Module 8

Configuring and managing Azure AD

Module Overview

- Overview of Azure AD
- Managing Azure AD authentication and authorization

Lesson 1: Overview of Azure AD

- What is AD DS?
- Implementing AD DS by using Azure VMs
- Overview of Azure AD
- Active Directory synchronization and Azure AD
- Demonstration: Creating and managing an Azure AD tenant
- AD FS and Azure AD

What is AD DS?

- Serves as a core infrastructure component
- Authenticates and authorizes domain users, computers, and Active Directory–aware applications
- Stores management data that you can use to control user and computer settings by using GPOs
- Relies on a secure channel with domain member computers established through a domain join
- Organizes objects into a customizable hierarchy
- Extends the scope of authentication and authorization by using forests and trust relationships

Implementing AD DS by using Azure VMs

- AD DS was designed for on-premises deployments:
  - Single-tenant by design
  - Relies on protocols not suitable for internet communication
  - Requires domain-joined computers to deliver full functionality
- You can install AD DS domain controllers in Azure VMs to:
  - Provide AD DS authentication for Azure VMs
  - Implement separate AD DS or extend existing on-premises AD DS
- You can implement Azure AD DS to:
  - Provide AD DS authentication for Azure VMs as a managed service
  - Synchronize with Azure AD and, optionally, with on-premises AD DS
- You can leverage AD DS to authenticate and authorize mobile devices and cloud-based services

Overview of Azure AD

- Microsoft-managed
- A PaaS offering:
  - Three service and pricing tiers (Free, Basic, and Premium P1 and P2)
- Multitenant by design
- Relies on internet-friendly protocols
- Supports users, groups, applications, and devices
- No organizational units or computer objects
- Does not support Group Policy–based management:
  - Consider using an MDM solution (such as Microsoft Intune)
- No support for forests or trust relationships:
  - Relies on federations to extend scope of authentication

Overview of Azure AD

- Delegation model within an Azure AD tenant:
  - A number of predefined Azure AD roles
  - Support for administrative units (preview)
  - Support for assigning users to applications
- Delegation model within an Azure AD subscription:
  - Built-in and custom RBAC roles are associated with Azure AD identities
  - RBAC role assignments to resources, resource groups, or the subscription
- The Azure AD authentication design models are:
  - Cloud identities: Hosted exclusively in Azure AD
  - Synchronized identities: Hosted in AD DS and synchronized to Azure AD (with password hashes)
  - Synchronized identities: Hosted in AD DS and synchronized to Azure AD, with pass-through authentication and optional Seamless SSO (without password hashes)
  - Federated identities: hosted in AD DS and synchronized to Azure AD (without password hashes)

Active Directory synchronization and Azure AD

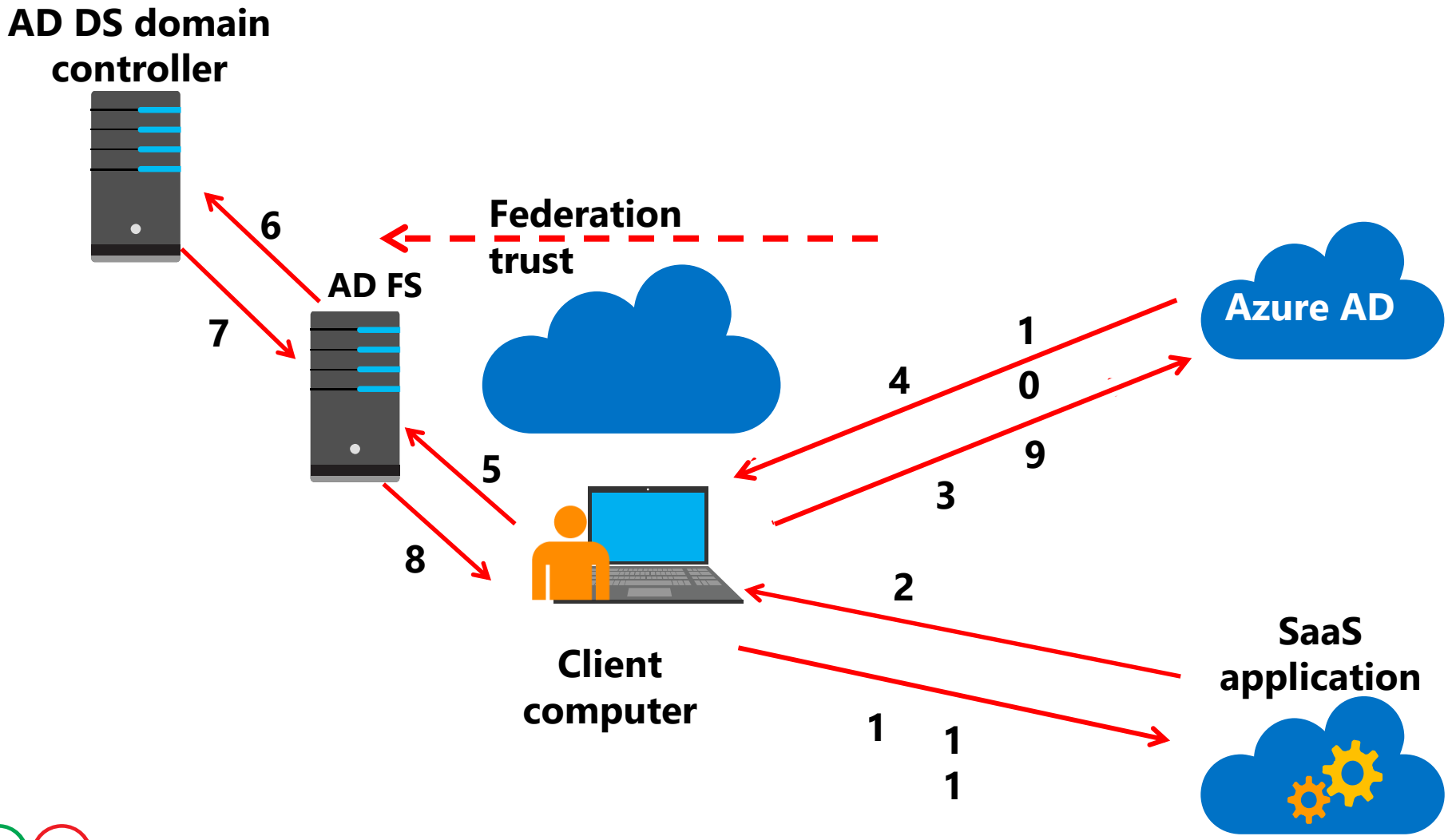
- Directory synchronization
- Directory synchronization with password hash synchronization (same sign-on)
- Directory synchronization with password hash synchronization and Seamless SSO
- Directory synchronization with pass-through authentication and same sign-on
- Directory synchronization with pass-through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

Demonstration: Creating and managing an Azure AD tenant

In this demonstration, you will learn how to:

- Create an Azure AD tenant
- Create a custom DNS domain and view the verification DNS records
- Associate an Azure AD tenant with an Azure subscription
- Create an Azure AD user account
- Grant an Azure AD user administrative access to an Azure subscription by assigning the owner role on the subscription level

AD FS and Azure AD



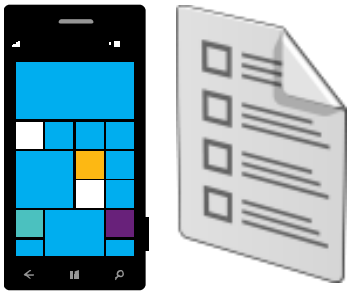
Lesson 2: Managing Azure AD authentication and authorization

- Azure AD Multi-Factor Authentication
- Demonstration: Configuring and using Multi-Factor Authentication
- Azure AD SSO via Access Panel
- Demonstration: Configuring password-based Azure AD SSO
- Azure AD conditional access, Privileged Identity Management, and Identity Protection

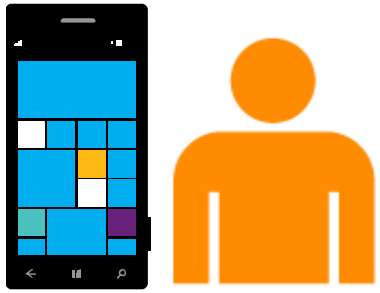
Azure AD Multi-Factor Authentication

Azure Multi-Factor Authentication adds an extra layer of authentication:

- Text message



- Phone call



- Mobile app

Demonstration: Configuring and using Multi-Factor Authentication

In this demonstration, you will learn how to:

- Enable Multi-Factor Authentication for an Azure AD user account
- Authenticate to the Azure portal as an Azure AD user with Multi-Factor Authentication enabled

Azure AD SSO via Access Panel

- You can use the following three mechanisms to implement application SSO support:
  - Password-based SSO
  - Federated SSO
  - Existing SSO
- The Access Panel (available at http://myapps.microsoft.com) offers the following functionality:
  - Application access
  - Self-service group management
  - User profile editing
  - Password changes
  - Configuring password resets
  - Setting up Multi-Factor Authentication

Demonstration: Configuring password-based Azure AD SSO

In this demonstration, you will learn how to:

- Add a gallery application to an Azure AD tenant
- Assign a registered application to an Azure AD user

Azure AD conditional access, Privileged Identity Management, and Identity Protection

- Conditional access (requires Premium P1):
  - Consists of:
    - Assignment conditions (user or group, client app, sign-in risk, device platform, device state, location)
    - Access controls (require multi-factor authentication, device marked as compliant, Azure AD–joined device, approved client app)
- Privileged Identity Management (requires Premium P2):
  - Identifies administrative users
  - Enables on-demand, just-in-time administrative access
  - Generates reports about administrator access history
- Identity Protection (requires Premium P2):
  - Monitors identity usage patterns
  - Assigns risk levels to users
  - Implements risk-based policies

Lab: Creating and managing Azure Active Directory

Logon Information

Virtual machine:	**10979F-MIA-CL1**
User name:	**Admin**
Password:	**Pa55w.rd**

Estimated Time: 30 minutes

Lab Scenario

Now that you have deployed several services for Azure, you must provide secure access to them by provisioning Azure AD user accounts for employees of Adatum Corporation. In the long term, you want to synchronize existing on-premises AD DS user accounts with the Azure AD Default Directory tenant associated with your Azure subscription. However, you first want to test Azure AD functionality by creating and configuring Azure AD user accounts. You also plan to test RBAC by delegating permissions to one of these accounts. In addition, you intend to create a new Azure AD tenant to use for further testing of Azure AD functionality. You will assign a custom DNS domain name to this tenant.

Lab Review

- What role should you assign to a user account in an Azure AD tenant to enable the user to fully manage all of its objects?

Module Review and Takeaways

- Review Question
- Tools

Course Evaluation

- Your evaluation of this course will help Microsoft understand the quality of your learning experience.
- Please work with your training provider to access the course evaluation form.
- Microsoft will keep your answers to this survey private and confidential and will use your responses to improve your future learning experience. Your open and honest feedback is valuable and appreciated.