Module 10

Managing an Active Directory infrastructure in a hybrid environment

Module Overview

- Extending an on-premises Active Directory domain to Azure IaaS
- Implementing directory synchronization by using Azure AD Connect
- Implementing federation

Lesson 1: Extending an on-premises Active Directory domain to Azure IaaS

- Demonstration: Preparing the Azure environment for the lab and the demonstrations in this module
- 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 virtual machines

Demonstration: Preparing the Azure environment for the lab and the demonstrations in this module

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

- Sign in to your Azure subscription
- Prepare the Azure environment

Overview of AD DS and Azure integration options

- AD DS was designed for on-premises deployments:
  - Single-tenant by design
  - Relies on protocols not suited for Internet communication
  - Requires domain-joined computers to deliver full functionality
- You can deploy AD DS domain controllers in Azure virtual machines to:
  - Implement an AD DS environment that you manage
    - Create a separate AD DS domain and forest
    - Extend your on-premises AD DS (this requires hybrid connectivity)
  - Implement a managed AD DS environment (Azure AD)

Planning to deploy Active Directory domain controllers on Azure virtual machines

- Reasons for placing domain controllers in Azure:
  - Keeping authentication requests for Azure-based services within Azure
  - Extending access to on-premises Active Directory to other regions
  - Enhancing resiliency of directory synchronization and federation deployments
- Deployment scenarios:
  - Deploy AD DS only in Azure
  - Deploy AD DS only in an on-premises infrastructure with cross-premises connectivity
  - Deploy AD DS in an on-premises infrastructure and on Azure virtual machines
- Planning considerations:
  - Inter-site connectivity
  - Active Directory topology
  - Read-only domain controllers
  - Global catalogs

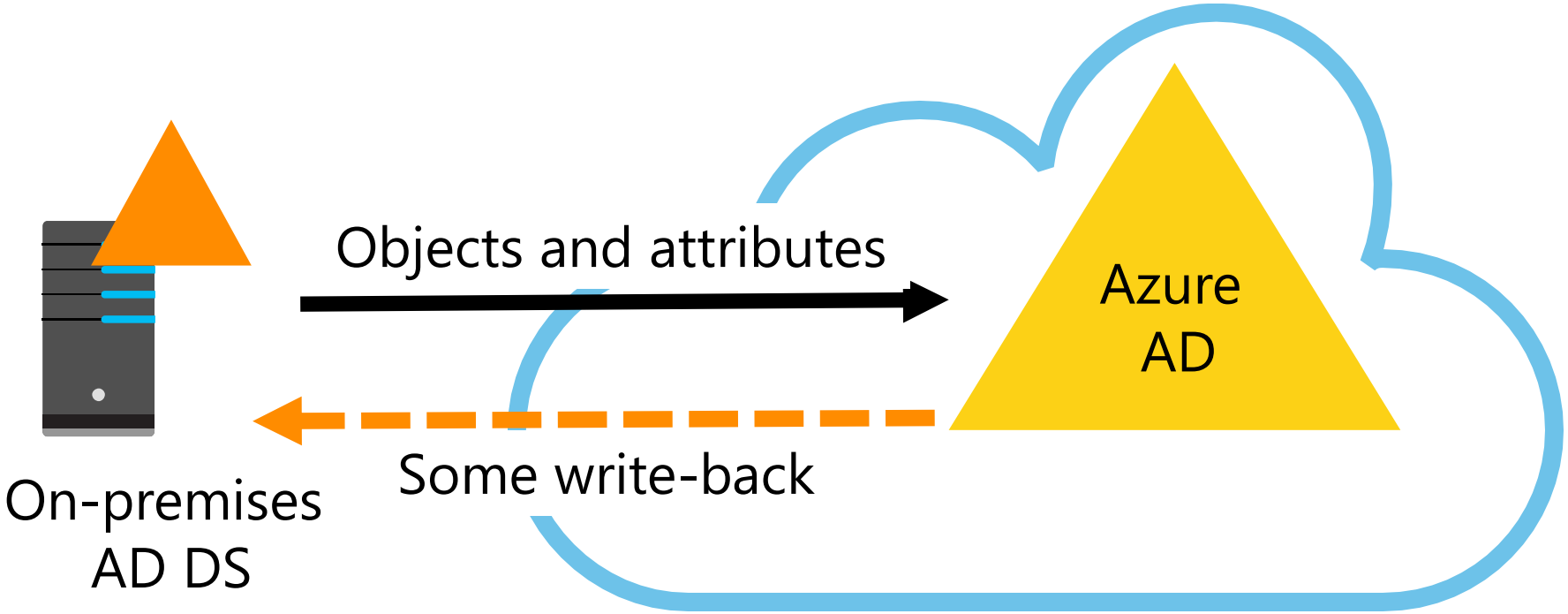
Implementing Active Directory domain controllers on Azure virtual machines

1. Create an Azure virtual network with cross-premises connectivity
2. Create an Azure storage account
3. Deploy an Azure VM into the virtual network and assign to it a static IP address
4. Install the AD DS and DNS server roles in the Azure VM

Lesson 2: Implementing directory synchronization by using Azure AD Connect

- Overview of directory synchronization
- Comparing Azure AD integration scenarios
- Discussion: Which directory synchronization option is suitable for my environment?
- Preparing on-premises Active Directory for directory synchronization
- Installing and configuring Azure AD Connect
- Managing and monitoring directory synchronization by using Azure AD Connect Health
- Implementing Azure AD Domain Services
- 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

Factor	Directory synchronization only	Directory synchronization with password synchronization	Directory synchronization with federation
Sync users, groups and contacts with Azure	Yes	Yes	Yes
Sync incremental updates with Azure	Yes	Yes	Yes
Enable hybrid Office 365 scenarios	Yes, limited support	Yes, limited support	Yes, full support
Users can sign in with on-premises credentials	No	Yes	Yes
Reduce password administration costs	No	Yes	Yes
Control password policies from an on-premises directory	No	Yes	Yes
Enable cloud-based multi-factor authentication	Yes	Yes	Yes
Enable on-premises multi-factor authentication	No	No	Yes
Authenticate against on-premises directory	No	No	Yes
Implement SSO with organizational credentials	No	No	Yes

Discussion: Which directory synchronization option is suitable for my environment?

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
- Clean up AD DS

Installing and configuring Azure AD Connect

- Use express settings for:
  - A single Active Directory forest
  - Signing in with the same password by using password synchronization
- 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

- Use customized settings when:
  - You have multiple forests and want to support many on-premises topologies
  - You want to customize your sign-in option, such as using AD FS for federation or using a non-Microsoft identity provider
  - You customize synchronization features, such as filtering and write-back
- Azure AD Connect filtering options:
  - Single group membership
  - Domain
  - OU
  - Attribute
- Manual or scheduled Azure AD Connect synchronization

Managing and monitoring directory synchronization by using Azure AD Connect Health

Azure AD Connect Health capabilities:

- Alerts provide:
  - Information about events
  - Synchronization status
  - Links to documentation
  - Email subscription for critical alerts
- Sync insight provides:
  - Latency of synchronization objects
  - Synchronization object change trend

Implementing Azure AD Domain Services

Azure AD Domain Services:

- Managed domain services on Azure
- Integrates with Azure AD
- Provides support for directory-aware applications
- Provides support for joining a domain
- Supports NTLM and Kerberos authentication
- Uses organizational credentials and passwords
- Manage by using Group Policy

Demonstration: Implementing directory synchronization by using Azure AD Connect

In this demonstration, you will learn how to:

- Enable directory synchronization
- Install Azure AD Connect by using custom settings
- Synchronize users from on-premises AD DS

Lesson 3: Implementing federation

- 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. A client makes an authentication request to a resource that Azure AD protects
2. The authentication request redirects to the on-premises federation service, typically through a proxy
3. The proxy passes the request to the server that runs the AD FS service; AD FS verifies that the user authenticates successfully against AD DS
4. AD FS creates a token that contains claims about the user
5. AD FS passes that token back to Azure AD
6. Azure AD generates a security token that grants access to the requested resource

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 Multi-Factor Authentication
- 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

- Plan for devices and browsers
- Plan server placement
- Plan scalability
- Plan conditional access
- Plan certificates
- Plan availability
- Plan database servers

Deploying AD FS

- Review account requirements:
  - Existing user accounts
  - gMSAs
- Review namespace requirements
- Review DNS requirements:
  - Host records configured for internal and external DNS
- Review certificate requirements:
  - Token-signing certificate
  - Encryption SSL certificates
- Review firewall requirements
- Review load-balancing requirements:
  - Server farms and proxies

Managing and maintaining AD FS

- Manage AD FS with Azure AD Connect
- Manage the certificate life cycle
- Convert domains to federated
- 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:	**20533C-MIA-CL1**
User name:	**Student**
Password:	**Pa55w.rd**

Estimated Time: 60 minutes

Lab Scenario

A. Datum Corporation users rely on SSO to access on-premises applications. While evaluating Azure for A. Datum, you need to verify that A. Datum users can use their existing credentials to access resources in Azure, including non-Microsoft software as a service (SaaS) applications. You need to verify that any changes to passwords or Active Directory user and group accounts in on-premises Active Directory automatically replicate to Azure AD.

Lab Review

- How do you configure OU-level filtering for directory synchronization?
- When do you use Azure AD Connect custom setup?

Module Review and Takeaways

- Common Issues and Troubleshooting Tips
- Review Question
- Tools