t - z

tail-logs

Cisco Technical Assistance Center（TAC）とともにトラブルシューティングを行う際に、システムログを開いてメッセージを書き込まれたとおりに表示するには、**tail-logs** コマンドを使用します。

tail-logs

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

tail-logs コマンドは、システムログを開き、メッセージを書き込まれたとおりに表示できるようにします。Cisco Technical Assistance Center（TAC）への問い合わせ時にこのコマンドを使用すると、出力を解釈して、適切なログを表示できるようになります。

このコマンドは、使用可能なすべてのログを表示するメニューを提示します。コマンドプロンプトに従ってログを選択します。ログが長い場合は多くの行が表示されます。Enter キーを押すと 1 行ずつ進み、スペースを押すと 1 ページずつ進みます。ログの表示を終了した後にコマンドプロンプトに戻るには、Ctrl+C を押します。

例

次の例は、ngfw.log ファイルがどのように列挙されるかを示しています。ファイル リストは、最上位のディレクトリで始まり、その後、現在のディレクトリ内のファイル リストが続きます。

```
> tail-logs
===Tail Logs===
============================
Directory: /ngfw/var/log
----------sub-dirs----------
cisco
mojo
removed_packages
setup
connector
sf
scripts
packages
removed_scripts
httpd
-----------files------------
2016-10-14 18:12:04.514783 | 5371       | SMART_STATUS_sda.log
2016-10-14 18:12:04.524783 | 353        | SMART_STATUS_sdb.log
2016-10-11 21:32:23.848733 | 326517     | action_queue.log
2016-10-06 16:00:56.620019 | 1018       | br1.down.log

<list abbreviated>

2016-10-06 15:38:22.630001 | 9194       | ngfw.log
```

```
<list abbreviated>

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s

Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> ngfw.log
2016-10-06 15:38:22 Running [rm -rf /etc/logrotate-dmesg.conf /etc/logrotate.conf
/etc/logrotate.d
/etc/logrotate_ssp.conf /etc/logrotate_ssp.d] ... success
2016-10-06 15:38:22 Running [ln -sf /ngfw/etc/logrotate-size.conf /etc/] ... success
2016-10-06 15:38:22 Running [ln -sf /ngfw/etc/logrotate-size.d /etc/] ... success
2016-10-06 15:38:22 Running [ln -sf /ngfw/etc/logrotate.conf /etc/] ... success
2016-10-06 15:38:22 Running [ln -sf /ngfw/etc/logrotate.d /etc/] ... success
2016-10-06 15:38:22 Running [rm -f /usr/sbin/ntpd] ... success
```

関連コマンド

Command	説明
system support view-files	ログファイルを開きます。

test aaa-server

デバイスが特定のAAAサーバーでユーザーを認証または認可できるかどうかを確認するには、**test aaa-server** コマンドを使用します。

test aaa-server {**authentication** *groupname* [**host** *ip_address*] [**username** *username*] [**password** *password*] | **authorization** *groupname* [**host** *ip_address*] [**username** *username*}

構文の説明

groupname	AAA サーバーグループまたはレルム名を指定します。
host *ip-address*	サーバーの IP アドレスを指定します。コマンドで IP アドレスを指定しないと、入力を求めるプロンプトが表示されます。
password *password*	ユーザー パスワードを指定します。コマンドでパスワードを指定しないと、入力を求めるプロンプトが表示されます。
username *username*	AAA サーバーの設定をテストするために使用するアカウントのユーザー名を指定します。ユーザー名が AAA サーバーに存在することを確認してください。存在しないと、テストは失敗します。コマンドでユーザー名を指定しないと、入力を求めるプロンプトが表示されます。

コマンド履歴

リリース	変更内容
6.2.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、システムが特定の AAA サーバーを使用してユーザーを認証または認可できることを検証できます。このコマンドを使用すると、実際のユーザーによる認証試行なしでAAAサーバーをテストできます。また、AAA障害の原因が、AAAサーバーパラメータの設定ミス、AAA サーバーへの接続問題、またはその他のコンフィギュレーション エラーのいずれによるものかを特定するうえで役立ちます。

例

次に、成功した認証の例を示します。

```
> test aaa-server authentication svrgrp1 host 192.168.3.4 username bogus password
mypassword
INFO: Attempting Authentication test to IP address <10.77.152.85> (timeout: 12 seconds)
INFO: Authentication Successful
```

次に、失敗した認証試行を示します。

```
> test aaa-server authentication svrgrp1
Server IP Address or name: 192.168.3.4
Username: bogus
Password: mypassword
```

```
INFO: Attempting Authentication test to IP address <192.168.3.4> (timeout: 10
          seconds)
ERROR: Authentication Rejected: Unspecified
```

関連コマンド

コマンド	説明
aaa-server active **aaa-server fail**	障害とマークされた AAA サーバーを再アクティブ化するか、アクティブな AAA サーバーを障害とマークします。
clear aaa-server statistics	AAA サーバー統計情報をクリアします。
show aaa-server	AAA サーバーの統計情報を表示します。

traceroute

パケットがデータインターフェイスを通って宛先に到達するまでのルートを特定するには、**traceroute** コマンドを使用します。パケットが管理 IP アドレスを経由して宛先に到達するまでのルートを特定するには、**traceroute system** コマンドを使用します。

traceroute *destination* [**source** {*source_ip* | *source-interface*}] [**numeric**] [**timeout** *timeout_value*] [**probe** *probe_num*] [**ttl** *min_ttl max_ttl*] [**port** *port_value*] [**use-icmp**]
traceroute system *destination*

構文の説明

destination	ルートをトレースする先のホストの IPv4 または IPv6 アドレス、またはホスト名。たとえば、10.100.10.10 または www.example.com などです。ホスト名を解決するには、DNS サーバーを設定する必要があります。 **system** キーワードを使用するトレースは、管理インターフェイス用に設定された DNS サーバーを使用します。その他のトレースでは、データインターフェイス用に設定された DNS サーバーを使用します。データインターフェイスに DNS が定義されていない場合は、まず **nslookup** コマンドを使用してホストの IP アドレスを決定し、次に FQDN の代わりにその IP アドレスを使用します。
numeric	出力に中間ゲートウェイの IP アドレスのみが示されるように指定します。このキーワードを指定しない場合は、トレース中に到達したゲートウェイのホスト名の検索を試みます。
port *port_value*	ユーザー データグラム プロトコル（UDP）プローブ メッセージによって使用される宛先ポート。デフォルトは 33434 です。
probe *probe_num*	TTL の各レベルで送信するプローブの数。デフォルト数は 3 です。
source {*source_ip* | *source_interface*}	トレースパケットの送信元として使用される IP アドレスまたはインターフェイスを指定します。この IP アドレスはいずれかのデータインターフェイスの IP アドレスにする必要があります。トランスペアレントモードの場合は、管理 IP アドレスにする必要があります。インターフェイス名を指定すると、インターフェイスの IP アドレスが使用されます。
system	traceroute がデータインターフェイスではなく管理インターフェイスを経由する必要があることを示します。
timeout *timeout_value*	接続をタイムアウトにする前に応答を待機する時間を指定します。デフォルトは 3 秒です。

ttl *min_ttl max_ttl*	プローブで使用する存続可能時間の値の範囲を指定します。 • *min_ttl*：最初のプローブの TTL 値。デフォルトは 1 ですが、既知のホップの表示を抑制するためにより大きい値を設定できます。 • *max-ttl*：使用可能な最大 TTL 値。デフォルトは 30 です。traceroute パケットが宛先に到達するか、値に達したときにコマンドは終了します。
use-icmp	UDP プローブ パケットの代わりに ICMP プローブ パケットを使用するように指定します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

traceroute コマンドは送信した各プローブの結果を示します。出力の各行が 1 つの TTL 値に対応します（昇順）。次に、**traceroute** コマンドによって表示される出力記号を示します。

出力記号	説明
*	タイムアウトの期間内にプローブへの応答を受信しませんでした。
nn msec	各ノードで、指定した数のプローブのラウンドトリップにかかる時間（ミリ秒）。
!N.	ICMP ネットワークに到達できません。
!H	ICMP ホストに到達できません。
!P	ICMP プロトコルに到達できません。
!A	ICMP が管理者によって禁止されています。
?	原因不明の ICMP エラーが発生しました。

例

次に、宛先 IP アドレスを指定した場合の traceroute 出力の例を示します。

```
> traceroute 209.165.200.225
Tracing the route to 209.165.200.225
 1  10.83.194.1 0 msec 10 msec 0 msec
 2  10.83.193.65 0 msec 0 msec 0 msec
 3  10.88.193.101 0 msec 10 msec 0 msec
 4  10.88.193.97 0 msec 0 msec 10 msec
 5  10.88.239.9 0 msec 10 msec 0 msec
 6  10.88.238.65 10 msec 10 msec 0 msec
 7 172.16.7.221 70 msec 70 msec 80 msec
```

```
 8 209.165.200.225 70 msec 70 msec 70 msec
```

次の例は、管理インターフェイスを介したホスト名に対する traceroute を示しています。

```
> traceroute system www.example.com
traceroute to www.example.com (172.163.4.161), 30 hops max, 60 byte packets
 1  192.168.0.254 (192.168.0.254)  0.213 ms  0.310 ms  0.328 ms
 2  10.88.127.1 (10.88.127.1)  0.677 ms  0.739 ms  0.899 ms
 3  lab-gw1.example.com (10.89.128.25)  0.638 ms  0.856 ms  0.864 ms
 4  04-bb-gw1.example.com (10.152.240.65)  1.169 ms  1.355 ms  1.409 ms
 5  wan-gw1.example.com (10.152.240.33)  0.712 ms  0.722 ms  0.790 ms
 6  wag-gw1.example.com (10.152.240.73)  13.868 ms  10.760 ms  11.187 ms
 7  rbb-gw2.example.com (172.30.4.85)  7.202 ms  7.301 ms  7.101 ms
 8  rbb-gw1.example.com (172.30.4.77)  8.162 ms  8.225 ms  8.373 ms
 9  sbb-gw1.example.com (172.16.16.210)  7.396 ms  7.548 ms  7.653 ms
10  corp-gw2.example.com (172.16.16.58)  7.413 ms  7.310 ms  7.431 ms
11  dmzbb-gw2.example.com (172.16.0.78)  7.835 ms  7.705 ms  7.702 ms
12  dmzdcc-gw2.example.com (172.16.0.190)  8.126 ms  8.193 ms  11.559 ms
13  dcz05n-gw1.example.com (172.16.2.106)  11.729 ms  11.728 ms  11.939 ms
14  www1.example.com (172.16.4.161)  11.645 ms  7.958 ms  7.936 ms
```

関連コマンド

Command	説明
capture	トレース パケットを含めて、パケット情報をキャプチャします。
show capture	オプションが指定されていない場合は、キャプチャ コンフィギュレーションを表示します。
packet-tracer	パケット トレース機能をイネーブルにします。

undebug

特定の機能に対するデバッグを無効にするには、**undebug** コマンドを使用します。このコマンドは **no debug** コマンドの同意語です。

undebug {*feature* [*subfeature*] [*level*] | **all**}

構文の説明

all	すべての機能のデバッグを無効にします。
feature	デバッグを無効にする機能を指定します。使用可能な機能を表示するには、**undebug ?** コマンドを使用して CLI ヘルプを表示します。
subfeature	（オプション）機能によっては、1 つ以上のサブ機能のデバッグメッセージを無効にできます。使用可能なサブ機能を表示するには ? を使用します。
level	（オプション）デバッグ レベルを指定します。このレベルは、一部の機能で使用できない場合があります。使用可能なレベルを表示するには ? を使用します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時か、または Cisco Technical Assistance Center（TAC）とのトラブルシューティング セッション時に限定してください。さらに、**debug**コマンドは、ネットワークトラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が低くなります。

デバッグ出力は、CLIセッションでのみ表示できます。出力は、コンソールポートに接続したときか、または診断 CLI（**system support diagnostic-cli** と入力）で直接入手できます。また、**show console-output** コマンドを使用して、通常の 脅威に対する防御 CLI からの出力を確認することもできます。

例

次の例では、有効になっているすべてのデバッグのデバッグを無効にします。

```
> undebug all
>
```

関連コマンド

Command	説明
debug	特定の機能に対するデバッグを有効にします。
show debug	現在アクティブなデバッグ設定を示します。

upgrade

システム ソフトウェア アップグレードを再試行したり、キャンセルしたり、または元に戻したりするには、**upgrade** コマンドを使用します。

upgrade { **cancel** | **cleanup-revert** | **revert** | **retry** }

構文の説明

cancel	メジャーアップグレードのインストールをキャンセルします。アップグレードに失敗したものの、アップグレードがまだ進行中であるとシステムが判断している場合は、そのジョブをキャンセルして、アップグレードを再試行できるジョブステータスに変更する必要があります。ほとんどの場合、システムは失敗したアップグレードを自動的にキャンセルできます。
cleanup-revert	以前のバージョンを完全に削除して、ディスク領域を解放します。復元可能なバージョンをクリーンアップした場合、そのバージョンに戻すために **revert** キーワードを使用することはできません。
revert	復元可能なバージョンが使用可能な場合は、以前のバージョンに戻してシステムソフトウェアのアップグレードを取り消します。まず**show upgrade revert-info** コマンドを使用して、復元可能なバージョンが存在するかどうか、それはどのバージョンかを確認します。復元可能なバージョンを許容できる場合は、このコマンドを使用してそのバージョンに戻すことができます。 高可用性/拡張性の展開では、すべてのユニットを同時に元に戻すと、元に戻す操作が成功する可能性が高くなります。CLI を使用して復元する場合は、すべてのユニットでセッションを開き、それぞれで復元が可能であることを確認してから、プロセスを同時に開始します。 の復元後、デバイスを Smart Software Manager に再登録する必要があります。 バージョン 6.7 ～ 7.1 では、**upgrade revert** はローカル管理システムでのみ使用できます。Management Center によって管理されるシステムでは、このコマンドを使用できません。バージョン 7.2+ では、管理センターとデバイス間の通信が中断された場合、このコマンドは Management Center の展開でサポートされます。 **注意** CLI から復元すると、アップグレード後に行った変更によっては、デバイスと Management Center 間で設定が同期されないことがあります。これにより、後に通信と展開の問題が発生する可能性があります。

retry	失敗したメジャーアップグレードを再試行します。再試行するアップグレードは、システムによって失敗したと見なされ、進行中ではないものでなければなりません。アップグレードを再試行する前に**upgrade cancel** を入力しなければならない場合があります。

コマンド履歴

リリース	変更内容
6.7	このコマンドが導入されました。
7.0	**upgrade revert** コマンドにより、Smart Software Manager からデバイスが自動的に登録解除されるようになりました。アップグレードを元に戻した後、デバイスを再登録する必要があります。
7.2	管理センターとデバイス間の通信が中断された場合、**upgrade revert** コマンドは Management Center の展開でサポートされるようになりました。

例

次に、進行中のシステムソフトウェア更新をキャンセルする例を示します。アップグレードのキャンセルが正常に完了すると、デバイスが自動的に再起動されます。

```
> upgrade cancel
Warning: Upgrade in progress (11%,  8 mins remaining).
Are you sure you want to cancel it(yes/no)? yes
```

次の例は、失敗したアップグレードを再試行する方法を示しています。失敗メッセージで示されているように、アップグレード失敗の原因となった問題を最初に修正する必要があります。アップグレードを再試行する前に **upgrade cancel** を使用しなければならない場合があります。すべての失敗したアップグレードを再試行できるわけではありません。

```
> upgrade retry
Tue Dec  3 23:50:31 UTC 2020: Resuming upgrade for
Cisco_FTD_Upgrade-6.7.0-32.sh.REL.tar
```

次の例は、ローカル管理システムで以前のバージョンに戻す方法を示しています。復元できるバージョンがあるかどうかを確認するには、**show upgrade revert-info** コマンドを使用します。

```
> upgrade revert
Current version is 6.7.0.50
Detected previous version 6.6.1.20
Are you sure you want to revert (Yes/No)? Yes
```

次の例は、以前のバージョンを削除してディスク領域をクリアする方法を示しています。このコマンドを使用すると、以前のバージョンに戻すことができなくなります。

```
> upgrade cleanup-revert
Version 6.6 was cleaned up successfully.
```

関連コマンド

Command	説明
show last-upgrade status	最後のシステム ソフトウェア アップグレードに関する情報を表示します。
show upgrade	現在のシステム ソフトウェア アップグレードに関する情報を表示します。

verify

ファイルのチェックサムを確認するには、**verify** コマンドを使用します。

verify ［**sha-512** | **/signature**］ *path*
verify/md5 *path* ［*md5-value*］

構文の説明

/md5	（オプション）指定したソフトウェア イメージの MD5 値を計算して表示します。この値を、Cisco.com で入手できるこのイメージの値と比較します。
sha-512	（オプション）指定したソフトウェアイメージの SHA-512 値を計算して表示します。この値を、Cisco.com で入手できるこのイメージの値と比較します。
/signature	（オプション）フラッシュに保存されているイメージの署名を確認します。
md5-value	（オプション）指定したイメージの既知の MD5 値。コマンドで MD5 値を指定すると、指定したイメージの MD5 値が計算され、MD5 値が一致するかどうかを示すメッセージが表示されます。

path	• *filename* 現在のディレクトリ内のファイルの名前。ディレクトリの内容を表示する場合は **dir**、ディレクトリを変更する場合は **cd** を使用します。 • **disk0:**/[*path*/]*filename* このオプションは、内部フラッシュメモリを示します。**disk0** の代わりに **flash:** を使用することもできます。これらはエイリアスになります。 • **disk1:**/[*path*/]*filename* このオプションは、外部フラッシュメモリカードを示します。 • **flash:**/[*path*/]*filename* このオプションは、内部フラッシュ カードを示します。ASA 5500 シリーズの場合、**flash** は **disk0:** のエイリアスです。 • **ftp:**//[*user*[**:***password*]**@**]*server*[: *port*]/[*path*/]*filename*[**;type=***xx*] 次のキーワードの 1 つを **type** として指定できます。 • **ap**：ASCII 受動モード • **an**：ASCII 通常モード • **ip**：（デフォルト）バイナリ受動モード • **in**：バイナリ通常モード • **http**[**s**]**:**//[*user*[:*password*] **@**]*server*[: *port*]/[*path*/]*filename* • **tftp:**//[*user*[:*password*]@]*server*[: *port*]/[*path*/]*filename*[**;int=***interface_name*] サーバーアドレスへのルートを上書きする場合は、インターフェイス名を指定します。パス名にスペースを含めることはできません。

コマンド デフォルト

現在のフラッシュ デバイスがデフォルトのファイル システムです。

（注） **/md5** オプションを指定する場合、ftp、http、tftp などのネットワークファイルをソースとして使用できます。**/md5** オプションを指定せずに **verify** コマンドを使用した場合は、フラッシュのローカルイメージのみを確認できます。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

ファイルを使用する前にそのチェックサムを確認するには、**verify** コマンドを使用します。

ディスクで配布される各ソフトウェアイメージでは、イメージ全体に対して1つのチェックサムが使用されます。このチェックサムは、イメージをフラッシュ メモリにコピーする場合にのみ表示され、イメージファイルをあるディスクから別のディスクにコピーする場合は表示されません。

新しいイメージをロードまたは複製する前に、そのイメージのチェックサムと MD5 情報を記録しておき、イメージをフラッシュ メモリまたはサーバーにコピーするときにチェックサムを確認できるようにします。Cisco.com では、さまざまなイメージ情報を入手できます。

フラッシュメモリの内容を表示するには、**show flash:** コマンドを使用します。フラッシュ メモリの内容のリストには、個々のファイルのチェックサムは含まれません。イメージをフラッシュメモリにコピーした後で、そのイメージのチェックサムを再計算して確認するには、**verify** コマンドを使用します。ただし、**verify** コマンドは、ファイルがファイルシステムに保存された後にのみ、整合性チェックを実行します。破損しているイメージがデバイスに転送され、検出されずにファイルシステムに保存される場合があります。破損しているイメージが正常にデバイスに転送されると、ソフトウェアはイメージが壊れていることを把握できず、ファイルの確認が正常に完了します。

メッセージダイジェスト 5（MD5）ハッシュアルゴリズムを使用してファイルを検証するには、**/md5** オプションを指定して **verify** コマンドを使用します。MD5（RFC 1321 で規定）は、一意の 128 ビットのメッセージダイジェストを作成することによってデータの整合性を確認するアルゴリズムです。**verify** コマンドの **/md5** オプションを使用すると、セキュリティアプライアンスのソフトウェアイメージの MD5 チェックサム値を、その既知の MD5 チェックサム値と比較することによって、イメージの整合性を確認できます。すべてのセキュリティアプライアンスのソフトウェアイメージの MD5 値は、ローカル システムのイメージの値と比較するために、Cisco.com から入手できるようになっています。

MD5 整合性チェックを実行するには、**/md5** キーワードを指定して **verify** コマンドを発行します。たとえば、**verify /md5 flash:cdisk.bin** コマンドを発行すると、ソフトウェアイメージの MD5 値が計算されて表示されます。この値を、Cisco.com で入手できるこのイメージの値と比較します。

または、まず Cisco.com から MD5 値を取得し、その値をコマンド構文で指定できます。たとえば、**verify /md5 flash:cdisk.bin 8b5f3062c4cacdbae72571440e962233** コマンドを発行すると、MD5 値が一致するかどうかを示すメッセージが表示されます。MD5 値が一致しない場合は、いずれかのイメージが破損しているか、または入力した MD5 値が正しくありません。

例

次の例では、イメージファイルを確認します。**/signature** キーワードを含めた場合と同じ結果が表示されます。

```
> verify os.img
Verifying file integrity of disk0:/os.img
Computed Hash   SHA2: 4916c9b70ad368feb02a0597fbef798e
                      ca360037fc0bb596c78e7ef916c6c398
                      e238e2597eab213d5c48161df3e6f4a7
                      66e4ec15a7b327ee26963b2fd6e2b347
```

```
Embedded Hash   SHA2: 4916c9b70ad368feb02a0597fbef798e
                      ca360037fc0bb596c78e7ef916c6c398
                      e238e2597eab213d5c48161df3e6f4a7
                      66e4ec15a7b327ee26963b2fd6e2b347
Digital signature successfully validated
```

次の例では、イメージのMD5値を計算します。簡潔にするため、ほとんどの感嘆符は削除されています。

```
> verify /md5 os.img
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!Done!
verify /MD5 (disk0:/os.img) = 0940c6c71d3d43b3ba495f7290f4f276
>
```

次の例では、MD5値を計算して期待値と比較します。この例での結果は検証済みで、計算値と期待値は一致します。

```
> verify /md5 os.img 0940c6c71d3d43b3ba495f7290f4f276
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!Done!
Verified (disk0:/os.img) = 0940c6c71d3d43b3ba495f7290f4f276
>
```

次の例では、イメージの SHA-512 値を計算します。

```
> verify /sha-512 os.img
!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done!
verify /SHA-512 (disk0:/os.img) = 77421c0f6498976fbe5300e62bd8b7e8140b52a851f055265080
a392299848a77227d6047827192f34d969d36944abf2bddd215ec4127f9503173f82a2d6c7e2
```

関連コマンド

Command	説明
copy	ファイルをコピーします。
dir	システム内のファイルを一覧表示します。

vpn-sessiondb logoff

すべてまたは選択した VPN セッションをログオフするには、**vpn-sessiondb logoff** コマンドを使用します。

vpn-sessiondb logoff {**all** | **index** *index_number* | **ipaddress** *IPaddr* | **l2l** | **name** *username* | **protocol** *protocol-name* | **tunnel-group** *groupname* } **noconfirm**

構文の説明

all	すべての VPN セッションをログオフします。
index *index_number*	インデックス番号で 1 つのセッションをログオフします。**show vpn-sessiondb detail** コマンドを使用して、各セッションのインデックス番号を表示できます。
ipaddress *IPaddr*	指定した IP アドレスに対応するセッションをログオフします。
l2l	すべての LAN-to-LAN セッションをログオフします。
name *username*	指定したユーザー名のセッションをログオフします。
protocol *protocol-name*	指定したプロトコルのセッションをログオフします。プロトコルは次のとおりです。 • **ikev1**：インターネット キー エクスチェンジ バージョン 1（IKEv1）セッション。 • **ikev2**：インターネット キー エクスチェンジ バージョン 2（IKEv2）セッション。 • **ipsec** ：IKEv1 または IKEv2 を使用する IPsec セッション。 • **ipseclan2lan**：IPsec LAN-to-LAN セッション。 • **ipseclan2lanovernatt**：IPsec LAN-to-LAN over NAT-T セッション。
tunnel-group *groupname*	指定したトンネル グループ（接続プロファイル）のセッションをログオフします。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、企業トンネルグループ（接続プロファイル）のセッションをログオフする例を示します。

```
> vpn-sessiondb logoff tunnel-group Corporate noconfirm
INFO: Number of sessions from TunnelGroup "Corporate" logged off : 1
```

write net

TFTP サーバーに実行コンフィギュレーションを保存するには、**write net** コマンドを使用します。

write net ［**interface** *if_name*］ *server***:**［*filename*］

構文の説明

:*filename*	パスとファイル名を指定します。
interface *if_name*	TFTP サーバーに到達するために使用するインターフェイスの名前です。
サーバー**:**	TFTP サーバーの IP アドレスまたは名前を設定します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

実行コンフィギュレーションとは、メモリ内にある現在実行中のコンフィギュレーションです。

例

次に、内部インターフェイスを介して実行コンフィギュレーションを TFTP サーバーにコピーする例を示します。

```
> write net interface inside 10.1.1.1:/configs/contextbackup.cfg
```

関連コマンド

Command	説明
show running-config	実行コンフィギュレーションを表示します。

write terminal

端末上の実行コンフィギュレーションを表示するには、**write terminal** コマンドを使用します。

write terminal

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、**show running-config** コマンドと同等です。

例

次に、実行コンフィギュレーションを端末に書き込む例を示します。

```
> write terminal
: Saved
:
: Serial Number: XXXXXXXXXXX
: Hardware:   ASA5516, 8192 MB RAM, CPU Atom C2000 series 2416 MHz, 1 CPU (8 cores)
:
NGFW Version 6.2.0
!
hostname firepower
(...remaining output deleted...)
```

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