ASR5x00 Copia de seguridad del archivo .chassisid (ID de chasis) en las versiones 20 y superiores de StarOS

Contenido

Introducción

Este documento describe cómo realizar una copia de seguridad del archivo **.chassisidfile** (ID de chasis) en las versiones 20 y superiores de StarOS.

Antecedentes

La clave del chasis se utiliza para cifrar y descifrar contraseñas cifradas en el archivo de configuración. Si dos o más chasis están configurados con el mismo valor de clave de chasis, cualquiera de los chasis que comparten el mismo valor de clave de chasis puede descifrar las contraseñas cifradas. Como corolario a esto, un valor de clave de chasis determinado no puede descifrar contraseñas que fueron cifradas con un valor de clave de chasis diferente.

La clave de chasis se utiliza para generar el ID de chasis que se almacena en un archivo y se utiliza como clave principal para proteger datos confidenciales (como contraseñas y secretos) en archivos de configuración

Para la versión 15.0 y posteriores, el ID de chasis es un hash SHA256 de la clave de chasis. Los usuarios pueden establecer la clave del chasis mediante un comando CLI o el asistente de configuración rápida. Si el ID de chasis no existe, se utiliza una dirección MAC local para generar el ID de chasis.

Para la versión 19.2 y posteriores, el usuario debe establecer explícitamente la clave del chasis mediante el asistente de configuración rápida o el comando CLI. Si no se configura, se genera un ID de chasis predeterminado que utiliza la dirección MAC local. En ausencia de una clave de chasis (y, por tanto, del ID de chasis), los datos confidenciales no aparecen en un archivo de configuración guardado.

El ID de chasis es el **hash SHA256 (codificado en formato base36) de la clave de chasis introducida por el usuario más un número aleatorio seguro de 32 bytes.** Esto garantiza que la clave del chasis y el ID del chasis tengan una entropía de 32 bytes para la seguridad de la clave.

Si un ID de chasis no está disponible, el cifrado y el descifrado de los datos confidenciales de los archivos de configuración no funcionan.

Problema: no es suficiente realizar una copia de seguridad del valor de la clave del chasis para ejecutar la misma configuración en el mismo nodo.

Debido al cambio en el comportamiento a partir de la versión 19.2, ya no es suficiente realizar una copia de seguridad del valor de la clave del chasis para poder ejecutar la misma configuración en el mismo nodo.

Además, debido al número aleatorio de 32 bytes asociado a la clave de chasis configurada, siempre se generan ID de chasis diferentes basados en las mismas claves de chasis.

Esa es la razón por la que el comando cli **chassis keycheck** se oculta ahora, ya que siempre devuelve negativo incluso si se ingresa la misma clave antigua.

Para poder recuperar una máquina StarOS de una configuración guardada (cuando, por ejemplo, se perdió todo el contenido de la unidad **/flash**), se requiere realizar una copia de seguridad de **.chassisid** (donde StarOS almacena el ID de chasis)

El ID del chasis se almacena en el archivo **/flash/.chassisid** en el disco duro de StarOS. El método más fácil de hacer una copia de seguridad de este archivo es transferirlo a través de algún protocolo de transferencia de archivos a un servidor de copia de seguridad:

Como puede ver, el **archivo .chassisid** está oculto y con las versiones más recientes no es posible realizar operaciones de administración de archivos con archivos ocultos. Por ejemplo, este error se muestra con la versión 20.0.1:

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

O bien:

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

Solución

Todavía hay una manera de acceder a este archivo a través de este procedimiento:

Paso 1. Asegúrese de que el archivo **.chassisid** esté presente en **/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
```

Paso 2. Inicie sesión en modo oculto.

```
[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**: Si no hay ninguna contraseña de modo oculto configurada, configúrela con lo siguiente:

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

Paso 3. Inicie un shell de depuración.

```
[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]
```

Paso 4. Muévase en el directorio **/flash**. Compruebe si el archivo está allí.

```
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
```

Paso 5. Copie el archivo oculto en uno no oculto.

```
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
```

Paso 6. Salga del shell de depuración. Debería poder transferir el archivo de copia de seguridad creado sin ningún 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
```

ACTUALIZAR para procedimiento de actualización de Ultra-M

La actualización de N5.1 a N5.5 destruirá la instancia de vpc y OSP. Antes de iniciar el procedimiento de actualización, debemos realizar una copia de seguridad del archivo de configuración de vPC y del chasis-id si queremos volver a utilizarlos.

Paso 1. copia de seguridad del chassisid y del último archivo de configuración:

```
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: el archivo de configuración tendrá una clave derivada de .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
```

Paso 2. Continúe con la actualización de Ultra-M

Paso 3. Una vez que el sistema se haya actualizado y se haya iniciado StarOS vpc CF, copie chassisid (el archivo regular) y el archivo de configuración (asegúrese de que la dirección IP de O&M adecuada también se cambie) a **/flash/sftp** (StarOS >R20)

Paso 4. Haga una copia de seguridad del archivo .chassisid predeterminado oculto desde /flash en el modo "test-command" y elimínelo.

Paso 5. Copie el archivo chassisid de /flash/sftp a /flash en modo oculto como "**.chassisid**". Copie también el archivo de configuración

Nota: puede verificar la clave derivada que emite cli - *show configuration* url */flash/xxxxxx.cfg | más* y compararlo con el archivo de configuración de copia de seguridad

Paso 6. Agregue la prioridad de arranque que apunta al nuevo archivo de configuración

Nota: En este momento StarOS dará un error:

```
[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
```

Si ha seguido los pasos correctos, tendrá un archivo de configuración con una clave derivada de chasis igual al archivo de configuración de copia de seguridad y un identificador de chasis igual al identificador de chasis de copia de seguridad.

Tenga en cuenta que cuando vea el archivo chassisid se agregará el mensaje PS1 :

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

Paso 7. Reiniciar vPC

En este momento, el sistema debe reiniciarse y puede utilizar las credenciales de inicio de sesión del archivo de configuración de copia de seguridad.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).