

Durée : 3 jours soit 21 heures

Référence : AZ-700T00

Public visé :

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

Pré-requis :

Pour suivre cette formation, les apprenants doivent :

- Connaître les technologies de virtualisation sur site, notamment : les machines virtuelles, les réseaux virtuels et les disques durs virtuels.
- Maîtriser les configurations réseau, y compris TCP/IP, système de noms de domaine (DNS), réseaux privés virtuels (VPN), pare-feu et technologies de cryptage.
- Connaître les réseaux définis par logiciel.
- Connaître les méthodes de connectivité réseau hybride, telles que VPN.
- Connaître la résilience et la reprise après sinistre, y compris les opérations de haute disponibilité et de restauration.

Les prérequis demandés ci-dessous, correspondent au contenu des formations "AZ-900T00 Microsoft Azure les fondamentaux" et "AZ-104T00 Configurer et gérer des réseaux virtuels pour les administrateurs Azure"

Objectifs pédagogiques :

A l'issue de la formation, les apprenants auront acquis les compétences suivantes :

- Concevoir, mettre en œuvre et gérer des connexions réseau hybrides
- Concevoir et mettre en œuvre l'infrastructure réseau Azure de base
- Concevoir et implémenter le routage et l'équilibrage de charge dans Azure
- Sécuriser et surveiller les réseaux
- Concevoir et mettre en œuvre un accès privé aux services 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.

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
- Vidéo-projection sur tableau blanc
- 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 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 validera la base de connaissances nécessaires.

Pendant

Après chaque module théorique, un ou des ateliers pratiques permettent la validation de l'acquisition des connaissances. Un Quizz peut accompagner l'atelier pratique.

Après

Un examen de certification si le programme de formation le prévoit dans les conditions de l'éditeur ou du centre de test (TOSA, Pearson Vue, ENI, PeopleCert)

Enfin

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

Description / Contenu

Module 1 : Introduction aux réseaux virtuels Azure

- Explorez les réseaux virtuels Azure

- Configurer les services IP publics
- Résolution de noms de conception pour votre réseau virtuel



- Activer la connectivité Cross-VNet avec l'appairage
- Mettre en œuvre le routage du trafic du réseau virtuel
- Configurer l'accès Internet avec Azure Virtual NAT

Ateliers :

- Concevoir et implémenter un réseau virtuel dans Azure
- Configurer les paramètres DNS dans Azure
- Connecter deux réseaux virtuels Azure à l'aide de l'appairage de réseaux virtuels mondiaux

Module 2 : Concevoir et mettre en œuvre un réseau hybride

- Concevoir et mettre en œuvre la passerelle VPN Azure
- Connecter des réseaux avec des connexions VPN de site à site
- Connecter des appareils aux réseaux avec des connexions VPN point à site
- Connecter des ressources distantes à l'aide d'Azure Virtual WAN
- Créer une appliance virtuelle réseau (NVA) dans un hub virtuel

Ateliers :

- Créer et configurer une passerelle de réseau virtuel

Module 3 : Concevoir et implémenter Azure ExpressRoute

- Explorez Azure ExpressRoute
- Concevoir un déploiement ExpressRoute
- Configurer l'appairage pour un déploiement ExpressRoute
- Connecter un circuit ExpressRoute à un réseau virtuel
- Connecter des réseaux géographiquement dispersés avec la portée mondiale d'ExpressRoute
- Améliorer les performances du chemin de données entre les réseaux avec ExpressRoute FastPath
- Résoudre les problèmes de connexion ExpressRoute

Ateliers :

- Configurer une passerelle ExpressRoute
- Provisionner un circuit ExpressRoute

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

- Découvrir l'équilibrage de charge
- Concevoir et implémenter l'équilibreur de charge Azure à l'aide du portail Azure
- Explorer Azure Traffic Manager

Ateliers :

- Créer un profil Traffic Manager à l'aide du portail Azure
- Créer et configurer un équilibreur de charge Azure

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

- Concevoir la passerelle d'application Azure
- Configurer la passerelle d'application Azure
- Concevoir et configurer la porte d'entrée Azure

Ateliers :

- Déployer la passerelle d'application Azure
- Créer une porte d'entrée pour une application web hautement disponible

Module 6 : Concevoir et mettre en œuvre la sécurité du réseau

- Sécuriser vos réseaux virtuels dans le portail Azure
- Déployer Azure DDoS Protection à l'aide du portail Azure
- Déployer des groupes de sécurité réseau à l'aide du portail Azure
- Concevoir et implémenter le pare-feu Azure
- Travailler avec Azure Firewall Manager
- Implémenter un pare-feu d'application Web sur Azure Front Door

Ateliers :

- Déployer et configurer le pare-feu Azure à l'aide du portail Azure
- Sécuriser votre hub virtuel à l'aide d'Azure Firewall Manager
- Configurer la protection DDoS sur un réseau virtuel à l'aide du portail Azure

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

- Définir le service de liaison privée et le point de terminaison privé
- Expliquer les points de terminaison de service de réseau virtuel
- Intégrer le lien privé avec DNS
- Intégrer votre App Service aux réseaux virtuels Azure

Ateliers :

- Créer un point de terminaison privé Azure à l'aide d'Azure PowerShell
- Restreindre l'accès réseau aux ressources PaaS avec des points de terminaison de service de réseau virtuel

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

- Surveillez vos réseaux avec Azure Monitor
- Surveillez vos réseaux avec Azure Network Watcher

Ateliers :

- Surveiller une ressource d'équilibreur de charge à l'aide d'Azure Monitor