03 20 61 95 06
formation@access-it.fr

Formation Microsoft Azure AZ-500 Technologies de sécurité

Durée de la formation : 4 jour(s) / 28 heure(s)

OBJECTIFS

A l'issue de la formation, l'apprenant sera capable de :
Comprendre comment gérer l'identité et l'accès sur Azure
Apprendre à mettre en oeuvre la protection de la plate-forme
Sécuriser les données et les applications
Comprendre comment gérer les opérations de sécurité

PREREQUIS

Il est recommandé que les participants soient certifiés Microsoft Azure Administrator Associate ou possèdent les connaissances équivalentes.
La connaissance des différentes charges de travail Azure ainsi que des notions de sécurité applicables à ces charges est recommandées. Un entretien en amont avec notre expert permet de prendre en compte le profil de chaque participant (niveau, objectifs et résultats attendus, contexte professionnel, enjeux...) et d'adapter le contenu de la formation si besoin.
Cette formation ne peut être financée que dans le cadre d'un projet d'entreprise (prise en charge entreprise ou OPCO). Les dossiers à financement personnel et CPF ne sont pas pris en compte.

PUBLIC

Cette formation est destinée aux administrateurs Azure ou professionnels IT souhaitant renforcer leurs compétences pratiques pour implémenter et gérer la sécurité dans des environnements cloud Azure.

03 20 61 95 06
formation@access-it.fr

Formation Microsoft Azure AZ-500 Technologies de sécurité

Durée de la formation : 4 jour(s) / 28 heure(s)

PROGRAMME

Gérer les contrôles de sécurité pour l'identité et l'accès

• Sécuriser les identités utilisateur dans Microsoft Entra ID en implémentant des contrôles de gestion des accès et d'authentification forts.
• Protéger les groupes et la gestion des accès en appliquant des mesures de sécurité pour empêcher toute modification ou mauvaise utilisation non autorisée.
• Gérer les identités externes en toute sécurité en définissant des stratégies qui garantissent la confidentialité, l'intégrité et le contrôle d'accès approprié.
• Implémenter Microsoft Entra ID Protection pour détecter, examiner et atténuer les menaces de sécurité liées aux identités.
• Appliquer des stratégies d'accès conditionnel pour appliquer des contrôles de sécurité en fonction du comportement de l'utilisateur, de la conformité des appareils et des risques contextuels.

Gérer l'accès aux applications dans Microsoft Entra ID

• Gérer l'accès aux applications d'entreprise dans Microsoft Entra ID, y compris les octrois d'autorisations OAuth pour le contrôle d'accès.
• Administrer l'intégration d'applications aux plateformes d'identité via les inscriptions d'applications Microsoft Entra ID.
• Configurer les étendues des autorisations d'inscription des applications pour les niveaux d'accès aux ressources appropriés.
• Gérer le consentement d'inscription des applications et utilisez les principaux de service et les identités managées pour la gestion automatisée et la sécurité améliorée.

Planifier et implémenter la sécurité pour les réseaux virtuels

• Implémenter des mesures de sécurité pour les réseaux virtuels Azure afin de protéger les données et les ressources.
• Utiliser des groupes de sécurité réseau (NSG) et des groupes de sécurité d'application (ASG) pour la sécurité du trafic réseau, et gérez les UDRs pour un routage optimal du trafic.
• Établir une connectivité réseau sécurisée via le peering de réseaux virtuels, les passerelles VPN et Virtual WAN.
• Améliorer la sécurité réseau avec les configurations VPN, le chiffrement ExpressRoute, les paramètres de pare-feu PaaS et la surveillance de Network Watcher.

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

• Développer des stratégies de sécurité pour l'accès privé aux ressources Azure afin de protéger les données sensibles.
• Utiliser des points de terminaison de service de réseau virtuel et des points de terminaison privés pour sécuriser l'accès au service Azure.
• Gérer les services Private Link pour sécuriser l'exposition des ressources et intégrer Azure App Service et Functions à des réseaux virtuels.
• Configurer la sécurité réseau pour App Service Environment et Azure SQL Managed Instance pour protéger les applications web et les bases de données.

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

• Développer des stratégies pour sécuriser l'accès public aux ressources Azure, ce qui empêche l'accès et les violations non autorisés.
• Implémenter TLS pour Azure App Service et Gestion des API pour chiffrer les données en transit.
• Protéger le trafic réseau avec le Pare-feu Azure et Application Gateway pour optimiser la sécurité et la remise des applications web.
• Améliorer les performances des applications web avec Azure Front Door et CDN, et déployez WAF et DDoS Protection pour

03 20 61 95 06
formation@access-it.fr

Formation Microsoft Azure AZ-500 Technologies de sécurité

Durée de la formation : 4 jour(s) / 28 heure(s)

une défense robuste contre les attaques.

Planifier et implémenter une sécurité avancée pour le calcul

• Améliorer la sécurité des ressources de calcul Azure contre les vulnérabilités et les attaques à l'aide de mesures avancées.
• Sécuriser l'accès à distance via Azure Bastion et l'accès aux machines virtuelles JIT et implémenter l'isolation réseau pour AKS.
• Renforcer la sécurité des clusters AKS, monitorer Azure Container Instances et Azure Container Apps et gérer l'accès à Azure Container Registry.
• Implémenter des méthodes de chiffrement de disque comme ADE et gérer l'accès aux API en toute sécurité dans Gestion des API Azure.

Planifier et implémenter la sécurité pour le stockage

• Développer des stratégies de sécurité pour des ressources de stockage Azure, ce qui permet une protection des données pendant le repos et le transit.
• Gérer l'accès au compte de stockage avec un contrôle d'accès efficace et une gestion de cycle de vie sécurisée des clés.
• Adapter des méthodes d'accès pour Azure Files, Stockage Blob, Tables et Files d'attente à des cas d'usage spécifiques.
• Renforcer la sécurité des données avec la suppression réversible, les sauvegardes, le contrôle de version, le stockage immuable, BYOK et le chiffrement double.

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

• Implémenter la sécurité pour Azure SQL Managed Instance afin de protéger les données sensibles.
• Utiliser Microsoft Enterprise Identity pour l'authentification de base de données et réaliser un audit de base de données à des fins de conformité.
• Utiliser Microsoft Purview pour la gouvernance et la classification des données afin de protéger les informations sensibles.
• Appliquer le masquage dynamique et le chiffrement TDE (Transparent Data Encryption), et recommander Always Encrypted pour la protection des données côté client.

Implémenter et gérer l'application des stratégies de gouvernance cloud

• Appliquer la conformité à l'aide d'Azure Policy pour créer et gérer des stratégies de sécurité.
• Simplifier le déploiement d'infrastructure sécurisée avec Azure Blueprint.
• Utiliser des zones d'atterrissage pour une sécurité Azure cohérente et gérer les données sensibles avec Azure Key Vault.

Gérer la posture de sécurité à l'aide de Microsoft Defender pour cloud

• Utiliser Microsoft Defender pour le degré de sécurité cloud et l'inventaire pour identifier et atténuer les risques de sécurité, ce qui améliore la posture globale de sécurité.
• Évaluer et aligner-les avec les frameworks de sécurité à l'aide de Microsoft Defender pour Cloud pour garantir l'adhésion aux normes de sécurité et aux meilleures pratiques.
• Intégrer des normes sectorielles et réglementaires spécifiques à Microsoft Defender pour cloud pour la conformité adaptée.
• Connecter des environnements hybrides et multiclouds à Microsoft Defender pour cloud pour la gestion centralisée de la sécurité et surveiller les ressources externes pour les protéger contre les menaces externes.

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

• Maîtriser la configuration de Microsoft Defender pour cloud pour surveiller et protéger efficacement les ressources cloud.

03 20 61 95 06
formation@access-it.fr

Formation Microsoft Azure AZ-500 Technologies de sécurité

Durée de la formation : 4 jour(s) / 28 heure(s)

• Implémenter des stratégies avancées de détection des menaces à l'aide des fonctionnalités intégrées de Microsoft Defender pour cloud.
• Utiliser le renseignement sur les menaces de Microsoft Defender pour cloud pour identifier et atténuer de manière proactive les risques de sécurité.
• Configurer et régler les stratégies de sécurité au sein de Microsoft Defender pour Cloud afin qu'elles s'alignent sur les exigences de sécurité de l'organisation.

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

• Utiliser Azure Monitor pour une surveillance efficace des événements de sécurité dans les environnements cloud.
• Implémenter des connecteurs de données dans Microsoft Sentinel pour une collecte complète des données de sécurité.
• Développer des règles d'analytique personnalisées dans Microsoft Sentinel pour la détection ciblée des menaces.
• Évaluer et automatiser les réponses aux incidents de sécurité dans Microsoft Sentinel pour améliorer l'efficacité du flux de travail.

03 20 61 95 06
formation@access-it.fr

Formation Microsoft Azure AZ-500 Technologies de sécurité

Durée de la formation : 4 jour(s) / 28 heure(s)

Prise en compte du handicap
Pour les personnes en situation de handicap, afin de nous permettre d'organiser le déroulement de la formation dans les meilleures conditions possibles, contactez-nous via notre formulaire de contact ou par mail (formation@access-it.fr) ou par téléphone (0320619506). Un entretien avec notre référente handicap pourra être programmé afin d'identifier les besoins et aménagements nécessaires.

Modalités et moyens Pédagogiques, techniques et d'encadrement mis en œuvre
Répartition théorie/pratique : 45%/55%. Cette formation se compose d'une alternance d'apports théoriques, de travaux pratiques s'articulant autour d'une application fil rouge, de démonstrations, de phases d'échanges entre participants et de synthèses de la part du formateur.
Formation accessible à distance de n'importe où et n'importe quand, via un ordinateur type PC disposant d'une connexion à Internet à haut débit (ADSL ou plus).
Pour assurer un démarrage dans les meilleures conditions au premier jour de la formation, notre service logistique se met systématiquement en relation, en amont, avec vous afin de réaliser un test de validation technique et de vous présenter l'environnement de formation.
Pendant toute la durée de la formation, le stagiaire dispose d'une assistance technique et pédagogique illimitée, par e-mail, avec un délai de prise en compte et de traitement qui n'excède pas 24h. En complément, le stagiaire peut planifier un rendez-vous pédagogique avec un formateur expert afin d'échanger sur des éléments de la formation.
La durée de la formation affichée sur cette page est une durée estimée qui peut varier en fonction du profil du stagiaire et de ses objectifs (notamment s'il souhaite valider sa formation par le passage d'un examen de certification).
Durant la formation, le formateur prévoit :
Des démonstrations organisées en modules et en séquences découpées le plus finement possible, en suivant le programme pédagogique détaillé sur cette page ;
Des énoncés et corrigés de travaux pratiques à réaliser tout au long de la formation ;
Des travaux pratiques sont proposés ; la plateforme prévoit l'environnement technique nécessaire à la réalisation de l'ensemble des travaux pratiques ;
Le formateur valide les connaissances acquises après chaque TP ;
Il est proposé un ou plusieurs livres numériques faisant office d'ouvrage(s) de référence sur le thème de la formation.

Validation et sanction de la formation
Une attestation mentionnant les objectifs, la nature et la durée de l'action et les résultats de l'évaluation des acquis de la formation sera remise au stagiaire à l'issue de sa formation par courrier électronique.
A la demande, il sera délivré un certificat de réalisation.

Type de formation
Professionnalisante ayant pour objectif le perfectionnement, l'élargissement des compétences

Moyens permettant de suivre l'exécution de l'action
Le contrôle de la présence des stagiaires sera assuré par la vérification de l'assiduité des participants. Le stagiaire signera une feuille de présence par demi-journée de formation. Celle-ci sera également signée par le formateur.

Modalité d'évaluation des acquis
Durant la formation, le participant est amené à mettre en pratique les éléments du cours par la réalisation de travaux pratiques réalisés sur PC.
La validation des acquis du stagiaire est faite par le formateur à la fin de chaque atelier. Cette validation individuelle est possible du fait du faible nombre de participants par session de formation (6 personnes maximum).
A la fin de la formation, le stagiaire a donc atteint les objectifs fixés par la formation.
En complément, pour les stagiaires qui le souhaitent, certaines formations peuvent être validées officiellement par l'éditeur en passant un examen de certification.
Access it étant centre d'examen ENI, les examens peuvent être réalisés sur demande à distance ou dans nos locaux de Villeneuve d'Ascq.
Les candidats à la certification doivent produire un travail personnel important en vue de se présenter au passage de l'examen, le seul suivi de la formation ne constitue pas un élément suffisant pour garantir un bon résultat et/ou l'obtention de la certification

Assistance Post-Formation
Toute personne ayant suivi une formation avec Access it bénéficie d'une assistance post-formation d'une durée de 1 mois. Ce nouveau service d'accompagnement permet aux stagiaires rencontrant des difficultés dans la mise en oeuvre des connaissances acquises de solliciter l'aide de nos formateurs sur des aspects relatifs aux programmes de formation suivis. Pour en bénéficier, il suffit de se rendre sur la page contact de notre site web et de remplir le formulaire. Une réponse est apportée par mail ou par téléphone dans un délai de 48 heures.

Centre d'Examen
Notre centre de formation agréé Qualiopi bénéficie de l'agrément d'ENI et ICDL pour les certifications informatiques. C'est pour nos clients la garantie de pouvoir suivre des formations préparant à des certifications professionnelles.

Aide à l'orientation
Pour chacune des grandes thématiques couvertes par notre offre de formation, nous proposons via nos spécialistes un rendez-vous physique ou téléphonique qui via un diagnostic permettra aux personnes souhaitant être accompagnées dans le choix d'un programme ou dans la définition d'un parcours de formation une orientation vers les programmes les plus adaptés à leurs besoins et à leur niveau.

Aspects Pratiques
Dès leur inscription, les participants sont contactés par nos services qui s'assurent que les débits internet constatés sur le lieu depuis lequel ils souhaitent se former sont suffisants pour suivre la formation dans des conditions optimales.
À l'occasion de cet appel, nos experts s'assurent également qu'ils disposent du matériel nécessaire pour suivre la formation (PC Portable, webcam, Micro-casque..).
Avant le début de la formation, les participants reçoivent un lien leur permettant d'accéder à la classe virtuelle et leurs identifiants personnels de connexion. Un aide à l'utilisation de la solution de visioconférence utilisée leur est également proposée.
Le jour de la formation, ils se connectent à la classe virtuelle depuis leur navigateur internet. Ils voient et entendent le formateur ainsi que les autres participants et peuvent à tout moment communiquer avec eux.
Ils participent aux échanges et réalisent les ateliers dans les mêmes conditions que s'ils étaient en salle. Grâce à nos outils de prise en main à distance, les formateurs peuvent à tout moment prendre la main sur leurs postes pour les aider ou vérifier leurs TP.
Tout au long de la formation, les participants peuvent bénéficier de l'assistance immédiate de nos experts en composant le numéro qui leur a été communiqué avant la formation.
Des bilans intermédiaires ont lieu en présence des participants du formateur et du référent pédagogique d'Access it afin de vérifier l'état d'avancement de la session, les difficultés rencontrées et permettre d'éventuels actions correctives.

Bénéfices pour les participants
Se former depuis leur lieu de travail ou leur domicile,
Accéder sans se déplacer à la qualité d'une formation délivrée par un formateur consultant ayant une expérience probante sur le sujet animé.
Bénéficier à distance de la richesse d'une formation interentreprises : échanges avec le formateur et les autres participants, partages d'expériences, ateliers pratiques…
Pouvoir se former en toutes circonstances et notamment en cas d'imprévus.

Bénéfices pour l'entreprise
Optimiser ses budgets en limitant les frais de déplacement et d'hébergement.
Proposer à tous ses collaborateurs, quelle que soit leur situation géographique, des formations de qualité (en Inter comme en Intra).
Limiter les temps de déplacement.
Proposer davantage de choix dans les formations à des collaborateurs peu mobiles.
Assurer la montée en compétences de ses collaborateurs quelles que soient les circonstances