

Microsoft 365 : administration des services essentiels (MS-102)

Date et durée
Code formation : MS-102T00 Durée : 5 jours Nombre d'heures : 35 heures
Formation avec certification
Enterprise Administrator Expert
Description
Utiliser les fonctionnalités de Microsoft 365 pour accéder aux applications Office et sa messagerie aussi bien en local que via le cloud, collaborer, profiter de la fonction vidéoconférence, etc. Les fonctionnalités de MS 365 permettent certes de larges possibilités aux utilisateurs, mais les administrateurs Windows Entreprise ne sont pas oubliés puisqu'ils disposent d'outils destinés à simplifier en particulier, la gestion de ces utilisateurs ainsi que celle des services. En participant à cette formation de 5 jours, vous développerez vos compétences théoriques et pratiques en matière de gestion des identités et des services Microsoft 365. Vous apprendrez à mettre en œuvre l'infrastructure Microsoft 365, à configurer Azure AD, à gérer les comptes et les droits des utilisateurs. De plus, vous réaliserez des synchronisations d'annuaires, déploierez des applis Office 365 et serez capable de gérer l'accès et l'authentification sur MS 365. Grâce à cette formation Microsoft 365, vous serez préparé pour le passage de l'examen MS-102 compris dans notre offre. Cet examen est un prérequis pour obtenir le titre de Microsoft Certified: Identity and Access Administrator Associate (<i>pour en savoir plus, consulter l'onglet Certification</i>).
Objectifs
Au cours de cette formation Microsoft 365 identités et services, vous atteindrez les objectifs de compétences suivants : • déployer et gérer un ou plusieurs locataires Microsoft 365 ; • implémenter et gérer les identités et les accès avec le service Microsoft Entra ID ; • garantir la sécurité et lutter contre les menaces à l'aide de Microsoft 365 Defender ; • gérer la conformité avec Microsoft Purview ; • réussir l'examen MS-102 et obtenir la certification Microsoft Certified: Identity and Access Administrator Associate.
Points forts
Des cours dispensés par un formateur expert et certifié Microsoft ; un programme officiel axé sur des travaux pratiques et le passage de l'examen MS-102 : Microsoft 365 Administrator.
Certification

Cette formation vous permet de passer l'examen MS-102 inclus dans notre offre. Sa réussite vous sera utile pour valider l'un des *prérequis nécessaires à la certification **Microsoft 365 Certified : Administrator Expert**. Pour réussir cet examen, vous devez maîtriser les éléments suivants : évaluation, planification, migration, déploiement et gestion de Microsoft 365. Vous devez être en mesure de planifier, mettre en œuvre et administrer des infrastructures cloud et hybrides au niveau du client.

De plus, **une expérience pratique est nécessaire** dans la gestion des charges de travail de Microsoft 365 et de Microsoft Azure Active Directory (Azure AD) ainsi que dans l'administration d'au moins une de ces charges de travail. Enfin, vous devez avoir une connaissance pratique des réseaux, de l'administration des serveurs, des DNS et de PowerShell.

***À noter :** si vous souhaitez obtenir le titre de Microsoft 365 Certified Administrator Expert, vous devez à la fois réussir l'examen MS-102 et détenir l'une des 5 certifications suivantes :

- [Microsoft 365 Certified: Endpoint Administrator Associate](#)
- [Microsoft 365 Certified: Teams Administrator Associate](#)
- [Microsoft Certified: Identity and Access Administrator Associate](#)
- [Microsoft Certified: Information Protection and Compliance Administrator Associate](#)

Modalités d'évaluation

Travaux Pratiques

Pré-requis

Suivre la **formation Microsoft 365 identités et services** nécessite les prérequis suivants :

- avoir suivi une formation de base d'administrateur Windows ;
- maîtriser le service Domain Name System (DNS) ;
- avoir une expérience pratique de base avec les services Microsoft 365 ;
- connaître les bonnes pratiques en matière de gestion des systèmes informatiques ;
- savoir utiliser les fonctions de PowerShell.

Public

Cette formation s'adresse aux publics suivants :

- toute personne souhaitant devenir administrateur Microsoft 365 et qui dispose déjà de compétences spécifiques liées à un rôle.

Cette formation s'adresse aux profils suivants

[Administrateur système](#)
[Technicien Support / HelpDesk](#)

Programme

Module 1 : déploiement et gestion des locataires Microsoft 365

- Implémenter et gérer un locataire :
 - la création du locataire ;
 - la mise en place et la gestion des domaines ;
 - la configuration des paramètres de l'organisation, incluant la sécurité, la confidentialité et le profil ;
 - l'identification et la réponse aux problèmes de fonctionnement des services ;

- la configuration des notifications d'état des services ;
- le suivi de l'adoption et de l'utilisation.
- Administrer les utilisateurs et les groupes :
 - la création et la gestion des utilisateurs ;
 - la création et la gestion d'utilisateurs invités ;
 - la création et la gestion des contacts ;
 - la création et la gestion de groupes, incluant les groupes Microsoft 365 ;
 - la gestion et la surveillance des attributions de licences Microsoft 365 ;
 - la gestion groupée des utilisateurs, incluant PowerShell.
- Administrer les rôles dans Microsoft 365 :
 - la gestion des rôles dans Microsoft 365 et Microsoft Entra ;
 - la gestion des groupes de rôles pour Microsoft Defender, Microsoft Purview et les charges de travail de Microsoft 365 ;
 - la gestion de la délégation à l'aide d'unités administratives ;
 - la mise en place d'une gestion des identités privilégiées pour les rôles de Microsoft Entra.

Module 2 : Implémentation et gestion des identités et des accès

- Implémenter et gérer la synchronisation des identités avec Microsoft Entra ID :
 - la préparation de la synchronisation des identités via IdFix ;
 - la mise en place et la gestion de la synchronisation d'annuaires via la synchronisation dans le cloud Microsoft Entra Connect ;
 - l'implémentation et la gestion de la synchronisation des répertoires via Microsoft Entra Connect ;
 - le contrôle de la synchronisation via Microsoft Entra Connect Health ;
 - la résolution des problèmes de synchronisation, incluant la synchronisation dans le Cloud de Microsoft Entra Connect.
- Implémenter et gérer l'authentification :
 - la mise en place et la gestion des méthodes d'authentification, incluant Windows Hello Enterprise et l'application Microsoft Authenticator ;
 - la mise en place et la gestion de la réinitialisation du mot de passe en libre-service (SSPR) ;
 - la mise en place et la gestion de la protection par mot de passe via Microsoft Entra ;
 - la mise en place et la gestion de l'authentification multifactorielle (MFA) ;
 - l'analyse et la résolution des problèmes d'authentification.
- Appliquer et gérer la sécurité des accès :
 - le plan de protection de l'identité ;
 - la mise en place et la gestion de la protection de l'identité via Microsoft Entra ;
 - la planification des politiques d'accès conditionnel ;
 - la mise en place et la gestion des politiques d'accès conditionnel.

Module 3 : gestion de la sécurité et des menaces

- Gérer les rapports et les alertes de sécurité avec Microsoft 365 Defender :
 - l'analyse et la prise de mesures visant à améliorer le Microsoft Secure Score ;
 - l'analyse et la réponse aux incidents et aux alertes de sécurité ;
 - l'analyse et la réponse aux problèmes identifiés dans les rapports de sécurité et de conformité ;
 - l'analyse et la réponse aux menaces identifiées dans les rapports de sécurité et de conformité.
- Implémenter et gérer la protection de la messagerie et de la collaboration via Microsoft Defender pour Office 365 :
 - la mise en place de politiques et de règles ;
 - l'analyse et la réponse aux menaces identifiées dans Defender pour Office 365, incluant les attaques et les enquêtes ;
 - la création et l'exécution de campagnes, telle que la simulation d'attaques ;
 - le déblocage des utilisateurs.
- Implémenter et gérer la protection des endpoints via Microsoft Defender pour Endpoint :

- l'intégration de périphériques ;
- la configuration des paramètres de Defender pour Endpoint ;
- l'analyse et la réponse aux vulnérabilités des points de terminaison ;
- l'analyse et la réponse aux risques identifiés dans le tableau de bord de Microsoft Defender Vulnerability Management.

Module 4 : gestion de la conformité via Microsoft Purview

- Implémenter la protection de l'information et la gestion du cycle de vie des données :
 - la gestion des types d'informations sensibles à l'aide de mots-clés, de listes de mots-clés ou d'expressions régulières ;
 - la mise en place d'étiquettes de rétention, de politiques d'étiquettes de rétention et de politiques de rétention ;
 - la mise en place d'étiquettes de confidentialité et de politiques d'étiquettes de confidentialité.
- Implémenter la prévention des pertes de données (DLP) de Microsoft Purview :
 - la mise en place de la DLP pour les charges de travail ;
 - la mise en place de la DLP pour les points de terminaison ;
 - l'analyse et la réponse aux alertes, aux événements et aux rapports DLP.

Microsoft®, Microsoft 365® et Office 365® sont des marques déposées ou des marques commerciales de Microsoft Corporation aux États-Unis et dans d'autres pays.