DAWAN

Plan de la formation

www.dawan.fr

Formation Microsoft Azure : Sécurité

Durée :	5 jours (35 heures)
Tarifs inter-entreprise :	3 475,00 € HT (standard) 2 780,00 € HT (remisé)
Public :	Administrateurs Systèmes Microsoft avec bonnes connaissances d'Azure
Pré-requis :	Formation Microsoft Azure AZ-104 Administration ou les connaissances équivalentes
Objectifs :	Gérer et comprendre les mécanismes de protection des données Azure - Savoir implémenter des méthodes de chiffrement de données Azure - Connaître les protocoles sécurisés et savoir les mettre en place sur Azure.
Modalités pédagogiques, techniques et d'encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l'Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat. • Un formateur expert.
Modalités d'évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	CLO101550-F
Note de satisfaction des participants:	Pas de données disponibles
Contacts :	commercial@dawan.fr - 09 72 37 73 73

Modalités d’accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Gérer les identités dans Azure Active Directory (Azure AD)

Créer et gérer des principaux pour les ressources Azure
Gérer les groupes Azure AD
Gérer les utilisaeurs Azure AD
Gérer les comptes externes en utilisant Azure AD
Gérer les unités d'aministration

Sécuriser les accès avec Azure AD

Configurer Azure AD Privileged Identity Management (PIM)
Mettre en place Conditional Access policies, ainsi que le MFA
Mettre en place Azure AD Identity Protection
Gérer de l'authentification sans mot de passe
Examiner les accès

Gérer les accès des applications

Intégrer le single sign-on (SSO) et les fournisseurs d'identités pour l'authentification
Créer une inscription d'application
Configurer les étendues des autorisations d'application
Gérer les consentement des autorisations d'application
Gérer l'accès via API permissions aux abonnements et aux ressources Azure
Configurer une méthode d'authentification pour les principal de service

Gérer le contrôle d'accès

Configurer les rôles et permissions Azure pour gérer les accès
Comprendre les rôles et les permissions des ressources
Utilisr des rôles standard Azure AD
Créer et utilser des rôles personnalisés

Sécurité réseau avancée

Sécuriser la connectivité des réseaux hybrides networks
Sécuriser les réseaux virtuels
Créer et configurer Azure Firewall
Créer et configurer Azure Firewall Manager
Créer et utiliser Azure Application Gateway
Créer et utiliser Azure Front Door
Utiliser le Web Application Firewall (WAF)
Configurer le pare-feu sur une ressource, dont les comptes de stockage, Azure SQL, Azure Key Vault ou Azure App Service
Isoler les réseaux pour les Web Apps et les Azure Functions
Mettre en oeuvre Azure Service Endpoints
Implémenter les Azure Private Endpoints, dont l'intégration avec les autres services -
Mettre en place Azure Private Links
Utiliser Azure DDoS Protection

Sécurité avancée pour VMs et containers

Configurer Azure Endpoint Protection pour les machines virtuelles(VMs)
Gérer les mise à jour de sécurité pour les VMs
Configurer la sécurité pour les services de container
Gérer les accès à Azure Container Registry
Sécuriser les containers
Sécuriser les Azure App Services
Chiffrer les données du tenant
Chiffrer les données en transit

Gestion des stratégies centralisées

Configurer une stratégie de sécurité personnalisée
Créer une stratégie d'initiatives
Configurer les paramètres de sécurité et d'audit avec Azure Policy

Configurer une protection contre les menaces

Configurer Azure Defender for Servers
Evaluer les scans de vulnerabilité d'Azure Defender
Configurer Azure Defender pour SQL
Utiliser Microsoft Threat Modeling Tool

Gérer les solutions de supervision de sécurité

Créer et personnaliser des règles d'alerte avec Azure Monitor
Configurer les logs de diagnostic et la rétention de log avec Azure Monitor
Surveiller les logs de sécurité avec Azure Monitor
Créer et personnaliser des règles d'alerte avec Azure Sentinel
Configurer des connecteurs avec Azure Sentinel
Evaluer les alertes et incidents dans Azure Sentinel

Sécuriser le stockage

Configurer le contrôle d'accès sur les comptes de stockage
Configurer les clés d'accès des comptes de stockage SAS
Configurer l'authentification via Azure AD pour Azure Storage et Azure Files
Configurer les accès délégués

Sécuriser les données

Activer authentification des base de données avec using Azure AD
Activer l'audit des bases de données
Configurer le masquage dynamique de données avec SQL workloads
Mettre en oeuvre le chiffrement de base de données pour Azure SQL Database
Implémenter l'isolation réseau pour le stockage des données, dont Azure Synapse Analytics et Azure Cosmos DB

Configurer et gérer Azure Key Vault

Créer et configurer Key Vault
Configurer les accès à Key Vault
Gérer les certificats, les secrets et les clés
Configurer la rotation de clé
Gérer les sauvegardes et récupération des certificats, secrets et clés