Présentiel/distanciel | Cours Officiel | Formation certifiante

TOP FORMATION

Microsoft Sécurité Administrer les identités et les accès

Cofinancé par l'Union européenne

Objectifs pédagogiques

- Décrire les concepts fondamentaux liés à l'identité numérique dans un environnement Microsoft.
- Comparer les approches centralisées et décentralisées de gestion des identités.
- Discuter de la pertinence du modèle Zero Trust dans le contexte de Microsoft Entra ID.
- Expliquer les mécanismes d'authentification, d'autorisation et d'audit dans le cadre de la gestion des identités.
- Configurer les paramètres initiaux d'un tenant Microsoft Entra ID (branding, rôles, unités administratives, domaines).
- Gérer le cycle de vie des identités (création, suppression, restauration, attribution de licences).
- Identifier les cas d'usage justifiant l'intégration d'identités externes (collaboration B2B, utilisateurs invités).
- Implémenter une architecture d'identité hybride avec Microsoft Entra Connect (PHS, PTA, fédération).
- Expliquer les principes de l'authentification multifacteur (MFA) et des méthodes d'authentification sans mot de passe.
- Déployer et configurer les mécanismes de sécurité d'authentification (FIDO2, OATH, Windows Hello).
- Élaborer des stratégies d'accès conditionnel adaptées aux besoins de l'organisation.
- Diagnostiquer et résoudre des problèmes liés à l'implémentation des politiques d'accès conditionnel.
- Configurer Microsoft Entra Identity Protection pour détecter et atténuer les risques d'identité.
- Déployer des stratégies RBAC pour la gestion des accès aux ressources Azure via des identités managées.
- Concevoir une stratégie d'intégration d'applications pour l'authentification unique (SSO).
- Intégrer des applications SaaS et on-premises avec Microsoft Entra (via connecteurs, proxy d'application).
- Implémenter l'approvisionnement automatisé des utilisateurs et gérer les collections d'applications.
- Définir les rôles et consentements liés à l'inscription d'applications métier.
- Élaborer une stratégie de gestion des droits d'utilisation avec des packages d'accès et des conditions d'utilisation.
- Configurer des révisions d'accès périodiques et automatisées pour les ressources critiques.
- Définir une politique d'accès privilégié avec Microsoft Entra Privileged Identity Management (PIM).
- Interpréter les journaux de connexion et d'audit pour améliorer la sécurité et la conformité.
- Explorer les fonctionnalités avancées de gestion des autorisations dans Microsoft Entra Permissions Management.

Prérequis

- Comprendre les bonnes pratiques de sécurité ainsi que les exigences de sécurité, telles que la défense en profondeur, l'accès avec privilèges minimaux, le contrôle d'accès basé sur les rôles, la responsabilité partagée et le modèle Zero Trust.
- Être familiarisé avec les fournisseurs d'identité tels que Microsoft Entra ID, Microsoft Entra Domain Services ou d'autres fournisseurs d'authentification.
- Avoir une certaine expérience du déploiement de charges de travail Azure. Cette formation ne couvre pas les notions de base de l'administration Azure ; elle s'appuie sur ces connaissances pour approfondir les aspects liés à l'identité et à la sécurité.
- Avoir de l'expérience avec les systèmes d'exploitation Windows et/ou Linux ainsi qu'une expérience de base en langages de script. Cette formation aborde l'utilisation de PowerShell et de l'interface en ligne de commande (CLI).

Public concerné

Ce cours est destiné aux administrateurs d'identité et d'accès qui prévoient de passer l'examen de certification associé ou qui effectuent des tâches d'administration des identités et de l'accès dans le cadre de leur travail quotidien. Ce cours est également utile aux administrateurs ou aux ingénieurs qui souhaitent se spécialiser dans les solutions d'identité et les systèmes de gestion des accès pour les solutions basées sur Azure, et qui jouent un rôle essentiel dans la protection d'une organisation.

ENI Service

référence
T126-SC300

28h

Microsoft Sécurité Administrer les identités et les accès

Mise à jour
13 juillet 2025

2690 € HT

Présentiel/distanciel

Cours Officiel

Formation certifiante

TOP FORMATION

Cofinancé par l'Union européenne

Certification

Cette formation prépare à l'examen « Microsoft Identity and Access Administrator » qui permet d'obtenir la certification Microsoft Certified : Identity and Access Administrator Associate

Programme détaillé

Explorer l'identité dans Microsoft Entra ID (2h00)

- Expliquer le paysage des identités
- Explorer la Confiance zéro avec l'identité
- Discuter de l'identité en tant que plan de contrôle
- Découvrir pourquoi nous avons une identitié
- Définir l'administration des identités
- Contraster les sustèmes d'identité décentralisée avec les systèmes d'identité centralisée
- Discuter des solutions de gestion des identités
- Expliquer Microsoft Entra Business to Business
- Comparer les fournisseurs d'identité Microsoft
- Définir la gestion des licences d'identité
- Explorer l'authentification
- Discuter de l'autorisation
- Expliquer l'audit dans l'identité

Mettre en oeuvre une solution de gestion des identités (5h00)

- Mettre en oeuvre la configuration initiale de Microsoft Entra ID
  - Configurer la marque de l'entreprise
  - Configurer et gérer les rôles Microsoft Entra
  - Travaux pratiques : gérer les rôles d'utilisateurs
  - Configurer la délégation à l'aide d'unités administratives
  - Analyser les autorisations de rôle Microsoft Entra
  - Configurer et gérer des domaines personnalisés
  - Configurer les paramètres au niveau du locataire
  - Travaux pratiques : définition des propriétés au niveau du locataire
- Créer, configurer et gérer les identités
  - Créer, configurer et gérer des identités
  - Travaux pratiques : attribuer des licences aux utilisateurs
  - Travaux pratiques : supprimer ou restaurer des utilisateurs supprimés
  - Créer, configurer et gérer des groupes
  - Travaux pratiques : ajouter des groupes dans Microsoft Entra ID
  - Configurer et gérer l'inscription des appareils
  - Gérer les licences
  - Travaux pratiques : modifier les affectations de licence de groupe
  - Travaux pratiques : modifier des affectations de licence utilisateur
  - Créer des attributs de sécurité personnalisés
  - Explorer la création automatique d'utilisateurs
- Mettre en oeuvre et gérer des identités externes
  - Description de l'accès invité et des comptes interentreprises
  - Gérer les collaborations externes
  - Travaux pratiques : configurer la collaboration externe
  - Inviter des utilisateurs externes : individuellement et en bloc
  - Travaux pratiques : ajouter des utilisateurs invités au répertoire
  - Travaux pratiques : Inviter des utilisateurs en bloc
  - Démonstration : gérer les utilisateurs invités dans Microsoft Entra ID
  - Gérer les comptes d'utilisateur externes dans l'ID Microsoft Entra
  - Gestion des utilisateurs externes dans des charges de travail Microsoft 365
  - Travaux pratiques : explorer les groupes dynamiques
  - Implémenter et gérer l'identité vérifiée Microsoft Entra
  - Configurer les fournisseurs d'identité
  - Implémenter des contrôles d'accès inter-locataires
- Mettre en oeuvre et gérer l'identité hybride
  - Planifier, concevoir et implémenter Microsoft Entra Connect
  - Implémenter et gérer la synchronisation de hachage de mot de passe (PHS)
  - Implémenter et gérer l'authentification directe (PTA)
  - Démonstration : gestion de l'authentification directe et de l'authentification unique (SSO) transparente
  - Implémenter et gérer la fédération
  - Résoudre les erreurs de synchronisation
  - Mettre en oeuvre Microsoft Entra Connect Health
  - Gérer Microsoft Entra Health

Mettre en oeuvre une solution d'authentification et de gestion des accès (7h00)

- Sécuriser les utilisateurs Microsoft Entra avec l'authentification multifacteur (MFA)
  - Qu'est-ce que l'authentification multifacteur Microsoft Entra ?
  - Planifiez votre déploiement de l'authentification multifacteur
  - Travaux pratiques : activer l'authentification multifacteur Microsoft Entra
  - Configurer les méthodes d'authentification multifacteur
- Gérer l'authentification utilisateur
  - Administrer les méthodes d'authentification FIDO2 et sans mot de passe
  - Explorer l'application Authenticator et les jetons OATH
  - Implémenter une solution d'authentification basée sur Windows Hello Entreprise
  - Travaux pratiques : configuration et déploiement de la réinitialisation du mot de passe en libre-service
  - Déployer et gérer la protection par mot de passe
  - Configurer des seuils de verrouillage intelligent
  - Travaux pratiques : gérer les valeurs de verrouillage intelligentes de Microsoft Entra
  - Implémenter l'authentification Kerberos et basée sur un certificat dans Microsoft Entra ID

- Configurer l'authentification utilisateur Microsoft Entra pour les machines virtuelles
- Planifier, mettre en oeuvre et administrer l'accès conditionnel
  - Planifier les paramètres de sécurité par défaut
  - Travaux pratiques : utiliser les paramètres de sécurité par défaut
  - Planifier les stratégies d'accès conditionnel
  - Implémenter des contrôles et des affectations de stratégie d'accès conditionnel
  - Travaux pratiques : implémenter des contrôles et des affectations de stratégie d'accès conditionnel
  - Tester et résoudre les problèmes des stratégies d'accès conditionnel
  - Implémenter des contrôles d'application
  - Implémenter la gestion des sessions
  - Travaux pratiques : configurer des contrôles de session d'authentification
  - Implémenter l'évaluation continue de l'accès
- Gérer Microsoft Entra Identity Protection
  - Passer en revue les principes fondamentaux de Identity Protection
  - Implémenter et gérer une stratégie de risque d'utilisateur
  - Travaux pratiques : activer la stratégie de connexion à risque
  - Travaux pratiques : configurer la stratégie d'inscription de l'authentification multifacteur Microsoft Entra
  - Surveiller, examiner et corriger les utilisateurs à risque
  - Implémenter la sécurité pour les identités de charge de travail
  - Explorer Microsoft Defender pour Identity
- Mettre en oeuvre le gestionnaire d'accès pour des ressources Azure
  - Affecter des rôles Azure
  - Configurer des rôles Azure personnalisés
  - Créer et configurer des identités managées
  - Accéder aux ressources Azure avec des identités managées
  - Analyser les autorisations des rôles Azure
  - Configurer des stratégies RBAC Azure Key Vault
  - Récupérer des objets auprès d'Azure Key Vault
  - Découvrir Gestion des autorisations Microsoft Entra
- Déployer et configurer l'accès global sécurisé Microsoft Entra
  - Explorer Accès global sécurisé
  - Déployer et configurer Accès Internet Microsoft Entra
  - Déployer et configurer Accès privé Microsoft Entra
  - Découvrir comment utiliser le tableau de bord pour piloter Accès global sécurisé
  - Créer des réseaux distants pour les utiliser avec Accès global sécurisé
  - Utiliser l'accès conditionnel avec Accès global sécurisé
  - Explorer les journaux et les options de surveillance d'Accès global sécurisé

Cofinancé par l'Union européenne

Mettre en oeuvre la gestion des accès pour les applications (7h00)

- Planifier et concevoir l'intégration des applications d'entreprise pour l'authentification unique (SSO)
  - Découvrir des applications à l'aide de Microsoft Defender pour les applications Cloud et du rapport d'application des services de fédération Active Directory (AD FS)
  - Configurer des connecteurs aux applications
  - Travaux pratiques : implémenter la gestion des accès pour les applications
  - Concevoir et implémenter des rôles de gestion des applications
  - Travaux pratiques : créer un rôle personnalisé pour gérer l'inscription d'application
  - Configurer des applications SaaS de galerie préintégrées
  - Implémenter et gérer des stratégies pour les applications OAuth
- Mettre en oeuvre et surveiller l'intégration des applications d'entreprise pour l'authentification unique (SSO)
  - Mettre en oeuvre des personnalisations de jetons
  - Mettre en oeuvre 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
  - Mettre en oeuvre l'approvisionnement des utilisateurs basé sur les applications
  - Surveiller et auditer l'accès aux applications d'entreprise intégrées à Microsoft Entra
  - Créer et gérer des collections d'applications
- Mettre en oeuvre l'inscription d'application
  - Planifier votre stratégie d'inscription d'application métier
  - Mettre en oeuvre l'inscription d'application
  - Inscrire une application
  - Configurer l'autorisation pour une application
  - Accorder le consentement administrateur au niveau locataire à des applications
  - Mettre en oeuvre l'autorisation d'application
  - Travaux pratiques : ajouter des rôles à une application et recevoir des jetons
  - Gérer et superviser une application à l'aide de la gouvernance des applications
- Inscrire des applications à l'aide de Microsoft Entra ID
  - Planifier une inscription d'application
  - Explorer des objets d'application et des principaux de service
  - Créer des inscriptions d'applications
  - Configurer l'authentification d'application
  - Configurer les autorisations d'API
  - Créer des rôles d'application

Planifier et mettre en oeuvre une stratégie de gouvernance des

identités (7h00)

- Planifier et mettre en oeuvre la gestion des droits d'utilisation
  - Définir des packages d'accès
  - Travaux pratiques : création et gestion d'un catalogue de ressources avec une gestion des droits d'utilisation de Microsoft Entra
  - Configurer la gestion des droits d'utilisation
  - Travaux pratiques : ajouter un rapport d'acceptation des conditions d'utilisation.
  - Travaux pratiques : gérer le cycle de vie des utilisateurs externes dans Gouvernance des ID Microsoft Entra
  - Configurer et gérer des organisations connectées
  - Passer en revue les droits par utilisateur
- Planifier, mettre en oeuvre et gérer la révision d'accès
  - Planifier des révisions d'accès
  - Créer des révisions d'accès pour les groupes et les applications
  - Créer et configurer des révisions d'accès par programmation
  - Surveiller les résultats de la révision d'accès
  - Automatiser les tâches de gestion de la révision d'accès
  - Configurer des révisions d'accès récurrentes
- Planifier et mettre en oeuvre l'accès privilégié
  - Définir une stratégie d'accès privilégié pour les utilisateurs administratifs
  - Configurer Privileged Identity Management pour les ressources Azure
  - Travaux pratiques : configurer Privileged Identity Management pour les rôles Microsoft Entra
  - Travaux pratiques : assignation de rôles Microsoft Entra dans la gestion des identités privilégiées
  - Travaux pratiques : assignation des rôles de ressources Azure dans la gestion des identités privilégiées
  - Planifier et configurer des groupes d'accès privilégiés
  - Analyser l'historique et les rapports d'audit Privileged Identity Management
  - Créer et gérer des comptes d'accès d'urgence
- Surveiller et gérer Microsoft Entra ID
  - Analyser et examiner les journaux de connexion pour résoudre les problèmes d'accès
  - Examiner et surveiller les journaux d'audit Microsoft Entra
  - Travaux pratiques : connexion de données de Microsoft Entra ID à Microsoft Sentinel
  - Exporter les journaux vers un système de gestion des événements et des informations de sécurité tiers
  - Analyser des classeurs et des rapports Microsoft Entra
  - Surveiller la posture de sécurité avec le score d'identité sécurisée
- Explorer les nombreuses fonctionnalités de gestion des autorisations Microsoft Entra
  - Une expérience complète pour tous les environnements cloud
  - Obtenir des insights généraux dans le tableau de bord Gestion des autorisations
  - Approfondir l'analyse grâce à l'onglet Analytics
  - Obtenir une meilleure compréhension de votre environnement avec les rapports
  - Analyser les données historiques avec l'onglet Audit
  - Prendre des mesures en réponse aux résultats avec l'onglet Correction de Gestion des autorisations
  - Adopter une approche plus proactive de la gestion avec une surveillance continue
  - Gérer l'accès à Gestion des autorisations Microsoft Entra
  - Exemple complet

ENI Service

référence
T126-SC300

28h

Microsoft Sécurité Administrer les identités et les accès

Mise à jour
13 juillet 2025

2690 € HT

Présentiel/distanciel

Cours Officiel

Formation certifiante

TOP FORMATION

Cofinancé par l'Union européenne

Documentation

Support de cours officiel en anglais
Travaux pratiques et/ou Labo en anglais

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, 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

ENI Service s'engage en faveur de l'accessibilité pour les personnes en situation de handicap (PSH). Toutes nos formations sont ainsi accessibles aux PSH. Pour en savoir plus, nous vous invitons à consulter la page "Accueil des personnes en situation de handicap" de notre site internet.