

Microsoft 365 Administrator

Durée: 5 Jours Réf de cours: M-MS102

Résumé:

Cette formation permet aux participants d'acquérir les compétences et connaissances nécessaires pour utiliser les éléments clés de l'administration de Microsoft 365 : Gestion des locataires Microsoft 365, Synchronisation des identités Microsoft 365 et Sécurité et conformité Microsoft 365.

Mise à jour : 12.04.2023

Public visé:

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

Fonction : Administrateur

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Configurer les locataires Microsoft 365, y compris le profil organisationnel, les options d'abonnement, les services de composants, les comptes d'utilisateurs et les licences, les groupes de sécurité et les rôles administratifs
- Configurer Microsoft 365, en mettant l'accent sur la configuration de la connectivité client Office et exploreront comment gérer les installations client de Microsoft 365 Apps pour les déploiements d'entreprise.
- Examiner la synchronisation des identités Microsoft 365, en mettant l'accent sur Azure Active Directory Connect et Connect Cloud Sync.
- Planifier et à mettre en œuvre chacune de ces options de synchronisation d'annuaire, à gérer les identités synchronisées et à mettre en œuvre la gestion des mots de passe dans Microsoft 365 à l'aide de l'authentification multifactorielle et de la gestion des mots de passe en libre-service.
- Examiner les types courants de vecteurs de menace et de violations de données auxquels les organisations sont confrontées aujourd'hui.
- Découvrir Microsoft Secure Score, ainsi que Azure Active Directory Identity Protection
- Gérer les services de sécurité de Microsoft 365, notamment Exchange Online Protection, Safe Attachments et Safe Links
- Découvrir les différents rapports qui permettent de contrôler la santé de la sécurité d'une organisation, utiliser Microsoft 365 Defender, Microsoft Defender for Cloud Apps et Microsoft Defender for Endpoint.
- Examiner les composants clés de la gestion de la conformité de Microsoft 365 : aspects clés de la gouvernance des données, notamment l'archivage et la conservation des données, le chiffrement des messages Microsoft Purview et la prévention de la perte de données (DLP).
- Approfondir l'archivage et la conservation, en accordant une attention particulière à la gestion du risque d'initié Microsoft Purview, aux barrières d'information et aux politiques de DLP

Pré-requis:

Avoir une bonne compréhension du DNS et une expérience fonctionnelle de base avec les services Microsoft 365, des pratiques informatiques générales et une connaissance pratique de PowerShell.

- M-MD102 - Administration des équipements Microsoft Windows

Test et certification

Cette formation prépare à l'examen MS102 Administrateur Microsoft 365

Contenu:

Configurer votre expérience Microsoft 365

- Gérer les abonnements de vos locataires dans Microsoft 365
- Intégrer Microsoft 365 avec les applications d'engagement client
- Terminer la configuration de vos locataires dans Microsoft 365

Gérer les utilisateurs, les contacts et les licences dans Microsoft 365

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

Gérer les groupes dans Microsoft 365

- Examiner les groupes dans Microsoft 365
- Créer et gérer des groupes dans Microsoft 365
- Créer des groupes dans Exchange Online et SharePoint Online

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

Configurer la connectivité du client à Microsoft 365

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

Configurer les rôles administratifs dans Microsoft 365

- Explorer le modèle de permission de Microsoft 365
- Explorer les rôles d'administrateur de

Se préparer à la synchronisation des identités avec Microsoft 365

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

Mettre en oeuvre des outils de synchronisation d'annuaires

- Configuration des conditions préalables d'Azure AD Connect
- Configurer Azure AD Connect
- Surveiller les services de synchronisation à l'aide de Azure AD Connect Health
- Configuration des prérequis d'Azure AD Connect Cloud Sync
- Configurer Azure AD Connect Cloud Sync

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 aider à maintenir la synchronisation de l'annuaire
- Configurer les filtres d'objets pour la synchronisation d'annuaire
- Dépannage de la synchronisation d'annuaire

Gérer l'accès sécurisé des utilisateurs dans Microsoft 365

- Gérer les mots de passe des utilisateurs
- Activer l'authentification pass-through
- Activer l'authentification multifactorielle
- Explorer la gestion des mots de passe en libre-service
- Mettre en œuvre Azure AD Smart Lockout
- Mettre en œuvre les paquets de droits dans Azure AD Identity Governance
- Mettre en œuvre des politiques d'accès conditionnel
- Créer et exécuter une revue d'accès
- Examiner les problèmes d'authentification à l'aide des journaux de connexion

Examiner les vecteurs de menace et les violations de données

- Explorer le travail et le paysage des menaces d'aujourd'hui

Examiner la protection d'Exchange Online

- Examiner le pipeline anti-malware
- Détecter les messages contenant du spam ou des logiciels malveillants à l'aide de la purge automatique zéro heure
- Explorer la protection anti-spoofing fournie par Exchange Online Protection
- Explorer d'autres protections anti-spoofing
- Examiner le filtrage des spams sortants

Examiner Microsoft Defender pour Office 365

- Grimper l'échelle de sécurité de l'EOP à Microsoft Defender pour Office 365
- Étendre les protections EOP en utilisant les pièces jointes sécurisées et les liens sécurisés
- Gérer les renseignements usurpés

Configurer les politiques de filtrage du spam sortant

- Débloquer l'envoi d'e-mails par les utilisateurs

Gérer les pièces jointes sécurisées

- Protéger les utilisateurs contre les pièces jointes malveillantes à l'aide des pièces jointes sécurisées
- Créer des politiques de pièces jointes sécurisées à l'aide de Microsoft Defender pour Office 365
- Créer des politiques de pièces jointes sécurisées à l'aide de PowerShell
- Modifier une politique de pièces jointes sécurisées existante
- Créer une règle de transport pour contourner une politique de pièces jointes sécurisées
- Examiner l'expérience de l'utilisateur final avec les pièces jointes sécurisées

Gérer les liens sécurisés

- Protéger les utilisateurs des URL malveillantes à l'aide des liens sécurisés
- Créer des politiques de liens sécurisés à l'aide de Microsoft 365 Defender
- Créer des politiques de liens sécurisés à l'aide de PowerShell
- Modifier une politique de liens sécurisés existante
- Créer une règle de transport pour contourner une politique Safe Links
- Examiner l'expérience de l'utilisateur final avec Safe Links

Explorer la veille sur les menaces dans Microsoft 365 Defender

- Explorer le graphique de sécurité

Microsoft 365 ■ Attribuer des rôles d'administrateur aux utilisateurs dans Microsoft 365 ■ Déléguer des rôles d'administrateur à des 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 (gestion des identités privilégiées) Gérer la santé et les services des locataires dans Microsoft 365 ■ Surveiller la santé de vos services Microsoft 365 ■ Surveiller l'état de santé des locataires à l'aide du score d'adoption de Microsoft 365 ■ Surveiller la santé des locataires à l'aide des analyses d'utilisation de Microsoft 365 ■ Élaborer un plan de réponse aux incidents Déployer Microsoft 365 Apps pour l'entreprise ■ Explorer les fonctionnalités de Microsoft 365 Apps for entreprise ■ Étudier la compatibilité de votre application en utilisant la boîte à outils de préparation (Readiness Toolkit) ■ Effectuer une installation en libre-service de Microsoft 365 Apps for entreprise ■ Déployer Microsoft 365 Apps for entreprise avec Microsoft Endpoint Configuration Manager ■ Déployer Microsoft 365 Apps pour l'entreprise à partir du cloud ■ Déployer Microsoft 365 Apps for entreprise à partir d'une source locale ■ Gérer les mises à jour de Microsoft 365 Apps for entreprise ■ Explorer les canaux de mise à jour pour Microsoft 365 Apps for entreprise ■ Gérer vos applications en nuage à l'aide du centre d'administration de Microsoft 365 Apps Analyser les données de votre environnement de travail Microsoft 365 à l'aide de Microsoft Viva Insights ■ Examiner les fonctions analytiques de Microsoft Viva Insights ■ Créer des analyses personnalisées 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 Explorer la synchronisation des identités ■ Examiner les options d'authentification et de provisionnement dans Microsoft 365 ■ Explorer la synchronisation des répertoires	■ Examiner comment le phishing récupère des informations sensibles ■ Examiner comment l'usurpation d'identité trompe les utilisateurs et compromet la sécurité des données ■ Comparer le spam et les logiciels malveillants ■ Examiner comment une violation de compte compromet un compte d'utilisateur ■ Examiner les attaques par élévation de privilèges ■ Examiner comment l'exfiltration de données déplace des données hors de votre locataire ■ Examiner comment les attaquants suppriment les données de votre locataire ■ Examiner comment le déversement de données expose des données en dehors de votre locataire ■ Examiner d'autres types d'attaques Explorer le modèle de sécurité "Zero Trust" ■ Examiner les principes et les composants du modèle de confiance zéro ■ Planifier la mise en place d'un modèle de sécurité de confiance zéro dans votre organisation ■ Examiner la stratégie de Microsoft pour le réseau Zero Trust ■ Adopter une approche Zero Trust Explorer les solutions de sécurité dans Microsoft 365 Defender ■ Renforcez la sécurité de votre messagerie à l'aide d'Exchange Online Protection et de Microsoft Defender for Office 365 ■ Protégez les identités de votre organisation avec Microsoft Defender for Identity ■ Protégez votre réseau d'entreprise contre les menaces avancées à l'aide de Microsoft Defender for Endpoint ■ Protéger contre les cyberattaques avec Microsoft 365 Threat Intelligence ■ Fournir un aperçu des activités suspectes à l'aide de Microsoft Cloud App Security ■ Examiner les rapports de sécurité dans Microsoft 365 Defender Examiner Microsoft Secure Score ■ Explorer Microsoft Secure Score ■ Évaluez votre posture de sécurité avec Microsoft Secure Score ■ Améliorer votre score de sécurité ■ Suivez l'historique de votre Microsoft Secure Score et atteignez vos objectifs Examiner la gestion des identités privilégiées	intelligent de Microsoft ■ Explorer les politiques d'alerte dans Microsoft 365 ■ Exécuter des enquêtes et des réponses automatisées ■ Découvrir la chasse aux menaces avec Microsoft Threat Protection ■ Découvrir la chasse aux menaces avancée dans Microsoft 365 Defender ■ Explorer l'analyse des menaces dans Microsoft 365 ■ Identifier les problèmes liés aux menaces à l'aide des rapports de Microsoft Defender Mettre en œuvre la protection des applications en utilisant Microsoft Defender for Cloud Apps ■ Explorer Microsoft Defender Cloud Apps ■ Déployer Microsoft Defender for Cloud Apps ■ Configurer les politiques de fichiers dans Microsoft Defender for Cloud Apps ■ Gérer et répondre aux alertes dans Microsoft Defender for Cloud Apps ■ Configurer Cloud Discovery dans Microsoft Defender for Cloud Apps ■ Dépanner Cloud Discovery dans Microsoft Defender for Cloud Apps Mettre en œuvre la protection des points d'extrémité en utilisant Microsoft Defender for Endpoint ■ Découvrir Microsoft Defender for Endpoint ■ Configurer Microsoft Defender for Endpoint dans Microsoft Intune ■ Embarquer des dispositifs dans Microsoft Defender for Endpoint ■ Gérer les vulnérabilités des terminaux avec Microsoft Defender Vulnerability Management ■ Gérer la découverte des appareils et l'évaluation des vulnérabilités Réduire l'exposition aux menaces et aux vulnérabilités Mettre en œuvre la protection contre les menaces en utilisant Microsoft Defender pour Office 365 ■ Explorer la pile de protection de Microsoft Defender for Office 365 ■ Étudier les attaques de sécurité à l'aide de Threat Explorer ■ Identifier les problèmes de cybersécurité à l'aide de Threat Trackers ■ Se préparer aux attaques grâce à la formation à la simulation d'attaques
---	---	---

■ Explorer Azure AD Connect

- 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
- Contrôler les tâches des administrateurs privilégiés à l'aide de la gestion des accès privilégiés

Examiner Azure Identity Protection

- Explorer Azure Identity Protection
- Activer les politiques de protection par défaut dans Azure Identity Protection
- Explorer les vulnérabilités et les événements à risque détectés par Azure Identity Protection
- Planifier votre enquête sur l'identité

Méthodes pédagogiques :

Pour profiter pleinement du support électronique dès le 1er jour, nous invitons les participants à se munir d'un PC ou d'une tablette, qu'ils pourront connecter en WiFi dans nos locaux de Rueil, Lyon ou Lille.

Le plus :

L'environnement des labs d'apprentissage reste accessible après la formation durant 365 jours. Ceux-ci peuvent être pratiqués de façon illimitée sur la période.

Important

Microsoft a sécurisé ses offres de formation en ajoutant l'authentification multi-facteurs (MFA) pour accéder aux tenants de Microsoft 365 et Dynamics 365.

Pour accéder à certains TP, les stagiaires devront activer la MFA. Ils auront besoin d'un téléphone portable pour configurer et vérifier la MFA. Ils auront également besoin d'une application capable de générer des codes d'authentification. L'application suggérée est Microsoft Mobile Phone Authenticator, qui est gratuite.

Voici le lien de téléchargement de l'application ainsi que la procédure d'installation :

[Download the Microsoft Mobile Phone Authenticator App](#)

[Set up your Microsoft 365 sign-in for multi-factor authentication](#)

Autres moyens pédagogiques et de suivi:

- Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
- Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
- En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

- Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
- Votre place sera confirmée à la réception d'un devis ou "booking form" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
- Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

- En cas de handicap : plus d'info sur globalknowledge.fr/handicap
- Le Règlement intérieur est disponible sur globalknowledge.fr/reglement