Microsoft Identity and Access Administrator

Duration: 4 Days   Course Code: M-SC300

Overview:

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.

Target 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.

Objectives:

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

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.

These courses (or equivalent knowledge and hands-on experience) cover the prerequisites

- SC-900 Security Fundamentals
- AZ-104:Microsoft Azure Administrator

Content:

Module 1: 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.

- Implement Initial configuration of Azure AD
- Create, configure, and manage identities
- Implement and manage external identities
- Implement and manage hybrid identity

Lab 1a: Manage user roles

Lab 1b: Setting tenant-wide properties

Lab 1c: Assign licenses to users

Lab 1d: Restore or remove deleted users

Lab 1e: Add groups in Azure AD

Lab 1f: Change group license assignments

Lab 1g: Change user license assignments

Lab 1h: Configure external collaboration

Lab 1i: Add guest users to the directory

Lab 1j: Explore dynamic groups

After completing module 1, students will be able to:

- Deploy an initail Azure AD with custom settings
- Manage both internal and external identities
- Implement a hybrid identity solution

Module 2: 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.

- Secure Azure AD user with MFA
- Manage user authentication

Lab 2a: Enable Azure AD MFA

Lab 2b: Configure and deploy self-service password reset (SSPR)

Lab 2c: Work with security defaults

Lab 2d: Implement conditional access policies, roles, and assignments

Lab 2e: Configure authentication session controls

Lab 2f: Manage Azure AD smart lockout values

Lab 2g: Enable sign-in risk policy

Lab 2h: Configure Azure AD MFA authentication registration policy

After completing module 2, students will be able to:

- Configure and manage user authentication including MFA
- Control access to resources using conditional access
- Use Azure AD Identity Protection to protect your organization

Module 3: 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.

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

Lab 3a: Implement access management for apps

Lab 3b: Create a custom role to management app registration

Lab 3c: Register an application

Lab 3e: Add app roles to applications and recieve tokens

After completing module 3, students will be able to:

- Register a new application to your Azure AD
- Plan and implement SSO for enterprise application
- Monitor and maintain enterprise applications

Module 4: 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).

- Plan and implement entitlement management
- Plan, implement, and manage access reviews
- Plan and implement privileged access
- Monitor and maintain Azure AD

Lab 4a: Creat and manage a resource catalog with Azure AD entitlement

Lab 4b: Add terms of use acceptance report

Lab 4c: Manage the lifecycle of external users with Azure AD identity governance

Lab 4d: Create access reviews for groups and apps

Lab 4e: Configure PIM for Azure AD roles

Lab 4f: Assign Azure AD role in PIM

Lab 4g: Assign Azure resource roles in PIM

Lab 4h: Connect data from Azure AD to Azure Sentinel

After completing module 4, students will be able to:

- Mange and maintain Azure AD from

- Plan, implement, and administer conditional access
- Manage Azure AD identity protection

Lab 3d: Grant tenant-wide admin consent to an application

creation to solution

- Use access reviews to maintain your Azure AD
- Grant access to users with entitlement management

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/