Présentiel/distanciel | Cours Officiel | Formation certifiante

Concevoir et mettre en oeuvre des solutions réseau Microsoft Azure

Objectifs pédagogiques

- Concevoir et implémenter une infrastructure réseau principale dans Microsoft Azure
- Mettre en oeuvre des solutions de connectivité hybride avec VPN, Virtual WAN et ExpressRoute
- Choisir et configurer les services Azure adaptés pour l'équilibrage de charge du trafic HTTP(S) et non-HTTP(S)
- Concevoir et déployer des services de sécurité réseau Azure, notamment NSG, Azure Firewall, Firewall Manager et WAF
- Mettre en oeuvre des solutions d'accès privé aux services Azure avec les points de terminaison de service, Private Link et Private Endpoints
- Superviser, diagnostiquer et dépanner les environnements réseau Azure avec Azure Monitor et Network Watcher

Prérequis

- Expérience en mise en réseau d'entreprise, infrastructure locale ou cloud, et sécurité réseau
- Compréhension des technologies de virtualisation locales, notamment la mise en réseau virtuelle et les machines virtuelles
- Compréhension des configurations réseau, notamment TCP/IP, DNS, pare-feu et technologies de chiffrement
- Compréhension des méthodes de connectivité réseau hybride, notamment les VPN
- Compréhension de la résilience et de la reprise d'activité, y compris la haute disponibilité et les opérations de restauration liées au réseau
- Idéalement, avoir suivi la formation Administrateur Microsoft Azure : gérer et administrer des environnements cloud

Certification

Cette formation prépare à l'examen**AZ-700**, qui permet d'obtenir la certification Microsoft Certified: Azure Network Engineer Associate

Public concerné

Cette formation s'adresse aux ingénieurs réseau Azure qui réalisent des tâches de mise en réseau dans leur activité quotidienne et souhaitent concevoir, implémenter et gérer des solutions réseau dans Microsoft Azure. Elle concerne les professionnels chargés de créer et configurer des infrastructures réseau, d'optimiser les performances, la résilience, l'évolutivité et la sécurité, ainsi que de superviser les environnements réseau pour identifier et résoudre les problèmes de connectivité.

Bénéfices pour les participants :

- Acquérir une vision structurée des services réseau Azure et de leurs cas d'usage
- Savoir choisir les composants de connectivité, de sécurité, d'équilibrage et d'accès privé adaptés
- Renforcer la capacité à concevoir des architectures réseau Azure robustes, sécurisées et supervisées
- Préparer efficacement la certification Azure Network Engineer Associate

Programme détaillé

Présentation des réseaux virtuels Azure (3h00)

- Concevoir et mettre en oeuvre un adressage IP pour des ressources Azure
- Concevoir et mettre en oeuvre la résolution de noms
- Concevoir et mettre en oeuvre la connectivité et le routage de réseau virtuel
- Réseaux virtuels, sous-réseaux et adressage IP
- Azure DNS, zones publiques, zones privées et DNS Private Resolver
- Routes système, routes définies par l'utilisateur, appairage, Route Server, Virtual Network Manager et NAT Gateway
- Travail pratique :
  - Concevoir et mettre en oeuvre un réseau virtuel dans Azure
  - Configurer des paramètres DNS dans Azure
  - Connecter deux réseaux virtuels Azure à l'aide de l'appairage de réseaux virtuels globaux

Concevoir et mettre en oeuvre un réseau hybride (3h00)

- Concevoir et mettre en oeuvre des passerelles VPN
- Concevoir et mettre en oeuvre une architecture Azure Virtual WAN
- Topologies VPN site à site, point à site et réseau virtuel à réseau virtuel
- Tunneling forcé, haute disponibilité, routage de hub virtuel et hubs sécurisés
- Travail pratique :
  - Créer et configurer une passerelle de réseau virtuel
  - Créer un Virtual WAN à l'aide du portail Azure

Concevoir et mettre en oeuvre Azure ExpressRoute (2h00)

- Qu'est-ce qu'Azure ExpressRoute
- Sélectionner un modèle de connectivité pour ExpressRoute
- Comparer l'appairage privé et l'appairage Microsoft
- Présentation d'ExpressRoute Global Reach
- Qu'est-ce qu'ExpressRoute FastPath
- Sélectionner un modèle de résilience ExpressRoute
- Résoudre les problèmes d'ExpressRoute
- Comparer les passerelles VPN à ExpressRoute
- Travail pratique :
  - Configurer un circuit ExpressRoute
  - Approvisionner un circuit ExpressRoute

Équilibrage de charge du trafic non-HTTP(S) dans Azure (2h30)

- Concevoir et mettre en oeuvre Azure Load Balancer
- Concevoir et mettre en oeuvre Azure Traffic Manager
- Niveaux d'équilibrage, règles, sondes d'intégrité et Gateway Load Balancer
- Traffic Manager, méthodes de routage, récupération d'urgence et détection des pannes
- Travail pratique :
  - Créer et configurer un équilibreur de charge Azure
  - Créer un profil Traffic Manager

Équilibrage de charge du trafic HTTP(S) dans Azure (2h30)

- Concevoir et mettre en oeuvre Azure Application Gateway
- Concevoir et mettre en oeuvre Azure Front Door
- Routage basé sur le chemin, routage multisite, écouteurs, certificats, redirection et jeux de réécriture
- Origines, groupes d'origines, règles de routage, redirection, sondes d'intégrité et comparaison Application Gateway / Front Door
- Travail pratique :
  - Déployer Azure Application Gateway
  - Créer une instance Front Door

Conception et mise en oeuvre de la sécurité réseau (3h00)

- Mettre en oeuvre une sécurité réseau Azure
- Mettre en oeuvre et gérer des groupes de sécurité réseau
- Concevoir et mettre en oeuvre Pare-feu Azure et Azure Firewall Manager
- Concevoir et mettre en oeuvre un déploiement de pare-feu d'applications web
- Microsoft Defender for Cloud, protection DDoS, groupes de sécurité d'applications, hub-and-spoke, traitement des règles Azure Firewall et WAF
- Travail pratique :
  - Configurer la protection DDoS sur un réseau virtuel
  - Déployer et configurer le Pare-feu Azure à l'aide du portail Azure
  - Sécuriser votre hub virtuel avec Azure Firewall Manager

Concevoir et mettre en oeuvre un accès privé aux services Azure (2h00)

- Concevoir et mettre en oeuvre des points de terminaison de service
- Concevoir et mettre en oeuvre le service Azure Private Link et des points de terminaison privés Azure
- Points de terminaison de service, stratégies de points de terminaison de service, Private Link, Private Endpoint et service Private Link
- Comparaison entre points de terminaison privés et points de terminaison de service
- Travail pratique :
  - Restreindre l'accès réseau aux ressources PaaS avec des points de terminaison de service de réseau virtuel
  - Restreindre l'accès réseau aux services PaaS

Concevoir et mettre en oeuvre la supervision réseau (3h00)

- Surveiller les réseaux avec Azure Monitor
- Dépanner et analyser votre réseau avec Network Watcher
- Metrics Explorer, Network Insights, journaux de flux, analyse du trafic, topologie, moniteur de connexion, capture de paquets, vérification des flux IP et résolution des problèmes VPN
- Travail pratique :
  - Surveiller une ressource d'équilibre de charge

Délais d'accès à la formation

Les inscriptions sont possibles jusqu'à 48 heures avant le début de la formation.
Dans le cas d'une formation financée par le CPF, ENI Service est tenu de respecter un délai minimum obligatoire de 11 jours ouvrés entre la date d'envoi de sa proposition et la date de début de la formation.

Modalités et moyens pédagogiques, techniques et d'encadrement

Formation avec un formateur, qui peut être suivie selon l'une des 3 modalités ci-dessous :
1 Dans la salle de cours en présence du formateur.
2 Dans l'une de nos salles de cours immersives, avec le formateur présent physiquement à distance. Les salles immersives sont équipées d'un système de visio-conférence HD et complétées par des outils pédagogiques qui garantissent le même niveau de qualité.
3 Depuis votre domicile ou votre entreprise. Vous rejoignez un environnement de formation en ligne, à l'aide de votre ordinateur, tout en étant éloigné physiquement du formateur et des autres participants. Vous êtes en totale immersion avec le groupe et participez à la formation dans les mêmes conditions que le présentiel. Pour plus d'informations : Le téléprésentiel notre solution de formation à distance.

Le nombre de stagiaires peut varier de 1 à 12 personnes (5 à 6 personnes en moyenne), ce qui facilite le suivi permanent et la proximité avec chaque stagiaire.
Chaque stagiaire dispose d'un poste de travail adapté aux besoins de la formation, d'un support de cours et/ou un manuel de référence au format numérique ou papier.
Pour une meilleure assimilation, le formateur alterne tout au long de la journée les exposés théoriques, les démonstrations et la mise en pratique au travers d'exercices et de cas concrets réalisés seul ou en groupe.

Modalités d'évaluation des acquis

En début et en fin de formation, les stagiaires réalisent une auto-évaluation de leurs connaissances et compétences en lien avec les objectifs de la formation. L'écart entre les deux évaluations permet ainsi de mesurer leurs acquis.
En complément, le formateur évalue chaque stagiaire sur l'atteinte des objectifs pédagogiques de la formation selon quatre niveaux (non évalué, non acquis, en cours d'acquisition, acquis). Cette évaluation repose sur une modalité choisie par le formateur en cohérence avec la formation : QCM, exercices pratiques réalisés pendant la formation, évaluation finale de synthèse, quiz interactif de validation, étude de cas, mise en situation, analyse de l'auto-évaluation, autres modalités adaptées.
Pour les stagiaires qui le souhaitent, certaines formations peuvent être validées officiellement par un examen de certification. 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.
Pour certaines formations certifiantes, le passage de l'examen de certification est inclus et réalisé en fin de formation. Les candidats sont alors préparés par le formateur au passage de l'examen tout au long de la formation.

Moyens de suivi d'exécution et appréciation des résultats

Feuille de présence, émargée par demi-journée par chaque stagiaire et le formateur.
Evaluation qualitative de fin de formation, qui est ensuite analysée par l'équipe pédagogique ENI.
Attestation de fin de formation, remise au stagiaire en main propre ou par courrier électronique.

Qualification du formateur

La formation est animée par un professionnel de l'informatique et de la pédagogie, dont les compétences techniques, professionnelles et pédagogiques ont été validées par des certifications et/ou testées et approuvées par les éditeurs et/ou notre équipe pédagogique.
Il est en veille technologique permanente et possède plusieurs années d'expérience sur les produits, technologies et méthodes enseignés.
Il est présent auprès des stagiaires pendant toute la durée de la formation.

Accessibilité de la formation