Course Outline

SC-300T00-A: Microsoft Identity and Access Administrator

Course Summary

Description

This course provides IT Identity and Access Professional, along with IT Security Professional, with the knowledge and skills needed to implement identity management solutions based on Microsoft Azure AD, and it connected identity technologies. This course includes identity content for Azure AD, enterprise application registration, conditional access, identity governance, and other identity tools.

Objectives

At the end of this course, students will be able to:

- Implement an identity management solution
- Implement an authentication and access management solutions
- Implement access management for apps
- Plan and implement an identity governancy strategy

Topics

- Implement an identity management solution
- Implement an authentication and access management solution
- Implement access management for Apps
- Plan and implement an identity governancy strategy

Audience

This course is for the Identity and Access Administrators who are planning to take the associated certification exam, or who are performing identity and access administration tasks in their day-to-day job. This course would also be helpful to an administrator or engineer that wants to specialize in providing identity solutions and access management systems for Azure-based solutions; playing an integral role in protecting an organization.

Prerequisites

Successful learners will have prior knowledge and understanding of:

- Security best practices and industry security requirements such as defense in depth, least privileged access, shared responsibility, and zero trust model.
- Be familiar with identity concepts such as authentication, authorization, and active directory.
- Have some experience deploying Azure workloads. This course does not cover the basics of Azure administration, instead the course content builds on that knowledge by adding security specific information.
- Some experience with Windows and Linux operating systems and scripting languages is helpful but not required. Course labs may use PowerShell and the CLI.

Prerequisite courses (or equivalent knowledge and hands-on experience):
This free online training will give you the experience you need to be successful in this course.

- SC-900 part 1: Describe the concepts of security, compliance, and identity - Learn | Microsoft Docs
- SC-900 part 2: Describe the capabilities of Microsoft Identity and access management solutions - Learn | Microsoft Docs
- SC-900 part 3: Describe the capabilities of Microsoft security solutions - Learn | Microsoft Docs
- SC-900 part 4: Describe the capabilities of Microsoft compliance solutions - Learn | Microsoft Docs
- AZ-104: Manage identities and governance in Azure - Learn | Microsoft Docs

Duration

Four days

Course Outline

SC-300T00-A: Microsoft Identity and Access Administrator

Course Outline

I. Implement an identity management solution

Learn to create and manage your initial Azure Active Directory (Azure AD) implementation and configure the users, groups, and external identities you will use to run your solution.

A. Implement Initial configuration of Azure AD
B. Create, configure, and manage identities
C. Implement and manage external identities
D. Implement and manage hybrid identity

- Lab : Manage user roles
- Lab : Setting tenant-wide properties
- Lab : Assign licenses to users
- Lab : Restore or remove deleted users
- Lab : Add groups in Azure AD
- Lab : Change group license assignments
- Lab : Change user license assignments
- Lab : Configure external collaboration
- Lab : Add guest users to the directory
- Lab : Explore dynamic groups

II. Implement an authentication and access management solution

Implement and administer your access management using Azure AD. Use MFA, conditional access, and identity protection to manager your identity solution.

A. Secure Azure AD user with MFA
B. Manage user authentication
C. Plan, implement, and administer conditional access
D. Manage Azure AD identity protection

- Lab : Enable Azure AD MFA
- Lab : Configure and deploy self-service password reset (SSPR)
- Lab : Work with security defaults
- Lab : Implement conditional access policies, roles, and assignments
- Lab : Configure authentication session controls
- Lab : Manage Azure AD smart lockout values
- Lab : Enable sign-in risk policy
- Lab : Configure Azure AD MFA authentication registration policy

III. Implement access management for Apps

Explore how applications can and should be added to your identity and access solution with application registration in Azure AD.

A. Plan and design the integration of enterprise for SSO
B. Implement and monitor the integration of enterprise apps for SSO
C. Implement app registration

- Lab : Implement access management for apps
- Lab : Create a custom role to management app registration
- Lab : Register an application
- Lab : Grant tenant-wide admin consent to an application
- Lab : Add app roles to applications and recieve tokens

IV. Plan and implement an identity governancy strategy

Design and implement identity governance for your identity solution using entitlement, access reviews, privileged access, and monitoring your Azure Active Directory (Azure AD).

A. Plan and implement entitlement management
B. Plan, implement, and manage access reviews
C. Plan and implement privileged access
D. Monitor and maintain Azure AD

- Lab : Creat and manage a resource catalog with Azure AD entitlement
- Lab : Add terms of use acceptance report
- Lab : Manage the lifecycle of external users with Azure AD identity governance
- Lab : Create access reviews for groups and apps
- Lab : Configure PIM for Azure AD roles
- Lab : Assign Azure AD role in PIM
- Lab : Assign Azure resource roles in PIM
- Lab : Connect data from Azure AD to Azure Sentinel