ASR5x00 Sicherung der .chassisid-Datei (Chassis-ID) auf StarOS-Versionen 20 und höher

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie **.chassisidfile (**Chassis-ID) auf StarOS 20 und höher sichern.

Hintergrundinformationen

Der Chassis-Schlüssel dient zum Verschlüsseln und Entschlüsseln verschlüsselter Kennwörter in der Konfigurationsdatei. Wenn zwei oder mehr Chassis mit demselben Chassis-Schlüsselwert konfiguriert werden, können die verschlüsselten Kennwörter von allen Chassis mit demselben Chassis-Schlüsselwert entschlüsselt werden. Folglich kann ein bestimmter Chassis-Schlüsselwert keine Passwörter entschlüsseln, die mit einem anderen Chassis-Schlüsselwert verschlüsselt wurden.

Der Chassis-Schlüssel dient zum Generieren der Chassis-ID, die in einer Datei gespeichert ist und als Primärschlüssel für den Schutz vertraulicher Daten (wie Kennwörter und Schlüssel) in Konfigurationsdateien verwendet wird.

Für Version 15.0 und höher ist die Gehäuse-ID ein SHA256-Hash des Gehäuseschlüssels. Der Chassis-Schlüssel kann von Benutzern über einen CLI-Befehl oder über den Quick Setup Wizard (Schnelleinrichtungsassistent) festgelegt werden. Wenn die Chassis-ID nicht vorhanden ist, wird eine lokale MAC-Adresse zum Generieren der Chassis-ID verwendet.

Für Version 19.2 und höher muss der Chassis-Schlüssel explizit über den Quick Setup Wizard (Schnelleinrichtungsassistent) oder den CLI-Befehl festgelegt werden. Wenn sie nicht festgelegt ist, wird eine Standard-Chassis-ID mit der lokalen MAC-Adresse generiert. Wenn kein Chassis-Schlüssel (und damit keine Chassis-ID) vorhanden ist, werden vertrauliche Daten nicht in einer gespeicherten Konfigurationsdatei angezeigt.

Die Chassis-ID ist der **SHA256-Hash (codiert im Base36-Format) des vom Benutzer eingegebenen Chassis-Schlüssels plus einer sicheren 32-Byte-Zufallszahl.** Dadurch wird sichergestellt, dass der Chassis-Schlüssel und die Chassis-ID aus Sicherheitsgründen eine Entropie von 32 Byte aufweisen.

Wenn keine Chassis-ID verfügbar ist, funktioniert die Verschlüsselung und Entschlüsselung vertraulicher Daten in Konfigurationsdateien nicht.

Problem: Unzureichende Sicherung des Chassis-Schlüsselwerts zur Ausführung für dieselbe Konfiguration auf demselben Knoten.

Aufgrund der Änderung des Verhaltens ab Version 19.2 reicht es nicht mehr aus, den Chassis-Schlüsselwert zu sichern, um dieselbe Konfiguration auf demselben Knoten ausführen zu können.

Aufgrund der zufälligen 32-Byte-Nummer, die mit dem konfigurierten Chassis-Schlüssel verbunden ist, werden außerdem immer andere Chassis-IDs generiert, die auf denselben Chassis-Schlüsseln basieren.

Dies ist der Grund, warum die CLI-Befehl-**Chassis-Schlüsselprüfung** jetzt verborgen ist, da sie immer negativ zurückgibt, selbst wenn derselbe alte Schlüssel eingegeben wird.

Um einen StarOS-Rechner aus einer gespeicherten Konfiguration wiederherstellen zu können (wenn z. B. alle Inhalte des **/Flash-**Laufwerks verloren gingen), muss die .chassisid-Datei gesichert werden (in der StarOS die Chassis-ID speichert).

Die Gehäuse-ID wird in der Datei **/flash/.chassisid** auf der StarOS-Festplatte gespeichert. Die einfachste Methode zum Sichern dieser Datei besteht darin, sie über ein Dateiübertragungsprotokoll auf einen Sicherungsserver zu übertragen:

Wie Sie sehen ist die **.chassisid Datei** versteckt und mit neueren Versionen ist es nicht möglich, Dateiverwaltungsoperationen mit versteckten Dateien durchzuführen. Dieser Fehler wird beispielsweise in Version 20.0.1 angezeigt:

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

ODER:

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

Lösung

Es gibt immer noch eine Möglichkeit, über dieses Verfahren auf diese Datei zuzugreifen:

Schritt 1: Stellen Sie sicher, dass die **.chassisid**-Datei in **/flash/.chassisid** vorhanden ist.

```
[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
```

Schritt 2: Im ausgeblendeten Modus anmelden.

```
[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#
```

> **Hinweis**: Wenn kein Kennwort für den versteckten Modus konfiguriert ist, konfigurieren Sie es wie folgt:

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

Schritt 3: Starten Sie eine Debugshell.

```
[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]
```

Schritt 4: Verschieben Sie das Verzeichnis **/flash**. Überprüfen Sie, ob die Datei vorhanden ist.

```
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
```

Schritt 5: Kopieren Sie die versteckte Datei in eine nicht versteckte.

```
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
```

Schritt 6: Beenden Sie die Debugshell. Sie sollten die erstellte Sicherungsdatei problemlos übertragen können.

```
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 für Ultra-M-Upgrade-Verfahren

Durch ein Upgrade von N5.1 auf N5.5 werden die vPC-Instanz und der OSP zerstört. Vor dem Beginn des Upgrade-Vorgangs sollten Sie die vPC-Konfigurationsdatei und die Chassis-ID sichern, wenn Sie sie wiederverwenden möchten.

Schritt 1: Sichern Sie die Chassis-ID und die letzte Konfigurationsdatei:

```
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^@
```

Hinweis: Die Konfigurationsdatei enthält einen abgeleiteten Schlüssel aus .chasssid:

```
[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
```

Schritt 2: Mit Ultra-M-Upgrade fortfahren

Schritt 3: Wenn das System aktualisiert und der StarOS vPC CF gestartet wurde, kopieren Sie das Chassis (die reguläre Datei) und die Konfigurationsdatei (stellen Sie sicher, dass auch die richtige O&M IP-Adresse geändert wird) nach **/flash/sftp (**StarOS >R20).

Schritt 4: Sichern Sie die versteckte .chassisid-Standarddatei von /flash im "test-command"-Modus, und löschen Sie sie.

Schritt 5: Kopieren Sie die chassisid-Datei von /flash/sftp nach /flash im versteckten Modus als "**.chassisid**". Kopieren Sie auch die Konfigurationsdatei

Hinweis: Sie können die *Konfigurations*-URL für die Ausgabe des abgeleiteten Schlüssels überprüfen: */flash/xxxxxx.cfg | mehr* und vergleichen Sie es mit der Sicherungskonfigurationsdatei

Schritt 6: Fügen Sie die Startpriorität hinzu, die auf die neue Konfigurationsdatei verweist.

Hinweis: Zu diesem Zeitpunkt gibt StarOS einen Fehler aus:

```
[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
```

Wenn Sie die richtigen Schritte ausgeführt haben, erhalten Sie eine Konfigurationsdatei mit einem vom Chassis abgeleiteten Schlüssel, der der Backup-Konfigurationsdatei entspricht, und einer chasssid, die der backup chasssid entspricht.

Beachten Sie, dass die Chassisid-Datei an die Eingabeaufforderung PS1 angehängt wird:

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

Schritt 7. Neustarten von vPC

An diesem Punkt sollte das System neu gestartet werden, und Sie können die Anmeldedaten der Sicherungskonfigurationsdatei verwenden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.