ASR5x00 Sauvegarde du fichier .chassisid (ID de châssis) sur StarOS versions 20 et ultérieures

Contenu

Introduction

Ce document décrit comment sauvegarder **.chassisidfile** (ID de châssis) sur StarOS versions 20 et ultérieures.

Informations générales

La clé de châssis est utilisée pour chiffrer et déchiffrer les mots de passe chiffrés dans le fichier de configuration. Si deux châssis ou plus sont configurés avec la même valeur de clé de châssis, les mots de passe chiffrés peuvent être décryptés par l'un des châssis partageant la même valeur de clé de châssis. En conséquence, une valeur de clé de châssis donnée ne peut pas déchiffrer les mots de passe chiffrés avec une valeur de clé de châssis différente.

La clé de châssis est utilisée pour générer l'ID de châssis stocké dans un fichier et utilisé comme clé principale pour protéger les données sensibles (par exemple, les mots de passe et les secrets) dans les fichiers de configuration

Pour les versions 15.0 et ultérieures, l'ID de châssis est un hachage SHA256 de la clé de châssis. La clé du châssis peut être définie par les utilisateurs via une commande CLI ou via l'Assistant de configuration rapide. Si l'ID du châssis n'existe pas, une adresse MAC locale est utilisée pour générer l'ID du châssis.

Pour les versions 19.2 et ultérieures, l'utilisateur doit définir explicitement la clé de châssis à l'aide de l'Assistant de configuration rapide ou de la commande CLI. Si elle n'est pas définie, un ID de châssis par défaut utilisant l'adresse MAC locale est généré. En l'absence de clé de châssis (et donc d'ID de châssis), les données sensibles n'apparaissent pas dans un fichier de configuration enregistré.

L'ID de châssis est le **hachage SHA256 (codé au format base36) de la clé de châssis entrée par l'utilisateur, plus un nombre aléatoire sécurisé de 32 octets.** Ceci garantit que la clé du châssis et l'ID du châssis ont une entropie de 32 octets pour la sécurité de la clé.

Si un ID de châssis n'est pas disponible, le chiffrement et le déchiffrement des données sensibles des fichiers de configuration ne fonctionnent pas.

Problème : Insuffisant pour sauvegarder la valeur de clé du châssis pour exécuter la même configuration sur le même noeud.

En raison du changement de comportement à partir de la version 19.2, il n'est plus suffisant de sauvegarder la valeur de clé du châssis pour pouvoir exécuter la même configuration sur le même noeud.

En outre, en raison du numéro aléatoire de 32 octets attaché à la clé de châssis configurée, il existe toujours des ID de châssis différents générés à partir des mêmes clés de châssis.

C'est la raison pour laquelle la **vérification des clés** du **châssis** de commande cli est dissimulée maintenant car elle renvoie toujours une valeur négative même si la même ancienne clé est entrée.

Pour pouvoir récupérer une machine StarOS à partir d'une configuration enregistrée (lorsque, par exemple, tout le contenu du lecteur **/flash** a été perdu), il est nécessaire de sauvegarder le fichier **.chassisid** (où StarOS stocke l'ID du châssis)

L'ID du châssis est stocké dans le fichier **/flash/.chassisid** sur le disque dur StarOS. La méthode la plus simple pour sauvegarder ce fichier est de le transférer via un protocole de transfert de fichiers vers un serveur de sauvegarde :

Comme vous voyez que le **.chassisid** est un fichier caché et avec les nouvelles versions il n'est pas possible de faire des opérations de gestion de fichiers avec des fichiers cachés. Par exemple, cette erreur s'affiche avec la version 20.0.1 :

```
[local]sim-lte# copy /flash/.chassisid /flash/backup
Failure: source is not valid.
[local]sim-lte#
```

OU:

```
[local]sim-lte# show file url /flash/.chassisid
Failure: file is not valid.
```

Solution

Il existe toujours un moyen d'accéder à ce fichier via cette procédure :

Étape 1. Assurez-vous que le fichier **.chassisid** est présent dans **/flash/.chassisid**.

```
[local]sim-lte# dir /flash/.chassisid
-rw-rw-r--    1 root     root           53 Jun 23 10:59 /flash/.chassisid
8       /flash/.chassisid
Filesystem           1k-blocks      Used Available Use% Mounted on
/var/run/storage/flash/part1   523992    192112    331880  37% /mnt/user/.auto/onboard/flash
```

Étape 2. Connectez-vous en mode masqué.

```
[local]sim-lte# cli test-commands
Password:
Warning: Test commands enables internal testing and debugging commands
USE OF THIS MODE MAY CAUSE SIGNIFICANT SERVICE INTERRUPTION
[local]sim-lte#
```

Note: Si aucun mot de passe de mode masqué n'est configuré, configurez-le avec ceci :

```
[local]sim-lte(config)# tech-support test-commands password <password>
```

Étape 3. Démarrez un shell de débogage.

```
[local]sim-lte# debug shell
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Cisco Systems QvPC-SI Intelligent Mobile Gateway
[No authentication; running a login shell]
```

Étape 4. Déplacez-vous dans le répertoire **/flash**. Vérifiez si le fichier est présent.

```
sim-lte:ssi#
sim-lte:ssi# ls
bin cdrom1 hd-raid param rmm1 tmp usr
boot dev include pcmcia1 sbin usb1 var
boot1 etc lib proc sftp usb2 vr
boot2 flash mnt records sys usb3
sim-lte:ssi#
sim-lte:ssi# cd flash
sim-lte:ssi# ls -a
. ldlinux.sys restart_file_cntr.txt
.. module.sys sftp
.chassisid patch staros.bin
crashlog2 persistdump syslinux.ban
crsh2 rc.local syslinux.cfg
```

Étape 5. Copiez le fichier caché dans un fichier non masqué.

```
sim-lte:ssi# cp .chassisid chassisid.backup
sim-lte:ssi#
sim-lte:ssi#
sim-lte:ssi# ls
chassisid.backup patch staros.bin
crashlog2 persistdump syslinux.ban
crsh2 rc.local syslinux.cfg
ldlinux.sys restart_file_cntr.txt
module.sys sftp
```

Étape 6. Quittez le shell de débogage. Vous devez pouvoir transférer le fichier de sauvegarde créé sans problème.

```
sim-lte:ssi# exit
Connection closed by foreign host.
[local]sim-lte#
[local]sim-lte# copy /flash/chassisid.backup /flash/chasisid.backup2
********************************************************************************
```

```
Transferred 53 bytes in 0.003 seconds (17.3 KB/sec)
[local]sim-lte#
[local]sim-lte#
[local]sim-lte# show file url /flash/chassisid.backup
1ke03dqfdb9dw3kds7vdslvuls3jnop8yj41qyh29w7urhno4ya6
```

UPDATE pour la procédure de mise à niveau UltraM

La mise à niveau de N5.1 vers N5.5 détruira l'instance vpc et le protocole OSP. Avant de lancer la procédure de mise à niveau, nous devons sauvegarder le fichier de configuration vPC et l'ID de châssis si nous voulons les réutiliser.

Étape 1. sauvegarde du fichier de configuration chassisid et du dernier fichier de configuration :

```
bash-2.05b# ls -alrt
-rwxrwxr-x 1 root root 53 Jul 11 14:43 .chassisid
-rwxrwxr-x 1 root root 381973 Jul 11 14:41 GGN-2017-07-28.cfg
```

```
from copied file :

cpedrode@CPEDRODE-xxxxx:~/Desktop$ more 2017-07-28.chassis-id
1swbwpd8fd8ca3kf33kn6qxb2h33ihfkqu1tu7x1ndf82znag1b5^@
```

Note: le fichier de configuration aura une clé dérivée de .chasssisid :

```
[local]GGN# show configuration url /flash/GGN-2017-07-28.cfg | more
Monday July 11 14:59:34 CEST 2016
#!$$ StarOS V21.1 Chassis c95bf13f030f6f68cae4e370b2d2482e
config
```

Étape 2. Procéder à la mise à niveau Ultra-M

Étape 3. Une fois le système mis à niveau et le démarrage de StarOS vpc CF, copiez chassisid (le fichier normal) et le fichier de configuration (assurez-vous que l'adresse IP O&M appropriée est également modifiée) en **/flash/sftp** (StarOS >R20)

Étape 4. Sauvegardez le fichier .chassisid par défaut caché depuis /flash en mode « test-command » et supprimez-le.

Étape 5. Copiez le fichier chassisid de /flash/sftp dans /flash en mode masqué en tant que **".chassisid**« . Copier également le fichier de configuration

Note: vous pouvez vérifier l'url *show configuration* cli d'émission de clé dérivée */flash/xxxxxx.cfg | plus* et comparer avec le fichier de configuration de sauvegarde

Étape 6. Ajouter la priorité de démarrage pointant vers le nouveau fichier de configuration

Remarque : à ce stade, StarOS va donner une erreur :

```
[local]GGN(config)# boot system priority 6 image /flash/staros.bin config /flash/GGN-2017-07-
28.cfg
Monday July 28 08:45:28 EDT 2017
Warning: Configuration was generated using a different chassis key, some encrypted information
may not
be valid
```

Si vous avez suivi les étapes correctes, vous disposerez d'un fichier de configuration avec une clé dérivée du châssis égale au fichier de configuration de sauvegarde et un chasssisid égal au chasssisid de sauvegarde.

Notez que lorsque vous affichez le fichier chassisid, il ajoute l'invite PS1 :

```
bash-2.05b# cat .chassisid
1swbwpd8fd8ca3kf33kn6qxb2h33ihfkqu1tu7x1ndf82znag1b5bash-2.05b#
```

Étape 7. Redémarrer vPC

Àce stade, le système doit redémarrer et vous pouvez utiliser les informations d'identification de connexion du fichier de configuration de sauvegarde.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.