

Référence : CERT-MS102	Niveau : Administrateur	Prochaines sessions
Durée : 5 jours	Tarif : 2 800,00 €	<a href="#">Intra à distance.</a>
Nombre de participants par session : 8 maximum	Offre certifiante	<a href="#">Intra sur site.</a>
		Inter à distance uniquement
		<a href="#">Prochaines dates en ligne</a>
Pour toutes demandes concernant cette formation <a href="#">Nous Contacter</a>		

Avec cette formation, vous acquerez les connaissances et les compétences nécessaires pour déployer et gérer Microsoft 365 dans un environnement d'entreprise.

Vous disposerez d'une vue d'ensemble des éléments clés de l'administration de Microsoft 365: le déploiement et la gestion des locataires, la gestion des identités ainsi que la gestion de la sécurité et conformité Microsoft 365.

**Vous disposerez pendant la formation d'un environnement Microsoft 365 répondant à tous les prérequis exigés pour la formation MS-102 Administrateur Microsoft 365.**

Si vous souhaitez passer la certification MS-102 nous proposons d'ajouter le prix du passage de l'examen (165 €/participant) et nous proposons un accompagnement jusqu'à la réussite de l'examen pour un montant de 400 €/participant.

L'accompagnement à la réussite de l'examen MS-102 vous permettra de vous entraîner sur des questions proches de l'examen et d'avoir 2 sessions d'accompagnement avec le formateur.

#### Public

Administrateurs Microsoft 365.

#### Pré-requis

Expérience dans l'administration des charges de travail Microsoft 365 et Entra (Azure Active Directory).

Connaissance pratique de la mise en réseau, de l'administration de serveurs, du DNS et de PowerShell.

#### Avant ce Stage

#### Pédagogie

50 % de cours et démonstrations - 50% de mise en pratique

#### Après ce Stage

## Objectifs

- Déployer et gérer un locataire Microsoft 365
- Implémenter et gérer les identités et les accès dans Entra
- Gérer la sécurité et les menaces à l'aide de Microsoft 365 Defender
- Gérer la conformité à l'aide de Microsoft Purview

- Le bon pour passer la certification peut être obtenu en plus pour un montant de 165 euros.
- Un suivi et du monitorat par un formateur certifié et une aide à la préparation à la certification MS-102 est possible pour un montant de 400 euros par participant.

## Profil de l'animateur

Formateur Microsoft Certified Trainer et certifié MS-102 Administrateur Microsoft 365.

## Méthode d'évaluation

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.

## Module 1 - Implémenter et gérer un locataire Microsoft 365

- Créer un locataire.
- Implémenter et gérer des domaines.
- Configurer les paramètres de l'organisation, y compris la sécurité, la confidentialité et le profil.
- Identifier et répondre aux problèmes dans Service Health.
- Configurer les notifications dans Service Health.
- Superviser l'adoption et l'usage.

### Travaux Pratiques

- Initialiser un tenant Microsoft 365
- Définir les paramètres globaux d'un tenant Microsoft 365
- Installer les bibliothèques PowerShell pour se connecter à Graph
- Personnalisation du Tenant avec la charte graphique de l'entreprise

## Module 2 - Gérer les utilisateurs et les groupes

- Créer et gérer des utilisateurs.
- Créer et gérer des utilisateurs invités.
- Créer et gérer des contacts.
- Créer et gérer des groupes, y compris des groupes Microsoft 365.
- Gérer et superviser les allocations des licences Microsoft 365.
- Réaliser une gestion groupée des utilisateurs, y compris sur PowerShell.

### Travaux Pratiques

- Gérer les utilisateurs et les groupes
- Ajouter un domaine d'entreprise

## Module 3 - Gérer les rôles dans Microsoft 365

- Gérer les rôles dans Microsoft 365 et Entra.
- Gérer des groupes de rôles pour les charges de travail Microsoft Defender, Microsoft Purview et Microsoft 365.
- Gérer la délégation à l'aide d'Administrative Units.
- Implémenter Privileged Identity Management pour les rôles Azure AD.

### Travaux Pratiques

- Administrer la délégation de l'administration
- Suivre et vérifier le fonctionnement de Microsoft 365
- Déployer la suite Microsoft 365

## Module 4 - Implémenter et gérer la synchronisation des identités avec Azure AD

- Préparer la synchronisation des identités à l'aide d'IdFix.
- Implémenter et gérer la synchronisation des annuaires à l'aide d'Entra Connect cloud sync.
- Implémenter et gérer la synchronisation des annuaires à l'aide d'Entra Connect.
- Superviser la synchronisation à l'aide d'Entra Connect Health.
- Résoudre les problèmes de synchronisation, y compris sur Entra Connect et Entra Connect cloud sync.

## Travaux Pratiques

- Préparer Active Directory pour une synchronisation
- Mise en place de la synchronisation avec Entra

## Module 5 - Implémenter et gérer l'authentification

- Implémenter et gérer les méthodes d'authentification.
- Implémenter et gérer Self-Service Password Reset (SSPR).
- Implémenter et gérer Entra Password Protection.
- Implémenter et gérer l'authentification multi-facteur (MFA).
- Investiguer et résoudre les problèmes d'authentification.

## Travaux Pratiques

- Configurer l'authentification unique fluide

## Module 6 - Implémenter et gérer l'accès sécurisé

- Planifier la protection des identités.
- Implémenter et gérer Azure AD Identity Protection.
- Planifier des stratégies d'accès conditionnel.
- Implémenter et gérer des stratégies d'accès conditionnel.

## Travaux Pratiques

- Accès conditionnel MFA en fonction de l'emplacement

## Module 7 - Gérer les rapports de sécurité et les alertes avec Microsoft 365 Defender

- Evaluer et prendre des mesures pour améliorer le niveau de sécurité Microsoft dans le portail Microsoft 365 Defender.
- Evaluer et répondre aux incidents et alertes de sécurité dans Microsoft 365 Defender.
- Examiner et répondre aux problèmes identifiés dans les rapports de sécurité et de conformité Microsoft 365 Defender.
- Evaluer et répondre aux menaces identifiées dans l'analyse des menaces.

## Travaux Pratiques

- Utiliser les recommandations pour améliorer sa posture de sécurité

- Etre alerter en cas d'attaques

## Module 8 - Implémenter et gérer la protection de la messagerie et de la collaboration

- Implémenter des stratégies et des règles dans Defender for Office 365.
- Examiner et répondre aux menaces identifiées dans Defender for Office 365, y compris les menaces et les investigations.
- Créer et exécuter des campagnes, telles que la simulation d'attaque.
- Débloquer les utilisateurs.

### Travaux Pratiques

- Conduire une simulation d'attaque auprès d'une population d'utilisateurs
- Analyser les résultats et prendre les mesures

## Module 9 - Implémenter et gérer la protection des Endpoint

- Intégrer des appareils dans Defender for Endpoint.
- Configurer les paramètres dans Defender for Endpoint.
- Examiner et répondre aux vulnérabilités des Endpoint.
- Examiner et répondre aux risques identifiés dans le tableau de bord de Microsoft Defender Vulnerability Management.

### Travaux Pratiques

- Atténuer la surface face aux ransomwares

## Module 10 - Implémenter la protection des informations et la gestion de cycle de vie

- Implémenter et gérer des informations sensibles.
- Implémenter des étiquettes de rétention, des stratégies d'étiquette de rétention et des stratégies de rétention.
- Implémenter des étiquettes de confidentialité et des stratégies d'étiquette de confidentialité.

### Travaux Pratiques

- Créer une étiquette de confidentialité pour du contenu crypté
- Créer une règle pour de l'archivage

## Module 11 - Implémenter Microsoft Purview Data Loss Prevention (DLP)

- Implémenter DLP pour les charges de travail.
- Implémenter Endpoint DLP.
- Examiner et répondre aux alertes, événements et rapports dans DLP.

## Travaux Pratiques

- Créer des stratégies DLP
- Tester le fonctionnement d'une DLP
- Mise en place d'étiquette de confidentialité

## Clôture de Stage

Rappel en synthèse de la formation, votre avis sur la formation et vos suggestions.