C04-backup - TP LINUX - MTN

Guillaume ASTIER

26/02/16

Table des matières

ISEN - TP Sysadmin - TP n°4

Sauvegardes en local

Le but de ce chapitre est de mettre en oeuvre une solution de sauvegarde.

1. Sauvegarde complète

1.0 SCRIPT

Faire un script qui réalise une sauvegarde complète des espaces /etc, /root, /home/M1, /home/M2, /home/MTN.

Le fichier de sortie, sera une archive compressée, placée dans le répertoire /backups. Son nom sera horodaté.

Exemple de fichier généré “/backups/full_20180405-2305.tgz”.

Ex de code :

```
#!/bin/bash
DIRS="/etc /root ..."
DATE="$(date +%Y%m%d-%H%M%S)"
# full backup
tar ...
if [ $? -ne 0 ]
    then
        echo "Backup failed."
        exit 1;
fi
```

1.1 LOGUER

En utilisant la commande “logger” :

- améliorer le script pour qu’il envoie des messages au service de journalisation (syslogd) en début et fin d’exécution. Par défaut, le service de journalisation envoie les messages dans le fichier “/var/log/messages”

ET/OU

- Utilisez si vous le souhaiez tout autre système de gestion de log . Même “maison”

---

2. Sauvegarde incrémentale

2.0 SCRIPT

L'option "-newer" de la commande "find" permet de rechercher et d'afficher les fichiers, dont la date de dernière modification est plus récente que celle du fichier passé en paramètre. (Tester cette option).

Modifier/copier le script de la question 1.0 pour qu'il réalise une sauvegarde incrémentale lorsqu'il est appelé avec l'option "-g".

Le fichier de sortie, sera une archive compressée contenant seulement les fichiers créés ou modifiés depuis la dernière sauvegarde. Exemple de fichier généré "/backups/inc_20180404-2305.tgz".

---

3. Planificateur de tâches

3.0 CRON

Avec la commande "crontab -e", planifier le lancement automatique de sauvegardes pour avoir chaque semaine:

• une sauvegarde compléte le vendredi soir ; • des sauvegardes incrémentales les autres jours ouvrés (càd du lundi soir au jeudi soir).

4. Configuration réseau & service OpenSSH

4.0 Préambule

Le but de ce chapitre est de se familiariser avec le protocole SSH, qui permet une prise de main à distance sécurisée.

Pour commencer, il faut configurer les deux machines machines pour qu'elles puissent communiquer. Pour chaque machine, il faut:

• définir un nom d'hôte (fichier /etc/hostname) ; • définir une adresse IP et un masque de sous-réseau (fichier /etc/network/interfaces) ; • renseigner les noms d'hôte (fichier /etc/hosts).

4.1 KEGEN

Générer des clés d'authentification (type RSA, sans passphrase) avec la commande "ssh-keygen".

4.2 COPY

Ces clés permettent d'établir une relation de confiance entre deux machines, et ainsi permettre une authentification sans que la saisie du mot de passe ne soit nécessaire.

Utiliser la commande "ssh-copy-id" pour établir une confiance vers la nouvelle machine importée

Ou envoyez la clef via scp .

4.3 What do you do ?

Expliquer ce que fait réellement cette commande "ssh-copy-id" qui est un script bash situé dans "/usr/bin/ssh-copy-id".

4.4 Test

Tester la confiance précédemment mise en place avec la commande ci-dessous (qui ne vous demandera plus de mot de passe) :

```
1 ssh <machine_distante>
```

---

5. Sauvegardes déportées

5.0 SCRIPT

Grâce à la relation de confiance établie dans le chapitre précédent, améliorer le script du chapitre 1 pour qu'il stocke les sauvegardes dans le répertoire "/backups/" de la deuxième machine. Utiliser les tubes '|' :

```
[...]
tar ... | ssh <machine_distante> "..."
[...]
```

---

6. Restauration

6.0 Delete

Effacer le contenu d'un répertoire sauvegardé et restaurer le grâce à la sauvegarde associée.

---

7. FAR FAR AWAY

7.0 Crypto

Pour aller plus loin (sauvegardes déportées chiffrées)

Le but de ce chapitre est de chiffrer la sauvegarde avant de la déporter sur un serveur distant.

Cela permet de préserver la confidentialité des données. Pour cela nous utiliserons GnuPG (commande "gpg"), un outil de chiffrement asymétrique.

7.1. GPG

Avec la commande “gpg –gen-key”, générer une paire de clés RSA (publique/privée) d’une longueur de 1024 bits qui n’expire jamais.

Par convention, utiliser “NOM Prénom” lors de la saisie du “Nom réel”.

Choisir une passphrase (un long mot de passe).

Pour lister le nouveau trousseau de clés :

```
1 gpg --list-keys
```

7.2. Chiffrer

Vous pouvez dès à présent chiffrer et déchiffrer des fichiers.

Par exemple (supposons que “.asc” soit l’extention du fichier chiffré) :

```
1 # gpg -ea -r <KEY_ID> < fichier > fichier.asc
2 # gpg -d < fichier.asc > fichier
```

7.3. SCRIPT

Améliorer le script du chapitre 3 pour qu’il chiffre la sauvegarde avant de l’envoyer sur la machine distante (utiliser les tubes ‘|’).

```
1 [...]
2 tar ... | gpg ... | ssh <machine_distante> "..."
3 [...]
```
