Module 9

Implementing Azure Active Directory

Module Overview

- Creating and managing Azure AD tenants
- Configuring application access with Azure AD
- Overview of Azure AD Premium

Lesson 1: Creating and managing Azure AD tenants

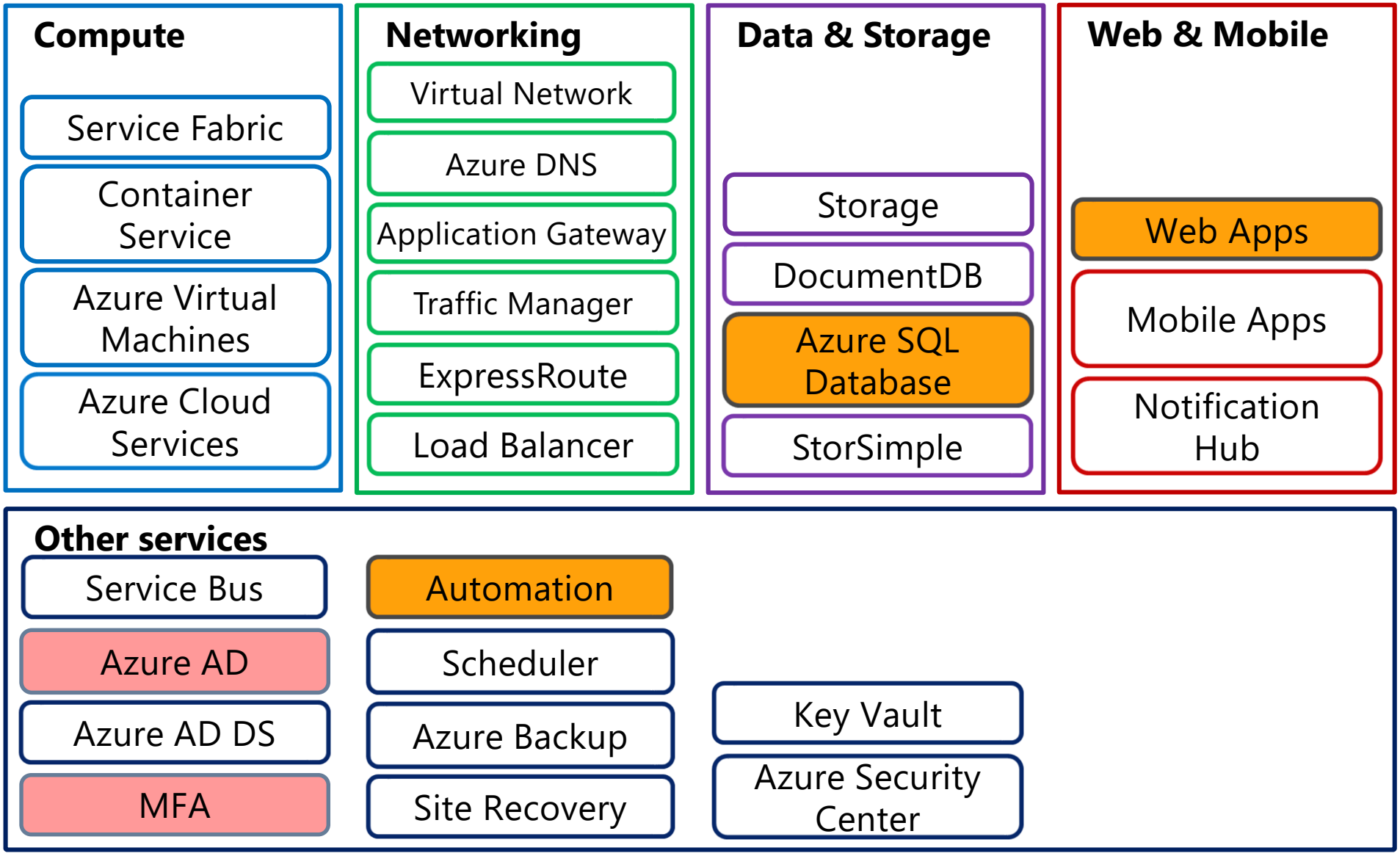
- Demonstration: Preparing the lab environment
- Active Directory as a component of Azure
- Overview of Azure AD
- Managing Azure AD users, groups, and devices
- Managing Azure AD tenants
- Implementing Azure AD B2B and Azure AD B2C
- Demonstration: Managing Azure AD users, groups, and devices

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

Active Directory as a component of Azure



Overview of Azure AD

- Microsoft-managed
- A platform as a service offering
- Multitenant by design
- Employs internet-friendly protocols
- Supports users, groups, applications, and devices
- No organizational units
- No support for GPO-based computer or user management:
  - Consider using an MDM solution (such as Microsoft Intune)
- Includes built-in MFA support
- No support for forests:
  - Relies on federations to extend scope of authentication

Managing Azure AD users, groups, and devices

- Azure AD users:
  - Cloud identities
  - Directory-synchronized identities
  - Guest users
- Management interfaces:
  - Azure portal
  - Windows PowerShell
    - Microsoft Azure Active Directory V2 PowerShell
    - MSOnline V1 PowerShell module for Azure Active Directory
  - Microsoft Intune admin console
  - Office 365 admin center

Managing Azure AD tenants

- Create multiple Azure AD tenants:
  - Separate production, test, and development environment
  - Consider adding existing users as guests
- Associate multiple cloud services and multiple Azure subscriptions with the same Azure AD tenant:
  - Consistent set of identities without the need for guest users
- To delete an Azure AD tenant:
  - Use a guest user with the Global admin role
  - Delete all users
  - Delete all applications
  - Remove associations with cloud services
  - Remove links to MFA providers

Implementing Azure AD B2B and Azure AD B2C

- Azure AD Business to Business (B2B)
  - sharing resources with a partner organization
  - two types of user accounts:
    - user accounts of employees of the host organization
    - guest accounts representing user accounts in the partner organization (support for any identity provider)
  - Support for SSO to all Azure AD-connected apps
  - Multi-factor authentication to hosted apps
- Azure AD Business to Consumer (B2C)
  - IDaaS for your applications
  - dedicated Azure AD tenant
  - customer user accounts only:
    - local accounts defined directly in the tenant
    - any identity provider, including social identities

Demonstration: Managing Azure AD users, groups, and devices

In this demonstration, you will learn how to:

- Create a new directory called Adatum
- Create a new Global Administrator user account
- Join a Windows 10-based computer to Azure AD

Lesson 2: Configuring application access with Azure AD

- Adding publicly accessible applications to Azure AD
- Adding on-premises applications to Azure AD
- Configuring access to Azure AD–integrated applications
- Implementing RBAC
- Demonstration: Integrating SaaS apps with Azure AD and configuring RBAC

Adding publicly accessible applications to Azure AD

Enterprise applications in the Azure portal:

- Add SaaS application from the Azure Marketplace:
  - more than 2,900 SaaS applications
  - automatic user provisioning (some apps)
  - SSO
- Add SaaS applications not listed in the Azure Marketplace:
  - Certificate-based:
    - SAML (directly from the portal)
    - WS-Federation
    - OpenID Connect
  - Password-based SSO:
    - HTML-based sign-in page

Adding on-premises applications to Azure AD

- Azure AD-based access to internal browser-based applications, such as:
  - SharePoint sites
  - Outlook Web Access
  - IIS-based applications
- Requirements:
  - An on-premises connector
  - Outbound connectivity on TCP 80 and 443
  - Basic or Premium edition of Azure AD

Configuring access to Azure AD–integrated applications

- Single Sign-On for SaaS apps
  - Password-based SSO
  - Federated SSO
  - Existing SSO
- Access Panel at http://myapps.microsoft.com
  - Application access
  - Self-service group management
  - User profile editing
  - Password changes
  - Configuring password resets
  - Setting up MFA

Implementing RBAC

- RBAC built-in roles:
  - Owner
  - Contributor
  - Reader
- RBAC custom roles:
  - Implement via Azure PowerShell or Azure CLI
  - Share across Azure subscriptions
- Manage role assignments by using:
  - The Azure portal
  - Azure PowerShell
  - Azure CLI

Demonstration: Integrating SaaS apps with Azure AD and configuring RBAC

In this demonstration, you will learn how to:

- Add a directory application and configure SSO
- Implement Role-Based Access Control

Lesson 3: Overview of Azure AD Premium

- Introducing Azure AD Premium
- Azure Multi-Factor Authentication
- Exploring advanced Multi-Factor Authentication settings
- Demonstration: Configuring and using Azure AD Premium Multi-Factor Authentication
- Azure AD Privileged Identity Management and Identity Protection

Introducing Azure AD Premium

The following features are available with the Azure AD Premium edition:

- Self-service group and app management
- Dynamic groups
- Conditional access
- Advanced security reports and alerts
- Multi-Factor Authentication
- MIM licensing
- Enterprise SLA of 99.9 percent
- Self-service password reset and account unlock with writeback
- Device writeback
- Cloud App Discovery
- Cloud App Security proxy
- Azure AD Connect Health
- Identity Protection and Privileged Identity Management
- Windows 10 Azure AD Join features

Azure Multi-Factor Authentication

- Azure MFA versions:
  - MFA for Azure administrators
  - Azure MFA licensed offers:
    - Azure AD Premium
    - Azure MFA
    - EMS
  - Azure MFA provider
  - MFA for Office 365
- Azure MFA deployments:
  - MFA in the cloud
  - MFA on-premises server

Exploring advanced Multi-Factor Authentication settings

- Fraud Alert
- One-Time Bypass
- Custom Voice Messages
- Trusted IPs
- App Passwords
- Remember Multi-Factor Authentication for trusted devices
- Caching
- Require selected users to provide contact methods again
- Delete all existing app passwords generated by the selected users
- Restore multi-factor authentication on all remembered devices

Demonstration: Configuring and using Azure AD Premium Multi-Factor Authentication

In this demonstration you will learn how to:

- Create a Multi-Factor Authentication provider
- Configure fraud alerts
- View fraud alert reports
- Configure one-time bypass settings
- Create a one-time bypass
- Configure trusted IP addresses
- Enable users to create app passwords

Azure AD Privileged Identity Management and Identity Protection

- Azure AD Privileged Identity Management:
  - Identifies administrative users
  - Enables on-demand, just-in-time administrative access
  - Generates reports about administrator access history
- Azure AD Identity Protection:
  - Monitors identity usage patterns
  - Assigns risk levels to users
  - Implements risk-based policies
- Azure AD Premium P2 required

Lab: Implementing Azure AD

- Exercise 1: Administering Azure AD
- Exercise 2: Configuring SSO
- Exercise 3: Configuring Multi-Factor Authentication
- Exercise 4: Configuring SSO from a Windows 10–based computer

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

Estimated Time: 60 minutes

Lab Scenario

The IT department at Adatum Corporation currently uses AD DS, and a range of Active Directory–aware applications. While preparing for synchronizing its AD DS to Azure AD, A. Datum wants you to test some of the features of Azure AD. The company wants you to evaluate Azure AD control mechanisms that restrict access to third-party SaaS apps by individual Azure AD users and groups. A. Datum also wants you to configure SSO for these apps and protect them by using Multi-Factor Authentication.

In addition to these tasks, Adatum wants you to evaluate some of the advanced features Azure AD Premium offers. In particular, you will need to test joining a Windows 10–based computer to an Azure AD tenant to prepare for implementing this configuration on all the Windows 10–based computers in the Research department.

Lab Review

- What is the major benefit of joining Windows 10–based devices to Azure AD?
- What is the requirement for Delegated Group Management in Azure AD?

Module Review and Takeaways

- Review Question
- Tools
- Best Practice
- Common Issues and Troubleshooting Tips