Microsoft Identity and Access Administrator (SC-300T00)

ID SC-300T00 **Preis** CHF 2'480.– (exkl. MwSt.) **Dauer** 4 Tage

Zielgruppe

Dieser Kurs richtet sich an Identitäts- und Zugriffsadministratoren, die die zugehörige Zertifizierungsprüfung ablegen möchten oder in ihrer täglichen Arbeit Identitäts- und Zugriffsverwaltungsaufgaben ausführen. Dieser Kurs ist auch für Administratoren oder Ingenieure hilfreich, die sich auf die Bereitstellung von Identitätslösungen und Zugriffsverwaltungssystemen für Azure-basierte Lösungen spezialisieren möchten, die eine wesentliche Rolle beim Schutz eines Unternehmens spielen.

Empfohlenes Training für die Zertifizierung zum

Microsoft Certified: Identity and Access Administrator Associate (MCIAAA)

Voraussetzungen

Erfolgreiche Teilnehmer verfügen über Vorkenntnisse und Verständnis für:

- Bewährte Praktiken für die Sicherheit und Sicherheitsanforderungen der Branche, z. B. Tiefenverteidigung, Zugriff mit den geringsten Berechtigungen, gemeinsame Verantwortung und Null-Vertrauens-Modell.
- Machen Sie sich mit Identitätskonzepten wie Authentifizierung, Autorisierung und Active Directory vertraut.
- Erfahrung in der Bereitstellung von Azure-Workloads. Dieser Kurs behandelt nicht die Grundlagen der Azure-Verwaltung, sondern der Kursinhalt baut auf diesem Wissen auf und vermittelt weitere sicherheitsspezifische Informationen.
- Erfahrung mit Windows- und Linux-Betriebssystemen und Skriptsprachen sind hilfreich, aber nicht erforderlich. In Kurslabs können PowerShell und die CLI verwendet werden.

Kursziele

- Implementieren einer Identitätsverwaltungslösung
- Implementieren einer Authentifizierungs- und Zugriffsverwaltungslösung
- Implementieren der Zugriffsverwaltung für Apps
- Planen und implementieren einer Strategie zur Identitätskontrolle

Kursinhalt

Modul 1: Implementieren einer Identitätsverwaltungslösung

Erfahren Sie, wie Sie Ihre anfängliche Azure Active Directory-Implementierung (Azure AD)erstellen und verwalten und die Benutzer, Gruppen und externen Identitäten konfigurieren, die Sie zum Ausführen Ihrer Lösung verwenden.

Lektionen

- Implementieren der Erstkonfiguration von Azure AD
- Identitäten erstellen, konfigurieren und verwalten
- Implementierung und Verwaltung externer Identitäten
- Implementierung und Verwaltung der hybriden Identität
- Lab: Benutzerrollen verwalten
- Lab: Festlegen mandantenweiter Eigenschaften
- Lab: Weisen Sie Benutzern Lizenzen zu
- Lab: Gelöschte Benutzer wiederherstellen oder entfernen
- Lab: Fügen Sie Gruppen in Azure AD hinzu
- Lab: Ändern Sie die Gruppenlizenzzuweisungen
- Lab: Benutzerlizenzzuweisungen ändern
- Lab: Konfigurieren Sie die externe Zusammenarbeit
- Lab: Fügen Sie dem Verzeichnis Gastbenutzer hinzu
- Lab: Untersuchen Sie dynamische Gruppen

Nach Abschluss dieses Moduls sind die Teilnehmer in der Lage:

- ein Azure AD mit benutzerdefinierten Einstellungen bereitzustellen
- sowohl interne als auch externe Identitäten verwalten
- eine hybride Identitätslösung zu verwalten

Modul 2: Implementieren Sie eine Authentifizierungs- und Zugriffsverwaltungslösung

Implementieren und verwalten Ihrer Zugriffsverwaltung mit Azure AD. Verwenden von MFA, bedingtem Zugriff und Identitätsschutz, um Ihre Identitätslösung zu verwalten.

Lektionen

- Sicheren Azure AD-Benutzer mit MFA
- Benutzerauthentifizierung verwalten
- Bedingten Zugriff planen, implementieren und verwalten
- Verwalten des Azure AD-Identitätsschutzes
- Lab: Azure AD MFA aktivieren
- Lab: Selbständig Kennwort zurücksetzen (SSPR) konfigurieren und bereitstellen
- Lab: Arbeiten mit Sicherheitsstandards
- Lab: Implementieren von Richtlinien, Rollen und Zuweisungen für den bedingten Zugriff
- Lab: Konfigurieren von Steuerelementen für Authentifizierungssitzungen
- Lab: Verwalten der Azure AD-Smart Verriegelungs-Werte
- Lab: Aktivieren der Anmelderisikorichtlinien
- Lab: Konfigurieren der Registrierungsrichtlinien für die Azure ADMFA-Authentifizierung

Nach Abschluss des Moduls sind die Teilnehmer in der Lage:

- die Benutzerauthentifizierung, einschliesslich MFA, zu konfigurieren und zu verwalten
- den Zugriff auf Ressourcen mit Hilfe des bedingten Zugriffs zu steuern
- den Azure AD-Identitätsschutz zu verwenden, um Ihr Unternehmen zu schützen

Modul 3: Implementieren der Zugriffsverwaltung für Apps

Erfahren Sie, wie Anwendungen mit der Anwendungsregistrierung in Azure AD zu Ihrer Identitäts- und Zugriffslösung hinzugefügt werden können und sollten.

Lektionen

- Integration von Unternehmen für SSO planen und gestalten
- Implementierung und Überwachung der Integration von Unternehmensanwendungen für SSO
- Implementieren der App-Registrierung
- Lab: Implementieren Sie die Zugriffsverwaltung für Apps
- Lab: Erstellen Sie eine benutzerdefinierte Rolle für die Registrierung der Verwaltungs-App
- Lab: Registrieren Sie eine Anwendung
- Lab: Erteilen Sie einer Anwendung die mandantenweite Zustimmung des Administrators
- Lab: Fügen Sie App-Rollen zu den Anwendungen hinzu und erhalten Sie Token

Nach Abschluss dieses Moduls sind die Teilnehmer in der Lage:

- eine neue Anwendung in Ihrem Azure AD zu registrieren
- SSO für Unternehmensanwendungen zu planen und zu implementieren
- Unternehmensanwendungen zu überwachen und zu warten

Modul 4: Planen und Implementieren einer Identitätsverwaltungsstrategie

Identitäts-Governance für Ihre Identitätslösung mit Hilfe von Berechtigungen, Zugriffsüberprüfungen, privilegiertem Zugriff und Überwachung Ihres Azure Active Directory (Azure AD) entwerfen und implementieren.

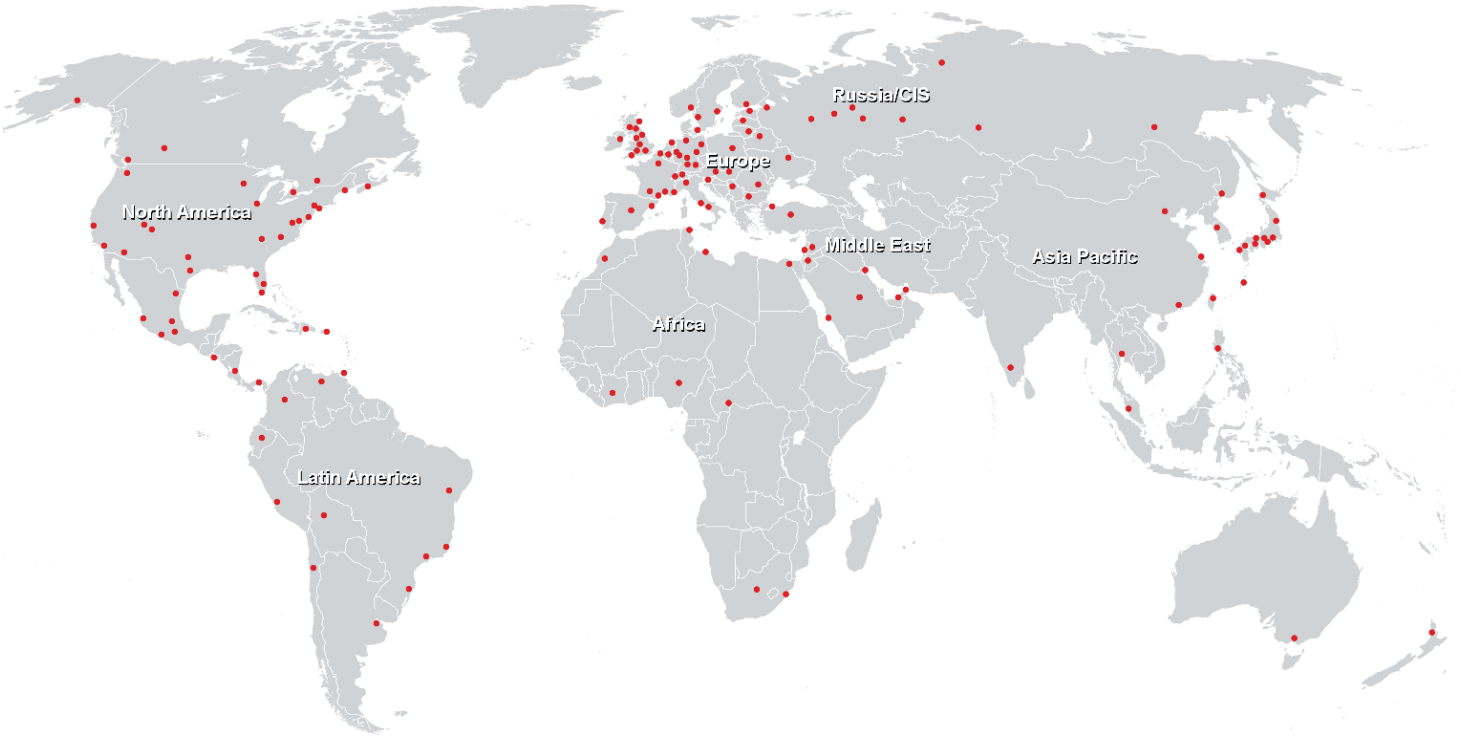
Lektionen

- Berechtigungsmanagement planen und implementieren
- Planen, Implementieren und Verwalten von Zugriffsüberprüfungen
- Privilegierten Zugriff planen und implementieren
- Azure AD überwachen und warten
- Lab: Erstellen und Verwalten eines Ressourcenkatalogs mit Azure AD-Berechtigung
- Lab: Akzeptanzbericht für Nutzungsbedingungen hinzufügen
- Lab: Verwalten Sie den Lebenszyklus externer Benutzer mit Azure AD Identity Governance
- Lab: Erstellen Sie Zugriffsüberprüfungen für Gruppen und Apps
- Lab: Konfigurieren Sie PIM für Azure AD-Rollen
- Lab: Weisen Sie die Azure AD-Rolle in PIM zu
- Lab: Weisen Sie Azure-Ressourcenrollen in PIM zu
- Lab: Verbinden Sie Daten aus Azure AD mit Azure Sentinel

Nach Abschluss dieses Moduls sind die Teilnehmer in der Lage:

- Azure AD von der Erstellung bis zur Lösung zu verwalten und zu pflegen
- Zugriffsüberprüfungen zu verwenden, um Azure AD zu verwalten
- Benutzern mit Verwaltungsberechtigung Zugriff zu gewähren

Weltweite Trainingscenter



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch