Design and Implement Microsoft Azure Networking Solutions (AZ-700)

Durée: 3 Jours **Réf de cours: M-AZ700** **Méthodes d'apprentissage: Intra-entreprise & sur-mesure**

Résumé:

Apprenez à concevoir et à mettre en œuvre une infrastructure réseau sécurisée et fiable dans Azure, ainsi qu'à établir une connectivité hybride, un routage, un accès privé aux services Azure et une surveillance dans Azure.
Ce cours présente aux ingénieurs réseau comment concevoir, mettre en œuvre et maintenir des solutions réseau Azure.
Ce cours couvre le processus de conception, de mise en œuvre et de gestion de l'infrastructure réseau Azure de base, des connexions réseau hybrides, de l'équilibrage de charge du trafic, du routage réseau, de l'accès privé aux services Azure, de la sécurité réseau et de la surveillance.
Mis à jour 25/08/2025

Formation intra-entreprise

Cette formation est délivrable en session intra-entreprise, dans vos locaux ou dans les nôtres. Son contenu peut être adapté sur-mesure pour répondre aux besoins de vos collaborateurs. Contactez votre conseiller formation Global Knowledge ou adressez votre demande à info@globalknowledge.fr.

Public visé:

Ce cours s'adresse aux ingénieurs réseau qui souhaitent se spécialiser dans les solutions réseau Azure.
Un ingénieur réseau Azure conçoit et met en œuvre l'infrastructure réseau Azure de base, les connexions réseau hybrides, l'équilibrage de charge du trafic, le routage réseau, l'accès privé aux services Azure, la sécurité réseau et la surveillance. L'ingénieur réseau Azure gère les solutions réseau afin d'optimiser les performances, la résilience, l'évolutivité et la sécurité.

Objectifs pédagogiques:

- À l'issue de cette formation, les participants devraient être capables de :
- Mettre en œuvre des réseaux virtuels.
- Configurer des services IP publics.
- Concevoir et mettre en œuvre la résolution de noms.
- Concevoir et mettre en œuvre la connectivité inter-VNET.
- Mettre en œuvre le routage de réseau virtuel.
- Concevoir et mettre en œuvre :
- Un NAT Azure Virtual Network.
- Une connexion VPN site à site.
- Une connexion VPN point à site.
- L'authentification pour les connexions VPN point à site
- Azure Virtual WAN
- ExpressRoute
- ExpressRoute Global Reach
- ExpressRoute FastPath
- Mettre en œuvre Azure Front Door
- Obtenir des recommandations en matière de sécurité réseau avec Microsoft Defender pour le cloud
- Déployer Azure DDoS Protection à l'aide du portail Azure
- Concevoir et implémenter :
- Groupes de sécurité réseau (NSG)
- Azure Firewall
- Un pare-feu d'application web (WAF) sur Azure Front Door
- Expliquer les points de terminaison du service de réseau virtuel
- Définir le service Private Link et les points de terminaison privés
- Intégrer les points de terminaison privés avec DNS
- Concevoir et configurer :
- Points de terminaison privés
- Accès aux points de terminaison de service
- Intégrer un service d'application aux réseaux virtuels Azure
- Configurer les alertes d'intégrité du réseau et le log à l'aide d'Azure Monitor

- Dépanner les problèmes de connexion ExpressRoute
- Identifier les fonctionnalités et capacités d'Azure Load Balancer
- Concevoir et mettre en œuvre un Azure Load Balancer
- Mettre en œuvre un profil Traffic Manager
- Concevoir et mettre en œuvre Azure Application Gateway
- Créer et configurer une instance Connection Monitor
- Configurer et utiliser Traffic Analytics
- Configurer les journaux de flux NSG
- Activer et configurer le log de diagnostic
- Configurer Azure Network Watcher

Pré-requis:

Les ingénieurs réseau Azure performants débutent dans ce poste avec une expérience dans les réseaux d'entreprise, les infrastructures sur site ou dans le cloud et la sécurité réseau.

Ils possèdent notamment une compréhension des :

- Technologies de virtualisation sur site, notamment : les machines virtuelles, les réseaux virtuels et les disques durs virtuels.
- Configurations réseau, notamment TCP/IP, le système de noms de domaine (DNS), les réseaux privés virtuels (VPN), les pare-feu et les technologies de chiffrement.
- Réseaux "software defined"
- Méthodes de connectivité réseau hybrides, telles que le VPN.
- Concepts de résilience et de reprise après sinistre, y compris la haute disponibilité et les opérations de restauration.

Test et certification

Contenu:

MODULE 1 : Introduction aux réseaux virtuels Azure

Concevoir et mettre en œuvre l'infrastructure réseau Azure de base, notamment les réseaux virtuels, les adresses IP publiques et privées, le DNS, le peering de réseaux virtuels, le routage et Azure Virtual NAT.

- Introduction
- Explorer les réseaux virtuels Azure
- Configurer les services IP publics
- Exercice : Concevoir et mettre en œuvre un réseau virtuel dans Azure
- Concevoir la résolution de noms pour votre réseau virtuel
- Exercice : Configurer les paramètres des serveurs de noms de domaine dans Azure
- Activer la connectivité entre réseaux virtuels grâce au peering
- Exercice : Connecter deux réseaux virtuels Azure à l'aide du peering de réseaux virtuels globaux
- Mettre en œuvre le routage du trafic réseau virtuel
- Configurer l'accès Internet avec Azure Virtual NAT

MODULE 2 : Concevoir et mettre en œuvre un réseau hybride

Concevoir et mettre en œuvre des solutions de réseau hybride telles que les connexions VPN site à site, les connexions VPN point à site, Azure Virtual WAN et les hubs Virtual WAN.

- Introduction
- Concevoir et mettre en œuvre Azure VPN Gateway
- Exercice : créer et configurer une passerelle réseau virtuelle
- Connecter des réseaux à l'aide de connexions VPN site à site
- Connecter des appareils à des réseaux à l'aide de connexions VPN point à site
- Connecter des ressources distantes à l'aide d'Azure Virtual WAN
- Exercice : créer un réseau WAN virtuel à l'aide du portail Azure
- Créer un Network Virtual Appliance (NVA) dans un hub virtuel

MODULE 3 : Concevoir et mettre en œuvre Azure ExpressRoute

- Introduction
- Découvrir Azure ExpressRoute
- Concevoir un déploiement ExpressRoute
- Exercice : configurer une passerelle ExpressRoute
- Exercice : provisionner un circuit

Découvrir les différentes options d'équilibrage de charge dans Azure et apprendre à choisir et à mettre en œuvre la solution Azure adaptée au trafic non HTTP(S).

- Introduction
- Découvrir l'équilibrage de charge
- Concevoir et implémenter un équilibreur de charge Azure à l'aide du portail Azure
- Exercice : créer et configurer un équilibreur de charge Azure
- Découvrir Azure Traffic Manager
- Exercice : créer un profil Traffic Manager à l'aide du portail Azure

MODULE 5 : Équilibrer la charge du trafic HTTP(S) dans Azure

Concevoir des solutions d'équilibrage de charge pour le trafic HTTP(S) et implémenter Azure Application Gateway et Azure Front Door.

- Introduction
- Concevoir Azure Application Gateway
- Configurer Azure Application Gateway
- Exercice : déployer Azure Application Gateway
- Concevoir et configurer Azure Front Door
- Exercice : créer un Front Door pour une application web hautement disponible

MODULE 6 : Concevoir et mettre en œuvre la sécurité réseau

Apprendre à concevoir et à mettre en œuvre des solutions de sécurité réseau telles qu'Azure DDoS, les groupes de sécurité réseau, Azure Firewall et Web Application Firewall.

- Introduction
- Obtenir des recommandations sur la sécurité réseau avec Microsoft Defender pour le cloud
- Déployer Azure DDoS Protection à l'aide du portail Azure
- Exercice : configurer DDoS Protection sur un réseau virtuel à l'aide du portail Azure
- Déployer des groupes de sécurité réseau à l'aide du portail Azure
- Concevoir et mettre en œuvre Azure Firewall
- Exercice : déployer et configurer Azure Firewall à l'aide du portail Azure
- Sécuriser les réseaux avec Azure Firewall Manager
- Exercice : sécuriser un hub virtuel à l'aide d'Azure Firewall Manager.
- Mettre en œuvre un pare-feu

Concevoir et à mettre en œuvre un accès privé aux services Azure à l'aide d'Azure Private Link et des points de terminaison de service de réseau virtuel.

- Introduction
- Expliquer les points de terminaison de service de réseau virtuel
- Définir le service Private Link et le point de terminaison privé
- Intégrer le point de terminaison privé au DNS
- Exercice : restreindre l'accès réseau aux ressources PaaS avec des points de terminaison de service de réseau virtuel à l'aide du portail Azure
- Exercice : créer un point de terminaison privé Azure à l'aide d'Azure PowerShell

MODULE 8 : Concevoir et mettre en œuvre la surveillance du réseau

Concevoir et à mettre en œuvre des solutions de surveillance du réseau telles qu'Azure Monitor et Network Watcher.

- Introduction
- Surveiller les réseaux à l'aide d'Azure Monitor
- Exercice : surveiller une ressource d'équilibrage de charge à l'aide d'Azure Monitor
- Surveiller les réseaux à l'aide d'Azure Network Watcher

Résumé et ressources

ExpressRoute
- Configurer le peering pour un déploiement ExpressRoute
- Connecter un circuit ExpressRoute à un réseau virtuel
- Connecter des réseaux géographiquement dispersés grâce à la portée mondiale d'ExpressRoute
- Améliorer les performances de l'accès aux données entre les réseaux avec ExpressRoute FastPath
- Dépanner les problèmes de connexion ExpressRoute

MODULE 4 : Équilibrage de charge du trafic non HTTP(S) dans Azure

d'application web sur Azure Front Door.

MODULE 7 : Concevoir et mettre en œuvre un accès privé aux services Azure

Méthodes pédagogiques :

Un support de cours officiel sera fourni aux participants.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement