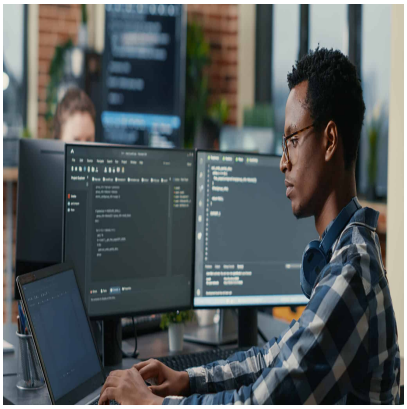

Configurer l’accès sécurisé à vos charges de travail à l’aide d’un réseau virtuel Azure (AZ-1002)

Description

Dans le monde numérique d’aujourd’hui, l’accès sécurisé et efficace aux charges de travail est essentiel. Microsoft Azure propose une plateforme cloud puissante avec des fonctionnalités complètes pour garantir que vos systèmes restent protégés tout en offrant un accès fluide. Le cours « Configurer l’accès sécurisé à vos charges de travail à l’aide d’un réseau virtuel Azure (AZ-1002) » est conçu pour vous fournir les compétences nécessaires pour gérer et optimiser les réseaux virtuels Azure afin d’assurer un accès sécurisé aux charges de travail.

Pourquoi choisir ce cours ?

Cette formation offre une approche pratique pour comprendre et mettre en œuvre des réseaux virtuels sécurisés dans Microsoft Azure. Vous apprendrez à utiliser des outils tels qu’Azure Virtual Network, Azure DNS et Azure Firewall pour créer et configurer des réseaux avec des fonctionnalités de sécurité renforcées. À la fin du cours, vous serez capable de concevoir, configurer et sécuriser des réseaux virtuels garantissant une communication fluide entre vos charges de travail.

Niveau
Intermédiaire
Contenu du cours
Module 1 : Configurer des réseaux virtuels

- Planifier des réseaux virtuels
- Créer des sous-réseaux
- Créer des réseaux virtuels
- Planifier l’adressage IP
- Créer un adressage IP public
- Associer des adresses IP publiques
- Allouer ou attribuer des adresses IP privées

Module 2 : Configurer un peering de réseaux virtuels Azure

- Déterminer les utilisations du peering de réseaux virtuels Azure

© Copyright ITTA – Tous les contenus sont protégés par le droit d’auteur.

- Déterminer le transit par passerelle et la connectivité
- Créer le peering de réseaux virtuels
- Étendre l'appairage avec des routes définies par l'utilisateur et le chaînage de services

Module 3 : Gérer le flux de trafic avec des routes

- Identifier les fonctionnalités de routage d'un réseau virtuel Azure
- Créer des routes personnalisées
- Créer une appliance virtuelle réseau
- Créer des machines virtuelles
- Faire transiter le trafic par l'appliance virtuelle réseau

Module 4 : Héberger un domaine avec Azure DNS

- Présentation d'Azure DNS
- Configurer Azure DNS pour héberger un domaine
- Créer une zone DNS et un enregistrement A
- Résoudre dynamiquement un nom de ressource en utilisant un enregistrement d'alias
- Créer des enregistrements d'alias pour Azure DNS

Module 5 : Configurer des groupes de sécurité réseau

- Implémenter des groupes de sécurité réseau
- Déterminer les règles des groupes de sécurité réseau
- Déterminer les règles de sécurité effectives
- Créer des règles pour les groupes de sécurité réseau
- Implémenter des groupes de sécurité d'applications

Module 6 : Présentation du Pare-feu Azure

- Qu'est-ce qu'un Pare-feu Azure ?
- Comprendre comment fonctionne le Pare-feu Azure
- Quand utiliser le Pare-feu Azure
- Quand utiliser le Pare-feu Azure Premium

Module 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
- Créer et configurer le Pare-feu Azure
- Configurer le routage réseau
- Créer et configurer des zones DNS

Lab / Exercices

- Ce cours vous donne un accès exclusif au laboratoire officiel Microsoft, vous permettant de mettre en pratique vos compétences dans un environnement professionnel.

Documentation

- Accès à Microsoft Learn, la plateforme d'apprentissage en ligne Microsoft, offrant des ressources interactives et des contenus pédagogiques pour approfondir vos connaissances et développer vos compétences techniques.

© Copyright ITTA – Tous les contenus sont protégés par le droit d'auteur.

Profils des participants

- Administrateurs Azure
- Ingénieurs Réseau
- Architectes de Solutions Cloud
- Professionnels IT gérant des environnements Azure
- Spécialistes en Sécurité Réseau
- Ingénieurs Systèmes intéressés par l'infrastructure cloud
- Ingénieurs DevOps travaillant avec Azure
- Consultants IT spécialisés dans les solutions de réseau Azure

Connaissances Préalables

- Compréhension des concepts réseau de base
- Notions générales sur l’administration de systèmes et infrastructures cloud

Objectifs

- Configurer des réseaux virtuels et sous-réseaux Azure
- Créer des connexions de peering entre réseaux virtuels Azure
- Gérer et contrôler le trafic avec des routes personnalisées
- Héberger un domaine sur Azure DNS
- Configurer des groupes de sécurité réseau et appliquer des règles
- Mettre en place et configurer Azure Firewall
- Configurer le routage réseau et la gestion de la sécurité via Azure Firewall Manager

Description
Configurer l’accès sécurisé à vos charges de travail à l’aide d’un réseau virtuel Azure (AZ-1002)
Prix de l'inscription en Présentiel (CHF)
900
Prix de l'inscription en Virtuel (CHF)
850
Durée (Nombre de Jours)
1
Reference
AZ-1002

© Copyright ITTA – Tous les contenus sont protégés par le droit d’auteur.