Administrateur des identités et des accès Microsoft

Objectifs pédagogiques

- Configurer et administrer les identités, groupes, rôles, appareils et paramètres de locataire dans Microsoft Entra ID
- Mettre en oeuvre des mécanismes d'authentification, d'accès conditionnel et de protection des identités
- Gérer l'accès aux applications d'entreprise, les inscriptions d'applications et l'authentification unique
- Déployer des solutions d'identité hybride, d'identités externes et de synchronisation avec Microsoft Entra Connect
- Mettre en oeuvre la gouvernance des identités avec les droits d'utilisation, les révisions d'accès et Privileged Identity Management

Prérequis

- Comprendre les bonnes pratiques de sécurité et les exigences courantes du secteur, notamment la défense en profondeur, le moindre privilège, le contrôle d'accès basé sur les rôles, la responsabilité partagée et le modèle Zero Trust
- Être familiarisé avec les fournisseurs d'identité comme Microsoft Entra ID, Microsoft Entra Domain Services ou d'autres fournisseurs d'authentification
- Avoir une première expérience du déploiement de charges de travail Azure
- Avoir une expérience de Windows et/ou Linux ainsi que des bases en scripting
- Une expérience pratique de Microsoft Entra ID, de l'administration Microsoft 365 et des concepts de sécurité d'identité est recommandée

Certification

Cette formation prépare à l'examen**SC-300**, qui permet d'obtenir la certification Microsoft Certified : Identity and Access Administrator Associate

Public concerné

Cette formation s'adresse aux professionnels de la gestion des identités et des accès qui souhaitent administrer, sécuriser et gouverner les identités dans Microsoft Entra ID.
Elle concerne les administrateurs, ingénieurs IAM, administrateurs Microsoft 365 et Azure, ainsi que les professionnels de la sécurité chargés de mettre en oeuvre des solutions d'authentification, d'autorisation, d'accès applicatif et de gouvernance des identités.

Bénéfices pour les participants :

- Structurer une approche complète de l'identité et de l'accès dans l'écosystème Microsoft
- Renforcer la sécurité des comptes, applications et ressources grâce aux mécanismes Microsoft Entra
- Développer des compétences concrètes en administration, protection et gouvernance des identités
- Préparer la montée en compétence vers un rôle IAM Microsoft de niveau administrateur

Programme détaillé

Explorer l'identité dans Microsoft Entra ID (3h00)

- Explorer l'identité
- Concepts d'administration des identités
- Authentification et autorisation
- Audit et autres concepts d'identité
- Paysage de l'identité
- Confiance Zéro et identité
- Pourquoi utiliser une identité
- Concepts d'administration des identités
- Sujets liés à l'authentification et l'autorisation
- Audit dans les sujets relatifs aux identités et aux sujets complémentaires

Implémenter une solution de gestion des identités (3h30)

- Créer, configurer et gérer des identités
- Créer, configurer et gérer des groupes
- Configurer et gérer l'identité des appareils
- Gérer des licences
- Attributs de sécurité personnalisés
- Approvisionnement à l'aide de SCIM
- Configurer la marque de la société
- Configurer et gérer les rôles Microsoft Entra
- Configurer la délégation à l'aide d'unités administratives
- Évaluer les autorisations effectives
- Configurer et gérer des domaines dans Microsoft Entra ID et Microsoft 365
- Configurer des paramètres au niveau du locataire
- Décrire les utilisateurs invités et les comptes B2B
- Gérer les collaborations externes
- Mode de gestion des utilisateurs externes dans Microsoft 365
- Inviter des utilisateurs externes individuellement ou en bloc
- Gérer les comptes d'utilisateur externes dans l'ID Microsoft Entra
- Implémentation de contrôles d'accès interlocataires
- Configurer les fournisseurs d'identité
- Implémenter et gérer l'ID vérifié
- Planifier, concevoir et implémenter Microsoft Entra Connect Sync
- Implémenter et gérer la synchronisation de hachage de mot de passe
- Implémenter et gérer l'authentification directe
- Implémenter et gérer la fédération
- Résoudre les erreurs de synchronisation
- Mettre en oeuvre Microsoft Entra Connect Health
- Gérer la santé de Microsoft Entra Connect
- Travail pratique :
  - Explorer les groupes dynamiques
  - Configurer la collaboration externe
  - Ajouter un utilisateur externe
  - Configurer Microsoft Entra Connect

Implémenter une solution de gestion des authentifications et des accès (3h00)

- Configurer et déployer la réinitialisation du mot de passe en libre-service
- Qu'est-ce que l'authentification multifacteur Microsoft Entra
- Planifier votre authentification multifacteur
- Configurer les méthodes d'authentification multifacteur
- Administrer les méthodes d'authentification
- Implémenter une solution d'authentification basée sur Windows Hello Entreprise
- Désactiver les comptes et révoquer des sessions
- Déployer et gérer la protection par mot de passe
- Configurer des seuils de verrouillage intelligent
- Kerberos dans Microsoft Entra ID
- Authentification par certificat
- Authentification utilisateur Microsoft Entra ID dans les machines virtuelles
- Travail pratique :
  - Configurer et déployer la réinitialisation du mot de passe en libre-service
  - Activer l'authentification multifacteur Microsoft Entra
  - Gérer les valeurs de verrouillage intelligent Microsoft Entra

Planifier, implémenter et administrer l'accès conditionnel, la protection des identités et l'accès aux ressources Azure (3h00)

- Planifier et implémenter les paramètres de sécurité par défaut
- Planifier les stratégies d'accès conditionnel
- Implémenter des contrôles et des affectations de stratégie d'accès conditionnel
- Accès conditionnel basé sur un modèle
- Tester et résoudre les problèmes des stratégies d'accès conditionnel
- Implémenter des contrôles d'application et la gestion des sessions
- Évaluation continue de l'accès
- Contexte d'authentification
- Passer en revue les principes fondamentaux de Identity Protection
- Implémenter et gérer une stratégie de risque d'utilisateur
- Implémenter une stratégie d'inscription MFA
- Surveiller, examiner et corriger les utilisateurs à risque
- Sécurité pour les identités de charge de travail
- Microsoft Defender pour Identity
- Implémenter le gestionnaire d'accès pour des ressources Azure
- Déployer et configurer l'accès global sécurisé
- Travail pratique :
  - Utiliser les paramètres de sécurité par défaut
  - Implémenter des stratégies d'accès conditionnel, des rôles et

des affectations
- Configurer des contrôles de session d'authentification
- Analyser les utilisateurs à risque
- Créer et configurer une identité managée
- Accéder à des ressources Azure avec des identités managées

Implémenter la gestion des accès pour les applications (3h00)

- Qu'est-ce qu'une application
- Explorer une application cloud
- Avantages de l'inscription d'une application
- Applications monolocataires et multilocataires
- Créer une inscription d'application
- Objet application et principal de service
- Découvrir des applications à l'aide de MDCA ou du rapport d'application ADFS
- Configurer des connecteurs aux applications dans MDCA
- Concevoir et implémenter la gestion des accès pour les applications
- Concevoir et implémenter des rôles de gestion des applications
- Configurer des applications SaaS préintégrées
- Implémenter et gérer des stratégies pour les applications OAuth
- Travail pratique :
  - Implémenter la gestion des accès pour les applications
  - Créer un rôle personnalisé pour gérer les inscriptions d'applications

Implémenter et surveiller l'intégration des applications d'entreprise pour l'authentification unique (3h00)

- Implémenter des personnalisations de jetons
- Implémenter et configurer les paramètres de consentement
- Intégrer des applications locales à l'aide du proxy d'application Microsoft Entra
- Intégrer des applications SaaS personnalisées pour l'authentification unique
- Implémenter l'approvisionnement des utilisateurs d'applications
- Superviser et auditer l'accès et l'authentification pour les applications d'entreprise intégrées à Microsoft Entra ID
- Créer et gérer des collections d'applications
- Travail pratique :
  - Ajouter une application locale pour un accès à distance via le proxy d'application
  - Résoudre les problèmes de l'authentification unique SAML pour les applications SaaS personnalisées

Implémenter l'inscription d'applications et l'autorisation d'application (3h00)

- Planifier votre stratégie d'inscription d'application métier
- Implémenter les inscriptions d'applications
- Configurer des autorisations de l'application
- Implémenter l'autorisation d'application
- Gérer et surveiller les applications avec la gouvernance des applications
- Travail pratique :
  - Configurer les autorisations d'une application
  - Tester l'accès à une API protégée
  - Superviser les applications d'entreprise

Planifier et implémenter la gestion des droits d'utilisation et les révisions d'accès (3h00)

- Gestion des droits d'utilisation
- Définir des catalogues
- Définir des packages d'accès
- Planifier, implémenter et gérer des droits d'utilisation
- Implémenter et gérer les conditions d'utilisation
- Gérer le cycle de vie des utilisateurs externes dans Microsoft Entra ID
- Configurer et gérer une organisation connectée
- Passer en revue les droits par utilisateur
- Planifier des révisions d'accès
- Créer des révisions d'accès pour les groupes et les applications
- Créer et configurer des programmes de révision d'accès
- Automatiser les tâches de gestion de la révision d'accès
- Configurer des révisions d'accès récurrentes
- Travail pratique :
  - Créer un catalogue de ressources dans Microsoft Entra ID
  - Implémenter et gérer les conditions d'utilisation
  - Gérer le cycle de vie des utilisateurs externes
  - Créer des révisions d'accès pour les groupes et les applications

Planifier et implémenter un accès privilégié et surveiller Microsoft Entra ID (3h30)

- Définir une stratégie d'accès privilégié pour les utilisateurs administratifs
- Configurer Privileged Identity Management pour les rôles Azure
- Configurer Privileged Identity Management pour les rôles Microsoft Entra
- Planifier et configurer des groupes d'accès privilégié
- Analyser l'historique et les rapports d'audit PIM
- Créer et gérer des comptes d'accès d'urgence
- Surveiller et gérer Microsoft Entra ID
- Surveiller la posture de sécurité avec Identity Secure Score
- Journaux, rapports, supervision et intégration avec Azure Monitor et Microsoft Sentinel
- Travail pratique :
  - Attribuer des rôles de ressources Azure dans PIM
  - Configurer PIM pour les rôles Microsoft Entra
  - Valider les comptes d'accès d'urgence
  - Analyser Identity Secure Score

ENI Service

référence
T126-SC300

28h

Administrateur des identités et des accès Microsoft

Mise à jour
24 avril 2026

2690 € HT

Présentiel/distanciel | Cours Officiel | Formation certifiante

TOP FORMATION

Délais d'accès à la formation

Les inscriptions sont possibles jusqu'à 48 heures avant le début de la formation.
Dans le cas d'une formation financée par le CPF, ENI Service est tenu de respecter un délai minimum obligatoire de 11 jours ouvrés entre la date d'envoi de sa proposition et la date de début de la formation.

Modalités et moyens pédagogiques, techniques et d'encadrement

Formation avec un formateur, qui peut être suivie selon l'une des 3 modalités ci-dessous :
1 Dans la salle de cours en présence du formateur.
2 Dans l'une de nos salles de cours immersives, avec le formateur présent physiquement à distance. Les salles immersives sont équipées d'un système de visio-conférence HD et complétées par des outils pédagogiques qui garantissent le même niveau de qualité.
3 Depuis votre domicile ou votre entreprise. Vous rejoignez un environnement de formation en ligne, à l'aide de votre ordinateur, tout en étant éloigné physiquement du formateur et des autres participants. Vous êtes en totale immersion avec le groupe et participez à la formation dans les mêmes conditions que le présentiel. Pour plus d'informations : Le téléprésentiel notre solution de formation à distance.

Le nombre de stagiaires peut varier de 1 à 12 personnes (5 à 6 personnes en moyenne), ce qui facilite le suivi permanent et la proximité avec chaque stagiaire.
Chaque stagiaire dispose d'un poste de travail adapté aux besoins de la formation, d'un support de cours et/ou un manuel de référence au format numérique ou papier.
Pour une meilleure assimilation, le formateur alterne tout au long de la journée les exposés théoriques, les démonstrations et la mise en pratique au travers d'exercices et de cas concrets réalisés seul ou en groupe.

Modalités d'évaluation des acquis

En début et en fin de formation, les stagiaires réalisent une auto-évaluation de leurs connaissances et compétences en lien avec les objectifs de la formation. L'écart entre les deux évaluations permet ainsi de mesurer leurs acquis.
En complément, le formateur évalue chaque stagiaire sur l'atteinte des objectifs pédagogiques de la formation selon quatre niveaux (non évalué, non acquis, en cours d'acquisition, acquis). Cette évaluation repose sur une modalité choisie par le formateur en cohérence avec la formation : QCM, exercices pratiques réalisés pendant la formation, évaluation finale de synthèse, quiz interactif de validation, étude de cas, mise en situation, analyse de l'auto-évaluation, autres modalités adaptées.
Pour les stagiaires qui le souhaitent, certaines formations peuvent être validées officiellement par un examen de certification. Les candidats à la certification doivent produire un travail personnel important en vue de se présenter au passage de l'examen, le seul suivi de la formation ne constitue pas un élément suffisant pour garantir un bon résultat et/ou l'obtention de la certification.
Pour certaines formations certifiantes (ex : ITIL, DPO, ...), le passage de l'examen de certification est inclus et réalisé en fin de formation. Les candidats sont alors préparés par le formateur au passage de l'examen tout au long de la formation.

Moyens de suivi d'exécution et appréciation des résultats

Feuille de présence, émargée par demi-journée par chaque stagiaire et le formateur.
Evaluation qualitative de fin de formation, qui est ensuite analysée par l'équipe pédagogique ENI.
Attestation de fin de formation, remise au stagiaire en main propre ou par courrier électronique.

Qualification du formateur

La formation est animée par un professionnel de l'informatique et de la pédagogie, dont les compétences techniques, professionnelles et pédagogiques ont été validées par des certifications et/ou testées et approuvées par les éditeurs et/ou notre équipe pédagogique.
Il est en veille technologique permanente et possède plusieurs années d'expérience sur les produits, technologies et méthodes enseignés.
Il est présent auprès des stagiaires pendant toute la durée de la formation.

Accessibilité de la formation