Durée :	3 jours soit 21 heures	Référence :	AZ-700T00

Public visé :

Cette formation est destinée aux **ingénieurs réseau Azure** qui souhaitent apprendre à **concevoir, mettre en œuvre et gérer des solutions de mise en réseau dans Microsoft Azure**, incluant la connectivité hybride, la sécurité réseau, le routage, l'accès privé aux services Azure et la supervision.

Public cible

- Ingénieurs réseau Azure
- Administrateurs réseau
- Architectes de solutions cloud
- Professionnels IT spécialisés dans les infrastructures réseau hybrides et cloud

Pré-requis :

Les stagiaires doivent avoir :

- Une **expérience en mise en réseau** : adressage IP, DNS, routage
- Une **connaissance des méthodes de connectivité** : VPN, WAN
- Une **maîtrise du portail Azure** et des outils comme **Azure PowerShell**
- Une compréhension des concepts de sécurité réseau, de virtualisation et de connectivité hybride

Objectifs pédagogiques :

À l'issue de la formation, les participants seront capables de :

- **Concevoir** et **implémenter** des réseaux virtuels Azure (VNet, peering, NAT, DNS).
- **Mettre en œuvre** des solutions de connectivité hybride (VPN, Azure Virtual WAN, ExpressRoute).
- **Configurer** des solutions de répartition de charge pour trafic HTTP(S) et non-HTTP(S).
- **Déployer** des solutions de sécurité réseau (NSG, Azure Firewall, DDoS Protection, WAF).
- **Implémenter** l'accès privé aux services Azure (Private Link, service endpoints).
- **Superviser** les infrastructures réseau avec Azure Monitor et Network Watcher.

Compétences acquises à l'issue de la formation :

- Configurer des réseaux virtuels Azure avec des adresses IP, DNS et peering.
- Implémenter des connexions hybrides sécurisées entre Azure et les environnements locaux.
- Déployer des solutions de répartition de charge adaptées aux différents types de trafic.
- Appliquer des stratégies de sécurité réseau avec NSG, Azure Firewall et DDoS Protection.
- Mettre en œuvre des solutions d'accès privé aux services Azure.
- Superviser les performances et la sécurité des réseaux Azure.
- Optimiser la connectivité et la résilience des infrastructures réseau.
- Diagnostiquer les problèmes de réseau à l'aide des outils de surveillance Azure.

Modalités pédagogiques :

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises ou intra-entreprises sur mesure. La formation est animée par un(e) formateur(trice) durant toute la durée de la session et présentant une suite de modules théoriques clôturés par des ateliers pratiques validant l'acquisition des connaissances. Les ateliers peuvent être accompagnés de Quizz. L'animateur(trice) présente la partie théorique à l'aide de support de présentation, d'animation réalisée sur un environnement de démonstration. En présentiel comme en téléprésentiel, l'animateur(trice) accompagne les participants durant la réalisation des ateliers.

Note relative au programme : Les ateliers, démonstrations, travaux pratiques et scénarios présentés dans ce programme sont fournis à titre d'exemples illustratifs et ne sont pas exhaustifs. Afin de garantir une adéquation permanente avec les évolutions technologiques, le contenu pédagogique ainsi que les environnements de travaux pratiques (TP) sont susceptibles d'être adaptés, ajustés ou mis à jour au cours du temps.

Moyens et supports pédagogiques :

Cadre présentiel

Salles de formation équipées et accessibles aux personnes à mobilité réduite.

- Un poste de travail par participant
- Un support de cours numérique ou papier (au choix)
- Un bloc-notes + stylo
- Vidéoprojection
- Connexion Internet
- Accès extranet pour partage de documents et émargement électronique

Cadre téléprésentiel

Session dispensée via notre solution iClassRoom s'appuyant sur Microsoft Teams.

- Un compte Office 365 par participant
- Un poste virtuel par participant
- Un support numérique (PDF ou Web)
- Accès extranet pour partage de documents et émargement électronique

Modalités d'évaluation et de suivi :

Avant

Afin de valider le choix d'un programme de formation, une évaluation des prérequis est réalisée à l'aide d'un questionnaire en ligne ou lors d'un échange avec le formateur(trice), qui valide la base de connaissances nécessaires.

Les stagiaires disposent également, depuis leur extranet, d'un **outil d'auto-positionnement** leur permettant d'évaluer leur niveau de maîtrise des compétences visées par la formation. Cette auto-évaluation est réalisée avant le démarrage de la formation à l'aide d'un curseur de positionnement allant du niveau le plus faible au niveau le plus élevé.

Pendant

Après chaque module théorique, un ou plusieurs ateliers pratiques permettent de valider progressivement l'acquisition des connaissances. Un quiz peut accompagner les ateliers pratiques afin de mesurer la compréhension des notions abordées.

Après

À l'issue de la formation, les stagiaires réalisent une nouvelle **auto-évaluation** sur les mêmes compétences que celles évaluées avant la formation. Cette comparaison permet de mesurer leur perception de la progression réalisée et de visualiser les compétences développées au cours de la formation.

Lorsque le programme de formation le prévoit, un examen de certification est organisé conformément aux modalités définies par l'éditeur ou le centre de certification (TOSA, Pearson VUE, ENI, PeopleCert…).

Le formateur réalise également une **évaluation individuelle des compétences** de chaque stagiaire sur l'ensemble des compétences visées par la formation. Pour chacune d'elles, il indique si la compétence est :

- Acquise ;
- En cours d'acquisition ;
- Non acquise.

Lorsque la compétence est évaluée comme **en cours d'acquisition** ou **non acquise**, le formateur formule des observations précisant les difficultés rencontrées ainsi que les actions ou recommandations permettant au stagiaire de poursuivre sa montée en compétences.

Enfin

Un questionnaire de satisfaction permet au participant d'évaluer la qualité de la prestation de formation.

Informations sur l'accessibilité :

Nos formations sont, dans la mesure du possible, conçues pour être accessibles à toutes et à tous. Afin de garantir les meilleures conditions d'accueil et d'apprentissage pour les personnes en situation de handicap, nous vous invitons à contacter notre référente handicap certifiée :
Céline SOLATGES – 05 61 34 39 80 – csolatges@iform.fr

Nous vous remercions de bien vouloir nous communiquer toute information utile à ce sujet en amont de la formation, afin de mettre en place les adaptations nécessaires et d'assurer un accompagnement optimal.
Pour en savoir plus sur les dispositifs d'accompagnement existants, vous pouvez consulter les sites suivants :

- AGEFIPH
- FIPHFP
- MDPH de votre département

Description / Contenu

Ce cours enseigne aux Network Engineers comment concevoir, implémenter et gérer des solutions de mise en réseau Azure. Ce cours aborde le processus de conception, d'implémentation et de gestion de l'infrastructure réseau principale d'Azure, les connexions réseau hybrides, le trafic d'équilibrage de charge, le routage réseau, l'accès privé aux services Azure, la sécurité réseau et l'analyse. Apprenez à concevoir et à implémenter une infrastructure réseau sécurisée et fiable dans Azure et à établir une connectivité hybride, un routage et un accès privé aux services Azure, ainsi qu'un monitoring dans Azure.

Module 1 : Introduction aux réseaux virtuels Azure

- Découvrir les réseaux virtuels Azure
- Configurer des services IP publics
- Exercice : Conception et implémentation d'un réseau virtuel dans Azure
- Conception de 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 avec le peering
- Exercice : Connecter deux réseaux virtuels Azure à l'aide du peering de réseaux virtuels globaux
- Implémenter le routage du trafic de réseau virtuel
- Configurer l'accès à Internet avec le NAT virtuel Azure

Module 2 :Concevoir et implémenter un réseau hybride

- Concevoir et implémenter une passerelle VPN Azure
- Exercice : Créer et configurer une passerelle de réseau virtuel
- Connecter des réseaux avec des connexions VPN site à site
- Connecter des appareils à des réseaux avec des connexions VPN point à site
- Connecter des ressources distantes à l'aide d'Azure Virtual WAN
- Exercice : Créer un réseau étendu virtuel à l'aide du portail Azure
- Créer une appliance virtuelle de réseau dans un hub virtuel

Module 3 : Concevoir et implémenter Azure ExpressRoute

- Explorer Azure ExpressRoute
- Concevoir un déploiement ExpressRoute
- Exercice : Configurer une passerelle ExpressRoute
- Exercice : Configurer un circuit ExpressRoute
- Configuration du peering pour un déploiement ExpressRoute
- Concevoir un circuit ExpressRoute pour la résilience
- Connecter des réseaux dispersés géographiquement avec ExpressRoute Global Reach
- Améliorer les performances du chemin aux données entre les réseaux avec ExpressRoute FastPath
- Résoudre les problèmes de connexion ExpressRoute

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

- Explorer l'équilibrage de charge
- Concevoir et implémenter l'équilibreur de charge Azure à l'aide du portail Azure
- Exercice : Créer et configurer un équilibreur de charge Azure
- Explorez le gestionnaire de trafic Azure
- Exercice : Créer un profil Traffic Manager à l'aide du portail Azure

Module 5 : Équilibrage de charge du trafic HTTP(S) dans Azure

- Concevoir Azure Application Gateway
- Configurer Azure Application Gateway
- Exercice : déployer Azure Application Gateway
- Concevoir et configurer Azure Front Door
- Exercice : Créer une porte d'entrée pour une application web hautement disponible

Module 6 : Conception et implémentation de la sécurité réseau

- Obtenir des recommandations de sécurité réseau avec Microsoft Defender pour le cloud
- Déployer Azure DDoS Protection à l'aide du portail Azure
- Exercice : Configurer la protection DDoS sur un réseau virtuel à l'aide du portail Azure
- Déployer des groupes de sécurité réseau à l'aide du portail Azure
- Concevoir et implémenter des Pare-feu Azure
- Exercice : Déployer et configurer le Pare-feu Azure à l'aide du portail Azure
- Sécuriser vos réseaux avec Azure Firewall Manager
- Exercice : Sécuriser votre Hub virtuel avec Azure Firewall Manager
- Implémenter un Web Application Firewall

Module 7 : Concevoir et implémenter un accès privé aux services Azure

Expliquer des points de terminaison de service de réseau virtuel
Définir Private Link service et point de terminaison privé
Intégrer un point de terminaison privé à DNS (Domain Name Service)
Exercice : Restreindre l'accès réseau aux ressources PaaS avec des points de terminaison de service de réseau virtuel en utilisant le portail Azure
Exercice : Créer un point de terminaison privé Azure à l'aide d'Azure PowerShell

Module 8 : Concevoir et implémenter la supervision réseau

- Surveiller vos réseaux à l'aide de Azure Monitor
- Exercice : Surveiller une ressource d'équilibreur de charge à l'aide d'Azure Monitor
- Surveiller vos réseaux à l'aide de Azure Network Watcher