Microsoft Identity and Access Administrator – Flexible Training («SC300V»)

Der Kurs Microsoft Identity and Access Administrator befasst sich mit dem Entwurf, der Implementierung und dem Betrieb von Identitäts- und Zugriffsverwaltungssystemen einer Organisation unter Verwendung von Azure AD.

Dauer: 3 Tage
Preis: 3'400.– zzgl. 8.1% MWST
Kursdokumente: Offizielle Microsoft-Unterlagen und Microsoft Learn
Herstellercode: SC-300

Inhalt

Der Inhalt dieses Flexible Trainings leitet sich aus der Prüfung «SC-300: Microsoft Identity and Access Administrator» ab. Beginnen Sie schon jetzt auf Microsoft Learn mit der Vorbereitung auf den Kurs und nutzen Sie den Learning Support, wenn Sie Fragen haben. Während der jeweiligen 3h-Trainer-Sessions arbeiten Sie mit den offiziellen Microsoft-Kursunterlagen (mehr Informationen unter «Methodik & Didaktik»).

Kursinhalt:

Modul 1: Erkunden von Identität und Azure AD

- In diesem Modul werden die Definitionen und verfügbaren Dienste für die in Azure AD bis Microsoft 365 bereitgestellte Identität behandelt. Sie beginnen mit Authentifizierung, Autorisierung und Zugriffstoken und erstellen dann vollständige Identitätslösungen.

Modul 2: Implementieren der Erstkonfiguration von Azure Active Directory

- Erfahren Sie, wie Sie eine Erstkonfiguration von Azure Active Directory erstellen, um sicherzustellen, dass alle in Azure verfügbaren Identitätslösungen einsatzbereit sind. In diesem Modul wird untersucht, wie ein Azure AD-System erstellt und konfiguriert wird.

Modul 3: Erstellen, Konfigurieren und Verwalten von Identitäten

- Der Zugriff auf cloudbasierte Workloads muss zentral gesteuert werden, indem für jeden Benutzer und jede Ressource eine definitive Identität bereitgestellt wird. Sie können sicherstellen, dass die Mitarbeiter*innen und Lieferant*innen nur über die Zugriffsrechte verfügen, die für ihre Arbeit erforderlich sind.

Modul 4: Implementieren und Verwalten externer Identitäten

- Externer Benutzer einzuladen, die Azure-Ressourcen Ihres Unternehmens zu nutzen, ist sehr nützlich. Das sollte jedoch nicht auf Kosten der Sicherheit passieren. Hier erfahren Sie, wie Sie eine sichere externe Zusammenarbeit ermöglichen.

Modul 5: Implementieren und Verwalten einer Hybrididentität

- Das Erstellen einer Hybrididentitätslösung zur Verwendung Ihrer lokalen Active-Directory-Instanz kann eine Herausforderung darstellen. Hier erfahren Sie, wie Sie eine sichere Hybrididentitätslösung implementieren.

Modul 6: Schützen von Azure Active Directory-Benutzern mit mehrstufiger Authentifizierung

- Hier erfahren Sie, wie Sie die mehrstufige Authentifizierung mit Azure AD kombinieren können, um Ihre Benutzerkonten zu härten.

Modul 7: Verwalten der Benutzer-Authentifizierung

- Es gibt mehrere Möglichkeiten für die Authentifizierung in Azure AD. Erfahren Sie, wie Sie die richtigen Authentifizierungen für Benutzer basierend auf Geschäftsanforderungen implementieren und verwalten.

Modul 8: Planen, Implementieren und Verwalten des bedingten Zugriffs

- Der bedingte Zugriff ermöglicht differenzierte Kontrolle darüber, welche Benutzer bestimmte Aktivitäten ausführen und auf Ressourcen zugreifen können, und gewährleistet die Sicherheit von Daten und Systemen.

Modul 9: Verwalten von Azure AD Identity Protection

- Das Schützen der Identität eines Benutzers durch Überwachen seiner Nutzungs- und Anmeldungsmuster gewährleistet eine sichere Cloudlösung. Erfahren Sie, wie Sie Azure AD Identity Protection entwerfen und implementieren.

Modul 10: Implementieren der Zugriffsverwaltung für Azure-Ressourcen

- Hier erfahren Sie, wie Sie mithilfe von integrierten Azure-Rollen, verwalteten Identitäten und RBAC-Richtlinien den Zugriff auf Azure-Ressourcen steuern. Identität ist der Schlüssel zu sicheren Lösungen.

Modul 11: Planen und Entwerfen der Integration von Unternehmens-Apps für SSO

- Sie können bei der Bereitstellung von Unternehmens-Apps steuern, welche Benutzer auf die Apps zugreifen können und ob sie sich ganz einfach über einmaliges Anmelden (Single Sign-on, SSO) bei den Apps anmelden können. Ausserdem können Sie festlegen, dass integrierte Nutzungsberichte erstellt werden.

Modul 12: Implementieren und Überwachen der Integration von Unternehmens-Apps für einmaliges Anmelden

- Durch die Bereitstellung und Überwachung von Unternehmensanwendungen in Azure-Lösungen kann Sicherheit gewährleistet werden. Erfahren Sie, wie Sie lokale und cloudbasierte Apps für Benutzer bereitstellen.

Modul 13: Implementieren der App-Registrierung

- Eine intern entwickelte Branchenanwendung muss in Azure AD registriert und Benutzern für eine sichere Azure-Lösung zugewiesen werden. Erfahren Sie, wie Sie die App-Registrierung implementieren.

Modul 14: Planen und Implementieren der Berechtigungsverwaltung

- Wenn neue oder externe Benutzer Ihrer Website beitreten, müssen Sie ihnen schnell Zugriff auf Azure-Lösungen zuweisen können. Hier erfahren Sie, wie Sie Benutzern die Berechtigungen für den Zugriff auf Ihre Website und Ressourcen gewähren.

Modul 15: Planen, Implementieren und Verwalten der Zugriffsüberprüfung

- Sobald eine Identität bereitgestellt wurde, ist eine ordnungsgemässe Governance mithilfe von Zugriffsüberprüfungen vonnöten, um eine sichere Lösung zu gewährleisten. Hier erfahren Sie, wie Sie Zugriffsüberprüfungen planen und implementieren.

Modul 16: Planen und Implementieren von privilegiertem Zugriff

- Der Schutz und die Verwaltung von Administratorrollen ist ein wichtiger Bestandteil zur Erhöhung der Sicherheit Ihrer Azure-Lösung. Hier erfahren Sie, wie Sie mit PIM (Privileged Identity Management) Ihre Daten und Ressourcen schützen.

Modul 17: Überwachen und Verwalten von Azure Active Directory

- Azure AD-Überwachungs- und Diagnoseprotokolle bieten einen umfassenden Überblick darüber, wie Benutzer auf Ihre Azure-Lösung zugreifen. Hier lernen Sie, wie Sie Anmeldedaten überwachen, Probleme beheben und die Daten analysieren.

Key Learnings

- Implementieren von Identitäten in Azure AD
- Implementieren von Authentifizierung und Zugriffsmanagement
- Implementieren von Zugriffsmanagement für Anwendungen
- Planen und Implementieren der Identitätsverwaltung in Azure AD

Methodik & Didaktik

Digicomp Flexible-Learning-Ansatz:

- **Trainings-Modalität:** Während einer Dauer von 4 Wochen finden 6-8 halbtägige (je 3h) virtuelle Live-Sessions mit unseren Azure-MCT-Experten statt. Die Sessions sind bereits geplant und lassen sich super mit dem Arbeitsalltag verbinden. Zwischen den Sessions bleibt genügend Zeit, das gelernte Wissen zu verarbeiten.
- **Detaillierter Session-Plan:** Klicken Sie dazu am Ende der Seite, wo Sie Ihr gewünschtes Datum auswählen, auf «**Stundenplan**».

Zielpublikum

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

Anforderungen

- Bewährte Sicherheitspraktiken und branchenspezifische Sicherheitsanforderungen wie Defense in Depth, Least Privileged Access, Shared Responsibility und Zero Trust Model.
- Vertrautheit mit Identitätskonzepten wie Authentifizierung, Autorisierung und Active Directory.
- Einige Erfahrung mit der Bereitstellung von Azure-Workloads. Dieser Kurs deckt nicht die Grundlagen der Azure-Administration 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 die CLI verwendet werden.

Empfohlen wird das im folgenden Kurs erlangte Grundwissen:

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

Zertifizierung

Dieses Flexible Training bereitet Sie vor auf:

- **Prüfung:** «SC-300: Microsoft Identity and Access Administrator» für die
- **Zertifizierung:** «Microsoft Certified: Identity and Access Administrator Associate»

Weiterführende Kurse

- Microsoft Cybersecurity Architect – Flexible Training («SC100V»)

Haben Sie Fragen oder möchten Sie einen Firmenkurs buchen?

Wir beraten Sie gerne unter 044 447 21 21 oder info@digicomp.ch. Detaillierte Infos zu den Terminen finden Sie unter www.digicomp.ch/weiterbildung-microsoft-technology/microsoft-security-compliance-and-identity/microsoft-certified-identity-and-access-administrator-associate/kurs-microsoft-identity-and-access-administrator-flexible-training-sc-300