ASR5x00 Back-up .chassisid-bestand (chassis ID) op StarOS-releases 20 en hoger

Inhoud

Inleiding

In dit document wordt beschreven hoe u een back-up kunt maken van het chassisidfile (chassis ID) op StarOS-releases van 20 en hoger.

Achtergrondinformatie

De sleutel van het chassis wordt gebruikt om versleutelde wachtwoorden in het configuratiebestand te versleutelen en te decrypteren. Als twee of meer chassis met dezelfde chassiswaarde zijn geconfigureerd, kunnen de versleutelde wachtwoorden worden gedecrypteerd door een chassis met dezelfde chassiswaarde. Als gevolgtrekking hiervan kan een bepaalde waarde van de chassis geen wachtwoorden decrypteren die met een andere waarde van de chassis sleutel werden gecodeerd.

De chassissleutel wordt gebruikt om de chassis-ID te genereren die in een bestand is opgeslagen en die wordt gebruikt als de primaire sleutel voor de bescherming van gevoelige gegevens (zoals wachtwoorden en geheimen) in configuratiebestanden

Voor release 15.0 en hoger is de chassis-ID een SHA256-hash van de chassis-toets. De sleutel van het chassis kan door gebruikers via een CLI-opdracht of via de Wizard Quick Setup worden ingesteld. Als de chassis ID niet bestaat, wordt een lokaal MAC-adres gebruikt om de chassis-ID te genereren.

Voor release 19.2 en hoger moet de gebruiker de chassissleutel expliciet instellen via de wizard Quick Setup of de CLI-opdracht. Als deze niet is ingesteld, wordt er een standaard chassis-ID gegenereerd met behulp van het lokale MAC-adres. Bij het ontbreken van een chassissleutel (en dus van de chassis-ID) verschijnen de gevoelige gegevens niet in een opgeslagen configuratiebestand.

De chassis-ID is de **SHA256-hash (gecodeerd in basis36-formaat) van de door de gebruiker ingevoerde sleutel plus een veilig willekeurig 32-byte-nummer.** Hierdoor wordt gegarandeerd dat de chassis-sleutel en de chassis-ID beschikken over een entropie van 32 bytes voor een belangrijke beveiliging.

Als een chassis-ID niet beschikbaar is, werkt encryptie en decryptie voor gevoelige gegevens in configuratiebestanden niet.

Probleem: Onvoldoende om een back-up te maken van de waarde van de chassissleutel voor dezelfde configuratie op hetzelfde knooppunt.

Vanwege de gedragsverandering die begint met release 19.2 is het niet langer voldoende om een back-up te maken van de waarde van de chassissleutel om dezelfde configuratie op hetzelfde knooppunt te kunnen uitvoeren.

Bovendien zijn er, gezien het willekeurige 32 byte-nummer dat aan de geconfigureerde chassissleutel is bevestigd, altijd verschillende chassis-ID's gegenereerd op basis van dezelfde chassissleutels.

Dat is de reden waarom cli commando **chassis keycheck** nu verhuld is aangezien het altijd negatief zal terugkeren zelfs als dezelfde oude sleutel is ingevoerd.

Om een StarOS-machine van een opgeslagen configuratie te kunnen herstellen (wanneer bijvoorbeeld alle inhoud van het station/flitser verloren is gegaan) moet er een back-up worden gemaakt van het **.chassisid** (waar de StarOS de chassis-ID opslaat)

De chassis-ID wordt opgeslagen in **flitser/.chassisid-**bestand op de harde schijf van StarOS. De eenvoudigste methode om een back-up van dit bestand te maken, is om het via een protocol voor bestandsoverdracht naar een reserveserver over te brengen:

Zoals u ziet is het **bestand.**chassisid verborgen en met nieuwere versies is het niet mogelijk om bestandsbeheerbewerkingen met verborgen bestanden uit te voeren. Deze fout wordt bijvoorbeeld weergegeven met release 20.0.1:

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

Of:

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

Oplossing

Er is nog steeds een manier om via deze procedure toegang tot dit bestand te krijgen:

Stap 1. Zorg ervoor dat het **.chassisid**-bestand aanwezig is in **Chassisid/flitser/.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
```

Stap 2. Meld u aan bij een verborgen modus.

```
[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#
```

> Opmerking: Als er geen wachtwoord voor de verborgen modus is ingesteld, moet u dit wachtwoord gebruiken:

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

Stap 3. Start een debug shell.

```
[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]
```

Stap 4. Gaat in de map**/flitser**. Controleer of het bestand er is.

```
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
```

Stap 5. Kopieer het verborgen bestand naar een niet-verborgen bestand.

```
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
```

Stap 6. Sluit de debug shell aan. U dient in staat te zijn het reservekopiebestand over te maken zonder problemen.

```
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 voor Ultra-M upgradeprocedure

Door de N5.1 te verbeteren naar N5.5 zal het VPC-exemplaar en OSP worden vernietigd. Voordat we de upgradeprocedure starten, moeten we een back-up maken van het vPC-configuratiebestand en de Chassis-id als we ze opnieuw willen gebruiken.

Stap 1. Back-up van het chassis en het vorige configuratiebestand:

```
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^@
```

Opmerking: het configuratiebestand heeft een afgeleide toets van .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
```

Stap 2. Ga verder met de Ultra-M upgrade

Stap 3. Wanneer het systeem is bijgewerkt en StarOS vpc CF-bootup, kopieer chassis (het normale bestand) en configuratiebestand (controleer of het juiste O&M-adres ook is gewijzigd) naar **/ flitser/sftp** (StarOS >R20)

Stap 4. Maak een back-up van het verborgen standaard .chassisid-bestand van /flitser in de modus "test-opdracht" en verwijder het.

Stap 5. Kopieer het bestand dat is geselecteerd uit /flitser/flitser/flitser in /flitser in de verborgen modus als "**.chassisid**". Kopieert ook het configuratiebestand

Opmerking: u kunt de afgeleide sleutel controleren die cli - *show configuratie* url */flash/xxxxxx.cfg | meer* en vergelijk het met het reservekopiebestand

Stap 6 Voeg de beginprioriteit toe aan de nieuwe configuratie-bestanden

Opmerking: Op dit punt geeft StarOS een fout:

```
[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
```

Als u de juiste stappen hebt gevolgd, zult u een configuratiebestand hebben met een Chassis afgeleid sleutel gelijk aan het backup configuratie bestand en een chassisid gelijk aan het back-upchassis.

Merk op dat wanneer u het bestand probeert te scannen, de PS1-melding wordt toegevoegd:

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

Stap 7. Herstart de computer

Op dit moment dient het systeem opnieuw te worden opgestart en u kunt de inlogaanmeldingsgegevens van het back-upconfiguratiebestand gebruiken.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.