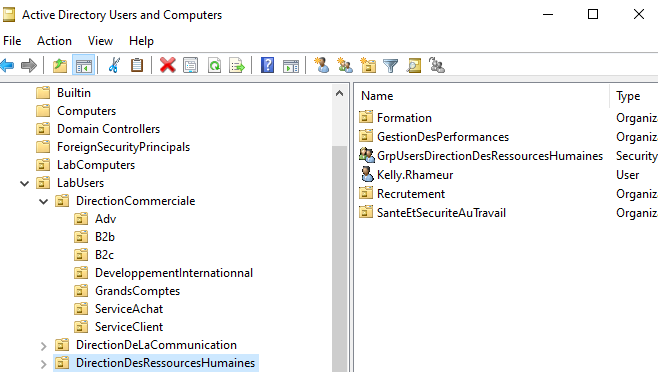
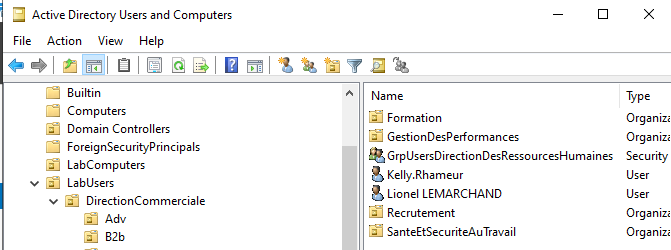
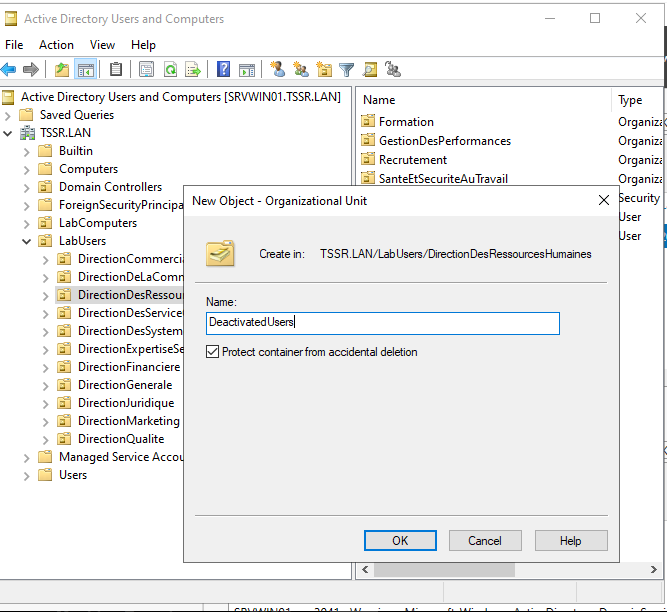
CHECKPOINT3

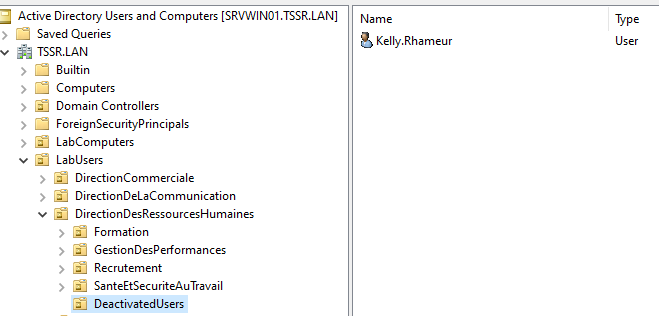
**Q.1.1.1**





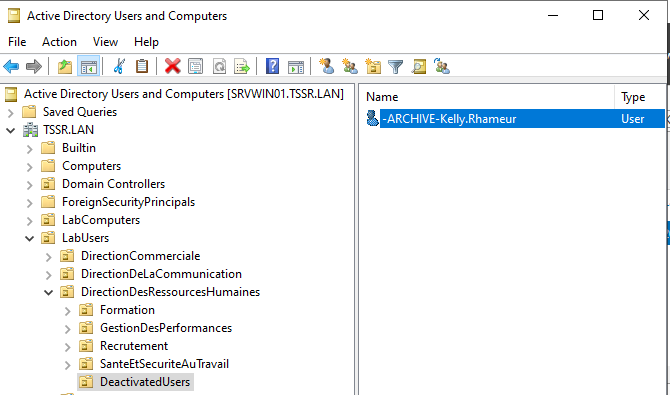
**Q.1.1.2**



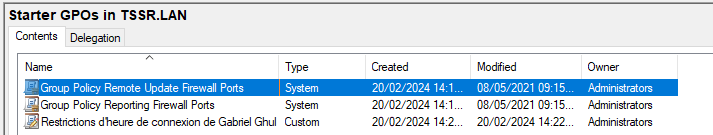


**Q.1.1.3**

**Q.1.1.4**



**Q.1.2.1**

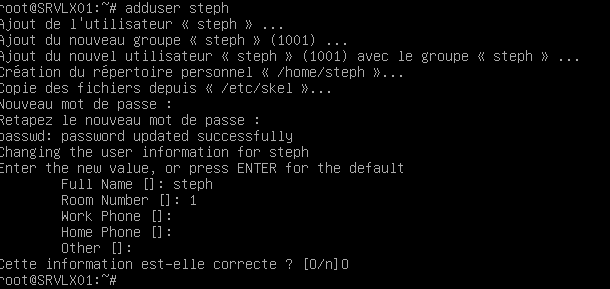


**Q.1.2.2**

**Q.1.2.3**

**Q.1.3.1**

**Q.2.1.1**



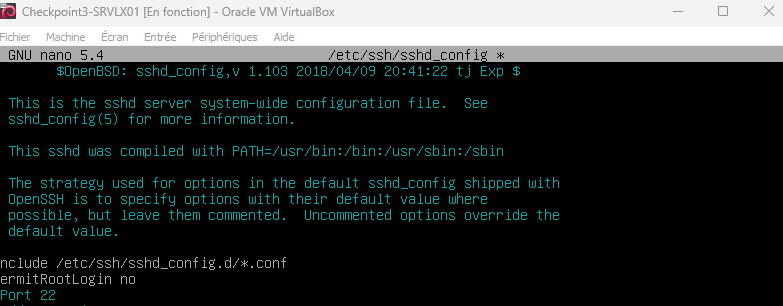
**Q.2.1.2**

1. **Complexité du mot de passe :** Assurez-vous que le mot de passe attribué au compte utilisateur est suffisamment complexe pour garantir la sécurité. Il doit contenir une combinaison de lettres majuscules et minuscules, de chiffres et de caractères spéciaux, et avoir une longueur suffisante.
2. **Attribution des privilèges :** Limitez les privilèges accordés aux utilisateurs en fonction de leurs besoins. Évitez d'attribuer des privilèges administratifs à des comptes utilisateur standard, sauf si cela est absolument nécessaire. Utilisez plutôt le mécanisme sudo pour accorder des privilèges temporaires lorsque c'est nécessaire.
3. **Gestion des groupes :** Ajoutez le nouvel utilisateur à des groupes pertinents en fonction de ses responsabilités. Par exemple, vous pouvez ajouter l'utilisateur à des groupes tels que **sudo** pour accorder des privilèges administratifs, ou à des groupes spécifiques à des projets ou des départements.
4. **Surveillance et journalisation :** Activez la journalisation des activités des utilisateurs pour surveiller les actions effectuées. Vous pouvez configurer des outils comme **auditd** pour suivre les changements effectués par les utilisateurs sur le système.
5. **Politiques de mot de passe :** Définissez des politiques de mot de passe appropriées pour le système, telles que des règles de rotation régulières des mots de passe, des exigences de longueur minimale des mots de passe, et des restrictions d'utilisation d'anciens mots de passe.
6. **Désactivation des comptes inutilisés :** Surveillez l'utilisation des comptes utilisateur et désactivez ou supprimez les comptes inutilisés pour réduire les risques de compromission de la sécurité.

En suivant ces préconisations, vous pouvez renforcer la sécurité et la gestion des comptes utilisateur sur votre serveur Linux.

**Q.2.2.1**

****

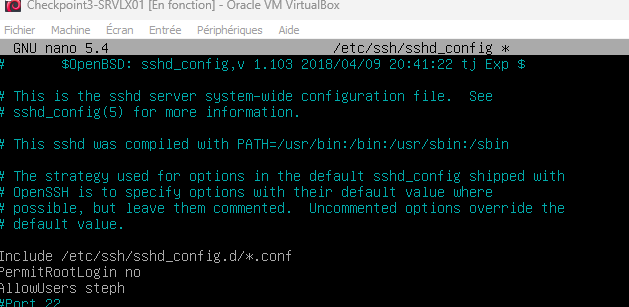




Une fois ces étapes effectuées, l'accès à distance en tant qu'utilisateur root sera désactivé sur votre serveur SSH, ce qui renforce la sécurité en limitant les risques associés à l'utilisation du compte root pour les connexions SSH.

**Q.2.2.2**

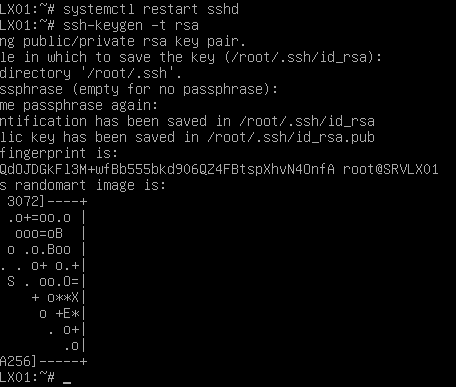






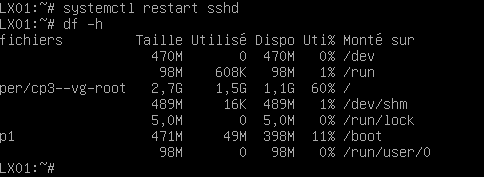
Une fois ces étapes effectuées, seuls les utilisateurs spécifiés dans la directive **AllowUsers** seront autorisés à se connecter via SSH. Assurez-vous que votre compte personnel est inclus dans cette liste pour garantir que vous seul pouvez accéder au serveur à distance.

**Q.2.2.3**





**Q.2.3.1**

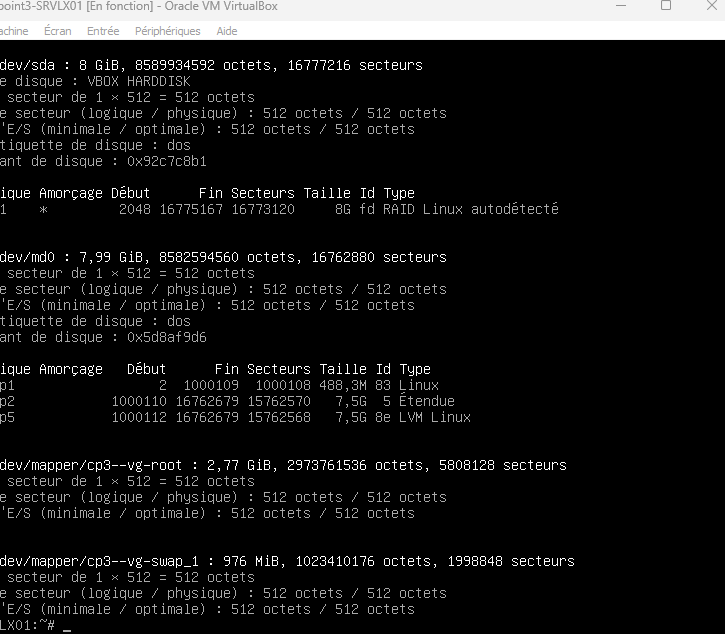


**Q.2.3.2**

**RAID**

**Q.2.3.3**

**Fdisk –l**



**Q.2.3.4**

**Q.2.3.5**

**Q.2.4.1**

Les trois composants Bareos installés sur la VM ont les rôles suivants :

1. **bareos-dir** : Le composant Director est responsable de la gestion globale du système Bareos. Il contrôle les jobs de sauvegarde, restauration et archivage, ainsi que la configuration des clients et des catalogues de sauvegarde. Le Director est essentiellement le cœur du système Bareos.
2. **bareos-sd** : Le composant Storage Daemon est responsable du stockage physique des données de sauvegarde. Il gère les dispositifs de stockage, tels que les disques, les bandes ou les répertoires, où les données sont sauvegardées et restaurées.
3. **bareos-fd** : Le composant File Daemon est installé sur chaque client que vous souhaitez sauvegarder. Il est responsable de la communication entre le client et le Director. Le File Daemon reçoit les instructions de sauvegarde/restauration du Director et effectue les opérations correspondantes sur les fichiers du client.

En résumé, le Director contrôle l'ensemble du processus de sauvegarde, le Storage Daemon gère le stockage des données sur les supports de sauvegarde, et le File Daemon permet la communication entre le client et le serveur Bareos pour la sauvegarde et la restauration des données.

**Q.2.5.1**



**Q.2.5.2**

Pour déterminer quels types de communications sont autorisés, vous devez examiner les règles actuellement configurées dans Netfilter (iptables). Les règles peuvent autoriser ou bloquer différents types de communications en fonction des ports, des adresses IP, des protocoles, etc.

Voici quelques exemples de types de communications qui pourraient être autorisés :

1. Communications HTTP (port 80) pour accéder à des sites web.
2. Communications HTTPS (port 443) pour accéder à des sites web sécurisés.
3. Communications SSH (port 22) pour accès distant sécurisé.
4. Communications DNS (port 53) pour résolution de noms de domaine.
5. Communications SMTP (port 25) pour l'envoi de courriels.
6. Communications IMAP (port 143) ou POP3 (port 110) pour la récupération de courriels.

Ces exemples représentent quelques-uns des types de communications couramment autorisés, mais cela dépendra entièrement de la configuration spécifique de vos règles iptables.

**Q.2.5.3**

Les types de communications qui sont interdits dépendent entièrement de la configuration spécifique des règles dans Netfilter (iptables) sur le serveur. Voici quelques exemples de types de communications qui pourraient être interdits :

1. Communications ICMP (par exemple, les pings) : Certains administrateurs choisissent de bloquer les requêtes ICMP pour des raisons de sécurité.
2. Communications sur des ports non autorisés : Les règles iptables peuvent bloquer les communications sur des ports spécifiques qui ne sont pas nécessaires pour les services en cours d'exécution sur le serveur.
3. Communications vers des adresses IP spécifiques : Il est possible de configurer des règles pour bloquer les communications vers des adresses IP spécifiques, par exemple, pour restreindre l'accès à certains sites web ou services.
4. Communications vers des sous-réseaux spécifiques : Les règles iptables peuvent également être configurées pour bloquer les communications vers des plages d'adresses IP spécifiques.
5. Communications sortantes non autorisées : Certaines configurations peuvent restreindre les communications sortantes depuis le serveur vers Internet pour des raisons de sécurité ou de conformité.

Ces exemples représentent quelques-uns des types de communications qui pourraient être interdits, mais la liste exacte dépendra de la politique de sécurité et des exigences spécifiques de l'infrastructure réseau.

**Q.2.5.4**

**Q.2.6.1**