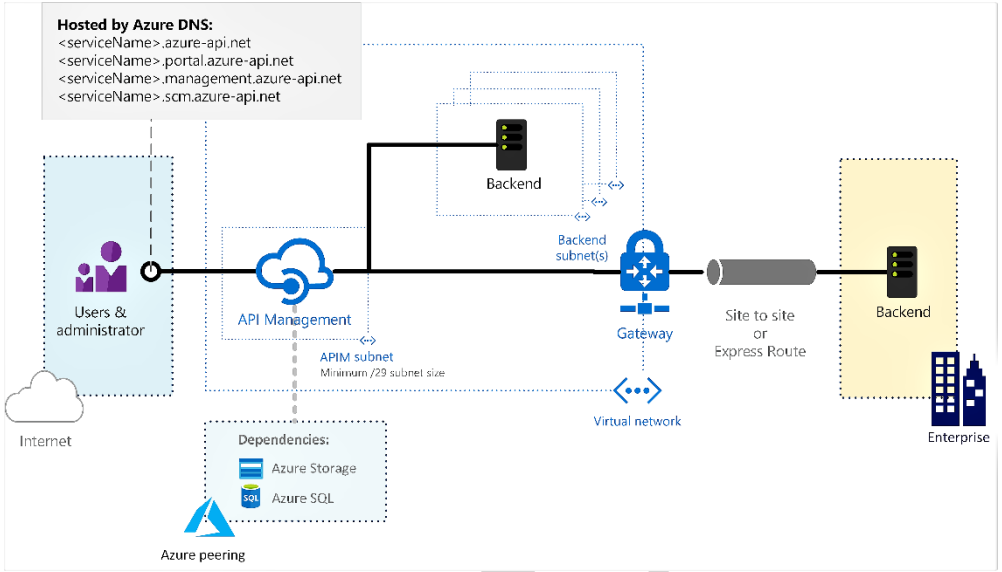
Source: Microsoft

Azure File Sync

Use Azure File Sync to centralize your organization's file shares in Azure Files, while keeping the flexibility, performance, and compatibility of an on-premises file server. Azure File Sync transforms Windows Server into a quick cache of your Azure file share. You can use any protocol that's available on Windows Server to access your data locally, including SMB, NFS, and FTPS. You can have as many caches as you need across the world.

Connect to a virtual network using Azure API Management

Azure API Management can be deployed inside an Azure virtual network (VNet) to access backend services within the network.

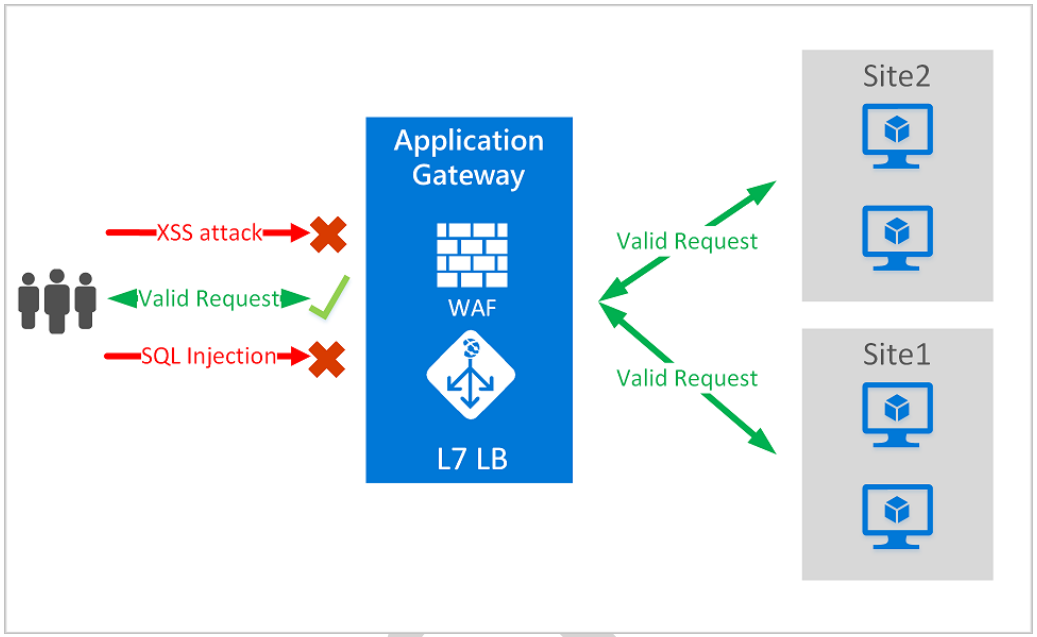


Source: Microsoft

What is Azure Web Application Firewall?

Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. SQL injection and cross-site scripting are among the most common attacks.

WAF can be deployed with Azure Application Gateway, Azure Front Door, and Azure Content Delivery Network (CDN) service from Microsoft.



Source: Microsoft

API Management

Azure API Management is a hybrid, multi-cloud management platform for APIs across all environments. Azure API Management is made up of an API gateway, a management plane, and a developer portal.

Microservices are perfect for building APIs. With Azure Kubernetes Service (AKS), you can quickly deploy and operate a microservices-based architecture in the cloud. You can then leverage Azure API Management (API Management) to publish your microservices as APIs for internal and external consumption.

App Service Environment

The Azure App Service Environment is an Azure App Service feature that provides a fully isolated and dedicated environment for securely running App Service apps at high scale. This capability can host your:

- Windows web apps
- Linux web apps
- Docker containers (Windows and Linux)
- Functions
- Logic Apps (Standard)

Azure Firewall Policy

A global Azure Firewall policy to govern the security posture across the global network environment, and then assign it to all Azure Firewall instances. This allows for granular policies to meet the requirements of specific regions, by delegating incremental Azure Firewall policies to local security teams, via RBAC.

Azure Migrate

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

What is Azure CycleCloud?

Azure CycleCloud is an enterprise-friendly tool for orchestrating and managing High Performance Computing (HPC) environments on Azure. With CycleCloud, users can provision infrastructure for HPC systems, deploy familiar HPC schedulers, and automatically scale the infrastructure to run jobs efficiently at any scale. Through CycleCloud, users can create different types of file systems and mount them to the compute cluster nodes to support HPC workloads.

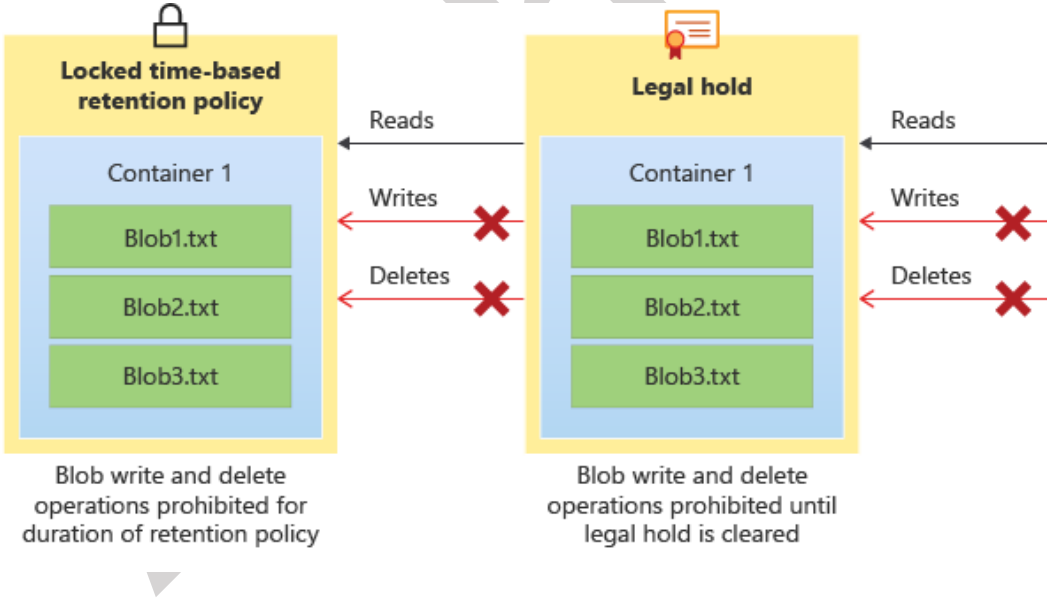
What is Traffic Manager?

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.

Traffic Manager delivers high availability for your critical applications by monitoring your endpoints and providing automatic failover when an endpoint goes down.

Immutable storage

Immutable storage for Azure Blob Storage enables users to store business-critical data in a WORM (Write Once, Read Many) state. While in a WORM state, data cannot be modified or deleted for a user-specified interval. By configuring immutability policies for blob data, you can protect your data from overwrites and deletes.



Source: Microsoft

[Akshay Tondak | LinkedIn]

What is Azure AD Identity Governance?

Azure Active Directory (Azure AD) Identity Governance allows you to balance your organization's need for security and employee productivity with the right processes and visibility. It provides you with capabilities to ensure that the right people have the right access to the right resources. These and related Azure AD and Enterprise Mobility + Security features allows you to mitigate access risk by protecting, monitoring, and auditing access to critical assets -- while ensuring employee and business partner productivity.

Identity Governance give organizations the ability to do the following tasks across employees, business partners and vendors, and across services and applications both on-premises and in clouds:

- Govern the identity lifecycle
- Govern access lifecycle
- Secure privileged access for administration

To get regular updated exam prep material, and other useful resources to help you upskill, you can follow me on:

Akshay Tondak | LinkedIn

akshayytondak (Akshay Tondak) (github.com)