Durée :	1 jour soit 7 heures	Référence :	AZ-1002

Public visé :

Cette formation est conçue pour les **professionnels IT** qui souhaitent apprendre à **configurer un accès sécurisé aux charges de travail** dans Azure à l'aide des services de **mise en réseau virtuelle**.

Public cible

- Administrateurs cloud
- Ingénieurs réseau
- Architectes de solutions Azure
- Professionnels en sécurité informatique
- Toute personne responsable de la configuration et de la sécurisation des infrastructures réseau dans Azure

Pré-requis :

- Expérience avec le portail Azure pour créer des ressources
- Connaissances de base en :
  - Mise en réseau dans le cloud
  - DNS
  - Groupes de sécurité réseau (NSG)
  - Azure Firewall

Objectifs pédagogiques :

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

- **Créer** et configurer des réseaux virtuels et des sous-réseaux dans Azure.
- **Définir** des règles de sécurité avec les groupes de sécurité réseau (NSG).
- **Configurer** des connexions de peering entre réseaux virtuels.
- **Implémenter** des solutions de sécurité avec Azure Firewall.
- **Gérer** le routage réseau et les zones DNS pour sécuriser les communications.

Compétences acquises à l'issue de la formation :

- Déployer des réseaux virtuels sécurisés dans Azure.
- Configurer des règles de sécurité réseau avec NSG et Azure Firewall.
- Administrer le routage et le peering pour optimiser la connectivité.
- Gérer les zones DNS et les enregistrements pour sécuriser les accès aux ressources.

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
- Vidéoprojection 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

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

Dans cette formation, vous allez vous entraîner à configurer l'accès sécurisé à vos charges de travail en utilisant des réseaux Azure.

Pour consulter le contenu officiel de cette formation éditeur, cliquez sur le lien ci-dessous :
https://learn.microsoft.com/fr-fr/training/paths/configure-secure-workloads-using-azure-virtual-networking/