SC-300T00

Microsoft Identity and Access Administrator

Der Kurs „Microsoft Identity and Access Administrator“ erkundet, wie die Identitäts- und Zugriffsverwaltungssysteme einer Organisation mithilfe von Azure AD entworfen, implementiert und betrieben werden. Erfahren Sie, wie Sie Aufgaben wie das Bereitstellen des sicheren Authentifizierungs- und Autorisierungszugriffs auf Unternehmensanwendungen bereitstellen. Sie lernen ferner, wie Sie nahtlose Benutzerumgebungen und Self-Service-Verwaltungsfunktionen für alle Benutzer bereitstellen. Schließlich erfahren Sie, wie Sie adaptive/n Zugriff und Governance Ihrer Identitäts- und Zugriffsverwaltungslösungen herstellen, um so sicherzustellen, dass Sie Probleme in Ihrer Umgebung behandeln, sie überwachen und Berichte dazu erstellen können. Der*Die Identity and Access Administrator kann eine einzelne Person oder ein Mitglied eines größeren Teams sein. Erfahren Sie, wie diese Rolle mit vielen anderen Rollen in der Organisation zusammenarbeitet, um strategische Identitätsprojekte voranzutreiben. Das endgültige Ziel besteht darin, Ihnen Wissen zur Modernisierung von Identitätslösungen sowie zur Implementierung hybrider Identitätslösungen und der Identitätsgovernance zu vermitteln.

Kursinhalt

- Erkunden der Identität und Microsoft Entra ID
- Implementieren der Erstkonfiguration von Microsoft Entra ID
- Erstellen, Konfigurieren und Verwalten von Identitäten
- Implementieren und Verwalten externer Identitäten
- Implementieren und Verwalten einer Hybrididentität
- Sichern von Microsoft Entra-Benutzern mit mehrstufiger Authentifizierung
- Verwalten der Benutzerauthentifizierung
- Planen, Implementieren und Verwalten des bedingten Zugriffs
- Verwalten von Microsoft Entra ID Protection
- Implementieren der Zugriffsverwaltung für Azure-Ressourcen
- Planen und Entwerfen der Integration von Unternehmens-Apps für SSO
- Implementieren und Überwachen der Integration von Unternehmens-Apps für einmaliges Anmelden
- Implementieren der App-Registrierung
- Planen und Implementieren der Berechtigungsverwaltung
- Planen, Implementieren und Verwalten der Zugriffsüberprüfung
- Planen und Implementieren von privilegiertem Zugriff
- Überwachen und Verwalten von Microsoft Entra ID

E-Book Die originalen Microsoft-Kursunterlagen werden Ihnen online zur Verfügung gestellt.

Zielgruppe

Dieser Kurs richtet sich an Identitäts- und Zugriffsadministratoren, die planen, die zugehörige Zertifizierungsprüfung abzulegen, oder die im Rahmen ihrer täglichen Arbeit Aufgaben im Bereich der Identitäts- und Zugriffsverwaltung erledigen. Dieser Kurs ist auch für Administratoren oder Techniker hilfreich, die sich auf die Bereitstellung von Identitäts- und Zugriffsverwaltungssystemen für Azure-basierte Lösungen spezialisieren möchten und eine wesentliche Rolle beim Schutz einer Organisation spielen.

Voraussetzungen

Vor der Teilnahme an diesem Kurs sollten die Teilnehmer über folgende Kenntnisse verfügen:

- Bewährte Sicherheitspraktiken und branchenübliche Sicherheitsanforderungen wie "Defense in depth", "least privileged access", "shared responsibility" und "zero trust model".
- Vertraut sein mit Identitätskonzepten wie Authentifizierung, Autorisierung und Active Directory.
- Sie haben bereits Erfahrung mit der Bereitstellung von Azure-Workloads. Dieser Kurs deckt nicht die Grundlagen der Azure-Verwaltung ab. Stattdessen baut der Kursinhalt auf diesem Wissen auf und fügt sicherheitsspezifische Informationen hinzu.
- Einige Erfahrungen mit Windows- und Linux-Betriebssystemen und Skriptsprachen sind hilfreich, aber nicht erforderlich. In den Kursübungen können PowerShell und CLI verwendet werden.

Vorausgesetzte Kurse (oder gleichwertige Kenntnisse und praktische Erfahrung):

- Grundlagen zu Sicherheit, Compliance und Identität (SC-900T00)
- Microsoft Azure Administrator (AZ-104T00)

Kursziel

Dieser Kurs unterstützt die Teilnehmer auf die Vorbereitung zum Examen SC-300, welches für die Zertifizierungen "Microsoft Certified: Identity and Access Administrator Associate" vorausgesetzt wird.

Dieser Kurs im Web

Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/go/**MC30**

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training	Preise zzgl. MwSt.
Termine in der Schweiz	**4 Tage**
Online Training	**4 TageCHF 2.855,-**
Termin/Kursort	Kurssprache Deutsch
17.06.-20.06.24 Online	21.10.-24.10.24 Online
29.07.-01.08.24 Online	02.12.-05.12.24 Online
09.09.-12.09.24 Online	

Stand 28.04.2024

Inhaltsverzeichnis

SC-300T00 – Microsoft Identity and Access Administrator

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.

Lessons

- Implement Initial configuration of Azure AD

- Create, configure, and manage identities

- Implement and manage external identities

- 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

After completing this module, 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.

Lessons

- Secure Azure AD user with MFA

- Manage user authentication

- Plan, implement, and administer conditional access

- 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

After completing this module, 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.

Lessons

- Plan and design the integration of enterprise for SSO

- Implement and monitor the integration of enterprise apps for SSO

- 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

After completing this module, 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).

Lessons

- Plan and implement entitlement management

- Plan, implement, and manage access reviews

- Plan and implement privileged access

- 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

After completing this module, students will be able to:

- Mange and maintain Azure AD from creation to solution

- Use access reviews to maintain your Azure AD

- Grant access to users with entitlement management

ExperTeach AG
Kronenstrasse 11 · 8735 St. Gallenkappel · Telefon: +41 55 420 2591 · Fax: +41 55 420 2592 · info@experteach.ch · www.experteach.ch