03-Exploitation

B - Backup-SI

1. Description :

Le serveur d'admin est accessible en SSH soit avec le clé SSH ou bien avec le login "adminme" et son mot de passe (Identique au Keepass Informatique afin que le service informatique puisse le connaître).

Le service Samba est installé permettant de transférer depuis l'AD01 les informatique du SI (Keepass et Zim) vers un espace local sur le serveur admin.v.sdem.fr:/home/share/backup-si/
Un lien symbolique est créé sur le compte adminme dans "/home/adminme"

```
lrwxrwxrwx 1 adminme adminme   22 Aug 18 08:59 backup-si -> /home/share/backup-si//
```

2. Emplacement du backup :

Le "Zim" et le "Keepass" du service informatique sont copiés dans "adminme@admin.v.sdem.fr:/home/share/backup-si/%YYYYMMDD%".

Le backup est géré par un script Powershell sur le serveur AD01 qui va se connecter en SSH sur le serveur admin.v.sdem.fr avec le compte samba "backup-si".

C - Procédure-récupération-données-SI

Copie des données de l'infrastructure du SI de Morbihan Energies vers le serveur physique d'administration local avec une rétention de 30 jours.

Sources copiées :
- Dossier Keepass
- Dossier Zim

Destination :
admin.v.sdem.fr:/home/share/backup-si/%YYYYMMDD% (AnnéeMoisJour)

Accès aux données :
En cas de besoin d'accès aux données, suivre la procédure ci-dessous :
- Se connecter avec un client FTP (Filezilla) sur adminme@admin.v.sdem.fr (Password identique au Keepass Informatique)
- Cliquer sur le lien symbolique backup-si
- Sélectionner le dossier correspondant à la date souhaitez et le transférer localement sur le poste

D - crontab

```
# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  *  user command to be executed
#
# Archive - mailreboot :
#20 12 * * 1,3 cd /root && ./mailreboot.sh
#


# ssl-cert-check :
00 01 * * * cd /usr/local/bin/ssl-cert-check/ && ./ssl-cert-check.sh -a -f ssldomains -q -x 60 -e
hostmaster@morbihan-energies.fr


## url-check :
# Demarrage script url-check.sh - Intervale 5mn :
*/05 * * * * cd /usr/local/bin/url-check/ && ./url-check.sh >/dev/null 2>&1
```

```
# Purge dossier de cache URL toutes les heures :
* */01 * * * rm -f /usr/local/bin/url-check/cache/*

# Purge dossier /home/share/backup-si des dossiers de plus de 30 jours :
00 01 * * * cd /usr/local/bin/ && ./purge-backup-si.sh 2>&1
```

E - Racktables - ARCHIVE

1. Création d'un accès en lecture seul pour script de Cable-ID :

```
# Création du compte :
CREATE USER 'readonly'@'localhost' IDENTIFIED BY 'PASSWORD';

# Attribue des accès en lecture seule :
GRANT SELECT ON *.* TO 'readonly'@'localhost';

# Application des changements :
FLUSH PRIVILEGES;
```

Cette procédure est à transférer sur le serveur racktables lors de la migration de Racktables en CT LXC.

F - Scripts

Ce serveur permet d'orchestrer un ensemble de script prévu pour l'administration du système dr'information de Morbihan Energies.

```
Emplacement des scripts :
/usr/local/bin/
```

1. purge-si-backup.sh

Description :

Purger le dossier "/home/share/backup-si" de tous les dossiers dont la date de création est supérieur à 30 jours.

Emplacement du script : /usr/local/bin/purge-backup-si.sh

```
#!/bin/bash


# Author : jkermorvant
# Version : 1.0
# Description : Purge du dossier /home/share/backup-si de tous les dossiers dont la date de création est suppérieur à 30 jours.
find /home/share/backup-si/* -ctime +30 -exec rm -rf {} \;
```

2. ssl-cert-check-master

Description :

Ce script permet d'alerter quand l'expiration des certificats approche des 60 jours.

Source :

> https://github.com/Matty9191/ssl-cert-check
> https://prefetch.net/articles/checkcertificate.html

Fonctionnement :

Le fichier "/usr/local/bin/ssl-cert-check-master/ssldomains" contient la liste des sites en SSL à scanner

```
morbihan-energies.fr 443
sdem.fr 443
```

Le fichier "/usr/local/bin/ssl-cert-check-master/ssl-cert-check" est le script qui permettra de vérifier l'état des certificats des sites web déclarés dans ssldomains.
La ligne 388 du script a été modifié pour configurer le FROM :

```
#   FROM="${1}"
    FROM="hostmaster@morbihan-energies.fr"
```

Exemple d'utilisation :

```
# Vérifier l'expiration des certificats listés dans le fichier ssldomains
./ssl-cert-check -f ssldomains

# Vérifier
./ssl-cert-check -a -f ssldomains -q -x 60 -e hostmaster@morbihan-energies.fr
```

Crontab :

Une tâche planifiée est créé pour analyser tous les jours à 1h00 l'état des certificats.

```
# Editer la crontab
crontab -e

# Crontab pour le ssl-cert-check :
00 01 * * * cd /usr/local/bin/ssl-cert-check-master/ && ./ssl-cert-check -a -f ssldomains -q -x 60 -e
hostmaster@morbihan-energies.fr
```

3. testssl.sh

Description :

La mise en place du chiffrement sur un serveur Web peut être parfois assez complexe en fonction du niveau de sécurité que vous souhaitez atteindre tout en prenant en compte la compatibilité avec les différents navigateurs et terminaux du marché.
Pour tester que votre serveur possède une configuration correcte, deux options s'offrent à vous :
- Dans le cas le plus simple, votre serveur possède déjà une entrée DNS publique, vous pourrez tout simplement utiliser le site SSLLabs pour vérifier la configuration de celui-ci. Une note de A est assez facilement atteignable en suivant les recommandations de safeciphers.
- Dans le cas contraire, si le DNS de votre serveur n'est pas encore exposé sur Internet, il faudra utiliser une autre solution : Testssl.sh
Testssl.sh est un script Unix permettant de vérifier la sécurité de votre configuration HTTPS. Il permettra de vous confirmer la compatibilité de votre site avec une exhaustivité de systèmes : Android, IE, Safari, Java ...

Documentation :

> https://www.geeek.org/testssl-test-tls-ssl-serveur/

Installation :

```
cd /usr/local/bin/
git clone https://github.com/drwetter/testssl.sh
mv testssl.sh testssl
cd testssl
chmod +x testssl.sh
```

Exploitation :

./testssl.sh site.morbihan-energies.fr

testssl.png
Image not found or type unknown

4. url-check

Revision #1
Created 8 February 2024 08:10:45 by Jérôme
Updated 3 March 2026 08:05:50 by Jérôme