Module 9

Implementing Azure Active Directory

Module Overview

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

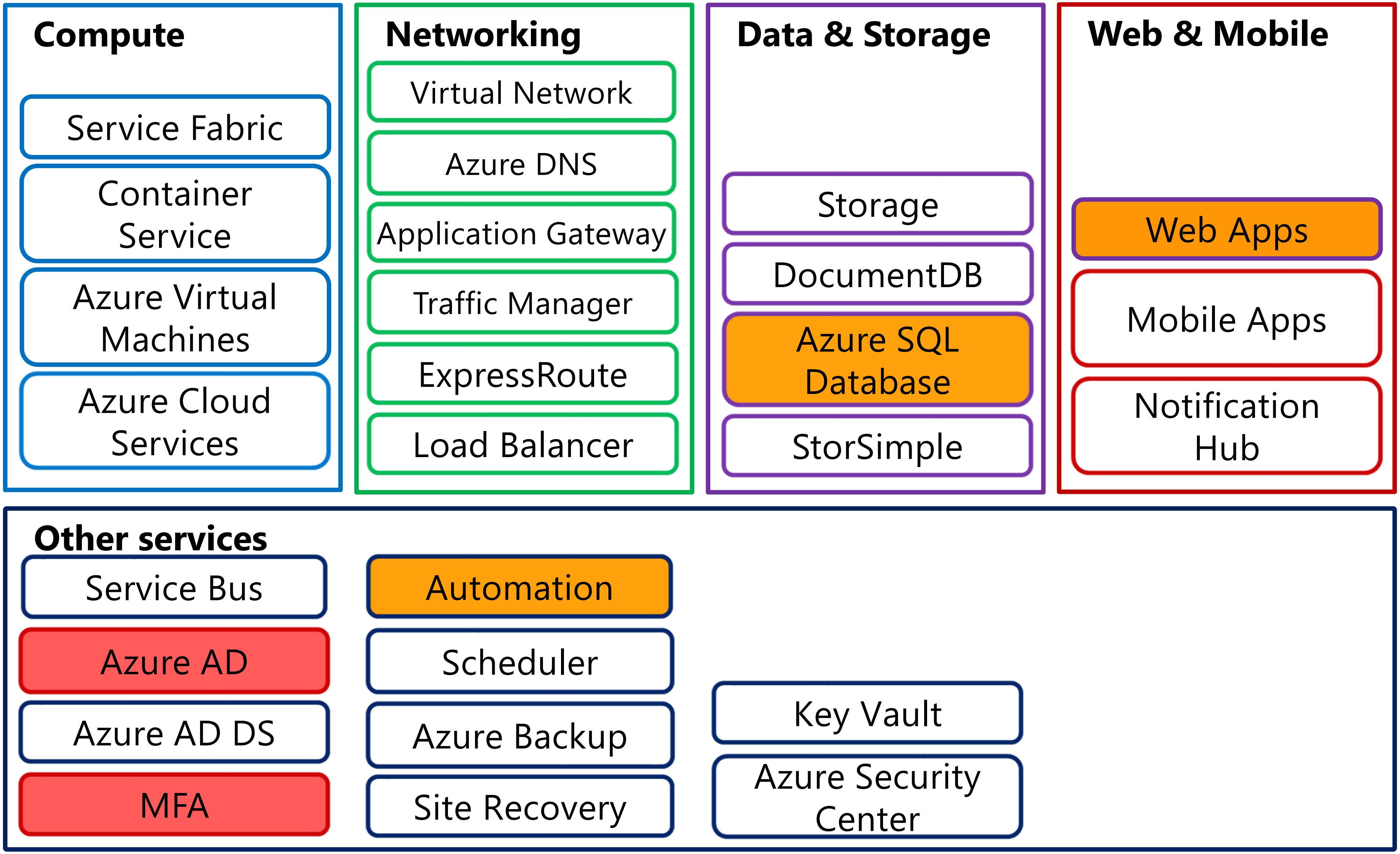
Lesson 1: Creating and managing Azure AD tenants

- Demonstration: Preparing the Microsoft Azure environment for the lab and demonstrations in this module
- Active Directory as a component of Azure
- Overview of Azure AD
- Managing Azure AD users, groups, and devices
- Managing multiple Azure AD tenants
- Implementing Azure AD B2B and Azure AD B2C
- Demonstration: Managing Azure AD users, groups, and devices

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

In this demonstration, you will see how to prepare the Azure environment for the lab and demos in this module

Active Directory as a component of Azure



Compute

- Service Fabric
- Container Service
- Azure Virtual Machines
- Azure Cloud Services

Networking

- Virtual Network
- Azure DNS
- Application Gateway
- Traffic Manager
- ExpressRoute
- Load Balancer

Data & Storage

- Storage
- DocumentDB
- Azure SQL Database
- StorSimple

Web & Mobile

- Web Apps
- Mobile Apps
- Notification Hub

Other services

- Service Bus
- Azure AD
- Azure AD DS
- MFA
- Automation
- Scheduler
- Azure Backup
- Site Recovery
- Key Vault
- Azure Security Center

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 or computer objects
- Does not support Group Policy objects
- No support for forests, relies on federations to extend scope of authentication and authorization
- Delegation model based on Role-based Access Control
- Easily extensible, includes multi-factor authentication support
- Provides authentication and authorization:
  - Cloud identity
  - Synchronized identity
  - Federated identity

Managing Azure AD users, groups, and devices

User tasks:

- Add, edit, delete a user
- Reset user's password

Group tasks:

- Add, edit, delete a group
- Manage group membership

Tools:

- The Azure portal
- Windows PowerShell
- Bulk creation and editing by using a CSV file

Managing multiple Azure AD tenants

Uses for multiple directories:

- Live directory
- Test directory
- Sync directory

Multiple cloud services can use Azure AD for authentication and authorization:

- Azure
- Office 365
- Intune

You can add users from one directory to another directory

Implementing Azure AD B2B and Azure AD B2C

Azure AD Business to Business (B2B)

- Provides simple and secure sharing of data and applications
- Works with partners that have their own Azure AD tenant and with partners that do not have an Azure AD tenant
- Requires a company to federate only once with Azure AD

Azure AD Business to Consumer (B2C)

- Provides Identity as a Service for applications
- Supports standard protocols, such as OpenID Connect and OAuth 2.0
- Supports identity management by using social accounts such as Facebook, Google, and LinkedIn

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 and resource access with Azure AD

- Overview of managing cloud applications
- Integrating applications with Azure AD
- Implementing access to on-premises applications
- Implementing RBAC
- Azure AD Privileged Identity Management
- Demonstration: Integrating SaaS apps with Azure AD and configuring RBAC

Overview of managing cloud applications

- Enable SSO for apps
- Use centralized application access management
- Grant access to users and groups from Azure AD or from AD DS
- Use unified reporting and monitoring
- Use the Application Access Panel

  http://myapps.microsoft.com
- Find SaaS apps by using the Cloud App Discovery tool
- Implement conditional access

Integrating applications with Azure AD

- Add an application from the Azure AD application gallery
  - http://azure.microsoft.com/en-us/gallery/active-directory/
- Add a custom LOB application in Azure AD:
  - Register the web app in the Azure AD tenant
  - Add logic or code to the web app:
    - Block and redirect unauthenticated request
    - Grant access to authenticated requests
- Add a SaaS application that is not listed in the Azure AD application gallery:
  - Register the web app in the Azure AD tenant
  - Configure SSO with Azure AD
  - Assign users and groups to the application

Implementing access to on-premises applications

- Use Azure AD to manage access to internal browser-based applications, such as:
  - SharePoint sites
  - Outlook Web Access
  - IIS-based applications
- Azure AD Application Proxy
  - Requires a connector installed in the on-premises infrastructure
  - Makes apps available to authenticated users only
  - Uses a cloud proxy hosted in Azure

Implementing RBAC

RBAC built-in roles

- Owner
- Contributor
- Reader

You can manage RBAC by using:

- The Azure portal
- Azure PowerShell in the Resource Manager mode
- Azure command-line interface

```
New-AzureRmRoleAssignment -UserPrincipalName
user@somedomain.com -RoleDefinitionName Reader -Scope
/subscriptions/GUID/resourceGroups/ResourceGroupName
```

Azure AD Privileged Identity Management

- Discover which users are the Azure AD administrators
- Enable on-demand, just-in-time administrative access to directory resources
- Get reports about administrator access history and the changes in administrator assignments
- Get alerts about access to a privileged role

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

Introducing Azure AD Premium

Features of Azure AD Premium:

- Self-service group management
- Advanced security reports and alerts
- Multi-Factor Authentication
- Microsoft Identity Manager (MIM)
- Enterprise SLA of 99.9 percent
- Self-service password reset with writeback
- Cloud App Discovery
- Azure AD Connect Health

Azure Multi-Factor Authentication

Azure Multi-Factor Authentication requires additional form of authentication:

- Mobile app authentication
- Phone call
- Text message
- Email message
- Third party OAuth token

Multi-factor security solution:

- For cloud-only apps
- For on-premises applications

Technical scenarios for Azure Multi-Factor Authentication

You can use Azure Multi-Factor Authentication:

- To provide multi-factor authentication for Office 365
- For federated users
- With Remote Desktop Gateway by using RADIUS
- With Active Directory Federation Services

Configuring advanced Multi-Factor Authentication settings

- Fraud Alert
- One-Time Bypass
- Custom Voice Messages
- Trusted IPs
- App Passwords
- Caching
- Suspend Multi-Factor Authentication
- Require selected users to provide contact methods again
- Delete users existing password
- Restore MFA on all suspended devices for a user

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

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 that is joined to Azure AD

Estimated Time: 60 minutes

Lab Scenario

The IT department at A. Datum 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 control access to third-party SaaS apps by using Azure AD users and groups. A. Datum also wants you to configure SSO to these apps and protect them by using Multi-Factor Authentication.

In addition to these tasks, A. Datum wants you to evaluate some of the advanced features Azure AD Premium offers. Additionally, it wants you join a Windows 10–based computer to an Azure AD tenant to test the Azure AD functionality and 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 Practices
- Common Issues and Troubleshooting Tips