

Certifiante Sessions garanties disponibles

Formation Administrateur d'identité et de l'accès Microsoft (SC-300)

Réf. SF33998

4 jours de formation pour maîtriser les fonctionnalités Microsoft Entra ID !

4 j Durée	3 000 € HT Inter / participant	9 800 € HT Intra (≤12 pers.)	2 Sessions à venir
--------------	-----------------------------------	---------------------------------	-----------------------

Objectifs pédagogiques

- ✓ Implémenter et gérer des identités utilisateur
- ✓ Implémenter la gestion des authentifications et des accès
- ✓ Planifier et implémenter des identités de charge de travail
- ✓ Planifier et implémenter la gouvernance des identités

Public visé & prérequis

Public visé Administrateurs systèmes et réseaux	Prérequis Avoir suivi les formations "Les fondamentaux de la sécurité, de la conformité et de l'identité Microsoft" (SC-900) et "Microsoft Azure Administration" (AZ-104) ou disposer des connaissances équivalentes.
--	--

Programme détaillé

Configurer et gérer une instance Microsoft Entra

Configurer et gérer des rôles Microsoft Entra intégrés et personnalisés
Recommander quand utiliser des unités administratives
Configurer et gérer des unités administratives
Évaluer les autorisations effectives pour les rôles Microsoft Entra
Configurer et gérer des domaines personnalisés
Configurer les paramètres de personnalisation de l'entreprise
Configurer les propriétés du locataire, les paramètres utilisateur, les paramètres de groupe et les paramètres de l'appareil

Créer, configurer et gérer des identités Microsoft Entra

Créer, configurer et gérer des identités
Créer, configurer et gérer des groupes
Gérer les attributs de sécurité personnalisés
Automatiser la gestion des utilisateurs et des groupes à l'aide de PowerShell
Attribuer, modifier et créer des rapports sur les licences

Implémenter et gérer des identités pour les utilisateurs et locataires externes

Gérer les paramètres de collaboration externe dans l>ID Microsoft Entra
Inviter des utilisateurs externes, individuellement ou en bloc
Gérer les comptes d'utilisateur externes dans l>ID Microsoft Entra
Implémenter les paramètres d'accès entre locataires
Implémenter et gérer la synchronisation entre locataires
Configurer des fournisseurs d'identité, notamment SAML et WS-Fed
Créer et gérer un locataire Microsoft Entra B2C (ID externe Microsoft Entra)

Implémenter et gérer l'identité hybride

Implémenter et gérer Microsoft Entra Connect
Implémenter et gérer la synchronisation cloud Microsoft Entra Connect
Implémenter et gérer la synchronisation de hachage de mot de passe

Implémenter et gérer l'authentification directe
Implémenter et gérer l'authentification unique transparente
Implémenter et gérer la fédération, à l'exception des déploiements manuels des services de fédération Active Directory (AD FS)
Implémenter et gérer Microsoft Entra Connect Health
Résoudre les erreurs de synchronisation

Planifier, implémenter et gérer l'authentification utilisateur Microsoft Entra

Planifier l'authentification
Implémenter et gérer des méthodes d'authentification
Implémenter et gérer les paramètres MFA (Multi-Factor Authentication) à l'échelle du locataire
Gérer les paramètres MFA par utilisateur
Configurer et déployer la réinitialisation de mot de passe en libre-service (SSPR)
Implémenter et gérer Windows Hello Entreprise
Désactiver les comptes et révoquer des sessions utilisateur
Implémenter et gérer la protection par mot de passe et les verrouillages intelligents
Activer l'authentification Microsoft Entra Kerberos pour les identités hybrides
Implémenter l'authentification basée sur des certificats dans Microsoft Entra

Planifier, implémenter et gérer l'accès conditionnel Microsoft Entra

Planifier les stratégies d'accès conditionnel
Implémenter des attributions de stratégie d'accès conditionnel
Implémenter des contrôles de stratégie d'accès conditionnel
Tester et résoudre les problèmes des stratégies d'accès conditionnel
Implémenter la gestion des sessions
Implémenter des restrictions appliquées par l'appareil
Implémenter l'évaluation continue de l'accès
Créer une stratégie d'accès conditionnel à partir d'un modèle

Gérer les risques à l'aide de Protection Microsoft Entra ID

Implémenter et gérer des stratégies de risque utilisateur
Implémenter et gérer des stratégies de risque de connexion
Implémenter et gérer des stratégies d'inscription MFA
Superviser, investiguer et corriger les utilisateurs à risque
Surveiller, examiner et corriger les identités de charge de travail à risque

Implémenter la gestion des accès pour les ressources Azure à l'aide de rôles Azure

Créer des rôles Azure personnalisés, notamment des autorisations de plan de contrôle et de plan de données
Attribuer des rôles Azure intégrés et personnalisés
Évaluer les autorisations effectives pour un ensemble de rôles Azure
Attribuer des rôles Azure pour activer la connexion Microsoft Entra ID aux machines virtuelles Azure
Configurer le contrôle d'accès en fonction du rôle Azure Key Vault (RBAC) et les stratégies d'accès

Planifier et implémenter des identités pour les applications et les charges de travail Azure

Sélectionner les identités appropriées pour les applications et les charges de travail Azure, notamment les identités managées, les principaux de service, les comptes d'utilisateur et les comptes de service gérés
Créer des identités managées
Attribuer une identité managée à une ressource Azure
Utiliser une identité managée affectée à une ressource Azure pour accéder à d'autres ressources Azure

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

Configurer et gérer le consentement de l'utilisateur et de l'administrateur
Découvrir des applications à l'aide de rapports d'activité d'application AD FS
Planifier et implémenter des paramètres pour les applications d'entreprise, y compris les paramètres au niveau de l'application et du locataire
Attribuer des rôles Microsoft Entra appropriés aux utilisateurs pour gérer les applications d'entreprise
Superviser et auditer l'activité dans des applications d'entreprise
Concevoir et implémenter l'intégration pour les applications locales à l'aide du proxy d'application Microsoft Entra
Concevoir et implémenter l'intégration pour les applications SaaS (Software as a Service)
Attribuer, classer et gérer des utilisateurs, des groupes et des rôles d'application pour les applications d'entreprise

Créer et gérer des collections d'applications

Planifier et implémenter des inscriptions d'applications

Planifier les inscriptions d'applications
Créer des inscriptions d'applications
Configurer l'authentification d'application
Configurer 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

Configurer et analyser les résultats de la découverte cloud à l'aide de Defender pour Cloud Apps
Configurer des applications connectées
Implémenter des restrictions appliquées par l'application
Configurer le contrôle d'application d'accès conditionnel
Créer des stratégies d'accès et de session dans Defender pour Cloud Apps
Implémenter et gérer des stratégies pour les applications OAuth
Gérer le catalogue d'applications cloud

Planifier et implémenter la gestion des droits d'utilisation dans Microsoft Entra

Planifier les droits
Créer et configurer des catalogues
Créer et configurer des packages d'accès
Gérer les demandes d'accès
Implémenter et gérer les conditions d'utilisation (ToU)
Gérer le cycle de vie des utilisateurs externes
Configurer et gérer des organisations connectées

Planifier, implémenter et gérer les révisions d'accès dans Microsoft Entra

Planifier des révisions d'accès
Créer et configurer des révisions d'accès
Superviser l'activité de révision d'accès
Répondre manuellement à l'activité de révision d'accès

Planifier et implémenter un accès privilégié

Planifier et gérer des rôles Azure dans Microsoft Entra Privileged Identity Management (PIM), y compris les paramètres et les affectations
Planifier et gérer les ressources Azure dans PIM, y compris les paramètres et les affectations
Planifier et configurer des groupes d'accès privilégiés
Gérer le processus de demande et d'approbation PIM
Analyser l'historique et les rapports d'audit PIM
Créer et gérer des comptes d'accès d'urgence

Surveiller l'activité des identités à l'aide des journaux, des classeurs et des rapports

Concevoir une stratégie pour surveiller Microsoft Entra
Examiner et analyser les journaux de connexion, d'audit et d'approvisionnement à l'aide du Centre d'administration Microsoft Entra
Configurer les paramètres de diagnostic, notamment la configuration des destinations telles que les espaces de travail Log Analytics, les comptes de stockage et les hubs d'événements
Surveiller Microsoft Entra à l'aide de requêtes KQL dans Log Analytics
Analyser Microsoft Entra à l'aide de classeurs et de rapports
Surveiller et améliorer la posture de sécurité à l'aide du score de sécurisation d'identité

Planifier et implémenter la gestion des autorisations Microsoft Entra

Intégrer des abonnements Azure à la gestion des autorisations
Évaluer et corriger les risques liés aux identités, ressources et tâches Azure
Évaluer et corriger les risques liés aux rôles hautement privilégiés Azure
Évaluer et corriger les risques liés à l'index PCI (Permissions Creep Index) dans Azure
Configurer des alertes d'activité et des déclencheurs pour les abonnements Azure

Prochaines sessions

DATE	LIEU	STATUT
30/11/2026	à distance	Sur confirmation
22/03/2027	à distance	Sur confirmation

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

Note moyenne des participants de la filière Cybersécurité et Protection des Données : 4,9/5 — 13 avis

William B. — Prévoir l'envoi à chaque participant du livre de CISS au moins un mois avant la formation.

Mickael L. — il est top Romain GARCIA

Votre formateur

Loïc D. — Formateur Microsoft Azure & Windows

Loïc intervient sur des formations portant sur Microsoft Azure. Les sujets abordés incluent notamment Windows. Son activité de formation remonte à 2018.

Ils nous font confiance

Cette année notre filière Gouvernance, Risques & Conformité (GRC) a accompagné plus de 30 entreprises dont :

AVEM MÉTROPOLE DE LYON ADISTA ALSTOM ASTEK FRANCE AXA ASSISTANCE FRANCE COMMUNAUTÉ DE COMMUNES DES HAUTS DE FLANDRE CONSORT FRANCE ECONOCOM SERVICES & SOLUTION EGIS +20 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com