Développez vos talents
Certifiez vos compétences

Cloud public

Microsoft Azure - Security Technologies

4 jours (28h00) | ★★★★½ 4,6/5 | MSAZ500 | Code Certif Info : 109833 | Certification AZ-500 (non incluse) | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel [1]

Formations Informatique › Cloud › Cloud public

À l'issue de ce stage vous serez capable de :

- Mettre en oeuvre des stratégies de gouvernance d'entreprise, notamment le contrôle d'accès en fonction du rôle, les stratégies Azure et le verrouillage des ressources
- Implémenter une infrastructure Azure AD, notamment des utilisateurs, des groupes et une authentification multifacteurs
- Mettre en oeuvre une protection de l'identité Azure AD, notamment des stratégies de risque, un accès conditionnel et des vérifications d'accès
- Implémenter la gestion de l'identité privilégiée Azure AD, notamment les rôles Azure AD et les ressources Azure
- Mettre en oeuvre Azure AD Connect, notamment les méthodes d'authentification et la synchronisation des répertoires sur site
- Implémenter des stratégies de sécurité du périmètre, notamment le pare-feu Azure
- Mettre en oeuvre des stratégies de sécurité de réseau, notamment les groupes de sécurité réseau et les groupes de sécurité d'application
- Implémenter des stratégies de sécurité de l'hôte, notamment la protection du point de terminaison, la gestion de l'accès à distance, la gestion des mises à jour et le cryptage du disque
- Mettre en oeuvre des stratégies de sécurité de conteneurs, notamment les instances de conteneurs Azure, le registre de conteneurs Azure et Azure Kubernetes
- Implémenter Azure Key Vault, notamment les certificats, les clés et les secrets
- Mettre en oeuvre des stratégies de sécurité d'applications, notamment l'inscription aux applications, les identités gérées et les points de terminaison des services
- Implémenter des stratégies de sécurité de stockage, notamment les signatures d'accès partagé, les stratégies de rétention de Blob, et l'authentification des fichiers Azure
- Mettre en oeuvre des stratégies de sécurité de bases de données, notamment l'authentification, la classification des données, le masquage dynamique des données et Always Encrypted
- Implémenter Azure Monitor, notamment les sources connectées, l'analyse des journaux et les alertes

(1) Modalité et moyens pédagogique :

Formation délivrée en présentiel ou distanciel * (e-learning, classe virtuelle, présentiel à distance). Le formateur alterne entre méthodes ** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification.

Les moyens pédagogiques mis en oeuvre (variables suivant les formations) sont : ordinateurs Mac ou PC (sauf pour les cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel). Environnements de formation installés sur les postes de travail ou en ligne. Supports de cours et exercices.

* Nous consulter pour la faisabilité en distanciel. ** Ratio variable selon le cours suivi.

- Mettre en oeuvre Azure Security Center, notamment les stratégies, les recommandations et l'accès aux machines virtuelles juste-à-temps
- Implémenter Azure Sentinel, notamment les classeurs, les incidents et les playbooks.

Niveau requis

Avoir suivi les formations MSAZ900T00 "Microsoft Azure - Fondamentaux" et MSAZ104 "Microsoft Azure - Administrateur" ou avoir les connaissances équivalentes. Avoir de l'expérience dans le déploiement des charges de travail Azure, ainsi qu'avec les systèmes d'exploitation Windows et Linux et les langages de script (les labs peuvent utiliser PowerShell et CLI). Il est également important de bien connaître les protocoles de sécurité, tels que les VPN (réseaux privés virtuels), le protocole de sécurité d'Internet (IPSec), le protocole SSL (Secure Socket Layer), les méthodes de cryptage du disque et des données. De plus, il est conseillé de comprendre les meilleures pratiques de sécurité et les exigences de l'industrie en matière de sécurité (comme la défense approfondie, l'accès le moins privilégié, le contrôle de l'accès en fonction du rôle, l'authentification multifacteurs, la responsabilité partagée et le modèle confiance zéro).

Public concerné

Ingénieurs de sécurité Azure.

Partenaire / éditeur

Microsoft Partner
Microsoft
Gold Datacenter
Silver Cloud Productivity
Silver Messaging
Silver Communications
Silver Collaboration and Content

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Gérer l'identité et l'accès

- Azure Active Directory
- La protection d'identité Azure
- La gouvernance d'entreprise
- La gestion de l'identité privilégiée Azure AD
- L'identité hybride

Mettre en oeuvre une protection de plateforme

- Sécurité du périmètre
- Sécurité du réseau
- Sécurité de l'hôte
- Sécurité du conteneur

Sécuriser les données et les applications

- Azure Key Vault
- Sécurité des applications
- Sécurité du stockage
- Sécurité des bases de données SQL

Gérer les opérations de sécurité

- Azure Monitor
- Azure Security Center
- Azure Sentinel

Certification (en option)

- Prévoir l'achat d'un voucher en supplément
- Le passage de l'examen se fera (ultérieurement) dans un centre agréé Pearson Vue
- L'examen (en anglais) s'effectuera en ligne

Modalités d'évaluation des acquis

L'évaluation des acquis se fait :

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation ou une certification (M2i ou éditeur)

Les + de la formation

Ce cours ne couvre pas les bases de la gestion d'Azure, mais tient plutôt compte des connaissances existantes et y ajoute des informations spécifiques à la sécurité.

Le support de cours et les Microsoft Labs Online sont en anglais.

Compétences visées

- Gérer l'identité et l'accès des utilisateurs aux applications et données selon les besoins
- Mettre en oeuvre la protection de la plateforme contre les accès indésirables
- Gérer les opérations de sécurité au quotidien pour surveiller et anticiper toute alerte malveillante
- Sécuriser les données et les applications en gérant le stockage, la sauvegarde et leurs accès.