

Microsoft Identity and Access Administrator (SC-300T00)

Duration: 4 days

Audience: Professionnel TI

Who is this training for?

This course is intended for Identity and Access Administrators who plan to take the associated certification exam, or who perform Identity and Access Administration tasks in their day-to-day work.

This course would also be useful for an administrator or engineer who wants to specialize in providing identity solutions and access management systems for Azure-based solutions, thus playing a critical role in protecting an organization.

Training objectives

- Implement an identity management solution • Implement an authentication and access management solution
- Implement access management for applications
- Plan and implement an identity governance strategy

Summary

This course provides identity and access IT professionals, as well as security IT professionals, with the knowledge and skills to implement identity management solutions based on Microsoft Azure AD and connected identity technologies. This course includes content on identity for Azure AD, enterprise application registration, Conditional Access, identity governance, and other identity tools.

Course outline

Learning Path 1: Implement an Identity Management Solution

- Implement the initial setup of Microsoft Entra ID
- Create, configure, and manage identities
- Implement and manage external identities
- Implement and manage hybrid identities

Learning Path 2: Implement an authentication and access management solution

- Secure Microsoft Entra users with multi-factor authentication (MFA)
- Manage User authentication
- Plan, implement, and administer Conditional Access
- Manage Microsoft Entra identity protection Learning

Path 3: Implement access management for apps

- Plan and design enterprise app integration for SSO
- Implement and monitor enterprise app integration for SSO
- Implement app registration

Learning path 4: Plan and implement an identity governance strategy

- Plan and implement entitlement management
- Plan, implement, and manage access reviews
- Plan and implement privileged access
- Monitor and maintain Microsoft Entra ID Learning

Path 5: Labs

- Manage user roles
- Configure and deploy self-service password reset (SSPR)
- Use security labels to implement Conditional Access
- Manage Azure resources using Azure RBAC
- Add a hybrid tenant with Microsoft Entra Connect
- Grant tenant-level admin consent to an app

- Secure user security information registration with required authentication methods
- Configure authentication for an Azure App Service app
- Create and manage a resource catalog in Azure App Service entitlement management Microsoft Entra
- Add conditions to terms of use and acceptance
- Configure and test a Conditional Access policy
- Configure a Microsoft Entra identity protection user risk policy
- Configure and deploy a custom app using an app governance model
- Configure registration and governance settings for an app
- Delegate identity administration
- Implement Multi-Factor Authentication (MFA)
- Create an Access Review for Groups and Applications

Approach and methodology

Practical and structured approach combining focused theory and guided workshops.

Participants gradually administer Microsoft identities and access through real-world exercises inspired by professional scenarios, promoting immediate application of learning. They learn how to manage identities, secure access, implement authentication and governance with Microsoft Entra ID.

Led by a Microsoft certified trainer, the training focuses on interactivity and the development of directly transferable technical skills to effectively protect resources and users in a professional context.

Prerequisites

Successful students 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 the zero trust model.
- Be familiar with identity concepts such as authentication, authorization, and active directory.
-

Have some experience deploying Azure workloads. This course doesn't cover the basics of Azure administration, but the course content builds on this knowledge by adding security-specific information.

- Some experience with Windows and Linux operating systems and scripting languages is helpful but not required.
- Labs in the course can use PowerShell and the CLI.

Recommendations

- Fundamentals in identity and access management (IAM)
- Knowledge of Microsoft Entra ID (Azure AD)
- Understanding of security concepts (authentication, MFA, conditional access)
- Notions of Microsoft 365 or Azure environments

Certifications

This course is for identity and access administrators who plan to take the associated certification exam.