

White Test RHCSA

Server 1 : node1.example.com

- 1- Configurer le serveur avec les informations IP ci-dessous :
 - a. Hostname=**node1.example.com**
 - b. Adresse IP : **192.168.120.133/24**
 - c. Passerelle : **192.168.120.2**
 - d. DNS : **192.168.120.2**
- 2- Ajoutez les adresses IP secondaires suivantes de manière statique à votre interface en cours d'exécution. Faites-le d'une manière qui ne compromet pas vos paramètres existants :
IPV4 – 10.0.0.5/24
IPV6 – fd01 ::100/64
- 3- Activer le transfert de paquets sur server1. Cela devrait persister après le redémarrage.
- 4- Configurez manuellement vos sources yum en respectant les liens suivants :
BaseOS : [http://vault.centos.org/\\$contentdir/\\$releasever/BaseOS/\\$basearch/os/](http://vault.centos.org/$contentdir/$releasever/BaseOS/$basearch/os/)
AppStream :
[http://vault.centos.org/\\$contentdir/\\$releasever/AppStream/\\$basearch/os/](http://vault.centos.org/$contentdir/$releasever/AppStream/$basearch/os/)
(vous pouvez utiliser un chemin local : /var/ftp/rep).
- 5- Diagnostic serveur web (SELinux) :
 - a. Un serveur web configuré sur le port 82 reste toujours inaccessible, résolvez ce problème.
 - b. Le répertoire /var/www/html contient 03 fichiers (test1, test2, test3) contenant chacun la phrase « **Examen EX200** ». Configurez le serveur web de sorte qu'il puisse exploiter le contenu provenant de ces fichiers. (Ne pas modifier le contenu de ces fichiers)
 - c. Le serveur web démarre automatiquement au redémarrage du système.
- 6- Créer un utilisateur patrice de telle sorte que tout fichier crée par cet utilisateur aura comme droits par défaut rw-r—r--, son uid est 1011 et un mot de passe tek-up2022
- 7- Gestion des utilisateurs & des groupes :
 - a. Créez 03 utilisateurs (natasha, harry, sarah)

- b. Natasha a comme groupe secondaire sysmgs.
- c. Harry a comme groupe secondaire sysmgs.
- d. Sarah ne doit pas pouvoir se logger dans le système n'est pas membre du groupe sysmgs.
- e. Le mot de passe pour tous les utilisateurs est tek-up2022.

8- Créez le répertoire /home/managers :

- a. Le groupe propriétaire de /home/managers est sysmgs.
Les membres du groupe sysmgs ont les droits de lecture et ecriture.
Les autres n'ont aucuns droits (sauf le root).
- b. Tous les fichiers créés dans chacun de ces répertoires appartiennent au groupe propriétaire.
- c. L'utilisateur Natasha a seulement le droit de lecture au répertoire /home/sysmgs.

9- Configurez une tâche crontab pour l'utilisateur natasha devant s'exécuter chaque 3 minutes de 9h00 à 12h00 du lundi au mercredi et du vendredi au samedi : « EX200 en cours ».

10- En tant que root, planifiez une tache qui supprime le contenu du fichier /tmp le 27/08/2022 à 16h30.

11- Configurer le système pour que les UID et GID des utilisateurs et groupes puissent commencer à 1050 ; La durée de validité du mot de passe doit être de 30 jours et le mot de passe minimale doit être composé de 08 caractères au minimum.

12- Ecrire un script shell script1.sh qui recherche, sous /usr, suivant le groupe propriétaire (suivant chaque GID indiqué dans /etc/group) tous les fichiers de taille inférieur à 10M , puis les copiez dans /root/files1.

13- Ecrire un script nommé script2.sh qui recherche, dans /usr/bin, tous les fichiers qui sont de taille plus petite que 50K et plus grande que 30K et qui ont des privilèges du propriétaire, copiez le résultat dans /root/files2.

- 14- Configurer votre serveur pour récupérer l'heure depuis le serveur de temps **node2.example.com**. Mettre le timezone sur Africa/Tunis.
- 15- Un partage NFS a été effectué depuis le serveur **node2.example.com** :
node2.example.com:/rhome/remotouser1.
Le répertoire personnel de remotouser1 est /rhome/remotouser1.
Configurez ce partage pour que son répertoire personnel soit monté automatiquement sous /rhome (utiliser autofs) (il faut configurer la partie serveur et partie client).
- 16- Sur votre serveur, le service httpd a été configuré pour utiliser NFS mais la configuration ne fonctionnera pas à cause de la politique SELinux. Corrigez cette situation en activant le booléen "httpd_use_nfs" et rendez-le persistant lors du redémarrage (même il est bien configuré, exécuter les commandes nécessaires pour répondre à la question).
- 17- Copiez le fichier /etc/fstab dans /var/tmp/fstab et configurez les droits :
a. /var/tmp/fstab appartient à l'utilisateur root et au groupe root.
b. L'utilisateur natasha a les droits de lecture et d'écriture.
c. L'utilisateur harry n'a pas les droits de lecture et d'écriture.
d. Tous les autres utilisateurs (actuels ou futurs) ont un accès en lecture uniquement.
- 18- Archiver et compressez le répertoire /var/tmp afin d'obtenir tmp.tar.gz
- 19- Chercher toutes les lignes contenant la chaîne « nologin » dans le fichier /etc/passwd et les placer dans le fichier /root/list dans l'ordre d'origine.
- 20- Créer un user iar (avec UID 3400, password redhat) de telle sorte que tout fichier crée par cet utilisateur aura comme droits par défaut 600.

Informations sur les registres de conteneurs :

registry.redhat.io/rhel8/rsyslog

(utiliser votre propre login et mot de passe)

- 21- Connectez-vous au repository et téléchargez l'image rsyslog.

- 22- Créer un rootless conteneur nommé « logserver » avec l'utilisateur paradise en utilisant l'image rsyslog (Le service démarre automatiquement au démarrage du système).
- 23- A partir du conteneur créer un service nommé « container-logserver » et l'attacher un stockage persistant pour monter automatiquement /home/paradise/container_logfile vers /var/log/journal.
- 24- Depuis le service passer la commande : `logger -p local5.info « This is an RHCSA exam »`.
- Il faut que ce message soit visible dans les deux chemins :
- Dans le conteneur : /var/log/journal
- Dans le host : /home/paradise/container_logfile
- 25- Localiser tous les fichiers appartenant à l'utilisateur **paradise** et les copier dans le repertoire /home/rootedfiles.
- 26- Réglez le contexte Selinux du port 2332 sur `xen_port_t` à l'aide du protocole tcp.
- Ajustez SELinux pour qu'il s'exécute en mode permissive et configurez votre firewall pour rejeter toutes les connexions/flux de trafic du serveur

Server 2 : node2.example.com (02 disques additionnels 20Go et 5Go)

1. Accéder au serveur ; configurez le mot de passe « tek-up2022 »
2. Ajoutez une partition swap supplémentaire 850M.
La partition swap doit être montée automatiquement au démarrage du système. (Ne supprimez ni modifiez aucune partition swap existante sur le système)
3. Utiliser un disque non partitionné de taille 7G pour créer un volume nommé « vdough » de taille logique 500M. Le volume doit être formaté avec xfs et monté automatiquement sur /vbrear au démarrage du système. Ajustez la taille du volume logique vdough à 700M. (Assurer que le contenu du système de fichiers reste inchangé).
4. Sur le même disque de 7G, créez un nouveau volume logique nommé « qa » de taille 256LE ; le groupe de ce volume est nommé « qagroup » et la taille de son PE= 16M.

Créez sur ce volume logique « qa » un VDO nommé vdoqa de taille logique 40G, puis le formatez en xfs et le montez automatiquement lors de démarrage.

5. Sur un disque de taille 10G, créer un pool stratis pool1, puis créez un file system fs1. Créer dans « fs1 » un fichier de taille 2G, puis créez un snapshot nommé « snap1 » pour ce file system. Montez automatiquement snap1 et fs1 lors de démarrage.
6. Configurez le profil recommandé comme étant actif.