Microsoft Identity and Access Administrator – Intensive Training («SC300»)

The Microsoft Identity and Access Administrator course explores how to design, implement, and operate an organization's identity and access management systems by using Azure AD.

Duration: 3 days
Price: 3'400.–
Course documents: Official Microsoft Courseware and Microsoft Learn
Vendor code: SC-300

Content

The content of this intensive training is derived from the exam «SC-300: Microsoft Identity and Access Administrator». Start preparing for the course on Microsoft Learn now and use the Learning Support if you have any questions. During the intensive training days with the instructor you will work with the official Microsoft course material (more information under «Methodology & didactics»).

Course details:

Module 1: Explore identity and Azure AD

- This module covers definitions and available services for identity provided in Azure AD to Microsoft 365. You start with authentication, authorization, and access tokens then build into full identity solutions.

Module 2: Implement initial configuration of Azure Active Directory

- Learn to create an initial Azure Active Directory configuration to ensure all the identity solutions available in Azure are ready to use. This module explores how to build and configure an Azure AD system.

Module 3: Create, configure, and manage identities

- Access to cloud-based workloads needs to be controlled centrally by providing a definitive identity for each user and resource. You can ensure employees and vendors have just-enough access to do their job.

Module 4: Implement and manage external identities

- Inviting external users to use company Azure resources is a great benefit, but you want to do it in a secure way. Explore how to enable secure external collaboration.

Module 5: Implement and manage hybrid identity

- Creating a hybrid-identity solution to use your on-premises active directory can be challenging. Explore how to implement a secure hybrid-identity solution.

Module 6: Secure Azure Active Directory users with Multi-Factor Authentication

- Learn how to use multi-factor authentication with Azure AD to harden your user accounts.

Module 7: Manage user authentication

- There are multiple options for authentication in Azure AD. Learn how to implement and manage the right authentications for users based on business needs.

Module 8: Plan, implement, and administer Conditional Access

- Conditional Access gives a fine granularity of control over which users can do specific activities, access which resources, and how to ensure data and systems are safe.

Module 9: Manage Azure AD Identity Protection

- Protecting a user's identity by monitoring their usage and sign-in patterns will ensure a secure cloud solution. Explore how to design and implement Azure AD Identity protection.

Module 10: Implement access management for Azure resources

- Explore how to use built-in Azure roles, managed identities, and RBAC-policy to control access to Azure resources. Identity is the key to secure solutions.

Module 11: Plan and design the integration of enterprise apps for SSO

- Enterprise app deployment enables control over which users can access the apps, easily log into apps with single-sign-on, and provide integrated usage reports.

Module 12: Implement and monitor the integration of enterprise apps for SSO

- Deploying and monitoring enterprise applications to Azure solutions can ensure security. Explore how to deploy on-premises and cloud based apps to users.

Module 13: Implement app registration

- Line of business developed in-house need registration in Azure AD and assigned to users for a secure Azure solution. Explore how to implement app registration.

Module 14: Plan and implement entitlement management

- When new users or external users join your site, quickly assigning them access to Azure solutions is a must. Explore how to entitle users to access your site and resources.

Module 15: Plan, implement, and manage access review

- Once identity is deployed, proper governance using access reviews is necessary for a secure solution. Explore how to plan for and implement access reviews.

Module 16: Plan and implement privileged access

- Ensuring that administrative roles are protected and managed to increase your Azure solution security is a must. Explore how to use PIM to protect your data and resources.

Module 17: Monitor and maintain Azure Active Directory

- Azure AD audit and diagnostic logs provide a rich view into how users are accessing your Azure solution. Learn to monitor, troubleshoot, and analyze sign-in data.

Key Learnings

- Implementing identities in Azure AD
- Implementing authentication and access management
- Implementing access management for applications
- Planning and implementing identity governance in Azure AD

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.

Requirements

- 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.

Basic knowledge gained in the following course is recommended:

- Microsoft Security, Compliance, and Identity Fundamentals – Intensive Training («SC900»)
- Microsoft Security, Compliance, and Identity Fundamentals – Flexible Training («SC900V»)

Certification

This intensive training prepares you for:

- **Exam:** «SC-300: Microsoft Identity and Access Administrator» for the
- **Certification:** «Microsoft Certified: Identity and Access Administrator Associate»

Further courses

- Microsoft 365 Administrator Essentials – Intensive Training («MS12BC»)
- Microsoft Cybersecurity Architect – Intensive Training («SC100»)

Any questions?

We are happy to advise you on +41 44 447 21 21 or info@digicomp.ch. You can find detailed information about dates on www.digicomp.ch/courses-digital-transformation-technologies/cloud/cloud-security/course-microsoft-identity-and-access-administrator-intensive-training-sc-300