Quatrième partie : Description des fonctionnalités de sécurité générale et de sécurité réseau

- Principes de base d'Azure - Quatrième partie : Description des fonctionnalités de sécurité générale et de sécurité réseau

Dans cette quatrième partie, il y a deux modules :

- Se protéger contre les menaces de sécurité sur Azure
  - Sécuriser son infrastructure dans le Cloud : conformité des services par rapport à un niveau de sécurité minimal et protection des données contre des attaques ;
  - Protection des menaces à l'aide d'Azure Security Center ;
  - Collecter et exploiter les données de sécurité de nombreuses sources différentes à l'aide d'Azure Sentinel ;
  - Stocker des informations sensibles (mots de passe et des clés de chiffrement) de manière sécurisée dans Azure Key Vault ;
  - Gérer dans Azure des serveurs physiques dédiés hébergeant des VM Windows et Linux à l'aide d'Azure Dedicated Host.
- Sécuriser la connectivité réseau sur Azure

Le module 1 propose l'activité bac à sable **Gérer un mot de passe dans Azure Key VaultL**.

Tailwind Traders doit gérer des informations sensibles indispensables au fonctionnement d'une application telles que :

- des mots de passe ;
- des clés de chiffrement et des certificats doivent être gérées avec prudence.

Comme ces informations pourraient permettre à une personne non autorisée d'accéder aux données d'application, l'entreprise souhaite utiliser le service Azure Key Vault, service cloud centralisé conçu pour le stockage des secrets d'une application, à un emplacement central unique.

- Lien vers l'Exercice : Gérer un mot de passe dans Azure Key Vault </WRAP>

Le module 2 propose l'activité bac à sable **Configurer l'accès réseau à une machine virtuelle à l'aide d'un groupe de sécurité réseau**.

Vous aller configurez l'accès réseau à une machine virtuelle s'exécutant sur Azure :

- créer une machine virtuelle Linux et installer Nginx (serveur web) ;
- rendre accessible votre serveur web en créant une règle de groupe de sécurité réseau (NSG) qui autorise l'accès entrant sur le port 80 (HTTP).

Pour cela vous allez utiliser Azure CLI à partir d'Azure Cloud Shell afin de vous connecter à Azure et d'exécuter des commandes d'administration. Azure Cloud Shell est un interpréteur de commandes basé sur un navigateur qui permet de gérer et développer des ressources Azure. Vous pouvez considérer que Cloud Shell est une console interactive qui s'exécute dans le cloud.

Il existe de nombreuses autres façons de créer et gérer des machines virtuelles, avec le portail Azure, Azure CLI, Azure PowerShell ou un modèle Azure Resource Manager (ARM).

- Lien vers l'Exercice – Configurer l'accès réseau à une machine virtuelle à l'aide d'un groupe de sécurité réseau </WRAP>

Retour au menu Formation AZ-900

- AZ-900 : les principes de base d'Azure