

Formation AZ-305 - Azure Solutions Architect Expert

| | |
|--|--|
| ■ Durée : | 4 jours (28 heures) |
| ■ Tarif inter-entreprise : | 3 275,00 CHF HT (standard) 2 620,00 CHF HT (remisé) |
| ■ Public : | Professionnels de l'informatique ayant une expertise dans la conception et la mise en œuvre de solutions s'exécutant sur Microsoft Azure Architectes |
| ■ Pré-requis : | Avoir suivi la formation Microsoft Azure - Administration Expérience sur du déploiement ou de l'administration de ressources Azure Posséder des connaissances sur Azure Active Directory, les technologies de calcul Azure, la mise en réseau virtuelle Azure, les technologies de stockage Azure Compréhension des concepts généraux de conception d'applications tels que la messagerie et la haute disponibilité |
| ■ Objectifs : | Sécuriser l'identité et l'accès (contrôles, MFA, accès conditionnel) - Sécuriser le réseau Azure (endpoints privés, Firewall, TLS, WAF) - Sécuriser le calcul, le stockage et les bases de données (chiffrement, isolation, sécurité container) - Sécuriser Azure avec Microsoft Defender et Microsoft Sentinel (politique, posture de sécurité, détection et réponse aux menaces) - Être préparé à passer la certification AZ-305 |
| ■ Modalités pédagogiques, techniques et d'encadrement : | <ul style="list-style-type: none">• 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. |

| | |
|---|---|
| <p>■ Modalité d'évaluation :</p> | <ul style="list-style-type: none"> • 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. |
| <p>■ Sanction :</p> | Attestation de fin de formation mentionnant le résultat des acquis |
| <p>■ Référence :</p> | CLO102960-F |
| <p>■ Note de satisfaction des participants :</p> | Pas de données disponibles |
| <p>■ Contacts :</p> | commercial@dawan.fr - 09 72 37 73 73 |
| <p>■ Modalités d'accès :</p> | Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard. |
| <p>■ Délais d'accès :</p> | Variable selon le type de financement. |
| <p>■ Accessibilité :</p> | 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 |

Concevoir des architectures Azure alignées sur les besoins métier

Analyser un besoin métier et le traduire en exigences d'architecture
 Identifier les contraintes de disponibilité, de sécurité, de coûts et d'exploitation
 Arbitrer entre plusieurs options de services Azure selon les cas d'usage
 Relier les choix d'architecture aux besoins de performance, de résilience et de maintenabilité
 Structurer une démarche de conception cohérente à l'échelle d'un système
 Documenter une architecture cible de manière lisible et argumentée

Atelier fil rouge

Analyser un scénario d'entreprise et formuler une première architecture Azure en justifiant les grands choix de conception

Sécuriser l'identité et l'accès dans une architecture Azure

Positionner l'identité comme composant central d'une architecture cloud
 Intégrer contrôles d'accès, MFA et accès conditionnel dans la conception
 Prévoir les mécanismes de séparation des rôles et de gouvernance des accès

Relier architecture de sécurité, administration et exploitation

Prendre en compte la protection des identités privilégiées et des comptes sensibles

Concevoir des accès cohérents avec les besoins métier et les exigences de conformité

Atelier fil rouge

Définir une stratégie d'identité et d'accès pour une architecture Azure multi-environnements

Sécuriser le réseau Azure dans une logique d'architecture cible

Structurer une architecture réseau Azure cohérente et cloisonnée

Intégrer endpoints privés, Azure Firewall, TLS et WAF dans une logique de défense en profondeur

Relier sécurité réseau, exposition applicative et segmentation des ressources

Prendre en compte les besoins de connectivité, de contrôle des flux et de simplicité d'exploitation

Comparer plusieurs options de sécurisation selon le contexte technique

Intégrer les contraintes de performance, de disponibilité et de sécurité dans le design

Atelier fil rouge

Concevoir la sécurisation réseau d'une architecture Azure exposée à des usages internes et externes

Sécuriser le calcul, le stockage et les bases de données dans une architecture Azure

Identifier les points de vigilance liés aux ressources de calcul, aux données et aux services applicatifs

Concevoir des mécanismes de chiffrement, d'isolation et de protection adaptés

Relier les choix de services Azure à la sécurité des traitements et des données

Intégrer les problématiques de durcissement, de segmentation et de cloisonnement

Prendre en compte les enjeux de continuité, de restauration et de protection applicative

Mettre en cohérence architecture technique et sécurité des ressources

Atelier fil rouge

Revoir une architecture Azure existante et proposer les améliorations de sécurité sur le calcul, le stockage et les bases de données

Sécuriser Azure avec Microsoft Defender et Microsoft Sentinel

Comprendre le rôle de la posture de sécurité dans une architecture Azure
Intégrer Microsoft Defender et Microsoft Sentinel dans un design de supervision de sécurité
Structurer la détection et la réponse aux menaces dans une logique d'exploitation continue
Relier visibilité, surveillance et réaction à la stratégie globale d'architecture
Prioriser les risques et les mesures de remédiation
Prévoir l'usage des outils de sécurité dans une approche gouvernée et industrialisée

Atelier fil rouge

Définir une logique de posture de sécurité, de détection et de réaction pour une architecture Azure critique

Préparer l'examen AZ-305 - Azure Solutions Architect Expert

Comprendre la structure de l'examen et les domaines évalués
Identifier les attentes d'un niveau Solutions Architect Expert
S'entraîner à raisonner à partir de scénarios de conception
Repérer les pièges liés aux arbitrages techniques, de sécurité et d'exploitation
Adopter une méthode de lecture et de décision adaptée aux questions d'architecture
Consolider les axes de révision avant inscription

Atelier fil rouge

Réaliser un entraînement guidé sur des questions de niveau AZ-305 et corriger les réponses de manière argumentée