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

SYSTÈMES RÉSEAUX ET SÉCURITÉ

Objectifs	À l'issue de ce cours / certification, tu seras capable de : Concevoir, implémenter et exploiter les systèmes de gestion des identités et des accès d'une organisation en utilisant Microsoft Entra ID - Fournir une authentification et une autorisation sécurisées pour les applications d'entreprise - Offrir aux utilisateurs une expérience fluide, avec des capacités de gestion en libre-service - Mettre en œuvre des solutions d'accès adaptatif (Conditional Access), des vérifications de risque, de l'authentification multi-facteurs (MFA), etc - Superviser, surveiller, rapporter et gouverner les identités et accès (logs, revues d'accès, gestion des privilèges, etc.) - Intégrer des environnements hybrides (on-prem + cloud) et des identités externes / intertenant.
Participants	Administrateur et responsable de solutions traditionnelles souhaitant évoluer vers Azure - Tout professionnel de l'informatique s'interrogeant sur Microsoft Azure.
Prérequis	Une bonne compréhension des concepts de base de la sécurité, tels que le modèle « zero trust », le moindre privilège (least privilege), la responsabilité partagée, etc - Connaissance des concepts fondamentaux liés à l'identité : authentification, autorisation, annuaires (Active Directory), etc - Expérience avec Azure / Microsoft 365 (services et workloads) et avec l'Active Directory (on-prem) pour comprendre les environnements hybrides - Compétences de base avec PowerShell, voire d'autres outils de scripting ou lignes de commande, pour les opérations automatisées - Parfois, des cours préalables recommandés comme SC-900 (Security, Compliance, and Identity Fundamentals) ou AZ-104 (Azure Administrator) selon le fournisseur de formation.
Moyens pédagogiques	1 poste par participant - 1 Vidéo projecteur - Support de cours fourni à chaque participant - Ateliers Individuels - Modalités d'évaluation : Ateliers (TP) pendant tout le long de la formation et Evaluation des acquis tout au long de la formation.
Méthodes pédagogiques	Exposés théoriques et démonstrations. Le formateur évalue la progression pédagogique des apprenants via des QCM et échanges d'expériences Mises en situation et travaux dirigés Accompagnement personnalisé du formateur avec des tests de positionnement.
Type de formation	Formation présentielle ou distancielle, selon les besoins et les contraintes des participants.
Tarif inter-entreprise	2790 € HT
Durée	4 jour(s) - 28 heure(s)

Code : NCI_10RTLNR

Programme :

Explorer l'identité dans Microsoft Entra ID

Comprendre le paysage de l'identité.
Découvrir le modèle Zéro Trust appliqué à l'identité.
L'identité comme plan de contrôle.
Comprendre pourquoi l'identité est essentielle.
Définir l'administration des identités.
Comparer identité décentralisée et systèmes d'identité centralisés.
Présentation des solutions de gestion des identités.
Comprendre Microsoft Entra Business to Business.
Comparer les fournisseurs d'identité Microsoft.
Définir la gestion des licences d'identité.
Explorer l'authentification.
Comprendre l'autorisation.

Implémenter une solution de gestion des identités

Configurer initialement Microsoft Entra ID.
Créer, configurer et gérer les identités.
Mettre en œuvre et gérer les identités externes.
Mettre en œuvre et gérer une identité hybride.

Implémenter une solution d'authentification et de gestion des accès

Sécuriser les utilisateurs Microsoft Entra avec l'authentification multifacteur (MFA).
Gérer l'authentification des utilisateurs.
Gérer la protection des identités Microsoft Entra.
Mettre en œuvre la gestion des accès aux ressources Azure.
Déployer et configurer l'accès global sécurisé Microsoft Entra.

Implémenter la gestion des accès pour les applications

Planifier et concevoir l'intégration des applications d'entreprise pour le SSO.
Mettre en œuvre et surveiller l'intégration des applications d'entreprise pour le SSO.
Mettre en œuvre l'enregistrement des applications.
Enregistrer les applications dans Microsoft Entra ID.

Planifier et mettre en œuvre une stratégie de gouvernance des identités

Planifier et mettre en œuvre la gestion des habilitations.
Planifier, mettre en œuvre et gérer les revues d'accès.
Planifier et mettre en œuvre l'accès privilégié.
Surveiller et maintenir Microsoft Entra ID.

WEDO 365 by NCI

Caen - Paris - Lyon - Rennes - Nantes - Le Havre - Nice - Montpellier - Lille - Toulon
Saint-Etienne - Toulouse - Montpellier - Bordeaux - Grenoble - Le Mans - Tours - Marseille
www.wedo365.fr - commercial@nci.fr - Tél : +33 (0)2 14 99 00 20

WEDO 365 by NCI
Caen - Paris - Lyon - Rennes - Nantes - Le Havre - Nice - Montpellier - Lille - Toulon
Saint-Etienne - Toulouse - Montpellier - Bordeaux - Grenoble - Le Mans - Tours - Marseille
www.wedo365.fr - commercial@nci.fr - Tél : +33 (0)2 14 99 00 20