

Administrateur Microsoft 365 (Microsoft MS-102)

Cours officiel MS-102, préparation à l'examen

Cours Pratique de 5 jours - 35h

Réf : MGJ - Prix 2024 : 3 170€ HT

Avec cette formation, vous acquerez les connaissances et les compétences nécessaires pour déployer et gérer Microsoft 365 dans un environnement d'entreprise. Vous disposerez d'une vue d'ensemble des éléments clés de l'administration de Microsoft 365: le déploiement et la gestion des locataires, la gestion des identités ainsi que la gestion de la sécurité et conformité Microsoft 365.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Déployer et gérer un locataire Microsoft 365

Implémenter et gérer les identités et les accès dans Azure AD

Gérer la sécurité et les menaces à l'aide de Microsoft 365 Defender

Gérer la conformité à l'aide de Microsoft Purview

MÉTHODES PÉDAGOGIQUES

Animation de la formation en français.

Support de cours officiel Microsoft au format numérique et en anglais.

Bonne compréhension de l'anglais à l'écrit.

CERTIFICATION

La réussite de l'examen MS-102 permet d'obtenir la certification Microsoft 365 Certified: Administrator Expert.

Pour devenir Microsoft 365 Certified: Administrator Expert, vous devez obtenir au moins l'un des éléments suivants : Microsoft 365 Certified : administrateurs Bureau moderne Associate, Microsoft 365 Certified: Security Administrator Associate, Microsoft 365 Certified : Messaging Administrator Associate, Microsoft 365 Certified: Teams Administrator Associate, Microsoft Certified: Identity and Access Administrator Associate certification.

LE PROGRAMME

dernière mise à jour : 05/2023

1) Implémenter et gérer un locataire Microsoft 365

- Créer un locataire.
- Implémenter et gérer des domaines.
- Configurer les paramètres de l'organisation, y compris la sécurité, la confidentialité et le profil.
- Identifier et répondre aux problèmes dans Service Health.
- Configurer les notifications dans Service Health.
- Superviser l'adoption et l'usage.

2) Gérer les utilisateurs et les groupes

- Créer et gérer des utilisateurs.
- Créer et gérer des utilisateurs invités.

PARTICIPANTS

Administrateurs Microsoft 365.

PRÉREQUIS

Expérience dans l'administration des charges de travail Microsoft 365 et Azure Active Directory. Connaissance pratique de la mise en réseau, de l'administration de serveurs, du DNS et de PowerShell.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils sont agréés par l'éditeur et sont certifiés sur le cours. Ils ont aussi été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Évaluation des compétences visées en amont de la formation.

Évaluation par le participant, à l'issue de la formation, des

compétences acquises durant la formation.

Validation par le formateur des acquis du participant en précisant les outils utilisés : QCM, mises en situation...

À l'issue de chaque stage, ITTCERT fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Les participants réalisent aussi une évaluation officielle de l'éditeur. Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les ressources pédagogiques utilisées sont les supports et les travaux pratiques officiels de l'éditeur.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Créer et gérer des contacts.
- Créer et gérer des groupes, y compris des groupes Microsoft 365.
- Gérer et superviser les allocations des licences Microsoft 365.
- Réaliser une gestion groupée des utilisateurs, y compris sur PowerShell.

3) Gérer les rôles dans Microsoft 365

- Gérer les rôles dans Microsoft 365 et Azure AD.
- Gérer des groupes de rôles pour les charges de travail Microsoft Defender, Microsoft Purview et Microsoft 365.
- Gérer la délégation à l'aide d'Administrative Units.
- Implémenter Privileged Identity Management pour les rôles Azure AD.

4) Implémenter et gérer la synchronisation des identités avec Azure AD

- Préparer la synchronisation des identités à l'aide d'IdFix.
- Implémenter et gérer la synchronisation des annuaires à l'aide d'Azure AD Connect cloud sync.
- Implémenter et gérer la synchronisation des annuaires à l'aide d'Azure AD Connect.
- Superviser la synchronisation à l'aide d'Azure AD Connect Health.
- Résoudre les problèmes de synchronisation, y compris sur Azure AD Connect et Azure AD Connect cloud sync.

5) Implémenter et gérer l'authentification

- Implémenter et gérer les méthodes d'authentification.
- Implémenter et gérer Self-Service Password Reset (SSPR).
- Implémenter et gérer Azure AD Password Protection.
- Implémenter et gérer l'authentification multi-facteur (MFA).
- Investiguer et résoudre les problèmes d'authentification.

6) Implémenter et gérer l'accès sécurisé

- Planifier la protection des identités.
- Implémenter et gérer Azure AD Identity Protection.
- Planifier des stratégies d'accès conditionnel.
- Implémenter et gérer des stratégies d'accès conditionnel.

7) Gérer les rapports de sécurité et les alertes avec Microsoft 365 Defender

- Evaluer et prendre des mesures pour améliorer le niveau de sécurité Microsoft dans le portail Microsoft 365 Defender.
- Evaluer et répondre aux incidents et alertes de sécurité dans Microsoft 365 Defender.
- Examiner et répondre aux problèmes identifiés dans les rapports de sécurité et de conformité Microsoft 365 Defender.
- Evaluer et répondre aux menaces identifiées dans l'analyse des menaces.

8) Implémenter et gérer la protection de la messagerie et de la collaboration

- Implémenter des stratégies et des règles dans Defender for Office 365.
- Examiner et répondre aux menaces identifiées dans Defender for Office 365, y compris les menaces et les investigations.
- Créer et exécuter des campagnes, telles que la simulation d'attaque.
- Débloquer les utilisateurs.

9) Implémenter et gérer la protection des Endpoint

- Intégrer des appareils dans Defender for Endpoint.
- Configurer les paramètres dans Defender for Endpoint.
- Examiner et répondre aux vulnérabilités des Endpoint.
- Examiner et répondre aux risques identifiés dans le tableau de bord de Microsoft Defender Vulnerability Management.

10) Implémenter la protection des informations et la gestion de cycle de vie

- Implémenter et gérer des informations sensibles.
- Implémenter des étiquettes de rétention, des stratégies d'étiquette de rétention et des stratégies de rétention.
- Implémenter des étiquettes de confidentialité et des stratégies d'étiquette de confidentialité.

11) Implémenter Microsoft Purview Data Loss Prevention (DLP)

- Implémenter DLP pour les charges de travail.
- Implémenter Endpoint DLP.
- Examiner et répondre aux alertes, événements et rapports dans DLP.

LES DATES

CLASSE À DISTANCE

2024 : 24 juin, 26 août, 21 oct., 09
déc.

PARIS

2024 : 17 juin, 19 août, 14 oct., 02
déc.