Activité 2 : Maintenir l’infrastructure et contribuer à son évolution et à sa sécurisation

5 compétences types :

* Maintenir des serveurs dans une infrastructure virtualisée
* Automatiser des tâches à l’aide de scripts
* Maintenir et sécuriser les accès à Internet et les interconnexions des réseaux
* Mettre en place, assurer et tester les sauvegardes et les restaurations des éléments de l’infrastructure
* Exploiter et maintenir les services de déploiement des postes de travail

Durée : 2h

**CCP5 - Maintenir des serveurs dans une infrastructure virtualisée**

1. Qu'est-ce qu'une image Docker ?

C’est un fichier qui contient tout le nécessaire pour exécuter une application (code, bibliothèques, dépendances, configurations).

On crée un conteneur Docker à partir d’une image.

1. Sur un équipement de gestion de VM, quels sont les éléments/composants matériels importants à prendre en compte ?

* La mémoire RAM
* Le stockage disque
* Le processeur
* Éventuellement la carte réseau

1. Qu’est-ce qu’un conteneur ?

Un conteneur est un environnement isolé qui regroupe une application et ses dépendances.

1. Quels sont les avantages et les inconvénients de la conteneurisation par rapport à la virtualisation ?

Par rapport à la virtualisation, la conteneurisation est plus légère, offre un démarrage plus rapide et une meilleure utilisation des ressources. Par contre, il peut y avoir une isolation moins forte et une complexité à faire cohabiter les applications des conteneurs.

1. Voici le contenu d’un fichier :

*<VirtualBox>*

*<Machine name="Linux VM" OSType="Linux26\_64" memory="8192" bootOrder="1" >*

*<Hardware>*

*<Disk type="Normal" size="10485760"/>*

*<BIOS>*

*<ACPI enabled="true"/>*

*<IOAPIC enabled="true"/>*

*</BIOS>*

*<Network>*

*<Adapter slot="0" enabled="true" type="virtio">*

*<NAT/>*

*</Adapter>*

*</Network>*

*</Hardware>*

*</Machine>*

*</VirtualBox>*

Quel est ce fichier ?

C’est un fichier de configuration pour une VM dans Virtualbox.

Quelles informations as-tu dans ce fichier ?

Nom de la VM : "Linux VM".

Type de l’OS : "Linux26\_64" (Linux avec un noyau 2.6 en 64 bits)

Mémoire RAM allouée à cette VM : "8192" soit 8 Go

Ordre de démarrage : "1", cela indique un boot sur le disque dur numéro 1

Disque dur de type "Normal" avec une taille de "10485760" soit 10 Go

Un BIOS avec l'ACPI activé ("true") et l'IOAPIC activé ("true").

Un adaptateur réseau dans le slot "0", activé ("true") avec un contrôleur "virtio", et configuré en NAT

1. Donne deux hyperviseurs de type 1 et deux de type 2

Hyperviseurs de type 1 :

* Proxmox
* VMware ESXi

Hyperviseurs de type 2 :

* VirtualBox
* VMware Workstation

**CCP6 - Automatiser des tâches à l’aide de scripts**

1. Comment récupérer et exploiter des arguments passés à un script ? Donne un exemple dans le langage de ton choix.

En Shell bash on les récupère avec des variables $1, $2, etc.

Exemple :

On exécute le script creationUtilisateur.sh qui créer un compte utilisateur avec le nom, le prénom, et l’age de la personne.

On exécute le script avec creationUtilisateur.sh john doe 42.

Dans le script on récupère les arguments avec $1 (qui vaut dans l’exemple “john”), $2 (qui vaut “doe”), et $3 (qui vaut “42”).

1. Quels sont les moyens d’automatiser la création d’utilisateur sur un serveur Windows ? Donne des précisions.

Avec une commande PowerShell, “New-LocalUser” pour un compte local ou bien “New-ADUser” sur un domaine.

On peut ensuite mettre ça dans un script et l’exécuter automatiquement avec une tâche planifiée.

1. Quels sont les avantages d’utiliser Ansible pour automatiser la configuration d’un serveur ?

* Simplicité
* Automatisation de tâches
* Fonctionne sans agent, sans logiciel à installer sur les serveurs

1. Comment vérifier qu’un script Bash ne contient pas d’erreurs avant son exécution ?

Avec la commande “-x”.

1. Sous Windows et sous Linux, comment planifier l'exécution automatique de tâches récurrentes ?

Sous Windows on utilise le Planificateur de tâches.

Sous Linux on utilise cron.

1. Comment exécuter automatiquement un script à l’ouverture d’une session utilisateur sous Windows ?

Soit par une GPO utilisateur ou bien par un script placé dans le dossier de démarrage d’une machine.

**CCP7 - Maintenir et sécuriser les accès à Internet et les interconnexions des réseaux**

1. Pourquoi est-ce important de mettre à jour le firmware d'un équipement réseau ?

- Corriger des vulnérabilités de sécurité

- Améliorer les performances ou la stabilité de l'appareil

- Ajouter ou mettre à jour des fonctionnalités

1. Explique les lignes suivantes :

*ssh adminDebian@DebianServer*

*ssh-keygen*

*Enter file in which to save the key (/home/adminDebian/.ssh/id\_rsa):*

*Enter passphrase (empty for no passphrase):*

*cat ~/.ssh/id\_rsa.pub*

*exit*

*ssh wilder@UbuntuClient*

*mkdir ~/.ssh*

*nano ~/.ssh/authorized\_keys*

Ces lignes configurent l'authentification par clé SSH entre deux machines (un serveur DebianServer et un client UbuntuClient).

1. Le routeur R1 a 2 interfaces g0/0 et g1/0. L’interface g0/0 (45.56.12.07/16) est connectée à l'extérieur du réseau. L’interface g1/0 (172.16.15.254/24) est connectée à l'intérieur du réseau.

Sur ce routeur on trouve les ACL suivantes :

access-list 101 permit udp any host 172.16.15.10 eq 67

access-list 101 permit udp any host 172.16.15.10 eq 68

access-list 101 permit tcp any host 172.16.15.10 eq 53

access-list 101 permit udp any host 172.16.15.10 eq 53

Explique chaque ligne d’ACL.

access-list 101 permit udp any host 172.16.15.10 eq 67

=> autorise le trafic UDP de n'importe quelle source vers l'hôte 172.16.15.10 sur le port 67 (DHCP)

access-list 101 permit udp any host 172.16.15.10 eq 68

=> autorise le trafic UDP de n'importe quelle source vers l'hôte 172.16.15.10 sur le port 68 (DHCP)

access-list 101 permit tcp any host 172.16.15.10 eq 53

=> autorise le trafic TCP de n'importe quelle source vers l'hôte 172.16.15.10 sur le port 53 (DNS)

access-list 101 permit udp any host 172.16.15.10 eq 53

=> autorise le trafic UDP de n'importe quelle source vers l'hôte 172.16.15.10 sur le port 53 (DNS)

Que peux-tu déduire de la machine 172.16.15.10 ?

La machine 172.16.15.10 est un serveur DHCP et DNS.

1. Bob a une clé publique PUB-Bob et une clé privée PRI-Bob. Alice a la même chose avec PUB-Alice et PRI-Alice. Dans le système de la cryptographie asymétrique, décrit les différentes étapes d'un envoi de message de Bob vers Alice.

- Bob utilise la clé publique d’Alice PUB-Alice pour chiffrer le message et l’envoie à Alice.

- Alice reçoit le message et le déchiffre avec sa clé privée PRI-Alice.

**CCP8 - Mettre en place, assurer et tester les sauvegardes et les restaurations des éléments de l’infrastructure**

1. Quelle est la différence entre un PRA et un PCA en termes d’objectifs et de mise en œuvre ?

Un PRA (Plan de Reprise d'Activité) est là pour restaurer un SI après un incident majeur (attaque cyber, problème électrique, incendie, etc.). Le but est de réduire le temps de reprise (RTO pour Recovery Time).

Mise en œuvre par redondance (HA ou High Availability), réplication des données, tests de panne.

Un PCA (Plan de Continuité d'Activité) est là pour s’assurer que l’activité continue sans interruption, même en cas de problème minime. Il est là pour garantir une disponibilité totale du SI.

Mise en oeuvre par sauvegarde/restauration.

1. Quelles sont les bonnes pratiques pour sécuriser une sauvegarde ?

Stockage hors site, chiffrement, règles 3-2-1, tests de restauration.

1. Quels outils et technologies sont recommandés pour garantir un PRA efficace ?

Hyperviseur (virtualisation du matériel), réplication de données, automatisation (Ansible)...

1. Votre entreprise a mis en cloud son système de messagerie. Quelle(s) solution(s) pouvez-vous utiliser pour disposer d’une sauvegarde locale ?

Export de la boite mail partielle ou complète en archive (PST/OST), utilisation de logiciel spécialisé comme Veeam Backup.

1. Quels sont les types de stockage les plus utilisés pour les sauvegardes ?

* Disque dur (HDD, SSD)
* Bande magnétique (LTO)
* NAS
* SAN
* Cloud

1. Quels sont les avantages et inconvénients du stockage sur bandes LTO ?

Avantages :

* Coût faible
* Durée de vie élevée
* Grande capacité de stockage

Inconvénients :

* Accès aux données lent
* Matériel spécifique (propriétaire)

1. Pourquoi est-il important d’avoir une politique de rétention des sauvegardes ?

* Conformité légale et réglementaire (facture, …)
* Permet une restauration à différentes dates

1. Quels outils permettent d’automatiser la gestion des sauvegardes ?

* Bareos
* Scripts (avec cron)
* Windows Server Backup
* Veeam Backup

**CCP9 - Exploiter et maintenir les services de déploiement des postes de travail**

1. A quoi servent les commandes "dism mount" et "dism umount" ?

"dism mount" et "dism umount" sont des commandes de gestion de montage d’image sous Windows.

On monte une image avec "dism mount" et on la démonte avec "dism umount".

1. Indiquer les différentes actions à faire, au niveau macro, pour faire un déploiement de masse.

Procédure :

* Préparation du PC modèle (master)
* Sysprep du PC modèle
* Capture de l’image
* Déploiement du master

1. On exécute les commandes suivante dans un terminal cmd sous Windows :

Diskpart

list disk

select disk 2

Clean

create partition primary

format fs=ntfs quick

Active

Assign

Exit

Quel est le but global de ces lignes de commandes ?

Diskpart ⇒ lance l’utilitaire Diskpart

list disk ⇒ affiche la liste des disque

select disk 2 ⇒ Sélectionne le disque 2 dans la liste

Clean ⇒ supprime les partitions du disque sélectionné

create partition primary ⇒ créer une partition primaire

format fs=ntfs quick ⇒ effectue un formatage rapide et met le système de fichiers NTFS

Active ⇒ met la partition comme active, donc on peut booter dessus

Assign ⇒ attribue une lettre de lecteur pour que la partition soit accessible sous Windows

Exit ⇒ sort du programme

Dans quel contexte peuvent-elles s'exécuter ?

Préparation d’un disque pour une nouvelle installation d’un OS (Par exemple création d’une clé USB bootable).

1. Qu’est-ce qu’un sysprep ? Donne un exemple de ligne de commande.

Un sysprep est un moyen de préparer un ordinateur pour qu’il devienne un master pour un déploiement de masse.

Exemple de commande : sysprep /oobe /generalize /shutdown

1. Qu’est-ce qu’un boot PXE ?

C’est un démarrage par le réseau. Il faut qu’il soit activé et mis en priorité dans le bios.

1. En quoi le rôle WSUS peut aider à la maintenance d’un parc informatique ?

Il permet de :

* Tester ces mises-à-jour avant de les déployer
* Sélectionner les mises-à-jour téléchargés sur les clients
* Réduire la bande passante

1. Quels sont les principaux services de déploiement pour automatiser l’installation d’OS et de logiciels ?

Il existe :

* SCCM (System Center Configuration Manager)
* WDS (Windows Deployment Services)
* FOG

1. Comment fonctionne le déploiement via PXE avec un service comme WDS ou FOG ?

Il faut que le boot PXE soit activé sur les PC client.

Il faut également un serveur DHCP et TFTP, et bien sûr un serveur de déploiement.

Fonctionnement :

* Le PC client démarre sur le réseau
* Il obtient une adresse IP via le serveur DHCP
* Il obtient le fichier de déploiement via le serveur TFTP
* Le fichier de déploiement va interagir avec le serveur de déploiement pour continuer les actions (téléchargement de l’image d’OS, script de configuration, etc.)

1. Quelles sont les bonnes pratiques pour maintenir un master à jour ?

* MAJ régulières de l’OS
* Choisir plutôt des images hybrides
* Automatiser le déploiement
* Tester régulièrement les images de déploiement