H3C S5560X-EI スイッチシリーズ
基本コンフィギュレーションガイド

New H3C Technologies Co., Ltd.
http://www.h3c.com

ソフトウェアバージョン:Release 1118、Release 1118P07
文書バージョン: 6W101-20180821

商標

H3C,,H3CS,H3CIE,H3CNE,Aolynk,,H³Care,,IRF,NetPilot,Netflow,SecEngine,
SecPath,SecCenter,SecBlade,Comware,ITCMM および HUASAN は,New H3C Technologies Co.,Ltd.の商標です。

その他のすべての商標は、各所有権者の財産です。

注意

このドキュメントの情報は、予告なく変更されることがあります。このドキュメントのすべての内容(説明、情報、推奨事項を含む)は正確であると考えられますが、明示的であるか黙示的であるかを問わず、いかなる種類の保証もなく提示されます。H3C は、このドキュメントに含まれる技術的または編集上の誤りや脱落について責任を負いません。

はじめに

このコンフィギュレーションガイドでは、スイッチの導入に役立つ次の機能と作業について説明します。

- CLI。
- RBAC、スイッチログイン、およびスイッチアクセス制御。
- スイッチ、ファイルシステム、コンフィギュレーションファイル、およびライセンスの管理。
- FTP および TFTP。
- Tcl と Python。
- ISSU および共通ソフトウェアアップグレード。
- オートマチックコンフィギュレーション。

ここでは、マニュアルに関する次のトピックについて説明します。

対象者

このマニュアルの対象者:

- ネットワークプランナー。
- フィールドテクニカルサポート/サービス・エンジニア
- S5560X-EI スイッチシリーズを使用するネットワーク管理者

表記法

ここでは、マニュアルで使用されている表記法について説明します。

コマンドの表記法

規約	説明
太字	**太字のテキストは、文字どおりに入力したコマンドとキーワードを示します。**
イタリック体	*斜体のテキストは、実際の値に置き換える引数を表します。*
[ ]	角カッコは、オプションの構文選択(キーワードまたは引数)を囲みます。
{ x | y | ... }	中カッコは、必要な構文の選択肢を縦棒で区切って囲みます。この中から1つを選択します。
[x | y | ...]	角カッコは、オプションの構文選択のセットを縦棒で区切って囲みます。この中から1つまたは何も選択しません。
{ x | y | ... } *	アスタリスクの付いた中括弧は、必須構文の選択肢を縦棒で区切って囲みます。この中から少なくとも1つを選択します。
[x | y | ...] *	アスタリスクの付いた角括弧は、オプションの構文選択肢を縦棒で区切って囲みます。選択肢は1つ、複数、または何も選択しません。
&<1-n>	アンパサンド(&)記号の前の引数またはキーワードと引数の組み合わせは、1～n回入力できます。
#	シャープ記号(#)で始まる行はコメントです。

GUI のルール

規約	説明
太字	ウィンドウ名、ボタン名、フィールド名およびメニュー・アイテムは太字で表示されます。たとえば、New Userウィンドウが開き、OKをクリックします。
>	マルチレベルメニューは、File > Create > Folderのように、山かっこで区切られています。

シンボル

規約	説明
⚠**警告!**	重要な情報を理解していない場合や、その情報に従っていない場合に、けがをするおそれがある場合に注意を促す警告。
△**注意:**	重要な情報が理解されていない場合、または情報が理解されていない場合に、データの損失、データの破損、またはハードウェアやソフトウェアの損傷につながる可能性がある場合に、注意を促す警告。
ⓘ**重要:**	重要な情報への注意を喚起するアラート。
注:	追加情報または補足情報を含むアラート。
ヒント:	役立つ情報を提供するアラート。

ネットワークトポロジーアイコン

規約	説明
	ルーター、スイッチ、ファイアーウォールなどの汎用ネットワークデバイスを表します。
	ルーターまたはレイヤー3スイッチなどのルーティング対応デバイスを表します。
	レイヤー2スイッチやレイヤー3スイッチなどの汎用スイッチ、またはレイヤー2および他のレイヤー2機能をサポートするルーターを表します。
	アクセスコントローラー、Unified Wired-WLANモジュール、またはUnified Wired-WLANスイッチ上のアクセスコントローラエンジンを表します。
	アクセスポイントを表します。
	ワイヤレスターミネータユニットを表します。
	ワイヤレスターミネータを表します。
	メッシュアクセスポイントを表します。
	全方向信号を表します。
	指向性信号を表します。
	ファイアーウォール、UTM、マルチサービス・セキュリティゲートウェイ、ロードバランシングデバイスなどのセキュリティ製品を表します。

規約	説明
	ファイアーウォール、ロードバランシング、NetStream、SSL VPN、IPS、またはACGモジュールなどのセキュリティモジュールを表します。

本書に記載されている例

このドキュメントの例では、ハードウェアモデル、設定、またはソフトウェアバージョンがデバイスと異なるデバイスを使用している場合があります。通常、例のポート番号、サンプル出力、スクリーンショット、およびその他の情報は、デバイスの内容とは異なります。

文書のフィードバック

製品マニュアルに関するコメントは、info@h3c.com まで電子メールでお送りください。

ご意見をお寄せください。

内容

CLI の使用

CLIについて

Command-Line Interface(CLI)でテキストコマンドを入力して、デバイスを設定、管理、および監視できます。

CLIへのログインには、様々な方法を使用できます。たとえば、コンソールポートまたはTelnetを介してログインできます。ログイン方法の詳細は、「ログインの概要」を参照してください。

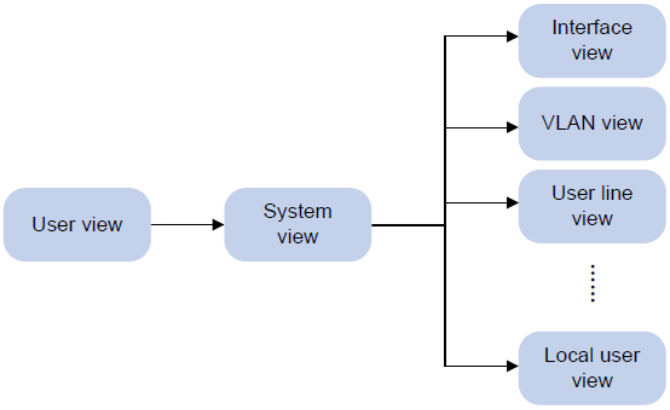
CLIビューの使用

CLI ビューについて

コマンドは、機能ごとに異なるビューにグループ化されます。コマンドを使用するには、そのビューに入る必要があります。

図1に示すように、CLIビューは階層的に編成されています。各ビューには一意のプロンプトがあり、ここから現在の場所と実行可能な操作を識別できます。たとえば、プロンプト[Sysname-vlan100]は、現在VLAN 100ビューにいることを示し、そのVLANの属性を設定できます。

図1 CLIビュー



CLIにログインすると、ただちにユーザービューが表示されます。ユーザービューでは、次のタスクを実行できます。

- 表示、デバッグ、ファイル管理、FTP、Telnet、クロック設定、リブートなどの基本操作を実行します。
- システムビューに入ります。

システムビューでは、次のタスクを実行できます。

- 夏時間、バナー、ホットキーなど、デバイス全体に影響する設定を構成します。
- 機能ビューに入ります。

  たとえば、次のタスクを実行できます:
  - interface ビューに入って、インターフェイスパラメーターを設定します。

- VLAN ビューに入って、ポートをVLANに追加します。
- user line ビューに入って、ログインユーザーアトリビュートを設定します。

機能ビューには子ビューがあります。たとえば、NQA操作ビューには子ビューのHTTP操作ビューがあります。

ビューで使用できるすべてのコマンドを表示するには、ビューのプロンプで疑問符 (?) を入力します。

ユーザービューからシステムビューへ入る

ユーザービューからシステムビューに入るには、次のコマンドを実行します。

system-view

現在のビューから上位レベルのビューに戻る

制限事項とガイドライン

ユーザービューでquitコマンドを実行すると、デバイスへの接続が終了します。

公開鍵ビューからシステムビューに戻るには、peer-public-key end コマンドを使用する必要があります。

手順

ビューから上位レベルのビューに戻るには、次のコマンドを実行します。

quit

ユーザービューに戻る

このタスクについて

この機能を使用すると、1回の操作で任意のビューからユーザービューに戻ることができ、quitコマンドを複数回実行する必要がなくなります。

手順

他のビューからユーザービューに直接戻るには、次のいずれかの方法を使用します。

- 任意のビューで**return**コマンドを実行します。
- 任意のビューで**Ctrl+Z**を押します。

CLIオンラインヘルプへのアクセス

CLIオンラインヘルプは、文脈に依存します。プロンプトまたはコマンドの任意の位置に疑問符を入力すると、使用可能なすべてのオプションが表示されます。

CLIオンラインヘルプにアクセスするには、次のいずれかの方法を使用します。

- ビュープロンプトに疑問符を入力すると、ビューで使用可能なすべてのコマンドの最初のキーワードが表示されます。次に例を示します。

```
<Sysname> ?
```

```
User view commands:
archive          Archive configuration
arp              Address Resolution Protocol (ARP) module
backup           Backup the startup configuration file to a TFTP server
boot-loader      Software image file management
…
```

- コマンドキーワードの後にスペースと疑問符を入力すると、使用可能なキーワードと引数がすべて表示されます。
  - 疑問符がキーワードの場所にある場合、CLIは、可能なすべてのキーワードと簡単な説明を表示します。次に例を示します。

    ```
    <Sysname> terminal ?
      Debugging     Enable to display debugging logs on the current terminal
      Logging       Display logs on the current terminal
      Monitor       Enable to display logs on the current terminal
    ```

  - 疑問符が引数の場所にある場合、CLIは引数の説明を表示します。次に例を示します。

    ```
    <Sysname> system-view
    [Sysname] interface vlan-interface ?
      <1-4094>Vlan-interface interface number

    [Sysname] interface vlan-interface 1 ?
      <cr>
    [Sysname] interface vlan-interface 1
    ```

    <1-4094>は、引数の値の範囲です。**<cr>は、**コマンドが完了し、**Enter**を押してコマンドを実行できることを示します。
- 不完全なキーワード文字列の後に疑問符を入力すると、その文字列で始まるすべてのキーワードが表示されます。CLIには、キーワードの説明も表示されます。次に例を示します。

```
<Sysname> f?
  Fdisk         Partition a storage  medium
  fixdisk       Check and repair a storage medium
  format        Format a storage medium
  Free          Release a connection
  ftp           Open an FTP connection
<Sysname> display ftp?
  ftp           FTP module
  ftp-server    FTP server information
  ftp-user      FTP user information
```

コマンドのundo形式を使う

ほとんどのコンフィギュレーションコマンドには、次の作業を元に戻す形式があります。

- コンフィギュレーションの取り消し。
- デフォルトに戻す。
- 機能の無効化

たとえば、**info-center enable** コマンドはインフォメーションセンターを有効にします。**undo info-center enable** コマンドはインフォメーションセンターを無効にします。

コマンドの入力

コマンドを入力すると、次のタスクを実行できます。

- キーまたはホットキーを使用して、コマンドラインを編集します。
- 省略キーワードまたはキーワードエイリアスを使用します。

コマンドラインの編集

コマンドラインを編集するには、表1に示すキーまたは表4に示すホットキーを使用します。完了したら、Enterを押してコマンドを実行できます。

表1 コマンドライン編集キー

キー	機能
共通キー	編集バッファーがいっぱいでない場合、共通キーを押すとカーソル位置に文字が挿入され、カーソルが右に移動します。編集バッファーには最大511文字を格納できます。バッファーがいっぱいでない場合は、**Enter**を押す前に入力したすべての共通文字が編集バッファーに保存されます。
バックスペース	カーソルの左側の文字を削除し、カーソルを1文字分戻します。
左矢印キー(←)	カーソルを1文字左に移動します。
右矢印キー(→)	カーソルを1文字右に移動します。
上矢印キー(↑)	コマンドヒストリーバッファー内の直前のコマンドを表示します。
下矢印キー(↓)	コマンドヒストリーバッファー内の次のコマンドを表示します。
タブ	キーワードの一部を入力した後に**Tab**キーを押すと、キーワードが自動的に補完されます。 • 一意の一致が見つかると、完全なキーワードが表示されます。 • 一致するキーワードが複数ある場合は、**Tab**を複数回押して、入力するキーワードを選択します。 • 一致するものがない場合、入力した内容は変更されず、次の行に再度表示されます。

デバイスは、次の特殊コマンドをサポートします。

- # - システムがコンフィギュレーションファイル内で、隣接するセクションのセパレータとして使用します。
- **Version** - ソフトウェアバージョン情報を示すために、システムがコンフィギュレーションファイルで使用します。たとえば、**version 7.1. xxx, Release xxx**です。

これらのコマンドは、次の理由により特殊です。

- これらのコマンドは、CLIで使用するためのものではありません。
- 任意のビューで#コマンドを入力するか、システムビューでversionコマンドを入力するか、または値を入力できます。たとえば、# **abc**または**version abc**と入力できます。ただし、設定は有効になりません。
- デバイスは、これらのコマンドのオンラインヘルプ情報を提供しません。

引数のテキストまたは文字列タイプの値の入力

引数text typeには、疑問符(?) 以外の任意の文字を指定できます。

文字列型の引数の値には、以下の文字以外の印刷可能な文字を含めることができます。

- 疑問符（？）。
- クォーテーションマーク (")。
- バックスラッシュ(\)。
- スペース

特定の引数には、より多くの要件がある場合があります。詳細については、関連するコマンドリファレンスを参照してください。

印刷可能な文字を入力するには、文字またはそのASCIIコードを32～126の範囲で入力します。

インターフェイスタイプの入力

インターフェイスタイプは、次のいずれかの形式で入力できます。

- インターフェイスタイプの完全なスペル。
- インターフェイスタイプを一意に識別する略語。
- インターフェイスタイプの頭字語。

コマンドラインでは、すべてのインターフェイスタイプで大文字と小文字が区別されません。表2に、インターフェイスタイプの完全なスペルと略語を示します。

たとえば、**interface**コマンドを使用してインターフェイスGigabitEthernet 1/0/1のビューに入るには、次の形式でコマンドラインを入力します。

- **interface gigabitethernet 1/0/1**
- **interface g 1/0/1**
- **interface ge 1/0/1**

インターフェイスタイプとインターフェイスの間にスペースを入れる必要はありません。

表2 インターフェイスタイプの完全な綴りと頭字語

完全なスペル	略称
Bridge-Aggregation	BAGG
FortyGigE	FGE
GigabitEthernet	GE
InLoopBack	InLoop
LoopBack	Loop
M-GigabitEthernet	MGE
Multicast Tunnel	MTunnel
NULL	NULL
Register-Tunnel	REG
Route-Aggregation	RAGG

Ten-GigabitEthernet	XGE
Tunnel	Tun
Vsi-interface	Vsi
Vlan-interface	Vlan-int

コマンドの省略

完全なコマンドを一意に識別する不完全なキーワードを入力すると、コマンドラインにすばやく入力できます。たとえば、ユーザービューで **s** で始まるコマンドには**startup**が含まれます。

system-view コマンドを入力するには、**sy** だけを入力する必要があります。**startup saved-configuration** コマンドを入力するには、**st s** と入力します。

Tabを押して、不完全なキーワードを入力することもできます。

コマンドエイリアスの設定と使用

このタスクについて

コマンドの1つ以上の別名またはコマンドの開始キーワードを構成できます。その後、別名を使用してコマンドを実行できます。コマンドに**undo**形式がある場合は、別名を使用して**undo**コマンドを実行することもできます。

たとえば、**display ip routing-table** の **shiprt** エイリアスを設定する場合、**shiprt** と入力して **display ip routing-table** コマンドを実行できます。**display ip** の **ship** エイリアスを設定する場合、**ship** を使用して **display ip** で始まるすべてのコマンドを実行できます。次のコマンドがあります。

- **ship routing-table**と入力して、**display ip routing-table**コマンドを実行します。
- **display ip interface**コマンドを実行するには、**ship interface**と入力します。デバイスには、表3

に示すシステム定義のコマンドエイリアスのセットが用意されています。

表3システム定義のコマンドエイリアス

コマンドエイリアス	コマンドまたはコマンドキーワード
access-list	**acl**
end	**return**
erase	**delete**
exit	**quit**
hostname	**sysname**
Logging	**info-center**
No	**undo**
show	**display**
write	**save**

制限事項とガイドライン

コマンドエイリアスは、コマンドの最初のキーワードまたは**undo** 形式のコマンドの2番目のキーワードと

してのみ使用できます。

エイリアスを使用してコマンドを正常に実行すると、エイリアスではなくコマンドが実行コンフィギュレーションに保存されます。

コマンド文字列には、最大 9 つのパラメーターを含めることができます。 各パラメーターは、ドル記号($)と 1～9 の範囲のシーケンス番号で始まります。たとえば、**display ip $ 1 | include $2** のエイリアス **shinc** を構成できます。次に、**display ip routing-table | include Static** コマンドを実行するには、**shinc Routing-table Static** のみを入力する必要があります。

パラメーターを持つコマンドに別名を使用するには、各パラメーターに値を指定する必要があります。指定に失敗すると、コマンドが不完全であることを示すメッセージが表示され、別名で表されるコマンド文字列が表示されます。

システム定義のコマンドエイリアスは削除できません。

手順

1. システムビューに入ります。

   system-view
2. コマンドエイリアスを設定します。

   alias *alias command*

   デフォルトでは、デバイスには表3に示すコマンドエイリアスのセットがあります。
3. (任意)コマンドエイリアスを表示します。

   display alias [*alias*]

   このコマンドは、どのビューでも使用できます。

ホットキーの設定と使用

ホットキーについて

デバイスは一連のホットキーをサポートしています。ホットキーを押すと、そのホットキーに割り当てられたコマンドまたは機能が実行されます。表4にホットキーとそのデフォルト定義を示します。Ctrl+以外のすべてのホットキーを設定できます。

デバイスとの対話に使用しているターミナルソフトウェアによってホットキーも定義されている場合は、ホットキーを再設定するか、ホットキーを削除できます。

制限事項とガイドライン

ホットキーは1つのコマンドまたはファンクションにのみ対応できます。同じホットキーに複数のコマンドまたはファンクションを割り当てると、最後に割り当てられたコマンドまたはファンクションが有効になります。

1つのコマンドまたはファンクションを複数のホットキーに割り当てることができます。任意のホットキーを使用してコマンドまたはファンクションを実行できます。

ホットキーがデバイスとの対話に使用している端末ソフトウェアによっても定義されている場合、端末ソフトウェア定義が有効になります。

手順

1. システムビューに入ります。

   system-view
2. コマンドをホットキーに割り当てます。

hotkey *hotkey* { *command* | **function** *function* | **none** }

表4に、ホットキーのデフォルト定義を示します。

3. (任意)ホットキーを表示します。

display hotkey

このコマンドは、どのビューでも使用できます。

表4 ホットキーのデフォルト定義

ホットキー	機能又はコマンド
Ctrl+A	move_the_cursor_to_the_beginning_of_the_line:カーソルを行の先頭に移動します。
Ctrl+B	move_the_cursor_one_character_to_the_left:カーソルを1文字左に移動します。
Ctrl+C	stop_the_current_command:現在のコマンドを停止します。
Ctrl+D	erase_the_character_at_the_cursor:カーソル位置の文字を削除します。
Ctrl+E	move_the_cursor_to_the_end_of_the_line:カーソルを行末に移動します。
Ctrl+F	move_the_cursor_one_character_to_the_right:カーソルを1文字右に移動します。
Ctrl+G	display current-configuration:稼働中のコンフィギュレーションを表示します。
Ctrl+H	erase_the_character_to_the_left_of_the_cursor:カーソルの左側の文字を削除します。
Ctrl+L	display ip routing-table:IPv4ルーティングテーブル情報を表示します。
Ctrl+N	display_the_next_command_in_the_history_buffer:ヒストリーバッファー内の次のコマンドを表示します。パスワードコンフィギュレーションコマンドがある場合はスキップされます。
Ctrl+O	undo debugging all:すべてのデバッグ機能を無効にします。
Ctrl+P	display_the_previous_command_in_the_history_buffer:ヒストリーバッファー内の直前のコマンドを表示します。パスワードコンフィギュレーションコマンドがある場合はスキップされます。
Ctrl+R	edisplay_the_current_line:現在の行を再表示します。
Ctrl+T	無効
Ctrl+U	無効
Ctrl+W	delete_the_word_to_the_left_of_the_cursor:カーソルの左側の単語を削除します。
Ctrl+X	delete_all_characters_from_the_beginning_of_the_line_to_the_cursor:カーソルの左側にあるすべての文字を削除します。
Ctrl+Y	delete_all_characters_from_the_cursor_to_the_end_of_the_line:カーソルから行末までのすべての文字を削除します。
Ctrl+Z	return_to_the_User_View:ユーザービューに戻ります。
Ctrl+	kill_incoming_connection_or_redirect_connection:現在の接続を終了します。
Esc+B	move_the_cursor_back_one_word:カーソルを1ワード戻します。
Esc+D	delete_all_characters_from_the_cursor_to_the_end_of_the_word:カーソルから単語の末尾までのすべての文字を削除します。

Esc+F	**move_the_cursor_forward_one_word**:カーソルを1ワード分前に移動します。
Esc+N	**move_the_cursor_down_a_line**: カーソルを1行下に移動します。Enterキーを押す前に、このホットキーを使用できます。 このホットキーは、現在のソフトウェアバージョンではサポートされていません。
Esc+P	**move_the_cursor_up_a_line**: カーソルを1行上に移動します。Enterキーを押す前に、このホットキーを使用できます。 このホットキーは、現在のソフトウェアバージョンではサポートされていません。
Esc+<	**move_the_cursor_to_the_beginning_of_the_clipboard**: カーソルをクリップボードの先頭に移動します。 このホットキーは、現在のソフトウェアバージョンではサポートされていません。
Esc+>	**move_the_cursor_to_the_end_of_the_clipboard**: カーソルをクリップボードの端に移動します。 このホットキーは、現在のソフトウェアバージョンではサポートされていません。

入力されたが送信されなかったコマンドの再表示を可能にする

入力されたが送信されなかったコマンドの再表示について

システム情報の出力によって入力が中断されている可能性があります。入力されたが送信されていないコマンドの再表示が有効になっている場合、出力の終了後に入力が再表示されます。その後、コマンドラインへの入力を続行できます。

手順

1. システムビューに入ります。

   system-view

2. 入力されたが送信されていないコマンドの再表示をイネーブルにします。

   info-center synchronous

   デフォルトでは、入力されたが送信されなかったコマンドは再表示されません。

   このコマンドの詳細については、「Network Management and Monitoring Command Reference」を参照してください。

コマンドライン構文エラーメッセージについて

Enterキーを押してコマンドをサブミットすると、コマンドラインインタプリターはコマンド構文を検査します。

- コマンドが構文チェックに合格すると、CLIはコマンドを実行します。
- コマンドが構文チェックに失敗すると、CLIはエラーメッセージを表示します。

表5一般的なコマンドライン構文エラーメッセージ

構文エラーメッセージ	原因
% Unrecognized command found at '^' position.	マークされた位置のキーワードが無効です。
% Incomplete command found at '^' position.	1つまたは複数の必須キーワードまたは引数がありません。

% Ambiguous command found at '^' position.	入力した文字シーケンスは、複数のコマンドに一致します。
% Too many parameters found at '^' position.	入力された文字シーケンスに過剰なキーワードまたは引数が含まれています。
% Wrong parameter found at '^' position.	マークされた位置の引数が無効です。

コマンドヒストリー機能を使う

コマンドヒストリーバッファーについて

システムは、ログインユーザーによって正常に実行されたコマンドを、次の2つのコマンドヒストリーバッファーに自動的に保存します。

- ユーザーラインのコマンドヒストリーバッファー。
- すべてのユーザー行のコマンドヒストリーバッファー。

表6 2種類のコマンドヒストリーバッファーの比較

項目	ユーザー行のコマンドヒストリーバッファー	すべてのユーザー行のコマンドヒストリーバッファー
バッファーに保存されるコマンドはどれですか?	ユーザーラインの現在のユーザーによって正常に実行されたコマンド。	すべてのログインユーザーによってコマンドが正常に実行されました。
バッファー内のコマンドを表示できますか?	はい。	はい。
バッファー内のコマンドを呼び出せますか?	はい。	いいえ。
ユーザーがログアウトすると、バッファーコマンドはクリアされますか。	はい。	いいえ。
サイズは調整可能ですか?	はい。	いいえ。バッファーサイズは1024に固定されています。

コマンドバッファーリングルール

コマンドをバッファーリングする場合、システムは次のルールに従います。

- コマンドの入力時に不完全なキーワードを使用すると、システムは使用した形式とまったく同じ形式でコマンドをバッファーリングします。
- コマンドの入力時にエイリアスを使用すると、コマンドをバッファーリングする前に、エイリアスが表示されたコマンドまたはコマンドキーワードに変換されます。
- 同じ形式のコマンドを連続して複数回入力した場合、システムはコマンドを1回だけバッファーリングします。異なる形式のコマンドを複数回入力した場合、システムは各コマンド形式をバッファーリングします。たとえば、**display cu**と**display current-configuration**は2つのエントリとしてバッファーリングされますが**display cu**はエントリを1つだけ作成します。

- バッファーがいっぱいになったときに新しいコマンドをバッファーリングするために、システムはバッファー内の最も古いコマンドエントリを削除します。

コマンドヒストリーバッファーの管理と使用

コマンドヒストリーバッファー内のコマンドの表示

コマンドヒストリーバッファー内のコマンドを表示するには、任意のビューで次のコマンドを実行します。

- ユーザーラインのコマンドヒストリーバッファー内のコマンドを表示します。

  display history-command

- すべてのユーザーラインのコマンドヒストリーバッファー内のコマンドを表示します。

  display history-command all

ユーザー行のコマンドヒストリーバッファー内のコマンドの呼び出し

上下の矢印キーを使用してコマンドに移動し、Enterを押します。

ユーザー行のコマンドヒストリーバッファーのサイズの設定

ユーザーラインまたはユーザーラインクラスビューで **history-command max-size** コマンドを使用します。詳細は、「基本コマンドリファレンス」を参照してください。

ユーザー行のコマンドヒストリーバッファーでコマンドを繰り返す

ユーザー行のコマンドヒストリーバッファーでコマンドを繰り返すについて

現在のユーザーラインのコマンドヒストリーバッファー内のコマンドを複数回呼び出して実行できます。

制限事項とガイドライン

repeatコマンドはどのビューでも使用できます。ただし、コマンドを繰り返すには、最初にコマンドのビューを入力する必要があります。複数のコマンドを繰り返すには、最初に最初のコマンドのビューを入力する必要があります。

repeatコマンドは、実行された順にコマンドを実行します。

システムはタイマーを開始し、対話型コマンドを繰り返すときにユーザーの対話を待機します。

手順

現在のユーザーラインのコマンドヒストリーバッファーでコマンドを繰り返すには、次のコマンドを実行します。

repeat [*number*] [**count** *times*] [**delay** *seconds* **]**

CLI出力の制御

この項では、目的の出力を識別するのに役立つCLI出力制御機能について説明します。

出力画面間の一時停止

このタスクについて

出力が長すぎて1画面に収まらない場合、デバイスは特定の行数を表示した後に自動的に一時停止できます。一時停止すると、デバイスは**----more----**と表示されます。表7に示すキーを使用すると、詳細情報を表示したり、表示を停止したりできます。

現在のセッションの出力画面間の一時停止を無効にすることもできます。その後、すべての出力が一度に表示され、最終画面が表示されるまで画面が継続的にリフレッシュされます。

表7 出力制御キー

キー	作用
スペース	次の画面を表示します。
Enter	次の行を表示します。
Ctrl+C	表示を停止し、コマンドの実行をキャンセルします。
<PageUp>	前ページを表示します。
<PageDown>	次のページを表示します。

出力画面間の一時停止を無効にする

出力画面間の一時停止を無効にするには、ユーザービューで次のコマンドを実行します。

screen-length disable

デフォルトは、ユーザーラインビューの**screen-length**コマンドの設定によって異なります。**screen-length**コマンドのデフォルト設定は次のとおりです。

- 出力画面間の一時停止が有効になります。
- 一度に表示される最大行数は24です。

screen-length コマンドの詳細は、「基本コマンドリファレンス」を参照してください。

このコマンドは1回限りのコマンドであり、現在のCLIセッションでのみ有効です。

表示コマンドからの各出力行の番号付け

このタスクについて

簡単に識別できるように、**by-linenum**オプションを使用して、**display**コマンドの出力行ごとに番号を表示できます。

各行番号は5文字の文字列として表示され、その後にコロン(:)またはハイフン(-)が続く場合があります。**display**コマンドに**| by-linenum**と**begin** *regular-expression*の両方を指定すると、正規表現と一致しないすべての行にハイフンが表示されます。

手順

表示コマンドから各出力行に番号を付けるには、任意のビューで次のコマンドを実行します。

display *command* **| by-linenum**

例

#VLAN 999に関する情報を表示し、各出力行に番号を付けます。

<Sysname> display vlan 999 | by-linenum

1: VLAN ID: 999

2: VLAN type: Static

3: Route interface: Configured

4: IPv4 address: 192.168.2.1

5: IPv4 subnet mask: 255.255.255.0

6: Description: For LAN Access

7: Name: VLAN 0999

8: Tagged ports: None

9: Untagged ports: None

display コマンドからの出力をフィルターする

このタスクについて

display コマンドからの出力をフィルタリングするには、**|** { **begin** | **exclude** | **include** } *regular-expression* オプションを使用します。

- **Begin** - 指定した正規表現に一致する最初の行と、それ以降のすべての行を表示します。
- **Exclude** - 指定した正規表現に一致しないすべての行を表示します。
- **Include** - 指定した正規表現に一致するすべての行を表示します。
- *regular-expression* - 大文字と小文字が区別される1～256文字列。表8で説明する特殊文字を含めることができます。

表8 正規表現でサポートされる特殊文字

文字	意味	実施例
^	行の先頭に一致します。	「^u」は、"u"で始まるすべての行に一致します。"Au"で始まる行は一致しません。
$	行の末尾に一致します。	"u$"は、"u"で終わるすべての行に一致します。"uA"で終わる行は一致しません。
.(ピリオド)	任意の1文字に一致します。	".s"は"as"および"bs"に一致します。
*	直前の文字または文字列0、1、または複数回に一致します。	"zo*"は"z"と"zoo"に一致し、"(zo)*"は"zo"と"zozo"に一致します。
+	直前の文字または文字列に1回または複数回一致します。	"zo+"は"zo"と"zoo"に一致しますが、"z"には一致しません。
|	前後の文字列に一致します。	"def int"は、"def"または"int"を含む行に一致します。
( )	括弧内の文字列に一致します。通常、プラス記号(+)またはアスタリスク記号(*)と一緒に使用されます。	"(123A)"は"123A"に一致します。 "408(12)+"は"40812"および"408121212"に一致しますが、"408"ではありません。

\N	括弧内の前の文字列に一致し、N番目の文字列が1回繰り返されます。	"(string)\1"は、"stringstring"を含む文字列に一致します。 "(string1)(string2)\2"は、"string1string2string2"を含む文字列に一致します。 "(string1)(string2)\1\2"は、"string1string2string1string2"を含む文字列に一致します。
[ ]	括弧内の1文字と一致します。	"[16A]"は1、6、またはAを含む文字列に一致し、"[1-36A]"は1、2、3、6、またはA (-はハイフン)を含む文字列に一致します。 文字"]"を一致させるには、"["の直後に入力します。例えば、[ ]abc])。"["にはこのような制限はありません。
[^]	括弧内にない1文字と一致します。	"[^16A]"は、"abc"など、1、6、またはA以外の1つ以上の文字を含む文字列に一致します。一致には、1、6、またはA("m16"など)を含めることもできますが、これら3つの文字(1、16、または16Aなど)のみを含めることはできません。
{n}	直前の文字にn回一致します。数値nは負でない整数である必要があります。	"o{2}"は"food"に一致しますが、"Bob"には一致しません。
{n,}	直前の文字にn回以上一致します。数値nは負でない整数である必要があります。	"o{2,}"は"foooood"に一致しますが、"Bob"には一致しません。
{n,m}	直前の文字nからm回以上に一致します。数値nとmは負でない整数である必要があり、nはmより大きくできません。	"o{1,3}"は"fod"、"food"、"foooood"に一致しますが、"fd"には一致しません。
\<	\<の後のパターンで始まる文字列に一致します。パターンの前の文字が数字、文字、アンダースコアでない場合は、パターンを含む文字列にも一致します。	"\<do"は"domain"と"doa"に一致します。
\>	\>の前のパターンで終わる文字列に一致します。パターンの後の文字が数字、文字、アンダースコアでない場合、パターンを含む文字列も一致します。	"do\>"は"undo"と"cdo"に一致します。
\b	\bの後のパターンで始まる単語、または\bの前のパターンで終わる単語に一致します。	"er\b"は"never"に一致しますが、"verb"や"erase"には一致しません。"\ber"は"erase"に一致しますが、"verb"や"never"には一致しません。
\B	パターンを含むが、パターンで開始または終了していない単語に一致します。	"er\B"は"verb"に一致しますが、"never"や"erase"には一致しません。
\w	[A-Za-z0-9_]と同じで、数字、文字、またはアンダースコアに一致します。	"v\w"は"vlan"と"service"に一致します。
\W	[^A-Za-z0-9_]と同じで、数字、文字、アンダースコア以外の文字に一致します。	"\Wa"は"-a"に一致しますが、"2a"または"ba"には一致しません。

\	エスケープ文字。この表に記載されている特殊文字が\の後に続く場合、その文字の特定の意味は削除されます。	"\\"は"\"、"\^"は"^"を含む文字列、"\\b"は"\b"を含む文字列に一致します。

制限事項とガイドライン

必要なフィルタリング時間は、正規表現が複雑になるほど長くなります。フィルタリング処理を中止するには、**Ctrl+C**キーを押します。

例

#実行コンフィギュレーションを、行を含む最初のコンフィギュレーション行から表示します。

```
<Sysname> display current-configuration | begin line

line class aux
 user-role network-admin
 #
line class vty
 user-role network-operator
 #
line aux 0
 user-role network-admin
 #
line vty 0 63
 authentication-mode none
 user-role network-admin
 user-role network-operator
#
...
```

#アップ状態のインターフェイスに関する簡単な情報を表示します。

```
<Sysname> display interface brief | exclude DOWN

Brief information on interfaces in route mode:

Link: ADM - administratively down; Stby – standby

Protocol: (s) - spoofing
Interface              Link Protocol      Primary IP
                       Description
InLoop0                UP   UP(s)         --
NULL0                  UP   UP(s)         --
Vlan1                  UP   UP            192.168.1.83
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby – standby

Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F – full
Type: A - access; T - trunk; H - hybrid
Interface              Link Speed         Duplex Type PVID Description
WGE1/0/1               UP   100M(a)       F(a)   A    1
```

SNMP関連の実行コンフィギュレーションラインを表示します。

<Sysname> display current-configuration | include snmp

snmp-agent
 snmp-agent community write private
 snmp-agent community read public
 snmp-agent sys-info version all
 snmp-agent target-host trap address udp-domain 192.168.1.26 params securityname public

displayコマンドの出力をファイルに保存する

displayコマンド出力保存について

dispalyコマンドは、デバイスの特定の構成および操作情報を表示します。その出力は、時間の経過やユーザーの構成または操作によって異なる場合があります。将来の検索またはトラブルシューティングのために、出力をファイルに保存できます。

displayコマンドの出力を保存するには、次のいずれかの方法を使用します。

- 出力を別のファイルに保存します。1つの**display**コマンドに1つのファイルを使用する場合は、この方法を使用します。
- 出力をファイルの最後に追加します。 1つのファイルを複数の**display**コマンドに使用する場合は、この方法を使用します。

手順

displayコマンドの出力をファイルに保存するには、任意のビューで次のいずれかのコマンドを使用します。

- **display**コマンドの出力を別のファイルに保存します。

  display *command* **>** *filename*
- **display**コマンドの出力をファイルの末尾に追加します。

  display *command* **>>** *filename*

例

#VLAN1の設定を**vlan.tx**tという名前の別のファイルに保存します。

<Sysname> display vlan 1 > vlan.txt

#VLAN1の設定が**vlan.txt**ファイルに保存されていることを確認します。

<Sysname> more vlan.txt
VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:None
 Untagged ports: None

#**vlan.txt**ファイルの最後にVLAN999設定を追加します。

<Sysname> display vlan 999 >> vlan.txt

#VLAN999の設定が**vlan.txt**ファイルの末尾に追加されていることを確認します。

<Sysname> more vlan.txt
VLAN ID: 1
 VLAN type: Static

Route interface: Not configured
Description: VLAN 0001
Name: VLAN 0001
Tagged ports:None
Untagged ports: None

VLAN ID: 999
VLAN type: Static
Route interface: Configured
IP address: 192.168.2.1
Subnet mask: 255.255.255.0
Description: For LAN Access
Name: VLAN 0999
Tagged ports:None
Untagged ports: None

displayコマンドの出力を効果的に表示および管理する

次の方法を組み合わせて使用すると、ディスプレイからの出力をフィルタリングおよび管理できます。
コマンド:

- 表示コマンドからの各出力行の番号付け
- 表示コマンドからの出力のフィルタリング
- 表示コマンドの出力をファイルに保存する

手順

複数のメジャーを使用して**display**コマンドの出力を効率的に表示および管理するには、任意のビューで次のコマンドを実行します。

Display *command* [**|** [**by-linenum**] { **begin | exclude | include }** *regular-expression] [> filename* | *>> filename]*

例

#実行コンフィギュレーションを**test.txt**という名前の別のファイルに保存し、各行に番号を付けます。

<Sysname> display current-configuration | by-linenum > test.txt

#実行コンフィギュレーションの**snmp**を含む行を**test.txt**ファイルに追加します。

<Sysname> display current-configuration | include snmp >> test.txt

#実行コンフィギュレーションの**user-group**で始まる最初の行と、それに続くすべての行を表示します。

<Sysname> display current-configuration | by-linenum begin user-group

114: user-group system
115- #
116- return

//行番号に続くコロン(:)は、その行にuser-groupという文字列が含まれていることを示します。行番号に続くハイフン(-)は、その行にuser-groupという文字列が含まれていないことを示します。

RBAC の設定

RBACについて

Role-Based Access Control(RBAC)はユーザーの役割に基づいてユーザーのアクセス許可を制御します。

RBACは、異なるジョブ機能用に作成されたユーザー役割にアクセス許可を割り当てます。ユーザーには、ユーザーのユーザー役割に基づいて、一連のアイテムとリソースにアクセスするためのアクセス許可が与えられます。アクセス許可をユーザーから分離すると、簡単なアクセス許可の承認管理が可能になります。

権限の割り当て

ユーザーロールに権限を割り当てるには、次の方法を使用します。

- ユーザーロールのアクセス可能またはアクセス不可能なアイテムを決定する一連のルールを定義します(「ユーザーロールルール」を参照)。
- リソースアクセスポリシーを構成して、ユーザーロールからアクセス可能なリソースを指定します(「リソースアクセスポリシー」を参照)。

システムリソースに関連するコマンドを使用するには、ユーザーロールがコマンドとリソースの両方にアクセスできる必要があります。

たとえば、ユーザーロールは**vlan**コマンドにアクセスでき、VLAN 10だけにアクセスできます。ユーザーロールが割り当てられている場合、**vlan**コマンドを使用してVLAN 10を作成し、そのビューに入れます。ただし、他のVLANは作成できません。ユーザーロールがVLAN 10にアクセスできても、**vlan**コマンドにアクセスできない場合、コマンドを使用してVLAN 10のビューに入れません。

ユーザーが任意のユーザーロールを使用してデバイスにログインし、ビューに<?>を入力すると、ビューのシステム定義コマンド別名のヘルプ情報が表示されます。ただし、ユーザーにはコマンド別名にアクセスする権限がない場合があります。ユーザーがコマンド別名にアクセスできるかどうかは、別名に対応するコマンドに対するユーザーロールの権限によって異なります。コマンド別名の詳細は、「CLIの使用」を参照してください。

任意のユーザーロールでデバイスにログインするユーザーは、**system-view**、**quit**、および **exit** コマンドにアクセスできます。

ユーザーロールルール

ユーザーロールルールは、コマンド、XML要素、またはMIBノードなどの項目へのアクセスを許可または拒否します。アクセス制御の権限ごとに、次のタイプのルールを定義できます。

- **Commandルール** - 正規表現に一致するコマンドまたはコマンドセットへのアクセスを制御します。
- **機能ルール** - 機能のコマンドへのアクセスをコマンドタイプ別にコントロールします。
- **機能グループルール** - 機能グループ内の機能のコマンドへのアクセスをコマンドタイプ別にコントロールします。
- **XML エレメントルール** - デバイスの設定に使用されるXMLエレメントへのアクセスを制御します。
- **OIDルール** - MIBノードおよびその子ノードへのSNMPアクセスを制御します。OIDは、ルートノードからリーフノードへのパスを一意に識別するドット付き数値文字列です。

項目(コマンド、XML要素、およびMIBノード)は、次のタイプに基づいて制御されます。

- **Read** - 構成および保守情報を表示する項目。たとえば**display**コマンドと**dir**コマンド。
- **Write** - システムの機能を設定する項目。たとえば、**info-center enable**コマンドや**debugging**コマンドなどです。
- **Execute** - 特定の機能を実行する項目。たとえば、**ping**コマンドと**ftp**コマンド。

ユーザーロールは、ユーザーロールルールで指定された許可されたアイテムのセットにアクセスできます。ユーザーロールルールには、事前定義済(*sys-n*で識別)およびユーザー定義のユーザーロールルールが含まれます。ユーザーロールルールの優先度の詳細は、「ユーザーロールルールの構成」を参照してください。

リソースアクセポリシー

リソースアクセスポリシーは、システムリソースへのユーザーロールのアクセスを制御します。次のタイプがあります。

- **Interface**ポリシー - インターフェイスへのアクセスを制御します。
- **VLAN**ポリシー - VLANへのアクセスを制御します。
- **VPN instance**ポリシー - VPNインスタンスへのアクセスを制御します。

リソースアクセスポリシーは、**display**コマンドのインターフェイス、VPNインスタンス、またはVLANオプションへのアクセスを制御しません。オプションが任意のユーザーロールルールで許可されている場合は、**display**コマンドでこれらのオプションを指定できます。

定義済みのユーザーロール

システムには、事前定義済のユーザーロールが用意されています。これらのユーザーロールは、すべてのシステムリソースにアクセスできます。ただし、表9に示すように、アクセス権限は異なります。

事前定義されたすべてのユーザーロールの中で、ローカルユーザーおよびローカルユーザーグループを作成、変更および削除できるのは、network-adminおよびlevel-15のみです。他のユーザーロールは、ローカルユーザーおよびローカルユーザーグループを構成する権限がある場合にのみ、独自のパスワードを変更できます。

レベル0からレベル14のユーザーロールのアクセス権は、ユーザーロールルールおよびリソースアクセスポリシーを使用して変更できます。ただし、これらのユーザーロールの事前定義済のアクセス権は変更できません。たとえば、これらのユーザーロールのアクセス権を**display history-command all**コマンドに変更することはできません。

表9 定義済みの役割と権限のマトリックス

ユーザーロール名	使用許可
network-admin	**display security-logfile summary**、**info-center security-logfile directory**、および**security-logfile save**コマンドを除く、システム内のすべての機能およびリソースにアクセスします。
network-operator	• システム内の機能およびリソースの**display**コマンドにアクセスします。ユーザーロールのアクセス可能なコマンドをすべて表示するには、**display role**コマンドを使用します。 • ローカル認証ログインユーザーが自分のパスワードを変更できるようにします。 • XMLビューの入力に使用するコマンドにアクセスします。 • すべての読み取り型XML要素にアクセスします。 • すべての読み取りタイプMIBノードにアクセスします。

レベル-n(n=0～15)	• **Level-0** - **ping**、**tracert**、**ssh2**、**telne**t、**mtrace**、**super**などのコマンドにアクセスできます。レベル0のアクセス権は設定可能です。 • **level-1** - システム内の機能およびリソースの**display**コマンドにアクセスできます。**level-1**ユーザーrロールには、level-0ユーザーロールのすべてのアクセス権も付与されます。level-1アクセス権は設定可能です。 • **level-2**から**level-8**、および**level-10**から**level-14 -** デフォルトでは、アクセス権はありません。アクセス権は構成可能です。 • **level-9** - システムのほとんどの機能およびリソースにアクセスできます。レベル9のユーザーロールを持つローカルユーザーアカウントでログインしている場合は、ローカルユーザーアカウントのパスワードを変更できます。 次に、レベル9ユーザーロールがアクセスできない主な機能とコマンドを示します。 ○ RBAC non-debuggingコマンド。 ○ ローカルユーザー。 ○ ファイル管理。 ○ デバイス管理。 ○ **display history-command all**コマンド。 ● **level-15** - network-adminと同じ権限を持ちます。
security-audit	セキュリティログマネージャ。ユーザーロールには、セキュリティログファイルへの次のアクセス権があります。 • セキュリティログファイルを表示および維持するためのコマンド**(dir**、**display security-logfile summary**と**more**などのコマンド)にアクセスします。 • セキュリティログファイルおよびセキュリティログファイルシステムを管理するためのコマンド(たとえば、**info-center security-logfile directory**, **mkdir**, と **security-logfile save**コマンド)にアクセスします。 セキュリティログ管理の詳細については、『ネットワーク管理および監視構成ガイド』を参照してください。ファイルシステム管理の詳細は、「ファイルシステムの管理」を参照してください。 重要: security-auditユーザーロールだけがセキュリティログファイルにアクセスできます。security-auditユーザーロールを非AAA認証ユーザーに割り当てることはできません。

ユーザーロールの割り当て

ユーザーにアクセス権を割り当てるには、少なくとも1つのユーザーロールを割り当てます。ユーザーは、ユーザーに割り当てられたすべてのユーザーロールにアクセス可能なアイテムおよびリソースのコレクションを使用できます。たとえば、次のユーザーロールが割り当てられている場合は、**qos apply policy**コマンドを使用するために任意のインターフェイスにアクセスできます。

- ユーザーロールAは**qos apply policy**コマンドへのアクセスを拒否し、interface GigabitEthernet 1/0/1へのアクセスだけを許可します。
- ユーザーロールBは、**qos apply policy**コマンドおよびすべてのインターフェイスへのアクセスを

許可します。

認証方式に応じて、ユーザーロール割り当てには次の方式があります。

- **AAA authorization** - AAA許可スキーム認証が使用される場合、AAAモジュールはユー

ザーロール割り当てを処理します。

- ユーザーがローカル認証に合格すると、デバイスはローカルユーザーアカウントで指定されたユーザーロールを割り当てます。
- ユーザーがリモート認証に合格すると、リモートAAAサーバーはサーバー上で指定されたユーザーロールを割り当てます。AAAサーバーには、RADIUSサーバーまたはHWTACACSサーバーを指定できます。

- **非AAA authorization** - ユーザーが認証なしで、またはユーザー回線でパスワード認証を渡すことによってデバイスにアクセスする場合、デバイスはユーザー回線で指定されたユーザーロールを割り当てます。この方式は、publickeyまたはpassword-publickey認証を使用するSSHクライアントにも適用されます。これらのSSHクライアントに割り当てられるユーザーロールは、それぞれのデバイス管理ユーザーアカウントで指定されます。

AAAおよびSSHの詳細については、『Security Configuration Guide』を参照してください。ユーザー回線の詳細については、「ログインの概要」および「CLIログインの設定」を参照してください。

FIPS準拠

デバイスは、**NIST FIPS140 - 2**要件に準拠するFIPSモードをサポートしています。機能、コマンド、およびパラメーターのサポートは、FIPSモードと非FIPSモードで異なる場合があります。FIPSモードの詳細については、Security Configuration Guideを参照してください。

RBACのタスクの概要

RBACを設定するには、以下のタスクを実行してください。

1. ユーザーロールの作成
2. ユーザーロールルールの設定
3. (任意)機能グループの設定
4. リソースアクセスポリシーの構成
   - ユーザーロールインターフェイスポリシーの設定
   - ユーザーロールVLANポリシーの設定
   - ユーザーロールVPNインスタンスポリシーの設定
5. ユーザーロールの割り当て
   - デフォルトユーザーロール機能のイネーブル化
   - リモートAAA認証ユーザーへのユーザーロールの割り当て
   - ローカルAAA認証ユーザーへのユーザーロールの割り当て
   - ユーザー回線上の非AAA認証ユーザーへのユーザーロールの割り当て
6. 一時的なユーザーロール許可の設定
   a. 一時ユーザー役割許可の認証モードの設定
   b. 一時ユーザー役割許可のデフォルトのターゲットユーザー役割の指定
   c. 一時的なユーザー役割許可の認証パスワードの設定
   d. (任意)一時的なユーザーロール認可のためのログインユーザー名の自動取得
   e. 一時的なユーザー役割許可の取得

ユーザーロールの作成

このタスクについて

事前定義されたユーザーロールに加えて、詳細なアクセス制御用に最大64のカスタムユーザーロールを作成できます。

手順

1. システムビューに入ります。

   system-view

2. ユーザーロールを作成し、そのビューに入ります。

   role name *role-name*

   デフォルトでは、システムには次の定義済みユーザーロールがあります。

   - network-admin
   - network-operator
   - level-n(nは0～15の整数)
   - security-audit

   これらのユーザーロールのうち、レベル0～レベル14のユーザーロールの権限と説明だけが設定可能です。

3. (任意)ユーザーロールの説明を設定します。

   description *text*

   デフォルトでは、ユーザーロールには説明がありません。

ユーザーロールルールの設定

ユーザーロールルールについて

特定のコマンド、XML要素、およびMIBノードへのユーザーロールのアクセスを許可または拒否するユーザーロールルールを設定できます。

非OIDルールには、次のガイドラインが適用されます。

- 同じタイプの2つのユーザー定義ルールが競合する場合、より高いIDを持つルールが有効になります。たとえば、ユーザーロールに次のコマンドを使用して構成されたルールが含まれている場合、ユーザーロールは**tracert**コマンドを使用できますが、**ping**コマンドは使用できません。
  - **rule** *1* **permit command** *ping*
  - **rule** *2* **permit command** *tracert*
  - **rule** *3* **deny command** *ping*
- 定義済みのユーザーロールルールとユーザー定義のユーザーロールルールが競合する場合、ユーザー定義のユーザーロールルールが有効になります。

OIDルールには、次のガイドラインが適用されます。

- システムは、OIDをユーザーロールルールで指定されたOIDと比較し、最長一致原則を使用してOIDのルールを選択します。たとえば、ユーザーロールに次のコマンドを使用して設定されたルールが含まれている場合、ユーザーロールはOIDが1.3.6.1.4.1.25506.141.3.0.1のMIBノードにアクセスできません。
  - **rule** *1* **permit read write oid** *1.3.6*
  - **rule** *2* **deny read write oid** *1.3.6.1.4.1*

- **rule** *3* **permit read write oid** *1.3.6.1.4*

- 同じOIDが複数のルールで指定されている場合、より高いIDを持つルールが有効になります。たとえば、ユーザーロールに次のコマンドを使用して設定されたルールが含まれている場合、ユーザーロールはOIDが1.3.6.1.4.1.25506.141.3.0.1のMIBノードにアクセスできます。
  - **rule** *1* **permit read write oid** *1.3.6*
  - **rule** *2* **deny read write oid** *1.3.6.1.4.1*
  - **rule** *3* **permit read write oid** *1.3.6.1.4.1*

制限事項とガイドライン

- 次のコマンドにアクセスできるのは、network-adminおよびlevel-15ユーザーロールだけです。
  - **display history-command all**コマンド。
  - startupで始まるすべてのコマンド**display role**、**display license**、**reboot**、**startup saved-configuration**、**undo saved-configuration**キーワード。
  - システムビューで**role**、**undo role**、**super**、**undo super**、**password-recovery**、および**undo password-recovery** キーワードで始まるすべてのコマンド。
  - システムビューで**snmp-agent community**、**undo snmp-agent community**、**snmp-agent usm-user**、**undo snmp-agent usm-user**、**snmp-agent group**、および**undo snmp-agent group** キーワードで始まるすべてのコマンド。
  - ユーザーラインビューまたはユーザーラインクラスビューで**user-role**、**undo user-role**、**authentication-mode**、**undo authentication-mode**、**set authentication password**、および**undo set authentication password** キーワードで始まるすべてのコマンド。
  - スケジュールビューまたはCLI定義ポリシービューで、**user-role**および**undo user-role** キーワードで始まるすべてのコマンド。
  - イベントMIB機能のすべてのコマンド。
- 1つのユーザーロールに対して最大256のユーザー定義ルールを設定できます。ユーザー定義ユーザーロールルールの総数は1024を超えることはできません。
- ユーザーロールに対するルールの変更、追加、または削除は、変更後にそのユーザーロールでログインしているユーザーに対してだけ有効になります。

手順

1. システムビューに入ります。

   system-view

2. ユーザーロールビューに入ります。

   role name *role-name*

3. ユーザーロールのルールを設定します。必要に応じて設定するオプションを選択します。
   - コマンドルールを設定します。

     rule *number* { **deny | permit** } **command** *command-string*
   - 機能 ルールを設定します。

     rule *numbe*r { **deny | permit** } { **execute | read | write } * feature** [*feature-name*]
   - 機能グループルールを設定します。

     rule *number* { **deny** | **permit** } { **execute** | **read** | **write** } * **feature-group** *feature-group-name*

     機能グループルールは、機能グループが作成された後にだけ有効になります。
   - XMLエレメントルールを設定します。

rule *number* { **deny** | **permit** } { **execute** | **read** | **write** } * **xml-element** [*xml-string*]

- OIDルールを設定します。

  rule *number* { **deny** | **permit** } { **execute** | **read** | **write** } ***oid** *oid-string*

機能グループの設定

このタスクについて

機能グループを使用して、コマンドアクセス権限を機能セットに一括で割り当てることができます。定義済みの機能グループに加えて、最大64個のカスタム機能グループを作成し、1つの機能を複数の機能グループに割り当てることができます。

手順

1. システムビューに入ります。

   system-view
2. 機能グループを作成し、そのビューに入ります。

   role feature-group name *feature-group-name*

   デフォルトでは、システムには次の定義済みフューチャーグループがあり、削除または修正できません。

   - **L2 -** すべてのレイヤー2コマンドが含まれます。
   - **L3 -** すべてのレイヤー3コマンドが含まれます。
3. 機能グループに機能を追加します。

   feature *feature-name*

   デフォルトでは、機能グループには機能がありません。

リソースアクセスポリシーの構成

リソースアクセスポリシーについて

すべてのユーザーロールには、1つのインターフェイスポリシー、VPNインスタンスポリシー、およびVLANポリシーがあります。デフォルトでは、これらのポリシーにより、ユーザーロールが任意のシステムリソースにアクセスできるようになります。任意のリソースへのアクセスを制限するように、ユーザー定義のユーザーロールまたは定義済みのレベルnユーザーロールのポリシーを設定できます。

リソースアクセスポリシー構成の制約事項およびガイドライン

ポリシー設定は、設定後にユーザーロールでログインしたユーザーにだけ有効です。

ユーザーロールインターフェイスポリシーの設定

1. システムビューに入ります。

   system-view
2. ユーザーロールビューに入ります。

role name *role-name*

3. ユーザーロールインターフェイスポリシービューを開始します。

   interface policy deny

   デフォルトでは、ユーザーロールのインターフェイスポリシーは、すべてのインターフェイスへのアクセスを許可します。

   もし、**permit interface**コマンドがコンフィギュレーションされていなければ、このコマンドは、すべてのインターフェイスへのユーザーロールのアクセスを拒否します。

4. (任意)ユーザーロールがアクセスできるインターフェイスのリストを指定します。

   permit interface *interface-list*

   デフォルトでは、ユーザーロールインターフェイスポリシービュー可能なインターフェイスはデフォルトで設定されていません。複数のアクセス可能なインターフェイスを追加するには、この手順を繰り返します。

ユーザーロール VLAN ポリシーの設定

1. システムビューに入ります。

   system-view

2. ユーザーロールビューに入ります。

   role name *role-name*

3. ユーザーロールVLANポリシービューに入ります。

   vlan policy deny

   デフォルトでは、ユーザーロールのVLANポリシーはすべてのVLANへのアクセスを許可します。

   permit vlanコマンドが設定されていない場合、このコマンドはすべてのVLANへのユーザーロールのアクセスを拒否します。

4. (任意)ユーザーロールがアクセスできるVLANのリストを指定します。

   permit vlan *vlan-id-list*

   デフォルトでは、ユーザーロールVLANポリシービューにアクセス可能なVLANは設定されていません。複数のアクセス可能なVLANを追加するには、この手順を繰り返します。

ユーザーロール VPN インスタンスポリシーの設定

1. システムビューに入ります。

   system-view

2. ユーザーロールビューに入ります。

   role name *role-name*

3. ユーザーロールVPNインスタンスポリシービューに入ります。

   Vlan-instance policy deny

   デフォルトでは、ユーザーロールのVPNインスタンスポリシーは、すべてのVPNインスタンスへのアクセスを許可します。

   permit vpn-instanceコマンドが設定されていない場合、このコマンドはすべてのVPNインスタンスへのユーザーロールのアクセスを拒否します。

4. (任意)ユーザーロールがアクセスできるVPNインスタンスのリストを指定します。

permit vpn-instance *vpn-instance-name*&<1-10>

デフォルトでは、ユーザーロールVPNインスタンスポリシービューでは、アクセス可能なVPNインスタンスは設定されません。複数のアクセス可能なVPNインスタンスを追加するには、この手順を繰り返します。

ユーザーロールの割り当て

ユーザーロール割り当てに関する制約事項とガイドライン

システムへのユーザーアクセスを制御するには、少なくとも1つのユーザーロールを割り当てる必要があります。サーバーによって割り当てられたユーザーロールのうち、少なくとも1つのユーザーロールがデバイス上に存在することを確認してください。

デフォルトユーザーロール機能の有効化

デフォルトユーザーロール機能について

デフォルトユーザーロール機能は、認証サーバー(ローカルまたはリモート)がユーザーにユーザーロールを割り当てない場合、AAA認証ユーザーにデフォルトユーザーロールを割り当てます。これらのユーザーは、デフォルトユーザーロールでシステムにアクセスできます。

システムに存在する任意のユーザーロールをデフォルトユーザーロールとして指定できます。

手順

1. システムビューに入ります。

   system-view

2. デフォルトユーザーロール機能を有効にします。

   role default-role enable [*role-name*]

   デフォルトでは、デフォルトユーザーロール機能は無効です。

   authorization-attribute user role コマンドを使用してユーザーロールをローカルユーザーに割り当てない場合は、デフォルトのユーザーロール機能をイネーブルにする必要があります。**authorization-attribute user role** コマンドの詳細については、『Security Command Reference』の「AAA commands」を参照してください。

リモート AAA 認証ユーザーへのユーザーロールの割り当て

リモートAAA認証ユーザーの場合、ユーザーロールはリモート認証サーバーで設定されます。RADIUSユーザーのユーザーロールの設定の詳細については、RADIUSサーバーのマニュアルを参照してください。HWTACACSユーザーの場合、ロール設定でroles="role-1role-2…role-n"形式を使用する必要があります。この場合、ユーザーロールはスペースで区切られます。たとえば、roles="level-0level-1level-2"を設定して、HWTACACSユーザーにlevel-0、level-1、およびlevel-2を割り当てます。

AAAサーバーがsecurity-auditユーザーロールと他のユーザーロールを同じユーザーに割り当てた場合、security-auditユーザーロールだけが有効になります。

ローカル AAA 認証ユーザーへのユーザーロールの割り当て

ローカル AAA 認証ユーザーへのユーザーロールの割り当てについて

ローカルユーザーカウントでローカルAAA認証ユーザーのユーザーロールを設定します。AAAおよびローカルユーザーの設定の詳細については、『Security Configuration Guide』の「AAA configuration」を参照してください。

制限事項とガイドライン

- すべてのローカルユーザーにはデフォルトのユーザーロールがあります。このデフォルトのユーザーロールが適切でない場合は削除してください。
- ローカルユーザーがsecurity-auditユーザーロールを持つ唯一のユーザーである場合、そのユーザーは削除できません。
- security-auditユーザーロールは、他のユーザーロールと相互に排他的です。
  - security-auditユーザーロールをローカルユーザーに割り当てると、システムはユーザーから他のすべてのユーザーロールを削除する確認を要求します。
  - security-auditユーザーロールを持つローカルユーザーに他のユーザーロールを割り当てると、システムはユーザーからsecurity-auditロールを削除する確認を要求します。
- ローカルユーザーには最大64のユーザーロールを割り当てることができます。

手順

1. システムビューに入ります。

   system-view
2. ローカルユーザーを作成し、そのビューに入ります。

   local-user *user-name* **class** { **manage** | **network** }
3. ローカルユーザーにユーザーロールを割り当てます。

   authorization-attribute user-role *role-name*

   デフォルトでは、network-operatorユーザーロールは、network-adminまたはlevel-15ユーザーによって作成されたローカルユーザーに割り当てられます。

ユーザー回線上の非 AAA 認証ユーザーへのユーザーロールの割り当て

ユーザー回線上の非 AAA 認証ユーザーへのユーザーロールの割り当てについて

ユーザー行で、次の2つのタイプのログインユーザーのユーザーロールを指定します。

- パスワード認証を使用するか、認証を使用しない非SSHユーザー。
- publickeyまたはpassword-publickey認証を使用するSSHクライアント。これらのSSHクライアントに割り当てられたユーザーロールは、それぞれのデバイス管理ユーザーカウントで指定されます。

ユーザー回線の詳細については、「ログインの概要」および「CLIログインの設定」を参照してください。SSHの詳細については、Security Configuration Guideを参照してください。

制限事項とガイドライン

- ユーザー回線上の非AAA認証ユーザーには、最大64のユーザーロールを割り当てることができます。
- ユーザー回線上の非AAA認証ユーザーにsecurity-auditユーザーロールを割り当てることはできませ

ん。

手順

1. システムビューに入ります。

   system-view

2. ユーザーラインビューまたはユーザーラインクラスビューに入ります。
   - ユーザーラインビューに入ります。

     line { *first-num1* [*last-num1*] | { **aux** | **vty** } *first-num2* [*last-num2*] }
   - ユーザーラインクラスビューに入ります。

     line class { **aux** | **vty** }

     ユーザーラインビューおよびユーザーラインクラスビューの設定の優先順位および適用範囲については、「CLIログインの設定」を参照してください。

3. ユーザー回線でユーザーロールを指定します。

   user-role *role-name*

   デフォルトでは、network-adminユーザーロールはAUXユーザー回線で指定され、network-operatorユーザーロールは他のユーザー回線で指定されます。

一時的なユーザーロール許可の設定

一時ユーザーロール許可について

一時的なユーザーロール認可を使用すると、デバイスに再接続せずに別のユーザーロールを取得できます。この機能は、ユーザーロールを一時的に使用して機能を設定する場合に便利です。

一時的なユーザーロールの承認は、現在のログインでのみ有効です。この機能では、でログインしたユーザーアカウントのユーザーロール設定は変更されません。次回、ユーザーアカウントでログインすると、元のユーザーロール設定が有効になります。

ユーザーがデバイスに再接続せずに別のユーザーロールを取得できるようにするには、ユーザーロール認証を設定する必要があります。表10に、使用可能な認証モードと設定要件を示します。

表10ユーザーロール認証モード

キーワード	認証モード	説明
local	ローカルパスワード認証のみ(local-only)	デバイスは、ローカルに設定されたパスワードを認証に使用します。 このモードでユーザーロールにローカルパスワードが設定されていない場合、AUXユーザーは文字列を入力するか、何も入力せずにユーザーロールを取得できます。

scheme	HWTACACSまたはRADIUSによるリモートAaa認証 (リモートのみ)	デバイスは、ユーザー名とパスワードをHWTACACSまたはRADIUSサーバーに送信してリモート認証を行います。 このモードを使用するには、以下の設定タスクを実行する必要があります。 • 必要なHWTACACSスキームまたはRADIUSスキームを構成し、ユーザーのスキームを使用するようにISPドメインを構成します。詳細については、「セキュリティ構成ガイド」を参照してください。 • HWTACACSまたはRADIUSサーバーにユーザーカウントとパスワードを追加します。
local scheme	最初にローカルパスワード認証、次にリモートAAA認証 (local-then-remote)	ローカルパスワード認証が最初に実行されます。 このモードでユーザーロールにローカルパスワードが設定されていない場合: • デバイスは、VTYユーザーのリモートAAA認証を実行します。 • AUXユーザーは、文字列を入力するか、何も入力しないことで、別のユーザーロールを取得できます。
scheme local	最初にリモートAAA認証、次にローカルパスワード認証 (リモートからローカルへ)	リモートAAA認証が最初に実行されます。 ローカルパスワード認証は、次のいずれかの状況で実行されます。 • HWTACACSまたはRADIUSサーバーが応答しない。 • デバイスのリモートAAA設定が無効です。

一時的なユーザーロール認可の制約事項およびガイドライン

HWTACACS認証を使用する場合は、次のルールが適用されます。

- デバイスが認証ユーザー名としてログインユーザー名を自動的に取得するように有効になっていない場合、ロール認証を要求するにはユーザー名を入力する必要があります。
- デデバイスは、ユーザー名またはユーザー名@ドメイン名の形式でユーザー名をサーバーに送信します。ドメイン名がユーザー名に含まれるかどうかは、HWTACACSスキームの**user-name-format**コマンドによって異なります。
- レベルnユーザーロールを取得するには、サーバー上のユーザーアカウントにターゲットユーザーロールレベルまたはターゲットユーザーロールより高いレベルが必要です。レベルnユーザーロールを取得するユーザーアカウントは、レベル0～レベルnの任意のユーザーロールを取得できます。
- 非レベルnユーザーロールを取得するには、サーバー上のユーザーカウントが次の要件を満たしていることを確認します。
  - アカウントにはユーザー権限レベルがあります。
  - HWTACACSのカスタム属性は、次の形式で設定されます。**allowed-roles="***role***"**。変数roleはターゲットユーザーロールを表します。

RADIUS認証を使用する場合は、次のルールが適用されます。

- デバイスは、入力したユーザー名または自動的に取得されたログインユーザー名を使用して、ユーザーロール認証を要求しません。**$ enab***n* **$**形式のユーザー名を使用します。変数nはユーザーの役割レベルを表し、ドメイン名はユーザー名に含まれていません。パスワードが正しい場合は、いつでもユーザーロール認証に合格できます。
- レベルnユーザーロールを取得するには、RADIUSサーバーでレベルnユーザーロールのユーザーアカウントを**$ enabn $**形式で作成する必要があります。変数nは、ターゲットユーザーの役割レベルを表します。たとえば、レベル3のユーザーロールの承認を取得するには、任意のユーザー名を入力できます。デ

バイスはユーザー名**$ enab3 $**を使用して、サーバーにユーザーロール認証を要求します。

- 非レベルnユーザーロールを取得するには、次の作業を実行する必要があります。
  - サーバー上に**$enab0$**という名前のユーザーアカウントを作成します。
  - アカウントのcisco-av-pairアトリビュートを**allowed-roles="***role***"**の形式で設定します。変数roleはターゲットユーザーロールを表します。

デバイスは、ユーザーロール認証用の認証ドメインを次の順序で選択します。

1. 入力したユーザー名に含まれるISPドメイン。
2. デフォルトのISPドメイン。

ユーザーロール認可の取得後に**quit**コマンドを実行すると、デバイスからログアウトされます。

一時ユーザーロール許可の認証モードの設定

1. システムビューに入ります。

   system-view
2. 認証モードを設定します。

   s**uper authentication-mode** { **local** | **scheme** }*

   デフォルトでは、local-only認証が適用されます。

一時ユーザーロール許可のデフォルトのターゲットユーザーロールの指定

1. システムビューに入ります。

   system-view
2. 一時ユーザーロール認可のデフォルトターゲットユーザーロールを指定します。

   super default role *role-name*

   デフォルトでは、デフォルトのターゲットユーザーロールはnetwork-adminです。

一時的なユーザーロール許可の認証パスワードの設定

認証パスワードについて

認証パスワードは、ローカルパスワード認証にのみ必要です。

手順

1. システムビューに入ります。

   system-view
2. ユーザーロールのローカル認証パスワードを設定します。

   非FIPSモードの場合:

   super password [**role** *role-name*] [{ **hash** | **simple** } *string*]

   FIPSモードの場合:

super password [role *role-name* **]**

デフォルトでは、パスワードは設定されていません。

role *role-name*オプションを指定しない場合、コマンドはデフォルトのターゲットユーザーロールのパスワードを設定します。

一時的なユーザーロール認可のためのログインユーザー名の自動取得

一時的なユーザーロール許可のためのログインユーザー名の自動取得について

この機能は、スキーム認証を使用するユーザー回線からのログインにだけ適用されます。スキーム認証では、ログインにユーザー名が必要です。この機能を使用すると、ログインユーザーがリモート認証サーバーから一時的なユーザーロール認可を要求したときに、デバイスが自動的にログインユーザー名を取得できます。

制限事項とガイドライン

ユーザーがパスワード認証を使用するユーザー回線からログインした場合、または認証を使用しないユーザー回線からログインした場合、デバイスはログインユーザー名を取得できません。リモート認証サーバーからの一時的なユーザーロール認可の要求は失敗します。

この機能は、一時的なユーザーロール認可のためのローカルパスワード認証では有効になりません。

手順

1. システムビューに入ります。

   system-view

2. ログインユーザーがリモート認証サーバーから一時的なユーザーロール認可を要求したときに、デバイスが自動的にログインユーザー名を取得できるようにします。

   super use-login-username

   デフォルトでは、ログインユーザーがリモート認証サーバーから一時的なユーザーロール認可を要求すると、デバイスはユーザー名の入力を要求します。

一時的なユーザーロール許可の取得

制限事項とガイドライン

一時的なユーザーロール認可を取得する操作は、認証試行が連続して3回失敗すると失敗します。

前提条件

一時的なユーザーロール認可を取得する前に、現在のユーザーアカウントに、一時的なユーザーロール認可を取得するための**super**コマンドを実行する権限があることを確認します。

手順

ユーザーロールを使用するための一時的な認可を取得するには、ユーザービューで次のコマンドを実行します。

super [*role-name*]

role-name引数を指定しない場合、一時的なユーザーロール認可のデフォルトターゲットユーザーロールが取得されます。

RBACの表示および保守コマンド

任意のビューで表示コマンドを実行します。

タスク	コマンド
ユーザーロール情報を表示します。	**display role** [**name** *role-name*]
ユーザーロール機能情報を表示します。	**display role feature** [**name** *feature-name*| **verbose**]
ユーザーロール機能グループ情報を表示します。	**display role feature-group** [**name** *feature-group-name*] [**verbose**]

RBACの設定例

例:ローカル AAA 認証ユーザー用の RBAC の設定

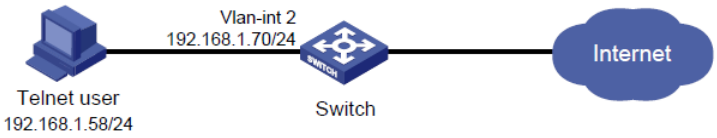
ネットワークの設定

図2に示すように、スイッチはTelnetユーザーに対してローカルAAA認証を実行します。Telnetユーザーのユーザーアカウントは**user1@bbb**でロール**role1**が割り当てられています。

role1に次の権限を設定します。

- 任意の機能の読み取りコマンドを実行します。
- VLAN 10～20にアクセスします。他のVLANへのアクセスは拒否されます。

図2ネットワーク図



手順

#VLAN-interface2(Telnetユーザーに接続されたインターフェイス)にIPアドレスを割り当てます。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0

[Switch-Vlan-interface2] quit

#Telnetサーバーを有効にします。

[Switch] telnet server enable

#Telnetユーザーのユーザー回線でスキーム認証をイネーブルにします。

[Switch] line vty 0 63

[Switch-line-vty0-63] authentication-mode scheme

[Switch-line-vty0-63] quit

#ISPドメインbbbのローカル認証と認可を有効にします。

[Switch] domain bbb

[Switch-isp-bbb] authentication login local

[Switch-isp-bbb] authorization login local

[Switch-isp-bbb] quit

#role1という名前のユーザーロールを作成します。

[Switch] role name role1

#ユーザーロールがすべての機能の読み取りコマンドにアクセスできるように、ルール1を設定します。

[Switch-role-role1] rule 1 permit read feature

#ユーザーロールがVLANを作成し、VLANビューでコマンドにアクセスできるように、ルール2を設定します。

[Switch-role-role1] rule 2 permit command system-view ; vlan *

#ユーザーロールがVLAN 10～20だけを設定できるように、VLANポリシーを変更します。

[Switch-role-role1] vlan policy deny

[Switch-role-role1-vlanpolicy] permit vlan 10 to 20

[Switch-role-role1-vlanpolicy] quit

[Switch-role-role1] quit

#user1という名前のデバイス管理ユーザーを作成し、ローカルユーザービューに入ります。

[Switch] local-user user1 class manage

#ユーザーに対して **abbcc** のプレーンテキストパスワードを設定します。

[Switch-luser-manage-user1] password simple aabbcc

#サービスタイプを **Telnet** に設定します。

[Switch-luser-manage-user1] service-type telnet

#ユーザーにrole1を割り当てます。

[Switch-luser-manage-user1] authorization-attribute user-role role1

#ユーザーからデフォルトのユーザーロール(**network-operator**)を削除します。この操作により、ユーザーには**role1**の権限のみが付与されます。

[Switch-luser-manage-user1] undo authorization-attribute user-role network-operator

[Switch-luser-manage-user1] quit

コンフィギュレーションの検証

#スイッチにTelnet接続し、スイッチにアクセスするためのユーザー名とパスワードを入力します(詳細は省略します)。

#VLAN 10～20を作成できることを確認します。この例では、VLAN 10を使用しています。

<Switch> system-view

[Switch] vlan 10

[Switch-vlan10] quit

#VLAN 10～20以外のVLANを作成できないことを確認します。この例では、VLAN 30を使用しています。

[Switch] vlan 30

Permission denied.

#任意の機能のすべての読み取りコマンドを使用できることを確認します。この例では、表示クロックを使用します。

[Switch] display clock

09:31:56.258 UTC Sun 01/01/2017

[Switch] quit

#任意の機能のwriteまたはexecuteコマンドを使用できないことを確認します。

<Switch> debugging role all

Permission denied.

<Switch> ping 192.168.1.58

Permission denied.

例:RADIUS 認証ユーザー用の RBAC の設定

ネットワークの設定

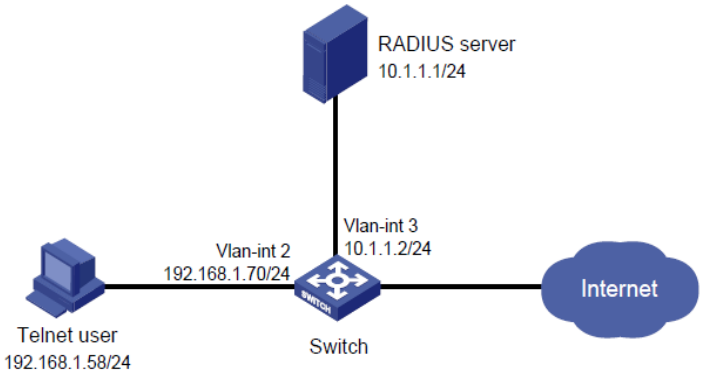
図3に示すように、スイッチはFreeRADIUSサーバーを使用して、Telnetユーザーを含むログインユーザーにAAAサービスを提供します。Telnetユーザーのユーザーアカウントは**hello@bbb**で、ユーザーロール**role2**が割り当てられています。

ユーザーロールrole2には、次の権限があります。

- ISPドメインビューのすべてのコマンドを使用します。
- **arp**および**radius**機能のreadおよびwriteコマンドを使用します。
- **acl**機能のreadコマンドにアクセスできません。
- VLAN 1～20およびインターフェイス GigabitEthernet 1/0/1～GigabitEthernet 1/0/4を設定します。他のVLANおよびインターフェイスへのアクセスは拒否されます。

スイッチとFreeRADIUSサーバーは、**expert**および認証ポート**1812**の共有キーを使用します。スイッチは、ドメイン名ともにユーザー名をサーバーに配信します。

図3 ネットワーク図



手順

スイッチとRADIUSサーバーの設定が一致していることを確認します。

1. スイッチを設定します。

   #VLAN-interface2に、Telnetユーザーと同じサブネットのIPアドレスを割り当てます。

   <Switch> system-view

   [Switch] interface vlan-interface 2

[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0

[Switch-Vlan-interface2] quit

#VLAN-interface3に、RADIUSサーバーと同じサブネットのIPアドレスを割り当てます。

[Switch] interface vlan-interface 3

[Switch-Vlan-interface3] ip address 10.1.1.2 255.255.255.0

[Switch-Vlan-interface3] quit

#Telnetサーバーを有効にします。

[Switch] telnet server enable

#Telnetユーザーのユーザー回線でスキーム認証をイネーブルにします。

[Switch] line vty 0 63

[Switch-line-vty0-63] authentication-mode scheme

[Switch-line-vty0-63] quit

#RADIUSスキーム**rad**を作成し、RADIUSスキームビューに入ります。

[Switch] radius scheme rad

#スキームのプライマリサーバードレスとサービスポートを指定します。

[Switch-radius-rad] primary authentication 10.1.1.1 1812

#スイッチがサーバーに対して認証するスキームで、共有キーを**expert**に設定します。

[Switch-radius-rad] key authentication simple expert

[Switch-radius-rad] quit

#ISPドメイン**bbb**の認証および認可スキームとしてスキーム **rad**を指定します。
ログインユーザーのアカウンティングを実行しないようにISPドメインを設定します。

ⓘ重要:

RADIUSユーザー認可情報は認証応答にピギーバックされるため、認証方式と認可方式は同じRADIUSスキームを使用する必要があります。

[Switch] domain bbb

[Switch-isp-bbb] authentication login radius-scheme rad

[Switch-isp-bbb] authorization login radius-scheme rad

[Switch-isp-bbb] accounting login none

[Switch-isp-bbb] quit

機能グループ**fgroup1**を作成します。

[Switch] role feature-group name fgroup1

#**arp**および**radius**機能を機能グループに追加します。

[Switch-featuregrp-fgroup1] feature arp

[Switch-featuregrp-fgroup1] feature radius

[Switch-featuregrp-fgroup1] quit

#ユーザーロール**role2**を作成します。

[Switch] role name role2

#ユーザーロールがISPドメインビューで使用できるすべてのコマンドを使用できるように、ルール1を構成します。

[Switch-role-role2] rule 1 permit command system-view ; domain *

#ルール2を設定して、ユーザーロールが**fgroup1**のすべての機能の読み取りおよび書き込みコマ

ンドを使用できるようにします。

[Switch-role-role2] rule 2 permit read write feature-group fgroup1

＃ルール 3を構成して、**acl** 機能の読み取りコマンドへのアクセスを無効にします。

[Switch-role-role2] rule 3 deny read feature acl

#ユーザーロールがVLANを作成し、VLANビューで使用可能なすべてのコマンドを使用できるように、ルール4を設定します。

[Switch-role-role2] rule 4 permit command system-view ; vlan *

#ユーザーロールがインターフェイスビューに入り、インターフェイスビューで使用できるすべてのコマンドを使用できるように、ルール5を設定します。

[Switch-role-role2] rule 5 permit command system-view ; interface *

#ユーザーロールVLANポリシーを設定して、VLAN 1～20以外のVLANの設定を無効にします。

[Switch-role-role2] vlan policy deny

[Switch-role-role2-vlanpolicy] permit vlan 1 to 20

[Switch-role-role2-vlanpolicy] quit

#ユーザーロールインターフェイスポリシーを設定して、GigabitEthernet 1/0/1～GigabitEthernet 1/0/4以外のインターフェイスの設定を無効にします。

[Switch-role-role2] interface policy deny

[Switch-role-role2-ifpolicy] permit interface gigabitethernet 1/0/1 to gigabitethernet 1/0/4

[Switch-role-role2-ifpolicy] quit

[Switch-role-role2] quit

2. RADIUSサーバーを設定します。

#ユーザーロール属性のいずれかをFreeRADIUSサーバーのディクショナリファイルに追加します。

Cisco-AVPair = "shell:roles=\"role2\""

Cisco-AVPair = "shell:roles*\"role2\""

#FreeRADIUSサーバーがスイッチと通信するために必要な設定を行います。
(詳細は省略します)。

コンフィギュレーションの検証

#スイッチにTelnet接続し、スイッチにアクセスするためのユーザー名とパスワードを入力します(詳細は省略します)。

#ISPドメインビューで使用できるすべてのコマンドを使用できることを確認します。

<Switch> system-view

[Switch] domain abc

[Switch-isp-abc] authentication login radius-scheme abc

[Switch-isp-abc] quit

#**radius**および**arp**機能のすべてのreadおよびwriteコマンドを使用できることを確認します。この例では**radius**を使用します。

[Switch] radius scheme rad

[Switch-radius-rad] primary authentication 2.2.2.2

[Switch-radius-rad] display radius scheme rad

...

#VLAN 1～20以外のVLANを設定できないことを確認します。この例では、VLAN 10およびVLAN 30を使用してい

ます。

[Switch] vlan 10

[Switch-vlan10] quit

[Switch] vlan 30

Permission denied.

#GigabitEthernet 1/0/1からGigabitEthernet 1/0/4以外のインターフェイスを設定できないことを確認します。この例では、GigabitEthernet 1/0/2とGigabitEthernet 1/0/5を使用します。

[Switch] vlan 10

[Switch-vlan10] port gigabitethernet 1/0/2

[Switch-vlan10] port gigabitethernet 1/0/5

Permission denied.

例:RBAC 一時ユーザーロール許可(HWTACACS 認証)の設定

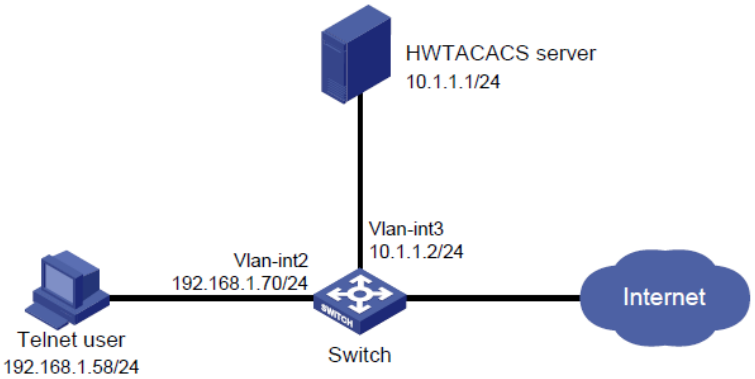
ネットワークの設定

図4に示すように、スイッチはTelnetユーザーを含むログインユーザーにローカル認証を使用します。

Telnetユーザーのユーザーアカウントは**test @ bbb**で、ユーザーロール**level-0**が割り当てられています。

一時的なユーザーロール認証用にリモート、次にローカル認証モードを構成します。スイッチはHWTACACSサーバーを使用して、**level-0**から**level-3**の間でユーザーのロールを変更したり、ユーザーのロール**をnetwork-admin**に変更したりするための認証を提供します。AAA設定が無効であるか、HWTACACSサーバーが応答しない場合、スイッチはローカル認証を実行します。

図4ネットワーク図



手順

1. スイッチを設定します。

   #VLAN-interface2(Telnetユーザーに接続されたインターフェイス)にIPアドレスを割り当てます。

   <Switch> system-view

   [Switch] interface vlan-interface 2

   [Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0

   [Switch-Vlan-interface2] quit

   #VLAN-interface 3 (HWTACACSサーバーに接続されているインターフェイス)にIPアドレスを割り当てます。

   [Switch] interface vlan-interface 3

[Switch-Vlan-interface3] ip address 10.1.1.2 255.255.255.0

[Switch-Vlan-interface3] quit
#Telnetサーバーを有効にします。

[Switch] telnet server enable

#Telnetユーザーのユーザー回線でスキーム認証をイネーブルにします。

[Switch] line vty 0 15

[Switch-line-vty0-15] authentication-mode scheme

[Switch-line-vty0-15] quit
#一時的なユーザーロール認可のために、リモートからローカルへの認証をイネーブルにします。

[Switch] super authentication-mode scheme local

#**hwta**cという名前のHWTACACSスキームを作成し、HWTACACSスキームビューに入ります。

[Switch] hwtacacs scheme hwtac

#スキーム内のプライマリ認証サーバードレスとサービスポートを指定します。

[Switch-hwtacacs-hwtac] primary authentication 10.1.1.1 49

#スキーム内の許可サーバードレスとサービスポートを指定します。

[Switch-hwtacacs-hwtac] primary authorization 10.1.1.1 49

#スイッチが認証サーバーに対して認証するためのスキームで、共有キーを**expert**に設定します。

[Switch-hwtacacs-hwtac] key authentication simple expert

#HWTACACSサーバーに送信されるユーザー名からISPドメイン名を除外します。

[Switch-hwtacacs-hwtac] user-name-format without-domain

[Switch-hwtacacs-hwtac] quit
#ISPドメイン**bbb**を作成し、ISPドメインビューに入ります。

[Switch] domain bbb

#ログインユーザーのローカル認証にISPドメイン**bbb**を設定します。

[Switch-isp-bbb] authentication login local

#ログインユーザーのローカル権限にISPドメイン**bbb**を設定します。

[Switch-isp-bbb] authorization login local

#ユーザーロール認証のために、ISPドメインにHWTACACSスキーム**hwtac**を適用します。

[Switch-isp-bbb] authentication super hwtacacs-scheme hwtac

[Switch-isp-bbb] quit

 # test という名前のデバイス管理ユーザーを作成し、ローカルユーザービューに入ります。
[Switch] local-user test class manage
ユーザーサービスタイプを**Telnet**に設定します。
[Switch-luser-manage-test] service-type telnet
ユーザーパスワードを**aabbcc**に設定します。
[Switch-luser-manage-test] password simple aabbcc
level-0 をユーザーに割り当てます。
[Switch-luser-manage-test] authorization-attribute user-role level-0
デフォルトユーザーロール (**network-operator**)を削除します。
[Switch-luser-manage-test] undo authorization-attribute user-role network-operator
[Switch-luser-manage-test] quit
#ユーザーロール**Level 3**のローカル認証パスワードを**654321**に設定します。

[Switch] super password role level-3 simple 654321

#ユーザーロールnetwork-adminのローカル認証パスワードを**654321**に設定します。

[Switch] super password role network-admin simple 654321

[Switch] quit

2. HWTACACSサーバーを設定します。

   次に、ACSv4.0を使用する例を示します。

   a. **User Setup**ページにアクセスします。

   b. **test**という名前のユーザーアカウントを追加します(詳細は省略します)。

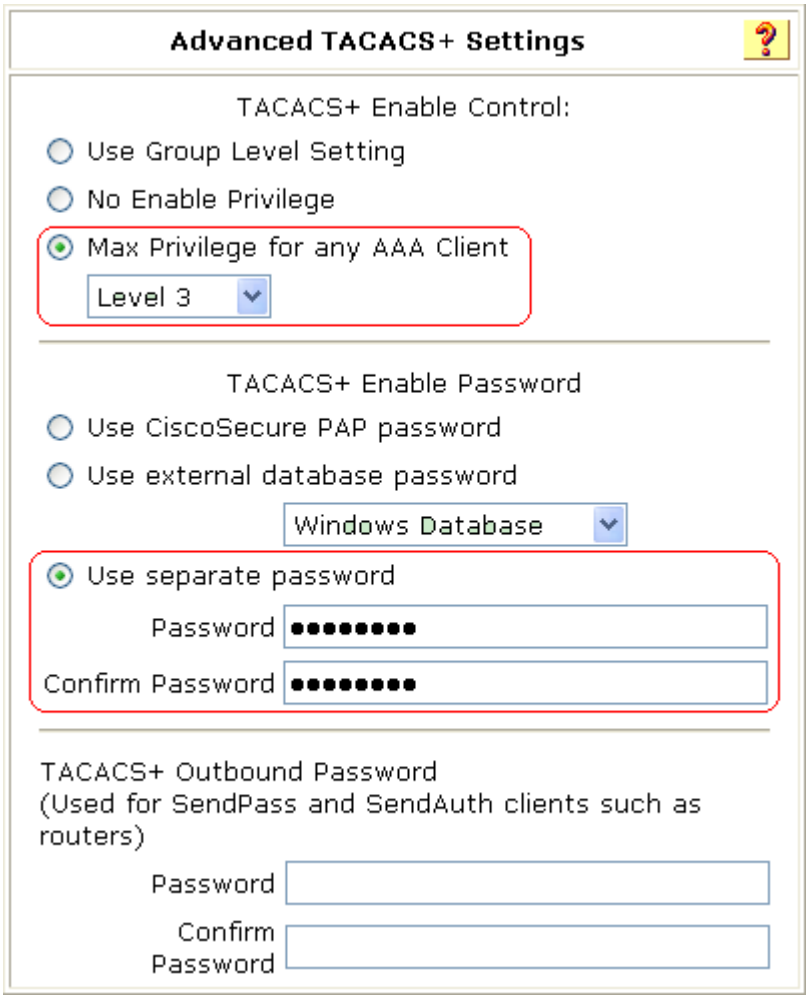
   c. **Advanced TACACS+Settings**領域で、次のパラメーターを設定します。

      - **Max Privilege for any AAA Client**オプションで**Level 3**を選択します。

        ターゲットユーザーロールが一時的なユーザーロール認可の**network-admin**だけの場合、オプションの任意のレベルを選択できます。

      - **Use separate password**オプションを選択し、パスワードとして**enabpass**を指定します。

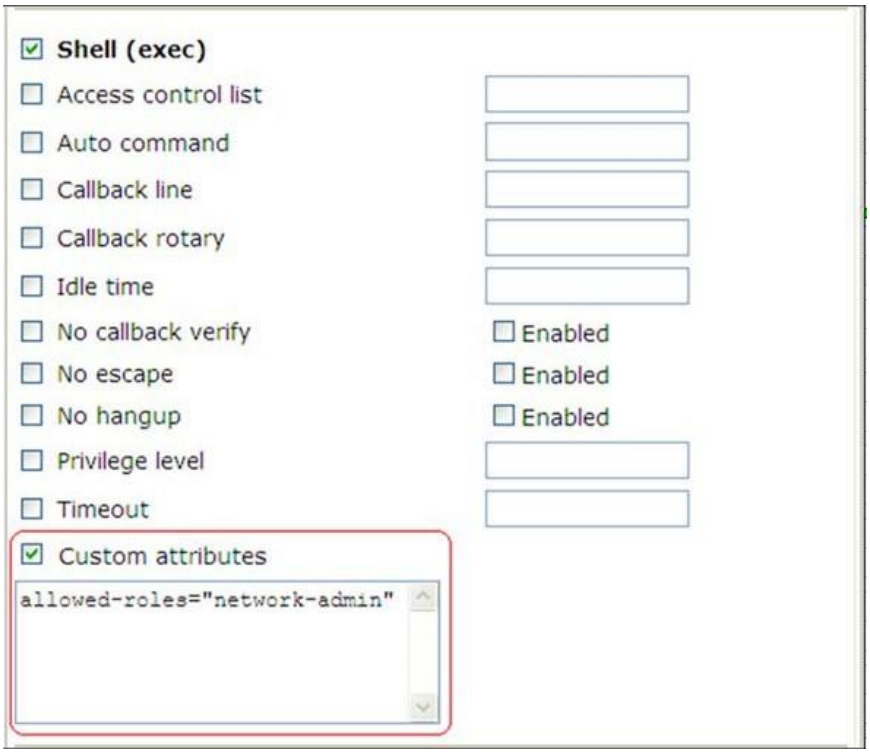
図5 TACACS+の詳細設定



   d. **Shell(exec)**と**Custom attribute**を選択し、**Custom attributes**フィールドに**allowed-roles="network-admin"**と入力します。

      許可されるロールを区切るには、空白を使用します。

図6 Telnetユーザーのカスタム属性の設定



コンフィギュレーションの検証

1. スイッチにTelnet接続し、ユーザー名を **test@bb**bとパスワードを**abbbcc**と入力してスイッチにアクセスします。診断コマンドにアクセスできることを確認します。

```
<Switch> telnet 192.168.1.70
Trying 192.168.1.70 ...
Press CTRL+K to abort

Connected to 192.168.1.70 ...

******************************************************************************
*  Copyright (c) 2004-2019 Hewlett Packard Enterprise Development LP*
*  Without the owner's prior written consent,*
*  no decompiling or reverse-engineering shall be allowed.*
******************************************************************************

login: test@bbb

Password:
<Switch>?
User view commands:
  ping          Ping function
  quit          Exit from current command view
  ssh2          Establish a secure shell client connection super
                Switch to a user role
  system-view   Enter the System View
  telnet        Establish a telnet connection
  tracert       Tracert function
```

<Switch>

2. レベル3ユーザーロールを取得できることを確認します。

   #スーパーパスワードを使用して、レベル3のユーザーロールを取得します。ユーザー名とパスワードの入力を求めるプロンプトが表示されたら、ユーザー名を**test@bbb**およびパスワードを**enabpass**と入力します。

   <Switch> super level-3

   Username: test@bbb

   Password:

   次の出力は、レベル3ユーザーロールを取得したことを示しています。

   User privilege role is level-3, and only those commands that authorized to the role can be used.

   #ACSサーバーが応答しない場合は、プロンプトでローカル認証パスワード**654321**を入力します。

   Invalid configuration or no response from the authentication server. Change authentication mode to local.

   Password:

   User privilege role is level-3, and only those commands that authorized to the role can be used.

   出力は、レベル3ユーザーロールを取得したことを示しています。

3. ステップ2の方法を使用して、レベル0、レベル1、レベル2、およびネットワーク管理者ユーザーロールを取得できることを確認します(詳細は省略します)。

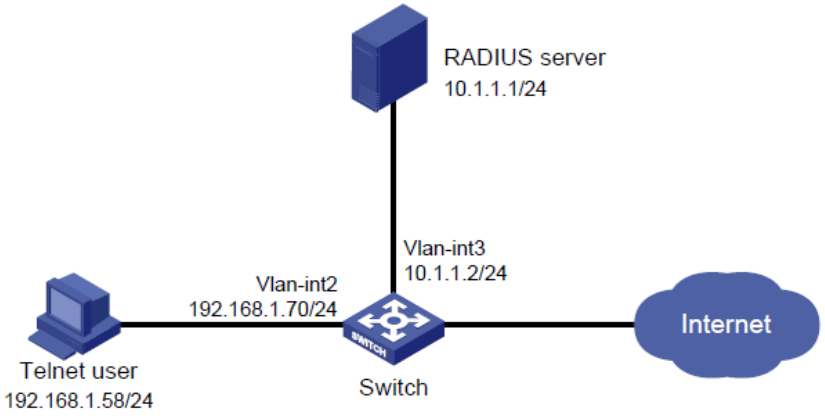
例:RBAC の一時的なユーザーロール認可(RADIUS 認証)の設定

ネットワークの設定

図7に示すように、スイッチはTelnetユーザーを含むログインユーザーに対してRADIUS認証を使用します。Telnetユーザーのユーザーアカウントは**test@bb**bで、ユーザーロール**level-0**が割り当てられています。

一時的なユーザーロール認可のためにリモート認証モードとローカル認証モードを設定します。スイッチはRADIUSサーバーを使用して**network-admin**ユーザーロールの認証を提供します。AAA設定が無効であるか、RADIUSサーバーが応答しない場合、スイッチはローカル認証を実行します。

図7ネットワーク図



手順

1. スイッチを設定します。

#VLAN-interface2(Telnetユーザーに接続されたインターフェイス)にIPアドレスを割り当てます。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0

[Switch-Vlan-interface2] quit

#VLAN-interface3(RADIUSサーバーに接続されたインターフェイス)にIPアドレスを割り当てます。

[Switch] interface vlan-interface 3

[Switch-Vlan-interface3] ip address 10.1.1.2 255.255.255.0

[Switch-Vlan-interface3] quit

#Telnetサーバーを有効にします。

[Switch] telnet server enable

#Telnetユーザーのユーザー回線でスキーム認証をイネーブルにします。

[Switch] line vty 0 15

[Switch-line-vty0-15] authentication-mode scheme

[Switch-line-vty0-15] quit

#一時的なユーザーロール認可のために、リモートからローカルへの認証をイネーブルにします。

[Switch] super authentication-mode scheme local

#RADIUSスキーム**radius**を作成し、RADIUSスキームビューに入ります。

[Switch] radius scheme radius

#スイッチとサーバー間のセキュアな通信を実現するために、プライマリ認証サーバーのアドレスと共有キーをスキームに指定します。

[Switch-radius-radius] primary authentication 10.1.1.1 key simple expert

#RADIUSサーバーに送信されるユーザー名からISPドメイン名を除外します。

[Switch-radius-radius] user-name-format without-domain

[Switch-radius-radius] quit

#ISPドメインbbbを作成し、ISPドメインビューに入ります。

[Switch] domain bbb

#ログインユーザー認証にRADIUSスキームradiusを使用するようにISPドメイン**bbb**を設定します。

[Switch-isp-bbb] authentication login radius-scheme radius

#ローカル認証を使用するようにISPドメイン**bbb**を設定します。

[Switch-isp-bbb] authorization login local

#ユーザーロール認証のために、RADIUSスキーム**radius**をISPドメインに適用します。

```
[Switch-isp-bbb] authentication super radius-scheme radius
[Switch-isp-bbb] quit
```

testという名前のデバイス管理ユーザーを作成し、ローカルユーザービューに入ります。

```
[Switch] local-user test class manage
```

ユーザーサービスタイプを**Telnet**に設定します。

```
[Switch-luser-manage-test] service-type telnet
```

ユーザーのパスワードを**aabbcc**にします。

```
[Switch-luser-manage-test] password simple aabbcc
```

level-0 をユーザーにアサインします。

```
[Switch-luser-manage-test] authorization-attribute user-role level-0
```

デフォルトユーザーロール(**network-operator**)を削除します。

```
[Switch-luser-manage-test] undo authorization-attribute user-role network-
operator
```

```
[Switch-luser-manage-test] quit
```
#ユーザーロールnetwork-adminのローカル認証パスワードをabcdef654321に設定します。

[Switch] super password role network-admin simple abcdef65432

[Switch] quit

2. RADIUSサーバーを設定します。

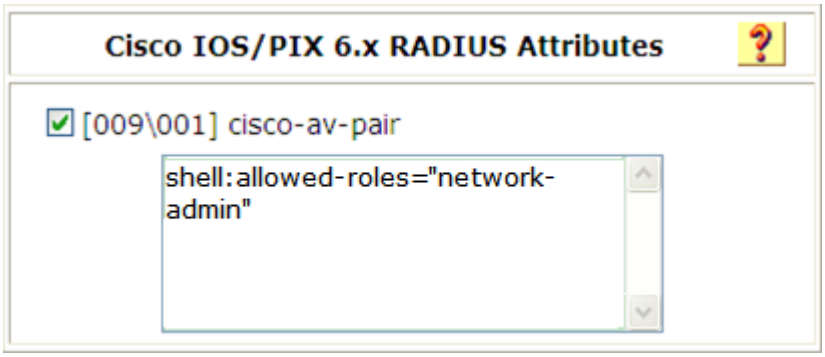
   この例では、ACSv4.2を使用します。

   a. $enab0$という名前のユーザーアカウントを追加し、パスワードを123456に設定します(詳細は省略します)。

   b. Cisco IOS/PIX6.x RADIUS Attributesページにアクセスします。

   c. 図8に示すように、cisco-av-pairアトリビュートを設定します。

図8 cisco-av-pairアトリビュートの設定



コンフィギュレーションの検証

1. スイッチにTelnet接続し、ユーザー名に **test@bbb**とパスワードに **abbbcc**を入力してスイッチにアクセスします。診断コマンドにアクセスできることを確認します。

```
<Switch> telnet 192.168.1.70
Trying 192.168.1.70 ...
Press CTRL+K to abort

Connected to 192.168.1.70 ...

******************************************************************************
*  Copyright (c) 2004-2019 Hewlett Packard Enterprise Development L*
*  Without the owner's prior written consent*
*  no decompiling or reverse-engineering shall be allowed.              *
******************************************************************************

login: test@bbb

Password:

<Switch>?
User view commands:
  ping              Ping function
  quit              Exit from current command view
  ssh2              Establish a secure shell client connection super
                    Switch to a user role
  system-view       Enter the System View
```

```
telnet          Establish a telnet connection
tracert         Tracert function
```

```
<switch>
```

2. network-adminユーザーロールを取得できることを確認します。

   #network-adminユーザーロールを取得するには、スーパーパスワードを使用します。ユーザー名とパスワードの入力を求めるプロンプトが表示されたら、ユーザー名に **test@bbb**とパスワードに**123456**を入力します。

   ```
   <Switch> super network-admin
   Username:  test@bbb
   Password:
   ```

   次の出力は、network-adminユーザーロールを取得したことを示しています。

   ```
   User privilege role is network-admin, and only those commands that authorized to the role can be used.
   ```

   #ACSサーバーが応答しない場合は、プロンプトでローカル認証パスワード**abcdef654321**を入力します。

   ```
   Invalid configuration or no response from the authentication server. Change
   authentication mode to local.

   Password:
   User privilege role is network-admin, and only those commands that authorized to the role can be used.
   ```

   この出力は、network-adminユーザーロールを取得したことを示しています。

RBACのトラブルシューティング

このセクションでは、RBACの一般的な問題とその解決方法について説明します。

ローカルユーザーが意図したよりも多くのアクセス許可を持っている

症状

ローカルユーザーは、割り当てられたユーザーロールで許可されているよりも多くのコマンドを使用できます。

分析

ローカルユーザーがユーザーロールに割り当てられている可能性があります。たとえば、ユーザーの作成時に、ローカルユーザーにデフォルトのユーザーロールが自動的に割り当てられます。

解決策

この問題を解決するには、次の手順に従います

1. 望ましくないユーザーロールのローカルユーザーカウントを調べて削除するには、**display local-user**コマンドを使用します。
2. 問題が解決しない場合は、H3Cサポートに連絡してください。

RADIUS ユーザーによるログイン試行が常に失敗する

症状

次の条件が存在する場合でも、RADIUSユーザーによるネットワークアクセスデバイスへのログイン試行は常に失敗します。

- ネットワークアクセスデバイスとRADIUSサーバーは相互に通信できます。
- すべてのAAA設定が正しい。

分析

RBACでは、ログインユーザーに少なくとも1つのユーザーロールが必要です。RADIUSサーバーがログインユーザーにユーザーロールの使用を許可しない場合、ユーザーはデバイスにログインできません。

解決策

この問題を解決するには、次の手順に従います

1. 次のいずれかの方法を使用します。
   - **role default-role enable**コマンドを設定します。RADIUSサーバーによってユーザーロールが割り当てられていない場合、RADIUSユーザーはデフォルトのユーザーロールでログインできます。
   - RADIUSサーバーにユーザーロール認可アトリビュートを追加します。
2. 問題が解決しない場合は、H3Cサポートに連絡してください。

ログインの概要

デバイスは、次のタイプのログイン方式をサポートしています。

- **CLIログイン:**CLIでテキストコマンドを入力して、デバイスを設定および管理できます。CLIにログインするには、次のいずれかの方法を使用できます。
  - コンソールポートに接続します。
  - Telnetを使います。
  - SSHを使います。
- **SNMPアクセス:**NMSでSNMPを実行してデバイスMIBにアクセスし、GetおよびSet操作を実行してデバイスを設定および管理できます。
- **RESTfulアクセス:**RESTful API操作を使用して、デバイスを設定および管理できます。

デバイスに初めてアクセスするときは、コンソールポート経由でのみCLIにログインできます。ログイン手順については、「最初のデバイスアクセスにコンソールポートを使用する」を参照してください。ログイン後、コンソールログインパラメーターを変更したり、他のアクセス方法を設定したりできます。

デバイスは、NIST FIPS140 - 2要件に準拠するFIPSモードをサポートしています。機能、コマンド、およびパラメーターのサポートは、FIPSモードと非FIPSモードで異なる場合があります。FIPSモードの詳細については、Security Configuration Guideを参照してください。

TelnetおよびHTTPベースのRESTfulアクセスは、FIPSモードではサポートされません。

最初のデバイスアクセスにコンソールポートを使用する

最初のデバイスアクセスにコンソールポートを使用するについて

コンソールログインは、基本的なログイン方法です。

前提条件

コンソールポートからログインするには、PCなどのコンソール端末を準備します。コンソール端末にハイパーターミナルやPuTTYなどの端末エミュレーションプログラムがあることを確認します。端末エミュレーションプログラムの使用方法については、プログラムのユーザーガイドを参照してください。

手順

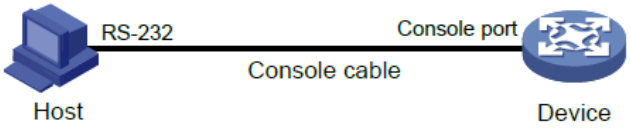
1. パソコンの電源を切る。

   PCのシリアルポートはホットスワップをサポートしていません。ケーブルをPCのシリアルポートに接続または接続解除する前に、PCの電源を切る必要があります。
2. デバイスに付属のコンソールケーブルを探し、コンソールケーブルのDB-9メスコネクタをPCのシリアルポートに接続します。
3. デバイスのコンソールポートを注意深く確認し、コンソールケーブルのRJ-45コネクタをコンソールポートに接続します。

重要:

PCを操作デバイスに接続するには、まずPC側を接続します。PCを操作デバイスから切断するには、まずデバイス側を接続します。

図9 コンソールポートへの端末の接続



4. PCの電源を入れる。
5. PCで、端末エミュレーションプログラムを起動し、デバイスに接続されているシリアルポートを使用する接続を作成します。ポートのプロパティ次のコンソールポートのデフォルト設定と一致するようにポートプロパティを設定します。
   - **Bits per second—**9600 bps。
   - **Flow control—**None。
   - **Parity—**None。
   - **Stop bits—**1。
   - **Data bits—**8。
6. デバイスの電源を入れ、プロンプトが表示されたら**Enter**キーを押します。

   ユーザービュープロンプトが表示されます。デバイスを設定または管理するコマンドを入力できます。ヘルプを表示するには、疑問符(?)を入力します。

CLI ログインの設定

CLIログインについて

デバイスはユーザーライン(ユーザーインターフェイスとも呼ばれる)を使用してCLIセッションを管理し、ユーザーの動作をモニタします。ユーザーラインの場合は、ログイン認証方式やユーザーロールなどのアクセスコントロール設定を設定できます。

ユーザー行

ユーザーラインタイプ

このデバイスでは、表11に示すタイプのユーザーラインがサポートされています。ユーザーラインによってログイン方法が異なります。

表11 CLIログイン方法およびユーザーラインマトリックス

ユーザーライン	ログイン方法
AUXライン	コンソールポート。
USBライン	USBポート
Virtual Type Terminal(VTY)ライン	TelnetまたはSSH。

ユーザーライン番号

ユーザーラインには絶対番号と相対番号があります。

絶対番号は、すべてのユーザーラインの中からユーザーラインを一意に識別します。ユーザーラインには、0から始まり、AUXラインとVTYラインの順序で1ずつ増分する番号が付けられます。パラメーターを指定せずに**display line**コマンドを使用すると、サポートされているユーザーラインとその絶対番号を表示できます。

相対番号は、同じタイプのすべてのユーザーラインの中からユーザーラインを一意に識別します。番号書式は、ユーザーラインタイプ+番号です。すべてのタイプのユーザーラインには、0から始まり1ずつ増分する番号が付けられます。たとえば、最初のVTYラインはVTY0です。

ユーザーラインの割り当て

デバイスは、表11に示すように、ログイン方法に応じてCLIログインユーザーにユーザーラインを割り当てます。ユーザーがログインすると、デバイスはアイドルユーザーラインのログイン方法をチェックし、最も小さい番号のユーザーラインをユーザーに割り当てます。たとえば、ユーザーがデバイスにTelnet接続するときにVTY0とVTY3がアイドル状態である場合、デバイスはユーザーにVTY0を割り当てます。

各ユーザーラインは、一度に1人のユーザーだけに割り当てることができます。ユーザーラインが使用できない場合、CLIログイン試行は拒否されます。

ログイン認証モード

ログイン認証を設定して、デバイスCLIへの不正アクセスを防止できます。非FIPSモードでは、デバイス

は次のログイン認証モードをサポートします。

- **None -** 認証を無効にします。このモードでは、認証なしでアクセスが許可されるので安全ではありません。
- **Password -** パスワード認証が必要です。ユーザーはログイン時に正しいパスワードを入力する必要があります。
- **Scheme -** AAAモジュールを使用して、ローカルまたはリモートログイン認証を提供します。ユーザーは、ログイン時に正しいユーザー名とパスワードを入力する必要があります。

FIPSモードでは、デバイスはスキーム認証モードだけをサポートします。

表12に示すように、ログイン認証モードが異なると、必要なユーザーライン設定も異なります。

表12さまざまなログイン認証モードに必要な構成

認証モード	設定タスク
None	認証モードをnoneに設定します。
Password	1. 認証モードをpasswordに設定します。 2. パスワードを設定します。
Scheme	1. 認証モードをschemeに設定します。 2. ISPドメインビューでログイン認証方法を構成します。詳細については、「セキュリティ構成ガイド」を参照してください。

ユーザーロール

ユーザーには、ログイン時にユーザーロールが割り当てられます。ユーザーロールは、ユーザーが使用できるコマンドを制御します。ユーザーロールの詳細は、「RBACの構成」を参照してください。

デバイスは、ログイン認証モードとユーザータイプに基づいてユーザーロールを割り当てます。

- noneまたはpassword認証モードでは、デバイスはユーザーラインに指定されたユーザーロールを割り当てます。
- scheme認証モードでは、デバイスは次のルールを使用してユーザーロールを割り当てます。
  - publickeyまたはpassword-publickey認証を使用するSSHログインユーザーの場合、デバイスはローカルデバイス管理ユーザーに指定されたユーザーロールを同じ名前で割り当てます。
  - 他のユーザーの場合、デバイスはAAAモジュールのユーザーロール設定に従ってユーザーロールを割り当てます。AAAサーバーがユーザーロールを割り当てず、デフォルトのユーザーロール機能が無効の場合、リモートAAA認証ユーザーはログインできません。

FIPS準拠

デバイスは、NIST FIPS140 - 2要件に準拠するFIPSモードをサポートしています。機能、コマンド、およびパラメーターのサポートは、FIPSモードと非FIPSモードで異なる場合があります。FIPSモードの詳細については、Security Configuration Guideを参照してください。

FIPSモードでは、Telnetログインはサポートされていません。

制約事項およびガイドライン:CLIログイン設定

ユーザーラインビューとユーザーラインクラスビューの両方で使用できるコマンドには、次のルールが適用されます。

- ユーザーラインビューの設定は、ユーザーラインにのみ適用されます。ユーザーラインクラスビューの設定は、クラスのすべてのユーザーラインに適用されます。
- いずれかのビューのデフォルト以外の設定は、他のビューのデフォルト設定より優先されます。ユーザーラインビューのデフォルト以外の設定は、ユーザーラインクラスビューのデフォルト以外の設定より優先されます。
- ユーザーラインクラスビューの設定は、設定後にログインしたユーザーにのみ有効です。設定時にすでにオンラインになっているユーザーには影響しません。

コンソール又はUSBログインの設定

コンソールと USB ログインについて

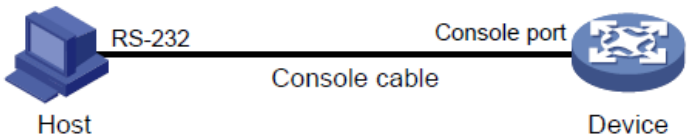
端末をデバイスのコンソールポートに接続すると、デバイスにログインして管理できます(図10を参照)。ログイン手順の詳細は、「最初のデバイスアクセスにコンソールポートを使用する」を参照してください。

次のタスクを実行して、USBポートを介してデバイスにログインすることもできます。

1. BluetoothモデムをデバイスのUSBポートに接続します。
2. モバイル端末を使用して、Bluetoothモデムへの接続を確立します。

デバイスにログインした後、モバイル端末のアプリケーションを使用してデバイスを管理できます。

図10 コンソールポートからのログイン



デフォルトでは、コンソールログインは有効になっており、認証は必要ありません。ユーザーロールは、コンソールユーザーのnetwork-adminです。デバイスのセキュリティを向上させるには、デバイスに初めてログインした直後に、コンソールログインのパスワードまたはスキーム認証を構成します。

デフォルトでは、USBログインは有効になっており、認証は必要ありません。デフォルトのユーザーロールは、USBユーザーのnetwork-adminです。デバイスのセキュリティを向上させるには、デバイスに初めてログインした直後にUSBラインのパスワードまたはスキーム認証を構成します。

制限事項とガイドライン

コンソールログイン構成の変更は、変更後にログインしたユーザーにのみ有効です。変更時にすでにオンラインになっているユーザーには影響しません。

FIPSモードでは、デバイスはスキーム認証だけをサポートします。認証を無効にしたり、パスワード認証を設定したりすることはできません。

コンソールまたは USB ログイン設定作業の概要

コンソールログインを設定するには、以下のタスクを実行してください。

1. コンソールまたはUSBログイン認証の設定
   - コンソールまたはUSBログインの認証の無効化
   - コンソールまたはUSBログインのパスワード認証の設定
   - コンソールまたはUSBログインのスキーム認証の設定
2. (オプション)共通コンソールログイン設定の構成

コンソールまたは USB ログイン認証の設定

コンソールログインの認証の無効化

1. システムビューに入ります。

   system-view
2. AUX/USBビューまたはクラスビューに入ります。
   - AUXまたはUSBビューに入ります。

     line { **aux** | **usb** } *first-number* [*last-number*]
   - AUXまたはUSBクラスビューに入ります。

   line class { **aux** | **usb** }
3. 認証を無効にします。

   authentication-mode none

   デフォルトではコンソールまたはUSBログインの認証は無効です。
4. ユーザーロールを割り当てます。

   user-role *role-name*

   デフォルトでは、コンソールまたはUSBユーザーにはnetwork-adminユーザーロールが割り当てられます。

コンソールまたは USB ログインのパスワード認証の設定

1. システムビューに入ります。

   system-view
2. 補助ビューまたはクラスビューに入ります。
   - AUXまたはUSBビューに入ります。

     line { **aux** | **usb** } *first-number* [*last-number*]
   - AUXまたはUSBクラスビューに入ります。

   line class { **aux** | **usb** }
3. パスワード認証をイネーブルにします。

   authentication-mode password

デフォルトではコンソールとUSBログインの認証は無効です。

4. パスワードを設定します。

   set authentication password { **hash** | **simple** } *password*

   デフォルトでは、パスワードは設定されていません。

5. ユーザーロールを割り当てます。

   user-role *role-name*

   デフォルトでは、コンソールユーザーにはnetwork-adminユーザーロールが割り当てられます。

コンソールまたは USB ログインのスキーム認証の設定

1. システムビューに入ります。

   system-view

2. 補助ビューまたはクラスビューに入ります。

   - 補助ビューに入ります。

     line { **aux** | **usb** } *first-number* [*last-number*]

   - 補助クラスビューに入ります。

   line class { **aux** | **usb** }

3. スキーム認証をイネーブルにします。

   非FIPSモードの場合:

   authentication-mode scheme

   コンソールログインのデフォルト認証モードは次のとおりです。

   デフォルトでは、コンソールまたはUSBログインに認証は無効です。

   FIPSモードの場合:

   authentication-mode scheme

   デフォルトでは、スキーム認証は有効です。

4. ISPドメインビューでユーザー認証パラメーターを構成します。

   ローカル認証を使用するには、ローカルユーザーを設定し、関連するアトリビュートを設定します。リモート認証を使用するには、RADIUS、LDAP、またはHWTACACSスキームを設定します。詳細については、『AAA Security Configuration Guide』を参照してください。

コンソールまたは USB 共通のログイン設定のコンフィギュレーション

制限事項とガイドライン

一部の一般的なコンソールログイン設定はすぐに有効になり、現在のセッションを中断できます。コンソールログイン設定を変更する前に、コンソールログインとは異なるログイン方法を使用してデバイスにログインしてください。

コンソールログイン設定を変更したら、ログインが成功するように設定端末の設定を調整します。

手順

1. システムビューに入ります。

system-view

2. 補助ビューまたはクラスビューに入ります。
   - AUXまたはUSBビューに入ります。

     line { aux | usb } *first-number* **[** *last-number* **]**
   - 補助クラスビューに入ります。

     line class { aux | usb }
3. 伝送パラメーターを設定します。
   - 伝送速度を設定します。

     speed *speed-value*

     デフォルトでは、伝送レートは9600bpsです。

     このコマンドは、ユーザーラインクラスビューでは使用できません。
   - パリティモードを指定します。

     parity { even | mark | none | odd | space }

     デフォルトでは、ユーザーラインはパリティを使用しません。

     このコマンドは、ユーザーラインクラスビューでは使用できません。
   - フロー制御を設定します。

     flow-control { none | software }

     デフォルトでは、デバイスはフロー制御を実行しません。

     このコマンドは、ユーザーラインクラスビューでは使用できません。
   - 文字のデータビット数を指定します。

     databits { 7 | 8 }

     デフォルトは8です。

     このコマンドは、ユーザーラインクラスビューでは使用できません。

パラメーター	説明
7	標準ASCII文字を使用します。
8	拡張ASCII文字を使用します。
   - 文字のストップビット数を指定します。

     stopbits { 1 | 1.5 | 2 }

     デフォルトは1です。

     ストップビットは文字の終わりを示します。ストップビットが多いほど、伝送速度が遅くなります。

     このコマンドは、ユーザーラインクラスビューでは使用できません。
4. 端末属性を設定します。
   - ターミナルサービスを有効にします。

     shell

     デフォルトでは、ターミナルサービスはすべてのユーザーラインでイネーブルになっています。AUXラインビューでは、**undo shell**コマンドは使用できません。
   - ターミナル表示タイプを指定します。

     terminal type { ansi | vt100 }

既定では、端子表示タイプはANSIです。

デバイスは、ANSIおよびVT100端末表示タイプをサポートしています。ベストプラクティスとして、デバイスと構成端末の両方でVT100タイプを指定することをお勧めします。両側にANSIタイプを指定することもできますが、コマンドラインの文字数が80文字を超えると、表示に問題が発生する可能性があります。

- 端末に一度に送信するコマンド出力の最大行数を設定します。

  screen-length *screen-length*

  デフォルトでは、デバイスは一度に最大24行を端末に送信します。出力画面間の一時停止を無効にするには、値を0に設定します。

- コマンドヒストリーバッファーのサイズを設定します。

  history-command max-size *value*

  デフォルトでは、バッファーサイズは10です。ユーザーラインのバッファーに保存できるヒストリーコマンドの最大数は10です。

- CLI接続アイドルタイムアウトタイマーを設定します。

  idle-timeout *minutes* **[** *seconds* **]**

  デフォルトでは、CLI接続アイドルタイムアウトタイマーは10分です。

  アイドルタイムアウト間隔内にデバイスとユーザーの間で対話が発生しない場合、システムはユーザーライン上のユーザー接続を自動的に終了します。

  タイムアウトタイマーを0に設定すると、接続はエージングアウトされません。

5. ライン上のログインユーザーに対して自動的に実行されるコマンドを指定します。

   auto-execute command *command*

   デフォルトでは、自動実行のコマンドは指定されていません。

   ユーザーがユーザーラインを介してログインすると、デバイスは自動的に指定されたコマンドを実行し、コマンドの実行後にユーザー接続を閉じます。

   このコマンドは、補助線ビューまたは補助線クラスビューでは使用できません。

6. ショートカットキーを設定します。

   - 端末セッションアクティベーションキーを指定します。

     activation-key *character*

     デフォルトでは、Enterキーを押すとターミナルセッションが開始されます。

   - エスケープキーを指定します。

     escape-key { *character* **| default }**

     既定では、Ctrl+Cを押すとコマンドが終了します。

   - ユーザーラインロックキーを設定します。

     lock-key *key-string*

     デフォルトでは、ユーザーラインロックキーは設定されていません。

Telnetログインの設定

Telnet ログインについて

デバイスは、Telnetログインを許可するTelnetサーバーとして、または他のデバイスにTelnet接続する

Telnetクライアントとして動作できます。

制限事項とガイドライン

FIPSモードでは、Telnetログインはサポートされていません。FIPSモードの詳細については、『Security Configuration Guide』を参照してください。

Telnetログインコンフィギュレーションの変更は、変更後にログインしたユーザーにのみ有効です。変更時にすでにオンラインになっているユーザーには影響しません。

Telnet サーバーとしてのデバイスの設定

Telnet サーバーの設定作業の概要

デバイスをTelnetサーバーとして設定するには、次の作業を行います。

1. Telnetサーバーの有効化
2. Telnetログイン認証の設定
   - Telnetログインの認証の無効化
   - Telnetログインのパスワード認証の設定
   - Telnetログインのスキーム認証の設定
3. (任意)一般的なTelnetサーバー設定の指定
4. (任意)一般的なVTYライン設定の設定

Telnet サーバーの有効化

1. システムビューに入ります。

   system-view
2. Telnetサーバーをイネーブルにします。

   telnet server enable

   デフォルトでは、Telnetサーバーは無効です。

Telnet ログインの認証の無効化

1. システムビューに入ります。

   system-view
2. VTYラインビューまたはクラスビューに入ります。
   - VTYラインビューに入ります。

     line vty *first-number* [*last-number*]
   - VTYラインクラスビューに入ります。

     line class vty
3. 認証を無効にします。

   authentication-mode none

   デフォルトでは、パスワード認証はTelnetログインに対してイネーブルです。

   VTYラインビューでは、このコマンドはprotocol inboundコマンドに関連付けられています。一方のコマンドがVTYラインビューでデフォルト以外の設定持つ場合、もう一方のコマンドは、VTYラ

インクラスビューの設定に関係なく、VTYラインビューの設定を使用します。

4. (任意)ユーザーロールを割り当てます。

   user-role *role-name*

   デフォルトでは、VTYラインユーザーにはネットワークオペレータユーザーロールが割り当てられます。

Telnet ログインのパスワード認証の設定

1. システムビューに入ります。

   system-view

2. VTYラインビューまたはクラスビューに入ります。
   - VTYラインビューに入ります。

     line vty *first-number* **[** *last-number* **]**
   - VTYラインクラスビューに入ります。

     line class vty

3. パスワード認証をイネーブルにします。

   authentication-mode password

   デフォルトでは、パスワード認証はTelnetログインに対してイネーブルです。

   VTYラインビューでは、このコマンドはprotocol inboundコマンドに関連付けられています。一方のコマンドがVTYラインビューでデフォルト以外の設定持つ場合、もう一方のコマンドは、VTYラインクラスビューの設定に関係なく、VTYラインビューの設定を使用します。

4. パスワードを設定します。

   set authentication password { hash | simple } *password*

   デフォルトでは、パスワードは設定されていません。

5. (任意)ユーザーロールを割り当てます。

   user-role *role-name*

   デフォルトでは、VTYラインユーザーにはnetwork-operatorタユーザーロールが割り当てられます。

Telnet ログインのスキーム認証の設定

1. システムビューに入ります。

   system-view

2. VTYラインビューまたはクラスビューに入ります。
   - VTYラインビューに入ります。

     line vty *first-number* [*last-number*]
   - VTYラインクラスビューに入ります。

     line class vty

3. スキーム認証をイネーブルにします。

   authentication-mode scheme

   デフォルトでは、パスワード認証はTelnetログインに対してイネーブルです。

   VTYラインビューでは、このコマンドは**protocol inbound**コマンドに関連付けられています。一方のコマンドがVTYラインビューでデフォルト以外の設定持つ場合、もう一方のコマンドは、VTYラインクラスビューの設定に関係なく、VTYラインビューの設定を使用します。

4. ISPドメインビューでユーザー認証パラメーターを構成します。

ローカル認証を使用するには、ローカルユーザーを設定し、関連するアトリビュートを設定します。

リモート認証を使用するには、RADIUS、LDAP、またはHWTACACSスキームを設定します。詳細については、『Security Configuration Guide』の「AAA」を参照してください。

一般的な Telnet サーバー設定の構成

1. システムビューに入ります。

   system-view

2. 発信TelnetパケットのDSCP値を設定します。

   IPv4:

   telnet server dscp *dscp-value*

   IPv6:

   telnet server ipv6 dscp *dscp-value*

   デフォルトでは、DSCP値は48です。

3. Telnetサービスポート番号を指定します。IPv4:

   telnet server port *port-number*

   IPv6:

   telnet server ipv6 port *port-number*

   デフォルトでは、Telnetサービスポート番号は23です。

4. 同時Telnetユーザーの最大数を設定します。

   aaa session-limit telnet *max-sessions*

   デフォルトでは、同時Telnetユーザーの最大数は32です。

   この設定を変更しても、現在オンラインであるユーザーには影響しません。新しい制限がオンラインTelnetユーザー数より少ない場合、新しい制限を下回るまで、追加のユーザーはTelnet接続できません。

   このコマンドの詳細については、「セキュリティコマンドリファレンス」を参照してください。

一般的な VTY ライン設定

1. システムビューに入ります。

   system-view

2. VTYラインビューまたはクラスビューに入ります。
   - VTYラインビューに入ります。

     line vty *first-number* [*last-number*]
   - VTYラインクラスビューに入ります。

     line class vty

3. VTY端末アトリビュートを設定します。
   - ターミナルサービスを有効にします。

     shell

     デフォルトでは、ターミナルサービスはすべてのユーザーラインで有効になっています。
   - 端子表示タイプを指定します。

     Terminal type { ansi | vt100 }

     デフォルトでは、端子表示タイプはANSIです。

- 端末に一度に送信するコマンド出力の最大行数を設定します。

  screen-length *screen-length*

  デフォルトでは、デバイスは一度に最大24行を端末に送信します。出力画面

  間の一時停止を無効にするには、値を0に設定します。
- コマンドヒストリーバッファーのサイズを設定します。

  history-command max-size *value*

  デフォルトでは、バッファーサイズは10です。ユーザーラインのバッファーに保存できるヒストリーコマンドの最大数は10です。
- CLI接続アイドルタイムアウトタイマーを設定します。

  idle-timeout *minutes [seconds]*

  デフォルトでは、CLI接続アイドルタイムアウトタイマーは10分です。

  アイドルタイムアウト間隔内にデバイスとユーザーの間で対話が発生しない場合、システムはユーザーライン上のユーザー接続を自動的に終了します。

  タイムアウトタイマーを0に設定すると、接続はエージングアウトされません。

4. サポートされているプロトコルを指定します。

protocol inbound { **all | ssh | telnet** }

デフォルトでは、TelnetとSSHがサポートされています。

プロトコルの変更は、設定後にログインしたユーザーにのみ有効です。設定時にすでにオンラインになっているユーザーには影響しません。

VTYラインビューでは、このコマンドはauthentication-modeコマンドに関連付けられます。一方のコマンドがVTYラインビューにデフォルト以外の設定を持つ場合、もう一方のコマンドは、VTYラインクラスビューの設定に関係なく、VTYラインビューの設定を使用します。

5. ユーザー行のログインユーザーに対して自動的に実行されるコマンドを指定します。

auto-execute command *command*

デフォルトでは、自動実行のコマンドは指定されていません。

重要:

このコマンドを設定して設定を保存する前に、他のVTYラインまたはAUXライン経由でCLIにアクセスして設定を変更できることを確認してください。

VTYラインでは、ユーザーのログイン時に自動的に実行されるコマンドを指定できます。指定したコマンドを実行すると、Telnetセッションが自動的に切断されます。

6. ショートカットキーを設定します。

- タスクを終了するためのショートカットキーを指定します。

  escape-key { *character* | **default** }

  デフォルトの設定は**Ctrl+C**です。
- ユーザーラインロックキーを設定します。

  lock-key *key-string*

  デフォルトでは、ユーザーラインロックキーは設定されていません。

デバイスを使用した Telnet サーバーへのログイン

デバイスを使用した telnet サーバーへのログインについて

デバイスをTelnetクライアントとして使用して、Telnetサーバーにログインできます。

図11デバイスからTelnetサーバーへのTelnet接続

前提条件

デバイスにIPアドレスを割り当て、Telnetサーバーの IPアドレスを取得します。デバイスがTelnetサーバーとは別のサブネット上にある場合は、デバイスとTelnetサーバーが互いに通信できることを確認します。

手順

1. システムビューに入ります。

   system-view

2. (任意)発信Telnetパケットの送信元IPv4アドレスまたは送信元インターフェイスを指定します。

   telnet client source { interface *interface-type interface-number* **| ip** *ip-address* **}**

   デフォルトでは、送信元IPv4アドレスまたは送信元インターフェイスは指定されません。デバイスは、出力インターフェイスのプライマリIPv4アドレスを発信Telnetパケットの送信元アドレスとして使用します。

3. ユーザービューに戻ります。

   quit

4. デバイスを使用して、Telnetサーバーにログインします。

   IPv4:

   telnet *remote-host* **[** *service-port* **] [vpn-instance** *vpn-instance-name* **] [source { interface** *interface-type interface-number* **| ip** *ip-address* **} | dscp** *dscp-value* **] ***

   IPv6:

   telnet ipv6 *remote-host* **[-i** *interface-type interface-number* **]** [*port-number*] [**vpn-instance** *vpn-instance-name*] [**source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* } | **dscp** *dscp-value*] *

SSHログインの設定

SSH ログインについて

SSHは、安全なリモートログイン方式を提供します。暗号化と強力な認証を提供することで、IPスプーフィングやプレーンテキストのパスワード傍受などの攻撃からデバイスを保護します。詳細については、「セキュリティの構成ガイド」を参照してください。

デバイスは、Telnetログインを許可するSSHサーバーとして、またはSSHサーバーにログインするSSHクライアントとして動作できます。

SSH サーバーとしてのデバイスの設定

SSH サーバーとしてのデバイス設定について

この項では、SSHクライアント認証方式がパスワードの場合に使用されるSSHサーバー構成手順について説明します。SSHおよびパブリックキー認証構成の詳細は、「セキュリティ構成ガイド」を参照してください。

手順

1. システムビューに入ります。

   system-view

2. ローカルキーペアを作成します。

   非FIPSモードの場合:

   public-key local create { dsa | ecdsa [secp192r1 | secp256r1 | secp384r1 | secp521r1] | rsa } [name *key-name*]

   FIPSモードの場合:

   public-key local create { dsa | ecdsa [secp256r1 | secp384r1 | secp521r1]

   | rsa } [name *key-name*]

3. SSHサーバーを有効にします。

   ssh server enable

   デフォルトでは、SSHサーバーは無効です。

4. (任意)SSHユーザーを作成し、認証モードを指定します。

   ssh user *username* **service-type stelnet authentication-type password**

5. VTYラインビューまたはクラスビューに入ります。

   - VTYラインビューに入ります。

     line vty *first-number* [*last-number*]

   - VTYラインクラスビューに入ります。

     line class vty

6. スキーム認証を有効にします。

   非FIPSモードの場合:

   authentication-mode scheme

   デフォルトでは、パスワード認証はVTYラインに対してイネーブルです。

   VTYラインビューでは、このコマンドはprotocol inboundコマンドに関連付けられています。一方のコマンドがVTYラインビューでデフォルト以外の設定持つ場合、もう一方のコマンドは、VTYラインクラスビューの設定に関係なく、VTYラインビューの設定を使用します。

   FIPSモードの場合:

   authentication-mode scheme

   デフォルトでは、スキーム認証はVTYラインに対してイネーブルです。

   VTYラインビューでは、このコマンドはprotocol inboundコマンドに関連付けられています。一方のコマンドがVTYラインビューでデフォルト以外の設定持つ場合、もう一方のコマンドは、VTYラインクラスビューの設定に関係なく、VTYラインビューの設定を使用します。

7. (任意)サポートするユーザーラインのプロトコルを指定します。

   非FIPSモードの場合:

   protocol inbound { all | ssh | telnet }

   デフォルトでは、TelnetとSSHがサポートされています。

   プロトコルの変更は、設定後にログインしたユーザーにのみ有効です。設定時にすでにオンラインになっているユーザーには影響しません。

   VTYラインビューでは、このコマンドはauthentication-modeコマンドに関連付けられます。一方のコマンドがVTYラインビューにデフォルト以外の設定を持つ場合、もう一方のコマンドは、VTYラインクラスビューの設定に関係なく、VTYラインビューの設定を使用します。

   FIPSモードの場合:

   protocol inbound ssh

   デフォルトでは、SSHがサポートされています。

   プロトコルの変更は、設定後にログインしたユーザーにのみ有効です。設定時にすでにオンラインになっているユーザーには影響しません。

   VTYラインビューでは、このコマンドは**authentication-mode**コマンドに関連付けられます。一方のコマンドがVTYラインビューにデフォルト以外の設定を持つ場合、もう一方のコマンドは、VTYラインクラスビューの設定に関係なく、VTYラインビューの設定を使用します。

8. (任意)同時SSHユーザーの最大数を設定します。

   aaa session-limit ssh *max-sessions*

   デフォルトでは、同時SSHユーザーの最大数は32です。

   この設定を変更しても、現在オンラインになっているユーザーには影響しません。新しい制限がオンラインSSHユーザーの数より少ない場合、その数が新しい制限を下回るまで、追加のSSHユーザーはログインできません。

   このコマンドの詳細については、「セキュリティコマンドリファレンス」を参照してください。

9. (任意)VTYラインの共通設定を行います。

   a. システムビューに戻ります。

      quit

   b. VTYラインの共通設定を構成します。

      「共通VTYライン設定の構成」を参照してください。

デバイスを使用した SSH サーバーへのログイン

デバイスを使用した SSH サーバーへのログインについて

デバイスをSSHクライアントとして使用して、SSHサーバーにログインできます。

図12 デバイスからSSHサーバーへのログイン

前提条件

デバイスにIPアドレスを割り当て、SSHサーバーのIPアドレスを取得します。デバイスがSSHサーバーとは別のサブネット上にある場合は、デバイスとSSHサーバーが互いに通信できることを確認しま

す。

手順

デバイスを使用してSSHサーバーにログインするには、ユーザービューで次のいずれかのコマンドを実行します。

IPv4:

ssh2 *server*

IPv6:

ssh2 ipv6 *server*

SSHサーバーを操作するには、一連のパラメーターを指定する必要がある場合があります。詳細については、「Security Configuration Guide」を参照してください。

CLIログインの表示およびメンテナンスコマンド

任意のビューで表示コマンドを実行します。

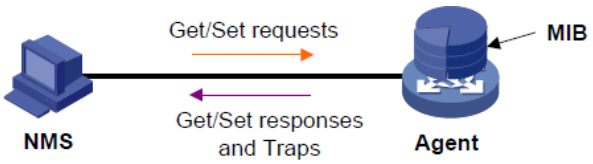
タスク	コマンド	注意
ユーザーライン情報を表示します。	**display line** [num1 | { **aux | usb | vty** } *num2*] [**summary**]	無効
Telnetクライアントのパケット送信元設定を表示します。	**display telnet client**	無効
オンラインCLIユーザーを表示します。	**display users [all]**	無効
ユーザーラインを解放します。	**free line** { *num1* | { **au**x | **usb** | **vty** } *num2* }	複数のユーザーがデバイスにログインして、デバイスを同時に設定できます。必要に応じて、このコマンドを実行して一部の接続を解放できます。 このコマンドを使用して、使用中の接続を解放することはできません。 このコマンドはユーザービューで使用できます。
現在のユーザーラインをロックし、ラインのロックを解除するためのパスワードを設定します。	**lock**	デフォルトでは、ユーザーラインはロックされません。 このコマンドはFIPSモードではサポートされていません。 このコマンドはユーザービューで使用できます。
現在のユーザーラインをロックし、認証のロック解除をイネーブルにします。	**lock reauthentication**	デフォルトでは、システムはユーザーラインをロックしたり、再認証を開始したりしません。 ロックされたユーザーラインのロックを解除するには、Enterキーを押してログインパスワードを入力し、再認証に合格する

		必要があります。 このコマンドは、どのビューでも使用できます。
ユーザーラインにメッセージを送信します。	**send** { **all** | *num1* | { **aux** | **usb** | **vty** } *num2* }	このコマンドはユーザービューで使用できます。

SNMP によるデバイスへのアクセス

NMSでSNMPを実行してデバイスMIBにアクセスし、GetおよびSet操作を実行してデバイスを設定および管理できます。

図13SNMPアクセス図



SNMP の詳細については、『Network Management and Monitoring Configuration Guide』を参照してください。

RESTful アクセスの設定

RESTfulアクセスについて

このデバイスは、Representational State Transfer Application Programming Interface(RESTful API)を提供します。このAPIに基づいて、Python、Ruby、Javaなどのプログラミング言語を使用して、次のタスクを実行するプログラムを記述できます。

- 認証を渡すためにRESTful要求をデバイスに送信します。
- RESTful API操作を使用して、デバイスを設定および管理します。RESTful API操作には、Get、Put、Post、およびDeleteがあります。

デバイスは、HTTPまたはHTTPSを使用したRESTfulパケットの転送をサポートしています。

FIPS準拠

デバイスは、NIST FIPS140 - 2要件に準拠するFIPSモードをサポートしています。機能、コマンド、お

よびパラメーターのサポートは、FIPSモードと非FIPSモードで異なる場合があります。FIPSモードの詳細については、Security Configuration Guideを参照してください。

HTTPを介したRESTfulアクセスは、FIPSモードではサポートされていません。

HTTPを介したRESTfulアクセスの設定

1. システムビューに入ります。

   system-view
2. HTTPを介したRESTfulアクセスを有効にします。

   restful http enable

   デフォルトでは、HTTPを介したRESTfulアクセスは無効になっています。
3. ローカルユーザーを作成し、ローカルユーザービューに入ります。

   local-user *user-name* [**class manage**]
4. ローカルユーザーのパスワードを設定します。

   password [{ hash | simple } *password* **]**
5. (任意)ユーザーロールをローカルユーザーに割り当てます。

   authorization-attribute user-role *user-role*

   デフォルトのユーザーロールは、RESTfulアクセスユーザーのネットワークオペレータです。
6. ローカルユーザーのHTTPサービスを指定します。

   service-type http

   デフォルトでは、ローカルユーザーにサービスタイプは指定されません。

HTTPSを介したRESTfulアクセスの設定

1. システムビューに入ります。

   system-view
2. HTTPSを介したRESTfulアクセスを有効にします。

   restful https enable

   デフォルトでは、HTTPSを介したRESTfulアクセスは無効になっています。
3. ローカルユーザーを作成し、ローカルユーザービューに入ります。

   local-user *user-name* **[class manage]**
4. ローカルユーザーのパスワードを設定します。

   非FIPSモードの場合:

   password [{ hash **| simple }** *password*]

   FIPSモードの場合:

   password
5. (任意)ユーザーロールをローカルユーザーに割り当てます。

   authorization-attribute user-role *user-role*

   デフォルトのユーザーロールは、RESTfulアクセスユーザーのネットワークオペレータです。

6. ローカルユーザーのHTTPSサービスを指定します。

   service-type https

   デフォルトでは、ローカルユーザーにサービスタイプは指定されません。

デバイスへのユーザーアクセスの制御

ログインユーザーアクセス制御について

ACLを使用して不正アクセスを防止し、コマンド認可とアカウンティングを設定してユーザーの動作を監視および制御します。

適用されたACLが存在しない場合、またはルールがない場合、ユーザーログイン制限は適用されません。ACLが存在し、ルールがある場合、ACLによって許可されたユーザーだけがデバイスにアクセスできます。

ACL の詳細については、『ACL and QoS Configuration Guide』を参照してください。

FIPS準拠

デバイスは、NIST FIPS140 - 2要件に準拠するFIPSモードをサポートしています。機能、コマンド、およびパラメーターのサポートは、FIPSモードと非FIPSモードで異なる場合があります。FIPSモードの詳細については、Security Configuration Guideを参照してください。

FIPSモードでは、Telnetはサポートされていません。

TelnetおよびSSHログインの制御

Telnet ログインの制御

1. システムビューに入ります。

   system-view

2. ACLを適用して、Telnetログインを制御します。

   IPv4:

   telnet server acl { *advanced-acl-number* | *basic-acl-number* **| mac** *mac-acl-number* }

   IPv6:

   telnet server ipv6 acl { ipv6 { *advanced-acl-number* | *basic-acl-number* **}** | **mac** *mac-acl-number* }

   デフォルトでは、Telnetログインの制御にACLは使用されません。

3. (任意)Telnetログイン制御ACLによって拒否されるTelnetログイン試行のロギングをイネーブルにします。

   telnet server acl-deny-log enable

   デフォルトでは、Telnetログイン制御ACLによって拒否されるTelnetログイン試行のロギン

グは無効です。

SSH ログインの制御

1. システムビューに入ります。

   system-view

2. SSHログインを制御するためにACLを適用します。

   IPv4:

   ssh server acl { *advanced-acl-number* **|** *basic-acl-numbe***r | mac** *mac-acl-number* }

   IPv6:

   ssh server ipv6 acl { ipv6 { *advanced-acl-number* **|** *basic-acl-number* **} | mac** *mac-acl-number* }

   デフォルトでは、SSHログインの制御にACLは使用されません。

3. (任意)SSHログイン制御ACLによって拒否されるSSHログイン試行のロギングをイネーブルにします。

   ssh server acl-deny-log enable

   デフォルトでは、SSHログイン制御ACLによって拒否されるSSHログイン試行のロギングは無効です。

   ssh コマンドの詳細については、Security Command Reference を参照してください。

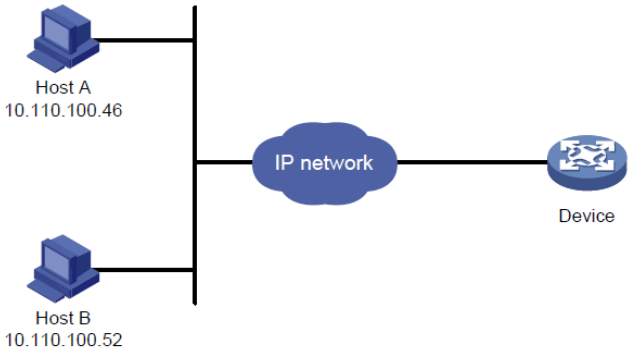
例:Telnet ログインの制御

ネットワークの設定

図14に示すように、デバイスはTelnetサーバーです。

ホストAおよびホストBから送信されるTelnetパケットだけを許可するようにデバイスを設定します。

図14 ネットワーク図



手順

#ホストAおよびホストBから送信されたパケットを許可するようにACLを設定します。

<Sysname> system-view

[Sysname] acl basic 2000 match-order config

[Sysname-acl-ipv4-basic-2000] rule 1 permit source 10.110.100.52 0

[Sysname-acl-ipv4-basic-2000] rule 2 permit source 10.110.100.46 0

[Sysname-acl-ipv4-basic-2000] quit

#ACLを適用して、Telnetログインをフィルタリングします。

[Sysname] telnet server acl 2000
[Sysname] snmp-agent group v2c groupa acl 2000

[Sysname] snmp-agent usm-user v2c usera groupa acl 2000

SNMPアクセスの制御

SNMP アクセス制御について

SNMP アクセスコントロールの詳細については、『Network Management and Monitoring Configuration Guide』の「SNMP」を参照してください。

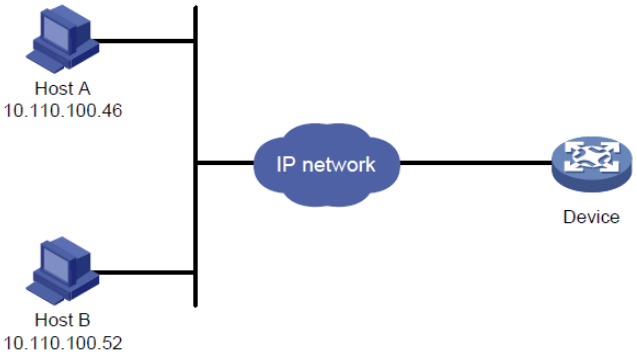
例:SNMP アクセスの制御

ネットワークの設定

図15に示すように、デバイスはSNMPを実行しています。

ホストAとホストBがSNMPを介してデバイスにアクセスできるようにデバイスを設定します。

図15ネットワーク図



手順

#ホストAおよびホストBから送信されるパケットを許可するACLを作成します。

<Sysname> system-view

[Sysname] acl basic 2000 match-order config

[Sysname-acl-ipv4-basic-2000] rule 1 permit source 10.110.100.52 0

[Sysname-acl-ipv4-basic-2000] rule 2 permit source 10.110.100.46 0

[Sysname-acl-ipv4-basic-2000] quit

ACLをSNMPコミュニティおよびSNMPグループに関連付けます。

[Sysname] snmp-agent community read aaa acl 2000

[Sysname] snmp-agent group v2c groupa acl 2000

[Sysname] snmp-agent usm-user v2c usera groupa acl 2000

コマンド認可の設定

コマンド認可について

デフォルトでは、ユーザーが使用できるコマンドは、ユーザーのユーザーロールだけに依存します。認証モードがschemeの場合、コマンド認可機能を設定して、コマンドへのアクセスをさらに制御できます。

コマンド認可をイネーブルにすると、ユーザーはAAAスキームとユーザーロールの両方で許可されているコマンドだけを使用できます。

制限事項とガイドライン

コマンド認可方式は、ユーザーログイン認可方式と異なる場合があります。

コマンド承認機能を有効にするには、ISPドメインビューでコマンド承認方法を構成する必要があります。詳細については、「セキュリティ構成ガイド」を参照してください。

手順

1. システムビューに入ります。

   system-view

2. ユーザーラインビューまたはユーザーラインクラスビューに入ります。
   - ユーザーラインビューに入ります。

     line { *first-number1* [*last-number1*] | { **aux | usb | vty }** *first-number2* [*last-number2*] }
   - ユーザーラインクラスビューに入ります。

     line class { aux | usb | vty }

   ユーザーラインビューの設定は、ユーザーラインにのみ適用されます。ユーザーラインクラスビューの設定は、クラスのすべてのユーザーラインに適用されます。いずれかのビューのデフォルト以外の設定は、他のビューのデフォルト設定より優先されます。ユーザーラインビューのデフォルト以外の設定は、ユーザーラインクラスビューのデフォルト以外の設定より優先されます。

   ユーザーラインクラスビューの設定は、設定後にログインしたユーザーにのみ有効です。設定時にすでにオンラインになっているユーザーには影響しません。

3. スキーム認証をイネーブルにします。

   非FIPSモードの場合:

   authentication-mode scheme

   デフォルトでは、コンソールログインとUSBログインでは認証が無効になっており、VTYログインではパスワード認証が有効になっています。

   VTYラインビューでは、このコマンドは**protocol inbound**コマンドに関連付けられています。一方のコマンドがVTYラインビューでデフォルト以外の設定持つ場合、もう一方のコマンドは、VTYラインクラスビューの設定に関係なく、VTYラインビューの設定を使用します。

FIPSモードの場合:

authentication-mode scheme

デフォルトでは、スキーム認証は有効です。

VTYラインビューでは、このコマンドは**protocol inbound**コマンドに関連付けられています。一方のコマンドがVTYラインビューでデフォルト以外の設定持つ場合、もう一方のコマンドは、VTYラインクラスビューの設定に関係なく、VTYラインビューの設定を使用します。

4. コマンド認可を有効にします。

command authorization

デフォルトでは、コマンド認可は無効になっており、ユーザーが使用できるコマンドはユーザーロールだけに依存します。

command authorization コマンドがユーザーラインクラスビューで設定されている場合、コマンド認可はクラス内のすべてのユーザーラインで有効になります。クラス内のユーザーラインのビューで **undo authorization** コマンドを設定することはできません。

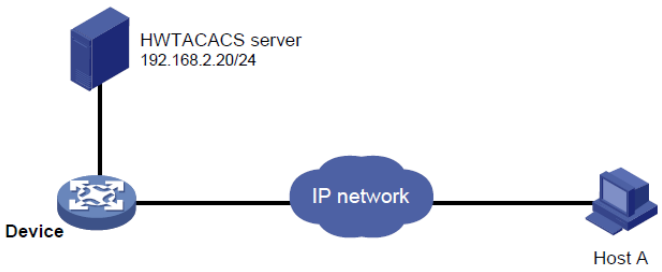
例:コマンド認可の設定

ネットワークの設定

図16に示すように、ホストAはデバイスを管理するためにデバイスにログインする必要があります。次の操作を実行するようにデバイスを構成します。

- 認証後にホストAがTelnet接続できるようにします。
- HWTACACSサーバーを使用して、ユーザーが実行できるコマンドを制御します。
- HWTACACSサーバーが使用できない場合は、ローカル認証を使用します。

図16ネットワーク図



手順

#関連するインターフェイスにIPアドレスを割り当てます。デバイスとHWTACACSサーバーが相互に到達できることを確認します。デバイスとホストAが相互に到達できることを確認します(詳細は省略します)。

#Telnetサーバーを有効にします。

<Device> system-view

[Device] telnet server enable

#ユーザーラインVTY0～VTY4のスキーム認証をイネーブルにします。

[Device] line vty 0 4

[Device-line-vty0-4] authentication-mode schem

ユーザー行のコマンド認証を有効にします。

[Device-line-vty0-4] command authorization

[Device-line-vty0-4] quit

#HWTACACSスキーム**tac**を作成します。

[Device] hwtacacs scheme tac

#認証および許可に192.168.2.20:49のHWTACACSサーバーを使用するようにスキームを設定します。

[Device-hwtacacs-tac] primary authentication 192.168.2.20 49

[Device-hwtacacs-tac] primary authorization 192.168.2.20 49

#共有キーを**expert**に設定します。

[Device-hwtacacs-tac] key authentication simple expert

[Device-hwtacacs-tac] key authorization simple expert

#HWTACACSサーバーに送信されたユーザー名からドメイン名を削除します。

[Device-hwtacacs-tac] user-name-format without-domain

[Device-hwtacacs-tac] quit

#システム定義ドメイン(**system**)を設定します。

[Device] domain system

#ログインユーザー認証およびコマンド認可にHWTACACSスキーム**tac**を使用します。バックアップ方式としてローカル認証およびローカル認可を使用します。

[Device-isp-system] authentication login hwtacacs-scheme tac local

[Device-isp-system] authorization command hwtacacs-scheme tac

local [Device-isp-system] quit

#ローカルユーザー**monitor**を作成します。simpleパスワードを123に、サービスタイプをTelnetに、デフォルトユーザーロールをレベル1に設定します。

[Device] local-user monitor

[Device-luser-manage-monitor] password simple 123

[Device-luser-manage-monitor] service-type telnet

[Device-luser-manage-monitor] authorization-attribute user-role level-1

コマンドアカウンティングの設定

コマンドアカウンティング

コマンドアカウンティングでは、HWTACACSサーバーを使用して、実行されたすべてのコマンドを記録し、デバイス上でのユーザーの動作をモニタします。

コマンドアカウンティングがイネーブルで、コマンド認可がイネーブルでない場合、実行されたすべてのコマンドが記録されます。コマンドアカウンティングとコマンド認可の両方がイネーブルの場合、実行された認可コマンドだけが記録されます。

制限事項とガイドライン

コマンドアカウンティング方式は、コマンド認可方式およびユーザーログイン認可方式と同じであっても異なっていてもかまいません。

コマンドアカウンティング機能を有効にするには、ISPドメインビューでコマンドアカウンティング方式を設定する必要があります。詳細については、「セキュリティ構成ガイド」を参照してください。

手順

1. システムビューに入ります。

   system-view

2. ユーザーラインビューまたはユーザーラインクラスビューに入ります。
   - ユーザーラインビューに入ります。

     line { *first-number1* [*last-number1*] | { **aux | usb | vty }** *first-number2* [*last-number2*] }
   - ユーザーラインクラスビューに入ります。

     line class { aux | usb | vty }

   ユーザーラインビューの設定は、ユーザーラインにのみ適用されます。ユーザーラインクラスビューの設定は、クラスのすべてのユーザーラインに適用されます。いずれかのビューのデフォルト以外の設定は、他のビューのデフォルト設定より優先されます。ユーザーラインビューのデフォルト以外の設定は、ユーザーラインクラスビューのデフォルト以外の設定より優先されます。

   ユーザーラインクラスビューの設定は、設定後にログインしたユーザーにのみ有効です。設定時にすでにオンラインになっているユーザーには影響しません。

3. スキーム認証をイネーブルにします。

   非FIPSモードの場合:

   authentication-mode scheme

   デフォルトでは、コンソールログインと USB ログインでは認証が無効になっており、VTY ログインではパスワード認証が有効になっています。

   VTYラインビューでは、このコマンドは**protocol inbound**コマンドに関連付けられています。一方のコマンドがVTYラインビューでデフォルト以外の設定持つ場合、もう一方のコマンドは、VTYラインクラスビューの設定に関係なく、VTYラインビューの設定を使用します。

   FIPSモードの場合:

   authentication-mode scheme

   デフォルトでは、スキーム認証は有効です。

   VTYラインビューでは、このコマンドは**protocol inbound**コマンドに関連付けられています。一方のコマンドがVTYラインビューでデフォルト以外の設定持つ場合、もう一方のコマンドは、VTYラインクラスビューの設定に関係なく、VTYラインビューの設定を使用します。

4. コマンドアカウンティングを有効にします。

   command accounting

   デフォルトでは、コマンドアカウンティングは無効です。アカウンティングサーバーは、ユーザーが実行したコマンドを記録しません。

   Command accountingコマンドがユーザーラインクラスビューで設定されている場合、コマンドア

カウンティングはクラス内のすべてのユーザーラインで有効になります。クラスのユーザーラインのビューで**undo command accounting**コマンドを設定することはできません。

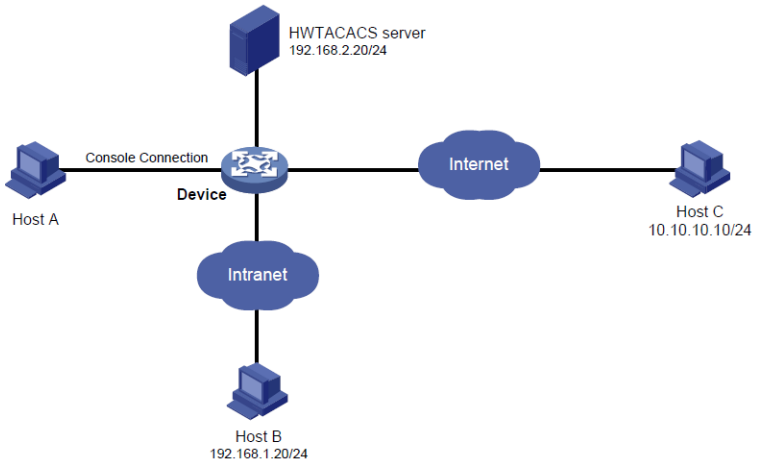
例:コマンドアカウンティングの設定

ネットワークの設定

図17に示すように、ユーザーはデバイスを管理するためにデバイスにログインする必要があります。

ユーザーが実行するコマンドをHWTACACSサーバーに送信して、デバイスでのユーザー操作をモニタおよび制御するように、デバイスを設定します。

図17 ネットワーク図



手順

#Telnetサーバーを有効にします。

<Device> system-view

[Device] telnet server enable

#ユーザーラインAUX0のコマンドアカウンティングを有効にします。

[Device] line aux 0

[Device-line-aux0] command accounting

[Device-line-aux0] quit

#ユーザーラインVTY0～VTY63のコマンドアカウンティングを有効にします。

[Device] line vty 0 63

[Device-line-vty0-63] command accounting

[Device-line-vty0-63] quit

#HWTACACSスキーム**tac**を作成します。

[Device] hwtacacs scheme tac

#アカウンティングに192.168.2.20:49のHWTACACSサーバーを使用するようにスキームを設定します。

[Device-hwtacacs-tac] primary accounting 192.168.2.20 49

#共有キーを**expert**に設定します。

[Device-hwtacacs-tac] key accounting simple expert

#HWTACACSサーバーに送信されたユーザー名からドメイン名を削除します。

[Device-hwtacacs-tac] user-name-format without-domain

[Device-hwtacacs-tac] quit

#コマンドアカウンティングにHWTACACS方式を使用するように、システム定義ドメイン(**system**)を設定します。

[Device] domain system

[Device-isp-system] accounting command hwtacacs-scheme tac

[Device-isp-system] quit

FTP の設定

FTPについて

File Transfer Protocol(FTP)は、IPネットワークを介してホスト間でファイルを転送するためのアプリケーション層プロトコルです。TCPポート20を使用してデータを転送し、TCPポート21を使用して制御コマンドを転送します。

FTPはクライアント/サーバーモデルに基づいています。デバイスはFTPサーバーまたはFTPクライアントとして動作できます。

FTP ファイル転送モード

FTPでは、次の転送モードがサポートされています。

- **Binaryモード:** .app、.bin、.btmなどの非テキストファイルに使用されます。
- **ASCIIモード: .txt、.bat、.cfg**ファイルなどのテキストファイルの転送に使用します。

デバイスがFTPクライアントとして動作する場合、転送モード(デフォルトではバイナリ)を設定できます。デバイスがFTPサーバーとして動作する場合、転送モードはFTPクライアントによって決定されます。

FTP 動作モード

FTPは、次のいずれかのモードで動作できます。

- **Activeモード(PORT)**: FTPサーバーがTCP接続を開始します。このモードは、FTPクライアントがファイアーウォールの背後にある場合(たとえば、FTPクライアントがプライベート・ネットワーク場合)には適していません。
- **Passiveモード(PASV):** FTPクライアントがTCP接続を開始します。このモードは、サーバーがクライアントに1024より大きいランダムな非特権ポートの使用を許可しない場合には適しません。

FTP動作モードは、FTPクライアントプログラムによって異なります。

FIPS準拠

デバイスは、NIST FIPS140 - 2要件に準拠するFIPSモードをサポートしています。機能、コマンド、およびパラメーターのサポートは、FIPSモードと非FIPSモードで異なる場合があります。FIPSモードの詳細については、Security Configuration Guideを参照してください。

FTPはFIPSモードではサポートされていません。

デバイスをFTPサーバーとして使用する

デバイスをFTPサーバーとして使用するには、FTPサーバーを有効にし、デバイス上で認証と認可を設定する必要があります。その他のコマンドはオプションです。

FTP サーバーの設定作業の概要

デバイスをFTPサーバーとして使用するには、次の作業を行います。

1. FTPサーバーの有効化
2. クライアントの認証許可の構成
3. (任意)FTPサーバーアクセスコントロールの設定
4. (任意)接続管理パラメーターの設定
5. (任意)SFTP接続用のSSLサーバーポリシーの指定
6. (任意)発信FTPパケットのDSCP値の設定
7. (任意)FTP接続を手動で解放する

FTP サーバーの有効化

1. システムビューに入ります。

   system-view
2. FTPサーバーを有効にします。

   ftp server enable

   デフォルトでは、FTPサーバーは無効です。

クライアントの認証許可の構成

FTPクライアントを認証し、認証されたクライアントがアクセスできる認可ディレクトリを設定するには、FTPサーバーで次の作業を実行します。

次の認証モードを使用できます。

- **ローカル認証:** デバイスはローカルユーザーカウントデータベースでクライアントのユーザー名とパスワードを検索します。一致するものが見つかると、認証は成功します。
- **リモート認証**: デバイスは、認証のためにクライアントのユーザー名とパスワードをリモート認証

サーバーに送信します。ユーザーカウントは、デバイスではなくリモート認証サーバーで設定されます。

次の許可モードを使用できます。

- **ローカル認可**: デバイスは、ローカルに設定された認可アトリビュートに基づいて、認可ディレクトリをFTPクライアントに割り当てます。
- **リモート許可**: リモート許可サーバーは、デバイス上の許可されたディレクトリをFTPクライアントに割り当てます。

認証および認可の設定の詳細については、『Security Configuration Guide』の「AAA」を参照してください。

FTP サーバーアクセス制御の設定

FTP サーバーアクセス制御について

ACLを使用して、不正アクセスを防止します。適用されたACLが存在しない場合、またはルールがない場合、ユーザーログイン制限は適用されません。ACLが存在し、ルールがある場合、ACLによって許可されたFTPクライアントのみがデバイスにアクセスできます。

制限事項とガイドライン

この構成は、FTP接続が確立されている場合にのみ有効です。既存のFTP接続には影響しません。

FTPサーバークセスコントロールを複数回設定すると、最新の設定が有効になります。

手順

1. システムビューに入ります。

   system-view
2. ACLを使用して、FTPサーバーへのアクセスを制御します。

   ftp server acl { *advanced-acl-number* **|** *basic-acl-number* **| ipv6** { *advanced-acl-number* | *basic-acl-number* } }

   デフォルトでは、アクセス制御にACLは使用されません。
3. FTPログイン制御ACLによって拒否されるFTPログイン試行のロギングを有効にします。

   ftp server acl-deny-log enable

   デフォルトでは、FTPログイン制御ACLによって拒否されるFTPログイン試行のロギングは無効です。

接続管理パラメーターの設定

1. システムビューに入ります。

   system-view
2. FTP接続アイドルタイムアウトタイマーを設定します。

   ftp timeout *minutes*

   デフォルトでは、FTP接続アイドルタイムアウトタイマーは30分です。

   アイドルタイムアウトタイマーが満了する前にFTP接続でデータ転送が行われない場合、FTPサーバーはFTP接続を閉じます。
3. 同時FTPユーザーの最大数を設定します。

aaa session-limit ftp *max-sessions*

デフォルトでは、同時FTPユーザーの最大数は32です。

この設定を変更しても、現在オンラインになっているユーザーには影響しません。新しい制限がオンラインFTPユーザーの数より少ない場合、新しい制限を下回るまで、追加のFTPユーザーはログインできません。このコマンドの詳細については、「セキュリティコマンドリファレンス」を参照してください。

SFTP 接続用の SSL サーバーポリシーの指定

SFTP 接続用の SSL サーバーポリシーの指定について

SSLサーバーポリシーをデバイスに関連付けると、SFTPをサポートするクライアントは、データセキュリティを確保するためにデバイスへのセキュアな接続を確立します。

手順

1. システムビューに入ります。

   system-view
2. SSLサーバーポリシーをFTPサーバーに関連付けて、データセキュリティを確保します。

   ftp server ssl-server-policy *policy-name*

   デフォルトでは、SSLサーバーポリシーはFTPサーバーに関連付けられていません。

送信 FTP パケットの DSCP 値の設定

1. システムビューに入ります。

   system-view
2. 送信FTPパケットのDSCP値を設定します。

   IPv4:

   ftp server dscp *dscp-value*

   IPv6:

   ftp server ipv6 dscp *dscp-value*

   デフォルトでは、DSCP値は0です。

FTP 接続を手動で解放する

FTP接続を手動で解放するには、ユーザービューで次のコマンドを実行します。

- 特定のユーザーカウントを使用して確立されたFTP接続を解除します。

  free ftp user *username*
- 特定のIPアドレスへのFTP接続を解除します。

  free ftp user-ip [ipv6] *ip-address* **[port** *port* **]**

FTP サーバーの表示コマンドおよびメンテナンスコマンド

任意のビューで表示コマンドを実行します。

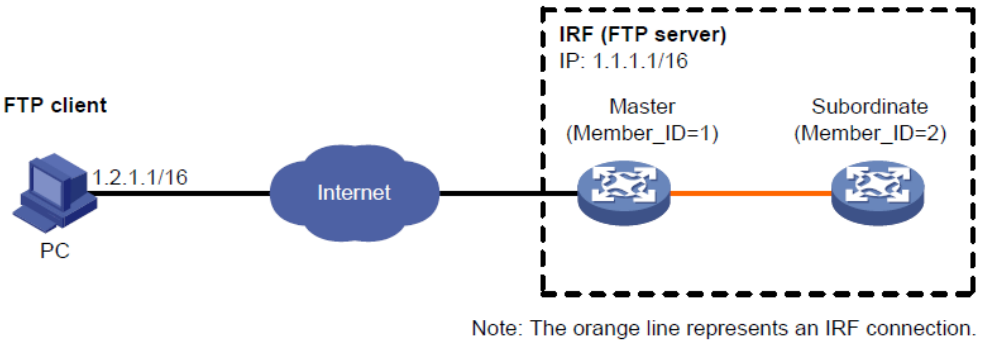
タスク	コマンド
FTPサーバーの設定およびステータス情報を表示します。	**display ftp-server**
オンラインFTPユーザーに関する詳細情報を表示します。	**display ftp-user**

例:デバイスを FTP サーバーとして使用する

ネットワークの設定

- IRFファブリックをFTPサーバーとして設定します。
- FTPサーバー上に**abc**という名前のローカルユーザーカウントを作成します。パスワードを**123456**に設定します。
- ユーザーカウントを使用して、FTPクライアントからFTPサーバーにログインします。
- **temp.bin**ファイルをFTPクライアントからFTPサーバーにアップロードします。
- FTPサーバーからFTPクライアントへバックアップの目的でonfig.cfgというファイルをダウンロードします。

図18ネットワーク図



手順

1. 図18のようにIPアドレスを設定します。IRFファブリックとPCが互いに通信できることを確認します(詳細は省略します)。
2. FTPサーバーを設定します。

   #メンバーデバイスのストレージスペースを調べます。空きスペースが不足している場合は

   delete/unreserved *file* コマンドを使って未使用のファイルを削除します(詳細は省略します)。

   # ユーザー名 **abc** でパスワードが **123456** のユーザーを作成する

   <Sysname> system-view

   [Sysname] local-user abc class manage

   [Sysname-luser-manage-abc] password simple 123456

   #**network-admin**ユーザーロールをユーザーに割り当てます。作業ディレクトリをマスター上のフ

ラッシュメモリーのルートディレクトリに設定します(下位メンバー上のフラッシュメモリーのルートディレクトリに作業ディレクトリを設定するには、ディレクトリパスにスロット番号を含める必要があります)。

[Sysname-luser-manage-abc] authorization-attribute user-role network-admin work-directory flash:/

#ユーザーにサービスタイプ FTP を割り当てます。

[Sysname-luser-manage-abc] service-type ftp

[Sysname-luser-manage-abc] quit

#FTP サーバーを有効にします。

[Sysname] ftp server enable

[Sysname] quit

3. FTPクライアントからFTP操作を実行します。

#ユーザー名**abc**とパスワード**123456を**使用して、1.1.1.1のFTPサーバーにログインします。

c:\> ftp 1.1.1.1

Connected to 1.1.1.1.

220 FTP service

ready.

User(1.1.1.1:(none)):a

bc

331 Password required for

abc. Password:

230 User logged in.

#ASCIIモードを使用して、バックアップ用にコンフィギュレーションファイル**config.cfg**をFTPサーバーからPCにダウンロードします。

ftp> ascii

200 TYPE is now ASCII

ftp> get config.cfg back-config.cfg

#バイナリモードを使用して、PCからマスター上のフラッシュメモリーのルートディレクトリに**temp.bin**ファイルをアップロードします。

ftp> binary

200 TYPE is now 8-bit

binary ftp> put temp.bin

#FTPを終了します。

ftp> bye

デバイスをFTPクライアントとして使用する

FTP クライアントの設定作業の概要

デバイスをFTPサーバーとして使用するには、次の作業を行います。

1. FTP接続の確立
2. (任意)コマンドヘルプ情報の表示
3. (オプション)FTPサーバー上のディレクトリとファイルの表示
4. (オプション)FTPサーバー上のディレクトリの管理
5. (任意)FTPサーバー上のファイルの操作
6. (オプション)別のユーザーカウントに変更する
7. (任意)FTP接続のメンテナンスとトラブルシューティング
8. (任意)FTP接続の終了

FTP 接続の確立

FTP 接続確立作業リスト

FTP接続を確立するには、以下のタスクを実行してください。

1. (任意)発信FTPパケットの送信元IPアドレスの指定
2. FTP接続の確立
3. FTPファイル転送モードと動作モードの設定

制限事項とガイドライン

ftpコマンドで指定された送信元IPアドレスは、**ftp client source**コマンドで設定されたアドレスよりも優先されます。

ftp ipv6 コマンドで指定された送信元 IP アドレスは、**ftp client ipv6source** コマンドで設定されたアドレスよりも優先されます。

送信 FTP パケットの送信元 IP アドレスの指定

1. システムビューに入ります。

   system-view

2. 送信FTPパケットの送信元IPアドレスを指定します。

   IPv4:

   ftp client source { interface *interface-type interface-number* **| ip** *source-ip-address* }

   デフォルトでは、送信元IPアドレスは指定されません。デバイスは、出力インターフェイスのプライマリIPアドレスを送信元IPアドレスとして使用します。

   IPv6:

   ftp client ipv6 source { interface *interface-type interface-number* **| ipv6** *source-ipv6-address* **}**

   デフォルトでは、送信元IPv6アドレスは指定されません。送信元アドレスは、RFC3484の定義に従って自動的に選択されます。

FTP 接続の確立

- ユーザービューからFTPサーバーにログインします。

  IPv4:

  ftp [*ftp-server* **[** *service-port* **] [vpn-instance** *vpn-instance-name* **]** [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** source-ip-address } | **-d**] *]

  IPv6:

  ftp ipv6 [*ftp-server* **[** *service-port* **] [vpn-instance** *vpn-instance-name* **]** [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* } | **-d**] * [**-i** *interface-type interface-number*]]

- FTPクライアントビューからFTPサーバーにログインします。
  a. FTPクライアントビューに入ります。

     ftp [ipv6]

  b. FTPサーバーにログインします。

     open *server-address* **[** *service-port* **]**

FTP ファイル転送モードと動作モードの設定

1. ユーザービューからFTPクライアントビューに入ります。

   ftp

2. ファイル転送モードを設定します。
   - ファイル転送モードをASCIIに設定します。

     ascii

   - ファイル転送モードをバイナリに設定します。

     binary

     デフォルトのファイル転送モードはバイナリです。

3. FTP動作モードを変更します。

   passive

   デフォルトのFTP動作モードはpassiveです。

コマンドヘルプ情報の表示

1. ユーザービューからFTPクライアントビューに入ります。

   ftp

2. コマンドヘルプ情報を表示します。
   - **help [** *command-name* **]**
   - **? [** *command-name* **]**

FTP サーバー上のディレクトリとファイルの表示

1. ユーザービューからFTPクライアントビューに入ります。

   ftp

2. FTPサーバー上のディレクトリとファイルを表示します。
   - **dir [** *remotefile* **[** *localfile* **]]**
   - **ls [** *remotefile* **[** *localfile* **]]**

FTP サーバー上のディレクトリの管理

前提条件

FTPサーバー上のディレクトリとファイルを表示するには、dirまたはlsコマンドを使用します。

手順

1. ユーザービューからFTPクライアントビューに入ります。

   ftp
2. FTPサーバー上のディレクトリを管理します。
   - FTPサーバー上でアクセスされている作業ディレクトリを表示します。

     pwd
   - FTPサーバー上の作業ディレクトリを変更します。

     cd { *directory* **| .. | / }**
   - FTPサーバーの上位ディレクトリに戻ります。

     cdup
   - FTPサーバー上にディレクトリを作成します。

     mkdir *directory*
   - リモートFTPサーバーからディレクトリを削除します。

     rmdir *directory*

FTP クライアント上のディレクトリの管理

1. ユーザービューからFTPクライアントビューに入ります。

   ftp
2. FTPクライアントのローカル作業ディレクトリを表示または変更します。

   lcd [*directory* **| /]**

   ファイルをアップロードするには、このコマンドを使用してファイルが存在するディレクトリに変更します。ダウンロードしたファイルは作業ディレクトリに保存されます。

FTP サーバー上のファイルの操作

前提条件

FTPサーバー上のディレクトリとファイルを表示するには、dirまたはlsコマンドを使用します。

手順

1. ユーザービューからFTPクライアントビューに入ります。

   ftp

2. FTPサーバー上のファイルを操作します。
   - FTPサーバーからファイルを完全に削除します。
     delete *remotefile*
     このコマンドを使用するには、削除権限が必要です。
   - ファイル名を変更する。
     rename [*oldfilename* **[** *newfilename* **]]**
   - ファイルをFTPサーバーにアップロードします。
     put *localfile* **[** *remotefile* **]**
   - FTPサーバーからファイルをダウンロードします。
     get *remotefile* **[** *localfile* **]**
   - FTPクライアント上のファイルの内容をFTPサーバー上のファイルに追加します。
     append *localfile* **[** *remotefile* **]**
   - 再送信マーカーを指定します。
     restart *marker*
     このコマンドは、put、get、または append コマンドと一緒に使用します。
   - ローカルファイルを更新します。
     newer *remotefile*
   - ファイルの欠落部分を取得します。
     reget *remotefile* **[** *localfile* **]**

別のユーザーカウントに変更する

別のユーザーアカウントに変更するについて

FTPサーバーにログインした後、FTP認証を開始して新規アカウントに変更できます。新規アカウントに変更すると、FTP接続を再確立せずに別の権限を取得できます。

制限事項とガイドライン

アカウントを正常に変更するには、新しいユーザー名とパスワードを正しく入力する必要があります。ユーザー名またはパスワードが正しくないと、FTP接続が切断される可能性があります。

手順

1. ユーザービューからFTPクライアントビューに入ります。
   ftp
2. 現在のFTP接続でFTP認証を開始します。
   user *username* **[** *password* **]**

FTP 接続の保守とトラブルシューティング

このタスクについて

デバイスを使用してFTPサーバーへのFTP接続を確立した後、このセクションのコマンドを使用して、FTP接続に関する問題の特定とトラブルシューティングを行います。

手順

1. ユーザービューからFTPクライアントビューに入ります。

   ftp

2. FTP接続のメンテナンスとトラブルシューティングを行います。
   - FTPサーバーでサポートされているFTPコマンドを表示します。

     rhelp
   - FTPサーバーでサポートされているFTPコマンドに関するヘルプ情報を表示します。

     rhelp *protocol-command*
   - FTPサーバーのステータスを表示します。

     rstatus
   - FTPサーバー上のディレクトリまたはファイルに関する詳細情報を表示します。

     rstatus *remotefile*
   - FTP接続ステータスを表示します。

     status
   - FTPサーバーのシステム情報を表示します。

     system
   - FTP動作情報表示を有効または無効にします。

     verbose

     デフォルトでは、この関数は有効になっています。
   - FTPクライアントのデバッグを有効にします。

     debug

     デフォルトでは、FTPクライアントのデバッグは無効です。
   - バッファー内の応答情報をクリアします。

     reset

FTP 接続の終了

1. ユーザービューからFTPクライアントビューに入ります。

   ftp

2. 接続を終了します。
   - FTPクライアントビューを終了せずに、FTPサーバーへの接続を終了します。

     disconnect

     close
   - FTPサーバーへの接続を終了し、ユーザービューに戻ります。

     bye

     quit

FTP クライアントの表示およびメンテナンスコマンド

任意のビューでdisplayコマンドを実行します。

タスク	コマンド
FTPクライアントの送信元IPアドレス情報を表示します。	**display ftp client source**

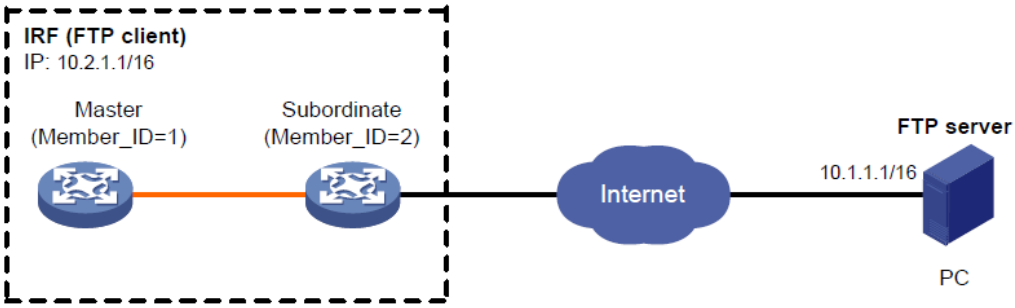
例:デバイスを FTP クライアントとして使用する

ネットワークの設定

図19に示すように、PCはFTPサーバーとして動作しています。ユーザー名**abc**、パスワード**123456**のユーザーカウントがPC上に作成されています。

- IRFファブリックをFTPクライアントとして使用して、FTPサーバーにログインします。
- FTPサーバーからFTPクライアントに**temp.bin**ファイルをダウンロードします。
- バックアップのために、FTPクライアントからFTPサーバーにコンフィギュレーションファイル**config.cfg**をアップロードします。

図19ネットワーク図



Note: The orange line represents an IRF connection.

手順

#図19のようにIPアドレスを設定します。IRFファブリックとPCが互いに通信できることを確認します(詳細は省略します)。

#メンバーデバイスのストレージスペースを調べます。空きスペースが不足している場合は**delete/unreserved** *file*コマンドを使用して、使用されていないファイルを削除します(詳細は省略します)。

#ユーザー名**abc**とパスワード**123456**を使用して、10.1.1.1のFTPサーバーにログインします。

<Sysname> ftp

10.1.1.1 Press

CTRL+C to abort.

Connected to 10.1.1.1 (10.1.1.1).

220 WFTPD 2.0 service (by Texas Imperial Software) ready for new

user User (10.1.1.1:(none)): abc

331 Give me your password,

please Password:

230 Logged in successfully

Remote system type is

MSDOS. ftp>

#ファイル転送モードをバイナリに設定します。

ftp> binary

200 TYPE is now 8-bit binary

temp.binファイルをPCからマスターデバイスのフラッシュメモリーのルートディレクトリにダウンロードします。

ftp> get temp.bin

local: temp.bin remote: temp.bin

150 Connecting to port 47457

226 File successfully transferred

23951480 bytes received in 95.399 seconds (251.0 kbyte/s)

temp.binファイルをPCから下位メンバー(メンバーIDが2)のフラッシュメモリーのルートディレクトリにダウンロードします。

ftp> get temp.bin slot2#flash:/temp.bin

#ASCIIモードを使用して、バックアップ用にIRFファブリックからPCにコンフィギュレーションファイル**config.cfg**をアップロードします。

ftp> ascii

200 TYPE is now ASCII

ftp> put config.cfg back-config.cfg local:

config.cfg remote: back-config.cfg

150 Connecting to port 47461

226 File successfully transferred

3494 bytes sent in 5.646 seconds (618.00

kbyte/s) ftp> bye

221-Goodbye. You uploaded 2 and downloaded 2 kbytes.

221 Logout.

<Sysname>

TFTP の設定

TFTPについて

Trivial File Transfer Protocol(TFTP)は、安全で信頼性の高いネットワーク上でファイルを転送するためのFTPの簡易バージョンです。TFTPでは、データ送信にUDPポート69が使用されます。TCPベースのFTPとは対照的に、TFTPは認証や複雑なメッセージ交換を必要とせず、導入が簡単です。TFTPは信頼性の高いネットワーク環境に適しています。

FIPS準拠

デバイスは、NIST FIPS140 - 2要件に準拠するFIPSモードをサポートしています。機能、コマンド、およびパラメーターのサポートは、FIPSモードと非FIPSモードで異なる場合があります。FIPSモードの詳細については、Security Configuration Guideを参照してください。

FIPSモードでは、TFTPはサポートされていません。

制約事項およびガイドライン

デバイスからTFTPサーバーにファイルをアップロードするか、TFTPサーバーからデバイスにファイルをダウンロードできます。

ファイルをダウンロードする際のベストプラクティスとして、存在しないファイル名を宛先ファイル名として指定します。ターゲットディレクトリに存在するファイル名のファイルをダウンロードすると、デバイスは既存のファイルを削除して新規ファイルを保存します。ネットワークの切断などの理由でファイルのダウンロードに失敗すると、元のファイルをリストアできません。

デバイスは、TFTPクライアントとしてだけ動作できます。

IP v4 TFTPクライアントの設定と使用

1. システムビューに入ります。

   system-view
2. (任意)ACLを使用して、TFTPサーバーへのクライアントのアクセスを制御します。

   tftp-server acl *acl-number*

   デフォルトでは、アクセス制御にACLは使用されません。
3. TFTPクライアントから送信されるTFTPパケットの送信元IPアドレスを指定します。

   tftp client source { interface i*nterface-type interface-number* **| ip** source-ip-address }

   デフォルトでは、送信元IPアドレスは指定されません。デバイスは、出力インターフェイスのプライマリIPアドレスを送信元IPアドレスとして使用します。
4. ユーザービューに戻ります。

   quit
5. IPv4ネットワークでファイルをダウンロードまたはアップロードします。

   tftp *tftp-server* **{ get | put | sget }** *source-filename* [*destination-filenam*e] [**vpn-instance** *vpn-instance-name*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }] *

   このコマンドで指定された送信元IPアドレスは、tftp client sourceコマンドを使用して設定された送信元IPアドレスよりも優先されます。

IP v6 TFTPクライアントの設定と使用

1. システムビューに入ります。

   system-view
2. (任意)ACLを使用して、TFTPサーバーへのクライアントのアクセスを制御します。

   tftp-server ipv6 acl *ipv6-acl-number*

   デフォルトでは、アクセス制御にACLは使用されません。
3. TFTPクライアントから送信されるTFTPパケットの送信元IPv6アドレスを指定します。

tftp client ipv6 source { *interface interface-type interface-number* **| ipv6** *source-ipv6-address* **}**

デフォルトでは、送信元IPv6アドレスは指定されません。送信元アドレスは、RFC3484の定義に従って自動的に選択されます。

4. ユーザービューに戻ります。

   quit

5. IPv6ネットワークでファイルをダウンロードまたはアップロードします。

   tftp ipv6 *tftp-server* **[-i** *interface-type interface-number* **] { get | put** | **sget** } *source-filename* [*destination-filename*] [**vpn-instance** *vpn-instance-name*] [**dscp** *dscp-value* | **source** { *interface interface-type interface-number* | **ipv6** *source-ipv6-address* }] *

   このコマンドで指定された送信元IPアドレスは、tftp client ipv6 sourceコマンドで設定された送信元IPアドレスよりも優先されます。

ファイルシステムの管理

この章では、ファイルシステムの管理方法について説明します。

ファイルシステム管理について

ストレージメディアとファイルシステム

デバイスは、固定ストレージメディア(フラッシュメモリー)とホットスワップ対応ストレージメディア(USBディスク)の両方をサポートします。

- 固定記憶媒体は、1つのファイルシステムを有します。
- ホットスワップ可能なストレージメディアはパーティション化できます。パーティション化されていない各ストレージメディアには1つのファイルシステムがあります。パーティション化されたストレージメディアでは、各パーティションに1つのファイルシステムがあります。

ストレージメディアとファイルシステムの命名ルール

フラッシュメモリー上のファイルシステムは、フラッシュメモリーと同じ名前です。この名前には次の部分があります。

- 記憶媒体タイプは**flash**。
- コロン(:)。

USBディスク名とファイルシステム名は、次の部分を共有します。

- 記憶媒体タイプは**usb**。
- シーケンス番号。a、b、cなどの小文字の英語。
- パーティション番号。0から始まり、1ずつ増加する数字です。ストレージメディアがパーティション化されていない場合、システムはストレージメディアにパーティションが1つあると判断します(ストレージメディア名にパーティション番号は含まれません)。
- コロン(:)。

たとえば、最初のUSBディスクの名前はusba:で、最初のUSBディスクの最初のパーティション上のファイルシステムの名前はusba0:です。

重要:

ファイルシステム名は大文字と小文字が区別されるため、小文字で入力する必要があります。

ファイルシステムの場所

マスターデバイス上のファイルシステムを識別するには、ファイルシステムの場所を指定する必要はありません。下位メンバーデバイス上のファイルシステムを識別するには、**slot***n*#形式でファイルシステムの場所を指定する必要があります。n引数は、メンバーデバイスのIRFメンバーIDを表します。例えば、メンバーデバイス2上にあるファイルシステムの場所は**slot2#**です。

重要:

ファイルシステムの場所の文字列では、大文字と小文字が区別されるため、小文字で入力する必要があります。

デフォルトファイルシステム

ログイン後、デフォルトのファイルシステムで作業しています。デフォルトのファイルシステム上のファイルまたはディレクトリを指定するには、ファイルシステム名を指定する必要はありません。たとえば、稼働中のコンフィギュレーションをデフォルトのファイルシステムのルートディレクトリに保存する場合、場所情報を指定する必要はありません。

デフォルトのファイルシステムを変更するには、BootWareまたはBoot ROMメニューを使用します。詳細については、ソフトウェアのリリースノートを参照してください。

ディレクトリ

ファイルシステム内のディレクトリは、ツリー形式で構造化されます。

ルートディレクトリ

ルートディレクトリは、スラッシュ(/)で表され、例えば、flash:/は、フラッシュメモリーのルートディレクトリを表します。

稼働中のディレクトリ

稼働中のディレクトリはカレントディレクトリとも呼ばれます。

ディレクトリの命名ルール

ディレクトリの名前を指定する場合は、次のルールに従います。

- ディレクトリ名には、アスタリスク(*)、縦棒(|)、スラッシュ(/)、バックスラッシュ(\)、疑問符 (?) 、左山カッコ (<) 、右山カッコ (>) 、引用符 (") 、コロン (:) 以外の文字、数字、および特殊文字を含めることができます。
- 名前がドット文字(.)で始まるディレクトリは非表示ディレクトリです。システムがディレクトリを非表示にしないようにするには、ディレクトリ名がドット文字で始まらないようにします。

一般的に使用されるディレクトリ

デバイスには工場出荷時のデフォルトディレクトリがいくつかあります。システムは、操作中に自動的にディレクトリを作成します。これらのディレクトリには、次のものが含まれます。

- **diagfile:** 診断情報ファイルを保存します。
- **license:** ライセンスを保存します。
- **logfile:** ログファイルを保存します。
- **seclog:** セキュリティログファイルを保存します。

- **versionInfo:** ソフトウェアバージョン情報ファイルを保存します。

ファイル

ファイルの命名ルール

ファイルの名前を指定する場合は、次のルールに従います。

- ファイル名には、アスタリスク(*)、縦棒()、スラッシュ(/)、円記号(\)、疑問符(?)、左山カッコ(<)、右山カッコ(>)、引用符(")、コロン(:)以外の文字、数字、特殊文字を使用できます。
- 名前がドット文字(.)で始まるファイルは隠しファイルです。システムがファイルを隠しないようにするには、ファイル名がドット文字で始まっていないことを確認してください。

一般的なファイルタイプ

デバイスには工場出荷時のデフォルトファイルがいくつかあり、操作中に自動的にいくつかのファイルが作成される場合があります。これらのファイルの種類は次のとおりです。

- **.ipe ファイル:** 圧縮されたソフトウェアイメージパッケージファイル。
- **.binファイル:** ソフトウェアイメージファイル。
- **.cfgファイル :** コンフィギュレーションファイル。
- **.mdbファイル:** バイナリコンフィギュレーションファイル。
- **.log ファイル:** ログファイル。

ディレクトリ名またはファイル名の指定

ディレクトリ名の指定

ディレクトリを指定するには、絶対パスまたは相対パスを使用できます。例えば、作業ディレクトリはflash:/です。図20のtest2ディレクトリを指定するには、次のメソッドを使用できます。

- **flash:/test/test1/test2(絶対パス)**
- **flash:/test/test1/test2/(絶対パス)**
- **test/test1/test2(相対パス)**
- **test/test1/test2/(相対パス)**

図20 ディレクトリ階層のサンプル

ファイル名の指定

ファイルを指定するには、次の方法を使用します。

- ファイルの絶対パスとファイル名filesystem/directory1/directory2/…/directoryn/filenameの形式で入力します。directorynはファイルが存在するディレクトリです。
- ファイルの相対パスとファイル名を入力します。

たとえば、作業ディレクトリは**flash:/**です。**samplefile.cfg**ファイルは、図20に示す**test2**ディレクトリにあります。ファイルを指定するには、次のメソッドを使用できます。

- **flash:/test/test1/test2/samplefile.cfg**
- **test/test1/test2/samplefile.cfg**

FIPS準拠

デバイスは、NIST FIPS140 - 2要件に準拠するFIPSモードをサポートしています。機能、コマンド、およびパラメーターのサポートは、FIPSモードと非FIPSモードで異なる場合があります。FIPSモードの詳細については、Security Configuration Guideを参照してください。

制約事項およびガイドライン:ファイルシステム管理

ファイルシステムの破損を回避するには、ファイルシステムの管理中に次のタスクを実行しないでください。

- ストレージメディアをインストールまたは削除します。
- マスター/下位スイッチオーバーを実行します。

メディア上のディレクトリまたはファイルにアクセス中にストレージメディアを削除すると、再インストール時にデバイスがメディアを認識しない場合があります。この種類のストレージメディアを再インストールするには、次のいずれかの作業を行います。

- ストレージメディア上のディレクトリにアクセスしていた場合は、作業ディレクトリを変更します。
- ストレージメディア上のファイルにアクセスしていた場合は、ファイルを閉じます。
- 別の管理者がストレージメディアにアクセスしていた場合は、ストレージメディア上のすべてのパーティションをアンマウントします。

ディスクへの書き込み権限が必要な操作を行う前に、USBディスクが書き込み保護されていないことを確認してください。

パーティション分割されているストレージメディアや、フォーマットまたは修復されているファイルシステムにはアクセスできません。

ファイルシステム、ディレクトリ、ファイルを管理する前に、考えられる影響を確認してください。

ストレージメディアとファイルシステムの管理

ストレージメディアのパーティション設定

このタスクについて

記憶媒体は、パーティションと呼ばれる論理デバイスに分割できます。1つのパーティションに対する操作は、他のパーティションに影響を与えません。

制限事項とガイドライン

重要:

ストレージメディアをパーティションに分割すると、メディア上のすべてのデータが消去されます。

フラッシュメモリーはパーティション分割をサポートしていません。

ストレージメディアをパーティションに分割する前に、次のタスクを実行します。

- 他のユーザーがメディアにアクセスしていないことを確認します。

- USBディスクをパーティション化するには、ディスクが書き込み保護されていないことを確認してください。ディスクが書き込み保護されている場合、パーティション化操作は失敗します。USBディスクへのアクセスを復元するには、ディスクを再インストールするか、ディスク上のファイルシステムを再マウントする必要があります。

パーティションには、32MB以上のストレージスペースが必要です。

実際のパーティションサイズと指定したパーティションサイズの差が、ストレージメディアの合計サイズの5%未満である可能性があります。

前提条件

ストレージメディアのファイルをバックアップします。

手順

ストレージメディアをパーティション分割するには、ユーザービューで次のコマンドを実行します。

fdisk *medium [Partition-number]*

記憶媒体を均等に分割するには、partition-number引数を指定します。パーティションのサイズをカスタマイズするには、partition-number引数を指定しないでください。このコマンドでは、パーティションごとにサイズを指定する必要があります。

ファイルシステムのマウントまたはアンマウント

制限事項とガイドライン

マウントまたはアンマウントできるのは、ホットスワップ可能なストレージメディア上にあるファ

イルシステムのみです。他のユーザーがファイルシステムにアクセスしていない場合にのみ、

ファイルシステムをアンマウントできます。

USBディスクとUSBインターフェイスが破損しないようにするには、USBディスク上のファイルシステムをアンマウントする前に、次の要件が満たされていることを確認します。

- システムはUSBディスクを認識。
- USBディスクのLEDは点滅しない。

ファイルシステムのマウント

ファイルシステムをマウントするには、ユーザービューで次のコマンドを実行します。

mount *filesystem*

ホットスワップ可能なストレージメディア上のファイルシステムは、ストレージメディアがデバイスに接続されると自動的にマウントされます。システムがファイルシステムを認識できない場合は、アクセスする前にファイルシステムをマウントする必要があります。

ファイルシステムのアンマウント

ファイルシステムをアンマウントするには、ユーザービューで次のコマンドを実行します。

umount *filesystem*

ホットスワップ可能なストレージメディアをデバイスから取り外すには、まずストレージメディア上のすべてのファイルシステムをアンマウントして、デバイスからメディアを切断する必要があります。接続されているホットスワップ可能なストレージメディアを取り外すと、ストレージメディア上のファイル、またはストレージメディア自体が破損する可能性があります。

ファイルシステムのフォーマット

制限事項とガイドライン

ファイルシステムをフォーマットすると、ファイルシステム内のすべてのファイルおよびディレクトリが完全に削除されます。削除したファイルまたはディレクトリはリストアできません。

他のユーザーがファイルシステムにアクセスしていない場合にのみ、ファイルシステムをフォーマットできます。

手順

ファイルシステムをフォーマットするには、ユーザービューで次のコマンドを実行します。

format *filesystem*

ファイルシステムの修復

制限事項とガイドライン

ファイルシステムの一部にアクセスできない場合、このタスクを使用してファイルシステムを

調査および修復します。他のユーザーがファイルシステムにアクセスしていない場合にの

み、ファイルシステムを修復できます。

手順

ファイルシステムを修復するには、ユーザービューで次のコマンドを実行します。

fixdisk *filesystem*

ファイルとディレクトリの管理

ファイルとディレクトリの動作モードの設定

このタスクについて

デバイスは、次の動作モードをサポートします。

- **alert:** ファイルの破損やデータの損失などの問題が発生する可能性がある操作について、確認を求めるプロンプトが表示されます。このモードでは、中断を伴う操作をキャンセルできます。
- **quiet:** ごみ箱を空にする操作を除き、ファイルまたはディレクトリの操作を実行するときに、確認メッセージは表示されません。

手順

1. システムビューに入ります。

   system-view
2. ファイルとディレクトリの操作モードを設定します。

   file prompt { alert | quiet }

デフォルトのモードはalertです。

ファイルおよびディレクトリ情報の表示

ファイルおよびディレクトリ情報を表示するには、ユーザービューで次のコマンドを実行します。

dir [/all] [*file* | *directory* | **/all-filesystems]**

複数のユーザーが同時にファイル操作(ファイルやディレクトリの作成や削除など)を実行すると、このコマンドの出力が正しくない場合があります。

テキストファイルの内容を表示する

テキストファイルの内容を表示するには、ユーザービューで次のコマンドを実行します。

more *file*

作業ディレクトリの表示

作業ディレクトリを表示するには、ユーザービューで次のコマンドを実行します。

pwd

稼働中のディレクトリの変更

このタスクについて

デフォルトの稼働中のディレクトリは、マスターデバイス上のデフォルトファイルシステムのルートディレクトリです。

手順

作業ディレクトリを変更するには、ユーザービューで次のコマンドを実行します。

cd { *directory* | *..* }

ディレクトリの作成

ディレクトリを作成するには、ユーザービューで次のコマンドを実行します。

mkdir *directory*

ファイルまたはディレクトリの名前の変更

ファイルまたはディレクトリの名前を変更するには、ユーザービューで次のコマンドを実行します。

rename *{ source-file* | *source-directory } { dest-file* | *dest-directory }*

ファイルのコピー

ファイルをコピーするには、ユーザービューでコマンドを実行します。

非FIPSモードの場合:

copy *source-file* { *dest-file* | *dest-directory* } [**vpn-instance** *vpn-instance-name] [* **source interface** *interface-type interface-number]*

FIPSモードの場合:

copy *source-file { dest-file* | *dest-directory }*

ファイルの移動

ファイルを移動するには、ユーザービューで次のコマンドを実行します。

move *source-file { dest-file* | *dest-directory }*

ファイルの削除と復元

ファイルの削除と復元について

ファイルは完全に削除することも、ファイルシステムのごみ箱に移動することもできます。ごみ箱に移動されたファイルは復元できますが、完全に削除されたファイルは復元できません。

各ファイルシステムにはごみ箱があります。ごみ箱は、ファイルシステムのルートディレクトリにある**.trash**という名前のディレクトリです。

制限事項とガイドライン

ごみ箱のファイルが記憶域を占有しています。占有している記憶域を解放するには、ごみ箱からファイルを削除してください。

ごみ箱からファイルを削除するには、**reset recycle-bin** コマンドを使用します。
deleteコマンドを実行すると、ごみ箱が正しく動作しない可能性があります。ごみ箱のファイルを表示するには、次のいずれかの方法を使用します。

- ファイルシステムのルートディレクトリにアクセスし、**dir / all .trash**コマンドを実行します。
- ファイルシステムのごみ箱ディレクトリにアクセスし、**dir**コマンドを実行します。

ファイルの削除

ファイルを削除するには、ユーザービューで次のいずれかのコマンドを実行します。

- ファイルをごみ箱に移動して削除します。
  delete *file*
- ファイルを完全に削除します。
  delete /unreserved *file*
- ごみ箱からファイルを削除します。
  reset recycle-bin [**/force**]

ファイルの復元

ごみ箱からファイルを復元するには、ユーザービューで次のコマンドを実行します。

undelete *file*

ディレクトリの削除

制限事項とガイドライン

ディレクトリを削除するには、ディレクトリ内のすべてのファイルとサブディレクトリを削除する必要があります。ディレクトリを削除すると、ごみ箱にあるすべてのファイルが完全に削除されます。

手順

ディレクトリを削除するには、ユーザービューで次のコマンドを実行します。

rmdir *directory*

ファイルとディレクトリのアーカイブ

このタスクについて

ファイルバックアップなどの目的で、ファイルおよびディレクトリを1つのファイルにアーカイブできます。元のファイルおよびディレクトリは引き続き存在します。

ファイルとディレクトリをアーカイブする場合は、アーカイブファイルを圧縮して、アーカイブファイルが使用するストレージスペースを少なくすることができます。

手順

ファイルとディレクトリをアーカイブするには、ユーザービューで次のコマンドを実行します。

tar create [gz] archive-file *dest-file* [**verbose**] **source** { *source-file* | *source-directory* } &<1-5>

ファイルとディレクトリの抽出

このタスクについて

この機能を使用して、アーカイブファイルからファイルとディレクトリを抽出します。

手順

ファイルとディレクトリを抽出するには、ユーザービューで次のコマンドを実行します。

1. (任意)アーカイブされたファイルおよびディレクトリを表示します。

   tar list archive-file *file*

2. ファイルとディレクトリを抽出します。

   tar extract archive-file *file* **[verbose] [screen | to** *directory* **]**

ファイルの圧縮

ファイルを圧縮するには、ユーザービューで次のコマンドを実行します。

gzip *file*

ファイルの解凍

ファイルを解凍するには、ユーザービューで次のコマンドを実行します。

gunzip *file*

ファイルダイジェストの計算

このタスクについて

ファイルダイジェストは、ファイルの整合性を検証するために使用されます。

手順

ファイルのダイジェストを計算するには、ユーザービューで次のいずれかのコマンドを実行します。

- SHA-256アルゴリズムを使用します。
  sha256sum *file*
- MD5アルゴリズムを使用します。
  md5sum *file*

コンフィギュレーションファイルの管理

コンフィギュレーションファイル管理について

コンフィギュレーションファイルは、CLIまたはBootWareメニューから管理できます。次に、CLIからコンフィギュレーションファイルを管理する方法について説明します。

コンフィギュレーションファイルには、デバイス上でソフトウェア機能を構成するための一連のコマンドが保存されます。コンフィギュレーションファイルに任意の構成を保存して、リブート後も構成を維持できます。また、将来使用するために、コンフィギュレーションファイルをホストにバックアップすることもできます。

コンフィギュレーションタイプ

初期設定

初期設定は、ソフトウェアのコンフィギュレーションコマンドの初期デフォルト設定の集合です。

BootWareメニューにアクセスして**Skip Current System Configuration**オプションを選択すると、デバイスは初期設定で起動します。この状況では、デバイスは空の設定で起動していると表示されることもあります。

初期設定を表示するコマンドはありません。コンフィギュレーションコマンドの初期デフォルト設定を表示するには、コマンドリファレンスのデフォルトセクションを参照してください。

出荷時のデフォルト設定

出荷時のデフォルトは、デバイスに付属のカスタム基本設定です。出荷時のデフォルトはデバイスモデルによって異なり、コマンドの初期デフォルト設定とは異なる場合があります。

次のスタートアップコンフィギュレーションファイルが使用できない場合、デバイスは工場出荷時のデフォルトで起動します。

工場出荷時のデフォルトを表示するには、**display default-configuration**コマンドを使用します。

スタートアップコンフィギュレーション

デバイスは、スタートアップコンフィギュレーションを使用して、起動時にソフトウェア機能を設定します。デバイスの起動後、次の起動時にロードするコンフィギュレーションファイルを指定できます。このコンフィギュレーションファイルは、次のスタートアップコンフィギュレーションファイルと呼ばれます。ロードされたコンフィギュレーションファイルは、現在のスタートアップコンフィギュレーションファイルと呼ばれます。

スタートアップコンフィギュレーションを表示するには、次のいずれかの方法を使用します。

- 現在のスタートアップコンフィギュレーションファイルの内容を表示するには、デバイスのリブート後にコンフィギュレーションを変更する前に、**display current-configuration**コマンドを実行します。
- 次のスタートアップコンフィギュレーションファイルの内容を表示するには、**display saved-configuration** コマンドを使用します。
- 現在のスタートアップコンフィギュレーションファイルおよび次のスタートアップコンフィギュレーションファイルの名前を表示するには、**display startup**コマンドを使用します。次に、**more**コマンドを使用して、指定したスタートアップコンフィギュレーションファイルの内容を表示できます。

稼働中のコンフィギュレーション

稼働中のコンフィギュレーションには、変更されていない起動設定と新しい設定が含まれます。稼働中のコンフィギュレーションはメモリーに保存され、デバイスのリブートまたは電源オフ時にクリアされます。電源の再投入またはリブート後に実行コンフィギュレーションを使用するには、コンフィギュレーションファイルに保存します。

稼働中のコンフィギュレーションを表示するには、**display current-configuration** コマンドを使用します。

コンフィギュレーションファイルの種類と起動時のファイル選択プロセス

コンフィギュレーションを保存すると、設定は.cfg コンフィギュレーションファイルと.mdbファイルに保存されます。

- .cfg コンフィギュレーションファイルは人が読めるテキストファイルであり、その内容は**more**コマンドを使用して表示できます。コンフィギュレーションを保存するために指定するコンフィギュレーションは拡張子は.cfgでなければなりません。
- .mdbファイルは、ユーザーがアクセスできないバイナリファイルで、.cfgファイルと同じ名前を持ちます。デバイスは、.cfgファイルをロードするよりも速く.mdbファイルをロードします。

起動時に、デバイスは次の手順を使用して、ロードするコンフィギュレーションファイルを識別します。

1. デバイスは、有効な.cfg 次のスタートアップコンフィギュレーションファイルを検索します。ファイル選択ルールの詳細については、「次のスタートアップコンフィギュレーションファイルの冗長性」を参照してください。
2. 有効な.cfg 次のスタートアップコンフィギュレーションファイルが見つかると、デバイスは.cfgファイルと同じ名前とチェックサムを持つ.mdbファイルを検索します。
3. 一致する.mdbファイルが見つかった場合、デバイスは.mdbファイルで起動します。見つからない場合、デバイスは.cfgファイルで起動します。

次のスタートアップコンフィギュレーションファイル.cfg が使用できない場合、デバイスは工場出荷時のデ

フォルトで起動します。

特に明記されていない限り、このドキュメントの"コンフィギュレーションファイル"という用語は.cfg コンフィギュレーションファイルを指します。

次のスタートアップコンフィギュレーションファイルの冗長性

冗長性を確保するために、1つのメイン次のスタートアップコンフィギュレーションファイルと1つのバックアップ次のスタートアップコンフィギュレーションファイルを指定できます。

起動時に、デバイスは次の順序で.cfgスタートアップコンフィギュレーションを選択しようとします。

1. メインの次のスタートアップコンフィギュレーションファイル。
2. バックアップ次のスタートアップコンフィギュレーションファイル(メインの次のスタートアップコンフィギュレーションファイルが存在しないか破損している場合)。

次のスタートアップコンフィギュレーションファイルがない場合、デバイスは工場出荷時のデフォルトで起動します。

コンフィギュレーションファイルの内容の構成と形式

重要:

デバイス上で実行するには、コンフィギュレーションファイルがコンテンツとフォーマットの要件を満たしている必要があります。コンフィギュレーションのロード、ロールバック、または復元を正常に実行するには、デバイス上に作成されたコンフィギュレーションファイルを使用します。コンフィギュレーションファイルを編集する場合は、すべての編集内容が要件を満たしていることを確認してください。

コンフィギュレーションファイルは、次の要件を満たす必要があります。

- すべてのコマンドは、完全な形式で保存されます。
- コマンドは、システムビュー、インターフェイスビュー、プロトコルビュー、ユーザーラインビューなど、コマンドビューごとにセクションに分類されます。
- 隣接する2つのセクションは、シャープ記号(#)で区切られます。
- コンフィギュレーションファイルは**return**という語で終わります。

次に、コンフィギュレーションファイルの抜粋の例を示します。

```
#
local-user root class manage
  password hash
$h$6$Twd73mLrN8O2vvD5$Cz1vgdpR4KoTiRQNE9pg33gU14Br2p1VguczLSVyJLO2huV5Syx/LfDIf8ROLtVErJ/C31oq2rFtmNuyZf4STw==
    service-type ssh telnet terminal
    authorization-attribute user-role network-admin authorization-
    attribute user-role network-operator
#
interface Vlan-interface1
  ip address 192.168.1.84 255.255.255.0
  #
```

コンフィギュレーションロールバック

コンフィギュレーションロールバックを使用すると、デバイスをリブートせずに、実行コンフィギュレーションをコンフィギュレーションファイル内のコンフィギュレーションに置き換えることができます。この機能は、次の目的で使用できます。

- 以前の設定状態に戻す。
- 異なるネットワーク環境への実行コンフィギュレーションの適応。

FIPS準拠

デバイスは、NIST FIPS140 - 2要件に準拠するFIPSモードをサポートしています。機能、コマンド、およびパラメーターのサポートは、FIPSモードと非FIPSモードで異なる場合があります。FIPSモードの詳細については、Security Configuration Guideを参照してください。

コンフィギュレーションの暗号化の有効化

コンフィギュレーションの暗号化の有効化について

コンフィギュレーシの暗号化を使用すると、デバイスは実行コンフィギュレーションを保存するときにスタートアップコンフィギュレーションファイルを自動的に暗号化できます。Comware7ソフトウェアを実行するすべてのデバイスは、同じ秘密キーまたは公開キーを使用してコンフィギュレーションファイルを暗号化します。

制限事項とガイドライン

Comware7ソフトウェアを実行しているすべてのデバイスは、暗号化されたコンフィギュレーションファイルを復号化できます。暗号化されたファイルが不正なユーザーによって復号化されないようにするには、許可されたユーザーだけがファイルにアクセスできるようにします。

暗号化されたコンフィギュレーションファイルの内容を表示するためにmoreコマンドを使用することはできません。

手順

1. システムビューに入ります。

   system-view
2. 設定の暗号化を有効にします。

   configuration encrypt { private-key | public-key }

   デフォルトでは、設定の暗号化は無効です。

稼働中のコンフィギュレーションの保存

このタスクについて

稼働中のコンフィギュレーションを.cfgコンフィギュレーションファイルに保存する場合、そのファイルを次のスタートアップコンフィギュレーションファイルとして指定するかどうかを指定できます。

このファイルを.cfg 次のスタートアップコンフィギュレーションファイルとして指定する場合は、次のいずれかの方法を使用して設定を保存します。

- **fastモード: safely**キーワードを指定せずに**save**コマンドを使用します。このモードでは、デバイスはターゲットの次のスタートアップコンフィギュレーションファイルを直接上書きします。このプロセス中にリブートまたは電源障害が発生すると、次のスタートアップコンフィギュレーションファイルは失われます。デバイスのリブート後に新しいスタートアップコンフィギュレーションファイルを指定する必要があります。「次のスタートアップコンフィギュレーションファイルの指定」を参照。
- **safeモード: save**コマンドに**safely**キーワードを指定して使用します。セーフモードは、高速モードよりも低速ですが、より安全です。セーフモードでは、保存操作の完了後に、一時ファイルに設定が保存され、ターゲットの次のスタートアップコンフィギュレーションファイルの上書きが開始されます。保存操作中にリブートまたは電源障害が発生しても、次のスタートアップコンフィギュレーションファイルは保持されます。

  電源が信頼できない場合、またはデバイスをリモートで設定する場合は、セーフモードを使用します。

制限事項とガイドライン

次のスタートアップコンフィギュレーションが失われないようにするには、デバイスが実行コンフィギュレーションを保存している間に、デバイスのリブートや電源のオフ/オンを行わないようにします。

IRFメンバーデバイスがIRFファブリックから分割されると、その設定はメモリーに保持されますが、IRFファブリック上の実行コンフィギュレーションから削除されます。IRFファブリックが回復する前に実行コンフィギュレーションを保存すると、メンバーデバイスの設定が次のスタートアップコンフィギュレーションファイルから削除されます。

メンバーデバイスがIRFファブリックに再加入する前に実行コンフィギュレーションを保存した場合は、次の手順を実行して、メンバーデバイスの設定を次のスタートアップコンフィギュレーションファイルに復元します。

1. 分割の問題を解決します。
2. メンバーデバイスをリブートして、IRFファブリックに再接続します。
3. メンバーデバイスがIRFファブリックに再加入したら、**display current-configuration**コマンドを使用して、メンバーデバイスの設定がメモリーから稼働中のコンフィギュレーションに復元されたことを確認します。
4. 稼働中のコンフィギュレーションをIRFファブリック上の次のスタートアップコンフィギュレーションファイルに保存します。

重要:

コンフィギュレーションが正常に復元されるようにするには、メンバーデバイスが終了した後にIRFファブリックがリブートされていないことを確認します。

拡張インターフェイスカードをシステムから取り外すと、その設定はメモリーに保持されますが、システムの実行コンフィギュレーションから削除されます。交換用カードをインストールする前に実行コンフィギュレーションを保存すると、次のスタートアップコンフィギュレーションファイルからカードの設定が削除されます。

カードを取り外した後に実行コンフィギュレーションを保存した場合は、次の手順を実行して、カード設定を次のスタートアップコンフィギュレーションファイルに復元します。

1. 交換用カードを取り付けます。
2. 交換用カードがオンラインになったら、**display current-configuration**コマンドを実行して、カードの設定がメモリーから実行コンフィギュレーションに自動的に復元されたことを確認します。

3. 稼働中のコンフィギュレーションを次のスタートアップコンフィギュレーションファイルに保存します。

重要:
設定を正しく復元するには、カードを取り外した後にシステムがリブートされていないことを確認します。

手順

稼働中のコンフィギュレーションを保存するには、任意のビューで次のいずれかの作業を行います。

- 稼働中のコンフィギュレーションをコンフィギュレーションファイルに保存します、実行コンフィギュレーションをコンフィギュレーションファイルに保存します。

  save *file-url* [**all** | **slot** *slot-number*]
- 稼働中のコンフィギュレーションをストレージメディアのルートディレクトリにあるコンフィギュレーションファイルに保存し、そのファイルを次のスタートアップコンフィギュレーションファイルとして指定します。

  save [safely] [backup | main] [force] [changed]

  設定を確実に保存するには、safelyキーワードを指定することをお勧めします。

コンフィギュレーションの違いを比較する

コンフィギュレーションの違いを比較するについて

コンフィギュレーションファイルを比較したり、コンフィギュレーションファイルと稼働中のコンフィギュレーションの違いを比較したりできます。

比較のために次のスタートアップコンフィギュレーションを指定すると、比較対象の次のスタートアップコンフィギュレーションファイルが次の順序で選択されます。

1. メインの次のスタートアップコンフィギュレーションファイル。
2. メインの次のスタートアップコンフィギュレーションファイルが使用できない場合のバックアップ次のスタートアップコンフィギュレーションファイル。

両方のコンフィギュレーションファイルが使用できない場合、次のスタートアップコンフィギュレーションファイルが存在しないことを示すメッセージが表示されます。

手順

コンフィギュレーションの違いを比較するには、任意のビューで次のいずれかの作業を行います。

- コンフィギュレーションファイル、実行コンフィギュレーション、または次のスタートアップコンフィギュレーションと、指定したソースコンフィギュレーションファイルとの違いを表示します。

  display diff configfile *file-name-s* **{ configfile** *file-name-d* **| current-configuration | startup-configuration**}
- コンフィギュレーションファイルまたは次のスタートアップコンフィギュレーションと実行コンフィギュレーションの違いを表示します。

  display diff current-configuration { configfile *file-name-d* **| startup-configuration** }
- コンフィギュレーションファイルと次のスタートアップコンフィギュレーションとの違いを表示します。

  display diff startup-configuration configfile *file-name-d*
- 実行コンフィギュレーションと次のスタートアップコンフィギュレーションの違いを表示します。
  - 方法1:

display diff startup-configuration current-configuration

- 方法2:
  display current-configuration diff

コンフィギュレーションのロールバックを設定する

コンフィギュレーションロールバックタスクの概要

コンフィギュレーションロールバックを設定するには、以下のタスクを実行してください。

1. コンフィギュレーションアーカイブパラメーターの設定
2. 稼働中のコンフィギュレーションのアーカイブ
   - 自動構成アーカイブの有効化
   - 稼働中のコンフィギュレーションの手動アーカイブ
3. コンフィギュレーションのロールバック

コンフィギュレーションアーカイブパラメーターの設定

コンフィギュレーションアーカイブパラメーターの設定について

実行コンフィギュレーションをアーカイブする前に、コンフィギュレーションアーカイブのファイルディレクトリとファイル名プレフィクスを設定する必要があります。

アーカイブディレクトリは、ローカルデバイスまたはリモートSCPサーバーに配置できます。

ローカルアーカイブを使用する場合、コンフィギュレーションアーカイブにはprefix_serial number.cfgの形式で名前が付けられ、例えば、**archive_1.cfg**と**archive_2.cfg**のようになります。シリアル番号は1から1000まで自動的に割り当てられ、1ずつ増加します。シリアル番号が1000に達すると、再び1から割り当てられます。

ローカルデバイスのファイルディレクトリまたはファイル名プレフィクスを変更すると、次のイベントが発生します。

- 古いコンフィギュレーションアーカイブは、共通のコンフィギュレーションファイルに変更されます。
- コンフィギュレーションアーカイブカウンタがリセットされます。
- **display archive configuration**コマンドは、古いコンフィギュレーションアーカイブを表示しなくなりました。
- 新しいコンフィギュレーションアーカイブのシリアル番号は1から始まります。

稼働中のコンフィギュレーションをリモートSCPサーバーにアーカイブする場合、コンフィギュレーションアーカイブにはprefix_YYYYMMDD_HHMMSS.cfgの形式で名前が付けられます(たとえば、**archive_20170526_203430.cfg**)。YYYYMMDD_HHMMSS文字列は、コンフィギュレーションアーカイブが保存されたデバイスシステムの日時を表します。

リモートSCPサーバー上のファイルディレクトリまたはファイル名プレフィクスを変更すると、**display archive configuration**コマンドは、変更前に保存されていた古いコンフィギュレーションアーカイブを表示しなくなります。

コンフィギュレーションアーカイブパラメーターの設定に関する制約事項とガイドライン

ローカルアーカイブ(**archive configuration location** コマンド)とリモートアーカイブ(**archive configuration server** コマンド)は相互に排他的です。2 つの機能を同時に使用することはできません。

重要:

FIPSモードでは、デバイスはリモートSCPサーバーへの実行コンフィギュレーションのアーカイブをサポートしません。

ローカルコンフィギュレーションアーカイブでは、コンフィギュレーションアーカイブの最大数に達すると、システムは最も古いアーカイブを削除して新しいアーカイブ用のスペースを確保します。

リモートSCPサーバー上のコンフィギュレーションアーカイブの最大数は、SCPサーバー設定によって異なり、**archive configuration max**コマンドによって制限されません。

undo archive configuration locationコマンドは、ローカルコンフィギュレーションアーカイブディレクトリおよびファイル名プレフィクス設定を削除しますが、デバイス上のコンフィギュレーションアーカイブは削除しません。このコマンドは、次の操作も実行します。

- 手動設定と自動設定の両方のアーカイブ機能を無効にします。
- **archive configuration interval**および**archive configuration max**コマンドのデフォルト設定を復元します。
- **display archive configuration**コマンドを使用して表示されるコンフィギュレーションアーカイブ情報を消去します。

undo archive configuration serverコマンドは、リモートコンフィギュレーションアーカイブディレクトリおよびファイル名プレフィクス設定を削除しますが、サーバー上のコンフィギュレーションアーカイブは削除しません。このコマンドは、次の操作も実行します。

- 手動設定と自動設定の両方のアーカイブ機能を無効にします。
- **archive configuration interval**コマンドのデフォルト設定を復元します。
- **display archive configuration**コマンドを使用して表示されるコンフィギュレーションアーカイブ情報を消去します。

ローカルアーカイブパラメーターの構成

1. システムビューに入ります。

   system-view

2. 実行コンフィギュレーションをローカルデバイスにアーカイブするためのディレクトリおよびファイル名プレフィクスを設定します。

   archive configuration location *directory* **filename-prefix** *filename-prefix*

   デフォルトでは、デバイス上のコンフィギュレーションアーカイブにパスまたはファイル名プレフィクスが設定されておらず、システムは定期的にコンフィギュレーションを保存しません。

   コンフィギュレーションアーカイブディレクトリはマスターデバイス上にすでに存在している必要があり、メンバーIDを含めることはできません。

3. (任意)設定アーカイブの最大数を設定します。

   archive configuration max *file-number*

   デフォルトの数は5です。

   デバイスで使用可能なストレージ容量に応じて設定を変更します。

リモートアーカイブパラメーターの構成

1. システムビューに入ります。

   system-view

2. リモートSCPサーバーに実行コンフィギュレーションをアーカイブするためのディレクトリおよびファイル名プレフィクスを設定します。

   archive configuration server scp { *ipv4-address* **| ipv6** *ipv6-address* **} [port** *port-number* **] [vpn-instance** *vpn-instance-name* **] [directory** *directory* **] filename-prefix** *filename-prefix*

   デフォルトでは、実行コンフィギュレーションをリモートSCPサーバーにアーカイブするためのパスまたはファイル名プレフィクスは設定されていません。

3. SCPサーバーにアクセスするためのユーザー名を設定します。

   Archive configuration server user *user-name*

   デフォルトでは、SCPサーバーにアクセスするためのユーザー名は設定されていません。

4. SCPサーバーにアクセスするためのパスワードを設定します。

   archive configuration server password { **cipher** | **simple** } *string*

   デフォルトでは、SCPサーバーにアクセスするためのパスワードは設定されていません。

稼働中のコンフィギュレーションのアーカイブ

稼働中のコンフィギュレーションのアーカイブについて

次に、稼働中のコンフィギュレーションをアーカイブする方法を示します。

- **自動コンフィギュレーションアーカイブ** - システムは、設定された間隔で実行コンフィギュレーションを自動的にアーカイブします。
- **手動コンフィギュレーションアーカイブ** - 構成が頻繁に変更されない場合は、自動構成アーカイブを無効にして、実行中の構成を手動でアーカイブできます。複雑な構成タスクを実行する前に、この方法を使用することもできます。構成に失敗した場合は、アーカイブを使用して構成を回復できます。

稼働中のコンフィギュレーションのアーカイブに関する制約事項およびガイドライン

ローカルアーカイブを使用する場合、コンフィギュレーションアーカイブ機能は稼働中のコンフィギュレーションをマスターデバイスだけに保存します。

アーカイブ処理中に、**display archive configuration**コマンドを使用して表示されたアーカイブ構成情報をクリアしないでください。

自動コンフィギュレーションアーカイブの有効化

1. システムビューに入ります。

   system-view

2. 自動構成アーカイブを有効にし、アーカイブ間隔を設定します。

   archive configuration interval *interval*

   デフォルトでは、自動設定アーカイブは無効です。

稼働中のコンフィギュレーションの手動アーカイブ

ユーザービューでruningコンフィギュレーションを手動でアーカイブします。

archive configuration

コンフィギュレーションのロールバック

コンフィギュレーションのロールバックについて

コンフィギュレーションロールバック機能は、稼働中のコンフィギュレーションを指定された置換コンフィギュレーションファイルと比較し、コンフィギュレーションの違いを次のように処理します。

- 稼働中のコンフィギュレーションのコマンドが置換ファイルにない場合、ロールバック機能はコマンドのundo形式を実行します。
- 置換ファイル内のコマンドが実行コンフィギュレーションに含まれていない場合、ロールバック機能によってコマンドが稼働中のコンフィギュレーションに追加されます。
- 稼働中のコンフィギュレーションと置換ファイルでコマンドの設定が異なる場合、ロールバック機能は稼働中のコマンドの設定を置換ファイルの設定で置き換えます。

制限事項とガイドライン

ロールバックを正常に実行するには、システムがコンフィギュレーションをロールバックしている間は、拡張インターフェイスカードの取り付けや取り外し、またはマスター/下位スイッチオーバーを実行しないでください。

コンフィギュレーションロールバック機能は、次のいずれかの理由により、実行コンフィギュレーション内の一部のコマンドの再設定に失敗する場合があります。

- コマンドの前にundoキーワードを付けると、有効なundoコマンドにならないため、コマンドを元に戻すことができません。たとえば、**A** [**B**] **C**コマンド用に設計されたundoフォームが**undo A C**である場合、コンフィギュレーションロールバック機能**はA B C**コマンドを元に戻すことができません。これは、システムがundo A B Cコマンドを認識しないためです。
- コマンド(たとえば、ハードウェア依存のコマンド)は、システムの制約により、削除、上書き、取り消しができません。
- 異なるビューのコマンドは互いに依存しています。
- デバイスがサポートしていないコマンドまたはコマンド設定は、実行コンフィギュレーションに追加できません。

コンフィギュレーションアーカイブ機能またはローカルデバイス上のsaveコマンドを使用して、置換コンフィギュレーションファイルが作成されていることを確認します。コンフィギュレーションファイルがローカルデバイス上に作成されていない場合は、コンフィギュレーションファイルラインがローカルデバイスと完全に互換性があることを確認します。

手順

1. システムビューに入ります。

   system-view
2. 実行コンフィギュレーションをコンフィギュレーションファイルで定義されたコンフィギュレーションにロールバックします。

   configuration replace file *filename*

   指定したコンフィギュレーションファイルは、ローカルシステムに保存する必要があります。

コンフィギュレーションコミット遅延の設定

このタスクについて

この機能を使用すると、コンフィギュレーションコミット遅延インターバルの間に行った設定が手動でコ

ミットされていない場合、設定を自動的に削除できます。

コンフィギュレーションコミット遅延間隔を指定するには、コンフィギュレーションコミット遅延タイマーを使用します。コンフィギュレーションコミット遅延間隔中に行った設定は、コンフィギュレーションコミット遅延タイマー期限が切れる前に手動で設定をコミットしていない場合、これらの設定は自動的に削除されます。

この機能を使用すると、設定ミスによってデバイスにアクセスできなくなるのを防ぐことができます。この機能は、デバイスをリモートで設定する場合に特に便利です。

制限事項とガイドライン

この機能を使用する場合は、次の制約事項および注意事項に従ってください。

- マルチユーザー環境では、他のユーザーがデバイスを設定していないことを確認します。
- 予期しないエラーを回避するには、コンフィギュレーションロールバック中に操作を実行しないでください。
- 構成コミット遅延機能は1回限りの設定です。この機能は、コミット遅延タイマーの期限が切れたとき、または手動コミットが実行された後に無効になります。
- コンフィギュレーションコミット遅延機能は、1回限りの設定です。コミット遅延タイマーが期限切れになるか、手動コミット操作が実行された後にロールバックポイントが削除さこの機能は無効になります。この機能を再度使用するには、タイマーをリブートする必要があります。

手順

1. システムビューに入ります。

   system-view
2. コンフィギュレーションコミット遅延機能を有効にし、コミット遅延タイマーを開始します。

   configuration commit delay *delay-time*
3. (任意)コミット遅延タイマーの起動後に設定された設定をコミットします。

   configuration commit

次のスタートアップコンフィギュレーションファイルの指定

制限事項とガイドライン

△注意:

undo startup saved-configurationコマンドを使用すると、IRFファブリックまたはIRFメンバーのリブート後にIRFスプリットが発生する可能性があります。このコマンドを実行するときは、ネットワークへの影響を理解していることを確認してください。

ベストプラクティスとして、メインおよびバックアップの次のスタートアップコンフィギュレーションファイルとして異なるファイルを指定します。

undo startup saved-configuration コマンドは、メインまたはバックアップの次のスタートアップコンフィギュレーションファイルの属性を、ファイルを削除するのではなく NULL に変更します。

前提条件

IRFファブリックでは、指定したコンフィギュレーションファイルが有効であり、各メンバーデバイスの記憶域メディアのルートディレクトリに保存されていることを確認します。また、すべてのIRFメンバーデバイスで記憶域メディアの種類が同じであることを確認します。

手順

1. 次のスタートアップコンフィギュレーションファイルを指定します。次のいずれかの方法を選択します。
   - 次のスタートアップコンフィギュレーションファイルを指定するには、ユーザービューで次のコマンドを実行します。

     startup saved-configuration *cfgfile* **[backup | main]**

     デフォルトでは、次のスタートアップコンフィギュレーションファイルは指定されません。
   - 任意のビューで次のコマンドを実行して、実行コンフィギュレーションをファイルに保存し、そのファイルを次のスタートアップコンフィギュレーションファイルとして指定します。

     save [safely] [backup | main] [force]

     このコマンドの詳細については、「実行コンフィギュレーションの保存」を参照してください。

   backupキーワードまたはmainキーワードを指定しない場合、このコマンドはコンフィギュレーションファイルをメインの次のスタートアップコンフィギュレーションファイルとして指定します。
2. (任意)設定を確認します。任意のビューで次のいずれかのコマンドを使用します。
   - このスタートアップと次のスタートアップのコンフィギュレーションファイルの名前を表示します。

     display startup
   - 次回のシステム起動時のコンフィギュレーションファイルの内容を表示します。

     display saved-configuration

メインの次のスタートアップコンフィギュレーションファイルのバックアップと復元

メインの次のスタートアップコンフィギュレーションファイルのバックアップと復元について

メインの次のスタートアップコンフィギュレーションファイルをTFTPサーバーにバックアップするか、TFTPサーバーからメインの次のスタートアップコンフィギュレーションファイルを復元できます。

設定のバックアップと復元に関する制約事項とガイドライン

設定のバックアップおよび復元は、FIPSモードではサポートされません。

設定のバックアップおよび復元の前提条件

メインの次のスタートアップコンフィギュレーションファイルをバックアップまたは復元する前に、次の作業を行います。

- 次の要件が満たされていることを確認します。
  - サーバーにアクセスできます。
  - サーバーでTFTPサービスが有効になっている。

- サーバーに対する読み取りおよび書き込み権限があります。

- コンフィギュレーションバックアップの場合、**display startup**コマンドを使用して、メインの次のスタートアップコンフィギュレーションファイルがユーザービューで指定されていることを確認します。次のスタートアップコンフィギュレーションファイルが指定されていない場合、または指定されたコンフィギュレーションファイルが存在しない場合、バックアップ操作は失敗します。

TFTP サーバーへのコンフィギュレーションファイルの TFTP サーバーへのバックアップ

メインの次のスタートアップコンフィギュレーションファイルをTFTPサーバーにバックアップするには、ユーザービューで次のコマンドを実行します。

Backup startup-configuration to { *ipv4-server* | **ipv6** *ipv6-server* } [*dest-filename*] [**vpn-instance** *vpn-instance-name*]

TFTP サーバーからのメインの次のスタートアップコンフィギュレーションファイルの復元

1. ユーザービューでTFTPサーバーからメインの次のスタートアップコンフィギュレーションファイルを復元します。

   restore startup-configuration from { ipv4-server | ipv6 ipv6-server } *src-filename [vpn-instance vpn-instance-name]*

2. (任意)指定したコンフィギュレーションファイルがメインの次のスタートアップコンフィギュレーションファイルとして設定されていることを確認します。任意のビューで次のいずれかのコマンドを使用します。

   - このスタートアップと次のスタートアップのコンフィギュレーションファイルの名前を表示します。

     display startup

   - 次回のシステム起動時のコンフィギュレーションファイルの内容を表示します。

     display saved-configuration

次のスタートアップコンフィギュレーションファイルの削除

このタスクについて

次のスタートアップコンフィギュレーションファイルを削除するには、この作業を実行します。

メインとバックアップの次のスタートアップコンフィギュレーションファイルの両方が削除された場合、デバイスは次のスタートアップ時に工場出荷時のデフォルトを使用します。

メインおよびバックアップの次のスタートアップコンフィギュレーションファイルとして設定されているファイルを削除するには、**reset saved-configuration backup** コマンドと **reset saved-configuration main** コマンドの両方を実行する必要があります。いずれかのコマンドだけを使用すると、ファイルを削除するのではなく、指定したファイルアトリビュートが削除されます。

たとえば、**reset saved-configuration backup** コマンドが実行されると、backup next-startup configuration file 設定が NULL に設定されます。ただし、このファイルは引き続きメインファイルとして使用されます。ファイルを削除するには、reset saved-configuration main コマンドも実行する必要があります。

制限事項とガイドライン

△注意:

このタスクは、すべてのIRFメンバーデバイスから次のスタートアップコンフィギュレーションファイルを完全に削除します。 ベストプラクティスとして、このタスクを実行する前に、構成のバックアップがあることを確認してください。

このタスクを実行するときにbackupまたはmainキーワードを指定しない場合、メインの次のスタートアップ設定は削除されます。

手順

次のスタートアップコンフィギュレーションファイルを削除するには、ユーザービューで次のコマンドを実行します。

reset saved-configuration [**backup** | **main**]

コンフィギュレーションファイルの表示およびメンテナンスコマンド

任意のビューで表示コマンドを実行し、ユーザービューでコマンドをリセットします。

タスク	コマンド
コンフィギュレーションアーカイブ情報を表示します。	**display archive configuration**
稼働中のコンフィギュレーションを表示します。	**display current-configuration** [[**configuration** [*module-name*] | **interface** [*interface-type* [*interface-number*]]] | **slot** *slot-number*]
稼働中のコンフィギュレーションと次のスタートアップコンフィギュレーションの違いを表示します。	**display current-configuration diff**
工場出荷時のデフォルトを表示します。	**display default-configuration**
コンフィギュレーションの違いを表示する	• **display diff configfile** *file-name-s* **{ configfile** *file-name-d* **| current-configuration | startup-configuration }** • **display diff current-configuration { configfile** *file-name-d* **| startup-configuration }** • **display diff startup-configuration { configfile** *file-name-d* **| current-configuration }**
次回のシステム起動のために、コンフィギュレーションファイルの内容を表示します。	**display saved-configuration**

このスタートアップと次のスタートアップのコンフィギュレーションファイルの名前を表示します。	**display startup**
現在のビューに有効な構成を表示します。	**display this**
次のスタートアップコンフィギュレーションファイルを削除します。	**reset saved-configuration** [**backup** | **main**]

ソフトウェアのアップグレード

ソフトウェアのアップグレードについて

ソフトウェアアップグレードを使用すると、ソフトウェアバージョンのアップグレード、新機能の追加、およびソフトウェアの不具合の修正を行うことができます。この章では、ソフトウェアのタイプとリリースフォーム、ソフトウェアアップグレード方法の比較、およびCLIからソフトウェアをアップグレードする手順について説明します。

ソフトウェアタイプ

次のソフトウェアタイプを使用できます。

- **BootWareイメージ** - ブートROMイメージとも呼ばれます。このイメージには、基本セグメントと拡張セグメントが含まれています。
  - 基本セグメントは、システムをブートストラップする最小コードです。
  - 拡張セグメントは、ハードウェアの初期化を可能にし、システム管理メニューを提供します。デバイスが正常に起動できない場合は、メニューを使用してソフトウェアとスタートアップコンフィギュレーションファイルをロードしたり、ファイルを管理したりできます。

  通常、BootWareイメージは、ソフトウェアの互換性エラーを回避するためにブートイメージに統合されます。
- **Comwareイメージ - 次のイメージサブカテゴリが含まれます。**
  - **ブートイメージ** - Linuxオペレーティングシステムカーネルを含む.binファイル。プロセス管理、メモリー管理およびファイルシステム管理を提供します。
  - **システムイメージ** - Comwareカーネルおよびデバイス管理、インターフェイス管理、コンフィギュレーション管理、ルーティングなどの標準機能を含む.binファイル。
  - **機能イメージ** - 高度なソフトウェア機能またはカスタマイズされたソフトウェア機能を含む.binファイル。必要に応じて機能イメージを購入できます。
  - **パッチイメージ**: - デバイスをリブートせずにバグを修正するためにリリースされる.binファイル。パッチイメージは機能を追加または削除しません。

  読み込まれたcomwareイメージを現在のソフトウェアイメージと呼び、次の起動時に読み込むように指定されたソフトウェアイメージをスタートアップソフトウェアイメージと呼びます。

デバイスが動作するには、BootWareイメージ、ブートイメージ、およびシステムイメージが必要です。

デバイスには、1つのブートイメージファイル、1つのシステムイメージファイル、最大30の機能イメージファイルとパッチイメージファイルなど、最大32個の.binファイルをインストールできます。

ソフトウェアリリース形式

ソフトウェアイメージは、次のいずれかの形式でリリースされます。

- 個別の.binファイル。ソフトウェアイメージ間の互換性を確認する必要があります。
- 1つの.ipeパッケージファイル全体。.ipeパッケージファイル内のイメージは互換性があります。システムはファイルを自動的に解凍し、.binイメージをロードして起動ソフトウェアイメージとして設定します。

注:

ソフトウェアイメージファイル名は、model-comware version-imagetype-release形式を使用します。 このドキュメントでは、ブートおよびシステムイメージファイル名として**boot.bin**および**system.bin**を使用しています。

アップグレード方法

アップグレード方法	ソフトウェアタイプ	注意
ブートローダー方式を使用したCLIからのアップグレード	Comwareイメージ(増分パッチを除く)	この方法は中断を伴います。アップグレードを完了するには、デバイス全体をリブートする必要があります。
CLIからのISSUの実行	Comwareイメージ	この方法では、最小限のダウンタイムでソフトウェアをアップグレードできます。可能であれば、この方法を使用してください。 ISSUの詳細については、「ISSUの実行」を参照してください。
BootWareメニューからアップグレードする	• BootWareイメージ • Comwareイメージ	デバイスが正常に起動できない場合は、この方法を使用します。 この方法を使用するには、まずコンソールポートに接続し、デバイスの電源を再投入します。次に、プロンプトでCtrl+Bを押して、BootWareメニューにアクセスします。 BootWareメニューからソフトウェアをアップグレードする方法の詳細については、ソフトウェアバージョンのリリースノートを参照してください。 重要: この方法は、他に方法がない場合にのみ使用してください。

この章では、ブートローダー方式を使用してCLIからソフトウェアをアップグレードする方法についてだけ説明します。

ソフトウェアイメージのロード

スタートアップソフトウェアイメージ

ソフトウェアをアップグレードするには、次回の起動時にロードするデバイスの起動ソフトウェアイメージとしてアップグレードファイルを指定する必要があります。ソフトウェイメージの2つのリスト(メインとバックアップ)を指定できます。デバイスは最初にメイン起動ソフトウェアイメージをロードします。メイン起動ソフトウェアイメージが使用できない場合、デバイスはバックアップ起動ソフトウェアイメージをロードします。

起動時のイメージローディング処理

起動時に、デバイスはBootWareをロードして初期化した後、次の操作を実行します。

1. メインイメージをロードします。
2. メインイメージが存在しないか無効な場合、バックアップイメージをロードします。
3. バックアップイメージが存在しないか無効な場合、デバイスは起動できません。

制約事項および注意事項:ソフトウェアアップグレード

起動イメージは固定の記憶媒体に保存することをお勧めします。起動イメージをホットスワップ可能な記憶媒体に保存する場合は、起動プロセス中にホットスワップ可能な記憶媒体を取り外さないでください。

ブートローダー方式を使用したデバイスソフトウェアのアップグレード

ソフトウェアアップグレードタスクの概要

ソフトウェアをアップグレードするには、以下のいずれかのタスクを実行してください。

- IRFファブリックをアップグレードします。
  a. （オプション）BootWareイメージをBootWareにプリロードする
  BootWareのアップグレードが必要な場合は、このタスクを実行して、後続のアップグレード時間を短縮できます。このタスクは、予期しない電源障害によって引き起こされるアップグレードの問題を減らすのに役立ちます。このタスクをスキップすると、デバイスはスタートアップソフトウェアイメージをアップグレードするときにBootWareを自動的にアップグレードします。
  b. スタートアップイメージを指定してアップグレードを完了する
- （オプション）マスターデバイスから下位デバイスへのスタートアップイメージの同期
  従属デバイスのスタートアップイメージがマスターデバイスのスタートアップイメージと同じバージョンでない場合に、このタスクを実行します。

前提条件

1. **display version**コマンドを使用して、現在のBootWareイメージバージョンとスタートアップソフトウェアバージョンを確認します。
2. アップグレードソフトウェアバージョンのリリースノートを使用して、アップグレードがネットワークに与える影響を評価し、次の項目を確認します。
   - ソフトウェアとハードウェアの互換性。
   - アップグレードソフトウェアのバージョンとサイズ。

- アップグレードソフトウェアと現在のBootWareイメージおよびスタートアップソフトウェアイメージとの互換性。

3. リリースノートを参照して、ソフトウェアイメージにライセンスが必要かどうかを確認します。 ライセンスが必要な場合は、ライセンスベースのソフトウェアイメージごとにライセンスを登録してアクティブ化します。 ライセンスの詳細については、「ライセンスの管理」を参照してください。
4. **dir**コマンドを使用して、すべてのIRFメンバーデバイスにアップグレードイメージ用の十分な記憶域があることを確認します。どのメンバーデバイスにも十分な記憶域がない場合は、**delete**コマンドを使用して未使用のファイルを削除します。詳細については、「ファイルシステムの管理」を参照してください。
5. FTPまたはTFTPを使用して、アップグレードイメージファイルをファイルシステムのルートディレクトリに転送します。FTPおよびTFTPの詳細は、「FTPの構成」または「TFTPの構成」を参照してください。ファイルシステムの詳細は、「ファイルシステムの管理」を参照してください。

BootWare イメージを BootWare にプリロードする

アップグレード BootWare イメージを BootWare の通常領域にプリロードするには、ユーザービューで次のコマンドを実行します。

bootrom update file *file* **slot** *slot-number-list*

ダウンロードしたソフトウェアイメージファイルを *file* 引数に指定します。

新しい BootWare イメージは、再起動時に有効になります。

起動イメージの指定とアップグレードの完了

ユーザービューで次の手順を実行します。

1. すべてのメンバーデバイスのメインまたはバックアップスタートアップイメージを指定します。
   - ipeファイルを使用する:

     boot-loader file *ipe-filenam*e [**patch** *filename*&<1-16>] { **all** | **slot** *slot-number* } { **backup** | **main** }
   - binファイルを使用:

     boot-loader file boot *filename* **system** *filename* [**feature** *filename*&<1-30>] [**patch** *filenam*e&<1-16>] { **all** | **slot** *slot-number* } { **backup** | **main** }

   マルチシャーシIRFファブリックでのベストプラクティスとして、コマンドにallキーワードを指定します。**slot** *slot-number*オプションを使用してメンバーデバイスを1つずつアップグレードすると、アップグレード中にメンバーデバイス間でバージョンの不一致が発生します。
2. 実行コンフィギュレーションを保存します。

   save

   この手順を実行すると、リブート後も設定を維持できます。
3. IRFファブリックをリブートします。

   reboot
4. (オプション)ソフトウェアイメージの設定を確認します。

   display boot-loader [**slot** *slot-number*]

   現在のソフトウェアイメージがスタートアップソフトウェアイメージと同じであることを確認します。

マスターデバイスから下位デバイスへのスタートアップイメージの同期

スタートアップイメージの同期について

下位デバイスの起動イメージがマスターデバイスの起動イメージと同じバージョンでない場合は、次の作業を実行します。

このタスクでは、マスターデバイスで実行されている起動イメージを下位デバイスに同期します。起動イメージが存在しないか無効な場合、同期は失敗します。

下位デバイスに同期されたスタートアップイメージは、ソーススタートアップイメージがメインかバックアップかにかかわらず、メインスタートアップイメージとして設定されます。

制限事項とガイドライン

マスターデバイスでISSUまたはパッチインストールが実行されている場合は、**install commit**コマンドを使用して、ソフトウェア同期化の前にマスターデバイス上のメインスタートアップイメージのセットを更新します。このコマンドにより、マスターデバイスと下位デバイス間のスタートアップイメージの一貫性が保証されます。

手順

ユーザービューで次の手順を実行します。

1. 起動イメージをマスターデバイスから下位デバイスに同期します。

   boot-loader update { all | slot *slot-number* **}**
2. 下位デバイスをリブートします。

   reboot slot *slot-number* [**force**]

ソフトウェアイメージ設定の表示およびメンテナンスコマンド

任意のビューで表示コマンドを実行します。

タスク	コマンド
現在のソフトウェアイメージと起動ソフトウェアイメージを表示します。	**display boot-loader** [**slot** *slot-number*]

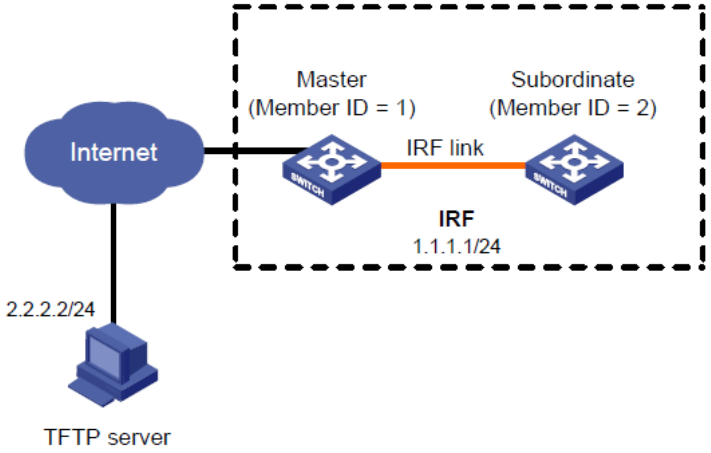
ソフトウェアアップグレードの例

例:デバイスソフトウェアのアップグレード

ネットワークの設定

図21に示すように、startup-a2105.ipeファイルを使用して、IRFファブリックのソフトウェアイメージをアップグレードします。

図21 ネットワーク図



手順

#IPアドレスとルートを設定します。デバイスとTFTPサーバーが互いに通信できることを確認します#(詳細は省略します)。
#デバイスとTFTPサーバーの両方でTFTP設定を行います(詳細は省略します)。
#現在のソフトウェアイメージに関する情報を表示します。

<Sysname> display version
#現在のソフトウェアイメージをバックアップします。
<Sysname> copy boot.bin boot_backup.bin
<Sysname> copy system.bin system_backup.bin
#すべてのIRFメンバーデバイスのバックアップスタートアップイメージファイルとして
boot_backup.binとsystem_backup.binを指定します。

<Sysname> boot-loader file boot flash:/boot_backup.bin systemflash:/system_backup.bin slot 1 backup

<Sysname> boot-loader file boot flash:/boot_backup.bin systemflash:/system_backup.bin slot 2 backup
#TFTPサーバーからマスターデバイス上のフラッシュメモリーのルートディレクトリに
startup-a2105.ipeイメージファイルをダウンロードするには、TFTPを使用します。

<Sysname> tftp 2.2.2.2 get startup-a2105.ipe
#すべてのIRFメンバーデバイスのメインスタートアップイメージファイルとして**startup-a2105.ipe**
#を指定します。

<Sysname> boot-loader file flash:/startup-a2105.ipe slot 1 main

<Sysname> boot-loader file flash:/startup-a2105.ipe slot 2 main
#起動イメージの設定を確認します。
<Sysname> display boot-loader
#デバイスをリブートしてアップグレードを完了します。
<Sysname > reboot
#デバイスが正しいソフトウェアを実行していることを確認します。
<Sysname > display version

ISSU の実行

ISSUについて

In-Service Software Upgrade(ISSU)機能は、最小限のダウンタイムでComwareソフトウェアをアップグレードします。

特に明記されていない限り、「アップグレード」という用語は、ISSUのソフトウェアアップグレードとダウングレードの両方を意味します。

ISSU の利点

Comwareソフトウェアには、ブートイメージ、システムイメージ、および機能イメージが含まれています。ISSUは、イメージの個別アップグレードをサポートします。

ISSUを使用して機能をアップグレードすると、関連する機能イメージだけが影響を受けます。その他の機能は引き続きサービスを提供できます。

ISSUは、システムをリブートせずにシステムの不具合を修正するパッチイメージのインストールをサポートします。

ISSU 方式

ISSU方式は、ソフトウェアリリース時にソフトウェアバージョン間の互換性に応じて決定されます。

ISSUは、次のアップグレードタイプをサポートします。

- **互換性のあるアップグレード** - 新しいソフトウェアバージョンは、実行中のソフトウェアバージョンと互換性があります。このアップグレードタイプは、表13のISSU方式をサポートします。
- **互換性のないアップグレード** - 新しいソフトウェアバージョンは、実行中のソフトウェアバージョンと互換性がありません。2つのバージョンを同時に実行することはできません。

  このアップグレードタイプでは、1つのアップグレード方法だけがサポートされます(互換性のないアップグレードとも呼ばれます)。この方法では、コントロールプレーンとデータプレーンの両方をアップグレードするためにコールドリブートが必要です。互換性のないアップグレードでは、ハードウェアの冗長性が利用できない場合にサービスが中断されます。

ISSU方式の識別については、「ISSU方式の識別」を参照してください。

表13 互換性のあるアップグレードのためのISSU方式

ISSU方式	説明
差分アップグレード: • サービスアップグレード • ファイルのアップグレード	新しいソフトウェアバージョンと古いソフトウェアバージョンが異なるユーザモードプロセスだけをアップグレードします。サービスの継続性を確保するには、バックアッププロセスとメイン/バックアッププロセスの切り替えが必要です。 • **サービスアップグレード** - サービス機能をアップグレードします。アップグレードは、アップグレードされていない機能の動作には影響しません。 • **ファイルアップグレード** - 非表示のシステムプログラムファイルをアップグレードします。システムはアップグレード中にサービスを提供できます。

リブート	△注意: ハードウェアの冗長性は、ハードウェアの冗長性が利用できない場合にサービスを中断します。サービスへのアップグレードの影響を最小限に抑えるために、ダウンタイムを慎重にスケジュールすることをお勧めします。 メンバーデバイスをリブートしてソフトウェアアップグレードを完了します。1つのメンバーデバイスがリブートしている間、他のメンバーデバイスはサービスを提供できます。

issu コマンド

ISSUには**install**コマンドセットと**issu**コマンドセットが含まれます。推奨されるISSU方式を特定したら、表14を参照して使用するコマンドセットを選択します。

表14 コマンドセットの比較

項目	issuコマンド	インストールコマンド
アップグレードタイプ	• 互換性あり。 • 互換性がありません。	互換性あり。
パッチのインストールとアンインストール	サポートされていません。	サポートされています。
システムへの影響	大	小さい。
技術的スキル要件	低 ベストプラクティスとして、このコマンドセットを使用してください。	高 管理者は、広範なシステム知識を持ち、各アップグレードタスクがネットワークに与える影響を理解している必要があります。
ワンステップISSU	サポートされています。	サポートされていません。
ステップバイステップISSU	サポートされています。	サポートされています。

制約事項および注意事項:ISSU

重要:

- ISSUを正常に実行するには、新しいバージョンでサポートされていないコマンドをすべて削除し、実行コンフィギュレーションを保存する必要があります。現在のバージョンと新しいバージョン間の機能変更を確認するには、デバイスのリリースノートを参照してください。
- システムが正しく動作するようにするには、機能をアンインストールする前に、アンインストールする機能用に構成されたコマンドを削除し、実行構成を保存する必要があります。

ISSUの実行中は、次の制約事項および注意事項に従ってください。

- 次の作業は実行しないでください。
  - メンバーデバイスをリブートします。
  - 設定の変更や情報の表示など、ISSUに関連しない作業を実行します。
  - イメージファイルを修正、削除、または名前変更します。
- 同じISSUに対して**install**コマンドと**issu**コマンドの両方を使用することはできません。ただし、両方

のコマンドセットで**display issu**コマンドを使用できます。詳細については、「ISSUの表示および保守コマンド」を参照してください。

- サービスの継続性を高めるために、推奨されるISSU手順に厳密に従ってください。次のステップに進む前に、ステップが完了していることを確認してください。
- 次のコマンドを実行する前に、**display system stable state**コマンドを使用して、システムが安定していることを確認してください。
  - **issu**コマンド – **issu load**、**issu run switchover**、および**issu commit**。
  - **install**コマンド – **install activate**および**install deactivate**。

  System stateフィールドに**stable**と表示されている場合、システムは安定しています。
- **issu**コマンドを使用して、ソフトウェアイメージのすべてまたは一部をアップグレードできます。一部のイメージのみをアップグレードする場合は、新しいイメージがアップグレードされないイメージと互換性があることを確認してください。競合が存在する場合、アップグレードは失敗します。ISSUを終了したら、変更または追加したコマンドを使用する前に、デバイスに再度ログインする必要があります。

ISSUが終了したら、変更または追加されたコマンドを使用する前に、デバイスに再度ログインする必要があります。

ISSUの前提条件

ISSUを正常に実行するには、すべての準備要件が満たされていることを確認します。

コンソールポートを介したデバイスへのログイン

コンソールポートからデバイスにログインします。TelnetまたはSSHを使用する場合、ISSUが完了する前にデバイスから切断される可能性があります。

マルチユーザー環境では、ISSUの実行中に他の管理者がデバイスにアクセスしないようにしてください。

ISSU の可用性とライセンス要件の識別

ソフトウェアリリースノートを参照して、以下の項目を確認する:

- 現在のソフトウェアバージョンと新しいソフトウェアバージョンの間のISSU用デバイスのサポート。
- アップグレードソフトウェアイメージのライセンス要件。 アップグレードソフトウェアイメージにライセンスが必要な場合は、デバイスに必要なライセンスがあることを確認してください。 ライセンスのインストールの詳細については、「ライセンスの管理」を参照してください。

デバイスの動作状態の確認

display deviceコマンドを使用して、すべてのコンポーネントが正しく動作していることを確認します。

アップグレードイメージの準備

1. すべてのファイルシステムにアップグレードイメージ用の十分な空きストレージスペースがあることを確認するには、dirコマンドを使用します。ストレージスペースが十分でない場合は、**delete /unreserved** *file-url*コマンド。削除するファイルを使用する場合は、削除する前にファイルをバックアップします。**/unreserved**キーワードを使用すると、削除したファイルを復元できません。詳細は、「ファイルシステムの管理」を参照してください。
2. FTPまたはTFTPを使用して、アップグレードイメージファイル(.binまたは.ipe内)をマスターデバイス上のファイルシステムのルートディレクトリに転送します。

ISSU 方式の識別

推奨されるISSU方式を特定するには、**display version comp-matrix file**コマンドを実行します。

- 互換性のあるアップグレードの場合は、**Upgrade Way**フィールドをオンにして、推奨されるISSU方式を特定します。
- 互換性のないアップグレードの場合は、**Incompatible upgrade**文字列のコマンド出力の最後を確認します。

ISSU方式の詳細については、表13を参照してください。

機能ステータスの確認

ISSU中のサービス継続性を確保するには、次の機能設定を行います。

機能	要件の設定
GRおよびNSR	LDP、OSPF、ISIS、BGP、FSPFなどのプロトコルのGRまたはNSRを有効にします。
BFD	LDP、OSPF、ISIS、RIP、BGP、VRRP、およびNQAなどのプロトコルのBFDを無効にします。
イーサネットリンクアグリゲーション	ダイナミックアグリゲーショングループのすべてのメンバーポートで、長いLACPタイムアウト間隔を使用します(**lacp period short**コマンドは設定されません)。
IRF	IRFファブリックの互換性のないアップグレードを実行する前に、IRF MADが無効になっていることを確認してください。IRF MADを使用するには、アップグレードの完了後にIRF MADを有効にします。 IRFブリッジMACパーシステンスを次のように設定します。 • **互換性のあるアップグレード** - **irf mac-address persistent timer**または**irf mac-address persistent always**コマンドを設定します。 • **互換性のないアップグレード** - ブリッジMACアドレスが**issu load**コマンドを実行するデバイスのMACアドレスである場合は、**irf mac-address persistent always**コマンドを設定します。

アップグレード手順の決定

1. 表14を使用して、ISSU方式に応じたアップグレードコマンドセットを選択します。
2. ハードウェアの冗長性の状態を確認します。

ISSUは、次の条件が満たされた場合にだけサービスの継続性を維持できます。

- IRFファブリックは複数のメンバーを持ち、リングトポロジを使用します。

重要:

ハードウェアの冗長性が利用できない場合、リブートアップグレードまたは互換性のないアップグレード中にサービスの中断を回避できません。アップグレードがネットワークに与える影響を理解していることを確認してください。

3. 「issuコマンドを使用したISSUの実行」または「インストールコマンドを使用したISSUの実行」で説明されている手順から正しい手順を選択します。

稼働中のコンフィギュレーションの調整と保存

1. 新しいソフトウェアバージョンでサポートされていないすべてのコマンドを稼働中のコンフィギュレーションから削除します。現在のバージョンと新しいバージョン間のすべての機能変更を確認するには、デバイスのリリースノートを参照してください。
2. 機能イメージをアンインストールするには、機能に設定されているコマンドを削除します。
3. 稼働中のコンフィギュレーションを保存するには、**save**コマンドを使用します。

issuコマンドを使用したISSUのステップバイステップ実行

マルチシャーシ IRF ファブリックで互換性のあるアップグレードを実行する

制限事項とガイドライン

最初に下位メンバーデバイスをアップグレードします。次に、元のマスターを含む残りのメンバーデバイスをアップグレードします。

手順

1. (任意)自動ロールバックを設定します。
   a. システムビューに入ります。

      system-view

   b. 自動ロールバックタイマーを設定します。

      issu rollback-timer *minutes*

      デフォルトでは、自動ロールバックタイマーは45分に設定されています。

      自動ロールバックタイマーは、issu run switchover コマンドを実行すると開始されます。

   c. ユーザービューに戻ります。

      quit
2. システムが安定していることを確認します。

   display system stable state

   System StateフィールドにStableと表示されている場合、システムは安定しています。ISSU

を正常に実行するには、システムが安定していることを確認してから、次の手順に進む必要があります。

3. アップグレードイメージをスタートアップイメージとして下位メンバーにロードします。
   - binファイルを使用:

     issu load file { boot *filename* **| system** *filename* **| feature** *filename*&<1-30> **} * slot** *slot-number*& <1-9> [**reboot**]
   - ipeファイルを使用する:

     issu load file ipe *ipe-filename* **slot** *slot-number*& <1-9> [**reboot**]
4. システムが安定していることを確認します。

   display system stable state

   System Stateフィールドに**Stable**と表示されている場合、システムは安定しています。ISSUを正常に実行するには、システムが安定していることを確認してから、次の手順に進みます。前の手順でエラーが報告された場合は、システムが安定していることを確認してから、**issu rollback**コマンドを使用してアップグレードをロールバックします。
5. ISSUスイッチオーバーを実行します。

   issu run switchover

   このコマンドは、自動ロールバックタイマーも起動します。タイマーが期限切れになると、システムは自動的に元のソフトウェアイメージにロールバックします。
6. (任意)アップグレードを受け入れ、自動ロールバックタイマーを削除します。

   issu accept

   自動ロールバックタイマーが期限切れになる前に、このコマンドを実行します。
7. システムが安定していることを確認します。

   display system stable state

   System Stateフィールドに**Stable**と表示されている場合、システムは安定しています。ISSUを正常に実行するには、システムが安定していることを確認する必要があります。前の2つの手順でシステムからエラーが報告された場合は、システムが安定していることを確認してから、issu **rollback**コマンドを使用してアップグレードをロールバックします。
8. 残りのメンバーをアップグレードして、ISSUを完了します。

   issu commit slot *slot-number*

   自動ロールバックタイマーが期限切れになる前に、このコマンドを実行します。1つのメンバーに対してこのコマンドを使用した後、メンバーがリブートしてIRFファブリックに参加するまで待ちます。次に、前の手順とこの手順を繰り返して、元のマスターを含む残りのメンバーデバイスを1つずつアップグレードします。
9. ISSUが終了していることを確認します。

   display issu state

   ISSU stateフィールドに**Init**と表示されている場合、ISSUは終了します。

マルチシャーシ IRF ファブリックで互換性のないアップグレードを実行する

制限事項とガイドライン

最初に1つ以上の下位メンバーデバイスをアップグレードします。次に、元のマスターを含む残りのメンバ

ーデバイスをアップグレードします。

手順

マルチシャーシIRFファブリックで互換性のないアップグレードを実行するには、ユーザービューで次のコマンドを実行します。

1. システムが安定していることを確認します。

   display system stable state

   System Stateフィールドに**Stable**と表示されている場合、システムは安定しています。
   ISSUを正常に実行するには、システムが安定していることを確認してから、次の手順に進む必要があります。

2. アップグレードイメージをスタートアップイメージとして下位メンバーにロードします。

   - binファイルを使用:

     issu load file { boot *filename* **| system** *filename* **| feature** *filename*&<1-30> **} * slot** *slot-number*&<1-9> **[reboot]**

   - ipeファイルを使用する:

     issu load file ipe *ipe-filename* **slot** *slot-number*&*<1-9>* [**reboot**]

   リングトポロジIRFファブリックのベストプラクティスとして、このコマンドに下位メンバーの半分を指定してサービスの中断を減らします。指定した下位メンバーが物理的に接続されていることを確認してください。

3. システムが安定していることを確認します。

   display system stable state

   System Stateフィールドに**Stable**と表示されている場合、システムは安定しています。ISSUを正常に実行するには、システムが安定していることを確認してから、次の手順に進みます。前の手順でエラーが報告された場合は、システムが安定していることを確認してから、**issu rollback**コマンドを使用してアップグレードをロールバックします。

4. ISSUスイッチオーバーを実行して、ISSUプロセスを完了します。

   issu run switchover

   このコマンドは、残りのメンバーをアップグレードします。

5. ISSUが終了していることを確認します。

   display issu state

   ISSU stateフィールドに**Init**と表示されている場合、ISSUは終了します。

シングルシャーシ IRF ファブリックでの差分アップグレードの実行

シングルシャーシIRFファブリックでインクリメンタルアップグレードを実行するには、ユーザービューで次のコマンドを実行します。

1. システムが安定していることを確認します。

   display system stable state

   System Stateフィールドに**Stable**と表示されている場合、システムは安定しています。
   ISSUを正常に実行するには、システムが安定していることを確認してから、次の手順に進む必要があります。

2. アップグレードイメージをスタートアップイメージとしてロードします。

- binファイルを使用:

  issu load file { boot *filename* **| system** *filename* **| feature** *filename*&<1-30> } *** slot** *slot-number* [**reboot**]
- ipeファイルを使用する:

  issu load file ipe *ipe-filename* **slot** *slot-number* [**reboot**]

3. システムが安定していることを確認します。

   display system stable state

   System Stateフィールドに**Stable**と表示されている場合、システムは安定しています。ISSUを正常に実行するには、システムが安定していることを確認してから、次の手順に進みます。前の手順でエラーが報告された場合は、システムが安定していることを確認してから、issu rollbackコマンドを使用してアップグレードをロールバックします。
4. ISSUプロセスを完了します。

   issu commit slot *slot-number*
5. ISSUが終了していることを確認します。

   display issu state

   ISSU stateフィールドに**Init**と表示されている場合、ISSUは終了します。

シングルシャーシ IRF ファブリックでのリブートまたは互換性のないアップグレードの実行

1. システムが安定していることを確認します。

   display system stable state

   System Stateフィールドに**Stable**と表示されている場合、システムは安定しています。
   ISSUを正常に実行するには、システムが安定していることを確認してから、次の手順に進む必要があります。
2. 親デバイスのアップグレードイメージをスタートアップイメージとして下位メンバーにロードします。
   - binファイルを使用:

     issu load file { boot *filename* **| system** *filename* **| feature** *filename*&<1-30> } *** slot** *slot-number* [**reboot**]
   - ipeファイルを使用する:

     issu load file ipe *ipe-filename* **slot** *slot-number* [**reboot**]
3. ISSUが終了していることを確認します。

   display issu state

   ISSU stateフィールドに**Init**と表示されている場合、ISSUは終了します。

installコマンドを使用したISSUの実行

ISSU タスクの概要

1. (オプション).ipeファイルの解凍
2. ソフトウェアイメージのインストールとアップグレード

3. (必要に応じて)ソフトウェアイメージの非アクティブ化
4. (任意)実行中のソフトウェアイメージのロールバック
5. (任意)ソフトウェアのアクティブ化操作または非アクティブ化操作を中断
6. (必要に応じて)ソフトウェアイメージの確認
7. ソフトウェア変更のコミット
8. (任意)非アクティブなソフトウェアイメージの削除

ipe ファイルの解凍

1. (オプション).ipeファイルに含まれるイメージを識別します。
   display install ipe-info
2. ipeファイルを解凍します。
   install add *ipe-filename filesystem*

ソフトウェアイメージのアクティブ化

ソフトウェアイメージのアクティブ化について

このタスクを使用して、新しい機能をインストールするか、ブート、システム、または機能のイメージをアップグレードします。

ソフトウェアイメージのアクティブ方法

ソフトウェアイメージのアクティブ化は以下の方法の1つを使います:

- **スロットごと** - 1つのスロットですべてのイメージをアクティブにしてから、次のスロットに移動します。
- **イメージごと** - 別のイメージをアクティブにする前に、すべてのスロットで1つのイメージをアクティブにします

制限事項とガイドライン

イメージをインストールするには、マスターデバイスから始める必要があります。イメージをアップグレードするには、下位デバイスから始める必要があります。

インクリメンタルアップグレードまたはパッチイメージのアクティブ化操作は、現在のソフトウェアイメージリストのみを更新します。リブート後にイメージの変更を有効にするには、メインのスタートアップイメージリストを更新するためにコミット操作を実行する必要があります

1つのブートイメージファイル、1つのシステムイメージファイル、および最大30の機能またはパッチイメージファイルを含む、最大32の.binファイルをデバイスにインストールできます。

前提条件

パッチイメージをアクティブ化する前に、デバイスでパッチイメージがすでに実行されているかどうかを確認してください。

- そうでない場合は、パッチイメージをアクティブにします。
- 「はい」の場合は、リリースノートを読んで、実行中のパッチイメージと新しいパッチイメージの機能の違いを確認します。
  - 新しいパッチイメージが古いパッチイメージによって提供されるすべての機能をカバーしている場合、新しいパッチイメージをアクティブにすると、古いパッチイメージが上書きされます。新しいパッチイメージをアクティブ化した後、古いパッチイメージを非アクティブ化して削除し、ソフトウェアイメージリストから削除して、ストレージスペースを解放します。
  - 新しいパッチイメージが古いパッチイメージによって提供される1つ以上の機能をカバーしていな

い場合、パッチイメージをアクティブ化しても古いパッチイメージには影響しません。デバイスは、新しいパッチイメージと古いパッチイメージの両方を使用します。古いパッチイメージを非アクティブ化または削除しないでください。

ブート、システムと機能イメージのアクティブ化

ブートイメージ、システムイメージ、および機能イメージをアクティブ化するには、ユーザービューで次のコマンドを実行します。

1. システムが安定していることを確認します。
   display system stable state
   system stateフィールドに**stable**と表示されている場合、システムは安定しています。ISSUを成功させるには、次の手順に進む前に、システムが安定していることを確認する必要があります。
2. （オプション）推奨されるISSUの方法とアップグレードの考えられる影響を特定します。
   install activate { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> } * **slot** *slot-number* **test**
3. イメージをアクティブにします。
   install activate { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> } * **slot** *slot-number*

パッチイメージのアクティブ化

パッチイメージをアクティブ化するには、ユーザービューで次のコマンドを実行します。

1. システムが安定していることを確認します。
   display system state stable
   system stateフィールドに**stable**と表示されている場合、システムは安定しています。インストールを成功させるには、次の手順に進む前に、システムが安定していることを確認する必要があります。
2. パッチイメージをアクティブにします。
   install activate patch *filename* { **all** | **slot** *slot-number* }

ソフトウェアイメージの非アクティブ化

制限事項とガイドライン

非アクティブ化できるのは、機能イメージとパッチイメージだけです。

非アクティブ化操作では、現在のソフトウェアイメージリストからイメージだけが削除されます。リブート後にイメージの変更を有効にするには、コミット操作を実行してメインの起動イメージリストからイメージを削除する必要があります。

非アクティブ化されたイメージは、記憶媒体に格納されたままです。イメージを完全に削除するには、**install remove**コマンドを実行します。詳細は、「非アクティブなソフトウェアイメージの削除」を参照してください。

機能イメージの非アクティブ化

機能イメージを非アクティブ化するには、ユーザービューで次のコマンドを実行します。

1. システムが安定していることを確認します。
   display system stable state
   system stateフィールドドに**stable**と表示されている場合、システムは安定しています。非アクティブ化操作を正常に実行するには、次のステップに進む前にシステムが安定していることを確認する必要があります。
2. 機能イメージを非アクティブ化します。
   install deactivate feature *filename*&<1-30> **slot** *slot-number*

パッチイメージの非アクティブ化

パッチイメージを非アクティブ化するには、ユーザービューで次のコマンドを実行します。

1. システムが安定していることを確認します。
   display system stable state
   system stateフィールドに**stable**と表示されている場合、システムは安定しています。非アクティブ化操作を正常に実行するには、次のステップに進む前にシステムが安定していることを確認する必要があります。
2. パッチイメージを非アクティブにします。
   install deactivate patch *filename* { **all** | **slot** *slot-number* }

稼働中のソフトウェアイメージのロールバック

ソフトウェアイメージのロールバックについて

増分アップグレードでは、ブート、システムまたは機能イメージのアクティブ化または非アクティブ化操作ごとにロールバックポイントが作成されます。システムでは、最大50個のロールバックポイントを保持できます。ロールバックポイントの作成時にこの制限に達した場合、最も古いロールバックポイントが削除されます。ソフトウェアは任意のロールバックポイントにロールバックできます。

リブートアップグレード中は、システムはロールバックポイントを作成しません。リブートアップグレード後は、アクティブ化操作または非アクティブ化操作が実行される前ののみソフトウェアをロールバックできます。

制限事項とガイドライン

このタスクは、ソフトウェア変更をコミットする前にのみ実行できます。コミット操作では、すべてのロールバックポイントが削除されます。

リブート後にインクリメンタルアップグレードロールバックを有効にするには、コミット操作を実行してメインスタートアップイメージリストを更新する必要があります。

手順

稼働中のソフトウェアイメージをロールバックするには、ユーザービューで次のコマンドを実行します。

1. (任意)使用可能なロールバックポイントを表示します。
   display install rollback
2. ソフトウェアをロールバックします。
   install rollback to { *point-id* | **original** }

ソフトウェアのアクティブ化操作または非アクティブ化操作を中止する

このタスクについて

サービスアップグレードまたはファイルアップグレードのためにソフトウェアイメージをアクティブ化または非アクティブ化している間は、アクティブ化操作または非アクティブ化操作を中断できます。操作が中断されると、システムは操作前に実行していたソフトウェアイメージで実行されます。

手順

ソフトウェアのアクティブ化または非アクティブ化操作を中止するには、次のいずれかの方法を使用します。

- ユーザービューで**install abort** [*job-id*]コマンドを実行します。
- **Ctrl+C**を押します。

ソフトウェア変更のコミット

このタスクについて

増分アップグレードのイメージをアクティブ化または非アクティブ化する場合、またはパッチイメージをアクティブ化または非アクティブ化する場合、メイン起動イメージリストは変更内容で更新されません。ソフトウェアの変更はリブート時に失われます。リブート後に変更を有効にするには、変更をコミットする必要があります。

手順

ソフトウェアの変更をコミットするには、ユーザービューで次のコマンドを実行します。
Install commit

ソフトウェアイメージの確認

このタスクについて

次の項目を確認するには、次の作業を実行します。

- **Integrity -** ブートイメージ、システムイメージ、および機能イメージが統合されていることを確認します。
- **整合性 -** システム全体で同じアクティブイメージが実行されていることを確認します。
- **ソフトウェアコミットステータス -** 必要に応じて必要に応じてコミットされていることを確認します。

手順

ソフトウェアイメージを確認するには、ユーザービューで次のコマンドを実行します。

1. ソフトウェアイメージを確認します。
   install verify
2. 必要に応じてイメージをアクティブまたは非アクティブにします。
   Install { **activate deactivate** }
3. ソフトウェアの変更をコミットします。
   Install commit

非アクティブなソフトウェアイメージの削除

非アクティブなソフトウェアイメージの削除について

ISSUの完了後、この作業を使用して、古いイメージファイルを永続的に削除できます。

制限事項とガイドライン

このタスクは、イメージファイルを永久に削除します。**install rollback to**コマンドを使用して操作を元に戻したり、**install abort**コマンドを使用して操作を中断したりすることはできません。

手順

非アクティブなソフトウェアイメージファイルを削除するには、ユーザービューで次のコマンドを実行します。

install remove [slot *slot-number*] { *filename* | **inactive** }

ISSUの表示およびメンテナンスコマンド

特に明記されていない限り、**display**コマンドおよび**reset**コマンドは、**install**コマンドまたは**issu**コマンドが使用されているかどうかに関係なく、ISSU中に使用できます。
任意のビューで表示コマンドを実行し、ユーザービューでコマンドをリセットします。

タスク	コマンド	注意
アクティブなソフトウェアイメージを表示します。	**display install active** [slot*slot-number*] [**verbose**]	該当せず
バックアップスタートアップソフトウェアイメージを表示します。	**display install backup** [slot*slot-number*] [**verbose**]	該当せず
メイン起動ソフトウェアイメージを表示します。	**display install committed** [slot *slot-number*] [**verbose**]	該当せず
ファイルシステムのルートディレクトリにある非アクティブなソフトウェアイメージを表示します。	**display install inactive** [slot*slot-number*] [**verbose**]	該当せず
ipeファイルに含まれるソフトウェアイメージを表示します。	**display install ipe-info** *ipe-filename*	該当せず
進行中のISSUのアクティブ化、非アクティブ化、およびロールバック動作を表示します。	**display install job**	該当せず
ISSUログエントリを表示します。	**display install log** [*log-id*] [**verbose**]	該当せず
ソフトウェアイメージファイル情報を表示します。	**display install package** { *filename* | **all** } [**verbose**]	該当せず
ロールバックポイント情報を表示します。	**display install rollback** [*point-id*]	issuコマンドを使用するISSUでは、ロールバックポイントは記録されません。
特定のコンポーネントまたはファイルを含むソフトウェアイメージファイルを表示します。	**display install which** {**component** *name* | **file** *filename* } [**slot** *slot-number*]	該当せず
自動ロールバックタイマー情報を表示します。	**display issu rollback-timer**	該当せず
ISSUステータス情報を表示します。	**display issu state**	このコマンドは、issuコマンドを使用するISSUだけに適用されます。

ISSU方式を表示します。	**Display version comp-matrix file** { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> * **Display version comp-matrix file ipe** *ipe-filename* **[patch *filename*&<1-30>]**	該当せず
ISSUログエントリをクリアします。	**reset install log-history oldest** *log-number*	該当せず
ISSUロールバックポイントをクリアします。	**reset install rollback oldest** *point-id*	該当せず

ISSUのためにissuコマンドを使用する例

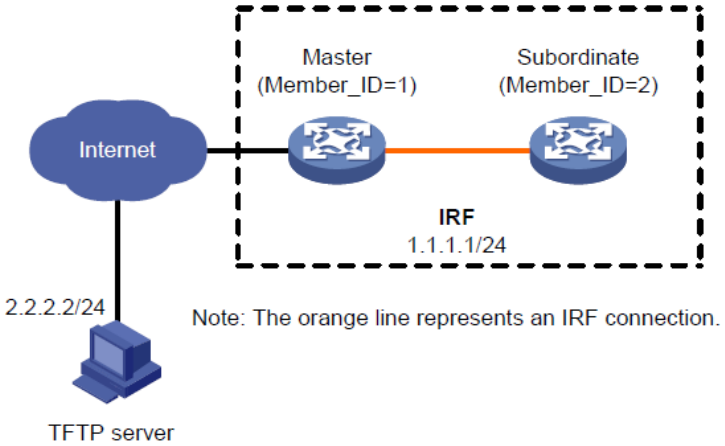
例:システムソフトウェアの互換バージョンへのアップグレード

アップグレード要件

図22に示すように、IRFファブリックには2つのメンバーを有しています。

ブートイメージ、システムイメージ、および機能イメージをT0001015からT0001016にアップグレードします。2つのバージョンに互換性があります。

図22ネットワーク図



アップグレード手順

TFTPサーバーからT0001016 Feature1機能を含むイメージファイルをダウンロードします。
<Sysname> tftp 2.2.2.2 get feature1-t0001016.bin
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 256 100 256 0 0 764 0 --:--:-- --:--:-- --:--:-- 810
Writing file...Done.
アクティブなソフトウェアイメージを表示します。
<Sysname> display install active

Active packages on slot 1:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
  flash:/feature1-t0001015.bin
Active packages on slot 2:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
  flash:/feature1-t0001015.bin
推奨されるISSUの方法とアップグレードの考えられる影響を特定します。
<Sysname> display version comp-matrix file feature flash:/feature1-t0001016.bin
Verifying the file flash:/feature1-t0001016.bin on slot 1...Done.
Identifying the upgrade methods.....Done.
Slot Upgrade Way
1 Service Upgrade
2 Service Upgrade
Influenced service according to following table on slot 1:
flash:/feature1-t0001016.bin
Feature1
Influenced service according to following table on slot 2:
flash:/feature1-t0001016.bin
Feature1
出力は、インクリメンタルアップグレードが推奨され、アップグレード中にFeature1モジュールがリブートされることを示しています。
#従属メンバーのFeature1機能をアップグレードします。

- 方法 1: 推奨された方式を使う。

<Sysname> issu load file feature flash:/feature1-t0001016.bin slot 2
This operation will delete the rollback point information for the previous upgrade
and maybe get unsaved configuration lost. Continue? [Y/N]:y
Verifying the file flash:/feature1-t0001016.bin on slot 1...Done.
Copying file flash:/feature1-t0001016.bin to
slot2#flash:/feature1-t0001016.bin.....Done.
Verifying the file flash:/feature1-t0001016.bin on slot 2...Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:

flash:/feature1-t0001016.bin
Running Version New Version
Test 0001015 Test 0001016

Slot Upgrade Way
2 Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.

- 方法 2: リブート方式を使う。

<Sysname> issu load file feature flash:/feature1-t0001016.bin slot 2 reboot
This operation will delete the rollback point information for the previous upgrade
and maybe get unsaved configuration lost. Continue? [Y/N]:y
Verifying the file flash:/feature1-t0001016.bin on slot 1...Done.
Copying file flash:/feature1-t0001016.bin to
slot2#flash:/feature1-t0001016.bin.....Done.

Verifying the file flash:/feature1-t0001016.bin on slot 2...Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:
flash:/feature1-t0001016.bin

Running Version	New Version
Test 0001015	Test 0001016

Slot	Upgrade Way
2	Reboot

Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
メイン/バックアップFeature1プロセスの切り替えを実行します。
<Sysname> issu run switchover
Verifying the file flash:/feature1-t0001016.bin on slot 1...Done.
Upgrade summary according to following table:

flash:/feature1-t0001016.bin

Running Version	New Version
Test 0001015	Test 0001016

Slot	Switchover Way
1	Active standby process switchover

Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
元のマスターの機能をアップグレードする

- アップグレードで推奨される方法を使用した場合：
  <Sysname> issu commit slot 1
  Verifying the file flash:/feature1-t0001016.bin on slot 1...Done.
  Upgrade summary according to following table:

  flash:/feature1-t0001016.bin

Running Version	New Version
Test 0001015	Test 0001016

Slot	Upgrade Way
1	Service Upgrade

  Upgrading software images to compatible versions. Continue? [Y/N]:y
  This operation might take several minutes, please wait...Done.
- リブート方式を使用した場合：
  <Sysname> issu commit slot 1
  Upgrade summary according to following table:

  flash:/feature1-t0001016.bin

Running Version	New Version
Test 0001015	Test 0001016
Slot	Upgrade Way
1	Reboot

  Upgrading software images to compatible versions. Continue? [Y/N]:y
  This operation might take several minutes, please wait...Done.

両方のメンバーが新しいFeature1イメージを実行していることを確認します

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
  flash:/feature1-t0001016.bin
Active packages on slot 2:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
  flash:/feature1-t0001016.bin
```

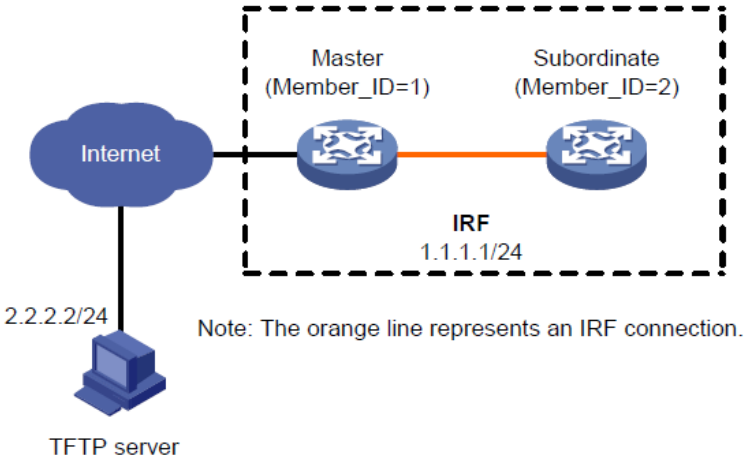
例:システムソフトウェアの互換性のないバージョンへのアップグレード

アップグレード要件

図23に示すように、IRFファブリックは2つのメンバーを有する。

ブートイメージ、システムイメージ、および機能イメージをT0001015から互換性のないバージョンのT0001017にアップグレードします。

図23ネットワーク図



アップグレード手順

#TFTPサーバーからアップグレードイメージファイルをダウンロードします。

```
<Sysname> tftp 2.2.2.2 get feature1-t0001016.bin
% Total % Received % Xferd Average Speed Time Time Time Current
                                 Dload Upload Total Spent Left Speed
100 256 100 256 0 0 764 0 --:--:-- --:--:-- --:--:-- 810
Writing file...Done.
```

#アクティブなソフトウェアイメージを表示します。

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
  flash:/feature-t0001015.bin
```

Active packages on slot 2:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
  flash:/feature-t0001015.bin
#推奨されるISSUの方法とアップグレードの考えられる影響を特定します。
<Sysname> display version comp-matrix file boot flash:/boot-t0001017.bin system flash:/system-t0001017.bin feature flash:/feature-t0001017.bin
Verifying the file flash:/feature-t0001017.bin on slot 1 Done.
Identifying the upgrade methods. Done.

Incompatible upgrade.
出力は、互換性のないアップグレードが推奨されることを示しています。カードはアップグレードのためにリブートされます。
#従属メンバーのFeature1機能をアップグレードします。
<Sysname> issu load file feature flash:/feature1-t0001016.bin slot 2
This operation will delete the rollback point information for the previous upgrade and
maybe get unsaved configuration lost. Continue? [Y/N]:y
Verifying the file flash:/feature1-t0001016.bin on slot 1...Done.
Copying file flash:/feature1-t0001016.bin to
slot2#flash:/feature1-t0001016.bin.....Done.
Verifying the file flash:/feature1-t0001016.bin on slot 2...Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:

flash:/feature1-t0001016.bin
  Running Version New Version
  Test 0001015 Test 0001016
  Slot Upgrade Way
  2 Reboot
Upgrading software images to incompatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
＃元のマスターのFeature1機能をアップグレードします。
<Sysname> issu run switchover
Upgrade summary according to following table:

flash:/feature1-t0001016.bin
  Running Version New Version
  Test 0001015 Test 0001016
  Slot Upgrade Way
  1 Reboot
Upgrading software images to incompatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
＃両方のメンバーが新しいFeature1イメージを実行していることを確認します
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
  flash:/feature1-t0001016.bin
Active packages on slot2:
  flash:/boot-t0001015.bin

flash:/system-t0001015.bin
flash:/feature1-t0001016.bin

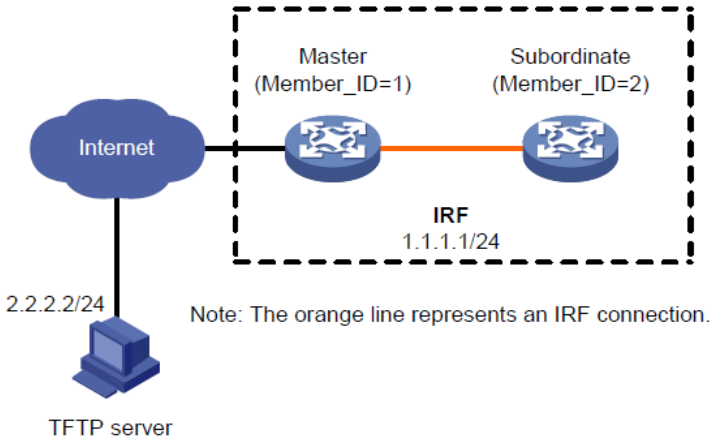
例:システムソフトウェアのロールバック

ロールバック要件

図24に示すように、IRFファブリックは2つの部材を有する。

T0001015からT0001016にアップグレードした後、ブートイメージ、システムイメージ、および機能イメージをT0001016からT0001015にロールバックします。T0001016とT0001015は互換性があります。

図24ネットワーク図



ロールバック手順

#TFTPサーバーからT0001016 Feature1 機能を含むイメージファイルをダウンロードします。

```
<Sysname> tftp 2.2.2.2 get feature1-t0001016.bin
% Total % Received % Xferd Average Speed Time Time Time Current
                                 Dload Upload Total Spent Left Speed
100 256 100 256 0 0 764 0 --:--:-- --:--:-- --:--:-- 810
Writing file...Done.
```

アクティブなソフトウェアイメージの表示

```
<Sysname> display install active
Active packages on slot 1:
   flash:/boot-t0001015.bin
   flash:/system-t0001015.bin
   flash:/feature1-t0001015.bin
Active packages on slot 2:
   flash:/boot-t0001015.bin
   flash:/system-t0001015.bin
   flash:/feature1-t0001015.bin
```

推奨されるISSUの方法とアップグレードの考えられる影響を特定する

```
<Sysname> display version comp-matrix file feature flash:/feature1-t0001016.bin
Verifying the file flash:/feature1-t0001016.bin on slot 1...Done.
Identifying the upgrade methods.....Done.

    Slot                Upgrade Way
    1              Service Upgrade
     2                 Service Upgrade

Influenced service according to following table on slot 1:
      flash:/feature1-t0001016.bin
```

```
        Feature1
Influenced service according to following table on slot 2:
    flash:/feature1-t0001016.bin
        Feature1
```

出力は、インクリメンタルアップグレードが推奨され、アップグレード中にFeature1モジュールがリブートされることを示しています。

従属メンバーのFeature1機能をアップグレードします

```
<Sysname> issu load file feature flash:/feature1-t0001016.bin slot 2
This operation will delete the rollback point information for the previous upgrade and
maybe get unsaved configuration lost. Continue? [Y/N]:y
Verifying the file flash:/feature1-t0001016.bin on slot 1...Done.
Copying file flash:/feature1-t0001016.bin to
slot2#flash:/feature1-t0001016.bin......Done.
Verifying the file flash:/feature1-t0001016.bin on slot 2...Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:

flash:/feature1-t0001016.bin
    Running Version          New Version
    Test 0001015             Test 0001016

    Slot                     Upgrade Way
    2                        Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
```

#メイン/バックアップFeature1プロセスの切り替えを実行します

```
<Sysname> issu run switchover
Upgrade summary according to following table:

flash:/feature1-t0001016.bin
 Running Version          New Version
 Test 0001015             Test 0001016

 Slot                     Switchover Way
 1              Active standby process switchover
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
```

アクティブなソフトウェアイメージを表示します。

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
  flash:/feature1-t0001015.bin
Active packages on slot 2:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
  flash:/feature1-t0001016.bin
```

Feature1機能をT0001015にロールバックします。

```
<Sysname> issu rollback
This command will quit the ISSU process and roll back to the previous version. Continue?
[Y/N]:Y
```

両方のメンバーが古いFeature1イメージを実行していることを確認します。

<Sysname> display install active
Active packages on slot 1:
flash:/boot-t0001015.bin
flash:/system-t0001015.bin
flash:/feature1-t0001015.bin
Active packages on slot 2:
flash:/boot-t0001015.bin
flash:/system-t0001015.bin
flash:/feature1-t0001015.bin

ISSUにinstallコマンドを使用する例

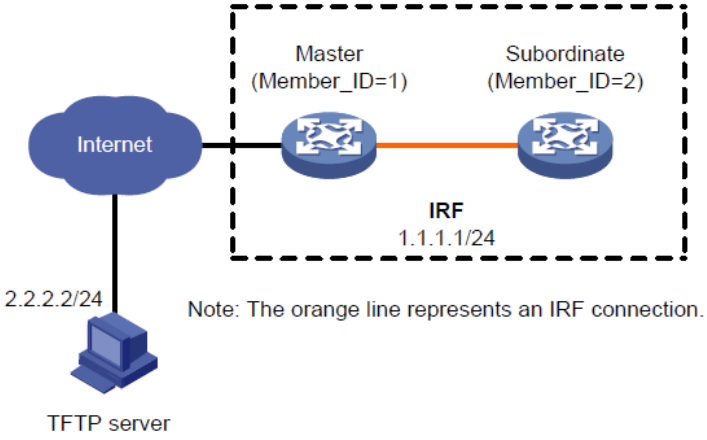
例:システムソフトウェアのアップグレード

アップグレード要件

図25に示すように、IRFファブリックは2つのメンバーを有する。

Feature 1の機能イメージをT0001015からT0001016にアップグレードします。2つのバージョンに互換性があります。

図25ネットワーク図



アップグレード手順

#T0001016 Feature1機能イメージを含む.ipeファイルをTFTPサーバーからダウンロードします。
<Sysname> tftp 2.2.2.2 get feature1-t0001016.ipe
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 256 100 256 0 0 764 0 --:--:-- --:--:-- --:--:-- 810
Writing file. Done.
#.ipeファイルを解凍します。
<Sysname> install add flash:/feature1-t0001016.ipe flash:
Verifying the file flash:/feature1-t0001016.ipe on slot 1 Done.
Decompressing file feature1-t0001016.bin to flash:/feature1-t0001016.bin Done.
#アクティブなソフトウェアイメージを表示します。
<Sysname> display install active Active packages on slot 1:
flash:/boot-t0001015.bin

flash:/system-t0001015.bin
flash:/feature1-t0001015.bin
Active packages on slot 2:
flash:/boot-t0001015.bin
flash:/system-t0001015.bin
flash:/feature1-t0001015.bin

#推奨されるISSU方式とアップグレードの影響を特定します。

<Sysname> install activate feature flash:/feature1-t0001016.bin slot 2 test
Copying file flash:/feature1-t0001016.bin to
slot2#flash:/feature1-t0001016.bin Done.
Verifying the file flash:/feature1-t0001016.bin on slot 2 Done.
Upgrade summary according to following table:

flash:/feature1-t0001016.bin

Running Version	New Version
Test 0001015	Test 0001016

Slot	Upgrade Way
2	Service Upgrade

Influenced service according to following table on slot 2
flash:/feature1-t0001016.bin
Feature1
<Sysname> install activate feature flash:/feature1-t0001016.bin slot 1 test
Verifying the file flash:/feature1-t0001016.bin on slot 1...Done.
Upgrade summary according to following table:

flash:/feature1-t0001016.bin

Running Version	New Version
Test 0001015	Test 0001016

Slot	Upgrade Way
1	Service Upgrade

Influenced service according to following table on slot 1:
flash:/feature1-t0001016.bin
Feature1

この出力は、両方のメンバーにサービスアップグレードが必要であり、アップグレード中にFeature 1モジュールがリブートされることを示しています。

#新しいFeature 1イメージをアクティブにして、Feature1機能をアップグレードします。

<Sysname> install activate feature flash:/feature1-t0001016.bin slot 2 Verifying the file flash:/feature1-t0001016.bin on slot 1...Done. flash:/feature1-t0001016.bin already exists on slot 2.
Overwrite it?[Y/N]:y
Copying file flash:/feature1-t0001016.bin to slot2#flash:/feature1-t0001016.bin Done.
Verifying the file flash:/feature1-t0001016.bin on slot 2 Done.
Upgrade summary according to following table:

flash:/feature1-t0001016.bin

Running Version	New Version
Test 0001015	Test 0001016

Slot	Upgrade Way
2	Service Upgrade

Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait. Done.
<Sysname> install activate feature flash:/feature1-t0001016.bin slot 1
Verifying the file flash:/feature1-t0001016.bin on slot 1 Done.

Upgrade summary according to following table:

flash:/feature1-t0001016.bin

Running Version	New Version
Test 0001015	Test 0001016
Slot	Upgrade Way
1	Service Upgrade

Upgrading software images to compatible versions. Continue? [Y/N]:y This operation might take several minutes, please wait...Done.

#アクティブなソフトウェアイメージを表示します。

<Sysname> display install active Active packages on slot 1:
flash:/boot-t0001015.bin flash:/system-t0001015.bin
flash:/feature1-t0001016.bin Active packages on slot 2:
flash:/boot-t0001015.bin flash:/system-t0001015.bin
flash:/feature1-t0001016.bin

#ソフトウェアの変更をコミットします。

<Sysname> install commit
This operation will take several minutes, please wait. Done.

例:機能をロールバックする

ロールバック要件

図25に示すように、IRFファブリックには2つのメンバーがあります。Feature 1機能はT0001015からT0001016にアップグレードされましたが、ソフトウェアの変更はコミットされていません。

Feature1機能をT0001016からT0001015にロールバックします。

ロールバック手順

#アクティブなソフトウェアイメージを表示します。

<Sysname> display install active
Active packages on slot 1:
flash:/boot-t0001015.bin
flash:/system-t0001015.bin
flash:/feature1-t0001016.bin
Active packages on slot2:
flash:/boot-t0001015.bin
flash:/system-t0001015.bin
flash:/feature1-t0001016.bin

#使用可能なロールバックポイントを表示します。

<Sysname> display install rollback
Install rollback information 1 on slot 1:
Updating from flash:/feature1-t0001015.bin
to flash:/feature1-t0001016.bin.
Install rollback information 2 on slot 2:
Updating from flash:/feature1-t0001015.bin
to flash:/feature1-t0001016.bin.

#Feature1機能をT0001015にロールバックします。

<Sysname> install rollback to original
This operation might take several minutes, please wait...Done.

#IRFメンバーが古いFeature1イメージを実行していることを確認します。

<Sysname> display install active

```
Active packages on slot 1:
   flash:/boot-t0001015.bin
   flash:/system-t0001015.bin
   flash:/feature1-t0001015.bin
Active packages on slot 2:
   flash:/boot-t0001015.bin
   flash:/system-t0001015.bin
   flash:/feature1-t0001015.bin
#ソフトウェアの変更をコミットします。
<Sysname> install commit
This operation will take several minutes, please wait.  Done.
```

デバイスの管理

この章では、基本的なデバイスパラメータを設定し、デバイスを管理する方法について説明します。

デバイス管理タスクの概要

デバイス管理タスクはすべてオプションです。任意のタスクを任意の順序で実行できます。

- 基本パラメーターの設定
  - デバイス名の構成
  - システム時刻の設定
  - 著作権表示の表示を有効にする
  - バナーの設定
- セキュリティパラメータの設定
  - パスワード回復機能の無効化
  - USB インターフェイスの無効化
- デバイス容量の調整
  - システム動作モードの設定
  - ポートステータス検出タイマーの設定
- デバイスの点検
  - CPU 使用率の監視
  - メモリーアラームしきい値の設定
  - 温度アラームしきい値の設定
- リソースの管理
  - 優先気流方向の指定
  - トランシーバーモジュールの検証と診断
- デバイスの保守
  - タスクのスケジュール
  - デバイスのリブート
  - 工場出荷時のデフォルトコンフィギュレーションの復元

デバイス名の設定

デバイス名について

デバイス名(ホスト名とも呼ばれる)は、ネットワーク内のデバイスを識別し、CLIビュープロンプトで使用されます。たとえば、デバイス名がSysnameの場合、ユーザービュープロンプトは<Sysname>です。

手順

1. システムビューに入ります。
   system-view
2. デバイス名を設定します。
   sysname *sysname*
   デフォルトでは、デバイス名はH3Cです。

システム時刻の設定

システム時刻について

システム時刻を正しく設定することは、ネットワーク不可欠です。ネットワーク上でデバイスを実行する前に、システム時刻を正しく設定してください。

デバイスは、次のいずれかの方法でシステム時刻を取得できます。

- ローカルに設定されたシステム時刻を使用し、内蔵の水晶発振器で生成されたクロック信号を使用してシステム時刻を維持します。
- NT P ソースから定期的に UTC 時刻を取得し、UTC 時刻、時間帯、および夏時間を使用してシステム時刻を計算します。NTP の詳細については、『Network Management and Monitoring Configuration Guide』を参照してください。

時刻ソースからUTC時刻を使用して計算されたシステム時刻の方が正確です。

システム時刻の設定に関する制約事項およびガイドライン

clock protocol noneコマンドを設定した後、**clock datetime**コマンドは、時間帯または夏時間が設定されているかどうかにかかわらず、システム時刻を判別します。

デバイスがシステム時刻を取得した後に時間帯または夏時間を設定または変更すると、デバイスはシステム時刻を再計算します。システム時刻を表示するには、**display clock**コマンドを使用します。

システム時刻設定タスクの概要

システム時刻を設定するには、以下のタスクを実行してください。

1. システム時刻の設定
   次のいずれかの操作を行います。

- CLI でのシステム時刻の設定
- 時間プロトコルを介して UTC 時間を取得する

2. (必要に応じて)。タイムゾーンの設定
   各ネットワークデバイスが、デバイスが存在する場所のタイムゾーンを使用していることを確認します。
3. (必要に応じて)。夏時間の設定
   各ネットワークデバイスで、デバイスが存在する場所の夏時間パラメーターが使用されていることを確認します。

CLI でのシステム時刻の設定

1. システムビューに入ります。
   system-view
2. ローカルシステム時刻を使用するようにデバイスを設定します。
   clock protocol none
   デフォルトでは、デバイスは NTP タイムソースを使用します。
   clock protocol コマンドを複数回実行すると、最新の設定が有効になります。
3. ユーザービューに戻ります。
   quit
4. ローカルシステムの時刻を設定します。
   clock datetime *time date*
   デフォルトでは、システム時刻は UTC 時刻 00:00:00 01/01/2013 です。

タイムプロトコルによる UTC 時刻の取得

1. システムビューに入ります。
   system-view
2. システム時刻ソースを指定します。
   clock protocol ntp
   デフォルトでは、デバイスは NTP タイムソースを使用します。
   このコマンドを複数回実行すると、最新の設定が有効になります。
3. タイムプロトコルパラメータを設定します。
   NT P 設定の詳細については、『Network Management and Monitoring Configuration Guide』を参照してください。

タイムゾーンの設定

1. システムビューに入ります。
   system-view
2. タイムゾーンを設定します。
   clock timezone *zone-name* { **add** | **minus** } *zone-offset*

デフォルトでは、システムは UTC 時間帯を使用します。

サマータイムの設定

1. システムビューに入ります。

   system-view
2. 夏時間を設定します。

   clock summer-time *name start-time start-date end-time end-date add-time*

   デフォルトでは、夏時間は設定されていません。

copyrightステートメントの表示を有効にする

著作権表示について

この機能を使用すると、デバイスは次の状況で著作権情報を表示できます。

- Telnet または SSH ユーザーがログインしたとき。
- コンソールユーザーがユーザービューを終了したとき。これは、デバイスが自動的にユーザーセッションをリブートしようとするためです。

copyright ステートメントの表示を無効にすると、デバイスはどのような状況でも copyright ステートメントを表示しません。

手順

1. システムビューに入ります。

   system-view
2. copyright ステートメントの表示を有効にします。

   copyright-info enable

   デフォルトでは、copyright ステートメントの表示は有効になっています。

バナーの設定

バナーについて

バナーは、ユーザーがログインしたときにシステムが表示するメッセージです。

システムでは、次のバナーがサポートされています。

- **Legal banner -** copyright ステートメントの後に表示されます。ログインを続行するには、Y を入力するか Enter キーを押す必要があります。プロセスを終了するには、N を入力する必要があります。Y と N は大文字と小文字を区別しません。
- **Message of the Day(MOTD)バナー -** 法的バナーの後、ログインバナーの前に表示されます。
- **Login banner -** パスワードまたはスキーム認証が設定されている場合にだけ表示されます。
- **Shell バナー -** ユーザーがユーザービューにアクセスしたときに表示されます。

バナーは、リーガルバナー、MOTDバナー、ログインバナー、シェルバナーの順に表示されます。

バナー入力方式

次のいずれかの方法でバナーを設定できます。

- コマンドライン全体を 1 行で入力します。

  バナーにキャリッジリターンを含めることはできません。コマンドキーワード、バナーおよび区切り文字を含むコマンドライン全体には、最大 511 文字を使用できます。バナーの区切り文字には、印刷可能な任意の文字を使用できますが、同じである必要があります。終了区切り文字を入力する前に **Enter** キーを押すことはできません。

  たとえば、シェルバナー「Have a nice day」を次のように設定できます。

  <System> system-view
  [System] header shell %Have a nice day.%

- コマンドラインを複数行で入力します。

  バナーには、キャリッジリターンを含めることができます。キャリッジリターンは 2 文字としてカウントされます。

  バナー設定コマンドラインを複数行で入力するには、次のいずれかの方法を使用します。

  - 最後のコマンドキーワードの後で **Enter** キーを押し、バナーを入力して、区切り文字%で最後の行を終了します。バナーと区切り文字は最大 1999 文字です。

    たとえば、バナー"Have a nice day."を次のように設定できます。

    <System> system-view
    [System] header shell
    Please input banner content, and quit with the character '%'.
    Have a nice day.%

  - 最後のコマンドキーワードを入力した後、バナーの開始デリミタとして表示可能な任意の文字を入力し、**Enter** キーを押します。次にバナーを入力し、同じデリミタで最終行を終了します。バナーと終了デリミタ文字です。1999

    たとえば、バナー「Have a nice day.」を次のように設定できます。

    <System> system-view
    [System] header shell A
    Please input banner content, and quit with the character 'A'.
    Have a nice day.A

  - 最後のコマンドキーワードを入力した後、開始区切り文字とバナーの一部を入力します。最後の文字列の最後の文字が開始区切り文字と異なることを確認します。次に、**Enter** キーを押して、残りのバナーを入力し、同じ区切り文字で最後の行を終了します。バナーと開始区切り文字および終了区切り文字は、最大 2002 文字です。

    たとえば、バナー"Have a nice day."を次のように設定できます。

    <System> system-view
    [System] header shell AHave a nice day.
    Please input banner content, and quit with the character 'A'.

手順

1. システムビューに入ります。

   system-view

2. リーガルバナーを設定します。

   header legal *text*

3. MOTD バナーを設定します。

   header motd *text*

4. ログインバナーを設定します。

header login *text*

5. シェルバナーを設定します。

   header shell *text*

パスワード回復機能の無効化

パスワード回復機能について

パスワード回復機能は、BootWare メニューからデバイス設定および SDRAM へのコンソールユーザーアクセスを制御します。BootWare メニューの詳細については、リリースノートを参照してください。

パスワード回復機能が有効の場合、コンソールユーザーは認証なしでデバイスコンフィギュレーションにアクセスして新しいパスワードを設定できます。

パスワード回復機能が無効になっている場合、コンソールユーザーは新しいパスワードを設定する前に、工場出荷時の設定を復元する必要があります。工場出荷時の設定を復元すると、次のスタートアップコンフィギュレーションファイルが削除されます。

システムセキュリティを強化するには、パスワード回復機能を無効にします。

手順

1. システムビューに入ります。

   system-view

2. パスワード回復機能を無効にします。

   undo password-recovery enable

   デフォルトでは、パスワード回復機能は有効です。

USBインターフェイスの無効化

USB インターフェイスの無効化について

USB インターフェイスを使用して、ファイルをアップロードまたはダウンロードできます。デフォルトでは、すべての USB インターフェイスが有効になっています。必要に応じて USB インターフェイスを無効にできます。

前提条件

このコマンドを使用する前に、umount コマンドを使用してすべての USB パーティションをアンマウントします。このコマンドの詳細については、「基本コマンドリファレンス」を参照してください。

手順

1. システムビューに入ります。

   system-view

2. USB インターフェイスを無効にします。

   usb disable

   デフォルトでは、すべての USB インターフェイスが有効になっています。

システム動作モードの設定

システム動作モードについて

デバイスは、次のいずれかのモードで動作できます。

- **0 -** 標準モード。
- **1 -** VXLAN モード。このモードは VXLAN をサポートし、VXLAN エントリを保存するために他の機能に使用される領域の量を減らします。VXLAN の詳細については、『VXLAN Configuration Guide』を参照してください。

制限事項とガイドライン

動作モードへの変更は、デバイスのリブート後に有効になります。

手順

1. システムビューに入ります。

   system-view
2. システムの動作モードを設定します。

   switch-mode { **0** | **1** }

   デフォルトでは、デバイスは標準モードで動作します。

ポートステータス検出タイマーの設定

ポート状態検出タイマーについて

ポートがプロトコルによってシャットダウンされると、デバイスはポートステータス検出タイマーを起動します。タイマーが期限切れになると、デバイスはポートを起動し、ポートステータスがポートの物理ステータスを反映するようにします。

手順

1. システムビューに入ります。

   system-view
2. ポートステータス検出タイマーを設定します。

   shutdown-interval *time*

   デフォルト設定は 30 秒です。

CPU使用率の監視

CPU 使用率の監視について

CPU使用率をモニタするために、デバイスは次の操作を実行します。

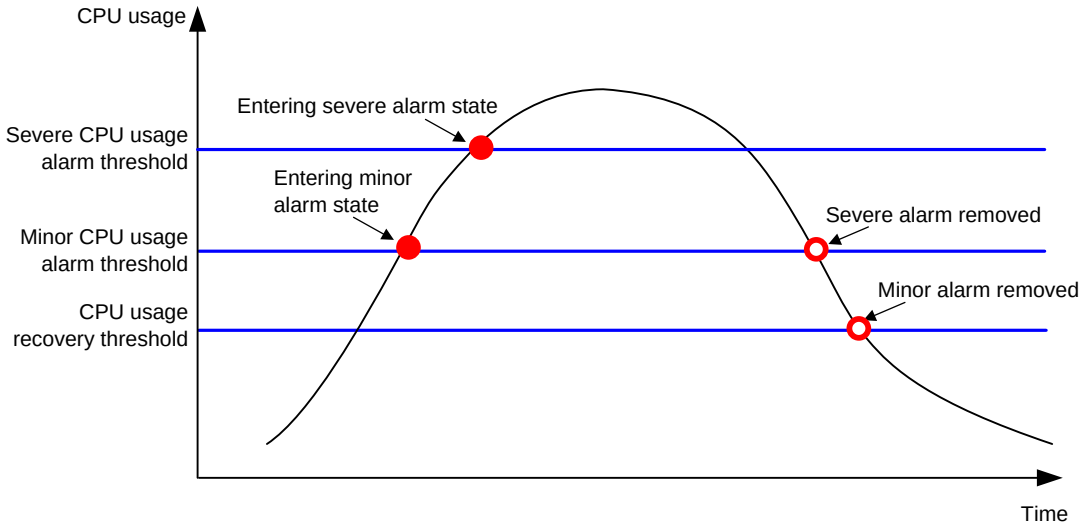
- 1 分間隔で CPU 使用率をサンプリングし、サンプルを CPU 使用率しきい値と比較して CPU 使用率ステータスを識別し、それに応じてアラームまたは通知を送信します。
- CPU 使用状況トラッキングが有効の場合、設定可能な間隔で CPU 使用状況をサンプリングして保存します。**display cpu-usage history** コマンドを使用すると、CPU 使用状況のヒストリー統計情報を座標系で表示できます。

デバイスは、次のCPU使用率しきい値をサポートします。

- **マイナーしきい値** - CPU 使用率がマイナーしきい値以上に増加したが、シビアしきい値未満の場合、CPU 使用率はマイナーアラーム状態になります。デバイスは、CPU 使用率がシビアしきい値以上に増加するか、マイナーアラームが削除されるまで、定期的にマイナーアラームを送信します。
- **重大なしきい値** - CPU 使用率が重大なしきい値を超えると、CPU 使用率は重大なアラーム状態になります。重大なアラームが削除されるまで、デバイスは定期的に重大なアラームを送信します。
- **リカバリーしきい値** - CPU 使用率がリカバリーしきい値を下回ると、CPU 使用率はリカバリー状態になります。デバイスはリカバリー通知を送信します。

CPU 使用率のアラームと通知は、NETCONF イベント、SNMP トラップと情報、およびログメッセージとしてカプセル化される NETCONF、SNMP、およびインフォメーションセンターに送信できます。詳細については、『Network Management and Monitoring Configuration Guide』の「NETCONF,SNMP,およびインフォメーションセンター」を参照してください。

図26 CPUアラームおよびアラーム削除通知



手順

1. システムビューに入ります

   system-view
2. CPU 使用率アラームしきい値を設定します。

   monitor cpu-usage threshold *severe-threshold* **minor-threshold** *minor-threshold* **recovery-threshold** *recovery-threshold* [**slot** *slot-number* [**cpu** *cpu-number*]]

   デフォルト設定は以下の通りです。

   - **重大な CPU 使用率アラームしきい値 99%。**
   - **マイナーCPU 使用率アラームしきい値 80%。**
   - **CPU 使用率リカバリーしきい値 60%。**
3. CPU 使用率アラーム再送間隔を設定します。

   monitor resend cpu-usage { **minor-interval** *minor-interval* | **severe-interval** *severe-interval* } * [**slot** *slot-number* [**cpu** *cpu-number*]]

   デフォルトでは、マイナーアラーム再送信間隔は 300 秒、シビアアラーム再送信間隔は 60 秒です。
4. CPU 使用率トラッキングのサンプリング間隔を設定します。

   monitor cpu-usage interval *interval* [**slot** *slot-number* [**cpu** *cpu-number*]]

   デフォルトでは、CPU 使用率トラッキングのサンプリング間隔は 1 分です。
5. CPU 使用率トラッキングを有効にします。

monitor cpu-usage enable [slot slot-number [cpu cpu-number]]

デフォルトでは、CPU 使用率トラッキングは有効です。

メモリーアラームしきい値の設定

メモリーアラームしきい値について

正常な動作を保証し、メモリー効率を向上させるために、システムは空きメモリースペースの量をリアルタイムで監視します。空きメモリースペースの量がマイナー、重大、またはクリティカルアラームしきい値に達すると、システムは影響を受けるサービスモジュールおよびプロセスにアラームを発行します。

早期警告機能は、メモリー不足状態が近づいていることを警告します。

表 15 と図 27 に示すように、システムは次の空きメモリーしきい値をサポートします。

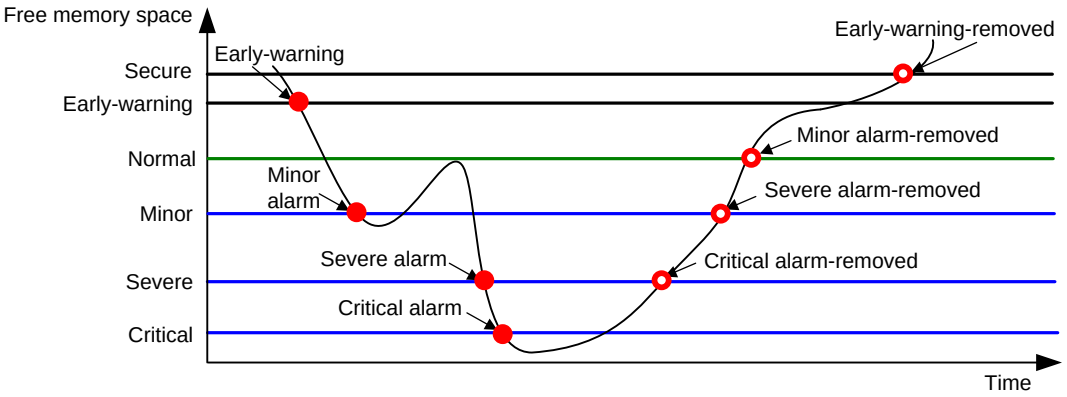
- 十分なメモリーのしきい値。
- 早期警告しきい値。
- 正常状態のしきい値。
- マイナーアラームしきい値。
- 重大アラームしきい値。
- クリティカルアラームしきい値。

表15 メモリーアラーム通知およびメモリーアラーム削除通知

通知	トリガー条件	注意
早期警告通知	空きメモリースペースの量が、初期警告しきい値以下に初めて減少します。	早期警告通知の生成および送信後、最初の早期警告が削除されるまで、システムは追加の早期警告通知を生成および送信しません。
マイナーアラーム通知	空きメモリースペースの量がマイナーアラームしきい値以下に初めて減少しました。	マイナーアラーム通知の生成および送信後、最初のマイナーアラームが削除されるまで、システムは追加のマイナーアラーム通知を生成および送信しません。
重大アラーム通知	空きメモリースペースの量が、重大アラームしきい値以下に初めて減少しました。	重大アラーム通知の生成および送信後、システムは、最初の重大アラームが削除されるまで、追加の重大アラーム通知を生成および送信しません。
クリティカルアラーム通知	空きメモリースペースの量が初めてクリティカルアラームしきい値以下に減少しました。	クリティカルアラーム通知の生成および送信後、最初のクリティカルアラームが削除されるまで、システムは追加のクリティカルアラーム通知を生成および送信しません。
クリティカルアラーム削除通知	空きメモリースペースの量は、重大アラームしきい値以上に増加します。	該当せず
重大アラーム削除通知	空きメモリー容量がマイナーアラームしきい値以上に増加しました。	該当せず
マイナーアラーム削除通知	空きメモリー容量が通常の状態しきい値以上に増加します。	該当せず
早期警告:削除された通知	空きメモリースペースの量が十分	該当せず

通知	トリガー条件	注意
	なメモリーしきい値以上に増加します。	

図27 メモリーアラーム通知およびアラーム削除通知



手順

1. システムビューに入ります

   system-view
2. メモリー使用量しきい値を設定します。

   memory-threshold [**slot** *slot-number* [**cpu** *cpu-number*]] **usage** *memory-threshold*

   デフォルトでは、メモリー使用量のしきい値は 100%です。
3. 空きメモリーしきい値を設定します。

   memory-threshold [**slot** *slot-number* [**cpu** *cpu-number*]] [**ratio**] *minor minor-value* **severe** *severe-value* **critical** *critical-value* **normal** *normal-value* [**early-warning** *early-warning-value* **secure** *secure-value*]

   デフォルト設定は以下の通りです。

   - **マイナーアラームしきい値 -** 96MB。
   - **重大アラームしきい値 -** 64MB。
   - **クリティカルアラームしきい値 -** 48MB。
   - **正常状態のしきい値 -** 128MB。
   - **早期警告しきい値 -** 192MB。
   - **十分なメモリーしきい値 - 304MB。**
4. メモリー不足アラームの再送間隔を設定します。

   monitor resend memory-threshold { **critical-interval** *critical-interval* | **early-warning-interval** *early-warning-interval* | **minor-interval** *minor-interval* | **severe-interval** *severe-interval* } * [**slot** *slot-numbe***r [cpu** *cpu-number*]]

   デフォルト設定は次のとおりです。

   - **早期警告再送信間隔 - 1 時間。**
   - **マイナーアラーム再送間隔 - 12 時間。**
   - **重大アラーム再送間隔 - 3 時間。**
   - **クリティカルアラーム再送信間隔 - 1 時間。**

温度アラームしきい値の設定

温度アラームしきい値について

デバイスは、次のしきい値に基づいて温度を監視します。

- 低温しきい値。
- 高温警告しきい値。
- 高温警告しきい値。

デバイスの温度が低温しきい値を下回るか、高温警告またはアラームのしきい値に達すると、デバイスは次の動作を実行します。

- ログメッセージとトラップを送信します。
- デバイスパネルの LED を設定します。

手順

1. システムビューに入ります。

   system-view
2. 温度アラームしきい値を設定します。

   temperature-limit slot *slot-number* **hotspot** *sensor-number lowlimit warninglimit* [*alarmlimit*]

   デフォルトは、温度センサーモデルによって異なります。デフォルトを表示するには、**undo temperature-limit** コマンドと **display environment** コマンドを順番に実行します。

   高温警告しきい値は高温警告しきい値よりならず、高温警報閾値は低温警報閾値よりも高くなければならない。

最適な風量方向の指定

好ましい気流方向について

このデバイスでは、2 つのファントレイモデルを使用できます。一方のモデルには、ポート側から電源側への空気の流れがあります。もう一方のモデルには、電源側からポート側への空気の流れがあります。

ファントレイは、機器室の換気システムと同じ気流方向を使用する場合にのみ効果的に動作できます。優先気流方向も同じである必要があります。

ファントレイが正常に動作していない場合、またはファントレイの通気方向が優先通気方向と異なる場合、システムはトラップとログを送信します。ファントレイを交換する必要があります。

制限事項とガイドライン

S5560X-34S-EI および S5560X-54S-EI スイッチは、この機能をサポートしていません。

手順

1. システムビューに入ります。

   system-view
2. 優先する風量方向を指定します。

   fan prefer-direction slot *slot-number* { **port-to-power** | **power-to-port** }

   デフォルトでは、推奨される通気方向は電源装置側からポート側です。

トランシーバーモジュールの確認と診断

トランシーバーモジュールの確認

トランシーバーモジュールの検証について

トランシーバーモジュールの真正性を確認するには、次のいずれかの方法を使用できます。

- トランシーバーモジュールの主要パラメーター(トランシーバタイプ、コネクタタイプ、送信レーザの中心波長、転送距離、ベンダー名など)を表示します。
- 電子ラベルを表示します。電子ラベルはトランシーバーモジュールのプロファイルで、シリアル番号、製造日およびベンダー名などの永続的な構成が含まれます。データは、トランシーバーモジュールまたはデバイスのデバッグまたはテスト中にトランシーバーモジュールまたはデバイスの記憶域コンポーネントに書き込まれました。

デバイスは、トランシーバーモジュールのベンダー名を定期的にチェックします。トランシーバーモジュールにベンダー名がない場合、またはベンダー名が H3C でない場合、デバイスはトラップとログメッセージを繰り返し出力します。ロギングルールの詳細については、『Network Management and Monitoring Configuration Guide』を参照してください。

手順

トランシーバーモジュールを確認するには、任意のビューで次のコマンドを実行します。

- トランシーバーモジュールのキーパラメータを表示します。

  display transceiver interface [*interface-type interface-number*]
- トランシーバーモジュールの電気ラベル情報を表示します。

  display transceiver manuinfo interface [*interface-type interface-number*]

トランシーバーモジュールの診断

トランシーバーモジュールの診断について

このデバイスは、トランシーバーモジュールのアラームおよびデジタル診断機能を提供します。トランシーバーモジュールに障害が発生した場合、またはトランシーバーモジュールが正常に動作していない場合は、次のタスクを実行できます。

- トランシーバーモジュールに存在するアラームをチェックして、障害の原因を特定します。
- 温度、電圧、レーザーバイアス電流、TX 出力、RX 出力など、デジタル診断機能によって監視される重要なパラメーターを調べます。

手順

トランシーバーモジュールを診断するには、任意のビューで次のコマンドを実行します。

- トランシーバーアラームを表示します。

  display transceiver alarm interface [*interface-type interface-number*]
- トランシーバーモジュールのデジタル診断パラメーターの現在の値を表示します。

  display transceiver diagnosis interface [*interface-type interface-number*]

タスクのスケジュール

タスクのスケジュールについて

管理者の干渉を受けることなく、コマンドまたは一連のコマンドを自動的に実行するようにデバイスをスケジュールできます。

定期スケジュールまたは非定期スケジュールを設定できます。非定期スケジュールはコンフィギュレーションファイルに保存されず、デバイスのリブート時に失われます。定期スケジュールはスタートアップコンフィギュレーションファイルに保存され、自動的に定期的に実行されます。

制限事項とガイドライン

- デフォルトのシステム時刻は、常にリブート時に復元されます。タスクスケジュールが正しく実行されるようにするには、デバイスのリブート後にシステム時刻を再設定するか、NTP を設定します。NTP の詳細については、『Network Management and Monitoring Configuration Guide』を参照してください。
- コマンド(コマンド A)をジョブに割り当てるには、最初にコマンド A のビューを入力するコマンドをジョブに割り当てる必要があります。
- スケジュール内のすべてのコマンドがコマンド構文に準拠していることを確認します。コマンドをジョブに割り当てるとき、構文はチェックされません。
- スケジュールには、**telnet**、**ftp**、**ssh2**、および **monitor process** のいずれかのコマンドを含めることはできません。
- スケジュールでは、ユーザーとの対話はサポートされていません。コマンドに yes または no の応答が必要な場合、システムでは常に **Y** または **Yes** が入力されているとみなされます。コマンドに文字列の入力が必要な場合、システムではデフォルトの文字列(ある場合)または NULL 文字列が入力されているとみなされます。
- スケジュールはバックグラウンドで実行され、スケジュールの出力(ログ、トラップ、およびデバッグ情報を除く)は表示されません。

手順

1. システムビューに入ります。

   system-view
2. ジョブを作成します。

   scheduler job *job-name*
3. ジョブにコマンドを割り当てます。

   command *id command*

   デフォルトでは、コマンドはジョブに割り当てられません。

   1 つのジョブに複数のコマンドを割り当てることができます。小さい ID のコマンドが最初に実行されます。
4. システムビューに戻ります。

   quit
5. スケジュールを作成します。

   scheduler schedule *schedule-name*

6. ジョブをスケジュールに割り当てます。

   job *job-name*

   デフォルトでは、ジョブはスケジュールに割り当てられません。

   1 つのスケジュールに複数のジョブを割り当てることができます。ジョブは同時に実行されます。
7. スケジュールにユーザーロールを割り当てます。

   user-role *role-name*

   デフォルトでは、スケジュールにはスケジュール作成者のユーザーロールが割り当てられます。

   スケジュールには最大 64 のユーザーロールを割り当てることができます。スケジュール内のコマンドは、スケジュールの 1 つ以上のユーザーロールによって許可されている場合に実行できます。
8. スケジュールの実行時間を指定します。

   必要に応じて、次のいずれかのオプションを選択します。

   - 特定の時点でスケジュールを実行します。

     time at *time date*

     time once at *time* [**month-date** *month-day* | **week-day** *week-day*&<1-7>]
   - 一定時間後にスケジュールを実行します。

     time once delay *time*
   - 月または週の指定した曜日の指定した時刻にスケジュールを実行します。

     time repeating at *time* [**month-date** [*month-day* | **last**] | **week-day** *week-day*&<1-7>]
   - 指定した時刻以降の間隔でスケジュールを実行します。

     time repeating [**at** *time* [*date*]] **interval** *interval*

   デフォルトでは、スケジュールの実行時間は指定されていません。

   time コマンドは互いに上書きします。最後に設定されたコマンドが有効になります。

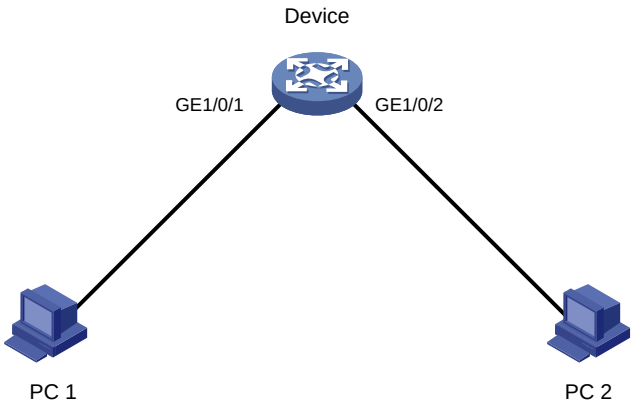
例:タスクのスケジュール

ネットワークの設定

図 28 に示すように、デバイスの 2 つのインターフェイスがユーザーに接続されています。
電力を節約するには、次の操作を実行するようにデバイスを設定します。

- 毎週月曜日から金曜日の午前 8:00 にインターフェイスを有効にします。
- 毎週月曜日から金曜日の 18:00 にインターフェイスを無効にします。

図28 ネットワーク図



手順

#システムビューに入ります。
<Sysname> system-view

#インターフェイスを無効にするジョブを設定します。
[Sysname] scheduler job shutdown-GigabitEthernet1/0/1
[Sysname-job-shutdown-] command 1 system-view
[Sysname-job-shutdown-] command 2 interface GigabitEthernet1/0/1
[Sysname-job-shutdown-] command 3 shutdown
[Sysname-job-shutdown-] quit

#インターフェイスを有効にするジョブを設定します。
[Sysname] scheduler job start-GigabitEthernet1/0/1
[Sysname-job-start-] command 1 system-view
[Sysname-job-start-] command 2 interface GigabitEthernet1/0/1
[Sysname-job-start-] command 3 undo shutdown
[Sysname-job-start-] quit

#インターフェイスを無効にするジョブを設定します。
[Sysname] scheduler job shutdown-GigabitEthernet1/0/2
[Sysname-job-shutdown-] command 1 system-view
[Sysname-job-shutdown-] command 2 interface GigabitEthernet1/0/2
[Sysname-job-shutdown-] command 3 shutdown
[Sysname-job-shutdown-] quit

#インターフェイスを有効にするジョブを設定します。
[Sysname] scheduler job start-GigabitEthernet1/0/2
[Sysname-job-start-] command 1 system-view
[Sysname-job-start-] command 2 interface GigabitEthernet1/0/2
[Sysname-job-start-] command 3 undo shutdown
[Sysname-job-start-] quit

#毎週月曜日から金曜日の午前8:00にインターフェイスを有効にする定期的なスケジュールを設定します。
[Sysname] scheduler schedule START-pc1/pc2
[Sysname-schedule-START-pc1/pc2] job start-GigabitEthernet1/0/1
[Sysname-schedule-START-pc1/pc2] job start-GigabitEthernet1/0/2
[Sysname-schedule-START-pc1/pc2] time repeating at 8:00 week-day mon tue wed thu fri
[Sysname-schedule-START-pc1/pc2] quit

#毎週月曜日から金曜日の18:00にインターフェイスを無効にする定期的なスケジュールを設定します。

```
[Sysname] scheduler schedule STOP-pc1/pc2
[Sysname-schedule-STOP-pc1/pc2] job shutdown-GigabitEthernet1/0/1
[Sysname-schedule-STOP-pc1/pc2] job shutdown-GigabitEthernet1/0/2
[Sysname-schedule-STOP-pc1/pc2] time repeating at 18:00 week-day mon tue wed thu fri
[Sysname-schedule-STOP-pc1/pc2] quit
```

コンフィギュレーションを検証する

```
#すべてのジョブの構成情報を表示します。
[Sysname] display scheduler job
Job name: shutdown-GigabitEthernet1/0/1
 system-view
 interface
 shutdown

Job name: shutdown-GigabitEthernet1/0/2
 system-view
 interface gigabitethernet 1/0/2
 shutdown

Job name: start-GigabitEthernet1/0/1
 system-view
 interface gigabitethernet 1/0/1
 undo shutdown

Job name: start-GigabitEthernet1/0/2
 system-view
 interface gigabitethernet 1/0/2
 undo shutdown
#スケジュール情報を表示します。
[Sysname] display scheduler schedule
Schedule name        : START-pc1/pc2
Schedule type        : Run on every Mon Tue Wed Thu Fri at 08:00:00
Start time           : Wed Sep 28 08:00:00 2011
Last execution time  : Wed Sep 28 08:00:00 2011
Last completion time : Wed Sep 28 08:00:03 2011
Execution counts     : 1
------------------------------------------------------------------------
Job name Last execution status
start-GigabitEthernet1/0/1                  Successful
start-GigabitEthernet1/0/2                  Successful

Schedule name        : STOP-pc1/pc2
Schedule type              : Run on every Mon Tue Wed Thu Fri at 18:00:00
Start time           : Wed Sep 28 18:00:00 2011
Last execution time  : Wed Sep 28 18:00:00 2011
Last completion time : Wed Sep 28 18:00:01 2011
Execution counts     : 1
------------------------------------------------------------------------
Job name                                Last execution status
```

shutdown- SuccessfulGigabitEthernet1/0/1
shutdown- SuccessfulGigabitEthernet1/0/2

#スケジュールログ情報を表示します。

[Sysname] display scheduler logfile
Job name : start-GigabitEthernet1/0/1
Schedule name:START-pc1/pc2
Execution time : Wed Sep 28 08:00:00 2011
Completion time : Wed Sep 28 08:00:02 2011
---------- Job output ----------
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]interface gigabitethernet 1/0/1
[Sysname-]undo shutdownGigabitEthernet1/0/1

Job name : start-GigabitEthernet1/0/2
Schedule name : START-pc1/pc2
Execution time : Wed Sep 28 08:00:00 2011
Completion time : Wed Sep 28 08:00:02 2011
---------- Job output ----------
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]interface gigabitethernet 1/0/2
[Sysname-]undo shutdownGigabitEthernet1/0/2

Job name : shutdown-GigabitEthernet1/0/1
Schedule name : STOP-pc1/pc2
Execution time : Wed Sep 28 18:00:00 2011
Completion time : Wed Sep 28 18:00:01 2011
---------- Job output ----------
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]interface gigabitethernet 1/0/1
[Sysname-]shutdownGigabitEthernet1/0/1

Job name : shutdown-GigabitEthernet1/0/2
Schedule name : STOP-pc1/pc2
Execution time : Wed Sep 28 18:00:00 2011
Completion time : Wed Sep 28 18:00:01 2011
---------- Job output ----------
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]interface gigabitethernet 1/0/2
[Sysname-]shutdownGigabitEthernet1/0/2

デバイスのリブート

デバイスのリブートについて

次のデバイスリブート方法を使用できます。

- CLI でリブートをスケジュールします。これにより、デバイスは指定した時刻または指定した時間が経過した後に自動的にリブートします。
- CLI でデバイスをただちにリブートします。

  リブートプロセス中、デバイスは次の操作を実行します。

  a. すべてのチップをリセットします。

  BootWare を使用して、スタートアップソフトウェアパッケージの確認、パッケージの解凍、およびイメージのロードを行います。

  b. システムを初期化します。
- デバイスの電源をオフにしてからオンにします。この方法はデータが失われる可能性があるため、最も推奨されない方法です。

CLIを使用すると、リモートホストからデバイスをリブートできます。

デバイスリブートに関する制限事項とガイドライン

デバイスをリブートすると、サービスが停止することがあります。

データセキュリティのため、デバイスはファイル操作の実行中にリブートしません。

CLI でのデバイスの即時リブート

前提条件

任意のビューで次の手順を実行します。

1. 次のスタートアップコンフィギュレーションファイルが正しく指定されていることを確認します。

   display startup

   display startup コマンドの詳細については、「基本コマンドリファレンス」を参照してください。
2. 起動イメージファイルが正しく指定されていることを確認します。

   display boot-loader

   1 つのメインスタートアップイメージファイルが破損しているか存在しない場合は、デバイスをリブートする前に別のメインスタートアップイメージファイルを指定する必要があります。

   display boot-loader コマンドの詳細については、基本コマンドリファレンスを参照してください。
3. 稼働中のコンフィギュレーションを次のスタートアップコンフィギュレーションファイルに保存します。

   save

   設定の損失を回避するには、リブートの前に実行コンフィギュレーションを保存します。

   save コマンドの詳細については、「基本コマンドリファレンス」を参照してください。

手順

CLIでデバイスをただちにリブートするには、ユーザービューで次のいずれかのコマンドを実行します。

reboot [**slot** *slot-number*] [**force**]

デバイスのリブートのスケジュール

制限事項とガイドライン

自動リブート設定は、すべてのメンバーデバイスで有効になります。マスター/下位スイッチオーバーが発生すると、自動リブート設定はキャンセルされます。

デバイスがサポートするデバイスリブートスケジュールは 1 つだけです。scheduler reboot コマンドを複数回実行すると、最新の設定が有効になります。

手順

リブートをスケジュールするには、ユーザービューで次のいずれかのコマンドを実行します。

- **Scheduler reboot at** *time* [*date*]
- **Scheduler reboot delay** *time*

デフォルトでは、デバイスのリブート時間は指定されていません。

工場出荷時のデフォルト設定の復元

工場出荷時の設定の復元について

別のシナリオでデバイスを使用する場合、または他の方法でデバイスをトラブルシューティングできない場合は、次の作業を実行して工場出荷時のデフォルト設定に戻します。

このタスクでは、.bin ファイルとライセンスファイルは削除されません。

制限事項とガイドライン

このタスクは中断を伴います。

手順

1. ユーザービューで次のコマンドを実行して、デバイスの工場出荷時のデフォルト設定を復元します。

   restore factory-default

2. デバイスをリブートします。

   reboot

   実行コンフィギュレーションを保存するかどうかを選択するプロンプトが表示されたら、N を入力します。実行コンフィギュレーションを保存する場合、デバイスは起動時に保存されたコンフィギュレーションをロードします。

デバイス管理設定の表示およびメンテナンスコマンド

任意のビューで **display** コマンドを実行します。ユーザービューで **reset scheduler logfile** コマンドを実行します。システムビューで **reset version-update-record** コマンドを実行します。

タスク	コマンド
システム時刻、日付、時間帯、および夏時間を表示します。	**display clock**
copyrightステートメントを表示します。	**display copyright**
CPU使用率統計情報を表示します。 coreキーワードは、control-planeキーワードおよびdata-planeキーワードと相互に排他的です。	**display cpu-usage** [**control-plane** | **data-plane**] [**summary**] [**slot** *slot-number* **[cpu** *cpu-number* [**core** { *core-number* | **all** }]]]
CPU使用率モニタリング設定を表示します。	**display cpu-usage configuration** [**slot** *slot-number* [**cpu** *cpu-number*]]
CPU使用率のヒストリー統計を座標系で表示します。	**display cpu-usage history** [**job** *job-id*] [**slot** *slot-number* [**cpu cpu-number]]**
ハードウェア情報を表示します。	**display device** [**flash** | **usb**] [**slot** *slot-number* [**subslot** *subslot-number*] | **verbose**]
デバイスの電子ラベル情報を表示します。	**display device manuinfo** [**slot** *slot-number*]
電源装置の電子ラベル情報を表示します。	**display device manuinfo slot** *slot-number* **power** *power-id*
機能およびハードウェアモジュールの動作情報を表示または保存します。	**display diagnostic-information** [**hardware** | **infrastructure** | **l2** | **l3** | **service**] [**key-info**] [*filename* **]**
デバイス温度情報を表示します。	**display environment** [**slot** *slot-number*]
ファントレイの動作状態を表示します。	**display fan** [**slot** *slot-number* [*fan-id*]]
メモリー使用状況の統計情報を表示します。	**display memory** [**summary**] [**slot** *slot-number* [**cpu** *cpu-number*]]
メモリーアラームしきい値と統計情報を表示します。	**display memory-threshold** [**slot** *slot-number* [**cpu** *cpu-number*]]
電源装置の情報を表示します。	**display power** [**slot** *slot-number* [*power-id*]]
ジョブ設定情報を表示します。	**display scheduler job** [**job-name**]
ジョブ実行ログ情報を表示します。	**display scheduler logfile**
自動リブートスケジュールを表示します。	**display scheduler reboot**
スケジュール情報を表示します。	**display scheduler schedule** [*schedule-name*]
システムの安定性とステータス情報を表示します。	**display system stable state**
システムバージョン情報を表示します。	**display version**

タスク	コマンド
スタートアップソフトウェアイメージアップグレードレコードを表示します。	**display version-update-record**
ジョブ実行ログ情報をクリアします。	**reset scheduler logfile**
スタートアップソフトウェアイメージアップグレードレコードをクリアします。	**reset version-update-record**

Tcl の使用

Tclについて

Comware V7には、組み込みのTool Command Language(Tcl)インタープリターが用意されています。ユーザービューから、**tclsh**コマンドを使用してTclコンフィギュレーションビューを開始し、次のコマンドを実行できます。

- Tcl 8.5コマンド。
- Comwareコマンド。

Tclコンフィギュレーションビューは、ユーザービューと同じです。Tclコンフィギュレーションビューでは、ユーザービューと同じ方法でComwareコマンドを使用できます。

制約事項および注意事項:Tcl

Tcl 設定ビューの下のサブビューから上位レベルのビューに戻るには、**quit**コマンドを使用します。

Tclコンフィギュレーションビューの下のサブビューからTclコンフィギュレーションビューに戻るには、**Ctrl+Z**を押します。

Tclコマンドを使用したデバイスの設定

制限とガイドライン

Tclを使用してデバイスを設定する場合は、次の制約事項および注意事項に従ってください。

- Tcl環境変数をComwareコマンドに適用できます。
- Tclコマンドに関するオンラインヘルプ情報は提供されていません。
- **Tab**キーを押して省略されたTclコマンドを完了することはできません。
- Tclコマンドが正しく実行できることを確認します。
- ベストプラクティスとして、TelnetまたはSSHを介してログインします。ショートカットキーまたはCLIコマンドを使用してTclコマンドを停止することはできません。Tclコマンドの実行中に問題が発生した場合、TelnetまたはSSHを介してログインしていれば、接続を閉じることでプロセスを終了できます。コンソールポートからログインした場合は、デバイスをリブートする必要があります。
- **Ctrl+D**を押すと、Tclコマンド**read stdin**を中止できます。

手順

1. ユーザービューからTcl設定ビューに入ります

   tclsh
2. Tclコマンドを実行します。

   Tcl command
3. Tcl設定ビューからユーザービューに戻ります。
   - **tclquit**
   - **quit**

Tcl設定ビューでのComwareコマンドの実行

Tcl 設定ビューでの Comware コマンドの実行について

Tcl設定ビューでComwareコマンドを実行するには、次のいずれかの方法を使用します。

- Comwareコマンドを直接入力します。TclコマンドがComwareコマンドと同じコマンド文字列を使用する場合、Tclコマンドが実行されます。
- Comwareコマンドの前にcliキーワードを付けます。TclコマンドがComwareコマンドと同じコマンド文字列を使用する場合、Comwareコマンドが実行されます。

制限とガイドライン

Tcl設定ビューでComwareコマンドを実行する場合は、次の制約事項および注意事項に従ってください。

- 引用符(")または中カッコ({および})で囲まれた文字列を指定するには、引用符または中カッコの前にエスケープ文字(\)を使用する必要があります。たとえば、インターフェイスの説明として**"a"**を指定するには、**description\"a\"**と入力する必要があります。**description"a"**と入力すると、説明は**a**になります。
- Comwareコマンドの場合は、?と入力してオンラインヘルプを表示するか、**Tab**を押して省略されたコマンドを完了します。詳細については、「CLIの使用」を参照してください。
- cliコマンドはTclコマンドであるため、？を入力することはできません。オンラインヘルプを取得するか、**Tab**キーを押して短縮コマンドを完了します。
- 正常に実行されたComwareコマンドは、コマンドヒストリーバッファーに保存されます。上矢印キーまたは下矢印キーを使用すると、実行されたコマンドを取得できます。
- 1回の操作で複数のComwareコマンドを実行するには、次のいずれかの方法を使用します。
  - コマンドを入力順に実行するには、複数のComwareコマンドをセミコロンで区切って入力します。たとえば、**ospf 100;area 0**のように入力します。
  - cliコマンドに複数のComwareコマンドを指定し、引用符で囲み、スペースとセミコロンで区切ります。たとえば、**cli "ospf 100; area 0"**のようになります。
  - cliコマンドごとに1つのComwareコマンドを指定し、スペースとセミコロンで区切ります。たとえば、**cli ospf 100 ; cli area** 0のようになります。

手順

1. Tcl設定ビューに入ります

   tclsh
2. Comwareコマンドを実行します。
   - Comwareコマンドを直接実行します。

     command
   - cliコマンドを使用してComwareコマンドを実行します。

     Cli *コマンド*
3. Tcl設定ビューからユーザービューに戻ります。
   - **tclquit**
   - **quit**

Python を使用する

Pythonについて

Comware7には、Pythonインタープリターが組み込まれています。Pythonを使用すると、次のタスクを実行できます。

- Pythonスクリプトを実行して、自動デバイス設定を実装します。
- Python shellと入力し、次の項目を使用してデバイスを設定します。
  - Python2.7コマンド。
  - Python2.7標準API。
  - 拡張API。拡張APIの詳細については、「Comware7extended Python API」を参照してください。

Pythonスクリプトの実行

Pythonスクリプトを実行するには、ユーザービューで次のコマンドを使用します。

python *filename*

Pythonシェルに入る

ユーザービューからPythonシェルに入るには、次のコマンドを実行します。

python

拡張Python APIのインポートと使用

拡張Python APIを使用するには、まずAPIをPythonにインポートする必要があります。

拡張 API 全体のインポートと API の使用

手順

1. ユーザービューからPythonシェルに入ります。

   python
2. 拡張API全体をインポートします。

   import comware
3. 拡張API関数を実行します。

   comware.*api*

例

#拡張API関数Transferを使用して、TFTPサーバー192.168.1.26からtest.cfgファイルをダウンロード
#します。

```
<Sysname> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2

Type "help", "copyright", "credits" or "license" for more information.
>>> import platformtools
>>> platformtools.Transfer('tftp', '192.168.1.26', 'test.cfg', 'flash:/test.cfg', user='', password='')
<platformtools.Transfer object at 0xb7eab0e0>
```

拡張 API 関数のインポートと関数の使用

手順

1. ユーザービューからPythonシェルに入ります。

   python
2. 拡張API関数をインポートします。

   from comware import *api-name*
3. 拡張API関数を実行します。

   api-function

例

拡張API関数Transferを使用して、TFTPサーバー192.168.1.26からtest.cfgファイルをダウンロードします。

```
<Sysname> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
```

Type "help", "copyright", "credits" or "license" for more information.

>>> from platformtools import Transfer

>>> Transfer('tftp', '192.168.1.26', 'test.cfg', 'flash:/test.cfg', user='', password='')

<platformtools.Transfer object at 0xb7e5e0e0>

Pythonシェルを終了する

Pythonシェルを終了するには、Pythonシェルで次のコマンドを実行します。

exit()

Pythonの使用例

例:デバイス設定に Python スクリプトを使用する

ネットワークの設定

Pythonスクリプトを使用して、次のタスクを実行します。

- コンフィギュレーションファイル**main.cfg**および**backup.cfg**をデバイスにダウンロードします。
- 次の起動時のメインおよびバックアップコンフィギュレーションファイルとしてファイルを設定します。

図29ネットワーク図

手順

#PC上のテキストエディタを使用して、Pythonスクリプトtest.pyを次のように設定します。

#!usr/bin/python

import platformtools

platformtools.Transfer('tftp', '192.168.1.26', 'main.cfg', 'flash:/main.cfg') platformtools.Transfer('tftp', '192.168.1.26', 'backup.cfg', 'flash:/backup.cfg')

platformtools.CLI('startup saved-configuration flash:/main.cfg main ;startup saved-configuration flash:/backup.cfg backup')

Use TFTP to download the script to the device.

<Sysname> tftp 192.168.1.26 get test.py

Execute the script.

<Sysname> python flash:/test.py

<Sysname>startup saved-configuration flash:/main.cfg main Please wait.

..... Done.

<Sysname>startup saved-configuration flash:/backup.cfg backup Please wait.

..... Done.

コンフィギュレーションの検証

#スタートアップコンフィギュレーションファイルを表示します。

<Sysname> display startup

Current startup saved-configuration file: flash:/startup.cfg Next main startup saved-configuration file: flash:/main.cfg Next backup startup saved-configuration file:flash:/backup.cfg

Comware 7 拡張Python API

Comware 7 拡張Python APIは、Python構文と互換性があります。

CLI

CLIを使用してComware7 CLIコマンドを実行し、CLIオブジェクトを作成します。

構文

CLI (*command*='', *do_print*=True)

パラメーター

command: - 実行するコマンドを指定します。複数のコマンドを入力するには、スペースとセミコロン(;)で区切ります。ユーザービュー以外のビューでコマンドを入力するには、最初にビューに入るためのコマンドを入力する必要があります。例えば、次のようにします。
'system-view;local-user test class manage'と入力して、**local-user test class manage**コマンドを実行します。
do_print:実行結果を出力するかどうかを指定します。

- **True**-実行結果を出力します。この値はデフォルトです。
- **False**-実行結果を出力しません。

利用の手引き

このAPI関数はComware7コマンドのみをサポートします。Linux、Python、またはTclコマンドはサポートしません。

戻り値

CLIオブジェクト

例

testという名前のローカルユーザーを追加します。

<Sysname> python

Python 2.7.3 (default)

[GCC 4.4.1] on linux2

Type "help", "copyright", "credits" or "license" for more information.

>>> import platformtools

```
>>> platformtools.CLI('system-view ;local-user test class manage')
```

出力例

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] local-user test class manage
New local user added.
<platformtools.CLI object at 0xb7f680a0>
```

get_error

get_errorを使用して、ダウンロード操作からエラー情報を取得します。

構文

Transfer.get_error()

戻り値

エラー情報(エラー情報がない場合は**None**が返されます)

例

#TFTPサーバー1.1.1.1から**test.cfg**ファイルをダウンロードし、操作からエラー情報を取得します。

```
<Sysname> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import platformtools
>>> c = platformtools.Transfer('tftp', '1.1.1.1', 'test.cfg', 'flash:/test.cfg', user='',
password='')
>>> c.get_error()
```

出力例

```
'Timeout was reached'
```

get_output

実行されたコマンドの出力を取得するには、**get_output**を使用します。

構文

CLI.get_output()

戻り値

実行されたコマンドの出力

例

#ローカルユーザーを追加し、コマンドの出力を取得します。

```
<Sysname> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import platformtools
>>> c = platformtools.CLI('system-view ;local-user test class manage', False)
>>> c.get_output()
```

出力例

```
['<Sysname>system-view', 'System View: return to User View with Ctrl+Z.',
'[Sysname]local-user test class manage', 'New local user added.']
```

get_self_slot

get_self_slotを使用して、マスターデバイスのメンバーIDを取得します。

構文

get_self_slot()

戻り値

[-1,slot-number]の形式のリストオブジェクト。slot-numberはマスター装置のIDを表します。

例

#マスターデバイスのメンバーIDを取得します。

```
<Sysname> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import platformtools
>>> platformtools.get_self_slot()
```

出力例

【-1,0】

get_slot_info

メンバーデバイスに関する情報を取得するには、get_slot_infoを使用します。

構文

get_slot_info()

戻り値

{'Slot':slot-number,'Status':'status','Chassis':chassis-number 'Role':'role','Cpu':CPU-number}形式の辞書オブジェクト。slot-number引数は装置のメンバーIDを表します。status引数は、メンバーデバイスのステータスを示します。chassis-numberおよび*CPU-number引数は0に固定されています。role引数は、メンバーデバイスのロールを示します。*

例

#デバイス、カード、またはメンバーデバイスに関する情報を取得します。

<Sysname> python

Python 2.7.3 (default)

[GCC 4.4.1] on linux2

Type "help", "copyright", "credits" or "license" for more information.

>>> import platformtools

>>> platformtools.get_slot_info(1)

出力例

{'Slot': 1, 'Status': 'Normal', 'Chassis': 0, 'Role': 'Master', 'Cpu': 0}

get_slot_range

サポートされているIRFメンバーID範囲を取得するには、**get_slot_range**を使用します。

構文

get_slot_range()

戻り値

{'MaxSlot':max-slot-number,'MinSlot':min-slot-number}の形式のディクショナリオブジェクト。
*max-slot-number引数は、最大メンバーIDを示します。min-slot-number引数は*最小メンバーIDを示します。

例

#サポートされているIRFメンバーID範囲を取得します。

<Sysname> python

Python 2.7.3 (default)

[GCC 4.4.1] on linux2

Type "help", "copyright", "credits" or "license" for more information.

>>> import platformtools

>>> platformtools.get_slot_range()

出力例

{'MaxSlot': 129, 'MinSlot': 1}

get_standby_slot

get_standby_slotを使用して、下位デバイスのメンバーIDを取得します。

構文

get_standby_slot()

戻り値

次のいずれかの形式のリストオブジェクト。

•[ ]:IRF ファブリックに下位デバイスがありません。

•[[-1,slot-number]]:IRF ファブリックには 1 つの下位デバイスしかありません。

•[[[-1,slot-number1],[-1,slot-number2],...]:IRF ファブリックには複数の下位デバイスがあります。
slot-number引数は、下位デバイスのメンバーIDを示します。

例

#下位デバイスのメンバーIDを取得します。

<Sysname> python

Python 2.7.3 (default)

[GCC 4.4.1] on linux2

Type "help", "copyright", "credits" or "license" for more information.

>>> import platformtools

>>> platformtools.get_standby_slot()

出力例

[[-1,1],[-1,2]]

Transfer

transferを使用して、サーバーからファイルをダウンロードします。

構文

Transfer (protocol='',host='',source='',dest='',vrf='',login_timeout=**10**,user='', *password='')*

パラメーター

*protocol:*ファイルのダウンロードに使用するプロトコルを指定します。

- **ftp** - FTPを使用します。
- **tftp** - TFTPを使用します。
- **http** - HTTPを使用します。

Host - リモートサーバーのIPアドレスを指定します。
Source - リモートサーバーからダウンロードするファイルの名前を指定します。
Dest - ダウンロードしたファイルの名前を指定します。
Vrf - リモートサーバーが属するVPNインスタンスを指定します。この引数は、VPNインスタンス名、大文字と小文字を区別する1～31文字の文字列を表します。サーバーがパブリックネットワークに属している場合は、

この引数を指定しないでください。
*login_timeout :*操作のタイムアウトを秒単位で指定します。デフォルトは10です。
User - サーバーにログインするためのユーザー名を指定します。
Password - ログインパスワードを指定します。

戻り値

Transfer オブジェクト

例

TFTPサーバー192.168.1.26からファイル**test.cfg**をダウンロードする。

```
<Sysname> python
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import platformtools
>>> platformtools.Transfer('tftp', '192.168.1.26', 'test.cfg', 'flash:/test.cfg',
user='', password='')
```

出力例

```
<platformtools.Transfer object at 0xb7f700e0>
```

ライセンスの管理

ライセンスについて

ライセンスベースの機能をデバイス上で実行するには、ライセンスが必要です。

ライセンスの種類

ライセンスには、トライアルライセンスと正式ライセンスが含まれます。トライアルライセンスには通常、時間制限があります。トライアルライセンスの有効期限が切れる前に、ライセンスベースの機能の正式ライセンスを購入してインストールし、機能を引き続き使用できるようにします。

異なるデバイスタイプのライセンス

IRF メンバーデバイスごとにライセンスを購入し、各 IRF メンバーデバイスにライセンスをインストールする必要があります。IRF メンバーデバイスは、デバイスが別の IRF ファブリックに参加している場合でもライセンスが付与されます。

制約事項およびガイドライン:ライセンス管理

ライセンス操作

作業中のデバイスで、他のユーザーがライセンス管理タスクを実行していないことを確認します。

アクティベーションファイルと DID ファイルの操作

DID ファイルまたはアクティベーションファイルを管理する場合は、次の制約事項およびガイドラインに従ってください。

- ファイルの破損を防ぐために、ファイルを開いたり編集したりしないでください。
- ライセンスエラーを回避するために、ファイルの名前を変更しないでください。
- ライセンス機能が正常に機能するためには、**flash:/license** ディレクトリで使用可能または使用中のファイルを削除しないでください。ライセンス管理機能は、このディレクトリをライセンス管理に使用します。

IRF ファブリックのライセンス整合性

ライセンス供与された機能を IRF ファブリックで正しく機能させるには、すべての IRF メンバーデバイスが同じライセンスがインストールされていることを確認してください。

ライセンス管理タスクの概要

ライセンスを管理するには、以下のタスクを実行してください。

1. ライセンスストレージの識別
2. (必要に応じて)。ライセンスストレージの圧縮
3. ライセンス登録に必要な情報の取得
4. ライセンスの登録
5. ライセンスのインストール
6. インストール済みライセンスの管理
   - ライセンスのアンインストール
   - ライセンスの転送
7. アクティベーションファイルを回復する

ライセンスストレージの識別

ライセンスストレージを識別するには、任意のビューで次のコマンドを実行します。

display license feature

コマンド出力から、**Total** および **Usage** フィールドを表示して、残りのライセンスストレージが新しいライセンスのインストールに十分かどうかを調べます。残りのライセンスストレージが十分でない場合は、ライセンスストレージを圧縮します。

ライセンスストレージの圧縮

ライセンスストレージ圧縮について

ライセンスストレージを圧縮して、期限切れおよびアンインストールされたライセンス情報を削除し、新しいライセンスをインストールするための十分なストレージスペースを確保します。

制限事項とガイドライン

DID は、ライセンスストレージが圧縮されるたびに変更されます。古い DID に基づいて生成されたライセンスは、圧縮後にインストールできません。

手順

1. アンインストールされたライセンスのアンインストールキーをバックアップします。
   有効期限が切れていないライセンスをアンインストールすると、アンインストールキーが作成されます。ライセンスを転送するには、アンインストールキーが必要です。
2. 古いDIDに基づいて生成されたすべてのライセンスがインストールされていることを確認します。
3. システムビューに入ります。
   system-view
4. ライセンスストレージを圧縮します。
   license compress slot *slot-number*

ライセンス登録に必要な情報の取得

1. (任意)display license featureコマンドを使用して、ライセンスを適用する機能を指定します。
2. 以下の情報を入手してください。
   - ライセンスキー。ライセンスを購入すると取得できます。
   - SNおよびDID情報。**display license device-id**コマンドを使用して取得できます。
3. FTPまたはTFTPを使用して、ファイルをPCなどのWebクライアントにアップロードします。
4. FTPを使用して.idファイルを転送する場合は、バイナリモードを使用します。
5. ライセンスキー、SN、およびDID情報を失われた場合に備えてバックアップします。

ライセンスの登録

制限とガイドライン

オペレーティングシステムやブラウザのエラーなどの問題が原因でアクティベーションファイルを取得または再登録できない場合は、H3C サポートに連絡してください。

手順

1. http://www.h3c.com/hk/Technical_Support___Documents/Product_Licensing/にアクセスし、ナビゲーションツリーから**Register the First Time**または**Register Upgrade Licenses**を選択します。

   アップグレードライセンスは、アドオンノード、アドオン機能、または時間延長に使用されます。
2. 製品カテゴリを選択し、ライセンスキー、SN、およびDIDを使用してライセンスを登録します。
3. アクティベーションファイルまたはアクティベーションキーを取得し、PCにダウンロードします。

ライセンスのインストール

ライセンスのインストールについて

ライセンスをインストールすると、システムは自動的にストレージメディアで一致する機能パッケージを検索します。一致する機能パッケージが見つかると、検索を停止してパッケージをインストールします。

アクティベーションファイルのインストール

1. システムビューに入ります。

   system-view
2. アクティベーションファイルをインストールします。

   license activation-file install *file-name* **slot** *slot-number*

ライセンスのアンインストール

ライセンスのアンインストールについて

ライセンスがしばらく使用されていない場合、または別のデバイスに転送する必要がある場合に、期限切れになっていない正式ライセンスをアンインストールするには、次の作業を実行します。

アンインストール後、アンインストールキーが生成され、ライセンス転送に使用されます。

ライセンスのアンインストールに関する制限事項とガイドライン

試用ライセンスは転送できません。試用ライセンスをアンインストールしても、アンインストール情報は作成されません。
期限切れのライセンスはアンインストールできません。

デバイスでアンインストールされたライセンスは、デバイスに再インストールできません。別のデバイスにのみ転送できます。

アクティベーションファイルのアンインストール

1. システムビューに入ります。

   system-view

2. アクティベーションファイルをアンインストールします。

   license activation-file uninstall *file-name* **slot** *slot-number*

   期限切れになっていないアクティベーションファイルだけをアンインストールできます。

ライセンスの転送

ライセンスの転送について

ライセンスの有効期限が切れていない場合は、デバイス間でライセンスを転送できます。

手順

1. ソースデバイスにログインし、ライセンスをアンインストールしてアンインストール情報を取得します。詳細については、「ライセンスのアンインストール」を参照してください。
2. **display license** コマンドを使用して、ライセンスのアンインストールキーを取得します。
3. ターゲットデバイスにアクセスし、SN および DID 情報を取得します。詳しくは、「ライセンス登録に必要な情報の入手」をご覧ください。
4. ターゲットデバイスのライセンスを登録します。詳細については、「ライセンスの登録」を参照してください。

   ライセンス登録時に、ターゲットデバイスの SN および DID 情報と、ソースデバイスのアンインストールキーを提供する必要があります。

5. ターゲットデバイスに新しいライセンスをインストールします。詳細については、「ライセンスのインストール」を参照してください。

アクティベーションファイルを回復する

アクティベーションファイルを誤って削除した場合は、次の手順に従ってアクティベーションファイルを回復します。

1. **copy**コマンドを使用して、バックアップアクティベーションファイルをディレクトリflash:/licenseにコピーします。
2. **display license**コマンドを使用して、回復されたアクティベーションファイルの状態が**in use**であることを確認します。
3. ライセンス状態が**In use**であるが、ライセンス機能が正しく機能しない場合は、デバイスをリブートします。

ライセンス管理の表示およびメンテナンスコマンド

任意のビューで表示コマンドを実行します。

タスク	コマンド
詳細なライセンス情報を表示します。	**display license** [**activation-file**] [**slot** *slot-number*]
SNおよびDID情報を表示します。	**display license device-id slot** slot-number
機能な機能ライセンス情報を表示します。	**display license feature**

オートマチックコンフィギュレーションの使用

オートマチックコンフィギュレーションについて

有効な次のスタートアップコンフィギュレーションファイルがない状態でデバイスが起動すると、デバイスはデフォルトのファイルシステムのルートディレクトリでautocfg.py、autocfg.tcl、およびautocfg.cfgファイルを検索します。ルートディレクトリに存在するファイルは1つだけです。ファイルが1つ存在する場合、デバイスはファイルをロードします。ファイルが1つも存在しない場合、デバイスはオートマチックコンフィギュレーション機能を使用して一連のコンフィギュレーション設定を取得します。

オートマチックコンフィギュレーション設定機能を使用すると、デバイスは起動時に一連の設定を自動的に取得できます。この機能により、ネットワークの設定とメンテナンスが簡単になります。

オートマチックコンフィギュレーションは、表15の実装方法を使用して実装できます。

表16 オートマチックコンフィギュレーションの実装方法

実施方法	コンフィギュレーションファイルの場所	アプリケーションのシナリオ
サーバーベースのオートマチックコンフィギュレーション	**ファイルサーバー**	**地理的に分散した多数のデバイスを設定する必要がある場合。**

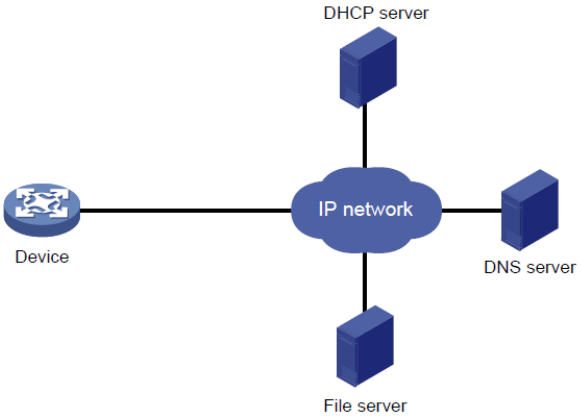
サーバーベースのオートマチックコンフィギュレーションの使用

サーバーベースのオートマチックコンフィギュレーションについて

図30に示すように、典型的なサーバーベースのオートマチックコンフィギュレーションネットワークは、次のサーバーで構成されています。

- DHCPサーバー。
- ファイルサーバー(TFTPまたはHTTPサーバー)。
- (必要に応じて)DNSサーバー。

図30 サーバーベースのオートマチックコンフィギュレーションネットワーク図



サーバーベースのオートマチックコンフィギュレーションタスクの概要

サーバーベースのオートマチックコンフィギュレーショを設定するには、次の作業を行います。

1. ファイルサーバーの設定
2. オートマチックコンフィギュレーション用にファイルを準備します。
   - コンフィギュレーションファイルの準備
   - スクリプトファイルの準備
3. DHCPサーバーの設定
4. (任意)DNSサーバーの設定
5. (必要に応じて)ゲートウェイの設定
6. オートマチックコンフィギュレーションに使用するインターフェイスの準備
7. オートマチックコンフィギュレーションの開始と完了

ファイルサーバーの設定

デバイスがTFTPサーバーから設定情報を取得するには、ファイルサーバーでTFTPサービスを開始します。

デバイスがHTTPサーバーから設定情報を取得するには、ファイルサーバー上でHTTPサービスを起動します。

コンフィギュレーションファイルの準備

コンフィギュレーションファイルタイプ

デバイスは、表17のタイプをサポートします。

表17 コンフィギュレーションファイルタイプ

コンフィギュレーションファイル形式	アプリケーションオブジェクト	ファイル名の要件	サポートされるファイルサーバータイプ
専用のコンフィギュレーションファイル	異なる設定が必要なデバイス	*File name**.cfg*** ファイル名を簡単に識別するにはスペースを含まないコンフィギュレーションファイル名。	• TFTPサーバー • HTTPサーバー
共通コンフィギュレーションファイル	すべてまたは一部の設定を共有するデバイス	*File name**.cfg***	• TFTPサーバー • HTTPサーバー
デフォルトコンフィギュレーションファイル	その他の装置。 このファイルには、デバイスが起動に使用する一般的な設定だけが含まれています。	**device.cfg**	• TFTPサーバー

コンフィギュレーションファイルの要件の特定と準備

1. コンフィギュレーションファイル用のデバイスの要件を確認します。
2. 異なる設定が必要なデバイスの場合は、それぞれのデバイス用コンフィギュレーションファイルを準備し、ファイルサーバーにファイルを保存します。
3. すべてまたは一部の設定を共有するデバイスの場合は、ファイルサーバー上の.cfgファイルに共通の設定を保存します。
4. TFTPファイルサーバーを使用する場合は、デバイスが起動に使用する共通設定をサーバー上の**device.cfg**ファイルに保存できます。このファイルは、デバイスに使用する他のコンフィギュレーションファイルがない場合にだけデバイスに割り当てられます。

TFTP サーバー上のホスト名ファイルの準備

TFTPサーバーが使用されていて、DHCPサーバーがコンフィギュレーションファイル名を割り当てていない場合は、TFTPサーバー上でホスト名ファイルを設定できます。ホスト名ファイルには、自動的に設定されるデバイスのホスト名とIPアドレスのマッピングが含まれます。

ホスト名ファイルを準備するには、次の手順に従います。

1. **network.cfg**という名前のホスト名ファイルを作成します。
2. **ip host** host-name ip-address形式の各マッピングエントリを別の行に追加します。次に例を示します。

   ip host host1 101.101.101.101

   ip host host2 101.101.101.102

   ip host client1 101.101.101.103

   ip host client2 101.101.101.104

重要:

デバイスのホスト名は、デバイスに設定されているコンフィギュレーションファイルの名前と同じである必要があります。

スクリプトファイルの準備

このタスクについて

スクリプトファイルは、ソフトウェアの自動アップグレードとオートマチックコンフィギュレーションに使用できます。

デバイスは、Pythonスクリプト(.pyファイル)およびTclスクリプト(.tclファイル)をサポートします。PythonおよびTclスクリプトの詳細については、「Pythonを使用する」および「Tclを使用する」を参照してください。

デバイスは、専用スクリプトファイルおよび共通専用スクリプトファイルをサポートしています。デフォルトのスクリプトファイルの使用はサポートしていません。専用スクリプトファイルおよび共通専用スクリプトファイルの詳細は、表17を参照してください。

スクリプトファイルを使用する場合、ホスト名ファイルを使用してデバイスのホスト名とIPアドレスのマッピングを提供することはできません。

制限とガイドライン

Tclスクリプトを使用するには、スクリプト内のすべてのコマンドがサポートされ、正しく設定されていることを確認します。コマンドにエラーが発生すると、オートマチックコンフィギュレーションプロセスが終了します。

手順

- すべてまたは一部の設定を共有するデバイスの場合は、共通の設定を含むスクリプトファイルを作成します。
- その他のデバイスの場合は、それぞれに対して個別のスクリプトファイルを作成します。

DHCP サーバーの設定

このタスクについて

DHCPサーバーは、自動的に設定する必要があるデバイスに次の項目を割り当てます。

- IPアドレス。
- コンフィギュレーションファイルまたはスクリプトファイルのパス。

制限とガイドライン

DHCPサーバーを設定する場合は、次の注意事項に従ってください。

- 異なるコンフィギュレーションファイルを準備したデバイスの場合、DHCPサーバー上のデバイスごとに次の作業を実行します。
  - DHCPアドレスプールを作成します。
  - スタティックアドレスバインディングを設定します。
  - コンフィギュレーションファイルまたはスクリプトファイルを指定します。

  アドレスプールは1つのコンフィギュレーションファイルだけを使用できるため、アドレスプールに指定できるスタティックアドレスバインディングは1つだけです。
- 同じコンフィギュレーションファイルを準備したデバイスの場合は、次のいずれかの方法を使用します。
  - 方法1:
    - デバイスのDHCPアドレスプールを作成します。
    - アドレスプール内の各デバイスにスタティックアドレスバインディングを設定します。

- デバイスのコンフィギュレーションファイルを指定します。
  - 方法2:
    - デバイスのDHCPアドレスプールを作成します。
    - ダイナミック割り当てのサブネットを指定します。
    - TFTPサーバーを指定します。
    - デバイスのコンフィギュレーションファイルを指定します。
- サブネット上のすべてのデバイスが同じコンフィギュレーションファイルまたはスクリプトファイルを共有している場合は、DHCPサーバーで次の作業を実行します。
  - ダイナミックアドレス割り当てを設定します。
  - デバイスのコンフィギュレーションファイルまたはスクリプトファイルを指定します。

  コンフィギュレーションファイルには、デバイスの共通設定のみを含めることができます。デバイス管理者がデバイスの起動後にコンフィギュレーションを変更できる方法を提供できます。

HTTP ファイルサーバー使用時の DHCP サーバーの設定

1. システムビューに入ります。

   system-view
2. DHCPを有効にする。

   dhcp enable

   デフォルトでは、DHCPは無効です。
3. DHCPアドレスプールを作成し、そのビューを開始します。

   dhcp server ip-pool *pool-name*
4. アドレスプールを設定します。

   必要に応じて、設定するオプションを選択します。
   - アドレスプールのプライマリサブネットを指定します。

     Network *network-address* [*mask-length* | **mask** *mask*]

     デフォルトでは、プライマリサブネットは指定されていません。
   - スタティックバインディングを設定します。

     static-bind ip-address *ip-address* [*mask-length* | **mask** *mask*] { **client-identifier** *client-identifier* | **hardware-address** *hardware-address* [**ethernet** | **token-ring**] }

     デフォルトでは、スタティックバインディングは設定されていません。

     複数のスタティックバインドを構成できます。ただし、1つのIPアドレスをバインドできるクライアントは1つだけです。DHCPクライアントのバインドを変更するには、バインドを削除してバインドを再構成する必要があります。
5. コンフィギュレーションファイルまたはスクリプトファイルのURLを指定します。

   bootfile-name *url*

   デフォルトでは、コンフィギュレーションファイルまたはスクリプトファイルのURLは指定されません。

TFTP ファイルサーバー使用時の DHCP サーバーの設定

1. システムビューに入ります。

   system-view
2. DHCPを有効にする。

   dhcp enable

デフォルトでは、DHCPは無効です。

3. DHCPアドレスプールを作成し、そのビューを開始します。

   dhcp server ip-pool *pool-name*

4. アドレスプールを設定します。

   必要に応じて、設定するオプションを選択します。

   - アドレスプールのプライマリサブネットを指定します。

     network *network-address* [*mask-length* | **mask** *mask*]

     デフォルトでは、プライマリサブネットは指定されていません。

   - スタティックバインディングを設定します。

     static-bind ip-address *ip-address* [*mask-length* | **mask** *mask*] { **client-identifier** *client-identifier* **| hardware-address** *hardware-address* [**ethernet** | **token-ring**] }

     デフォルトでは、スタティックバインディングは設定されていません。

     複数のスタティックバインドを構成できます。ただし、1つのIPアドレスをバインドできるクライアントは1つだけです。DHCPクライアントのバインドを変更するには、バインドを削除してバインドを再構成する必要があります。

5. TFTPサーバーを指定します。必要に応じて次のいずれかのオプションを選択します。

   - TFTPサーバーのIPアドレスを指定します。

     tftp-server ip-address *ip-address*

     デフォルトでは、TFTPサーバーのIPアドレスは指定されていません。

   - TFTPサーバーの名前を指定します。

     tftp-server domain-name *domain-name*

     デフォルトでは、TFTPサーバー名は指定されません。

     TFTPサーバーを名前で指定する場合は、ネットワーク上にDNSサーバーが必要です。

6. コンフィギュレーションファイルまたはスクリプトファイルの名前を指定します。

   bootfile-name *bootfile-name*

   デフォルトでは、コンフィギュレーションファイル名またはスクリプトファイル名は指定されません。

DNS サーバーの設定

DNSサーバーは、次の状況で必要です。

- TFTPサーバーにホスト名ファイルがありません。

  デバイスは、ホスト名を取得するためにIPアドレスをDNSサーバーに提供する必要があります。その後、デバイスは、ホスト名.cfg形式で指定されたコンフィギュレーションファイルをTFTPサーバーから取得できます。

- DHCPサーバーは、DHCP応答メッセージを通じてTFTPサーバードメイン名を割り当てます。デバイスは、TFTPサーバーのIPアドレスを取得するためにドメイン名を使用する必要があります。

ゲートウェイの設定

オートマチックコンフィギュレーションされるデバイスとオートマチックコンフィギュレーション用のサーバーが異なるネットワークセグメントに存在する場合は、次の作業を実行する必要があります。

- ゲートウェイを導入し、デバイスがサーバーと通信できることを確認します。
- ゲートウェイでDHCPリレーエージェント機能を設定します。
- ゲートウェイでUDPヘルパー機能を設定します。

  この作業は、デバイスがブロードキャストパケットを使用してTFTPサーバーに要求を送信する場合に必要です。次の状況では、デバイスはブロードキャストパケットを使用してTFTPサーバーに要求を送信します。

  - DHCP応答には、TFTPサーバーのIPアドレスまたはドメイン名が含まれていません。
  - TFTPサーバーのIPアドレスまたはドメイン名が無効です。

  UDPヘルパーは、ブロードキャストパケットをユニキャストパケットに変換し、そのユニキャストパケットをファイルサーバーに転送します。UDPヘルパーの詳細については、『Layer3IP Services Configuration Guide』を参照してください。

オートマチックコンフィギュレーションに使用するインターフェイスの準備

デバイスは次の手順を使用して、オートマチックコンフィギュレーションのインターフェイスを選択します。

1. レイヤー2の管理イーサネットインターフェイスのステータスを識別します。ステータスがアップの場合、デバイスは管理イーサネットインターフェイスを使用します。
2. レイヤー2イーサネットインターフェイスのステータスを識別します。1つまたは複数のレイヤー2イーサネットインターフェイスがアップ状態の場合、デバイスはデフォルトVLANのVLANインターフェイスを使用します。
3. すべてのレイヤー3イーサネットインターフェイスを、最初にインターフェイスタイプの辞書順で、次にインターフェイス番号の昇順で、そしてアップ状態でソートします。最初のインターフェイスタイプのインターフェイスの中でインターフェイス番号が最も小さいインターフェイスを使用します。
4. アップ状態のレイヤー3イーサネットインターフェイスがない場合、デバイスは30秒待機し、ステップ1に進んで再試行します。

高速な自動デバイス設定を行うには、各デバイスの管理イーサネットインターフェイスだけをネットワークに接続します。

オートマチックコンフィギュレーションの開始と完了

1. オートマチックコンフィギュレーションするデバイスの電源を入れます。

   ローカルで次のスタートアップコンフィギュレーションファイルが見つからない場合、デバイスはオートマチックコンフィギュレーションプロセスを開始してコンフィギュレーションファイルを取得します。

   - デバイスがコンフィギュレーションファイルを取得し、そのファイルを正常に実行すると、オートマチックコンフィギュレーションプロセスは終了します。
   - 1回の試行が失敗すると、デバイスは最大試行回数に達するまで再試行します。プロセスを停止するには、**Ctrl+C**または**Ctrl+D**を押します。

   デバイスがコンフィギュレーションファイルの取得に失敗すると、デバイスはコンフィギュレーションをロードせずに起動します。
2. 稼働中のコンフィギュレーションを保存します。

   save

   デバイスは取得したコンフィギュレーションファイルをローカルに保存しません。稼働中のコンフィ

ギュレーションを保存しない場合、デバイスはリブート後にオートマチックコンフィギュレーション機能を再度使用する必要があります。

save コマンドの詳細については、「基本コマンドリファレンス」を参照してください。

サーバーベースのオートマチックコンフィギュレーションの例

例:TFTP サーバーを使用したオートマチックコンフィギュレーション

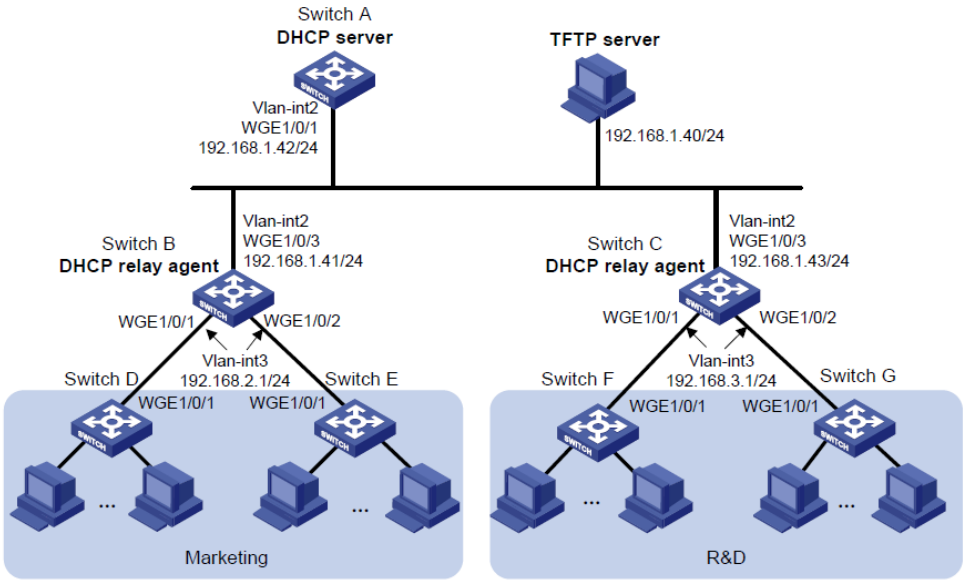
ネットワークの設定

図31に示すように、企業の2つの部門(スイッチBとスイッチC)がゲートウェイを介してネットワークに接続されています。アクセスデバイススイッチD、スイッチE、スイッチF、およびスイッチGにはコンフィギュレーションファイルがありません。

アクセスデバイスがコンフィギュレーションファイルを取得して次の設定作業を完了できるように、サーバーおよびゲートウェイを設定します。

- アクセスデバイスの管理者がそれぞれのアクセスデバイスにTelnet接続して管理できるようにします。
- 管理者は、ログイン時にそれぞれのユーザー名とパスワードを入力する必要があります。

図31 ネットワーク図



手順

1. DHCPサーバーのコンフィギュレーション:

   #VLANインターフェイスを作成し、そのインターフェイスにIPアドレスを割り当てます。

   <SwitchA> system-view

   [SwitchA] vlan 2

[SwitchA-vlan2] port twenty-fivegige 1/0/1

[SwitchA-vlan2] quit

[SwitchA] interface vlan-interface 2

[SwitchA-Vlan-interface2] ip address 192.168.1.42 24

[SwitchA-Vlan-interface2] quit

#DHCPを有効にします。

[SwitchA] dhcp enable

#VLAN N-interface 2 で DHCP サーバーを有効にします。

[SwitchA] interface vlan-interface 2

[SwitchA-Vlan-interface2] dhcp select server

[SwitchA-Vlan-interface2] quit

#192.168.2.0/24サブネット上のIPアドレスをマーケティング部のクライアントクライアントの
#TFTPサーバー、ゲートウェイ、およびコンフィギュレーションファイル名を指定します。

[SwitchA] dhcp server ip-pool market

[SwitchA-dhcp-pool-market] network 192.168.2.0 24

[SwitchA-dhcp-pool-market] tftp-server ip-address 192.168.1.40

[SwitchA-dhcp-pool-market] gateway-list 192.168.2.1

[SwitchA-dhcp-pool-market] bootfile-name market.cfg

[SwitchA-dhcp-pool-market] quit

#アドレスプールrdを構成して、192.168.3.0/24サブネット上のIPアドレスを研究開発部門クラ
#イアントのTFTPサーバー、ゲートウェイ、およびコンフィギュレーションファイル名を指定します。

[SwitchA] dhcp server ip-pool rd

[SwitchA-dhcp-pool-rd] network 192.168.3.0 24

[SwitchA-dhcp-pool-rd] tftp-server ip-address 192.168.1.40

[SwitchA-dhcp-pool-rd] gateway-list 192.168.3.1

[SwitchA-dhcp-pool-rd] bootfile-name rd.cfg

[SwitchA-dhcp-pool-rd] quit

#DHCP リレーエージェントへのスタティックルートを設定します

[SwitchA] ip route-static 192.168.2.0 24 192.168.1.41

[SwitchA] ip route-static 192.168.3.0 24 192.168.1.43

[SwitchA] quit

2. ゲートウェイスイッチBを設定します。

#VLANインターフェイスを作成し、インターフェイスにIPアドレスを割り当てます。

<SwitchB> system-view

[SwitchB] vlan 2

[SwitchB-vlan2] port twenty-fivegige 1/0/3

[SwitchB-vlan2] quit

[SwitchB] interface vlan-interface 2

[SwitchB-Vlan-interface2] ip address 192.168.1.41 24

[SwitchB-Vlan-interface2] quit

[SwitchB] vlan 3

[SwitchB-vlan3] port twenty-fivegige 1/0/1

[SwitchB-vlan3] port twenty-fivegige 1/0/2

[SwitchB-vlan3] quit

[SwitchB] interface vlan-interface 3

[SwitchB-Vlan-interface3] ip address 192.168.2.1 24

[SwitchB-Vlan-interface3] quit

#DHCPを有効にします。

[SwitchB] dhcp enable

#VLAN N-interface 3でDHCPリレーエージェントを有効にします。

[SwitchB] interface vlan-interface 3

[SwitchB-Vlan-interface3] dhcp select relay

#DHCP サーバーアドレスを指定します。

[SwitchB-Vlan-interface3] dhcp relay server-address 192.168.1.42

3. ゲートウェイスイッチCを設定します。

Create VLANインターフェイスを作成し、そのインターフェイスにIPアドレスを割り当てる。

<SwitchC> system-view

[SwitchC] vlan 2

[SwitchC-vlan2] port twenty-fivegige 1/0/3

[SwitchC-vlan2] quit

[SwitchC] interface vlan-interface 2

[SwitchC-Vlan-interface2] ip address 192.168.1.43 24

[SwitchC-Vlan-interface2] quit

[SwitchC] vlan 3

[SwitchC-vlan3] port twenty-fivegige 1/0/1

[SwitchC-vlan3] port twenty-fivegige 1/0/2

[SwitchC-vlan3] quit

[SwitchC] interface vlan-interface 3

[SwitchC-Vlan-interface3] ip address 192.168.3.1 24

[SwitchC-Vlan-interface3] quit

DHCPを有効にします

[SwitchC] dhcp enable

VLAN-interface 3でDHCPリレーエージェントを有効にします

[SwitchC] interface vlan-interface 3

[SwitchC-Vlan-interface3] dhcp select relay

DHCP サーバーアドレスを指定します

[SwitchC-Vlan-interface3] dhcp relay server-address 192.168.1.42

4. TFTPサーバーを設定します。

TFTPサーバー上に**market.cfg**というファイル名のコンフィギュレーションファイルを作成します。

#

sysname Market #

telnet server enable #

vlan 3#

local-user market password simple

market service-type telnet quit

```
#
interface Vlan-interface3 ip address
dhcp-alloc quit

#
interface twenty-fivegige 1/0/1 port access vlan
3
quit #

user-interface vty 0 63 authentication-
mode scheme user-role network-admin

#
return
```

#**TFTP**サービスソフトウェアを起動し、2つのコンフィギュレーションファイルが存在するフォルダを作業ディレクトリとして指定します(詳細は省略します)。

#TFTPサーバーとDHCPリレーエージェントが互いに通信できることを確認します(詳細は省略します)。

コンフィギュレーションの検証

1. スイッチD、スイッチE、スイッチF、およびスイッチGの電源を入れます。
2. アクセスデバイスの起動後、割り当てられたIPアドレスをスイッチAに表示します。

```
<SwitchA> display dhcp server ip-in-use
```

IP address	Client-identifier/ Hardware address	Lease expiration	Type
192.168.2.2	3030-3066-2e65-3233-642e-3561-6633-2d56-6c61-6e2d-696e-7465-7266-6163-6533	May 6 05:21:25 2013	Auto(C)
192.168.2.3	3030-3066-2e65-3230-302e-3232-3033-2d56-6c61-6e2d-696e-7465-7266-6163-6533	May 6 05:22:50 2013	Auto(C)
192.168.3.2	3030-6530-2e66-6330-302e-3335-3131-2d56-6c61-6e2d-696e-7465-7266-6163-6531	May 6 05:23:15 2013	Auto(C)
192.168.3.3	3030-6530-2e66-6330-302e-3335-3135-2d56-6c61-6e2d-696e-7465-7266-6163-6532	May 6 05:24:10 2013	Auto(C)

3. スイッチAから192.168.2.2にTelnetします。

   <SwitchA>telnet 192.168.2.2
4. プロンプトに従って、ユーザー名**market**とパスワード**market**を入力します(詳細は省略します)。スイッチDまたはスイッチEにログインしています。

例:HTTP サーバーおよび Tcl スクリプトを使用したオートマチックコンフィギュレーション

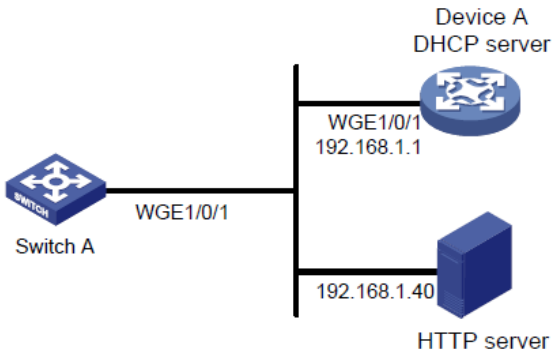
ネットワークの設定

図32に示すように、スイッチAにはコンフィギュレーションファイルがありません。

スイッチAがTclスクリプトを取得して次の設定作業を完了できるように、サーバーを設定します。

- 管理者がスイッチAにTelnet接続してスイッチAを管理できるようにします。
- 管理者は、ログイン時に正しいユーザー名とパスワードを入力する必要があります。

図32ネットワーク図



手順

1. DHCPサーバーを設定します。#DHCPを有効にします。

   <DeviceA> system-view
   [DeviceA] dhcp enable

   #192.168.1.0/24サブネット上のIPアドレスをクライアントに割り当てるように
   #アドレスプール1をコンフィギュレーションします。
   [DeviceA] dhcp server ip-pool 1
   [DeviceA-dhcp-pool-1] network 192.168.1.0 24
   #クライアントのスクリプトファイルのURLを指定します。
   [DeviceA-dhcp-pool-1]bootfile-name http://192.168.1.40/device.tcl

2. HTTPサーバーをコンフィギュレーションします。

   #HTTPサーバー上にdevice.tclという名前のコンフィギュレーションファイルを作成します。
   system-view
   telnet server enable
   local-user user password
   simple abcabc service-
   type telnet quit
   user-interface vty 0 63
   authentication-mode scheme
   user-role network-admin quit

   interface twenty-fivegige 1/0/1 port
   link-mode route

ip address dhcp-alloc

return

#HTTPサービスソフトウェアを起動し、HTTPサービスを有効にします(詳細は省略します)。

コンフィギュレーションの検証

1. スイッチAの電源を入れます。
2. スイッチAの起動後、デバイスAに割り当てられたIPアドレスを表示します。

<DeviceA> display dhcp server ip-in-use

IP address	Client identifier/ Type Hardware address	Lease	expiration
192.168.1.2	0030-3030-632e-3239-3035-2e36-3736-622d-4574-6830-2f30-2f32	Dec 12 17:41:15 2013	Auto(C)

3. デバイスAから192.168.1.2にTelnet接続します。

<DeviceA>telnet 192.168.1.2

4. プロンプトに従って、ユーザー名**user**とパスワード**abcabc**を入力します(詳細は省略します)。スイッチAにログインしています。

例:HTTP サーバーと Python スクリプトを使用したオートマチックコンフィギュレーション

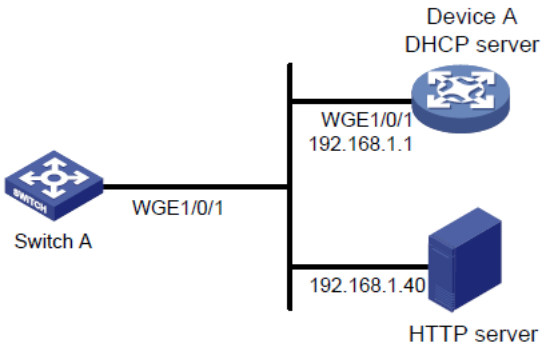
ネットワークの設定

図33に示すように、スイッチAにはコンフィギュレーションファイルがありません。

スイッチAがPythonスクリプトを取得して次の設定作業を完了できるように、サーバーを設定します。

- 管理者がスイッチAにTelnet接続してスイッチAを管理できるようにします。
- 管理者は、ログイン時に正しいユーザー名とパスワードを入力する必要があります。

図33ネットワーク図



手順

1. DHCPサーバーを設定します。

#DHCPを有効にします。

<DeviceA> system-view

[DeviceA] dhcp enable

#192.168.1.0/24サブネット上のIPアドレスをクライアントに割り当てるのIPアドレスをクライ

#アントに割り当てます。

[DeviceA] dhcp server ip-pool 1

[DeviceA-dhcp-pool-1] network 192.168.1.0 24

#クライアントのスクリプトファイルのURLを指定します。

[DeviceA-dhcp-pool-1] bootfile-name http://192.168.1.40/device.py

2. HTTPサーバーをコンフィギュレーションします。

   #HTTPサーバー上にdevice.pyという名前のコンフィギュレーションファイルを作成します。

   #!usr/bin/python

   import comware

   comware.CLI('system-view ;telnet server enable ;local-user user ;password simple abcabc ;service-type telnet ;quit ;user-interface vty 0 63 ;authentication-mode scheme ;user-role network-admin ;quit ;interface twenty-fivegige 1/0/1 ;port link-mode route ;ip address dhcp-alloc ;return')

   #HTTPサービスソフトウェアを起動し、HTTPサービスを有効にします(詳細は省略します)。

コンフィギュレーションの検証

1. スイッチAの電源を入れます。
2. スイッチAの起動後、デバイスAに割り当てられたIPアドレスを表示します。

<DeviceA> display dhcp server ip-in-use

IP address	Client identifier/ Type Hardware address	Lease	expiration
192.168.1.2	0030-3030-632e-3239-3035-2e36-3736-622d-4574-6830-2f30-2f32	Dec 12 17:41:15 2013	Auto(C)

3. デバイスAから192.168.1.2にTelnet接続します。

   <DeviceA>telnet 192.168.1.2

4. プロンプトに従って、ユーザー名userとパスワード**abcabc**を入力します(詳細は省略します)。スイッチAにログインしています。

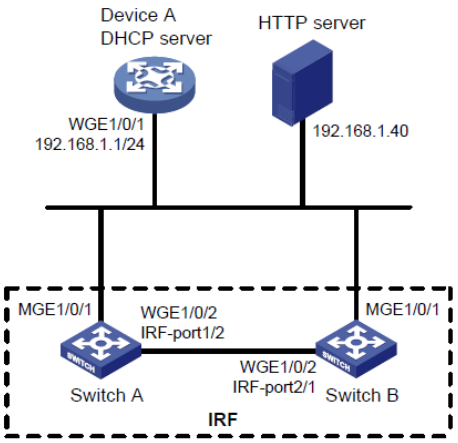
例:IRF ファブリックの設定

ネットワークの設定

図34に示すように、スイッチAとスイッチBにはコンフィギュレーションファイルがありません。

スイッチがPythonスクリプトを取得してそれぞれの設定を完了し、IRFファブリックを形成できるようにサーバーを設定します。

図34ネットワーク図



手順

1. インターフェイスにIPアドレスを割り当てます。デバイスが相互に到達できることを確認します(詳細は省略します)。
2. HTTPサーバーで次のファイルを設定します。

ファイル	内容	注意
.Cfg コンフィギュレーションファイル	IRFセットアップに必要なコマンド。	既存のIRFファブリックのコンフィギュレーションファイルをコピーおよび変更することで、コンフィギュレーションファイルを作成できます。
sn.txt	メンバースイッチのシリアル番号。	各SNはスイッチを一意に識別します。 これらのSNは、各メンバースイッチに一意のIRFメンバーIDを割り当てるために使用されます。
(オプション).ipeまたは.binソフトウェアイメージファイル	ソフトウェアイメージ。	メンバースイッチが異なるソフトウェアバージョンを実行している場合は、ソフトウェアアップグレードに使用するソフトウェアイメージファイルを準備する必要があります。
	次のタスクを実行するPythonコマンド: a (任意)フラッシュメモリーにファイルをダウンロードするための十分なスペースがあることを確認します。	

.py Pythonスクリプトファイル	**b** コンフィギュレーションファイル**sn.txt**をダウンロードします。 **c** (任意)ソフトウェアイメージファイルをダウンロードし、メインスタートアップイメージファイルとして指定します。 **d** **sn.txt**を解決し、各SNに一意のIRFメンバーIDを割り当てます。 **e** コンフィギュレーションファイルをメインの次のスタートアップコンフィギュレーションファイルとして指定します。 **f** メンバースイッチをRebootします。	Pythonスクリプトの設定の詳細については、「Pythonを使用する」を参照してください。

3. デバイスAをDHCPサーバーとして設定します。#DHCPを有効にします。

<DeviceA> system-view

[DeviceA] dhcp enable

#192.168.1.0/24サブネット上のIPアドレスをクライアントに割り当てるのIPアドレスを
#クライアントに割り当てます。

[DeviceA] dhcp server ip-pool 1

[DeviceA-dhcp-pool-1] network 192.168.1.0 24

#クライアントのスクリプトファイルのURLを指定します。

[DeviceA-dhcp-pool-1] bootfile-name http://192.168.1.40/device.py

[DeviceA-dhcp-pool-1] quit

#Twenty-FiveGigE1/0/1でDHCPサーバーを有効にします。

[DeviceA] interface twenty-fivegige 1/0/1

[DeviceA-Twenty-FiveGigE1/0/1] dhcp select server

[DeviceA-Twenty-FiveGigE1/0/1] quit

4. スイッチAとスイッチBの電源を入れます。

スイッチAとスイッチBは、DHCPサーバーからPythonスクリプトファイルを取得し、スクリプトを実行します。IRF設定が完了すると、スイッチAとスイッチBがリブートします。

5. スイッチAとスイッチBがリブートしたら、ケーブルを使用して、IRF物理ポート経由でスイッチAとスイッチBを接続します。

スイッチAとスイッチBはマスターメンバーを選択します。下位メンバーはリブートしてIRFファブリックに加入します。

コンフィギュレーションの検証

#スイッチAで、IRFメンバーデバイスを表示します。スイッチBでdisplay irfコマンドを使用して、

#IRFメンバーデバイスを表示することもできます。

<Switch A> display irf

MemberID	Slot	Role	Priority	CPU-Mac	Description
1	1	Standby	1	00e0-fc0f-8c02	---
*+2	1	Master	30	00e0-fc0f-8c14	---

---

* indicates the device is the master.

+ indicates the device through which the user logs in.

The Bridge MAC of the IRF is: 000c-1000-1111 Auto
upgrade : yes
Mac persistent : always
Domain ID : 0
Auto merge : yes

出力は、スイッチがIRFファブリックを形成したことを示しています。