

Configurez un accès sécurisé à vos charges de travail à l'aide du réseau virtuel Azure (AZ-1002)

Durée: 1 jour

Public cible: Professionnel TI

À qui s'adresse cette formation ?

- Intermédiaire
- Administrateur
- Ingénieur réseau
- Gestionnaire de pare-feu Azure

Objectifs de la formation

À l'issue de cette formation, les participants seront en mesure de :

- Configurer des réseaux virtuels Azure (VNet) et leur segmentation (subnets, adressage IP)
- Mettre en place des connexions entre réseaux (peering) pour assurer une communication sécurisée
- Contrôler le trafic réseau à l'aide de routes personnalisées et du routage Azure
- Gérer la résolution de noms avec Azure DNS (zones DNS, enregistrements) [learn.microsoft.com]
- Sécuriser les communications en configurant des Network Security Groups (NSG) et leurs règles
- Protéger les ressources avec Azure Firewall et ses politiques de sécurité
- Mettre en œuvre un accès sécurisé aux charges de travail à travers un scénario complet (projet guidé)

Description sommaire

Les formations Applied Skills sont conçues pour valider des compétences spécifiques en étant orientées vers des scénarios réels. Elles offrent une alternative ciblée aux certifications traditionnelles basées sur des rôles, en mettant l'accent sur l'application des compétences techniques dans des situations professionnelles concrètes. Dans cet atelier de formation, vous vous entraînerez à configurer un accès sécurisé aux charges de travail à l'aide du réseau Azure.

Contenu du plan de cours

- Configurer les réseaux virtuels
- Configurer le peering de réseau virtuel Azure
- Gérez et contrôlez le flux de trafic dans votre déploiement Azure avec des itinéraires
- Hébergez votre domaine sur Azure DNS
- Configurer les groupes de sécurité réseau
- Introduction au pare-feu Azure
- Projet guidé - Configurer un accès sécurisé aux charges de travail avec les services de réseau virtuel Azure
- Découvrez les autres Applied Skills: Microsoft applied skills (afiexpertise.com)

Approche et méthode pédagogique

Approche pratique et structurée combinant théorie ciblée et ateliers guidés. Les participants configureront progressivement un accès sécurisé aux charges de travail à l'aide du réseau virtuel Azure à travers des exercices concrets inspirés de scénarios réels, favorisant une mise en application immédiate des apprentissages. Ils apprennent à concevoir des architectures réseau sécurisées, à gérer les accès et à protéger les ressources dans le cloud. Animée par un formateur certifié Microsoft, la formation privilégie l'interactivité et le développement de compétences techniques directement transférables pour sécuriser efficacement des environnements Azure en contexte professionnel.

Prérequis

Vous avez besoin d'un abonnement Azure pour effectuer ces exercices. Si vous ne disposez pas d'un abonnement Azure, créez un compte gratuit et ajoutez un abonnement avant de commencer. Si vous êtes étudiant, vous pouvez profiter de l'offre Azure pour étudiants.

Recommandations

- Bases en réseautique (IP, DNS, sous-réseaux, routage)
- Connaissance des concepts de sécurité réseau (pare-feu, segmentation, accès sécurisé)
-

Familiarité avec Microsoft Azure

- Notions de gestion des identités et des accès (Entra ID)
- Compréhension des architectures cloud