Devenir certifié Microsoft Azure Security Engineer Associate (AZ-900+AZ-500)

Date et durée

Code formation : AZ-500-BIS
Durée : 5 jours
Nombre d'heures : 35 heures

Formation avec certification

Azure Security Engineer Associate

Description

Les solutions informatiques offertes grâce à **Microsoft Azure** permettent plus de mobilité, d'ouverture, d'applications et d'échanges avec l'extérieur à l'entreprise. La sécurité tient ainsi une place primordiale dans la **stratégie IT des entreprises** utilisant ces solutions.
Dans cette formation Azure AZ-500, vous acquerrez toutes les compétences théoriques et pratiques dont vous avez besoin pour devenir un ingénieur associé en sécurité Azure certifié Microsoft. Pendant la 1ère journée, vous aborderez **les concepts fondamentaux du cloud computing**, mais aussi les différents modèles et types de services, tels que le cloud privé, le cloud public et le cloud hybride

Ensuite, durant 4 jours, vous développerez vos connaissances pour **définir et mettre en œuvre des contrôles de sécurité pour Azure**. Cela vous permettra de mettre en place des politiques de sécurité adéquates, d'identifier et de corriger des éventuelles vulnérabilités. Enfin, vous serez formé aux outils de script, à l'automatisation, à la virtualisation et à l'architecture cloud N-tier.

A l'issue de cette formation sur la sécurité dans Azure, vous serez en mesure de **passer l'examen AZ-500 inclus dans notre offre**. La réussite de celui-ci, vous permettra d'obtenir le titre de *Microsoft Certified Azure Security Engineer Associate*.

Objectifs

À l'issue de la **formation Microsoft Azure AZ-500**, vous atteindrez les objectifs de compétences suivants :

- découvrir et comprendre les différents concepts du cloud computing ;
- connaitre et décrire les principaux services et outils de gestion disponible sur Azure.
- connaitre et décrire les principales fonctions de sécurité générale ainsi que celles de la sécurité des réseaux ;
- connaitre et décrire les services d'identité, les services de gouvernance, les services de confidentialité et les services de conformité ;
- comprendre les accords de niveau de service Azure et la gestion des coûts sont organisés ;
- maitriser la gestion des identités et des accès (IAM) ;
- implémenter la sécurité pour la plateforme Azure ;
- comprendre et intégrer les processus liés aux activités de sécurité ;
- mettre en place une protection pour les données et les applications ;
- réussir l'examen AZ-500 et obtenir la certification Azure Security Engineer Associate.

Points forts

Des cours dispensés par un formateur expert des solutions cloud et certifiée Microsoft Azure ; un programme officiel axé sur des travaux pratiques et une préparation à l'examen Microsoft Azure AZ-500.
Garantie de certification : cette formation inclut le "Microsoft Exam Replay", ce qui vous permet de repasser l'examen gratuitement en cas d'échec à la première tentative.

Certification

Cette formation qui vous permet de passer l'examen AZ-500, vous permettra d'obtenir la certification **Microsoft : Azure Security Engineer Associate**. Elle est idéale si vous souhaitez prétendre au **rôle d'ingénieur sécurité** .
Afin de réussir cet examen, vous devez maîtriser les éléments suivants : gérer l'identité et l'accès, mettre en œuvre une protection de plateforme, gérer les opérations de sécurité et sécuriser les données ainsi que les applications.
De plus, vous devez **avoir une expérience en matière d'administration d'Azure** et des environnements hybrides et connaître l'infrastructure en tant que code, les processus d'opérations de sécurité, les fonctionnalités du cloud ainsi que les services Azure.
Pour conclure, la **certification Azure Security Engineer Associate** permet de se préparer à passer d'autres certifications Azure orientées sur les rôles, telles que *Azure Database Administrator Associate* ou *Azure Data Engineer Associate*, sans toutefois être une condition requise pour les obtenir.
En savoir + sur les certifications Azure

Modalités d'évaluation

Travaux Pratiques

Pré-requis

Suivre la **formation Microsoft Azure AZ 500** nécessite les prérequis suivants :

- avoir des connaissances en matière de bonnes pratiques et d'exigences de sécurité liées à l'informatique ;
- connaître les protocoles de sécurité (VPN, IPSec, SSL, etc.) et les diverses mesures de chiffrement des disques et des données ;
- posséder une expérience dans le déploiement des charges de travail Azure ;
- disposer de compétences en matière de systèmes d'exploitation Windows et Linux ainsi que des langages de script.

Pour obtenir ces prérequis, vous pouvez suivre cette formation :

Les formations ci-dessous sont recommandées.

Public

Cette formation s'adresse aux publics suivants :

- les ingénieurs en sécurité Azure qui souhaitent se préparer à l'examen de certification Associate ou qui ont des responsabilités en matière de sécurité dans leur poste ;
- les professionnels IT qui désirent se spécialiser dans la sécurité des plates-formes numériques basées sur Azure et qui jouent un rôle essentiel dans la protection des données d'une organisation.

Cette formation s'adresse aux profils suivants

Ingénieur système
Administrateur système

Programme

Les fondamentaux de Microsoft Azure AZ-900 *(1 jour)*

Module 1 : Qu'est-ce que le cloud computing ?

- Présentation et explication des différents concepts du Cloud Computing.
- Introduction aux services du Cloud (Iaas, Paas Saas).
- Présentation des modèles de cloud publics, privés et hybrides.

Module 2 : les services Azure de base

- Présentation des principaux éléments de l'architecture de Azure.
- Présentation générale des charges de travail d'Azure.
- Présentation des services réseau Azure.
- Présentation des services de stockage Azure.
- Présentation de la structure de la base de données Azure.

Module 3 : les solutions et les outils Azure de base

- Comment choisir son service Azure IoT ?
- Comment choisir son service d'IA ?
- Comment choisir sa technologie de serveurs Azure ?
- Comment choisir les outils les plus adaptés pour DevOPS et GitHub ?
- Comment choisir ses outils de gestion ?
- Comment choisir son service de monitoring Azure ?

Module 4 : les fonctions de sécurité et de réseau Azure de base

- Aperçu des outils et des fonctions de sécurité.
- Configuration de la connexion réseau.

Module 5 : les services d'identités, la gouvernance et la conformité

- Présentation des principaux services d’identité Azure.
- Instauration d'une stratégie de gouvernance Azure.
- Implantation de normes de confidentialité, de conformité et de protection des données.

Module 6 : la maîtrise des coûts et le cycle de vie des services Azure

- Prévision et management des dépenses.
- Gestion des accords de niveau de service (SLA).

Mise en œuvre des fonctions de sécurité AZ-500 *(4 jours)*

Module 1 : gestion des identités et des accès

- Gérer les identités avec Azure Active Directory :
    - sécuriser les utilisateurs et les groupes de répertoires ;
    - l'utilisation des identités externes (recommandation et sécurisation) ;
    - mettre en place une protection d'identité via Azure AD.
- Gérer l'authentification avec Azure Active Directory :
    - paramétrer Microsoft Entra Verified ID ;

    - implémenter l'authentification multifactorielle (MFA) ;
    - implémenter l'authentification sans mot de passe ;
    - implémenter la protection par mot de passe ;
    - implémenter l'authentification unique (SSO) et les fournisseurs d'identité ;
    - utiliser des protocoles d'authentification modernes (recommandation).
- Gérer les accès avec Azure Active Directory :
    - paramétrer les droits pour les rôles Azure, les groupes de gestion, les abonnements, les groupes de ressources et les ressources ;
    - assigner des rôles intégrés à Azure AD et à Azure ;
    - créer et assigner des rôles personnalisés ;
    - gérer Microsoft Entra Permissions Management ;
    - configurer la gestion des identités privilégiées d'Azure AD (PIM) ;
    - configurer la gestion des rôles et les contrôles d'accès à l'aide de Microsoft Entra Identity Governance ;
    - définir des politiques d'accès conditionnel.
- Gérer les accès aux applications dans Azure AD :
    - configurer l'accès aux applications d'entreprise dans Azure AD, incluant les autorisations OAuth ;
    - paramétrer les enregistrements des apps dans Azure AD ;
    - configurer les champs d'autorisation de l'enregistrement des applications ;
    - gérer le consentement à l'enregistrement des apps ;
    - gérer les identités gérées pour les ressources Azure
    - utiliser et configurer l'authentification pour un proxy d'application Azure AD (recommandation).

Module 2 : sécurisation du réseau et des accès

- Planifier et sécuriser les réseaux virtuels :
    - créer des groupes de sécurité réseau (NSG) et des groupes de sécurité applicative (ASG) ;
    - configurer des routes définies par l'utilisateur (UDR) ;
    - installer un peering VNET ou une passerelle VPN ;
    - installer un WAN virtuel, incluant un hub virtuel sécurisé ;
    - sécuriser la connectivité VPN, notamment les connexions point à site et site à site ;
    - implémenter le cryptage avec ExpressRoute ;
    - configurer les paramètres du pare-feu sur les ressources PaaS ;
    - surveiller la sécurité du réseau à l'aide de Network Watcher, notamment la journalisation des flux NSG.
- Planifier et sécuriser l'accès privé aux ressources Azure :
    - créer des nœuds de terminaison de service pour le réseau virtuel ;
    - créer des nœuds de terminaison privés ;
    - configurer les services Private Link ;
    - planifier et configurer l'intégration réseau pour Azure App Service et Azure Functions ;
    - définir des paramètres de sécurité réseau pour un environnement App Service (ASE) ;
    - définir des paramètres de sécurité réseau pour une instance gérée Azure SQL et les implanter.
- Planifier et sécuriser l'accès public aux ressources Azure :
    - configurer le protocole TLS pour les applications, incluant Azure App Service et API Management ;
    - paramétrer le pare-feu Azure, et notamment le gestionnaire et les règles de ce dernier ;
    - déployer une passerelle d'application Azure Planifier et déployer une passerelle principale Azure, incluant le réseau de diffusion de contenu (CDN) ;
    - installer un pare-feu d'application Web (WAF) ;
    - utiliser le système Azure DDoS Protection Standard (recommandation).

Module 3 : sécurisation des ordinateurs, du stockage et des bases de données

- Implémenter des mesures de sécurité avancées pour les ordinateurs :
    - configurer un accès distant aux points de terminaison publics, dont Azure Bastion et JIT ;

    - configurer l'isolation du réseau pour Azure Kubernetes Service (AKS) Sécuriser et monitorer AKS ;
    - configurer l'authentification pour AKS ;
    - configurer la surveillance de la sécurité pour les instances de conteneurs Azure (ACI) ;
    - configurer la surveillance de la sécurité pour les Azure Container Apps (ACAs) ;
    - gérer l'accès à Azure Container Registry (ACR)
    - configurer le chiffrement de disque, incluant Azure Disk Encryption (ADE), le chiffrement en tant qu'hôte et le chiffrement de disque confidentiel ;
    - utiliser des configurations de sécurité pour Azure API Management (recommandation).
- Planifier et implémenter des mesures de sécurité pour le stockage :
    - configurer le contrôle d'accès pour les comptes de stockage ;
    - gérer le cycle de vie des clés d'accès aux comptes de stockage ;
    - choisir et configurer une méthode appropriée pour l'accès aux fichiers Azure ;
    - choisir et configurer une méthode adaptée pour l'accès à Azure Blob Storage ;
    - choisir et configurer une méthode adaptée pour l'accès à Azure Tables ;
    - choisir et configurer une méthode adaptée pour l'accès aux files d'attente Azure ;
    - choisir et configurer des méthodes adaptées pour se protéger contre les menaces à la sécurité des données, y incluant la suppression programmée, les sauvegardes, le versionnage et le stockage immuable ;
    - configurer le système Bring your own key (BYOK) ;
    - activer le double cryptage au niveau de l'infrastructure de stockage Azure.
- Planifier et implémenter des mesures de sécurité pour Azure SQL Database et Azure SQL Managed Instance :
    - activer l'authentification de la base de données via Microsoft Azure AD qui est inclus dans Microsoft Entra ;
    - activer l'audit de la base de données ;
    - identifier les cas d'utilisation du portail de gouvernance Microsoft Purview ;
    - effectuer la classification des données sensibles à l'aide du portail de gouvernance Microsoft Purview Planifier et utiliser le masquage dynamique ;
    - paramétrer le chiffrement transparent des bases de données (TDE) ;
    - utiliser Azure SQL Database Always Encrypted (recomandation).

Module 4 : gestion des opérations de sécurité

- Créer, attribuer et interpréter les politiques et initiatives de sécurité dans Azure Policy.
- Configurer les paramètres de sécurité en utilisant Azure Blueprint.
- Déployer des infrastructures sécurisées en utilisant une zone de déploiement
- Créer et configurer un coffre-fort avec Azure Key Vault.
- Utiliser un système de gestion des clés dédié (HSM) configurer les accès au coffre-fort des clés, incluant les politiques et le contrôle d'accès basé sur les rôles d'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.