

Durée : 5 jours soit 35 heures

Référence : MS-102T00

**Public visé :**

- Cette formation est destinée personnes qui aspirent au rôle d'administrateur Microsoft 365 et qui ont suivi au moins l'un des parcours de certification d'administrateur basés sur les rôles Microsoft 365.

**Pré-requis :**

Pour suivre cette formation les apprenants doivent avoir :

- Avoir suivi un cours d'administrateur basé sur les rôles, tel que la messagerie, le travail d'équipe, la sécurité, la conformité ou la collaboration.
- Une compréhension approfondie du DNS et une expérience fonctionnelle de base avec les services Microsoft 365.
- Une compréhension approfondie des pratiques informatiques générales.
- Une connaissance pratique de PowerShell.

**Objectifs pédagogiques :**

- Configurer le profil d'organisation de votre entreprise dans Microsoft 365.
- Maintenir les exigences minimales d'abonnement pour votre entreprise.
- Gérer les services et compléments de Microsoft 365 en attribuant des licences supplémentaires, en achetant plus de stockage, etc.
- Créer une liste de contrôle pour vérifier si votre locataire Microsoft 365 répond aux besoins de votre entreprise.
- Identifier le modèle d'identité utilisateur le mieux adapté à votre organisation.
- Créer des comptes d'utilisateurs à partir du Centre d'administration Microsoft 365 et de Windows PowerShell.
- Gérer les comptes d'utilisateurs et les licences dans Microsoft 365.
- Récupérer les comptes d'utilisateurs supprimés dans Microsoft 365.
- Effectuer une maintenance utilisateur en bloc dans Azure Active Directory.
- Créer et gérer des contacts de messagerie à partir du Centre d'administration Exchange et d'Exchange Online PowerShell.
- Décrire les différents types de groupes disponibles dans Microsoft 365 et les créer et les gérer.
- Ajouter un domaine personnalisé à votre déploiement Microsoft 365 et planifier les zones DNS et les enregistrements nécessaires.

**Modalités pédagogiques :**

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises ou intra-entreprises sur mesure.

La formation est animée par un(e) formateur(trice) durant toute la durée de la session et présentant une suite de modules théoriques clôturés par des ateliers pratiques validant l'acquisition des connaissances. Les ateliers peuvent être accompagnés de Quizz.

L'animateur(trice) présente la partie théorique à l'aide de support de présentation, d'animation réalisée sur un environnement de démonstration.

En présentiel comme en téléprésentiel, l'animateur(trice) accompagne les participants durant la réalisation des ateliers.

**Moyens et supports pédagogiques :**

**Cadre présentiel**

Salles de formation équipées et accessibles aux personnes à mobilité réduite.

- Un poste de travail par participant
- Un support de cours numérique ou papier (au choix)
- Un bloc-notes + stylo
- Vidéoprojection sur tableau blanc
- Connexion Internet
- Accès extranet pour partage de documents et émargement électronique

**Cadre téléprésentiel**

Session dispensée via notre solution iClassroom s'appuyant sur Microsoft Teams.

- Un compte Office 365 par participant
- Un poste virtuel par participant
- Un support numérique (PDF ou Web)
- Accès extranet pour partage de documents et émargement électronique

**Modalités d'évaluation et suivi :**

**Avant**

Afin de valider le choix d'un programme de formation, une évaluation des prérequis est réalisée à l'aide d'un questionnaire en ligne ou lors d'un échange avec le formateur(trice) qui validera la base de connaissances nécessaires.

**Pendant**

Après chaque module théorique, un ou des ateliers pratiques permettent la validation de l'acquisition des connaissances. Un Quizz peut accompagner l'atelier pratique.

**Après**

Un examen de certification si le programme de formation le prévoit dans les conditions de l'éditeur ou du centre de test (TOSA, Pearson Vue, ENI, PeopleCert)

**Enfin**

Un questionnaire de satisfaction permet au participant d'évaluer la qualité de la prestation.

**Description / Contenu**

**Module 1 : Configurez votre expérience Microsoft 365**

- Configurez votre expérience Microsoft 365

- Gérer vos abonnements de locataire dans Microsoft 365
- Intégrez Microsoft 365 aux applications d'engagement client



- Terminer la configuration de votre client dans Microsoft 365
- Quizz

**Module 2 : Gérer les utilisateurs, les licences et les contacts de messagerie dans Microsoft 365**

- Déterminer le modèle d'identité utilisateur pour votre organisation
- Créer des comptes d'utilisateurs dans Microsoft 365
- Gérer les paramètres de compte d'utilisateur dans Microsoft 365
- Gérer les licences utilisateur dans Microsoft 365
- Récupérer les comptes d'utilisateurs supprimés dans Microsoft 365
- Effectuer la maintenance en masse des utilisateurs dans Azure Active Directory
- Créer et gérer des utilisateurs invités
- Créer et gérer des contacts de messagerie
- Quizz

**Module 3 : Gérer les groupes dans Microsoft 365**

- Examiner les groupes dans Microsoft 365
- Créer et gérer des groupes dans Microsoft 365
- Créer des groupes dynamiques à l'aide du générateur de règles Azure
- Créer une stratégie de nommage de groupe Microsoft 365
- Créer des groupes dans Exchange Online et SharePoint Online
- Quizz

**Module 4 : Ajouter un domaine personnalisé dans Microsoft 365**

- Planifier un domaine personnalisé pour votre déploiement Microsoft 365
- Planifier les zones DNS pour un domaine personnalisé
- Planifier les exigences d'enregistrement DNS pour un domaine personnalisé
- Créer un domaine personnalisé dans Microsoft 365
- Quizz

**Module 5 : Configurer la connectivité client à Microsoft 365**

- Examiner le fonctionnement de la configuration automatique du client
- Explorer les enregistrements DNS requis pour la configuration du client
- Configurer les clients Outlook
- Dépanner la connectivité client
- Quizz

**Module 6 : Configurer les rôles administratifs dans Microsoft 365**

- Explorer le modèle d'autorisation Microsoft 365
- Explorer les rôles d'administrateur de Microsoft 365
- Attribuer des rôles d'administrateur aux utilisateurs dans Microsoft 365
- Déléguez les rôles d'administration aux partenaires
- Gérer les autorisations à l'aide d'unités administratives dans Azure Active Directory
- Élever les privilèges à l'aide d'Azure AD Privileged Identity Management
- Examiner les meilleures pratiques lors de la configuration des rôles administratifs
- Quizz

**Module 7 : Gérer la santé et les services des locataires dans Microsoft 365**

- Surveillez la santé de vos services Microsoft 365

- Surveiller la santé des locataires à l'aide du score d'adoption de Microsoft 365
- Surveiller la santé des locataires à l'aide de l'analyse de l'utilisation de Microsoft 365
- Élaborer un plan de réponse aux incidents
- Demander de l'aide à Microsoft
- Quizz

**Module 8 : Déployer les applications Microsoft 365 pour les entreprises**

- Explorer les fonctionnalités des applications Microsoft 365 pour les entreprises
- Explorez la compatibilité de votre application à l'aide de la boîte à outils de préparation
- Effectuez une installation en libre-service des applications Microsoft 365 pour les entreprises
- Déployer les applications Microsoft 365 pour les entreprises avec Microsoft Configuration Manager
- Déployez les applications Microsoft 365 pour les entreprises à partir du cloud
- Déployer les applications Microsoft 365 pour les entreprises à partir d'une source locale
- Gérer les mises à jour des applications Microsoft 365 pour les entreprises
- Explorez les canaux de mise à jour pour les applications Microsoft 365 pour les entreprises
- Gérez vos applications cloud à l'aide du centre d'administration des applications Microsoft 365
- Quizz

**Module 9 : Analysez les données de votre lieu de travail Microsoft 365 à l'aide de Microsoft Viva Insights**

- Examiner les fonctionnalités analytiques de Microsoft Viva Insights
- Créez une analyse personnalisée avec Microsoft Viva Insights
- Configurer Microsoft Viva Insights
- Examiner les sources de données Microsoft 365 utilisées dans Microsoft Viva Insights
- Préparer les données organisationnelles dans Microsoft Viva Insights
- Quizz

**Module 10 : Explorer la synchronisation des identités**

- Examiner les modèles d'identité pour Microsoft 365
- Examiner les options d'authentification pour le modèle d'identité hybride
- Explorer la synchronisation d'annuaires
- Quizz

**Module 11 : Préparer la synchronisation des identités avec Microsoft 365**

- Planifiez votre déploiement Azure Active Directory
- Préparer la synchronisation d'annuaires
- Choisissez votre outil de synchronisation d'annuaires
- Planifier la synchronisation d'annuaires à l'aide d'Azure AD Connect
- Planifier la synchronisation d'annuaires à l'aide d'Azure AD Connect Cloud Sync
- Quizz

**Module 12 : Implémenter des outils de synchronisation d'annuaires**

- Configurer les prérequis Azure AD Connect
- Configurer Azure AD Connect

- Surveiller les services de synchronisation à l'aide d'Azure AD Connect Health
- Configurer les prérequis Azure AD Connect Cloud Sync
- Configurer Azure AD Connect Cloud Sync
- Quiz

**Module 13 : Gérer les identités synchronisées**

- Gérer les utilisateurs avec la synchronisation d'annuaire
- Gérer les groupes avec la synchronisation d'annuaire
- Utiliser les groupes de sécurité Azure AD Connect Sync pour maintenir la synchronisation des annuaires
- Configurer des filtres d'objets pour la synchronisation d'annuaires
- Résoudre les problèmes de synchronisation d'annuaire
- Quiz

**Module 14 : Gérer l'accès utilisateur sécurisé dans Microsoft 365**

- Gérer les mots de passe des utilisateurs
- Activer l'authentification unique
- Activer l'authentification multifacteur
- Activer la connexion sans mot de passe avec Microsoft Authenticator
- Découvrez la gestion des mots de passe en libre-service
- Découvrir Windows Hello Entreprise
- Implémenter Azure AD Smart Lockout
- Mettre en œuvre des politiques d'accès conditionnel
- Explorer les paramètres de sécurité par défaut dans Azure AD
- Enquêter sur les problèmes d'authentification à l'aide des journaux de connexion
- Quiz

**Module 15 : Examiner les vecteurs de menace et les violations de données**

- Explorez le paysage actuel du travail et des menaces
- Examiner comment le phishing récupère des informations sensibles
- Examinez comment l'usurpation d'identité trompe les utilisateurs et compromet la sécurité des données
- Comparez les spams et les logiciels malveillants
- Examiner comment une violation de compte compromet un compte utilisateur
- Examiner les attaques d'élévation de privilèges
- Examiner comment l'exfiltration de données déplace les données hors de votre locataire
- Examiner comment les attaquants suppriment les données de votre locataire
- Examiner comment le déversement de données expose les données en dehors de votre locataire
- Examiner d'autres types d'attaques
- Quiz

**Module 16 : Découvrez le modèle de sécurité Zero Trust**

- Examiner les principes et les composants du modèle Zero Trust
- Planifiez un modèle de sécurité Zero Trust dans votre organisation
- Examiner la stratégie de Microsoft pour la mise en réseau Zero Trust
- Adoptez une approche Zero Trust
- Quiz

**Module 17 : Explorer les solutions de sécurité dans Microsoft 365 Defender**

- Améliorez la sécurité de votre messagerie à l'aide d'Exchange Online Protection et de Microsoft Defender pour Office 365
- Protégez les identités de votre organisation à l'aide de Microsoft Defender pour Identity

- Protégez votre réseau d'entreprise contre les menaces avancées à l'aide de Microsoft Defender pour Endpoint
- Protégez-vous contre les cyberattaques à l'aide de Microsoft 365 Threat Intelligence
- Fournir des informations sur les activités suspectes à l'aide de Microsoft Cloud App Security
- Examiner les rapports de sécurité dans Microsoft 365 Defender
- Quiz

**Module 18 : Examiner le score de sécurité Microsoft**

- Explorer Microsoft Secure Score
- Évaluez votre posture de sécurité avec Microsoft Secure Score
- Améliorez votre score sécurisé
- Suivez votre historique Microsoft Secure Score et atteignez vos objectifs
- Quiz

**Module 19 : Examiner la gestion des identités privilégiées**

- Explorer la gestion des identités privilégiées dans Azure AD
- Configurer la gestion des identités privilégiées
- Auditer la gestion des identités privilégiées
- Explorer Microsoft Identity Manager
- Contrôlez les tâches d'administration privilégiées à l'aide de Privileged Access Management
- Quiz

**Module 20 : Examiner Azure Identity Protection**

- Explorer Azure Identity Protection
- Activer les stratégies de protection par défaut dans Azure Identity Protection
- Explorez les vulnérabilités et les événements à risque détectés par Azure Identity Protection
- Planifiez votre enquête d'identité
- Quiz

**Module 21 : Examiner la protection en ligne d'Exchange**

- Examiner le pipeline anti-malware
- Détectez les messages contenant du spam ou des logiciels malveillants à l'aide de la purge automatique en une heure zéro
- Découvrez la protection anti-usurpation d'identité fournie par Exchange Online Protection
- Découvrez d'autres protections anti-usurpation d'identité
- Examiner le filtrage des spams sortants
- Quiz

**Module 22 : Examiner Microsoft Defender pour Office 365**

- Gravissez les échelons de la sécurité d'EOP à Microsoft Defender pour Office 365
- Étendre les protections EOP en utilisant des pièces jointes et des liens fiables
- Gérer les renseignements usurpés
- Configurer les politiques de filtrage des spams sortants
- Empêcher les utilisateurs d'envoyer des e-mails
- Quiz

**Module 23 : Gérer les pièces jointes sécurisées**

- Protégez les utilisateurs contre les pièces jointes malveillantes à l'aide de pièces jointes approuvées
- Créer des stratégies de pièces jointes approuvées à l'aide de Microsoft Defender pour Office 365

- Créer des stratégies de pièces jointes approuvées à l'aide de PowerShell
- Modifier une stratégie de pièces jointes approuvées existante
- Créer une règle de transport pour contourner une stratégie de pièces jointes approuvées
- Examinez l'expérience de l'utilisateur final avec les pièces jointes approuvées
- Quizz

#### Module 24 : Gérer les liens sécurisés

- Protégez les utilisateurs contre les URL malveillantes en utilisant des liens sécurisés
- Créer des stratégies de liens fiables à l'aide de Microsoft 365 Defender
- Créer des politiques de liens fiables à l'aide de PowerShell
- Modifier une politique de liens fiables existante
- Créer une règle de transport pour contourner une politique de liens fiables
- Examinez l'expérience de l'utilisateur final avec les liens sécurisés
- Quizz

#### Module 25 : Explorer les renseignements sur les menaces dans Microsoft 365 Defender

- Explorer le graphique de sécurité intelligente de Microsoft
- Explorer les stratégies d'alerte dans Microsoft 365
- Exécutez des enquêtes et des réponses automatisées
- Explorez la chasse aux menaces avec Microsoft Threat Protection
- Explorez la chasse avancée aux menaces dans Microsoft 365 Defender
- Explorer l'analyse des menaces dans Microsoft 365
- Identifiez les problèmes de menace à l'aide des rapports Microsoft Defender
- Quizz

#### Module 26 : Implémenter la protection des applications à l'aide de Microsoft Defender pour les applications cloud

- Explorer les applications cloud Microsoft Defender
- Déployer Microsoft Defender pour les applications cloud
- Configurer les stratégies de fichiers dans Microsoft Defender pour Cloud Apps
- Gérer et répondre aux alertes dans Microsoft Defender pour Cloud Apps
- Configurer Cloud Discovery dans Microsoft Defender pour les applications cloud
- Résoudre les problèmes de découverte du cloud dans Microsoft Defender pour les applications cloud
- Quizz

#### Module 27 : Implémenter la protection des points de terminaison à l'aide de Microsoft Defender pour point de terminaison

- Explorer Microsoft Defender pour Endpoint
- Configurer Microsoft Defender pour Endpoint dans Microsoft Intune
- Appareils intégrés dans Microsoft Defender pour Endpoint
- Gérer les vulnérabilités des terminaux avec Microsoft Defender Vulnerability Management
- Gérer la découverte d'appareils et l'évaluation des vulnérabilités
- Réduisez votre exposition aux menaces et aux vulnérabilités
- Quizz

#### Module 28 : Implémenter la protection contre les menaces à l'aide de Microsoft Defender pour Office 365

- Explorer la pile de protection Microsoft Defender pour Office 365
- Enquêter sur les attaques de sécurité à l'aide de Threat Explorer
- Identifiez les problèmes de cybersécurité à l'aide de Threat Trackers
- Préparez-vous aux attaques avec la formation de simulation d'attaque
- Quizz

#### Module 29 : Examiner les solutions de gouvernance des données dans Microsoft Purview

- Explorer la gouvernance et la conformité des données dans Microsoft Purview
- Protégez les données sensibles avec Microsoft Purview Information Protection
- Gouverner les données organisationnelles à l'aide de Microsoft Purview Data Lifecycle Management
- Minimisez les risques internes avec Microsoft Purview Insider Risk Management
- Explorer les solutions Microsoft Purview eDiscovery
- Quizz

#### Module 30 : Explorer l'archivage et la gestion des enregistrements dans Microsoft 365

- Explorer les boîtes aux lettres d'archivage dans Microsoft 365
- Activer les boîtes aux lettres d'archivage dans Microsoft 365
- Explorer la gestion des enregistrements Microsoft Purview
- Mettre en œuvre la gestion des enregistrements Microsoft Purview
- Restaurer les données supprimées dans Exchange Online
- Restaurer les données supprimées dans SharePoint Online
- Quizz

#### Module 31 : Explorer la rétention dans Microsoft 365

- Explorer la rétention à l'aide de stratégies de rétention et d'étiquettes de rétention
- Comparer les fonctionnalités des politiques de rétention et des étiquettes de rétention
- Définir la portée d'une politique de rétention
- Examiner les principes de rétention
- Mettre en œuvre la rétention à l'aide de stratégies de rétention, d'étiquettes de rétention et de conservations eDiscovery
- Restreindre les modifications de rétention à l'aide du verrouillage de conservation
- Quizz

#### Module 32 : Découvrez le chiffrement des messages Microsoft Purview

- Examiner le chiffrement des messages Microsoft Purview
- Configurer le chiffrement des messages Microsoft Purview
- Définir des règles de flux de messagerie pour chiffrer les e-mails
- Ajouter une image de marque organisationnelle aux e-mails chiffrés
- Découvrez le chiffrement avancé des messages Microsoft Purview
- Quizz

#### Module 33 : Explorer la conformité dans Microsoft 365

- Planifier la sécurité et la conformité dans Microsoft 365
- Planifiez vos premières tâches de conformité dans Microsoft Purview
- Gérez vos exigences de conformité avec Compliance Manager
- Examiner le tableau de bord du gestionnaire de conformité
- Analyser le score de conformité Microsoft
- Quizz

**Module 34 : Mettre en œuvre la gestion des risques Microsoft Purview**

**Insider**

- Explorer la gestion des risques internes
- Planifier la gestion des risques internes
- Explorer les politiques de gestion des risques internes
- Créer des politiques de gestion des risques internes
- Enquêter sur les activités de gestion des risques internes et les alertes
- Explorer les cas de gestion des risques internes
- Quizz

**Module 35 : Mettre en œuvre les barrières d'information Microsoft Purview**

- Explorer les barrières d'information de Microsoft Purview
- Configurer les barrières d'informations dans Microsoft Purview
- Examiner les barrières à l'information dans Microsoft Teams
- Examiner les barrières à l'information dans OneDrive
- Examiner les barrières à l'information dans SharePoint
- Quizz

**Module 36 : Découvrez Microsoft Purview Data Loss Prevention**

- Examiner la prévention des pertes de données
- Découvrez la prévention des pertes de données Endpoint
- Examiner les stratégies DLP
- Afficher les résultats de la stratégie DLP
- Explorer les rapports DLP
- Quizz

**Module 37 : Mettre en œuvre la prévention des pertes de données**

**Microsoft Purview**

- Planifier la mise en œuvre de la protection contre la perte de données Microsoft Purview
- Implémenter les politiques DLP par défaut de Microsoft Purview
- Concevoir une politique DLP personnalisée
- Créer une stratégie DLP personnalisée à partir d'un modèle
- Configurer les notifications par e-mail pour les stratégies DLP
- Configurer les conseils de stratégie pour les stratégies DLP
- Quizz

**Module 38 : Mettre en œuvre la classification des données des informations sensibles**

- Explorer la classification des données
- Mettre en œuvre la classification des données dans Microsoft 365
- Explorez les classificateurs entraînaables
- Créer et recycler un classifieur entraînaable
- Afficher les données sensibles à l'aide de l'explorateur de contenu et de l'explorateur d'activités
- Détectez les documents d'information sensibles à l'aide de l'empreinte digitale des documents
- Quizz

**Module 39 : Explorer les étiquettes de confidentialité**

- Gérer la protection des données à l'aide d'étiquettes de confidentialité
- Découvrez ce que les étiquettes de confidentialité peuvent faire
- Déterminer la portée d'une étiquette de confidentialité
- Appliquer automatiquement les étiquettes de confidentialité
- Explorer les politiques d'étiquette de confidentialité
- Quizz

**Module 40 : Mettre en œuvre des étiquettes de confidentialité**

- Planifiez votre stratégie de déploiement pour les étiquettes de sensibilité
- Examiner les exigences pour créer une étiquette de confidentialité
- Créer des étiquettes de confidentialité
- Publier des étiquettes de sensibilité
- Supprimer et supprimer les étiquettes de sensibilité
- Quizz