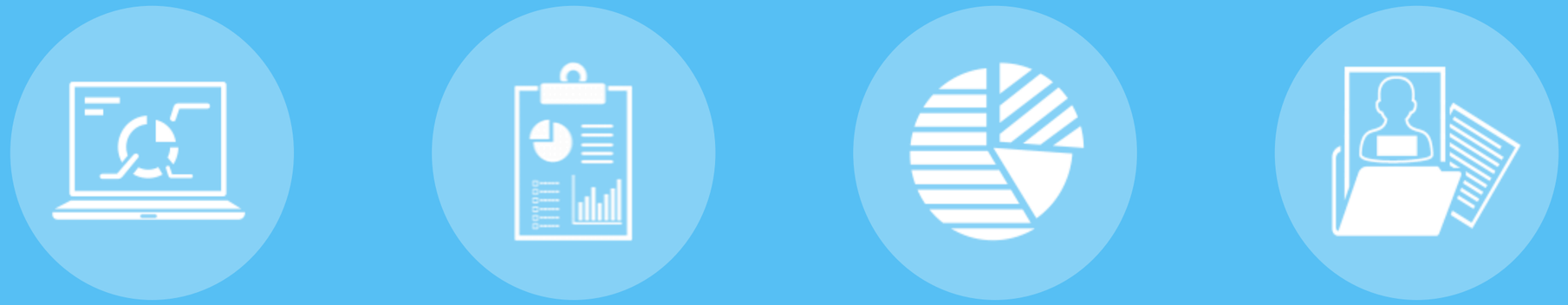
Microsoft Azure Fundamentals

Lesson 08 – Creating and Managing Azure AD



What's in It for Me

- Overview of Azure AD
- Manage Azure AD authentication

Overview of Azure AD

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

What is Active Directory Domain Services?

- 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 Group Policy Objects (GPOs)
- Relies on a secure channel with domain member computers established through domain join
- Organizes objects into a customizable hierarchy
- Extends the scope of authentication and authorization by using forests and trust relationships

Implementing AD DS in Azure

- 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 install AD DS Domain Controllers in Azure virtual machines to:
  - Utilize an AD DS domain that you manage
  - Utilize a separate AD DS or your on-premises AD DS
- You can implement Azure AD DS to:
  - Utilize a separate AD DS domain that is 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 platform as a service offering:
    - Three service and pricing tiers (Free, Basic, Premium)
- Multi-tenant 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 Azure AD tenant:
    - Several predefined Azure AD roles
    - Permissions based on users, groups, and applications
    - Assigned applications automatically accessible via Access Panel
- Delegation model within Azure AD subscription:
    - Role-based access control (RBAC) using Azure AD principals
    - Predefined and custom roles
    - Roles assigned on the resource, resource group, or subscription level
- Native support for Multi-Factor Authentication
- Azure AD identity types:
    - Cloud identity
    - Synchronized identity
    - Federated identity

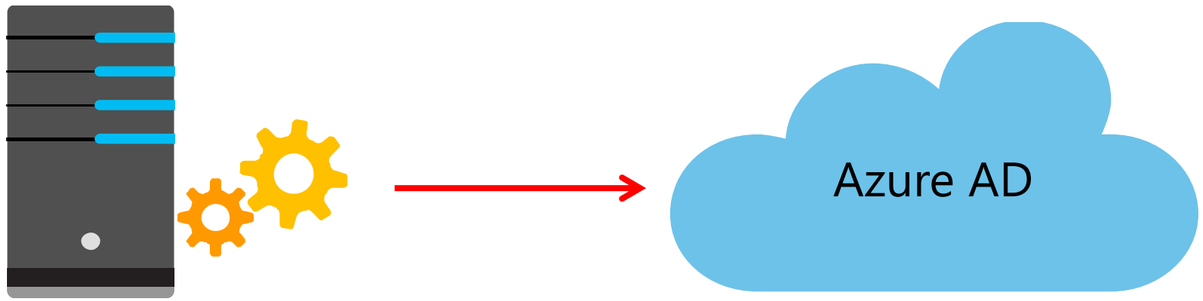
Demonstration: Creating and Managing an Azure AD Tenant

In this demonstration, you will learn how to:

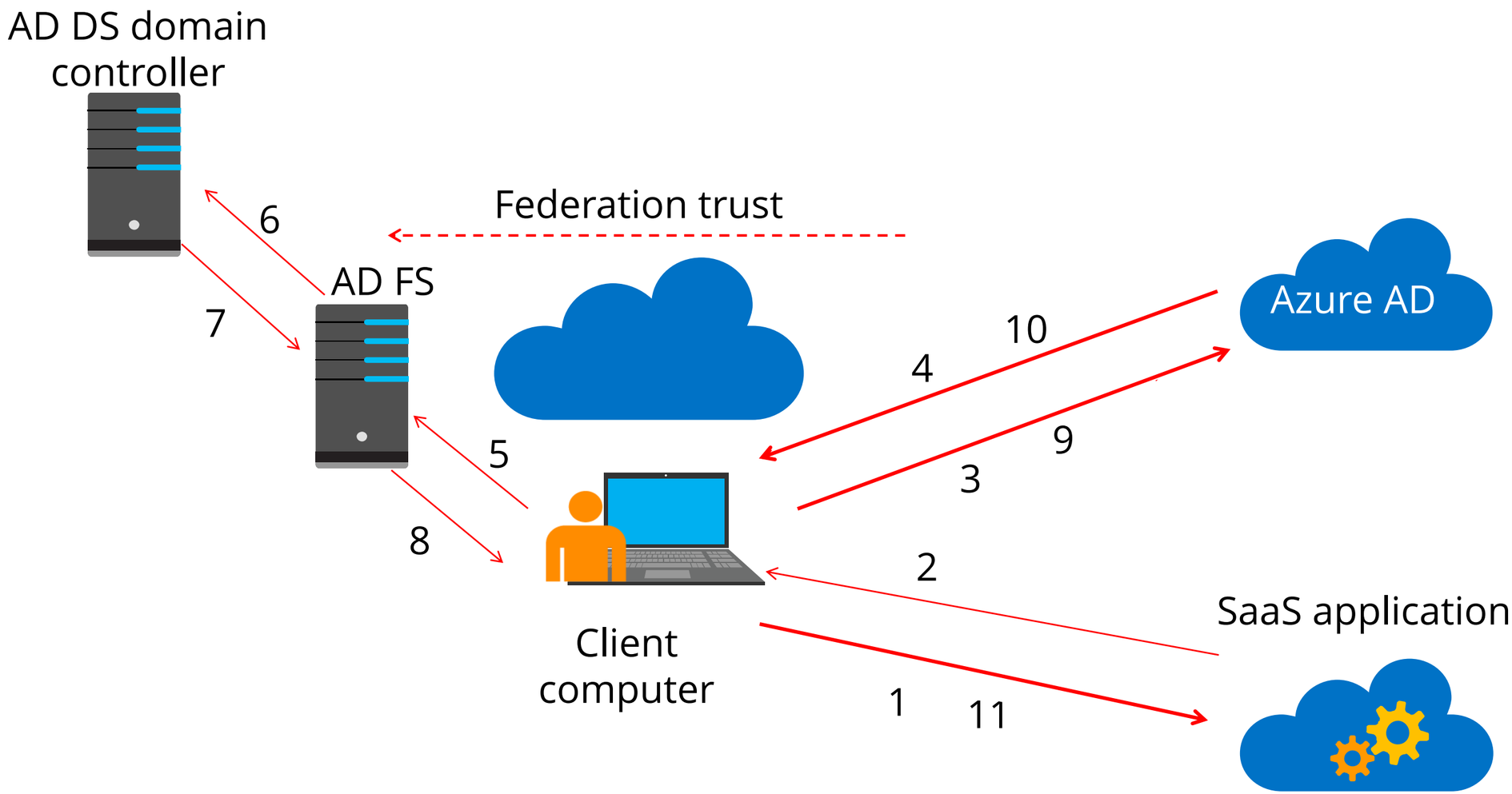
- Create an Azure AD tenant, assign to it a custom domain, and view the verification DNS records
- Associate an Azure AD instance with the current Azure subscription
- Create an Azure AD user account
- Grant an Azure AD user access to an Azure subscription

Active Directory Synchronization and Azure AD

- Directory synchronization tool (AAD Connect) synchronizes objects between AD DS and Azure AD
- Cloud-based users can use Password Hash Synchronization to minimize password related issues
- Federated users scenario:
  - Uses an STS (For example, AD FS) to perform authentication
  - Eliminates password related issues (SSO)



AD FS and Azure AD



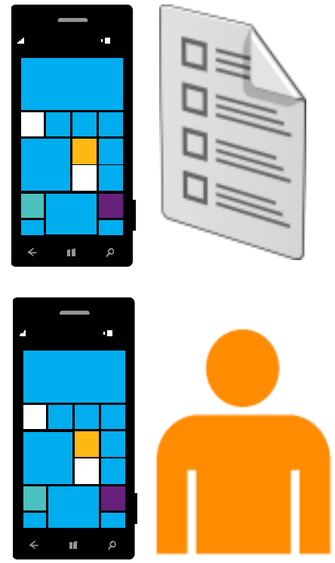
Manage Azure AD Authentication

- Multi-Factor Authentication
- Demonstration: Configuring and using Multi-Factor Authentication
- SSO via Access Panel
- Demonstration: Configure Password-based SSO

Multi-Factor Authentication

Azure Multi-Factor Authentication adds a second level 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

SSO via Access Panel

Single Sign-On implementations:

- Password-based SSO:
  - Administrator managed credentials
  - User managed credentials
- Azure AD SSO
- Existing SSO

Azure AD Access Panel:

- Lists all applications assigned to a user
- Implements SSO
- Relies on Access Panel Extension browser add-on for password-based SSO

Demonstration: : Configure Password-based SSO

In this demonstration, you will learn how to:

- Add a directory application
- Assign a directory application to a user

Key Takeaways

- Azure Active Directory Domain Services was designed for on-premise deployments.
- You can use Azure AD DS to authenticate and authorize mobile devices and cloud-based services.
- Azure AD does not support group policy-based management.
- Azure AD connect synchronizes objects between AD DS and Azure AD.
- The purpose of Multi-Factor Authentication is to increase security.
- SSO allows users to access Azure AD applications without having to provide a user name and password if they have already successfully authenticated.

This concludes the course “Microsoft Azure Fundamentals.”

Happy Learning!

THANK YOU