ASR5x00 que suporta o arquivo .chassisid (chassi ID) em StarOS libera 20 e mais alto

Índice

Introdução

Este documento descreve como suportar **.chassisidfile** (chassi ID) nas liberações 20 de StarOS e mais alto.

Informações de Apoio

A chave do chassi é usada para cifrar e decifrar senhas criptografada no arquivo de configuração. Se dois ou mais chassis são configurados com o mesmo valor chave do chassi, as senhas criptografada podem ser decifradas por algum do chassi que compartilha do mesmo valor chave do chassi. Como um corolário a isto, um valor chave dado do chassi não pode decifrar as senhas que foram cifradas com um valor chave diferente do chassi.

A chave do chassi é usada para gerar o chassi ID que é armazenado em um arquivo e usado como o chave mestre para dados sensíveis de proteção (tais como senhas e segredos) nos arquivos de configuração

Para a liberação 15.0 e mais alto, o chassi ID é uma mistura SHA256 da chave do chassi. A chave do chassi pode ser ajustada por usuários através de um comando CLI ou através do assistente de configuração rápido. Se o chassi ID não existe, um endereço MAC local está usado para gerar o chassi ID.

Para a liberação 19.2 e mais alto, o usuário deve explicitamente ajustar a chave do chassi através do assistente de configuração ou do comando CLI rápido. Se não é ajustada, um chassi ID do padrão que usa o endereço MAC local está gerado. Na ausência de uma chave do chassi (e daqui do chassi ID), os dados sensíveis não aparecem em um arquivo de configuração salva.

O chassi ID é a **mistura SHA256 (codificada no formato base36) da chave incorporada usuário do chassi mais um 32-byte fixa o número aleatório.** Isto assegura que a chave do chassi e os chassis ID têm a entropia 32-byte para a Segurança chave.

Se um chassi ID não está disponível a criptografia e a descriptografia para dados sensíveis nos arquivos de configuração não trabalham.

Problema: Insuficiente para suportar o valor chave do chassi para ser executado para a mesma configuração no mesmo nó.

Devido à mudança no comportamento que começa com liberação 19.2, não é suficiente anymore suportar o valor chave do chassi para poder executar a mesma configuração no mesmo nó.

Além disso, devido ao número aleatório de 32 bytes anexado à chave configurada do chassi, há sempre os chassis diferentes ID gerados com base nas mesmas chaves do chassi.

Aquela é a razão pela qual o **keycheck do chassi do** comando cli é escondido agora desde que ele sempre negativo do retorno mesmo se a mesma chave velha é incorporada.

Para poder recuperar uma máquina de StarOS de uma configuração salva (quando, por exemplo todos os índices da movimentação de **/flash** foram perdidos) é backup requred o **.chassisid** (onde o StarOS armazena o chassi ID)

O chassi ID é armazenado no arquivo de **/flash/.chassisid no** disco rígido de StarOS. O método o mais fácil de suportar este arquivo é transferi-la através de algum protocolo do trasfer do arquivo a um servidor de backup:

Como você vê que o **arquivo .chassisid** é hidden e com mais novo libera-o não é possível fazer operações do gerenciamento de arquivos com os arquivos ocultos. Por exemplo este erro é indicado com liberação 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.
```

Solução

Há ainda uma maneira de alcançar este arquivo através deste procedimento:

Etapa 1. Assegure-se de que o arquivo **.chassisid** este presente em **/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
```

Etapa 2. Entre hidden no modo.

```
[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#
```

Nota: Se não há nenhuma hidden senha de modo configurada, configurar-la com esta:

```
[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#
```

Etapa 3. Ligue um shell debugar.

```
[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]
```

Etapa 4. Mova-se no diretório de /flash. Verifique se o arquivo está lá.

```
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
```

Etapa 5. Copie o arquivo oculto a um NON-hidden um.

```
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
```

Etapa 6. Retire o shell debugar. Você deve poder transferir o arquivo de backup criado sem nenhumas edições.

```
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
```