Microsoft 365 Administrator Essentials

Description

En suivant cette formation officielle Microsoft, les participants acquerront une compréhension approfondie de comment gérer les clients Microsoft 365, de synchroniser les identités et de maintenir un niveau élevé de sécurité et de conformité au sein de l'environnement Microsoft 365.

Prix de l'inscription en Présentiel (CHF)
3900
Prix de l'inscription en Virtuel (CHF)
3650
Contenu du cours
Module 1 : Configurer votre expérience Microsoft 365

- Configurer votre expérience Microsoft 365
- Gérer vos abonnements de locataire dans Microsoft 365
- Intégrer Microsoft 365 aux applications d'engagement client
- Terminer la configuration de votre client dans Microsoft 365

Module 2 : Gérer les utilisateurs, les contacts et les licences 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

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 dans Exchange Online et SharePoint Online

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

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

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
- Déléguer 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

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

- Surveiller 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

Module 8 : Déployer les applications Microsoft 365 pour les entreprises

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

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

- Examiner les fonctionnalités analytiques de Microsoft Viva Insights
- Créer 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

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

Module 11 : Préparer la synchronisation des identités avec Microsoft 365

- Planifier 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

Module 12 : Mettre en œuvre 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

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 aider à maintenir le répertoire
- Configurer des filtres d'objets pour la synchronisation d'annuaires
- Résoudre les problèmes de synchronisation d'annuaire

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
- Découvrir 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

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

- Explorer le paysage actuel du travail et des menaces
- Examiner comment le phishing récupère des informations sensibles
- Examiner comment l'usurpation d'identité trompe les utilisateurs et compromet la sécurité des données
- Comparer 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

Module 16 : Explorer le modèle de sécurité Zero Trust

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

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

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

- Protéger votre réseau d'entreprise contre les menaces avancées à l'aide de Microsoft Defender pour Endpoint
- Protéger 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

Module 18 : Examiner Microsoft Secure Score

- Explorer Microsoft Secure Score
- Évaluer votre posture de sécurité avec Microsoft Secure Score
- Améliorer votre score sécurisé
- Suivre votre historique Microsoft Secure Score et atteindre vos objectifs

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
- Contrôler les tâches d'administration privilégiées à l'aide de Privileged Access Management

Module 20 : Examiner Azure Identity Protection

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

Module 21 : Examiner la protection en ligne d'Exchange

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

Module 22 : Examiner Microsoft Defender pour Office 365

- Gravir 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 courriels

Module 23 : Gérer les pièces jointes approuvées

- Protéger 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
- Examiner l'expérience de l'utilisateur final avec les pièces jointes approuvées

Module 24 : Gérer les liens sécurisés

- Protéger 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
- Examiner l'expérience de l'utilisateur final avec les liens sécurisés

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
- Exécuter des enquêtes et des réponses automatisées
- Explorer la chasse aux menaces avec Microsoft Threat Protection
- Explorer la chasse avancée aux menaces dans Microsoft 365 Defender
- Explorer l'analyse des menaces dans Microsoft 365
- Identifier les problèmes de menace à l'aide des rapports Microsoft Defender

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

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
- Réduire votre exposition aux menaces et aux vulnérabilités

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
- Identifier les problèmes de cybersécurité à l'aide de Threat Trackers
- Se préparer aux attaques avec la formation de simulation d'attaque

Lab / Exercices

- Laboratoires officiels Microsoft

Documentation

- Accès à Microsoft Learn (contenu d’apprentissage en ligne)

Examen

- Ce cours prépare à la certification **MS-102: Microsoft 365 Administrator**
- Si vous souhaitez passer cet examen, veuillez le sélectionner lors de l’ajout de la formation dans votre panier

Profils des participants

- Ce cours est conçu pour les personnes qui aspirent au rôle d'administrateur Microsoft 365 et qui ont déjà terminé au moins l'un des parcours de certification d'administrateur basé sur les rôles de Microsoft 365

Connaissances Préalables

- Avoir suivi avec succès une formation d'administrateur basée sur des rôles tels que Messagerie, Travail d'équipe, Sécurité, Conformité ou Collaboration
- Une compréhension approfondie des DNS et une expérience fonctionnelle de base avec les services Microsoft 365
- Une compréhension compétente des pratiques générales de l'informatique
- Une connaissance pratique de PowerShell

Objectifs

- Déployer et gérer un Microsoft 365 tenant
- Implémenter et gérer l'identité et l'accès dans Azure AD
- Gérer la sécurité et les menaces en utilisant Microsoft 365 Defender
- Gérer la conformité en utilisant Microsoft Purview

Niveau
Intermédiaire
Durée (Nombre de Jours)
5
Reference
MS-102T00