Smartfuture
Certifications | Training | Technology solutions

Formation & Certification •AZ-500

Technologies de sécurité Microsoft Azure

La formation « Technologies de sécurité Microsoft Azure » permet d'apprendre à sécuriser les environnements cloud Azure grâce à la gestion des accès, la mise en place de solutions de sécurité et la prévention des menaces.

Durée	Examen
4 jours (28heures)	AZ-500
Modalité	**Niveau**
Présentiel — Distanciel	Associate

INSCRIPTION / RÉSERVATION

Je m'inscris maintenant

Formateurs certifiés Microsoft

Orientation pratique sur la sécurité Azure

OBJECTIFS PÉDAGOGIQUES

- Comprendre les fonctionnalités de sécurité de Microsoft Azure.
- Sécuriser les identités, les accès et les ressources cloud.
- Protéger les réseaux, le stockage, les bases de données et les charges de travail.
- Superviser la sécurité et automatiser les opérations de protection.

PUBLIC CIBLE

- Professionnels de l'informatique.
- Administrateurs de sécurité.
- Architectes cloud.
- Ingénieurs en sécurité.
- Administrateurs réseau.

PRÉREQUIS

- Bonne compréhension des concepts de base du cloud et de Microsoft Azure.
- Bonne compréhension des concepts de base du cloud et de Microsoft Azure.
- Expérience préalable avec Azure (services de base et développement d'applications cloud).
- Expérience préalable dans l'administration de solutions de sécurité informatique.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Gérer l'identité et l'accès

Gérer les identités Microsoft Entra

- Gérer les identités Microsoft Entra.
- Sécuriser des utilisateurs Microsoft Entra.
- Sécuriser des groupes Microsoft Entra.
- Recommander quand utiliser des identités externes.
- Sécuriser les identités externes.
- Implémenter Protection des ID Microsoft Entra.

Gérer l'authentification Microsoft Entra

- Gérer l'authentification Microsoft Entra.
- Implémenter l'authentification multifacteur (MFA).
- Configurer la vérification d'identité Microsoft Entra.
- Implémenter l'authentification sans mot de passe.
- Implémenter la protection par mot de passe.
- Implémenter l'authentification unique (SSO).
- Intégrer l'authentification unique (SSO) et les fournisseurs d'identité.
- Recommander et appliquer des méthodes d'authentification modernes.

Gérer les autorisations Microsoft Entra

- Configurer les autorisations des rôles Azure pour les groupes d'administration, les abonnements, les groupes de ressources et les ressources.
- Attribuer des rôles intégrés Microsoft Entra.
- Attribuer des rôles intégrés Azure.
- Créer et attribuer des rôles personnalisés, notamment des rôles Azure et des rôles Microsoft Entra.
- Implémenter et gérer la gestion des autorisations Microsoft Entra.
- Configurer Microsoft Entra Privileged Identity Management.
- Configurer la gestion des rôles et les révisions d'accès dans Microsoft Entra.
- Implémenter des stratégies d'accès conditionnel.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Gérer l'accès aux applications Microsoft Entra

- Gérer l'accès aux applications d'entreprise dans Microsoft Entra ID, y compris les octrois d'autorisations OAuth.
- Gérer des inscriptions d'applications Microsoft Entra.
- Configurer les étendues des autorisations d'inscription d'une application.
- Gérer le consentement des autorisations d'inscription d'une application.
- Gérer et utiliser des principaux de service.
- Gérer les identités managées pour des ressources Azure.
- Recommander quand utiliser et configurer un proxy d'application Microsoft Entra, y compris l'authentification.

Sécuriser le réseau

Planifier et implémenter la sécurité pour les réseaux virtuels

- Planifier et implémenter des groupes de sécurité réseau (NSG) et des groupes de sécurité d'application (ASG).
- Planifier and implémenter des routes définies par l'utilisateur.
- Planifier et implémenter le peering de réseaux virtuels ou la passerelle VPN.
- Planifier et implémenter Virtual WAN, y compris un hub virtuel sécurisé.
- Sécuriser la connectivité VPN, y compris de point à site et de site à site.
- Implémenter le chiffrement sur ExpressRoute.
- Configurer les paramètres de pare-feu sur des ressources PaaS.
- Superviser la sécurité réseau en utilisant Network Watcher, y compris la journalisation des flux NSG.

Planifier et implémenter la sécurité pour l'accès privé à des ressources Azure

- Planifier et implémenter des points de terminaison de service de réseau virtuel.
- Planifier et implémenter des points de terminaison privés.
- Planifier et implémenter des services Private Link.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

- Planifier et implémenter l'intégration réseau pour Azure App Service et Azure Functions.
- Planifier et implémenter des configurations de sécurité réseau pour un environnement App Service.
- Planifier et implémenter des configurations de sécurité réseau pour une instance Azure SQL Managed Instance.

Planifier et implémenter la sécurité pour l'accès public à des ressources Azure

- Planifier et implémenter le protocole TLS (Transport Layer Security) aux applications, notamment Azure App Service et Gestion des API.
- Planifier, implémenter et gérer un Pare-feu Azure, y compris Azure Firewall Manager et des stratégies de pare-feu.
- Planifier et implémenter une passerelle d'application Azure.
- Planifier et implémenter une instance Azure Front Door, y compris un réseau de distribution de contenu (CDN).
- Planifier et implémenter un pare-feu d'applications web.
- Recommander quand utiliser Azure DDoS Protection Standard.

Sécuriser le calcul, le stockage et les bases de données

Planifier et implémenter une sécurité avancée pour le calcul

- Planifier et implémenter l'accès à distance aux points de terminaison publics, y compris l'accès juste-à-temps (JIT) à des machines virtuelles et Azure Bastion.
- Configurer l'isolation réseau pour Azure Kubernetes Service (AKS).
- Sécuriser et superviser AKS.
- Configurer l'authentification pour AKS.
- Configurer la supervision de la sécurité pour Azure Container Instances (ACI).
- Configurer la supervision de la sécurité pour Azure Container Apps (ACA).
- Gérer l'accès à Azure Container Registry (ACR).
- Configurer le chiffrement de disque, y compris Azure Disk Encryption (ADE), le chiffrement sur l'hôte et le chiffrement de disque confidentiel.
- Recommander des configurations de sécurité pour Gestion des API Azure.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Planifier et implémenter la sécurité pour le stockage

- Configurer le contrôle d'accès pour les comptes de stockage.
- Gérer le cycle de vie pour les clés d'accès du compte de stockage.
- Sélectionner et configurer une méthode appropriée pour accéder à Azure Files.
- Sélectionner et configurer une méthode appropriée pour accéder à Stockage Blob Azure.
- Sélectionner et configurer une méthode appropriée pour accéder à Tables Azure.
- Sélectionner et configurer une méthode appropriée pour accéder à Files d'attente Azure.
- Sélectionner et configurer les méthodes appropriées pour la protection contre les menaces de sécurité des données, y compris la suppression réversible, les sauvegardes, le contrôle de version et le stockage immuable.
- Configurer BYOK (Bring Your Own Key).
- Activer le chiffrement double au niveau de l'infrastructure de stockage Azure.

Planifier et implémenter la sécurité pour Azure SQL Database et Azure SQL Managed Instance

- Activer l'authentification de base de données Microsoft Entra.
- Activer l'audit pour les bases de données.
- Identifier les cas d'usage pour le portail de gouvernance Microsoft Purview.
- Implémenter la classification des données des informations sensibles en utilisant le portail de gouvernance Microsoft Purview.
- Planifier et implémenter le masquage dynamique.
- Implémenter TDE (Transparent Data Encryption).
- Recommander quand utiliser Azure SQL Database Always Encrypted.

Gérer les opérations de sécurité

Planifier, implémenter et gérer la gouvernance pour la sécurité

- Créer, affecter et interpréter des stratégies et des initiatives de sécurité dans Azure Policy.
- Configurer des paramètres de sécurité à l'aide d'Azure Blueprints.
- Déployer des infrastructures sécurisées en utilisant une zone d'atterrissage.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

- Recommander quand utiliser un module de sécurité matériel dédié (HSM).
- Configurer l'accès à Key Vault, y compris les stratégies d'accès au coffre et le contrôle d'accès en fonction du rôle Azure.
- Gérer les certificats, les secrets et les clés.
- Configurer la rotation des clés.
- Configurer la sauvegarde et la récupération des certificats, des secrets et des clés.
- Configurer la rotation des clés.
- Configurer la sauvegarde et la récupération des certificats, des secrets et des clés.

Gérer la posture de sécurité en utilisant Microsoft Defender pour le cloud

- Identifier et corriger les risques de sécurité en utilisant le niveau de sécurité et l'inventaire de Microsoft Defender pour le cloud.
- Évaluer la conformité aux cadres de sécurité en utilisant Microsoft Defender for Cloud.
- Ajouter des normes sectorielles et réglementaires à Microsoft Defender pour le cloud.
- Ajouter des initiatives personnalisées à Microsoft Defender pour le cloud.
- Connecter des environnements cloud hybrides et multiclouds à Microsoft Defender pour le cloud.
- Identifier et superviser les ressources externes en utilisant la gestion des surfaces d'attaque externe de Microsoft Defender.

Configurer et gérer la protection contre les menaces en utilisant Microsoft Defender pour le cloud

- Activer les services de protection des charges de travail dans Microsoft Defender pour le cloud, y compris Microsoft Defender pour le stockage, les bases de données, les conteneurs, App Service, Key Vault et Resource Manager.
- Configurer Microsoft Defender pour serveurs.
- Configurer Microsoft Defender pour Azure SQL Database.
- Gérer et répondre aux alertes de sécurité dans Microsoft Defender pour le cloud.
- Configurer l'automatisation des workflows en utilisant Microsoft Defender pour le cloud.
- Évaluer les analyses des vulnérabilités de Microsoft Defender pour le cloud.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Configurer et gérer des solutions de supervision et d'automatisation de la sécurité

- Superviser les événements de sécurité en utilisant Azure Monitor.
- Configurer des connecteurs de données dans Microsoft Sentinel.
- Créer et personnaliser des règles d'analytique dans Microsoft Sentinel.
- Évaluer les alertes et les incidents dans Microsoft Sentinel.
- Configurer l'automatisation dans Microsoft Sentine