Formation Administration des points de terminaison avec Microsoft Intune

Durée :	4.0 jour(s)
Objectifs :	• Explorer la gestion des points de terminaison • Exécuter l'inscription d'appareils • Examiner la gestion des applications • Gérer l'authentification et la conformité • Gérer la sécurité des points de terminaison et déployer à l'aide d'outils sur le cloud
Public :	Cette formation Microsoft s'adresse aux Administrateurs Endpoint qui gèrent l'identité, la sécurité, l'accès, les politiques, les mises à jour et les applications pour les points finaux. Ils mettent en œuvre des solutions pour un déploiement et une gestion efficace des points de terminaison sur divers systèmes d'exploitation, plates-formes et types d'appareils. Ils implémentent et gèrent les points de terminaison à grande échelle en utilisant Microsoft Intune, Windows 365.
Prérequis :	Les candidats à cet examen ont de l'expérience avec les technologies Azure AD et Microsoft 365, notamment Intune. Ils doivent posséder de solides compétences et une expérience dans le déploiement, la configuration et la maintenance des appareils clients Windows et non Windows.
Modalités et moyens pédagogiques	Salle de formation équipée d'un poste PC par personne et de dispositif vidéo Grand Ecran / Accès au portail web : maformation.vaelia.fr - support de cours en format numérique (PDF) intégré en fin de session de formation.
Modalités d'évaluation	Démonstrations visuelles et pratique à travers des exercices d'application, cas concrets de stagiaires, tests de validation des acquis sous différents formats (quiz, cahier exercices, …).
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.*

Explorer la gestion des points de terminaison

- **1/ COMPRENDRE MICROSOFT ENTRA ID**
- Décrire Microsoft Entra ID.
- Comparer Microsoft Entra ID à Active Directory Domain Services (AD DS).
- Décrire comment Microsoft Entra ID est utilisé comme annuaire pour les applications cloud.
- Décrire Microsoft Entra ID P1 et P2.
- Décrire Microsoft Entra Domain Services.
- **2/ GÉRER LES IDENTITÉS MICROSOFT ENTRA**
- Décrire les rôles RBAC et utilisateur dans Microsoft Entra ID.
- Créer et gérer des utilisateurs dans Microsoft Entra ID.
- Créer et gérer des groupes dans Microsoft Entra ID.
- Utiliser les cmdlets Windows PowerShell pour gérer Microsoft Entra ID.
- Décrire comment synchroniser les objets AD DS avec Microsoft Entra ID.
- Décrire la jointure à Microsoft Entra.
- Décrire les prérequis, les limitations et les avantages de la jonction Microsoft Entra.
- Joindre un appareil à Microsoft Entra ID.
- Gérer la jointure d'appareils à Microsoft Entra ID.

Exécuter l'inscription d'appareils

- **1/ GÉRER LES PARAMÈTRES DES PÉRIPHÉRIQUES**
- Découvrir l'authentification et la gestion des appareils dans Microsoft Entra ID.
- **2/ INSCIRE DES APPAREILS AVEC MICROSOFT INTUNE**
- Préparer Microsoft Intune pour l'inscription d'appareils.
- Configurer Microsoft Intune pour l'inscription automatique.
- Expliquer comment inscrire des appareils Windows, Android et iOS dans Intune.
- Expliquer quand et comment utiliser le gestionnaire d'inscription Intune.
- Comprendre comment monitorer et effectuer des actions à distance sur des appareils inscrits.

Configurer des profils pour les utilisateurs et les appareils

- **1/ EXÉCUTER DES PROFILS D'APPAREILS**
- Découvrir les différents types de profils d'appareil (création et gestion)
- Décrire les différents types de profils d'appareils dans Intune.
- Expliquer la différence entre les profils intégrés et les profils personnalisés.
- Créer et gérer des profils.
- **2/ SUPERVISER LES PROFILS D'APPAREILS**
- Monitorer les affectations de profils.
- Comprendre comment les profils sont synchronisés et comment forcer manuellement la synchronisation.
- Utiliser PowerShell pour exécuter et monitorer des scripts sur des appareils.

Examiner la gestion des applications

- **1/ EXÉCUTER LA GESTION DES APPLICATIONS MOBILES**
- Expliquer la gestion des applications mobiles.
- Comprendre les considérations relatives aux applications dans GAM.
- Expliquer l'utilisation de Configuration Manager pour GAM.
- Utiliser Intune pour GAM.
- Implémenter et gérer des stratégies GAM.
- **2/ DÉPLOYER ET METTRE À JOUR LES APPLICATIONS**
- Expliquer comment déployer des applications en utilisant Intune
- Découvrir comment déployer des applications avec une stratégie de groupe.
- Comprendre les applications du Microsoft Store.
- Découvrir comment déployer des applications en utilisant des applications du Microsoft Store.
- Découvrir comment configurer des applications du Microsoft Store.
- **3/ ADMINISTRER LES APPLICATIONS DE POINT DE TERMINAISON**
- Expliquer comment gérer des applications dans Intune.
- Comprendre comment gérer des applications sur des appareils non-inscrits.
- Comprendre comment déployer Microsoft 365 Apps avec Intune.
- Découvrir les options d'inventaire d'applications dans Intune.

Gérer l'authentification et la conformité

- **1/ IMPLÉMENTER LA CONFORMITÉ DES PÉRIPHÉRIQUES**
- Décrire la stratégie de conformité des appareils
- Déployer une stratégie de conformité des appareils
- Décrire l'accès conditionnel
- Créer des stratégies d'accès conditionnel
- **2/ GÉNÉRER DES RAPPORTS D'INVENTAIRE ET DE CONFORMITÉ**
- Générer des rapports d'inventaire et des rapports de conformité à l'aide de Microsoft Intune

- Signaler et analyser la conformité des périphériques
- Créer des rapports personnalisés à l'aide de la Data Warehouse Intune
- Utiliser l'API Microsoft Graph pour créer des rapports personnalisés

Gérer la sécurité des points de terminaison

- **1/ GÉRER MICROSOFT DEFENDER POUR POINT DE TERMINAISON**
- Décrire Microsoft Defender for Endpoint.
- Décrire les fonctionnalités clés de Microsoft Defender for Endpoint.
- Décrire Microsoft Defender Application Guard.
- Décrire Microsoft Defender Exploit Guard.
- Décrire Windows Defender System Guard.
- **2/ GÉRER MICROSOFT DEFENDER FOR CLOUD APPS**
- Décrire Microsoft Defender for Cloud Apps
- Planifier l'utilisation de Microsoft Defender for Cloud Apps
- Implémenter et utiliser Microsoft Defender for Cloud Apps

Déploiement à l'aide d'outils sur le cloud

- **1/ DÉPLOYER DES APPAREILS AVEC WINDOWS AUTOPILOT**
- Expliquer les avantages d'un déploiement moderne pour les nouveaux appareils.
- Décrire le processus de préparation d'un déploiement Autopilot.
- Décrire le processus d'inscription des appareils dans Autopilot.
- Décrire les différentes méthodes et différents scénarios des déploiements Autopilot.
- Décrire comment résoudre les problèmes courants d'Autopilot.
- Décrire le processus de déploiement avec des méthodes traditionnelles.
- **2/ IMPLÉMENTER DES MÉTHODES DE DÉPLOIEMENT DYNAMIQUE**
- Décrire comment fonctionne une activation d'abonnement.
- Décrire les avantages du provisionnement de packages.
- Expliquer comment le Concepteur de configuration Windows crée des packages de provisionnement.
- Décrivez les avantages de l'utilisation de l'inscription GPM avec la jonction Microsoft Entra.