

Administrateur d'identité et d'accès Microsoft

4 jours (28 heures)

Expertise

Présentiel ou classe à distance

à partir de

2 780 € HT par personne (TVA en vigueur)

Repas inclus en présentiel

Contenu mis à jour le 30/09/2026. Document téléchargé le 04/10/2026.

Objectifs

A l'issue de cette formation, vous serez capable de :

- Concevoir, mettre en oeuvre et faire fonctionner les systèmes de gestion des identités et des accès d'une organisation avec Microsoft Entra ID
- Gérer des tâches telles que la fourniture d'un accès sécurisé par authentification aux applications d'entreprise
- Fournir une expérience fluide ainsi que des fonctionnalités de gestion en libre-service à tous les utilisateurs
- Créer un accès adaptatif et une gouvernance de vos solutions de gestion des identités et des accès, en veillant à ce que vous puissiez dépanner, surveiller et établir des rapports sur votre environnement
- Moderniser les solutions d'identité, implémenter des solutions d'identité hybrides et implémenter la gouvernance des identités.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

Administrateurs d'identité et d'accès, ingénieurs.

Prérequis

Avoir suivi les cours MSAZ104 "Microsoft Azure – Administrateur" et SC-900 "Présentation de la sécurité, de la conformité et de l'identité Microsoft" ou avoir les connaissances équivalentes. Connaître les bonnes pratiques de sécurité et exigences de sécurité de l'industrie. Être familiarisé avec les concepts d'identité, comme l'authentification, l'autorisation et Active Directory. Avoir de l'expérience dans le déploiement des charges de travail Azure. Une expérience de base des systèmes d'exploitation Windows et Linux et des langages de script est utile mais pas obligatoire.

Programme

1 Pendant votre formation

Administrateur d'identité et d'accès Microsoft

Explorer l'identité dans Microsoft Entra ID

- Expliquer le paysage des identités
- Explorer "confiance zéro" avec l'identité
- Discuter de l'identité en tant que plan de contrôle
- Découvrir pourquoi nous avons une identité
- Définir l'administration des identités
- Contraster les systèmes 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

Implémenter une solution de gestion des identités

Implémenter la configuration initiale de Microsoft Entra ID

- Configurer la marque de l'entreprise
- Configurer et gérer les rôles Microsoft Entra
- 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

Exemples de travaux pratiques (à titre indicatif)

- Gérer les rôles d'utilisateurs
- Définir des propriétés au niveau du locataire

Créer, configurer et gérer des identités

- Créer, configurer et gérer des identités et des groupes
- Configurer et gérer l'inscription des appareils
- Gestion des licences
- Créer des attributs de sécurité personnalisés
- Explorer la création automatique d'utilisateurs

Exemples de travaux pratiques (à titre indicatif)

- Attribuer des licences aux utilisateurs
- Supprimer ou restaurer des utilisateurs supprimés
- Ajouter des groupes dans Microsoft Entra ID
- Modifier les affectations de licence de groupe
- Modifier les affectations de licence utilisateur

Implémenter et gérer des identités externes

- Description de l'accès invité et des comptes interentreprises
- Gérer les collaborations externes
- Inviter des utilisateurs externes : individuellement et en bloc
- Démonstration : gérer les utilisateurs invités dans Microsoft Entra ID
- Gérer les comptes d'utilisateurs externes dans l'ID Microsoft Entra
- Gestion des utilisateurs externes dans des charges de travail Microsoft 365
- Implémenter et gérer l'identité vérifiée Microsoft Entra
- Configurer les fournisseurs d'identité
- Implémenter des contrôles d'accès interlocataires

Exemples de travaux pratiques (à titre indicatif)

- Configurer la collaboration externe
- Ajouter des utilisateurs invités au répertoire
- Inviter des utilisateurs en bloc
- Explorer les groupes dynamiques

Implémenter 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)
- Explorer l'authentification directe et l'authentification unique transparente

- Implémenter et gérer la fédération
- Résoudre les erreurs de synchronisation
- Mettre en oeuvre Microsoft Entra Connect Health
- Gérer Microsoft Entra Health

Implémenter une solution de gestion des accès et de l'authentification

Sécuriser les utilisateurs Microsoft Entra avec l'authentification multifacteur

- Qu'est-ce que l'authentification multifacteur Microsoft Entra ?
- Planifier votre déploiement de l'authentification multifacteur
- Configurer des méthodes d'authentification multifacteur

Exemple de travaux pratiques (à titre indicatif)

- Activer l'authentification multifacteur Microsoft Entra

Gérer l'authentification des utilisateurs

- 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
- Déployer et gérer la protection par mot de passe
- Configurer des seuils de verrouillage intelligent
- Implémenter l'authentification Kerberos et basée sur un certificat dans Microsoft Entra ID
- Configurer l'authentification utilisateur Microsoft Entra pour les machines virtuelles

Exemples de travaux pratiques (à titre indicatif)

- Configuration et de déploiement de la réinitialisation du mot de passe en libre-service
- Gérer les valeurs de verrouillage intelligentes de Microsoft Entra

Planifier, implémenter et administrer l'accès conditionnel

- Planifier les paramètres de sécurité par défaut
- Planifier les stratégies d'accès conditionnel
- Implémenter les contrôles et les attributions de la stratégie d'accès conditionnel
- Tester et résoudre les problèmes des stratégies d'accès conditionnel
- Implémenter des contrôles d'application
- Implémenter la gestion des sessions et l'évaluation continue de l'accès
- Agent d'optimisation de l'accès conditionnel Microsoft Entra

Exemples de travaux pratiques (à titre indicatif)

- Utiliser les paramètres de sécurité par défaut
- Implémenter des contrôles et des affectations de stratégie d'accès conditionnel
- Configurer des contrôles de session d'authentification

Gérer Microsoft Entra Identity Protection

- Passer en revue les principes fondamentaux de Identity Protection
- Implémenter et gérer une stratégie de risque d'utilisateur
- Surveiller, examiner et corriger les utilisateurs à risque
- Implémenter la sécurité pour les identités de charge de travail
- Explorer Microsoft Defender pour Identity

Exemples de travaux pratiques (à titre indicatif)

- Activer la stratégie de connexion à risque
- Configurer la stratégie d'inscription de l'authentification multifacteur Microsoft Entra

Implémenter 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

Déployer et configurer l'accès sécurisé global de Microsoft Entra

- Explorer l'accès global sécurisé
- Déployer et configurer l'accès Internet Microsoft Entra
- Déployer et configurer l'accès privé Microsoft Entra
- Découvrir comment utiliser le tableau de bord pour piloter l'accès global sécurisé
- Créer des réseaux distants pour les utiliser avec l'accès global sécurisé
- Utiliser l'accès conditionnel avec l'accès global sécurisé
- Explorer les journaux et les options de surveillance de l'accès global sécurisé

Implémenter la gestion des accès pour les applications

Planifier et concevoir l'intégration des applications d'entreprise pour l'authentification unique

- Découvrir les applications à l'aide du rapport d'applications Microsoft Defender pour Cloud Apps et Active Directory Federation Services
- Configurer des connecteurs sur des applications
- Concevoir et implémenter des rôles de gestion des applications
- Configurer des applications SaaS de galerie préintégrées
- Implémenter et gérer des stratégies pour les applications OAuth

Exemples de travaux pratiques (à titre indicatif)

- Implémenter la gestion des accès pour les applications
- Créer un rôle personnalisé pour gérer l'inscription d'application

Implémenter et surveiller l'intégration des applications d'entreprise pour l'authentification unique

- Implémenter des personnalisations de jetons
- Implémenter et configurer les paramètres de consentement
- Intégrer des applications locales avec le proxy d'application Microsoft Entra
- Intégrer des applications SaaS personnalisées pour l'authentification unique
- Implémenter le provisionnement d'utilisateurs basé sur l'application
- Surveiller et auditer l'accès aux applications d'entreprise intégrées Microsoft Entra
- Créer et gérer des collections d'applications

Implémenter l'inscription d'application

- Planifier votre stratégie d'inscription d'application métier
- Implémenter l'inscription d'application
- Inscrire une application
- Configurer l'autorisation pour une application
- Accorder le consentement administrateur au niveau locataire à des applications
- Implémenter l'autorisation d'application
- Gérer et surveiller l'application à l'aide de la gouvernance des applications

Exemple de travaux pratiques (à titre indicatif)

- Ajouter des rôles à une application et recevoir des jetons

Inscrire des applications à l'aide de Microsoft Entra ID

- Planifier une inscription d'application
- Explorer des objets d'application et des principaux services
- Créer des inscriptions d'applications
- Configurer l'authentification d'application
- Configurer les autorisations d'API
- Créer des rôles d'application

Planifier et implémenter une stratégie de gouvernance des identités

Planifier et implémenter la gestion des droits d'utilisation

- Définir des packages d'accès
- Configurer la gestion des droits d'utilisation
- Configurer et gérer des organisations connectées
- Passer en revue les droits par utilisateur

Exemples de travaux pratiques (à titre indicatif)

- Créer et gérer un catalogue de ressources avec une gestion des droits d'utilisation de Microsoft Entra
- Ajouter un rapport d'acceptation des conditions d'utilisation
- Gérer le cycle de vie des utilisateurs externes avec la gouvernance des identités Microsoft Entra

Planifier, implémenter 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 implémenter un accès privilégié

- Définir une stratégie d'accès privilégié pour les utilisateurs administratifs
- Configurer Privileged Identity Management pour les ressources Azure
- 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

Exemples de travaux pratiques (à titre indicatif)

- Configurer Privileged Identity Management pour les rôles Microsoft Entra
- Attribuer des rôles Microsoft Entra dans Privileged Identity Management
- Assigner des rôles de ressources Azure dans Privileged Identity Management

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
- 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

Exemple de travaux pratiques (à titre indicatif)

- Connexion de données de Microsoft Entra ID à Microsoft Sentinel

Certification (en option)

- Prévoir l'achat d'un voucher en supplément
- Le passage de l'examen se fera (ultérieurement) dans un centre agréé Pearson Vue
- L'examen (en anglais) s'effectuera en ligne

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2I, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

* nous consulter pour la faisabilité en distanciel

** ratio variable selon le cours suivi

[Accessibilité aux personnes en situation de handicap](#)

Détails de la session

Du 2 novembre 2027 au 5 novembre 2027 (4 jours / 28 heures)

Paris La Défense

Du 2 novembre 2027 au 5 novembre 2027

Paris La Défense

- 2 novembre 2027 9h00 – 15h30
- 3 novembre 2027 9h00 – 15h30
- 4 novembre 2027 9h00 – 15h30
- 5 novembre 2027 9h00 – 15h30