Configurer l’accès sécurisé à vos charges de travail en utilisant des réseaux Azure

Durée: 1 Jour **Réf de cours: M-AZ1002** **Méthodes d'apprentissage: Intra-entreprise & sur-mesure**

Résumé:

Cette formation est conçue pour les participants qui prévoient de passer l'évaluation Configure Secure Access to your Workloads using Azure Virtual Networking (APL-1002).
Il constitue une passerelle entre les compétences de niveau fondamental (Initiation) et les compétences "Associate" (niveau Débutant).
Dans ce cours, les participants auront de nombreuses occasions de pratiquer la configuration et la sécurisation des ressources réseau à travers des exercices pratiques.
Les compétences abordées comprendront la création et la configuration d'architectures réseau sécurisées, de réseaux virtuels, le routage réseau, les zones DNS, les paramètres DNS, les groupes de sécurité réseau le pare-feu Azure et les solutions de connectivité hybride.
Mis à jour 04/07/2025

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 est conçu pour les participants qui effectuent des tâches de sécurisation du réseau Azure Administrator dans leur activité professionnelle et/ou qui prévoient de passer l'évaluation "Configurer un accès sécurisé à vos charges de travail à l'aide du réseau virtuel Azure" (APL-1002)

Objectifs pédagogiques:

- A l'issue de cette formation, les participants seront en mesure de :
- Configurer les réseaux virtuels
- Configurer le peering des réseaux virtuels Azure
- Gérer et contrôler le flux de trafic dans le déploiement Azure avec des routes
- Héberger un domaine sur Azure DNS
- Configurer les groupes de sécurité réseau
- Configurer Azure Firewall

Pré-requis:

- Expérience de l'utilisation du portail Azure pour créer des ressources.
- Connaissance de base des concepts de réseaux d'entreprise et de cloud networking
- Connaissance de base des concepts de sécurité réseau tels que les pare-feu, le routage et les listes de contrôle d'accès.

Contenu:

Module 1: Configurer des réseaux virtuels

- Introduction
- Déterminer les utilisations du peering de réseau virtuel Azure
- Déterminer le transit et la connectivité de la passerelle
- Créer un peering de réseau virtuel
- Étendre le peering avec des routes définies par l'utilisateur et la chaînage de services
- Simulation

Module 2: Configurer un peering de réseaux virtuels Azure

- Déterminer les utilisations du peering de réseau virtuel Azure
- Déterminer le transit et la connectivité de la passerelle
- Créer un peering de réseau virtuel
- Étendre le peering avec des routes définies par l'utilisateur et la chaînage de services
- Simulation

Module 3: Gérer et contrôler le flux de trafic dans votre déploiement Azure à l'aide de routes

- Identifier les capacités de routage d'un réseau virtuel Azure
- Exercice – Créer des routes personnalisées
- Qu'est-ce qu'un NVA ?
- Exercice – Créer un NVA et des machines virtuelles
- Exercice – Router le trafic à travers le NVA

Module 4: Héberger votre domaine sur Azure DNS

- Qu'est-ce qu'Azure DNS ?
- Configurer Azure DNS pour héberger votre domaine
- Exercice – Créer une zone DNS et un enregistrement A en utilisant Azure DNS
- Exercice – Créer des enregistrements alias pour Azure DNS

Module 5: Configurer des groupes de sécurité réseau

- Mettre en œuvre des groupes de sécurité réseau
- Déterminer les règles des groupes de sécurité réseau
- Déterminer les règles effectives des groupes de sécurité réseau
- Créer des règles de groupe de sécurité réseau
- Mettre en œuvre des groupes de sécurité d'application
- Simulation

Module 6: Présentation du Pare-feu Azure

- Qu'est-ce qu'Azure Firewall ?
- Comment fonctionne Azure Firewall
- Quand utiliser Azure Firewall et Azure Firewall Premium

Module 7: Projet final : configurer l'accès sécurisé aux charges de travail avec les services de réseau virtuel Azure

- Exercice – Fournir une isolation et une segmentation du réseau pour l'application web
- Exercice – Contrôler le trafic réseau vers et depuis l'application web
- Exercice – Protéger l'application web contre le trafic malveillant et bloquer l'accès non autorisé
- Exercice – Opérationnaliser et appliquer des politiques pour filtrer le trafic
- Exercice – Enregistrer et résoudre les noms de domaine en interne

Méthodes pédagogiques :

Un support de cours officiel en langue anglaise 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