

ASR5x00 sauvegardant .chassisid classent (ID de châssis) sur des versions 20 de StarOS et plus élevé

Contenu

[Introduction](#)

[Informations générales](#)

[Problème : Insuffisant pour sauvegarder la valeur principale de châssis pour s'exécuter pour la même configuration sur le même noeud.](#)

[Solution](#)

Introduction

Ce document décrit comment sauvegarder `.chassisidfile` (ID de châssis) sur des versions 20 de StarOS et plus élevé.

Informations générales

La clé de châssis est utilisée pour chiffrer et déchiffrer des mots de passe chiffrés dans le fichier de configuration. Si deux châssis ou plus sont configurés avec la même valeur principale de châssis, les mots de passe chiffrés peuvent être déchiffrés par le châssis l'un des partageant la même valeur principale de châssis. Comme corollaire à ceci, un châssis donné la valeur principale ne peut pas déchiffrer les mots de passe qui ont été chiffrés avec une valeur principale de châssis différent.

La clé de châssis est utilisée pour générer l'ID de châssis qui est enregistré dans un fichier et est utilisé comme clé principale pour protéger des données sensibles (telles que des mots de passe et des secrets) dans des fichiers de configuration

Pour la version 15.0 et plus élevé, l'ID de châssis est des informations parasites SHA256 de la clé de châssis. La clé de châssis peut être placée par des utilisateurs par une commande CLI ou par l'intermédiaire de l'assistant de configuration rapide. Si l'ID de châssis n'existe pas, une adresse MAC locale est utilisée pour générer l'ID de châssis.

Pour la version 19.2 et plus élevé, l'utilisateur doit explicitement placer la clé de châssis par le magicien de configuration rapide ou la commande CLI. S'il n'est pas placé, un ID par défaut de châssis utilisant l'adresse MAC locale est généré. Faute de clé de châssis (et par conséquent ID de châssis), les données sensibles n'apparaissent pas dans un fichier de configuration enregistrée.

L'ID de châssis est les **informations parasites SHA256 (encodées dans format base36) de la clé de châssis écrite par utilisateur plus un 32-byte sécurisent le nombre aléatoire**. Ceci s'assure que la clé de châssis et l'ID de châssis ont l'entropie 32-byte pour la Sécurité principale.

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

Problème : Insuffisant pour sauvegarder la valeur principale de châssis pour s'exécuter pour la même configuration sur le même noeud.

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

D'ailleurs, en raison du nombre aléatoire de 32 octets relié à la clé configurée de châssis, il y a toujours de différents id de châssis générés basés sur les mêmes clés de châssis.

C'est la raison pour laquelle le **keycheck de châssis de** commande cli est caché maintenant puisqu'il toujours négatif de retour même si la même vieille clé est écrite.

Pour pouvoir récupérer un ordinateur de StarOS d'une configuration enregistrée (quand, par exemple tout le contenu du lecteur de **/flash** a été perdu) c'est sauvegarde required le **.chassisid** (où le StarOS enregistre l'ID de châssis)

L'ID de châssis est enregistré dans le fichier de **/flash/.chassisid** sur le disque dur de StarOS. La méthode facile de sauvegarder ce fichier est de le virer par l'intermédiaire d'un certain protocole de trasfer de fichier sur un serveur de sauvegarde :

Comme vous voyez que le **fichier .chassisid** est masqué et avec plus nouveau le libère n'est pas possible de faire des exécutions de gestion de fichiers avec les fichiers masqués. Par exemple cette erreur est affichée 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 y a toujours une manière d'accéder à ce fichier par l'intermédiaire de cette procédure :

Étape 1. Assurez 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. Ouvrez une session dans le 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#
```

Remarque: S'il n'y a aucun mot de passe configuré masqué de mode, configurez-le avec ceci :

```
[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#
```

Étape 3. Mettez en marche 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 le répertoire de /flash. Vérifiez si le fichier est là.

```
sim-lte:ssi#
sim-lte:ssi# ls
bin cdrom1 hd-raid param rmm1 tmp usr
boot dev include pcmcial 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 masqué sur 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 devriez pouvoir transférer le fichier de sauvegarde non créé sans aucune question.

```
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  
1ke03dqfdb9dw3kds7vds1vuls3jnop8yj41qyh29w7urhno4ya6
```