Formation Administrateur Microsoft 365

Durée :	5.0 jour(s)
Objectifs :	• Gestion des locataires Microsoft 365 • Synchronisation des identités Microsoft 365 • Mettre en œuvre la sécurité et la conformité de Microsoft 365
Prépare à la certification :	• Certification MCP
Public :	Cette formation est conçue pour les personnes qui aspirent au rôle d'administrateur de Microsoft 365.
Prérequis :	Avoir terminé au moins un des chemins de certification d'administrateur basé sur les rôles Microsoft 365.
Modalités et moyens pédagogiques	Démonstrations visuelles et pratiques à travers des exercices d'application et/ou des cas concrets des stagiaires. Salle de formation équipée d'un poste PC par personne et de dispositif vidéo Grand Ecran. Portail web: maformation.vaelia.fr
Modalités d'évaluation	Auto-évaluation des acquis, exercices pratiques et/ou échanges avec le formateur.
Moyens d'encadrement	Un formateur expert spécialisé en Systèmes et Réseaux dont les compétences ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou Vaelia.
Satisfaction globale :	/5 *Calculée à partir des évaluations stagiaires sur les 12 derniers mois.*

Jour 1

Configurez votre expérience Microsoft 365

- Explorer l'environnement Microsoft 365 cloud
- Configurer votre profil organisation Microsoft 365
- Gérer les inscriptions de vos locataires dans Microsoft 365
- Intégrer Microsoft 365 avec les applications d'engagement client
- Terminer la configuration de vos locataires dans Microsoft 365

Gérez les utilisateurs, les licences et les contacts mail dans Microsoft 365

- Identifiez le modèle d'identité utilisateur le mieux adapté à votre organisation.
- Créez des comptes d'utilisateur à partir du centre d'administration Microsoft 365 et de Windows PowerShell.
- Gérez les comptes d'utilisateurs et les licences dans Microsoft 365.
- Récupérez les comptes d'utilisateurs supprimés dans Microsoft 365.
- Effectuez une maintenance groupée des utilisateurs dans Microsoft Entra ID.
- Créez et gérez des contacts de messagerie à partir du nouveau centre d'administration Exchange et d'Exchange Online PowerShell.

Gérez les groupes dans Microsoft 365

- Décrire les différents types de groupes disponibles dans Microsoft 365.
- Créez et gérez des groupes à l'aide du centre d'administration Microsoft 365 et de Windows PowerShell.
- Créez et gérez des groupes dans Exchange Online et SharePoint Online.

Ajoutez un domaine personnalisé dans Microsoft 365

- Identifiez les facteurs à prendre en compte lors de l'ajout d'un domaine personnalisé à Microsoft 365.
- Planifiez les zones DNS utilisées dans un domaine personnalisé.
- Planifiez les exigences en matière d'enregistrement DNS pour un domaine personnalisé.
- Ajoutez un domaine personnalisé à votre déploiement Microsoft 365.

Configurez la connectivité du client à Microsoft 365

- Décrivez comment Outlook utilise la découverte automatique pour connecter un client Outlook à Exchange Online.
- Identifiez les enregistrements DNS nécessaires à Outlook et aux autres clients liés à Office pour localiser automatiquement les services dans Microsoft 365 à l'aide du processus de découverte automatique.
- Décrivez les protocoles de connectivité qui permettent à Outlook de se connecter à Microsoft 365.
- Identifiez les outils qui peuvent vous aider à résoudre les problèmes de connectivité dans les déploiements Microsoft 365.

Configurez les rôles administratifs dans Microsoft 365

- Décrire le modèle d'autorisation RBAC Azure utilisé dans Microsoft 365.
- Décrire les rôles d'administrateur Microsoft 365 les plus courants.
- Identifiez les tâches clés affectées aux rôles d'administrateur Microsoft 365 courants.
- Déléguer des rôles d'administrateur aux partenaires.
- Gérer les autorisations à l'aide d'unités administratives dans l'ID de Microsoft Entra.
- Elever les privilèges pour accéder aux centres d'administration à l'aide de Privileged Identity Management d'ID Microsoft Entra Privileged Identity Management.

Gérez l'intégrité et les services du locataire dans Microsoft 365

- Surveillez l'intégrité du service Microsoft 365 de votre organisation dans le Centre d'administration Microsoft 365.
- Développez un plan de réponse aux incidents pour gérer les incidents qui peuvent se produire avec votre service Microsoft 365.
- Demandez de l'aide à Microsoft pour résoudre les problèmes de support technique, de prévente, de facturation et d'abonnement.

Déployez les Applications Microsoft 365 pour les grandes entreprises

- Décrire la fonctionnalité Applications Microsoft 365 pour entreprise.
- Planifier une stratégie de déploiement pour Microsoft 365 Apps pour entreprise.
- Effectuer une installation pilotée par l'utilisateur de Microsoft 365 Apps pour entreprise.
- Déployez Applications Microsoft 365 pour les grandes entreprises avec Microsoft Endpoint Configuration Manager.
- Identifier les mécanismes de gestion des déploiements centralisés d'applications Microsoft 365 pour entreprise.
- Déployez Microsoft 365 Apps pour entreprise avec le Kit de ressources déploiement d'Office.
- Expliquer comment gérer les mises à jour de Microsoft 365 Apps pour entreprise.
- Déterminer le canal de mise à jour et la méthode d'application qui s'appliquent à votre organisation.

Jour 2

Analysez les données de votre espace de travail Microsoft 365 à l'aide de Microsoft Viva Insights

- Identifier comment Microsoft Viva Insights peut aider à améliorer les comportements de collaboration dans votre organisation.
- Décrire comment l'application Personal Insights analyse votre façon de travailler.
- Décrivez comment l'application Team Insights offre une visibilité sur les habitudes de travail en équipe susceptibles d'entraîner stress et

épuisement professionnel.
- Décrire comment l'application Organization Insights permet aux responsables de voir comment leur culture de travail affecte le bien-être des employés.
- Décrivez comment l'application Insights avancés répond aux questions critiques sur la résilience et la culture de travail.

Explorez la synchronisation des identités

- Décrire les options d'authentification et de provisionnement de Microsoft 365
- Expliquer les deux modèles d'identité dans Microsoft 365 : identité cloud uniquement et identité hybride
- Expliquer les trois méthodes d'authentification dans le modèle d'identité hybride : synchronisation du hachage de mot de passe, authentification directe et authentification fédérée
- Décrire comment Microsoft 365 utilise couramment la synchronisation d'annuaires

Préparez la synchronisation des identités avec Microsoft 365

- Identifiez les tâches nécessaires pour configurer votre environnement Azure Active Directory.
  Planifiez la synchronisation des annuaires pour synchroniser vos objets Active Directory locaux avec Azure AD.
- Identifiez les fonctionnalités de Microsoft Entra Connect Sync et de Microsoft Entra Cloud Sync.
- Choisissez la synchronisation d'annuaire la mieux adaptée à votre environnement et aux besoins de votre entreprise.

Implémentez des outils de synchronisation d'annuaire

- Configurez les prérequis de Microsoft Entra Connect Sync et de Microsoft Entra Cloud Sync.
- Configurez Microsoft Entra Connect Sync et Microsoft Entra Cloud Sync.
- Surveillez les services de synchronisation à l'aide de Microsoft Entra Connect Health.

Gérez les identités synchronisées

- Assurez-vous que les utilisateurs se synchronisent efficacement
- Gérer les groupes avec la synchronisation d'annuaire
- Utilisez les groupes de sécurité Microsoft Entra Connect Sync pour aider à maintenir la synchronisation des annuaires
- Configurer les filtres d'objets pour la synchronisation d'annuaire
- Expliquer comment Microsoft Identity Manager aide les organisations à gérer et synchroniser les identités des utilisateurs dans leurs organisations et environnements hybrides.
- Dépanner la synchronisation des annuaires à l'aide de diverses tâches et outils de dépannage

Gérez l'accès utilisateur sécurisé dans Microsoft 365

- Gérer les mots de passe des utilisateurs
- Décrire l'authentification directe
- Activer l'authentification multifacteur
- Décrire la gestion des mots de passe en libre-service
- Implémenter le verrouillage intelligent Microsoft Entra

Examinez les vecteurs de menaces et les violations de données

- Décrire les techniques utilisées par les pirates pour compromettre les comptes d'utilisateurs par courrier électronique
- Décrire les techniques utilisées par les pirates pour prendre le contrôle des ressources
- Décrire les techniques utilisées par les pirates pour compromettre les données
- Atténuer une violation de compte
- Empêcher une attaque par élévation de privilèges
- Empêcher l'exfiltration, la suppression et la fuite de données.

Explorez le modèle de sécurité Zero Trust

- Décrire l'approche Zero Trust en matière de sécurité dans Microsoft 365
- Décrire les principes et les composants du modèle de sécurité Zero Trust
- Décrivez les cinq étapes pour mettre en œuvre un modèle de sécurité Zero Trust dans votre organisation
- Expliquer l'histoire et la stratégie de Microsoft autour du réseau Zero Trust

Jour 3

Explorez les solutions de sécurité dans Microsoft Defender XDR

- Identifier les fonctionnalités de Microsoft Defender pour Office 365 qui améliorent la sécurité de la messagerie dans un déploiement Microsoft 365
- Expliquer comment Microsoft Defender pour Identity identifie, détecte et enquête sur les menaces avancées, les identités compromises et les actions internes malveillantes dirigées contre votre organisation
- Expliquer comment Microsoft Defender for Endpoint aide les réseaux d'entreprise à prévenir, détecter, enquêter et répondre aux menaces avancées
- Décrivez comment Microsoft 365 Threat Intelligence peut être bénéfique pour les responsables de la sécurité et les administrateurs de votre organisation.
- Décrire comment Microsoft Cloud App Security améliore la visibilité et le contrôle de votre locataire Microsoft 365 à travers trois domaines principaux.

Examinez le score de sécurité Microsoft

- Décrire les avantages de Secure Score et quels types de services peuvent être analysés
- Décrire comment collecter des données à l'aide de l'API Secure Score
- Décrivez comment utiliser l'outil pour identifier les écarts entre votre état actuel et l'endroit où vous aimeriez en être en matière de sécurité.
- Identifiez les actions qui augmentent votre sécurité en atténuant les risques
- Expliquer où chercher pour déterminer les menaces atténuées par chaque action et l'impact qu'elle a sur les utilisateurs

Examinez la gestion des identités privilégiées

- Décrire comment Privileged Identity Management vous permet de gérer, contrôler et surveiller l'accès aux ressources importantes de votre organisation.
- Configurer la gestion des identités privilégiées pour une utilisation dans votre organisation
- Décrire comment l'historique d'audit de Privileged Identity Management vous permet de voir toutes les attributions et activations d'utilisateurs au cours d'une période donnée pour tous les rôles privilégiés.
- Expliquer comment la gestion des accès privilégiés fournit un contrôle d'accès granulaire sur les tâches d'administration privilégiées dans Microsoft 365

Examinez la protection Microsoft Entra ID

- Décrire Azure Identity Protection (AIP) et quels types d'identités peuvent être protégées
- Activer les trois stratégies de protection par défaut dans AIP
- Identifier les vulnérabilités et les événements à risque détectés par AIP
- Planifiez votre enquête sur la protection des identités basées sur le cloud
- Planifiez comment protéger votre environnement Azure Active Directory contre les failles de sécurité

Examinez la protection du courrier électronique dans Microsoft 365

- Décrivez comment Exchange Online Protection analyse le courrier électronique pour fournir une protection contre les logiciels malveillants.
- Répertoriez plusieurs mécanismes utilisés par Exchange Online Protection pour filtrer le spam et les logiciels malveillants.
- Décrivez d'autres solutions que les administrateurs pourraient mettre en œuvre pour fournir une protection supplémentaire contre le phishing et l'usurpation d'identité.
- Comprenez comment EOP offre une protection contre le spam sortant.

Améliorez la protection de votre messagerie à l'aide de Microsoft Defender pour Office 365

- Décrivez comment la fonctionnalité Pièces jointes sécurisées de Microsoft Defender pour Office 365 bloque les logiciels malveillants Zero Day dans les pièces jointes et les documents.
- Décrivez comment la fonctionnalité Liens sécurisés dans Microsoft Defender pour Office 365 protège les utilisateurs contre les URL malveillantes intégrées dans les courriers électroniques et les documents qui pointent vers des sites Web malveillants.
- Créez des politiques de filtrage du spam sortant.
- Débloquez les utilisateurs qui ont enfreint les politiques de filtrage du spam afin qu'ils puissent recommencer à envoyer des e-mails.

Gérez les pièces jointes fiables

- Créer et modifier une stratégie de pièces jointes fiables à l'aide de Microsoft 365 Defender
- Créer une stratégie de pièces jointes fiables à l'aide de PowerShell
- Configurer une stratégie des pièces jointes fiables
- Décrire comment une règle de transport peut désactiver une stratégie pièces jointes fiables
- Décrire l'expérience de l'utilisateur final lorsqu'une pièce jointe est analysée et détectée comme malveillante

Gérez des liens fiables

- Créer et modifier une stratégie de liens fiables à l'aide de Microsoft 365 Defender
- Créer une stratégie de liens fiables à l'aide de PowerShell
- Configurer une stratégie de liens fiables
- Décrire comment une règle de transport peut désactiver une stratégie de liens fiables
- Décrire l'expérience de l'utilisateur final lorsque des liens fiables identifient un lien vers un site web malveillant incorporé dans un e-mail et un lien vers un fichier malveillant hébergé sur un site web

Jour 4

Explorez les renseignements sur les menaces dans Microsoft Defender XDR

- Décrivez comment les renseignements sur les menaces dans Microsoft 365 sont optimisés par Microsoft Intelligent Security Graph.
- Créez des alertes capables d'identifier les événements malveillants ou suspects.
- Comprendre comment fonctionne le processus automatisé d'enquête et de réponse dans Microsoft Defender XDR.
- Décrire comment la chasse aux menaces permet aux opérateurs de sécurité d'identifier les menaces de cybersécurité.
- Décrivez comment la recherche avancée dans Microsoft Defender XDR inspecte de manière proactive les événements sur votre réseau pour localiser les indicateurs et les entités de menace.

Implémentez la protection des applications à l'aide de Microsoft Defender pour les applications cloud

- Décrivez comment Microsoft Defender pour les applications cloud offre une visibilité améliorée sur l'activité cloud du réseau et augmente la protection des données critiques dans les applications cloud.
- Expliquez comment déployer Microsoft Defender pour les applications cloud.
- Contrôlez vos applications cloud avec des politiques de fichiers.
- Gérez et répondez aux alertes générées par ces politiques.
- Configurez et dépannez Cloud Discovery

Implémentez endpoint Protection à l'aide de Microsoft Defender pour point de terminaison

- Découvrez comment Microsoft Defender for Endpoint aide les réseaux d'entreprise à prévenir, détecter, examiner et répondre aux menaces avancées.
- Intégrez des appareils pris en charge à Microsoft Defender pour point de terminaison.
- Implémentez le module sur la Gestion des menaces et des vulnérabilités pour identifier, évaluer et corriger efficacement les faiblesses du point de terminaison.
- Configurez la détection d'appareils afin de découvrir des appareils non managés connectés à votre réseau d'entreprise.
- Réduisez l'exposition aux menaces et aux vulnérabilités de votre organisation en corrigeant des problèmes basés sur des recommandations de sécurité prioritaires.

Implémentez une protection contre les menaces à l'aide de Microsoft Defender pour Office 365

- Décrivez la pile de protection fournie par Microsoft Defender pour Office 365.
- Comprenez comment Threat Explorer peut être utilisé pour enquêter sur les menaces et aider à protéger votre locataire.
- Décrivez les widgets et les vues Threat Tracker qui vous fournissent des informations sur les différents problèmes de cybersécurité susceptibles d'affecter votre entreprise.
- Exécutez des scénarios d'attaque réalistes à l'aide d'Attack Simulator pour vous aider à identifier les utilisateurs vulnérables avant qu'une véritable attaque n'affecte votre organisation.

Examinez les solutions de gouvernance des données dans Microsoft Purview

- Protégez les données sensibles avec Microsoft Purview Information Protection.
- Gouvernez les données organisationnelles à l'aide de Microsoft Purview Data Lifecycle Management.
- Minimisez les risques internes avec Microsoft Purview Insider Risk Management.
- Expliquer les solutions Microsoft Purview eDiscovery.

Explorez l'archivage et la gestion des enregistrements dans Microsoft 365

- Activez et désactivez une boîte aux lettres d'archives dans le portail de conformité Microsoft Purview et via Windows PowerShell.
- Exécutez des tests de diagnostic sur une boîte aux lettres d'archive.
- Découvrez comment les étiquettes de conservation peuvent être utilisées pour autoriser ou bloquer des actions lorsque des documents et des e-mails sont déclarés enregistrements.
- Créez votre plan de fichiers pour les paramètres et les actions de conservation et de suppression.
- Déterminez quand les éléments doivent être marqués comme enregistrements en important un plan existant (si vous en avez déjà un) ou créez de nouvelles étiquettes de rétention.
- Restaurez les données supprimées dans Exchange Online et SharePoint Online.

Explorez la rétention dans Microsoft 365

- Expliquez le fonctionnement des politiques de rétention et des étiquettes de rétention.
- Identifiez les capacités des stratégies de rétention et des étiquettes de rétention.
- Sélectionnez la portée appropriée pour une stratégie en fonction des exigences de l'entreprise.
- Expliquer les principes de rétention.
- Identifiez les différences entre les paramètres de conservation et les conservations eDiscovery.
- Limitez les modifications de conservation en utilisant le verrouillage de préservation.

Explorez le chiffrement des messages Microsoft Purview

- Décrire les fonctionnalités de Microsoft Purview Message Encryption.
- Expliquez comment fonctionne Microsoft Purview Message Encryption et comment le configurer.
- Définissez des règles de flux de messagerie qui appliquent des modèles de personnalisation et de chiffrement pour chiffrer les messages électroniques.
- Ajoutez la marque de votre organisation aux messages électroniques chiffrés.
- Expliquer les fonctionnalités supplémentaires fournies par Microsoft Purview Advanced Message Encryption.

Jour 5

Explorez la conformité dans Microsoft 365

- Décrivez comment Microsoft 365 aide les organisations à gérer les risques, à protéger les données et à rester conformes aux réglementations et aux normes.
- Planifiez vos premières tâches de conformité dans Microsoft Purview.
- Gérez vos exigences de conformité avec Compliance Manager.
- Gérez l'état de conformité et les actions d'amélioration à l'aide du tableau de bord Compliance Manager.
- Expliquez comment le score de conformité d'une organisation est déterminé.

Mettre en œuvre la gestion des risques internes de Microsoft Purview

- Décrire la fonctionnalité de gestion des risques internes dans Microsoft 365.
- Élaborer un plan pour mettre en œuvre la solution Microsoft Purview Insider Risk Management.
- Créez des politiques de gestion des risques internes.
- Gérer les alertes et les cas de gestion des risques internes.

Implémentez les barrières liées aux informations Microsoft Purview

- Décrivez comment les barrières d'information peuvent restreindre ou permettre la communication et la collaboration entre des groupes spécifiques d'utilisateurs.
- Décrire les composants d'une barrière d'information et comment activer les barrières d'information.
- Découvrez comment les barrières d'information aident les organisations à déterminer quels utilisateurs ajouter ou supprimer d'une équipe Microsoft, d'un compte OneDrive et d'un site SharePoint.
- Décrivez comment les barrières d'information empêchent les utilisateurs ou les groupes de communiquer et de collaborer dans Microsoft Teams, OneDrive et SharePoint.

Explorez la prévention contre la perte de données Microsoft Purview

- Décrire comment la prévention contre la perte de données (DLP) est gérée dans Microsoft 365
  Comprendre comment DLP dans Microsoft 365 utilise les types d'informations sensibles et les modèles de recherche
- Décrivez comment Microsoft Endpoint DLP étend les capacités de surveillance et de protection des activités DLP.
- Décrire ce qu'est une stratégie DLP et ce qu'elle contient
- Afficher les résultats de la stratégie DLP à l'aide de requêtes et de rapports

Implémentez la prévention contre la perte de données Microsoft Purview

- Créez un plan de mise en œuvre de la prévention des pertes de données. Implémentez la stratégie DLP par défaut de Microsoft 365.
- Créez une stratégie DLP personnalisée à partir d'un modèle DLP et à partir de zéro.
- Créez des notifications par e-mail et des conseils de stratégie pour les utilisateurs lorsqu'une règle DLP s'applique.
- Créer des conseils de stratégie pour les utilisateurs lorsqu'une règle DLP s'applique
- Configurer les notifications par e-mail pour les stratégies DLP

Mettre en œuvre la classification des données des informations sensibles

- Expliquez les avantages et les inconvénients de la création d'un cadre de classification des données.
- Identifiez comment la classification des données des éléments sensibles est gérée dans Microsoft 365.
- Comprenez comment Microsoft 365 utilise des classificateurs entraînables pour protéger les données sensibles.
- Créez puis recyclez des classificateurs personnalisés pouvant être entraînés.
- Analysez les résultats de vos efforts de classification des données dans l'explorateur de contenu et l'explorateur d'activités.
- Implémentez la prise d'empreintes digitales des documents pour protéger les informations sensibles envoyées via Exchange Online.

Explorez les étiquettes de sensibilité

- Décrivez comment les étiquettes de sensibilité vous permettent de classer et de protéger les données de votre organisation
- Identifiez les raisons courantes pour lesquelles les organisations utilisent des étiquettes de sensibilité
- Expliquer ce qu'est une étiquette de sensibilité et ce qu'elle peut faire pour une organisation
- Configurer la portée d'une étiquette de sensibilité
- Expliquez pourquoi l'ordre des étiquettes de sensibilité dans votre centre d'administration est important
- Décrire ce que les politiques d'étiquetage peuvent faire

Mettre en œuvre des étiquettes de sensibilité

- Décrire le processus global de création, de configuration et de publication d'étiquettes de sensibilité
- Identifiez les autorisations administratives qui doivent être attribuées aux membres de l'équipe de conformité pour mettre en œuvre des étiquettes de sensibilité
- Développez un cadre de classification des données qui constitue la base de vos étiquettes de sensibilité
- Créer et configurer des étiquettes de sensibilité
- Publier des étiquettes de sensibilité en créant une stratégie d'étiquette
- Identifier les différences entre la suppression et la suppression des étiquettes de sensibilité