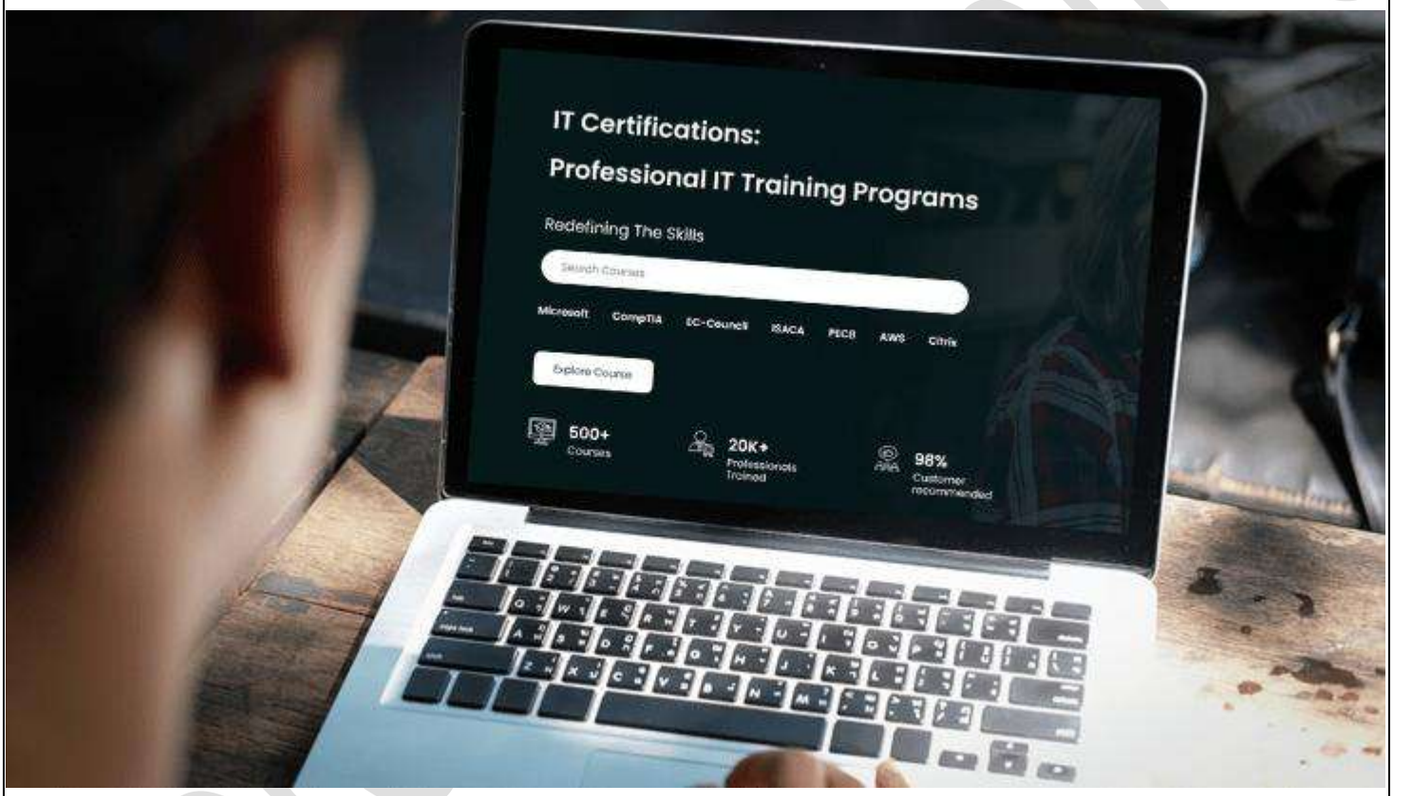
MICROTEK LEARNING | Redefining The Skills



SC-300: MICROSOFT IDENTITY & ACCESS ADMINISTRATOR TRAINING

Duration: 4 Days

Course Description

SC-300: Microsoft Identity & Access Administrator Training course is designed for identity and access administrators who are already performing. This course requires implementing identity management solutions. These solutions are based on the Microsoft Azure AD.

This course also involves the identity content for Azure AD, enterprise application registration, conditional permissions, identity, governance, and other tools related to identity.

Given below are some of the basic skills professionals will be learning:

- Implementing on an identity management solution
- Implementing authentication and access management program
- Access management for applications
- Strategies for identity governance

After completing this course, professionals will find themselves as identity and access administrators and security engineers.

Who should attend this course?

- This course is designed for Identity and Access Administrators who are willing to upskill their current position by taking associated certification exams and are currently performing.
- This course is also helpful to an administrator or engineer who is looking to specialize in providing identity solutions and access management systems for Azure-based solutions.
- Given below are professionals who can use SC-300: Microsoft Identity & Access Administrator Training to upskill their current positions:
    - System Administrators
    - Identity and Access Administrators
    - Azure Administrators
    - IT Security Professionals
    - Network Administrators
    - IT Support Staff
    - Cloud Solution Architects
    - Security Engineers
    - Enterprise Architects

What you will learn

- Implementing an identity management solution
- Implementing access management for applications
- Implementing authentication and access management solutions
- Planning and implementing an identity governance strategy

Prerequisites

- Familiar with the security best practices and industry security requirements that can include defense in depth, least privileged access, shared responsibility, and zero trust model.
- Familiarity with identity concepts such as authentication, authorization, and active directory.
- Having experience in deploying Azure workloads.
- Please note this course does not cover the basics of Azure Administration, instead, the course content builds on that knowledge by adding security-specific information.

- Experience with Windows and Linux Operating Systems and scripting languages is an advantage but not required.

Curriculum

Module 1: Explore identity in Microsoft Entra ID

- Define common identity terms and explain how they're used in the Microsoft Cloud
- Explore the common management tools and needs of an identity solution
- Review the goal of Zero Trust and how it's applied in the Microsoft Cloud
- Explore the available identity services in the Microsoft Cloud

Module 2: Implement an identity management solution

- Implement initial configuration of Microsoft Entra ID
  - Implement initial configuration of Microsoft Entra ID.
  - Create, configure, and manage identities.
  - Implement and manage external identities (excluding B2C scenarios).
  - Implement and manage hybrid identity.
- Create, configure, and manage identities
  - Create, configure, and manage users
  - Create, configure, and manage groups
  - Manage licenses
  - Explain custom security attributes and automatic user provisioning
- Implement and manage external identities
  - Manage external collaboration settings in Microsoft Entra ID
  - Invite external users (individually or in bulk)
  - Manage external user accounts in Microsoft Entra ID
  - Configure identity providers (social and SAML/WS-fed)
- Implement and manage hybrid identity
  - Plan, design, and implement Microsoft Entra Connect
  - Manage Microsoft Entra Connect
  - Manage password hash synchronization (PHS)
  - Manage pass-through authentication (PTA)
  - Manage seamless single sign-on (seamless SSO)
  - Manage federation excluding manual ADFS deployments
  - Troubleshoot synchronization errors
  - Implement and manage Microsoft Entra Connect Health

Module 3: Implement an Authentication and Access Management solution

- Secure Microsoft Entra users with multifactor authentication
  - Learn about Microsoft Entra multifactor authentication.
  - Create a plan to deploy Microsoft Entra multifactor authentication.
  - Turn on Microsoft Entra multifactor authentication for users and specific apps.
- Manage user authentication
  - Administer authentication methods (FIDO2 / Passwordless)
  - Implement an authentication solution based on Windows Hello for Business
  - Configure and deploy self-service password reset
  - Deploy and manage password protection
  - Implement and manage tenant restrictions
- Plan, implement, and administer Conditional Access
  - Plan and implement security defaults.
  - Plan conditional access policies.

- Implement conditional access policy controls and assignments (targeting, applications, and conditions).
  - Test and troubleshoot conditional access policies.
  - Implement application controls.
  - Implement session management.
  - Configure smart lockout thresholds.
- Manage Microsoft Entra Identity Protection
  - Implement and manage a user risk policy.
  - Implement and manage sign-in risk policies.
  - Implement and manage MFA registration policy.
  - Monitor, investigate, and remediate elevated risky users.
- Implement access management for Azure resources
  - Configure and use Azure roles within Microsoft Entra ID
  - Configure and managed identity and assign it to Azure resources
  - Analyze the role permissions granted to or inherited by a user
  - Configure access to data in Azure Key Vault using RBAC-policy
- Deploy and Configure Microsoft Entra Global Secure Access
  - Define Global Secure Access and its components.
  - Explore deployment and configuration of Microsoft Entra Internet Access.
  - Explore deployment and configuration of Microsoft Entra Private Access.
  - Use the Global Secure Access Dashboard to monitor your systems.
  - Configure Remote Networks.
  - Create Conditional Access policies to protect your networks, data, and applications.

Module 4: Implement Access Management for Apps

- Plan and design the integration of enterprise apps for SSO
  - Discover apps by using Defender for Cloud Apps or ADFS app report.
  - Design and implement access management for apps.
  - Design and implement app management roles.
  - Configure preintegrated (gallery) SaaS apps.
- Implement and monitor the integration of enterprise apps for SSO
  - Implement token customizations
  - Implement and configure consent settings
  - Integrate on-premises apps by using Microsoft Entra application proxy
  - Integrate custom SaaS apps for SSO
  - Implement application user provisioning
  - Monitor and audit access/Sign-On to Microsoft Entra ID integrated enterprise applications
- Implement app registration
  - Plan your line of business application registration strategy
  - Implement application registrations
  - Configure application permissions
  - Plan and configure multi-tier application permissions
- Register apps using Microsoft Entra ID
  - Explain the benefits of registering apps in Microsoft Entra ID
  - Compare and contrast single and multitenant apps
  - Describe what happens and the primary settings when registering an app
  - Describe the relationship between application objects and service principals

Module 5: Plan and implement an identity governance strategy

- Plan and implement entitlement management
  - Define catalogs.
  - Define access packages.

- Plan, implement and manage entitlements.
- Implement and manage terms of use.
- Manage the lifecycle of external users in Microsoft Entra Identity Governance settings.

- Plan, implement, and manage access review
  - Plan for access reviews
  - Create access reviews for groups and apps
  - Monitor the access review findings
  - Manage licenses for access reviews
  - Automate management tasks for access review
  - Configure recurring access reviews
- Plan and implement privileged access
  - Define a privileged access strategy for administrative users (resources, roles, approvals, and thresholds)
  - Configure Privileged Identity Management for Microsoft Entra roles
  - Configure Privileged Identity Management for Azure resources
  - Assign roles
  - Manage PIM requests
  - Analyze PIM audit history and reports
  - Create and manage emergency access accounts
- Monitor and maintain Microsoft Entra ID
  - Analyze and investigate sign in logs to troubleshoot access issues
  - Review and monitor Microsoft Entra audit logs
  - Enable and integrate Microsoft Entra diagnostic logs with Log Analytics / Azure Sentinel
  - Export sign in and audit logs to a third-party SIEM (security information and event management)
  - Review Microsoft Entra activity by using Log Analytics / Azure Sentinel, excluding KQL (Kusto Query Language) use
  - Analyze Microsoft Entra workbooks / reporting
  - Configure notifications
- Explore the many features of Microsoft Entra Permissions Management
  - Understand the features of Microsoft Entra Permissions Management
  - Learn more specifics about how Permissions Management allows you to discover, remediate, and monitor identities, permissions, and resources
  - Get real-world views of the data and analytics Permissions Management provides