Module 10

Managing Active Directory infrastructure in hybrid and cloud only scenarios

Module Overview

- Designing and implementing an Active Directory environment by using Azure IaaS
- Implementing directory synchronization between AD DS and Azure AD
- Implementing single sign-on in federated scenarios

Lesson 1: Designing and implementing an Active Directory environment by using Azure IaaS

- Demonstration: Preparing the lab environment
- Overview of AD DS and Azure integration options
- Planning to deploy Active Directory domain controllers on Azure virtual machines
- Implementing Active Directory domain controllers on Azure VMs

Demonstration: Preparing the lab environment

In this demonstration, you will learn how to prepare the lab environment

Note: To prepare the lab environment for this module, you must complete this task

Overview of AD DS and Azure integration options

- AD DS was designed for on-premises deployments:
  - Relies on protocols not suited for Internet communication
  - Requires domain-joined computers to deliver full functionality
- Two primary deployment AD DS options in Azure:
  - Azure VMs:
    - Domain controllers managed by a customer
    - Implement on the AD DS environment that you manage
    - Two basic Active Directory architecture choices:
      - Separate AD DS domain and forest
      - Extension of an existing on-premises AD DS (this requires hybrid connectivity)
  - Azure AD DS
    - Domain controllers managed by Microsoft
    - Single domain forest on an Azure virtual network

Planning to deploy Active Directory domain controllers on Azure virtual machines

- Primary reasons for placing domain controllers in Azure:
  - Keeping authentication requests from Azure-based services within Azure
  - Extending on-premises Active Directory to Azure
  - Enhancing resiliency of directory synchronization with Azure AD and Azure AD-federated deployments
- Main deployment scenarios:
  - AD DS on Azure VMs
  - On-premises AD DS with cross-premises connectivity
  - On-premises AD DS and AD DS on Azure VMs
- Important planning considerations:
  - Inter-site connectivity
  - Active Directory topology
  - Read-only domain controllers
  - Global catalogs

Implementing Active Directory domain controllers on Azure VMs

Extending Active Directory into Azure IaaS:

1. Create an Azure virtual network with cross-premises connectivity
   - Configure DNS to point to on-premises DNS servers
2. Create an Azure storage account
   - Data disks (when using unmanaged disk)
   - Diagnostics
3. Deploy an Azure VM with a static IP address into the virtual network
4. Install the AD DS and DNS server roles in the Azure VM

Creating a new Active Directory forest in Azure IaaS

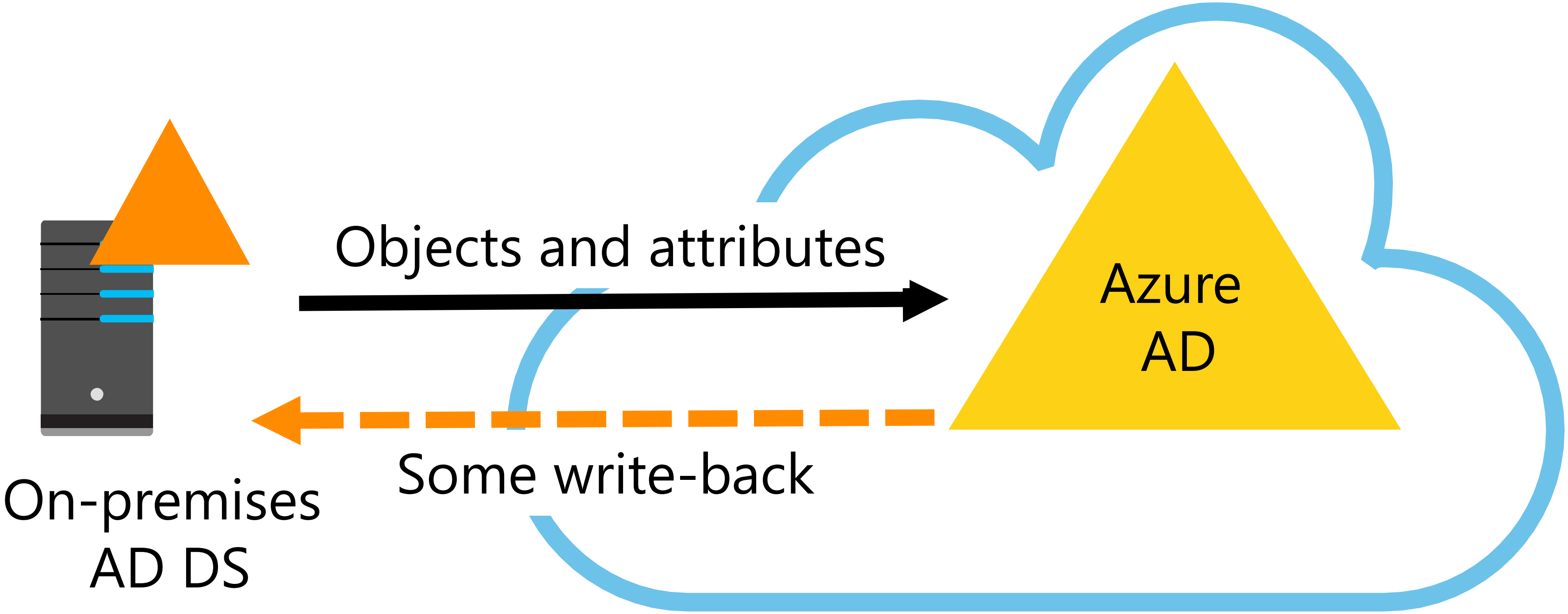
Creating a new Active Directory forest in Azure IaaS:

1. Create an Azure virtual network
   - Configure DNS to point to the IP address you will assign to the Azure VM
2. Create an Azure storage account (optional)
   - Data disks (when using unmanaged disk)
   - Diagnostics
3. Deploy an Azure VM with a static IP address into the virtual network
4. Install the AD DS and DNS server roles in the Azure VM

Lesson 2: Implementing directory synchronization between AD DS and Azure AD

- Overview of directory synchronization
- Comparing Azure AD integration scenarios
- Discussion: Which directory synchronization option would be optimal for your organization?
- Preparing on-premises Active Directory for directory synchronization
- Installing and configuring Azure AD Connect
- Managing and monitoring directory synchronization
- Implementing Azure AD DS
- Demonstration: Implementing directory synchronization by using Azure AD Connect

Overview of directory synchronization



Azure AD Connect is made up of three primary components:

- Synchronization
- AD FS
- Health monitoring

Comparing Azure AD integration scenarios

- Directory synchronization
- Directory synchronization with password hash synchronization (same sign-on)
- Directory synchronization with password hash synchronization and Seamless SSO
- Directory synchronization with pass-through authentication and same sign-on
- Directory synchronization with pass-through authentication and Seamless SSO
- Directory synchronization with federation (single sign-on)

Discussion: Which directory synchronization option would be optimal for your organization?

Which directory synchronization option would be optimal for your organization?

5 minutes

Preparing on-premises Active Directory for directory synchronization

- Review domain controller requirements
- Review Azure AD Connect computer requirements
- Review hardware recommendations
- Review accounts and required permissions
- Review network connectivity requirements
- Review certificate requirements
- Review Azure AD Connect supporting components
- Review UPN requirements
- Prepare AD DS

Installing and configuring Azure AD Connect

- Use express settings for:
  - Single Active Directory forest
  - Default synchronization settings
- Use customized settings for:
  - Multiple forests with duplicate identities
  - Federation scenarios
  - Custom synchronization settings, for example writeback
- Installing Azure AD Connect with express settings:
  - Installs the synchronization engine
  - Configures Azure AD Connector
  - Configures the on-premises AD DS connector
  - Enables password synchronization
  - Configures synchronization services
  - Configures synchronization services for Exchange hybrid deployment (optional)

Installing and configuring Azure AD Connect

- Azure AD Connect filtering options:
  - Single group membership
  - Domain
  - OU
  - Attribute
- Run profiles:
  - Full Import
  - Full Synchronization
  - Delta Import
  - Delta Synchronization
  - Export
- Windows PowerShell
- Start-ADSyncSyncCycle

Managing and monitoring directory synchronization

- Azure AD Sync Scheduler:
  - Object and attribute sync:
    - Set-ADSyncScheduler
    - Start-ADSyncCycle
  - Password sync
- Azure AD Connect Health:
  - Azure AD Connect Health for Sync
  - Azure AD Connect Health for AD DS
  - Azure AD Connect Health for AD FS

Implementing Azure AD DS

- Managed AD DS in Azure
- Integrates with Azure AD and (optionally) with AD DS
- Facilitates deployment of Active Directory-aware applications
- Offers support for:
  - Domain join
  - NTLM and Kerberos authentication
  - Group Policy
  - LDAP reads
- Does not support:
  - Trust relationships
  - Schema extensions
  - LDAP writes (users and groups are synchronized from Azure AD)

Demonstration: Implementing directory synchronization by using Azure AD Connect

In this demonstration, you will learn how to:

- Create an Azure AD tenant
- Create an Azure AD Global Admin user account.
- Install Azure AD Connect with custom settings

Lesson 3: Implementing single sign-on in federated scenarios

- Overview of AD FS and Web Application Proxy
- Planning for the deployment of AD FS with Azure
- Deploying AD FS
- Managing and maintaining AD FS

Overview of AD FS and Web Application Proxy

How AD FS works with Azure AD:

1. The user opens a web browser and sends an HTTPS request to the SaaS application.
2. The SaaS application determines if the user belongs to an Azure AD tenant.
3. The SaaS application provider redirects the user to the user’s Azure AD tenant.
4. The user’s browser sends an HTTPS authentication request to the Azure AD tenant.
5. If the user’s Azure AD account represents a federated identity, the user’s browser is redirected to the on-premises federation server.
6. The user’s browser sends an HTTPS request to the on-premises federation server.
7. If the user is signed in to the on-premises AD DS domain, the federation server requests the AD DS authentication, based on the user’s existing Kerberos ticket. Otherwise, the user receives a prompt to authenticate with the AD DS credentials, which the federation server relays to an AD DS domain controller.

Overview of AD FS and Web Application Proxy

How AD FS works with Azure AD (continued):

8. The AD DS domain controller verifies the authentication request and then sends the successful authentication message back to the federation server.
9. Federation server creates the claim for the user based on the rules defined as part of the AD FS configuration.
10. The federation server places the claims data in a digitally signed security token and forwards it to the user's browser.
11. The user's browser forwards the security token containing claims to Azure AD.
12. Azure AD verifies the validity of the AD FS security token based on the existing federation trust.
13. Azure AD creates a new token to access the SaaS application and sends it back to the user's browser.
14. The user uses the Azure AD–issued token to access the SaaS application.

Overview of AD FS and Web Application Proxy

- AD FS servers:
  - Authenticate users against an Active Directory domain controller
- AD FS authentication methods:
  - Forms authentication
  - Certificate authentication
  - Windows authentication
  - Device authentication
  - Azure MFA
- AD FS proxy or Web Application Proxy servers:
  - Provide internet-accessible service and protect AD FS servers
  - Are located in the perimeter network and redirect incoming authentication requests to the AD FS server

Planning for the deployment of AD FS with Azure

- Server placement
- Network connectivity
- Name resolution
- Certificates
- Capacity
- Availability
- Database servers
- Service accounts
- Conditional access
- End-user devices and browsers

Deploying AD FS

- Configure a new AD FS farm:
  - Provide an SSL certificate
  - Select the subject name and prefix
- Add one or more AD FS servers
- Add one or more Web Application Proxy servers
- Provide an AD FS service account:
  - An existing gMSA
  - A new gMSA
  - An existing domain user
- Select the Azure AD domain:
  - Must be verified

Managing and maintaining AD FS

- Manage AD FS certificate renewal
- Convert domains to federated domains
- Monitor AD FS with Azure AD Connect Health

Lab: Implementing and managing Azure AD synchronization

- Exercise 1: Configuring directory synchronization
- Exercise 2: Synchronizing directories

Logon Information

Virtual machine:	**20533E-MIA-CL1**
User name:	**Student**
Password:	**Pa55w.rd**

Estimated Time: 60 minutes

Lab Scenario

Adatum Corporation users access on-premises applications by authenticating once, during initial sign-in to their client computers.

While evaluating Azure for Adatum, you must verify that Adatum users can continue using their existing credentials to access Azure resources.

In addition, you must verify that attribute changes to Active Directory user and group accounts will automatically replicate to Azure AD.

Lab Review

- How would you implement OU–level filtering for directory synchronization?
- When would you use Azure AD Connect custom setup?

Module Review and Takeaways

- Common Issues and Troubleshooting Tips
- Review Question