New

Sécuriser l'accès aux Workloads avec Azure Virtual Network

Renforcer la protection de vos services et données avec Azure Virtual Network

A distance

7 h

Prix inter : 950,00 € HT
Forfait intra : 2.850,00 € HT

Réf.: MSAZ1002

La mise en réseau virtuelle Azure est essentielle pour déployer des charges de travail sécurisées et performantes dans le cloud. Cette formation permet d'acquérir les compétences nécessaires pour configurer des réseaux virtuels, créer des sous-réseaux, gérer les groupes de sécurité réseau et configurer des tables de routage personnalisées.
Les participants apprennent également à **intégrer des services comme Azure Firewall et Azure Bastion pour renforcer la protection et contrôler finement le trafic**. Un parcours incontournable pour administrer et sécuriser efficacement des environnements Azure tout en assurant la disponibilité et la conformité des charges de travail déployées.

A qui s'adresse cette formation ?

Pour qui

- Administrateurs
- Ingénieurs réseaux

Prérequis

- Aucun.

Programme

1 - Configurer des réseaux virtuels

- Découvrir les composants et fonctionnalités d'un réseau virtuel Azure
- Identifier les fonctionnalités et la mise en oeuvre des sous-réseaux
- Comprendre les cas d'usage des adresses IP privées et publiques
- Créer un réseau virtuel et configurer une adresse IP

Atelier

Mettre en place et paramétrer des réseaux virtuels

2 - Configurer le peering de réseaux virtuels Azure

- Identifier les cas d'usage et les fonctionnalités du peering de réseaux virtuels Azure
- Configurer un réseau pour mettre en oeuvre la passerelle VPN Azure et assurer la connectivité de transit
- Étendre le peering avec une architecture hub-and-spoke, des itinéraires définis par l'utilisateur et le chaînage de services

Atelier

Implémenter la connectivité réseau intersite

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

- Identifier les fonctionnalités de routage d'un réseau virtuel Azure

- Configurer le routage au sein d'un réseau virtuel
- Déployer une appliance virtuelle réseau de base
- Mettre en place un routage pour faire transiter le trafic via une appliance virtuelle réseau
  Atelier

  Créer des routes personnalisées dans un réseau virtuel Azure

  Déployer une appliance virtuelle réseau et des machines virtuelles associées

  Configurer le routage pour faire transiter le trafic via l'appliance virtuelle réseau

4 - Héberger votre domaine sur Azure DNS

- Mettre en place l'hébergement de votre domaine avec Azure DNS
  Atelier

  Créer une zone DNS et configurer un enregistrement A dans Azure DNS

  Mettre en place des enregistrements d'alias dans Azure DNS

5 - Configurer des groupes de sécurité réseau

- Identifier les situations où utiliser des groupes de sécurité réseau (NSG)
- Créer et configurer des groupes de sécurité réseau
- Mettre en oeuvre et évaluer des règles dans un groupe de sécurité réseau
- Comprendre le rôle et les fonctionnalités des groupes de sécurité d'application (ASG)
  Atelier

  Concevoir et implémenter la mise en réseau virtuelle

6 - Présentation du Pare-feu Azure

- Comprendre le fonctionnement conjoint d'Azure Firewall et d'Azure Firewall Manager pour protéger les réseaux virtuels
- Évaluer si Azure Firewall est adapté pour sécuriser vos réseaux virtuels contre le trafic malveillant entrant et sortant
- Évaluer si Azure Firewall Premium répond à vos besoins de protection avancée contre le trafic malveillant
- Déterminer si Azure Firewall Manager est la solution appropriée pour déployer des stratégies sur plusieurs pare-feu
- Identifier et décrire les principaux cas d'usage d'Azure Firewall et d'Azure Firewall Manager

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

- Créer et configurer des réseaux virtuels
- Créer et configurer des groupes de sécurité réseau (NSG)Créer et configurer un Pare-feu Azure
- Configurer le routage réseau
- Créer des zones DNS et configurer des paramètres DNS
  Atelier

  01 – Mettre en place et configurer des réseaux virtuels

  02 – Créer et gérer des groupes de sécurité réseau (NSG)

  03 – Déployer et configurer un pare-feu Azure

  04 – Configurer et optimiser le routage réseau

  05 – Créer et administrer des zones DNS

Les objectifs de la formation

- Configurer des virtual networks, des subnets et l'IP addressing
- Mettre en oeuvre Azure Virtual Network peering et user-defined routes
- Contrôler le trafic réseau avec un network virtual appliance
- Créer des DNS zones et gérer des DNS records dans Azure DNS
- Déployer des network security groups et définir des security rules
- Créer un Azure Firewall et appliquer des firewall policies

Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- Acquisition de méthodes professionnelles pour concevoir une architecture réseau fiable et évolutive
- Exercices pratiques sur des cas concrets pour configurer sous-réseaux, pare-feu et passerelles
- Utilisation optimisée des règles de sécurité, groupes et services managés d’Azure
- Alternance entre apports théoriques et mises en application guidées dans Azure

Dates 2026 - Référence MSAZ1002

Dernières places disponibles Session garantie

le 30 janv.
- le 30 janv. 9h00 -> 17h00

le 17 mars
- le 17 mars 9h00 -> 17h00

le 13 mai
- le 13 mai 9h00 -> 17h00

le 2 juin
- le 2 juin 9h00 -> 17h00

le 18 août
- le 18 août 9h00 -> 17h00

le 4 sept.
- le 4 sept. 9h00 -> 17h00

le 6 oct.
- le 6 oct. 9h00 -> 17h00

le 13 nov.
- le 13 nov. 9h00 -> 17h00

le 1 déc.
- le 1 déc. 9h00 -> 17h00

le 23 déc.
- le 23 déc. 9h00 -> 17h00