



Together for
a BRIGHTER
FUTURE

Formation sur MICROSOFT 365 ADMINISTRATION



Durée
5 jours



<https://urlz.fr/pxkc>



Pourquoi suivre la formation MICROSOFT 365 **ADMINISTRATION**

Suivre une formation en administration Microsoft 365 peut être extrêmement bénéfique pour plusieurs raisons :

- **Maîtrise des outils essentiels** : En suivant cette formation, vous allez acquérir une connaissance approfondie des outils et des fonctionnalités de Microsoft 365, y compris la gestion des utilisateurs, des groupes, des licences, des services cloud tels que Exchange Online, SharePoint Online, et bien d'autres.
- **Adaptation aux besoins du marché** : Avec de nombreuses entreprises qui adoptent Microsoft 365 comme plateforme principale pour leurs besoins en informatique en nuage, la demande de professionnels possédant une expertise dans l'administration de cette plateforme est très élevée.
- **Gestion efficace de la productivité** : En maîtrisant les compétences d'administration Microsoft 365, vous serez en mesure d'optimiser les fonctionnalités de collaboration et de productivité offertes par la suite bureautique. Cela peut inclure la configuration de la messagerie, la gestion des documents, la collaboration en ligne, etc.
- **Sécurité et conformité** : La formation en administration Microsoft 365 comprend souvent des modules sur la sécurité et la conformité, ce qui est essentiel dans un environnement où la protection des données et la conformité aux réglementations sont des priorités majeures pour les entreprises.
- **Opportunités de carrière** : En obtenant une certification en administration Microsoft 365, vous augmentez vos chances de trouver un emploi dans des entreprises de toutes tailles qui utilisent ou prévoient d'adopter la suite Microsoft 365. De plus, vous pouvez également vous positionner pour des rôles de consultant ou d'expert en la matière.
- **Évolution constante des compétences** : Microsoft 365 est une plateforme en constante évolution, avec de nouvelles fonctionnalités et mises à jour régulières. En suivant une formation régulière dans ce domaine, vous pouvez rester à jour avec les dernières technologies et les meilleures pratiques en matière d'administration.

En résumé, suivre une formation en administration Microsoft 365 peut vous fournir les compétences et les connaissances nécessaires pour réussir dans un environnement de travail moderne axé sur le cloud, tout en vous offrant des opportunités de carrière intéressantes dans un domaine en pleine croissance.

Plan du cours

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

Plan du cours

Configurer les rôles administratifs dans Microsoft 365

- Explorer le modèle de permission de Microsoft 365
- Explorer les rôles d'administrateur de 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 enterprise
- 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 enterprise
- Déployer Microsoft 365 Apps for enterprise avec Microsoft Endpoint Configuration Manager
- Déployer Microsoft 365 Apps pour l'entreprise à partir du cloud
- Déployer Microsoft 365 Apps for enterprise à partir d'une source locale
- Gérer les mises à jour de Microsoft 365 Apps for enterprise
- Explorer les canaux de mise à jour pour Microsoft 365 Apps for enterprise
- 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

Plan du cours

Explorer la synchronisation des identités

- Examiner les options d'authentification et de provisionnement dans Microsoft 365
- Explorer la synchronisation des répertoires
- Explorer Azure AD Connect

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

Plan du cours

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 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

Plan du cours

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

- 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

Plan du cours

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

Plan du cours

Explorer la veille sur les menaces dans Microsoft 365 Defender

- Explorer le graphique de sécurité 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