Smartfuture
Certifications | Training | Technology solutions

FORMATION & CERTIFICATION • SC-300

Administrateur d'identité et de l'accès Microsoft

La formation SC-300 enseigne la gestion des identités dans le cloud et le renforcement de la sécurité.

Formation présentielle

Formateurs certifiés Microsoft

Distributeur officiel Certiport

4 jours	Examen
28 heures	SC-300
Modalité	**Niveau**
Présentiel Distanciel	termédiaire / Avancéire

INSCRIPTION / RÉSERVATION

Je m'inscris maintenant

OBJECTIFS PÉDAGOGIQUES

- Maîtriser les concepts d'identité, d'authentification et d'autorisation dans Microsoft Entra ID.
- Gérer les identités utilisateurs et hybrides dans des environnements cloud.
- Administrer l'authentification multifacteur, l'accès conditionnel et la gestion des risques.
- Mettre en œuvre une gouvernance des identités incluant droits d'utilisation, accès privilégié et supervision.

PUBLIC CIBLE

- Administrateurs d'identité.
- Administrateurs de sécurité.
- Ingénieurs cloud.
- Professionnels IT responsables de la gestion des identités et des accès.

PRÉREQUIS

- Connaissance de base des concepts du cloud et des services Microsoft.
- Expérience recommandée dans la gestion des environnements hybrides et cloud
- Familiarité avec les notions d'identité, d'authentification et de sécurité..

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Implémenter et gérer des identités utilisateur

Configurer et gérer un locataire Microsoft Entra

- Configurer et gérer les rôles Microsoft Entra intégrés et personnalisés.
- Recommander et implémenter l'utilisation des unités administratives.
- Évaluer les autorisations effectives pour les rôles Microsoft Entra.
- Configurer et gérer les domaines dans Microsoft Entra ID et Microsoft 365.
- Configurer les paramètres de personnalisation de l'entreprise.
- Configurer les propriétés du locataire, les paramètres utilisateur, groupe et appareil.

Créer, configurer et gérer des identités Microsoft Entra

- Créer, configurer et gérer des identités et des groupes.
- Gérer les attributs de sécurité personnalisés.
- Automatiser les opérations en bloc via le centre d'administration et PowerShell.
- Gérer la jonction et l'inscription des appareils dans Microsoft Entra ID.
- Attribuer, modifier et suivre les licences.

Implémenter et gérer des identités pour les utilisateurs et locataires externes

- Gérer les paramètres de collaboration externe dans Microsoft Entra ID.
- Inviter et gérer des utilisateurs externes, individuellement ou en bloc.
- Implémenter des paramètres d'accès entre locataires.
- Implémenter et gérer la synchronisation entre locataires.
- Configurer des fournisseurs d'identité externes (SAML, WS-Fed, etc.).

Implémenter et gérer l'identité hybride

- Implémenter et gérer Microsoft Entra Connect Sync et Cloud Sync.
- Implémenter et gérer la synchronisation de hachage de mot de passe.
- Implémenter l'authentification directe et l'authentification unique transparente.
- Migrer depuis AD FS vers d'autres mécanismes d'authentification.
- Implémenter et gérer Microsoft Entra Connect Health.

Implémenter la gestion des authentifications et des accès

Planifier, implémenter et gérer l'authentification utilisateur

- Planifier l'authentification dans Microsoft Entra ID.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

- Implémenter et gérer les méthodes d'authentification (certificats, passe d'accès temporaire, OAUTH, Microsoft Authenticator, FIDO2, etc.).
- Configurer et gérer les paramètres MFA à l'échelle du locataire.
- Configurer la réinitialisation de mot de passe en libre-service (SSPR).
- Implémenter et gérer Windows Hello Entreprise.
- Désactiver des comptes et révoquer des sessions utilisateur.
- Implémenter et gérer la protection par mot de passe Microsoft Entra.
- Activer l'authentification Microsoft Entra Kerberos pour les identités hybrides.

Planifier, implémenter et gérer l'accès conditionnel

- Planifier les stratégies d'accès conditionnel.
- Implémenter des attributions et contrôles d'accès conditionnel.
- Tester et résoudre les problèmes des stratégies d'accès conditionnel.
- Implémenter la gestion des sessions et des restrictions appliquées par l'appareil.
- Implémenter l'évaluation continue de l'accès et le contexte d'authentification.
- Créer des stratégies d'accès conditionnel à partir de modèles.

Gérer les risques avec Microsoft Entra ID Protection

- Implémenter et gérer les risques utilisateur et connexions à risque.
- Configurer les stratégies d'inscription MFA.
- Surveiller, investiguer et corriger utilisateurs et identités de charge de travail à risque.

Implémenter la gestion des accès pour les ressources Azure

- Créer et attribuer des rôles Azure intégrés et personnalisés.
- Évaluer les autorisations effectives pour un ensemble de rôles Azure.
- Attribuer des rôles pour permettre la connexion Entra ID aux machines virtuelles Azure.
- Configurer le RBAC Azure Key Vault et les stratégies d'accès.

Implémenter l'accès global sécurisé

- Déployer des clients d'accès global sécurisé.
- Déployer l'accès privé et l'accès Internet, y compris pour Microsoft 365.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Planifier et implémenter des identités de charge de travail

Identités applicatives et charges de travail Azure

- Planifier et implémenter des identités pour les applications et charges de travail Azure (identités managées, principaux de service, comptes d'utilisateur, comptes de service gérés).
- Créer des identités managées et les associer à des ressources Azure.
- Utiliser une identité managée pour accéder à d'autres ressources Azure.

Planifier, implémenter et superviser l'intégration des applications d'entreprise

- Planifier et implémenter des paramètres pour les applications d'entreprise (au niveau de l'application et du locataire).
- Attribuer des rôles Microsoft Entra appropriés pour la gestion des applications.
- Intégrer des applications locales via le proxy d'application Microsoft Entra.
- Intégrer des applications SaaS et gérer les utilisateurs, groupes et rôles d'application.
- Configurer et gérer le consentement utilisateur et administrateur.
- Créer et gérer des collections d'applications.

Planifier et implémenter des inscriptions et l'accès aux applications

- Planifier et créer des inscriptions d'applications.
- Configurer l'authentification d'application et les autorisations d'API.
- Créer des rôles d'application.
- Gérer et surveiller l'accès aux applications à l'aide de Microsoft Defender pour Cloud Apps (découverte cloud, applications connectées, contrôle d'application d'accès conditionnel).
- Créer des stratégies d'accès et de session et gérer des stratégies pour les applications OAuth.
- Gérer le catalogue d'applications cloud.

Planifier et automatiser la gouvernance des identités

- Gestion des droits d'utilisation et cycle de vie
- Planifier et implémenter la gestion des droits d'utilisation dans Microsoft Entra.
- Créer et configurer des catalogues et des packages d'accès.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

- Gérer les demandes d'accès et les conditions d'utilisation (ToU).
- Gérer le cycle de vie des utilisateurs externes et des organisations connectées.

Révisions d'accès et gestion des accès privilégiés

- Planifier, créer et superviser des révisions d'accès dans Microsoft Entra.
- Planifier et gérer les rôles Azure et les ressources dans PIM.
- Configurer des groupes managés par PIM et gérer les demandes / approbations.
- Analyser l'historique et les rapports d'audit PIM.
- Créer et gérer des comptes d'accès d'urgence.

Surveillance, audit et gestion des autorisations

- Examiner et analyser les journaux de connexion, d'audit et d'approvisionnement via le Centre d'administration Microsoft Entra.
- Configurer les paramètres de diagnostic (Log Analytics, comptes de stockage, hubs d'événements).
- Superviser Microsoft Entra ID via des requêtes KQL, classeurs et rapports.
- Améliorer la posture de sécurité avec le score de sécurisation d'identité.
- Planifier et implémenter la gestion des autorisations Microsoft Entra (Permissions Management) : intégration des abonnements, évaluation et correction des risques (identités, rôles privilégiés, PCI, etc.).
- Configurer des alertes d'activité et des déclencheurs pour les abonnements Azure.