


## AZ-500: Devenir certifié Microsoft Azure Security Engineer Associate

Date et durée
<p>Code formation : AZ-500</p> <p>Durée : 4 jours</p> <p>Nombre d'heures : 28 heures</p>

Formation avec certification
Azure Security Engineer Associate
Description
<p>Cette formation prépare les participants à l'examen <b>Microsoft AZ-500</b>. Elle répond à toutes les exigences de Microsoft et est dispensée par un formateur certifié Microsoft, avec des labs officiels et un support de cours officiel Microsoft.</p> <p>Dans un environnement où la sécurité du cloud est cruciale, cette formation permet d'acquérir les compétences essentielles pour protéger les infrastructures Azure. Les participants apprendront à <b>mettre en œuvre des contrôles de sécurité, sécuriser les identités et accès, protéger les applications et surveiller les menaces</b>.</p> <p>Le programme alterne <b>théorie et mises en pratique</b> pour maîtriser la gestion des identités, la sécurisation des réseaux et hôtes, l'automatisation des tâches de sécurité et la surveillance proactive via Azure Security Center et Azure Sentinel.</p> <p>À l'issue de cette formation, les participants pourront passer l'examen <b>AZ-500</b>, leur permettant d'obtenir la certification <b>Microsoft Certified: Azure Security Engineer Associate</b>. Reconnu sur le marché, le titre <b>Azure Security Engineer Associate</b> ouvre des opportunités dans les métiers de la <b>cybersécurité et de la gestion des infrastructures cloud sécurisées</b>.</p> <p>Cette certification professionnelle est également inscrite au Répertoire Spécifique sous le numéro <b>RS5308 "Garantir la sécurité de l'infrastructure Cloud Microsoft Azure"</b>, rendant cette formation éligible au Compte Personnel de Formation (CPF) et le passage de l'examen obligatoire.</p>
Objectifs
<p>À l'issue de la <b>formation Microsoft Azure AZ-500</b>, vous atteindrez les objectifs de compétences suivants :</p> <ul style="list-style-type: none"><li>• Maîtriser les concepts de sécurité spécifiques au cloud Azure et à l'infrastructure hybride.</li><li>• Configurer et sécuriser les identités et accès avec <b>Azure Active Directory (Entra ID)</b>.</li><li>• Déployer et configurer les protections avancées de sécurité pour les workloads Azure.</li><li>• Maîtriser la gestion des identités et des accès (<b>IAM - Identity &amp; Access Management</b>).</li><li>• Implémenter la sécurité pour la <b>plateforme Azure</b>.</li><li>• Comprendre et intégrer les processus liés aux activités de sécurité.</li><li>• Mettre en place une <b>protection pour les données et les applications</b>.</li><li>• Réussir l'examen <b>AZ-500</b> et obtenir la certification <b>Azure Security Engineer Associate</b>.</li></ul>
Points forts

Tarif tout inclus: support de cours officiel Microsoft, labs Microsoft AZ-500 et examen de certification.

Les cours sont dispensés par un formateur expert des solutions cloud et certifié Microsoft Azure ; Programme officiel axé sur des travaux pratiques

Le support de cours et l'examen sont en anglais

**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 prépare au passage de l'examen AZ-500, permettant d'obtenir la certification **Microsoft Certified : Azure Security Engineer Associate**.

Cet examen dure 2h, il se déroule en ligne dans un centre Pearson Vue ou avec surveillance à distance.

Les candidats doivent **prouver leurs compétences en contrôle de sécurité, en gestion de l'identité et de l'accès, et en maintenance de la structure de sécurité**. À travers cette épreuve, quatre branches distinctes de connaissance sont passées en revue:

- Gérer l'identité et l'accès
- Mettre en œuvre une protection de plateforme
- Gérer les opérations de sécurité
- Sécuriser les données et les applications

À noter que, contrairement à d'autres certifications Microsoft, l'examen AZ-500 est la seule épreuve à réussir pour devenir certifié Azure Security Engineer Associate.

+ d'infos sur le processus de certification Microsoft: <https://learn.microsoft.com/en-us/credentials/certifications/certification-process-overview?types=true>

+ d'infos sur les modalités d'évaluation: <https://learn.microsoft.com/fr-fr/credentials/certifications/resources/study-guides/az-500>

À noter: après la certification AZ-500, vous pourrez vous spécialiser davantage en passant les certifications SC-200 (Security Operations Analyst) ou SC-300 (Identity & Access Administrator). Cette certification ouvre également la voie à des postes d'architecte sécurité cloud ou de consultant en cybersécurité Azure.

## Modalités d'évaluation

Quiz / QCM

Travaux Pratiques

Etude de cas

## Pré-requis

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

- Avoir suivi la formation préparant à l'examen AZ-900 et obtenir sa certification Azure Fundamentals est fortement recommandé. À défaut, vous aurez besoin de :
  - 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.

Les formations ci-dessous sont recommandées.

Les fondamentaux de Microsoft Azure (AZ-900)

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

### Tour de table

- Introduction individuelle
- Introduction au cadre de la formation
- Alignement avec les objectifs et enjeux spécifiques
- Identification des attentes et des perspectives individuelles des participants

### Module 1 : Gestion des identités et des accès

- Configuration d'Azure Active Directory (AD) et des identités gérées
  - Implémentation de l'authentification multifactorielle (MFA) et des politiques d'accès conditionnel
  - Gestion des identités privilégiées avec Azure AD Privileged Identity Management (PIM)
- Lab** : Configuration et gestion des accès avec Azure AD

### Module 2 : Sécurisation des réseaux et des accès

- Sécurisation des connexions réseau avec NSG, VPN, ExpressRoute et Private Link
  - Configuration et gestion des pare-feu Azure et des protections contre les attaques DDoS
  - Implémentation des accès privés et publics aux ressources Azure
- Lab** : Implémentation des règles de sécurité réseau sur Azure

### Module 3 : Sécurisation des hôtes et des conteneurs

- Protection des machines virtuelles et durcissement des configurations
  - Sécurisation des environnements Kubernetes (AKS) et des registres de conteneurs (ACR)
  - Surveillance et protection des workloads cloud
- Lab** : Sécurisation d'une infrastructure Kubernetes et d'Azure Container Registry

### Module 4 : Surveillance et gestion des incidents de sécurité

- Utilisation d'Azure Monitor, Log Analytics et Azure Security Center
  - Gestion des alertes de sécurité et des recommandations avec Defender for Cloud
  - Réponse aux incidents avec Azure Sentinel et automatisation des playbooks
- Lab** : Surveillance de la sécurité et investigation avec Azure Sentinel

### Module 5 : Sécurisation des données et des applications

- Mise en œuvre du chiffrement des données et des bases de données Azure

- Gestion des certificats, clés et secrets avec Azure Key Vault
- Sécurisation des applications via des stratégies d'accès et des certificats SSL/TLS

**Lab** : Configuration de la protection des données avec Azure Key Vault

## **Module 6 : Gouvernance et conformité en entreprise**

- Implémentation des politiques de sécurité avec Azure Policy
- Configuration des contrôles d'accès RBAC et audits de conformité
- Application des bonnes pratiques de sécurité Microsoft pour les environnements cloud

**Lab** : Déploiement des politiques de gouvernance et conformité sur Azure

## **Module 7 : Automatisation et gestion avancée de la sécurité**

- Automatisation de la gestion de la sécurité avec PowerShell et Azure CLI
- Création et gestion d'environnements sécurisés avec des templates ARM
- Orchestration des réponses aux incidents avec Logic Apps et playbooks Sentinel

**Lab** : Automatisation des tâches de sécurité avec PowerShell et Azure CLI

Microsoft® et Microsoft Azure® sont des marques déposées ou des marques commerciales de Microsoft Corporation aux États-Unis et dans d'autres pays.