La Plateforme

Un peu de scripts

Automatización con unos escriptos

Projet

Dans ce projet nous allons explorer plus en profondeur le scripting sous linux.
Vous allez automatiser la récupération de logs sur votre système et faire de la rotation de logs.

Vous pouvez réaliser ces scripts de préférence en bash mais aussi en python sur une VM debian, ubuntu ou kalinux.

Faites des recherches sur le répertoire /var/log de votre système.

Que contient-il? A quoi correspondent les principaux fichiers logs?
Qu'est-ce qu'un log rotatif?

Documentez vous car vous allez devoir mettre ça en place.

Job 1

Vous allez réaliser un script de backup de tous les fichiers du répertoire $HOME de chacun des utilisateurs de votre système offrant ces différentes possibilités:

- Fichiers créés depuis moins de 7 jours
- Fichiers modifiés depuis plus de 7 jours
- Répertoires dont le contenu est > 10 Mo
- Répertoire et fichiers cachés

Les répertoires et fichiers collectés par votre script seront regroupés dans un .tar.gz avec le nom de l'utilisateur, l'option choisie et la date et rangés dans le répertoire /var/backup/. Les backups ne devront être rwx que par l'utilisateur concerné.

Par exemple:
-rw------- 1 john users 99 jun. 30 2023 /var/backup/john-fichiers-moins-7-jours-10-SEP-2023.tar.gz

Job 2

On aimerait pouvoir récupérer des données en fonction d'un écart de date.
Vous allez donc mettre au point un script qui récupère le nombre de connexions journalier en fonction de deux dates au format jj-mm-aaaa passé en arguments.

Créez une fonction que vous pourrez réutiliser dans d'autres scripts.

exemple: ./script-recuperation.sh 10-03-2023 12-03-2023

Les données collectées seront regroupées dans un .tar.gz avec la date et rangés dans le répertoire /var/backup/.

exemple: */var/backup/recuperation-10-SEP-2023.tar.gz*

Job 3

Utilisez la commande **tshark** pour capturer toutes les trames circulant sur le réseau pendant 1 minute et sauvegardez-les dans le fichier /var/log/tshark.log.
Automatisez ce script pour qu'il se lance toutes les 5 minutes avec un cron.

Le fichier de log /var/log/tshark.log doit garder toutes les captures (et non pas que la dernière), il va donc grossir de plus en plus.

Lorsque ce fichier fera plus 1 Mo, on aimerait qu'il reparte à 0 tout en conservant les données dans d'autres fichiers /var/log/tshark.log.1.gz et ainsi de suite 4 fois (tshark.log.2.gz, tshark.log.3.gz, tshark.log.4.gz).

En gros, vous allez mettre en place une rotation de logs.

C’est une manière de conserver un intervalle de logs sans risque de saturer votre espace de stockage.
La rotation de log est beaucoup utilisée dans la conservation de vidéo de surveillance par exemple.

Pour faire de la rotation de logs, on peut utiliser la commande ***logrotate.***
A vous de jouer!

Pour aller plus loin...

Deamonizer la job 3, de manière à ce que la rotation de logs tourne en background dès le démarrage du système.

Rendu

Vous rendrez vos scripts sur github dans un repo nommé ***logrotate-exercices***.

Compétences visées

- Administration Système sous linux
- Scripting Bash / Python
- Automatisation d’événements

Base de connaissances

- https://fr.wikibooks.org/wiki/Programmation_Bash/Fonctions
- Deamonize a process
- https://github.com/awesome-lists/awesome-bash
- https://linux.die.net/man/8/logrotate
- https://en.wikipedia.org/wiki/Log_rotation

Log système sous linux

- /var/log/auth.log --- logs authorization attempts
- /var/log/kern.log --- logs kernel data
- /var/log/syslog --- logs system data
- /var/log/faillog --- logs failed logins