✓ 100 XP ▶

Describe Azure directory services

6 minutes

Azure Active Directory (Azure AD) is a directory service that enables you to sign in and access both Microsoft cloud applications and cloud applications that you develop. Azure AD can also help you maintain your on-premises Active Directory deployment.

For on-premises environments, Active Directory running on Windows Server provides an identity and access management service that's managed by your organization. Azure AD is Microsoft's cloud-based identity and access management service. With Azure AD, you control the identity accounts, but Microsoft ensures that the service is available globally. If you've worked with Active Directory, Azure AD will be familiar to you.

When you secure identities on-premises with Active Directory, Microsoft doesn't monitor sign-in attempts. When you connect Active Directory with Azure AD, Microsoft can help protect you by detecting suspicious sign-in attempts at no extra cost. For example, Azure AD can detect sign-in attempts from unexpected locations or unknown devices.

Who uses Azure AD?

Azure AD is for:

- **IT administrators**. Administrators can use Azure AD to control access to applications and resources based on their business requirements.
- **App developers**. Developers can use Azure AD to provide a standards-based approach for adding functionality to applications that they build, such as adding SSO functionality to an app or enabling an app to work with a user's existing credentials.
- **Users**. Users can manage their identities and take maintenance actions like self-service password reset.
- **Online service subscribers**. Microsoft 365, Microsoft Office 365, Azure, and Microsoft Dynamics CRM Online subscribers are already using Azure AD to authenticate into their account.

What does Azure AD do?

Azure AD provides services such as:

- **Authentication**: This includes verifying identity to access applications and resources. It also includes providing functionality such as self-service password reset, multifactor authentication, a custom list of banned passwords, and smart lockout services.
- **Single sign-on**: Single sign-on (SSO) enables you to remember only one username and one password to access multiple applications. A single identity is tied to a user, which simplifies the security model. As users change roles or leave an organization, access modifications are tied to that identity, which greatly reduces the effort needed to change or disable accounts.
- **Application management**: You can manage your cloud and on-premises apps by using Azure AD. Features like Application Proxy, SaaS apps, the My Apps portal, and single sign-on provide a better user experience.
- **Device management**: Along with accounts for individual people, Azure AD supports the registration of devices. Registration enables devices to be managed through tools like Microsoft Intune. It also allows for device-based Conditional Access policies to restrict access attempts to only those coming from known devices, regardless of the requesting user account.

Can I connect my on-premises AD with Azure AD?

If you had an on-premises environment running Active Directory and a cloud deployment using Azure AD, you would need to maintain two identity sets. However, you can connect Active Directory with Azure AD, enabling a consistent identity experience between cloud and on-premises.

One method of connecting Azure AD with your on-premises AD is using Azure AD Connect. Azure AD Connect synchronizes user identities between on-premises Active Directory and Azure AD. Azure AD Connect synchronizes changes between both identity systems, so you can use features like SSO, multifactor authentication, and self-service password reset under both systems.

What is Azure Active Directory Domain Services?

Azure Active Directory Domain Services (Azure AD DS) is a service that provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos/NTLM authentication. Just like Azure AD lets you use directory services without having to maintain the infrastructure supporting it, with Azure AD DS, you get the benefit of 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.

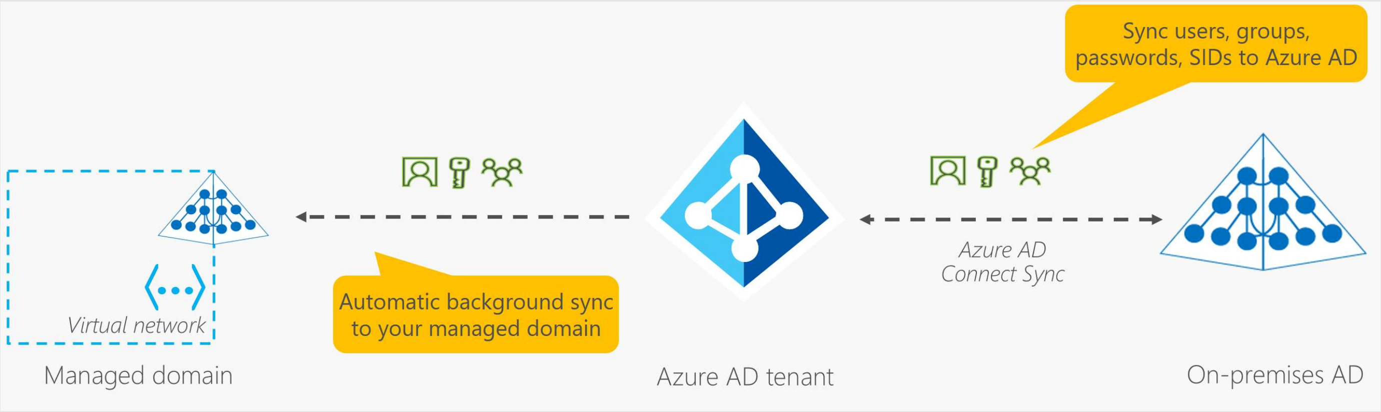
How does Azure AD DS work?

When you create an Azure AD DS managed domain, you define a unique namespace. This namespace is the domain name. Two Windows Server domain controllers are then deployed into your selected Azure region. This deployment of DCs is known as a replica set.

You don't need to manage, configure, or update these DCs. The Azure platform handles the DCs as part of the managed domain, including backups and encryption at rest using Azure Disk Encryption.

Is information synchronized?

A managed domain is configured to perform a one-way synchronization from Azure AD to Azure AD DS. You can create resources directly in the managed domain, but they aren't synchronized back to Azure AD. In a hybrid environment with an on-premises AD DS environment, Azure AD Connect synchronizes identity information with Azure AD, which is then synchronized to the managed domain.


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

Applications, services, and VMs in Azure that connect to the managed domain can then use common Azure AD DS features such as domain join, group policy, LDAP, and Kerberos/NTLM authentication.

Next unit: Describe Azure authentication methods

Continue ›