Microsoft AD

Identity Management

https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/identity/

Choose a solution for integrating on-premises Active Directory with Azure

Many organizations use Active Directory Domain Services (AD DS) to authenticate identities associated with users, computers, applications, or other resources that are included in a security boundary. Directory and identity services are typically hosted on-premises, but if your application is hosted partly on-premises and partly in Azure, there may be latency sending authentication requests from Azure back to on-premises. Implementing directory and identity services in Azure can reduce this latency.

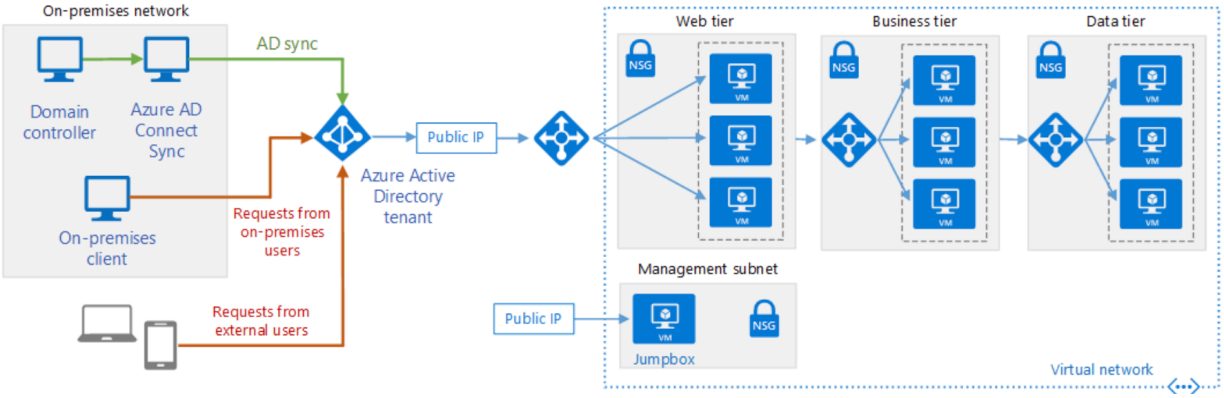
Azure provides two solutions for implementing directory and identity services in Azure:

- Use Azure AD to create an Active Directory domain in the cloud and connect it to your on-premises Active Directory domain. Azure AD Connect integrates your on-premises directories with Azure AD.
- Extend your existing on-premises Active Directory infrastructure to Azure, by deploying a VM in Azure that runs AD DS as a Domain Controller. This architecture is more common when the on-premises network and the Azure virtual network (VNet) are connected by a VPN or ExpressRoute connection. Several variations of this architecture are possible:
    - Create a domain in Azure and join it to your on-premises AD forest.
    - Create a separate forest in Azure that is trusted by domains in your on-premises forest.
    - Replicate an Active Directory Federation Services (AD FS) deployment to Azure.

Type-1

Integrate your on-premises domains with Azure AD

Use Azure Active Directory (Azure AD) to create a domain in Azure and link it to an on-premises AD domain.
The Azure AD directory is not an extension of an on-premises directory. Rather, it's a copy that contains the same objects and identities. Changes made to these items on-premises are copied to Azure AD, but changes made in Azure AD are not replicated back to the on-premises domain.
You can also use Azure AD without using an on-premises directory. In this case, Azure AD acts as the primary source of all identity information, rather than containing data replicated from an on-premises directory.



Benefits

- You don't need to maintain an AD infrastructure in the cloud. Azure AD is entirely managed and maintained by Microsoft.
- Azure AD provides the same identity information that is available on-premises.
- Authentication can happen in Azure, reducing the need for external applications and users to contact the on-premises domain.

Challenges

- You must configure connectivity with your on-premises domain to keep the Azure AD directory synchronized.
- Applications may need to be rewritten to enable authentication through Azure AD.
- If you wish to authenticate service and computer accounts, you will have to also deploy Azure Active Directory Domain Services.

Typical uses for this reference architecture include:

- Web applications deployed in Azure that provide access to remote users who belong to your organization.
- Implementing self-service capabilities for end-users, such as resetting their passwords, and delegating group management. This requires Azure AD Premium edition.
- Architectures in which the on-premises network and the application's Azure

VNet are not connected using a VPN tunnel or ExpressRoute circuit.

General recommendations

The architecture has the following components.

- **Azure AD tenant**. An instance of Azure AD created by your organization. It acts as a directory service for cloud applications by storing objects copied from the on-premises Active Directory and provides identity services.
- **Web tier subnet**. This subnet holds VMs that run a web application. Azure AD can act as an identity broker for this application.
- **On-premises AD DS server**. An on-premises directory and identity service. The AD DS directory can be synchronized with Azure AD to enable it to authenticate on-premises users.
- **Azure AD Connect sync server**. An on-premises computer that runs the Azure AD Connect sync service. This service synchronizes information held in the on-premises Active Directory to Azure AD. For example, if you provision or deprovision groups and users on-premises, these changes propagate to Azure AD.
- **VMs for N-tier application**. The deployment includes infrastructure for an N-tier application.

The Azure AD Connect sync service ensures that identity information stored in the cloud is consistent with that held on-premises. You install this service using the Azure AD Connect software.
You can run the Azure AD Connect sync service on a VM or a computer hosted on-premises.
If you have multiple on-premises domains in a forest, we recommend storing and synchronizing information for the entire forest to a single Azure AD tenant. Filter information for identities that occur in more than one domain, so that each identity appears only once in Azure AD, rather than being duplicated.

Security recommendations

User password management. The Azure AD Premium editions support password writeback, enabling your on-premises users to perform self-service password resets from within the Azure portal.
Actively monitor Azure AD for signs of suspicious activity. Consider using Azure AD Premium P2 edition, which includes Azure AD Identity Protection. Identity Protection uses adaptive machine learning algorithms and heuristics to detect anomalies and risk events that may indicate that an identity has been compromised. For example, it can detect potentially unusual activity such as irregular sign-in activities, sign-ins from unknown sources or from IP addresses with suspicious activity, or sign-ins from devices that may be infected.

Topology recommendations

Single forest, single Azure AD directory
Multiple forests, single Azure AD directory.
Multiple forests, separate topologies. This topology merges identity information from separate forests into a single Azure AD tenant, treating all forests as separate entities.
Staging server. In this configuration, you run a second instance of the Azure AD Connect sync server in parallel with the first. For high-availability.
Multiple Azure AD directories. It is recommended that you create a single Azure AD directory for an organization, but there may be situations where you need to partition information across separate Azure AD directories. In this case, avoid synchronization and password write-back issues by ensuring that each object from the on-premises forest appears in only one Azure AD directory. To implement this scenario, configure separate Azure AD Connect sync servers for each Azure AD directory, and use filtering so that each Azure AD Connect sync server operates on a mutually exclusive set of objects.

User authentication
By default, the Azure AD Connect sync server configures password hash synchronization between the on-premises domain and Azure AD, and the Azure AD service assumes that users authenticate by providing the same password that they use on-premises.

Monitoring
Health monitoring is performed by the following agents installed on-premises:

- Azure AD Connect installs an agent that captures information about synchronization operations. Use the Azure AD Connect Health blade in the Azure portal to monitor its health and performance. For more information, see Using Azure AD Connect Health for sync.
- To monitor the health of the AD DS domains and directories from Azure, install the Azure AD Connect Health for AD DS agent on a machine within the on-premises domain. Use the Azure Active Directory Connect Health blade in the Azure portal for health monitoring. For more information, see Using Azure AD Connect Health with AD DS
- Install the Azure AD Connect Health for AD FS agent to monitor the health of services running on on-premises, and use the Azure Active Directory Connect Health blade in the Azure portal to monitor AD FS. For more information, see Using Azure AD Connect Health with AD FS

Availability considerations
The Azure AD service is geo-distributed and runs in multiple datacenters spread around the world with automated failover. If a datacenter becomes unavailable, Azure AD ensures that your directory data is available for instance access in at least two more regionally dispersed datacenters.

Type-2

AD DS in Azure joined to an on-premises forest

Deploy AD Domain Services (AD DS) servers to Azure. Create a domain in Azure and join it to your on-premises AD forest.
Consider this option if you need to use AD DS features that are not currently implemented by Azure AD.

Benefits

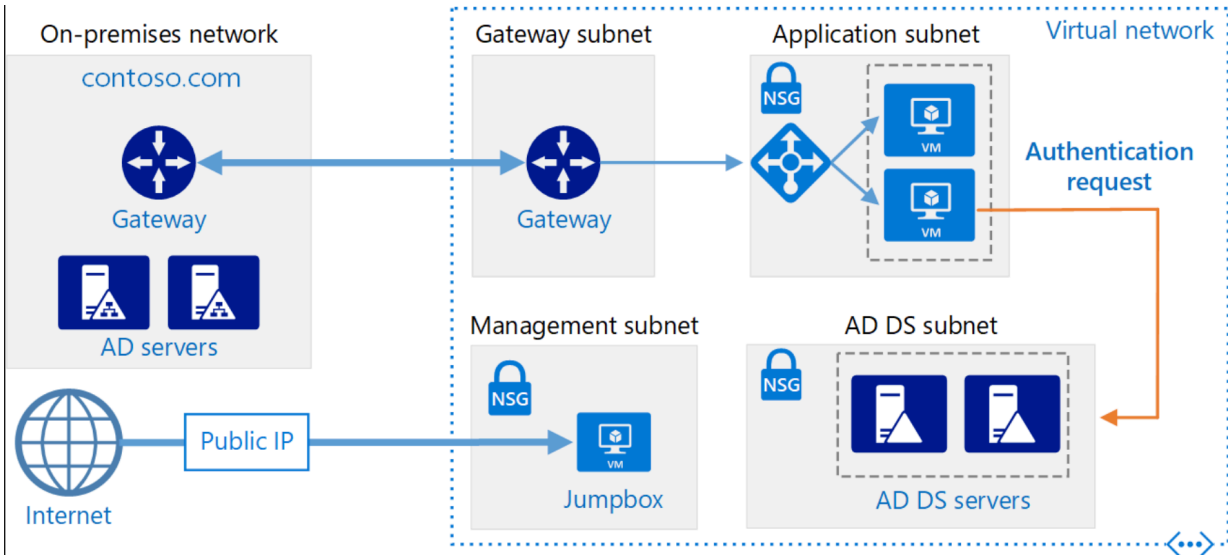
- Provides access to the same identity information that is available on-premises.
- You can authenticate user, service, and computer accounts on-premises and in Azure.
- You don't need to manage a separate AD forest. The domain in Azure can belong to the on-premises forest.
- You can apply group policy defined by on-premises Group Policy Objects to the domain in Azure.

Challenges

- You must deploy and manage your own AD DS servers and domain in the cloud.
- There may be some synchronization latency between the domain servers in the cloud and the servers running on-premises.

If your application is hosted partly on-premises and partly in Azure, it may be more efficient to replicate Active Directory Domain Services (AD DS) in Azure. This can reduce the latency caused by sending authentication requests from the cloud back to AD DS running on-premises.

This architecture is commonly used when the on-premises network and the Azure virtual network are connected by a VPN or ExpressRoute connection. This architecture also supports bidirectional replication, meaning changes can be made either on-premises or in the cloud, and both sources will be kept consistent.
Typical uses for this architecture include hybrid applications in which functionality is distributed between on-premises and Azure, and applications and services that perform authentication using Active Directory.



- **On-premises network**. The on-premises network includes local Active Directory servers that can perform authentication and authorization for components located on-premises.
- **Active Directory servers**. These are domain controllers implementing directory services (AD DS) running as VMs in the cloud. These servers can provide authentication of components running in your Azure virtual network.
- **Active Directory subnet**. The AD DS servers are hosted in a separate subnet. Network security group (NSG) rules protect the AD DS servers and provide a firewall against traffic from unexpected sources.
- **Azure Gateway and Active Directory synchronization**. The Azure gateway provides a connection between the on-premises network and the Azure VNet. This can be a VPN connection or Azure ExpressRoute. All synchronization requests between the Active Directory servers in the cloud and on-premises pass through the gateway. User-defined routes (UDRs) handle routing for on-premises traffic that passes to Azure.

Active Directory site

In AD DS, a site represents a physical location, network, or collection of devices. AD DS sites are used to manage AD DS database replication by grouping together AD DS objects that are located close to one another and are connected by a high-speed network. AD DS includes logic to select the best strategy for replicating the AD DS database between sites.

We recommend that you create an AD DS site including the subnets defined for your application in Azure. Then, configure a site link between your on-premises AD DS sites, and AD DS will automatically perform the most efficient database replication possible. This database replication requires little beyond the initial configuration.

Scalability considerations

AD DS is designed for scalability. You don't need to configure a load balancer or traffic controller to direct requests to AD DS domain controllers. The only scalability consideration is to configure the VMs running AD DS with the correct size for your network load requirements, monitor the load on the VMs, and scale up or down as necessary.

Availability considerations

Deploy the VMs running AD DS into an availability set. Also, consider assigning the role of standby operations master to at least one server, and possibly more depending on your requirements. A standby operations master is an active copy of the operations master that can be used in place of the primary operations masters server during failover.

Security considerations

AD DS servers provide authentication services and are an attractive target for attacks. To secure them, prevent direct Internet connectivity by placing the AD DS servers in a separate subnet with an NSG acting as a firewall. Close all ports on the AD DS servers except those necessary for authentication, authorization, and server synchronization.

Type-3

AD DS in Azure with a separate forest

Deploy AD Domain Services (AD DS) servers to Azure, but create a separate Active Directory forest that is separate from the on-premises forest. This forest is trusted by domains in your on-premises forest.
Typical uses for this architecture include maintaining security separation for objects and identities held in the cloud, and migrating individual domains from on-premises to the cloud.

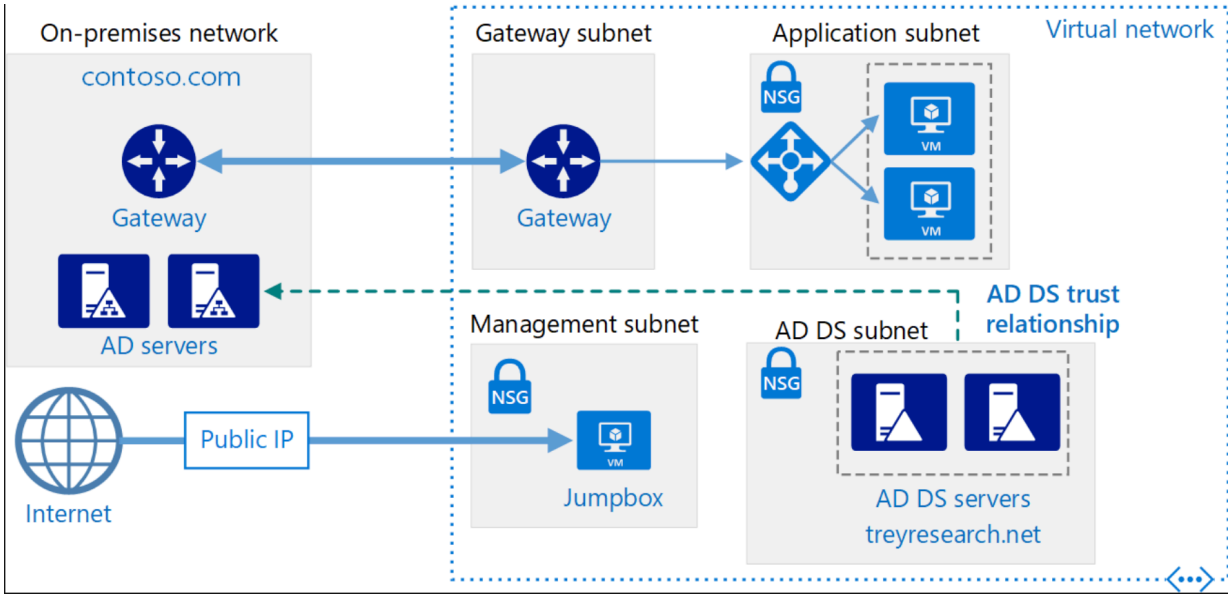
Benefits

- You can implement on-premises identities and separate Azure-only identities.
- You don't need to replicate from the on-premises AD forest to Azure.

Challenges

- Authentication within Azure for on-premises identities requires extra network hops to the on-premises AD servers.
- You must deploy your own AD DS servers and forest in the cloud, and establish the appropriate trust relationships between forests.

Active Directory Domain Services (AD DS) stores identity information in a hierarchical structure. The top node in the hierarchical structure is known as a forest. A forest contains domains, and domains contain other types of objects. This reference architecture creates an AD DS forest in Azure with a one-way outgoing trust relationship with an on-premises domain. The forest in Azure contains a domain that does not exist on-premises. Because of the trust relationship, logons made against on-premises domains can be trusted for access to resources in the separate Azure domain.
Typical uses for this architecture include maintaining security separation for objects and identities held in the cloud, and migrating individual domains from on-premises to the cloud.



- **On-premises network**. The on-premises network contains its own Active Directory forest and domains.
- **Active Directory servers**. These are domain controllers implementing domain services running as VMs in the cloud. These servers host a forest containing one or more domains, separate from those located on-premises.
- **One-way trust relationship**. The example in the diagram shows a one-way trust from the domain in Azure to the on-premises domain. This relationship enables on-premises users to access resources in the domain in Azure, but not the other way around. It is possible to create a two-way trust if cloud users also require access to on-premises resources.
- **Active Directory subnet**. The AD DS servers are hosted in a separate subnet. Network security group (NSG) rules protect the AD DS servers and provide a firewall against traffic from unexpected sources.

- **Azure gateway**. The Azure gateway provides a connection between the on-premises network and the Azure VNet. This can be a VPN connection or Azure ExpressRoute.

The on-premises domains are contained within a different forest from the domains in the cloud. To enable authentication of on-premises users in the cloud, the domains in Azure must trust the logon domain in the on-premises forest. Similarly, if the cloud provides a logon domain for external users, it may be necessary for the on-premises forest to trust the cloud domain.

Trusts can be unidirectional (one-way) or bidirectional (two-way):

- A one-way trust enables users in one domain or forest (known as the *incoming* domain or forest) to access the resources held in another (the *outgoing* domain or forest).
- A two-way trust enables users in either domain or forest to access resources held in the other.

Scalability considerations

Active Directory is automatically scalable for domain controllers that are part of the same domain. Requests are distributed across all controllers within a domain. You can add another domain controller, and it synchronizes automatically with the domain. Do not configure a separate load balancer to direct traffic to controllers within the domain. Ensure that all domain controllers have sufficient memory and storage resources to handle the domain database. Make all domain controller VMs the same size.

Availability considerations

Provision at least two domain controllers for each domain. This enables automatic replication between servers. Create an availability set for the VMs acting as Active Directory servers handling each domain. Put at least two servers in this availability set.

Type-4

Extend AD FS to Azure

Replicate an Active Directory Federation Services (AD FS) deployment to Azure, to perform federated authentication and authorization for components running in Azure.
Typical uses for this architecture:

- Authenticate and authorize users from partner organizations.
- Allow users to authenticate from web browsers running outside of the organizational firewall.
- Allow users to connect from authorized external devices such as mobile devices.

Benefits

- You can leverage claims-aware applications.
- Provides the ability to trust external partners for authentication.
- Compatibility with large set of authentication protocols.

Challenges

- You must deploy your own AD DS, AD FS, and AD FS Web Application Proxy servers in Azure.
- This architecture can be complex to configure.

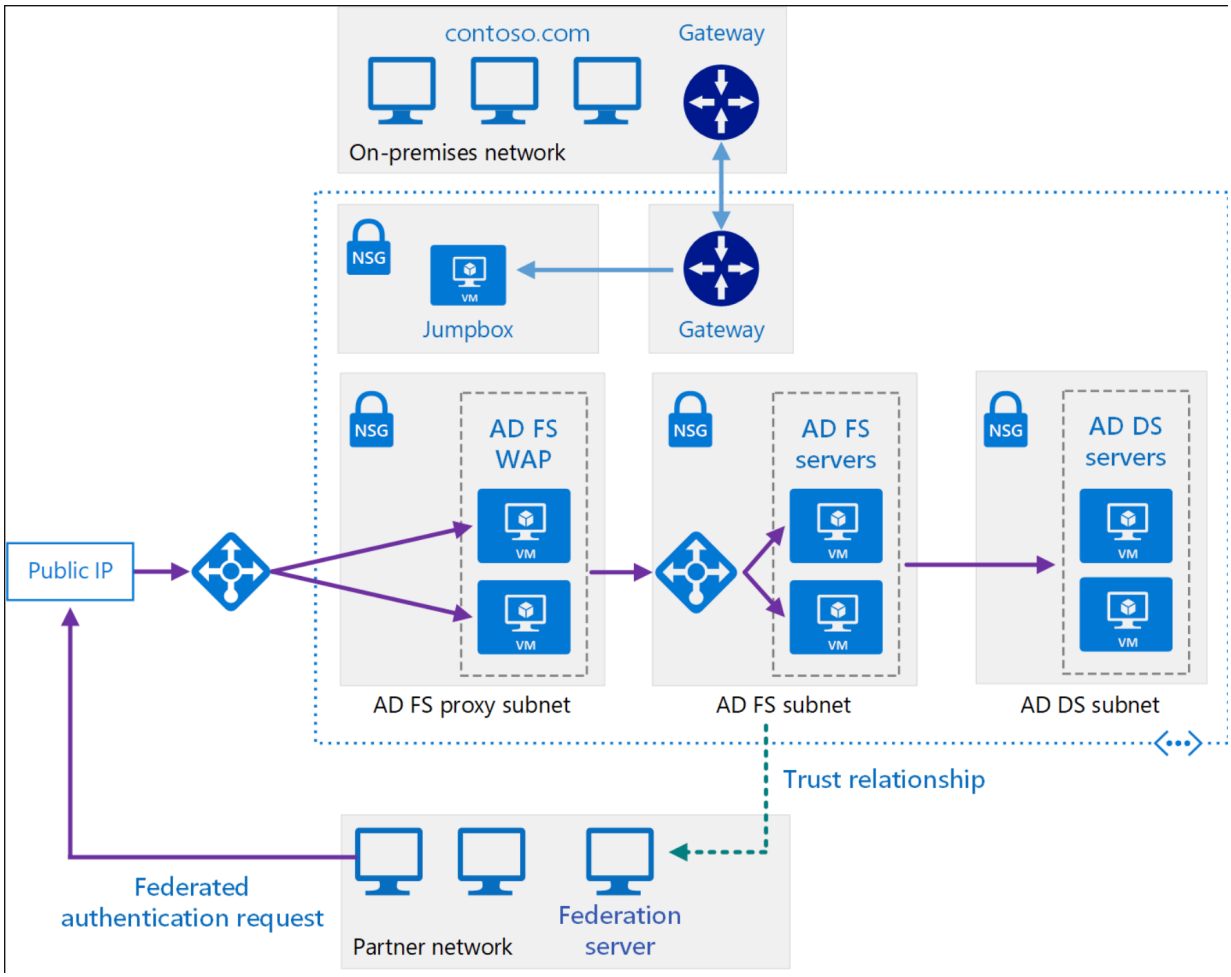
This reference architecture implements a secure hybrid network that extends your on-premises network to Azure and uses Active Directory Federation Services (AD FS) to perform federated authentication and authorization for components running in Azure.

AD FS can be hosted on-premises, but if your application is a hybrid in which some parts are implemented in Azure, it may be more efficient to replicate AD FS in the cloud.
The diagram shows the following scenarios:

- Application code from a partner organization accesses a web application hosted inside your Azure VNet.
- An external, registered user with credentials stored inside Active Directory Domain Services (DS) accesses a web application hosted inside your Azure VNet.
- A user connected to your VNet using an authorized device executes a web application hosted inside your Azure VNet.

Typical uses for this architecture include:

- Hybrid applications where workloads run partly on-premises and partly in Azure.
- Solutions that use federated authorization to expose web applications to partner organizations.
- Systems that support access from web browsers running outside of the organizational firewall.
- Systems that enable users to access to web applications by connecting from authorized external devices such as remote computers, notebooks, and other mobile devices.



- **AD DS subnet**. The AD DS servers are contained in their own subnet with network security group (NSG) rules acting as a firewall.
- **AD DS servers**. Domain controllers running as VMs in Azure. These servers provide authentication of local identities within the domain.
- **AD FS subnet**. The AD FS servers are located within their own subnet with NSG rules acting as a firewall.
- **AD FS servers**. The AD FS servers provide federated authorization and authentication. In this architecture, they perform the following tasks:
    - Receiving security tokens containing claims made by a partner federation server on behalf of a partner user. AD FS verifies that the tokens are valid before passing the claims to the web application running in Azure to authorize requests.
      The application running in Azure is the *relying party*. The partner federation server must issue claims that are understood by the web application. The partner federation servers are referred to as *account partners*, because they submit access requests on behalf of authenticated

accounts in the partner organization. The AD FS servers are called *resource partners* because they provide access to resources (the web application).
    - Authenticating and authorizing incoming requests from external users running a web browser or device that needs access to web applications, by using AD DS and the Active Directory Device Registration Service.
- The AD FS servers are configured as a farm accessed through an Azure load balancer. This implementation improves availability and scalability. The AD FS servers are not exposed directly to the Internet. All Internet traffic is filtered through AD FS web application proxy servers and a DMZ (also referred to as a perimeter network).
  For more information about how AD FS works, see Active Directory Federation Services Overview. Also, the article AD FS deployment in Azure contains a detailed step-by-step introduction to implementation.
- **AD FS proxy subnet**. The AD FS proxy servers can be contained within their own subnet, with NSG rules providing protection. The servers in this subnet are exposed to the Internet through a set of network virtual appliances that provide a firewall between your Azure virtual network and the Internet.
- **AD FS web application proxy (WAP) servers**. These VMs act as AD FS servers for incoming requests from partner organizations and external devices. The WAP servers act as a filter, shielding the AD FS servers from direct access from the Internet. As with the AD FS servers, deploying the WAP servers in a farm with load balancing gives you greater availability and scalability than deploying a collection of stand-alone servers.
- **Partner organization**. A partner organization running a web application that requests access to a web application running in Azure. The federation server at the partner organization authenticates requests locally, and submits security tokens containing claims to AD FS running in Azure. AD FS in Azure validates the security tokens, and if valid can pass the claims to the web application running in Azure to authorize them.

Networking recommendations
Configure the network interface for each of the VMs hosting AD FS and WAP servers with static private IP addresses.
Do not give the AD FS VMs public IP addresses.

AD FS trust
Establish federation trust between your AD FS installation, and the federation servers of any partner organizations. Configure any claims filtering and mapping required.

- DevOps staff at each partner organization must add a relying party trust for the web applications accessible through your AD FS servers.
- DevOps staff in your organization must configure claims-provider trust to

enable your AD FS servers to trust the claims that partner organizations provide.
- DevOps staff in your organization must also configure AD FS to pass claims on to your organization's web applications.

Publish your organization's web applications and make them available to external partners by using preauthentication through the WAP servers.
AD FS supports token transformation and augmentation. Azure Active Directory does not provide this feature. With AD FS, when you set up the trust relationships, you can:
- Configure claim transformations for authorization rules. For example, you can map group security from a representation used by a non-Microsoft partner organization to something that Active Directory DS can authorize in your organization.
- Transform claims from one format to another. For example, you can map from SAML 2.0 to SAML 1.1 if your application only supports SAML 1.1 claims.

AD FS monitoring
The Microsoft System Center Management Pack for Active Directory Federation Services 2012 R2 provides both proactive and reactive monitoring of your AD FS deployment for the federation server. This management pack monitors:
- Events that the AD FS service records in its event logs.
- The performance data that the AD FS performance counters collect.
- The overall health of the AD FS system and web applications (relying parties), and provides alerts for critical issues and warnings.

Scalability considerations

The following considerations, summarized from the article Plan your AD FS deployment, give a starting point for sizing AD FS farms:
- If you have fewer than 1000 users, do not create dedicated servers, but instead install AD FS on each of the Active Directory DS servers in the cloud. Make sure that you have at least two Active Directory DS servers to maintain availability. Create a single WAP server.
- If you have between 1000 and 15000 users, create two dedicated AD FS servers and two dedicated WAP servers.
- If you have between 15000 and 60000 users, create between three and five dedicated AD FS servers and at least two dedicated WAP servers.

Availability considerations

Create an AD FS farm with at least two servers to increase availability of the

service. Use different storage accounts for each AD FS VM in the farm. This approach helps to ensure that a failure in a single storage account does not make the entire farm inaccessible.
Create separate Azure availability sets for the AD FS and WAP VMs. Ensure that there are at least two VMs in each set. Each availability set must have at least two update domains and two fault domains.

Manageability considerations

DevOps staff should be prepared to perform the following tasks:

- Managing the federation servers, including managing the AD FS farm, managing trust policy on the federation servers, and managing the certificates used by the federation services.
- Managing the WAP servers including managing the WAP farm and certificates.
- Managing web applications including configuring relying parties, authentication methods, and claims mappings.
- Backing up AD FS components.

Security considerations

AD FS uses HTTPS, so make sure that the NSG rules for the subnet containing the web tier VMs permit HTTPS requests. These requests can originate from the on-premises network, the subnets containing the web tier, business tier, data tier, private DMZ, public DMZ, and the subnet containing the AD FS servers.
Prevent direct exposure of the AD FS servers to the Internet. AD FS servers are domain-joined computers that have full authorization to grant security tokens. If a server is compromised, a malicious user can issue full access tokens to all web applications and to all federation servers that are protected by AD FS.