Programme de cours
Microsoft Azure Security Technologies

Durée :	4 jours soit 28 heures	Référence :	AZ-500T00

Public visé :

Ce cours est destiné aux administrateurs Azure. Les administrateurs Azure gèrent les services cloud qui couvrent les capacités de stockage, de mise en réseau et de cloud computing, avec une compréhension approfondie de chaque service. Les administrateurs Azure utilisent le portail Azure et à mesure qu'ils deviennent plus compétents, ils utilisent PowerShell et l'interface de ligne de commande.

Pré-requis :

Les participants reçus auront une connaissance préalable et une compréhension des éléments suivants :

- meilleures pratiques de sécurité et 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 zero trust,
- bien connaître les protocoles de sécurité, tels que les réseaux privés virtuels (VPN), le protocole de sécurité d'Internet (IPSec), le protocole Secure Socket Layer (SSL) , les méthodes de chiffrement de disque et des données,
- avoir de l'expérience dans le déploiement des charges de travail Azure. 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.
- Avoir de l'expérience avec les systèmes d'exploitation Windows et Linux et les langages de script. Les cours de laboratoires peuvent utiliser PowerShell et CLI.

Objectifs pédagogiques :

- Mettre en œuvre des stratégies de gouvernance d'entreprise, notamment le contrôle d'accès en fonction du rôle, les stratégies Azure et le verrouillage des ressources.
- Mettre en œuvre une infrastructure Azure AD, notamment des utilisateurs, des groupes, et une authentification multifacteurs.
- Mettre en œuvre une protection de l'identité Azure AD, notamment des stratégies de risque, un accès conditionnel et des vérifications d'accès.
- Mettre en œuvre la gestion de l'identité privilégiée Azure AD, notamment les rôles Azure AD et les ressources Azure.
- Mettre en œuvre Azure AD Connect, notamment les méthodes d'authentification et la synchronisation des répertoires sur site.
- Mettre en œuvre des stratégies de sécurité du périmètre, notamment le pare-feu Azure.
- Mettre en œuvre des stratégies de sécurité de réseau, notamment les groupes de sécurité réseau et les groupes de sécurité d'application.
- Mettre en œuvre 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 œuvre des stratégies de sécurité de conteneurs, notamment les instances de conteneurs Azure, le registre de conteneurs Azure, et Azure Kubernetes.
- Mettre en œuvre Azure Key Vault, notamment les certificats, les clés et les secrets.
- Mettre en œuvre des stratégies de sécurité d'applications, notamment l'inscription aux applications, les identités gérées et les points de terminaison des services.
- Mettre en œuvre 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 œuvre des stratégies de sécurité de bases de données, notamment l'authentification, la classification des données, el masquage dynamique des données, et Always Encrypted.
- Mettre en œuvre Azure Monitor, notamment les sources connectées, l'analyse des journaux et les alertes.
- Mettre en œuvre Azure Security Center, notamment les stratégies, les recommandations, et l'accès aux machines virtuelles juste-à-temps.
- Mettre en œuvre Azure Sentinel, notamment les classeurs, les incidents et les playbooks.

Compétences acquises à l'issue de la formation :

- Mettre en œuvre des stratégies de gouvernance d'entreprise
- Mettre en œuvre une infrastructure Azure AD
- Mettre en œuvre une protection de l'identité Azure AD
- Mettre en œuvre la gestion de l'identité privilégiée Azure AD
- Mettre en œuvre Azure AD Connect
- Mettre en œuvre des stratégies de sécurité du périmètre
- Mettre en œuvre des stratégies de sécurité de réseau
- Mettre en œuvre des stratégies de sécurité de l'hôte
- Mettre en œuvre des stratégies de sécurité de conteneurs
- Mettre en œuvre Azure Key Vault
- Mettre en œuvre des stratégies de sécurité d'applications
- Mettre en œuvre des stratégies de sécurité de stockage
- Mettre en œuvre des stratégies de sécurité de bases de données
- Mettre en œuvre Azure Monitor
- Mettre en œuvre Azure Security Center
- Mettre en œuvre Azure Sentinel, notamment les classeurs, les incidents et les playbooks.

Modalités pédagogiques :

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises ou intra-entreprises sur mesure.
La formation est animée par un(e) formateur(trice) durant toute la durée de la session et présentant une suite de modules théoriques clôturés par des ateliers pratiques validant l'acquisition des connaissances. Les ateliers peuvent être accompagnés de Quizz.
L'animateur(trice) présente la partie théorique à l'aide de support de présentation, d'animation réalisée sur un environnement de démonstration.
En présentiel comme en téléprésentiel, l'animateur(trice) accompagne les participants durant la réalisation des ateliers.

Moyens et supports pédagogiques :

Cadre présentiel

Salles de formation équipées et accessibles aux personnes à mobilité réduite.
- Un poste de travail par participant
- Un support de cours numérique ou papier (au choix)
- Un bloc-notes + stylo
- Vidéoprojection sur tableau blanc
- Connexion Internet
- Accès extranet pour partage de documents et émargement électronique

Cadre téléprésentiel

Session dispensée via notre solution iClassroom s'appuyant sur Microsoft Teams.
- Un compte Office 365 par participant
- Un poste virtuel par participant
- Un support numérique (PDF ou Web)
- Accès extranet pour partage de documents et émargement électronique

Informations sur l'accessibilité :

Description / Contenu

Module 1 : Gérer l'identité et l'accès

- Configurer Azure AD PIM
- Configurer et gérer Azure Key Vault
- Configurer Azure AD pour les charges de travail Azure
- Sécurité pour un abonnement Azure

Ateliers :

- Contrôle d'accès en fonction du rôle
- Azure Policy
- Verrous Resource Manager
- MFA, accès conditionnel et protection des identités AAD
- Azure AD Privileged Identity Management
- Implémenter la synchronisation des annuaires

Module 2 : Implémenter la protection de la plateforme

- Comprendre la sécurité du cloud
- Mise en réseau Azure
- Sécurisez le réseau
- Implémentation de la sécurité de l'hôte
- Mettre en œuvre la sécurité de la plateforme
- Mettre en œuvre la sécurité des abonnements

Ateliers :

- Configuration et sécurisation d'ACR et d'AKS
- Pare-feu Azure
- Groupes de sécurité réseau et groupes de sécurité des applications

Module 3 : Données et applications sécurisées

- Configurer des politiques de sécurité pour gérer les données
- Configurer la sécurité de l'infrastructure de données
- Configurer le chiffrement des données au repos
- Comprendre la sécurité des applications
- Mettre en œuvre la sécurité pour le cycle de vie des applications
- Applications sécurisées
- Configurez des politiques de sécurité pour gérer les données.
- Configurez la sécurité de l'infrastructure de données.
- Configurez le chiffrement des données au repos.
- Implémentez la sécurité pour la livraison des applications.
- Configurez la sécurité des applications.

Ateliers :

- Sécurisation d'Azure SQL Database
- Points de terminaison des services et sécurisation du stockage

Module 4 : Gérer les opérations de sécurité

- Configurer les services de sécurité
- Configurer des stratégies de sécurité à l'aide d'Azure Security Center
- Gérer les alertes de sécurité
- Répondre à une correction des problèmes de sécurité
- Créer des références de sécurité

Ateliers :

- Azure Sentinel
- Azure Security Center
- Azure Monitor