非双方向 HUU（NI-HUU）を使用した Cisco UCS C シリーズ サーバーのファームウェアの更新

概要

非インタラクティブ ホスト アップグレード ユーティリティまたは NI-HUU は、Cisco C シリーズ サーバのファームウェアを更新するために使用されるアプリケーションです。マルチサーバー NI-HUU を使用すると、スクリプトを使用して複数の C シリーズ サーバーを同時に更新できます。この機能を使用するために、Linux 用のツールが用意されています。

前提条件

次のものがインストールされていることを確認します。

1. Python バージョン 3,x
2. Python マルチプロセッシング パッケージ
3. Pycrypto-2.6

Linux ツールとコマンド

これは python ベースのユーティリティです。このユーティリティを使用すると、Linux ホストマシンから複数の C シリーズ サーバを同時に更新できます。ユーティリティの使用方法は次のとおりです。

使用法： `update_firmware.py` *`[options]`*

このユーティリティのパラメータは、コマンドラインまたは構成ファイルから指定できます。

表 *1:* オプション

コマンド	説明
--version	プログラムのバージョン番号を表示し、終了します。
-h, --help	このヘルプメッセージを表示して終了します。

表 *2:* シングル サーバーオプション

コマンド	説明
-a a.b.c.d, --address=a.b.c.d	CIMCのIPアドレス
-u USERNAME、--user=USERNAME	CIMC 管理ユーザーのユーザー名
-p PASSWORD、--password=PASSWORD	CIMC 管理ユーザーのパスワード
-q SKIPMEMORYTEST、--skipMemoryTest=有効/無効	スキップ メモリ テスト機能は、有効または無効にすることができます
-m ucs-c240-huu-146.iso、 --imagefile=ucs-c240-huu-146.iso	HUU iso 画像ファイル名
-i a.b.c.d、--remoteshareip=a.b.c.d	リモート共有の IP アドレス
-d /data/image、--sharedirectory=/data/image	リモート共有内のイメージ ファイルのディレクトリの場所
-t cifs/nfs/www, --sharetype=cifs/nfs/www	リモート共有のタイプ
-r REMOTESHAREUSER、 --remoteshareuser=REMOTESHAREUSER	リモート共有ユーザー名
-w REMOTESHAREPASSWORD、 –remotesharepassword=REMOTESHAREPASSWORD	リモート共有ユーザーのパスワード
-y COMPONENTLIST、 --componentlist=COMPONENTLIST	Component List

コマンド	説明
-f LOGFILE、--logrecordfile=LOGFILE	ログ データを保存するログ ファイル名
-b CIMCSECUREBOOT、 --cimcsecureboot=CIMCSECUREBOOT	CimcSecureBoot を使用します。デフォルトは NO です。オプション yes/no
-k CMCSECUREBOOT、 --cmcsecureboot=CMCSECUREBOOT	CmcSecureBoot を使用します。デフォルトは NO です。オプション yes/no
-M MOUNTOPTION、 --mountOption=MOUNTOPTION	CIFS 共有の場合は、マウント オプションを使用してセキュリティ オプションを指定します。
-R REBOOTCIMC、--reboot=REBOOTCIMC	更新を開始する前に CIMC を再起動します。オプション yes/no
-T UPDATETIMEOUT、 --timeoutalue=UPDATETIMEOUT	更新のタイムアウト値
-o UPDATESTOPONERROR、 --stopOnError=UPDATESTOPONERROR	エラーが発生したときにファームウェアの更新を停止する場合は、このオプションを使用しますか?
-v UPDATEVERIFY、 --updateverify=UPDATEVERIFY	このオプションを使用して、再起動後に更新を確認します
-S USESECURE、--Secure=USESECURE	HTTPS を使用する。デフォルトは yes です。オプション yes/no

表 *3 :* 複数のサーバー更新オプション

コマンド	説明
-c CONFIGFILE, --configfile=CONFIGFILE	CIMC IP アドレスおよびその他のデータのリストを含むファイルの名前
-f LOGFILE、--log=LOGFILE	ログデータが保存されるログファイル名
-s USESECURE、--secure=USESECURE	HTTPS を使用する。デフォルトは yes です。オプション yes/no
-e INFILE、--encrypt=INFILE	公開キー ファイル。
-g、--generatekey	公開キーおよび秘密キーの生成
-j、--displayComponentList	コンポーネントのリストを表示
-V、--Version	バージョンを表示。

構成サンプル

```
#--------------START CNF--------------------------
#
# Use this flag use_http_secure to toggle betwwen https and http protocol
use_http_secure=yes
# Firmware update should complete within this many minutes. This value will be
# sent along with the firmware update XML request to the CIMC
update_timeout=60
graceful_timeout=3
doForceDown=yes
# Should the firmware update process stop the update once an error is encountered?
update_stop_on_error=no
# Is it required to verify the update by rebooting to the same HUU image after the update

# gets completed?
update_verify=no
# Do you wish to secure Cimc Boot.Use this flag use_cimc_secure.
use_cimc_secure=no
# Do you wish to secure Cmc Boot.Use this flag use_cimc_secure.
use_cmc_secure=no
# Feature is used for skip Memory Test and it reduce the boot time. It support Enabled
or
Disabled options.
#skipMemoryTest=Disabled
# List of components to be updated. Check the HUU release note for the list of
# supported components. Multiple components should be comma separated.
update_component=I350
#update_component=9266-8i, BIOS, CIMC, I350
#update_component=all
#update_component=HDD

#update_type=immediate
#update type can be either delay for a delayed firmware update upon host reboot or
immediate,
to start firmware update

#reboot CIMC before Update
reboot_cimc=no
# IP address of the remoted share (cifs/nfs/www) holding the HUU image for booting
# for www share ip address can be given as http://<IPAddr>, https://<IPAddr> or <IPAddr>
remoteshareip=10.104.255.254
# Directory within the share where the HUU image is being kept
sharedirectory=/CIFSShare
# Type of share (nfs/cifs/www)
sharetype=cifs
# Username of the remote share to login to
remoteshareuser=username
# Password corresponding to the remote user
remotesharepassword=password
#Optional mount parameter for CIFS share only. Provide "ntlm,vers=2.0" for CIFS server
version 2.0
(SMB protocol version), default supported version is 3.0
#mountOption=ntlm
#If the running CIMC version is 4.2.2a and above, please provide "ntlmssp or
ntlmv2,vers=2.0".
#mountOption=ntlmv2,vers=2.0 or
#mountOption=ntlmssp,vers=2.0

# Password file for remoteshare. If this option is provided, then the above option
(remotesharepassword) should not be given
#remoteshare_passwordfile=/home/arunven/Python_Script/python_script_old/Pyrhon_loop/CRYPTO/remshare.pass

#Common CIMC password --> The password provided below along with CIMC information will
```

```
be ignored.
#cimc_password_file=/home/arunven/Python_Script/python_script_old/Pyrhon_loop/CRYPTO/cimc.pass


# Enter the list of CIMC ip addresses where the firmware needs to be updated
address=10.104.255.180, user=cimc_user, password=cimc_password, imagefile=huu.iso

#-------------------------END CNF-------------------------
```

これをファイル (例 config.in) に保存し、次のコマンドを使用します。

```
./update_firmware.py -c config.in
```

遅延更新のキャンセル

サーバーファームウェアの更新に使用されたのと同じ構成ファイルを、更新をキャンセルする必要があるすべてのサーバーの詳細とともに渡す必要があります。

（注） ファームウェア更新のキャンセル要求は、ファームウェアの更新が遅延している場合、およびファームウェアの破損を避けるために更新が開始されていない場合にのみ送信されます。

```
./update_firmware.py cancel -c config.in
```

サンプルの設定ファイル multiserver_config も SVN の場所にあります。

このユーティリティは、Python インタープリターが /usr/bin/ にインストールされていることを前提としています。Python インタープリターが他の場所にインストールされている場合、このユーティリティは次のように呼び出すこともできます。

```
./update_firmware.py -c config.in
```

このユーティリティは、構成ファイルに記載されている CIMC に接続し、ホストを記載されている HUU iso で起動します。HUU ISO の起動時に、非対話型の更新を実行する必要があることが検出されます。HUU は更新を完了し、結果を CIMC に送信します。CIMC は、表示されるように python ユーティリティに返信されます。Python ユーティリティ構成ファイルに**検証**オプションも指定されている場合、ホストは HUU で再起動し、検証を完了します。

パスワードの暗号化

秘密キーおよび公開キーの生成

このユーティリティを使用すると、ユーザーは暗号化されたパスワードを生成して使用できるようになります。公開キーと秘密キーを生成するには、**-g** オプションを使用します。

例：

```
./update_firmware.py -c config.in
```

このオプションは、キーのパスフレーズの入力を求めます。パスフレーズを入力しない場合は、**Enter** キーを押します。このコマンドの出力は、次の 2 つのファイルです。

- 秘密キー ファイル—keys.pem
- 公開キー ファイル—keys.pub

暗号化されたパスワードの生成

暗号化されたパスワードを生成するには、**-e** オプションを使用します。これにより、パスフレーズの入力も求められます。キー生成時に提供されたパスフレーズと、暗号化するテキストを入力する必要があります。このTEXTがパスワードです。このコマンドは、暗号化されたパスワードを含むファイルを生成します。オプション **-e** のパラメーターは、公開鍵ファイルです。

例：

```
./update_firmware.py -e keys.pub
```

暗号化されたパスワード ファイル — password.key

名前を変更して保存する必要があります。リモート共有パスワードとCIMCパスワードが互いに異なる場合は、それらに異なる暗号化パスワード ファイルを生成する必要があります。

暗号化されたパスワード ファイルの使用

これらの暗号化されたパスワードを使用できるのは、構成ファイルのみです。設定ファイルには、CIMCおよびリモート共有パスワードに暗号化されたパスワードファイルを提供するために使用できる 2 つのオプションがあります。

- remoteshare_passwordfile=<File Path>
- cimc_password_file=<File Path>

remoteshare のパスワード ファイル — このオプションが指定されている場合、上記のオプションに
remoteshare_passwordfile=/home/arunven/Python_Script/python_script_old/Pyrhon_loop/CRYPTO/remshare.pass
を指定しないでください。

一般的な CIMC パスワード — 以下で提供されるパスワードは無視されます
cimc_password_file=/home/arunven/Python_Script/python_script_old/Pyrhon_loop/CRYPTO/cimc.pass

（注） **cimc_password_file** オプションを使用すると、設定に記載されているすべての CIMC がこの共通ファイルを使用します。

`update_firmware.py` スクリプトを実行して更新を開始すると、鍵の生成中に指定したパスフレーズの入力を求められます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。