ASR5x00 StarOSリリース20以降で.chassisidファイル（シャーシID）をバックアップ

内容

概要

このドキュメントでは、StarOSリリース20以降で**.chassisidfile**（シャーシID）をバックアップする方法について説明します。

背景説明

シャーシキーは、コンフィギュレーションファイル内の暗号化されたパスワードを暗号化および復号化するために使用されます。複数のシャーシが同じシャーシキー値で設定されている場合、暗号化されたパスワードは、同じシャーシキー値を共有するシャーシのいずれかで復号化できます。これに関連して、特定のシャーシキー値は、異なるシャーシキー値で暗号化されたパスワードを復号化できません。

シャーシキーは、ファイルに保存され、コンフィギュレーションファイルの機密データ（パスワードや秘密など）を保護するためのプライマリキーとして使用されるシャーシIDを生成するために使用されます

リリース15.0以降では、シャーシIDはシャーシキーのSHA256ハッシュです。シャーシキーは、ユーザがCLIコマンドまたはクイックセットアップウィザードを使用して設定できます。シャーシIDが存在しない場合、ローカルMACアドレスを使用してシャーシIDが生成されます。

リリース19.2以降では、ユーザはクイックセットアップウィザードまたはCLIコマンドを使用してシャーシキーを明示的に設定する必要があります。設定されていない場合、ローカルMACアドレスを使用するデフォルトシャーシIDが生成されます。シャーシキー（およびシャーシID）がない場合、機密データは保存されたコンフィギュレーションファイルに表示されません。

シャーシIDは、ユーザが入力した**シャーシキーのSHA256ハッシュ（Base36形式でエンコード）と32バイトのセキュアな乱数です。**これにより、シャーシキーとシャーシIDのキーセキュリティのために32バイトのエントロピーが保証されます。

シャーシIDが使用できない場合、コンフィギュレーションファイルの機密データの暗号化と復号化は機能しません。

問題：同じノード上の同じ設定で実行するには、シャーシキーの値をバックアップするのに不十分です。

リリース19.2以降の動作の変更により、シャーシキーの値をバックアップして、同じノードで同じ設定を実行できるだけでは不十分になりました。

さらに、設定されたシャーシキーに32バイトのランダムな数字が付加されるため、同じシャーシキーに基づいて生成されるシャーシIDは常に異なります。

cliコマンドchassis keycheckは、同じ古いキーが入力されている場合でも常に負の値を返すために、現在は隠されているのはそのためです。

StarOSマシンを保存された構成から回復するには(たとえば、フラッシュ**ドライブのすべての内容が失われた**場合).chassisidをバックアップする必要があります（StarOSがシャーシIDを保存する場所）

シャーシIDは、StarOSハードド**ライブの/flash/.chassisidフ**ァイルに保存されます。このファイルをバックアップする最も簡単な方法は、ファイル転送プロトコルを介してバックアップサーバにファイルを転送することです。

.chassisidファイルは隠し**ファイルであ**り、新しいリリースでは隠しファイルに対するファイル管理操作を行うことはできません。たとえば、リリース20.0.1では次のエラーが表示されます。

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

または

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

解決方法

この手順を使用して、このファイルにアクセスする方法は依然として存在します。

ステップ1:.chassisidファイ**ルが**/flash/.chassisidにあることを**確認します**。

```
[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
```

ステップ2：隠しモードにログインします。

```
[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#
```

注：隠しモードパスワードが設定されていない場合は、次のように設定します。

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

ステップ3：デバッグシェルを開始します。

```
[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]
```

ステップ4:/flashディレクトリ内を移動します。ファイルがあるかどうかを確認します。

```
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
```

ステップ5：隠しファイルを隠しファイルにコピーします。

```
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
```

ステップ6：デバッグシェルを終了します。作成したバックアップファイルは、問題なく転送できます。

```
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
```

Ultra-Mアップグレード手順の更新

N5.1をN5.5にアップグレードすると、vpcインスタンスとOSPが破棄されます。アップグレード手順を開始する前に、vPCコンフィギュレーションファイルとシャーシIDを再利用する必要があります。

ステップ1:chassisidと最後の設定ファイルをバックアップします。

```
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^@
```

注： コンフィギュレーションファイルには、.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
```

ステップ2: Ultra-Mアップグレードの手順

ステップ3：システムのアップグレードとStarOS vpc CFのブートアップが完了したら、chassisid（通常のファイル）とコンフィギュレーションファイル（適切なO&M IPアドレスも変更されていることを確認してください）を**/flash/sftpにコピーしま**す。

ステップ4:「test-command」モードで/flashから隠しデフォルトの.chassisidファイルをバックアップし、削除します。

ステップ5:/flash/sftpから/flashにchassidファイルを隠しモードで「**.chassid」としてコピー**します。 コンフィギュレーションファイルもコピーします

注：派生キー発行cliの*show configuration* url /flash/xxxxxx.cfgを確認できます。 | *more*と、backup configファイルと比較してください

ステップ6：新しい設定ファイルを指すブート優先順位を追加します

注：この時点で、StarOSは次のエラーを表示します。

```
[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
```

正しい手順に従っている場合は、シャーシ派生キーがバックアップ設定ファイルと等しい設定ファイルと、シャーシidがバックアップchassisidと等しい設定ファイルがあります。

chassisidファイルを表示すると、PS1プロンプトが追加されることに注意してください。

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

ステップ7:vPCをリブートする

この時点でシステムがリブートし、バックアップコンフィギュレーションファイルのログインクレデンシャルを使用できます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。