ASR5x00 Backup del file .chassisid (ID chassis) su StarOS versione 20 e successive

Sommario

Introduzione

Questo documento descrive come eseguire il backup del file **.chassisidfile** (ID chassis) su StarOS versione 20 e successive.

Premesse

La chiave dello chassis viene utilizzata per crittografare e decrittografare le password crittografate nel file di configurazione. Se due o più chassis sono configurati con lo stesso valore di chiave, le password crittografate possono essere decrittografate da qualsiasi chassis che condivida lo stesso valore di chiave. Di conseguenza, un determinato valore della chiave dello chassis non può decrittografare le password crittografate con un valore diverso.

La chiave dello chassis viene utilizzata per generare l'ID dello chassis, che viene memorizzato in un file e utilizzato come chiave primaria per la protezione dei dati riservati (ad esempio password e segreti) nei file di configurazione

Per la versione 15.0 e successive, l'ID chassis è un hash SHA256 della chiave chassis. La chiave dello chassis può essere impostata dagli utenti tramite un comando CLI o tramite la procedura guidata di configurazione rapida. Se l'ID dello chassis non esiste, viene utilizzato un indirizzo MAC locale per generare l'ID dello chassis.

Per la versione 19.2 e successive, l'utente deve impostare esplicitamente la chiave dello chassis tramite la procedura guidata di configurazione rapida o il comando CLI. Se non è impostato, viene generato un ID chassis predefinito che utilizza l'indirizzo MAC locale. In assenza di una chiave dello chassis (e quindi dell'ID dello chassis), i dati sensibili non vengono visualizzati in un file di configurazione salvato.

L'ID chassis è l'**hash SHA256 (codificato nel formato base36) della chiave dello chassis immessa dall'utente più un numero casuale sicuro di 32 byte.** Ciò garantisce che la chiave dello chassis e l'ID dello chassis abbiano un'entropia di 32 byte per la sicurezza della chiave.

Se non è disponibile un ID chassis, la crittografia e la decrittografia per i dati sensibili nei file di configurazione non funzionano.

Problema: Insufficiente per eseguire il backup del valore della chiave dello chassis per eseguire la stessa configurazione sullo stesso nodo.

A causa del cambiamento di comportamento a partire dalla release 19.2, non è più sufficiente eseguire il backup del valore della chiave dello chassis per poter eseguire la stessa configurazione sullo stesso nodo.

Inoltre, a causa del numero casuale di 32 byte collegato alla chiave dello chassis configurata, esistono sempre ID di chassis diversi generati in base alle stesse chiavi dello chassis.

Ecco perché il comando cli **keycheck** è ora nascosto, in quanto restituisce sempre un valore negativo anche se viene immessa la stessa vecchia chiave.

Per poter ripristinare un computer StarOS da una configurazione salvata (quando, ad esempio, tutto il contenuto dell'unità **/flash** è andato perso) è necessario eseguire il backup dell'ID **.chassisid** (dove l'ID dello chassis è memorizzato da StarOS)

L'ID dello chassis è memorizzato nel file **/flash/.chassisid** sul disco rigido StarOS. Il metodo più semplice per eseguire il backup di questo file consiste nel trasferirlo tramite un protocollo di trasferimento file a un server di backup:

Come si vede il **.chassisid** è un file nascosto e con le nuove versioni non è possibile eseguire operazioni di gestione dei file con i file nascosti. Ad esempio, questo errore viene visualizzato nella release 20.0.1:

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

O:

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

Soluzione

Esiste ancora un modo per accedere al file tramite la procedura seguente:

Passaggio 1. Verificare che il file **.chassisid** sia presente in **/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
```

Passaggio 2. Accedere in modalità nascosta.

```
[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 non è stata configurata una password per la modalità nascosta, configurarla con quanto segue:

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

Passaggio 3. Avviare una shell di debug.

```
[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]
```

Passaggio 4. Spostarsi nella directory **/flash**. Verificare se il file è presente.

```
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
```

Passaggio 5. Copiare il file nascosto in un file non nascosto.

```
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
```

Passaggio 6. Uscire dalla shell di debug. Dovrebbe essere possibile trasferire il file di backup creato senza alcun problema.

```
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
```

Procedura UPDATE per l'aggiornamento di Ultra-M

L'aggiornamento da N5.1 a N5.5 eliminerà l'istanza vpc e l'OSP. Prima di avviare la procedura di aggiornamento è consigliabile eseguire il backup del file di configurazione vPC e dell'ID dello chassis se si desidera riutilizzarli.

Passaggio 1. Eseguire il backup dello chassid e dell'ultimo file di configurazione:

```
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^@
```

Nota: il file di configurazione avrà una chiave derivata da .chassisid:

```
[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
```

Fase 2. Procedere con l'aggiornamento di Ultra-M

Passaggio 3. Dopo aver aggiornato il sistema e avviato StarOS vpc CF, copiare lo chassisid (il file normale) e il file di configurazione (accertarsi che venga modificato anche l'indirizzo IP O&M appropriato) in **/flash/sftp** (StarOS >R20)

Passaggio 4. Eseguire il backup del file .chassisid predefinito nascosto da /flash in modalità "test-command" ed eliminarlo.

Passaggio 5. Copiare il file chassisid da /flash/sftp in /flash in modalità nascosta come "**.chassisid**". Copiare anche il file di configurazione

Nota: è possibile controllare la cli di emissione della chiave derivata - *show configuration* url */flash/xxxxxx.cfg | altro* e confrontarlo con il file di configurazione di backup

Passaggio 6. Aggiungere la priorità di avvio che punta al nuovo file di configurazione

Nota: a questo punto StarOS restituirà un errore:

```
[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
```

Se sono stati seguiti i passaggi corretti, si disporrà di un file di configurazione con una chiave derivata Chassis uguale al file di configurazione di backup e un ID dello chassis uguale all'ID dello chassis di backup.

Notare che quando si visualizza il file chassisid verrà aggiunto il prompt di PS1:

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

Passaggio 7. Riavviare vPC

A questo punto, il sistema dovrebbe riavviarsi ed è possibile utilizzare le credenziali di login del file di configurazione di backup.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).