**📝 Objectifs**

✅ Répondre à un maximum de question du challenge  
✅ Valider les compétences acquises durant ces dernières semaines de formations

**Sommaire**

* [**🤓 Contexte de ce checkpoint**](https://odyssey.wildcodeschool.com/expeditions/11070/quests/2934#-contexte-de-ce-checkpoint)
* [**📖 Répondre aux questions (*How to*)**](https://odyssey.wildcodeschool.com/expeditions/11070/quests/2934#-r%C3%A9pondre-aux-questions-how-to)
* [**💪 Challenge**](https://odyssey.wildcodeschool.com/expeditions/11070/quests/2934#-challenge)
  + [**Exercice 1 : Manipulations pratiques sur VM Windows (temps estimé : 1h30)**](https://odyssey.wildcodeschool.com/expeditions/11070/quests/2934#exercice-1--manipulations-pratiques-sur-vm-windows-temps-estim%C3%A9--1h30)
    - [**Partie 1 : Gestion des utilisateurs**](https://odyssey.wildcodeschool.com/expeditions/11070/quests/2934#partie-1--gestion-des-utilisateurs)
    - [**Partie 2 : Restriction utilisateurs**](https://odyssey.wildcodeschool.com/expeditions/11070/quests/2934#partie-2--restriction-utilisateurs)
    - [**Partie 3 : Lecteurs réseaux**](https://odyssey.wildcodeschool.com/expeditions/11070/quests/2934#partie-3--lecteurs-r%C3%A9seaux)
  + [**Exercice 2 : Manipulations pratiques sur VM Linux (temps estimé : 2h30)**](https://odyssey.wildcodeschool.com/expeditions/11070/quests/2934#exercice-2--manipulations-pratiques-sur-vm-linux-temps-estim%C3%A9--2h30)
    - [**Partie 1 : Gestion des utilisateurs**](https://odyssey.wildcodeschool.com/expeditions/11070/quests/2934#partie-1--gestion-des-utilisateurs-1)
    - [**Partie 2 : Configuration de SSH**](https://odyssey.wildcodeschool.com/expeditions/11070/quests/2934#partie-2--configuration-de-ssh)
    - [**Partie 3 : Analyse du stockage**](https://odyssey.wildcodeschool.com/expeditions/11070/quests/2934#partie-3--analyse-du-stockage)
    - [**Partie 4 : Sauvegardes**](https://odyssey.wildcodeschool.com/expeditions/11070/quests/2934#partie-4--sauvegardes)
    - [**Partie 5 : Filtrage et analyse réseau**](https://odyssey.wildcodeschool.com/expeditions/11070/quests/2934#partie-5--filtrage-et-analyse-r%C3%A9seau)
    - [**Partie 6 : Analyse de logs**](https://odyssey.wildcodeschool.com/expeditions/11070/quests/2934#partie-6---analyse-de-logs)
* [**🧐 Critères d'acceptation**](https://odyssey.wildcodeschool.com/expeditions/11070/quests/2934#-crit%C3%A8res-dacceptation)

**🤓 Contexte de ce checkpoint**

Dans ce checkpoint, tu interviens sur 2 machines virtuelles VirtualBox :

* Une VM Windows Server nommée **SRVWIN01**
* Une VM GNU/Linux nommée **SRVLX01**

La VM Windows a une interface réseau configurées en mode Réseau interne.  
La VM GNU/Linux a une interface réseau configurée en mode Bridge et utilise DHCP en IPv4 et l'auto-configuration IPv6 standard. Il est possible d'y accéder via ssh.

Détails sur les VM :

| **Type de machine** | **Nom** | **Utilisateur** | **Mot de passe** |
| --- | --- | --- | --- |
| Windows Server | SRVWIN01 | Administrator | %Adm!n@2k=T0p |
| GNU/Linux | SRVLX01 | wilder | wcs4ever |
|  |  | root | MXtTvqGXmZDf |

**📖 Répondre aux questions (*How to*)**

Les réponses à ce checkpoint sont à fournir en markdown dans un lien git.

2 types de questions te sont posées :

* Des questions ouvertes

Pour ces questions, les réponses (jamais plus d'un court paragraphe de quelques lignes) sont à écrire dans la solution en dessous du numéro de la question. Le nom et le numéro de la partie du checkpoint (Partie 1, ...) est également à mettre en début de chapitre.

**Exemple :**

Pour la question :

**Partie 1 : Particularité des Unix**

**Q.1.1.1** Comment s'appelle le compte administrateur sur les systèmes Unix ?

La réponse doit être de la forme :

**Partie 1 : Particularité des Unix**

**Q.1.1.1**  
Le compte administrateur sous Unix est **root**

* Des questions pratiques

Ces questions demande de lancer des commandes et à effectuer des actions sur les VM du checkpoint.

Pour ces questions, la réponse a fournir consiste dans la solution, là aussi en dessous du numéro de la question, soit à copier les commandes exactes que tu as utilisés pour faire ce qui était demandé avec les affichages correspondants, ainsi que les commandes exactes que tu as utilisés pour vérifier que ton action a réussi et les affichages correspondants, ou bien à mettre une copie d'écran des actions et du résultat.

**Exemple :**

Pour la question :

**Partie 2 : Manipulation de fichiers sous Unix**

**Q.1.1.2** Créé un fichier vide nommé fichier\_vide dans un dossier temp dans ton homedir.

La réponse doit être de la forme :

**Partie 2 : Manipulation de fichiers sous Unix**

**Q.1.1.2**

1# Création du dossier si nécessaire

2wilder@host:~$ mkdir -p ~/temp

3# Création du fichier vide

4wilder@host:~$ touch ~/temp/fichier\_vide

5# Vérification de la création : la taille doit être 0

6wilder@host:~$ ls -lh ~/temp/fichier\_vide

7total 0

8-rw-rw-r-- 1 wilder wilder 0 janv. 2 09:58 fichier\_vide

**💪 Challenge**

**Exercice 1 : Manipulations pratiques sur VM Windows (temps estimé : 1h30)**

Pour cet exercice tu as besoin de la VM **SRVWIN01**.

**Partie 1 : Gestion des utilisateurs**

L'utilisateur **Kelly Rhameur** a quitté l'entreprise.  
Elle est remplacée par **Lionel Lemarchand**

**Q.1.1.1** Créer l'utilisateur **Lionel Lemarchand** avec les même attribut de société que **Kelly Rhameur**.

**Q.1.1.2** Créer une OU **DeactivatedUsers** et déplace le compte désactivé de **Kelly Rhameur** dedans.

**Q.1.1.3** Modifier le groupe de l'OU dans laquelle était **Kelly Rhameur** en conséquence.

**Q.1.1.4** Créer le dossier Individuel du nouvel utilisateur et archive celui de **Kelly Rhameur** en le suffixant par **-ARCHIVE**.

**Partie 2 : Restriction utilisateurs**

**Q.1.2.1** Faire en sorte que l'utilisateur **Gabriel Ghul** ne puisse se connecter que du lundi au vendredi, de 7h à 17h.

**Q.1.2.2** De même, bloquer sa connexion au seul ordinateur **CLIENT01**.

**Q.1.2.3** Mettre en place une stratégie de mot de passe pour durcir les comptes des utilisateurs de l'OU **LabUsers**.

**Partie 3 : Lecteurs réseaux**

**Q.1.3.1** Créer une GPO **Drive-Mount** qui monte les lecteurs **E:** et **F:** sur les clients.

**Exercice 2 : Manipulations pratiques sur VM Linux (temps estimé : 2h30)**

Pour cet exercice tu as besoin de la VM **SRVLX01**.

**Partie 1 : Gestion des utilisateurs**

**Q.2.1.1** Sur le serveur, créer un compte pour ton usage personnel.

**Q.2.1.2** Quelles préconisations proposes-tu concernant ce compte ?

**Partie 2 : Configuration de SSH**

Un serveur SSH est lancé sur le port par défaut.  
Il est possible de s'y connecter avec n'importe quel compte, y compris le compte root.

**Q.2.2.1** Désactiver complètement l'accès à distance de l'utilisateur root.

**Q.2.2.2** Autoriser l'accès à distance à ton compte personnel uniquement.

**Q.2.2.3** Mettre en place une authentification par clé valide et désactiver l'authentification par mot de passe

**Partie 3 : Analyse du stockage**

**Q.2.3.1** Quels sont les systèmes de fichiers actuellement montés ?

**Q.2.3.2** Quel type de système de stockage ils utilisent ?

**Q.2.3.3** Ajouter un nouveau disque de 8,00 Gio au serveur et réparer le volume RAID

**Q.2.3.4** Ajouter un nouveau volume logique LVM de 2 Gio qui servira à héberger des sauvegardes. Ce volume doit être monté automatiquement à chaque démarrage dans l'emplacement par défaut : /var/lib/bareos/storage.

**Q.2.3.5** Combien d'espace disponible reste-t-il dans le groupe de volume ?

**Partie 4 : Sauvegardes**

Le logiciel bareos est installé sur le serveur.  
Les composants bareos-dir, bareos-sd et bareos-fd sont installés avec une configuration par défaut.

**Q.2.4.1** Expliquer succinctement les rôles respectifs des 3 composants bareos installés sur la VM.

**Partie 5 : Filtrage et analyse réseau**

**Q.2.5.1** Quelles sont actuellement les règles appliquées sur Netfilter ?

**Q.2.5.2** Quels types de communications sont autorisées ?

**Q.2.5.3** Quels types sont interdit ?

**Q.2.5.4** Sur nftables, ajouter les règles nécessaires pour autoriser bareos à communiquer avec les clients bareos potentiellement présents sur l'ensemble des machines du réseau local sur lequel se trouve le serveur.

Rappel : Bareos utilise les ports TCP 9101 à 9103 pour la communication entre ses différents composants.

**Partie 6 : Analyse de logs**

**Q.2.6.1** Lister les 10 derniers échecs de connexion ayant eu lieu sur le serveur en indiquant pour chacun :

* La date et l'heure de la tentative
* L'adresse IP de la machine ayant fait la tentative

**🧐 Critères d'acceptation**

Les réponses aux questions sont mise dans 2 fichiers accessible par un lien git.  
Ils sont rédigé sous format markdown et contiennent l'ensemble des réponses aux questions, ainsi que les commandes et/ou les copies d'écran.

Nom des fichiers :

* Exercice 1 : Checkpoint3\_Exercice1.md
* Exercice 2 : Checkpoint3\_Exercice2.md

Seront considéré comme faux :

* Toutes les questions non répondues
* Toutes les réponses fausses ou hors-sujet
* Toutes les réponses n'ayant pas de justification
* Des commandes ou des captures d'écran sans rapport avec la question
* Des commandes ou des captures d'écran manquantes