

Script automatisé de backup

Nous travaillons avec un outil qui s'appelle CyberWatch.

C'est un outil de gestion de la vulnérabilité qui aide les entreprises à identifier, évaluer et prioriser les vulnérabilités de sécurité dans leur système d'information. Il offre une vue d'ensemble de l'état de sécurité de l'entreprise, en identifiant les vulnérabilités potentielles et en fournissant des recommandations pour les corriger.

En plus de ses fonctionnalités de gestion de la vulnérabilité, Cyberwatch peut également être utilisé comme un serveur de logs pour collecter, analyser et stocker des données de sécurité à partir de différents systèmes et applications.

En tant que serveur de logs, Cyberwatch est capable de collecter des informations sur les événements de sécurité tels que les tentatives d'intrusion, les anomalies de connexion, les erreurs système et les activités suspectes. Il peut également collecter des informations sur les mises à jour de sécurité et les correctifs appliqués aux systèmes de l'entreprise.

Il m'a donc été demandé de réaliser un script de backup de notre serveur cyberwatch. Pour faire notre backup nous envoyons nos logs vers Restic qui est un outil open-source de sauvegarde et de restauration de données. Il permet de créer des sauvegardes incrémentielles et chiffrées, et de les stocker sur différents types de supports tels que des disques durs externes, des serveurs de fichiers, des services de stockage en nuage, etc.

Ensuite notre backup est envoyé vers scaleway qui est une solution de stockage et de sauvegarde. Pour réaliser mon script j'ai fait un Bash car notre serveur cyberwatch est un Linux :

```
#!/bin/bash
dossierbackup="/var/lib/cyberwatch/backups"
export RESTIC_PASSWORD=Re[REDACTED]
export AWS_ACCESS_KEY_ID=SC[REDACTED]
export AWS_SECRET_ACCESS_KEY=ba4[REDACTED]
cd /restic
echo "Création de la backup..."
cyberwatch backup save
echo "Backup créée avec succès !"
echo "Copie en cours vers $dossierbackup..."
cp -r /etc/cyberwatch $dossierbackup
echo "Copie terminée !"
echo "Envoi vers le dossier de sauvegarde S3..."
restic -r s3:https://s3.fr-par.scw.cloud/t[REDACTED] backup /var/lib/cyberwatch/backups
echo " Envoi terminé !"
echo "Suppression du backup en local..."
rm -r /var/lib/cyberwatch/backups
echo "Suppression terminée !"
echo "Sauvegarde terminé !"
```

