# Cisco Secure Firewall Threat Defense コマンド リファレンス

**初版**：2017 年 9 月 25 日

**最終更新**：2023 年 5 月 2 日

**シスコシステムズ合同会社**
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

# コマンドライン インターフェイス（CLI）の使用方法

次のトピックでは、Secure Firewall Threat Defenseデバイスのコマンドライン インターフェイス（CLI）を使用する方法と、コマンドリファレンストピックの解釈方法について説明します。基本的なシステム設定およびトラブルシューティングに CLI を使用します。

（注） Secure Firewall Management Centerまたは Secure Firewall デバイスマネージャを使用して設定変更を展開する場合は、長時間実行されるコマンド（膨大な繰り返し回数やサイズの ping など）に 脅威に対する防御 CLI を使用しないでください。これらのコマンドが原因で展開が失敗する可能性があります。

# CLI（コマンドライン インターフェイス）へのログイン

CLIにログインするには、SSHクライアントを使用して、管理IPアドレスに接続します。**admin** ユーザー名（デフォルトのパスワードはAdmin123です）または別のCLIのユーザー アカウントを使用してログインします。

SSH 接続用のインターフェイスを開いている場合、データ インターフェイス上のアドレスにも接続できます。データ インターフェイスへの SSH アクセスはデフォルトで無効になっています。SSHアクセスを有効にするには、デバイスマネージャ（Management CenterまたはDevice Manager）を使用して、特定のデータインターフェイスへのSSH接続を許可します。診断インターフェイスに SSH 接続することはできません。

**configure user add** コマンドを使用して CLI にログイン可能なユーザーアカウントを作成できます。ただし、これらのユーザはCLIのみにログインできます。Device Manager Webインターフェイスにはログインできません。CLIはローカル認証のみをサポートします。外部認証を使用して CLI にアクセスすることはできません。

### コンソールポートアクセス

SSHの他に、デバイスのコンソールポートに直接接続することもできます。デバイスに付属のコンソール ケーブルを使用し、9600 ボー、8 データ ビット、パリティなし、1 ストップ ビット、フロー制御なしに設定されたターミナル エミュレータを用いてPCをコンソールに接続します。コンソール ケーブルの詳細については、デバイスのハードウェア ガイドを参照してください。

コンソール ポートでアクセスする最初の CLI は、デバイス タイプによって異なります。

- ASA ハードウェア プラットフォーム：コンソールポートの CLI は通常の 脅威に対する防御 CLI です。
- その他のハードウェア プラットフォーム：コンソールポートの CLI は Secure Firewall eXtensible オペレーティングシステム です（FXOS）。**connect** コマンドを使用して 脅威に対する防御 CLI にアクセスできます。FXOS CLI はシャーシ レベルの設定およびトラブルシューティングにのみ使用します。 Firepower 2100 の場合、FXOS CLI で設定を行うことはできません。 基本設定、モニタリング、および通常のシステムのトラブルシューティングには 脅威に対する防御CLIを使用します。FXOSコマンドの詳細については、Firepower 4100 および 9300 の FXOS コマンドに関する情報を参照してください。その他のモデルの FXOS コマンドについては、FXOS のトラブルシューティング ガイドを参照してください。

# コマンド モード

脅威に対する防御 デバイスの CLI にはさまざまなモードがあります。これらのモードは、単一の CLI のサブモードではなく、実際には別の CLI です。どのモードになっているかは、コマンドプロンプトで確認できます。

### 通常の Threat Defense CLI

この CLI は、脅威に対する防御 の管理設定とトラブルシューティングに使用します。

```
>
```

### 診断 CLI

この CLI を使用して、高度なトラブルシューティングを行います。この CLI では、追加の show コマンドや、ASA 5506W-X ワイヤレスアクセスポイントの CLI へのアクセスに必要な **session wlan console** コマンドなど、その他のコマンドが利用できます。この CLI には 2 つのサブモードがあり、特権 EXEC モードの方が使用できるコマンドが多くなります。

このモードを開始するには、脅威に対する防御 CLI で **system support diagnostic-cli** コマンドを使用します。

- ユーザー EXEC モード。プロンプトには、実行コンフィギュレーションで定義されているシステムホスト名が反映されます。

  ```
  firepower>
  ```

- 特権 EXEC モード。このモードを開始するには、**enable** コマンドを入力します（パスワードプロンプトに対してパスワードを入力せずに Enter を押します）。このモードではパスワードを設定できないことに注意してください。アクセスは、脅威に対する防御 CLI へのアカウントログインによってのみ保護されます。ただし、ユーザーは特権 EXEC モードでコンフィギュレーション モードを開始できないため、追加のパスワード保護は必要ありません。

  ```
  firepower#
  ```

### エキスパート モード

マニュアルの手順で求められた場合、または Cisco Technical Assistance Center から求められた場合のみ、エキスパート モードを使用します。このモードを開始するには、脅威に対する防御 CLI で **expert** コマンドを使用します。

管理者ユーザーでログインする場合、プロンプトは username@hostname です。別のユーザーを使用する場合は、ホスト名のみが表示されます。ホスト名は、管理インターフェイスに対して設定された名前です。次に例を示します。

```
admin@firepower:~$
```

### FXOS CLI

ASA ハードウェアモデルを除き、FXOS はシャーシ全体を制御するオペレーティング システムです。モデルによっては、設定とトラブルシューティングにFXOSを使用します。FXOS から 脅威に対する防御 CLI にアクセスするには、**connect** コマンドを使用します。

すべてのアプライアンスモードモデル（Firepower 4100/9300 以外のモデル）では、**connect fxos** コマンドを使用して 脅威に対する防御 CLI から FXOS CLI に移動できます。

FXOS コマンドプロンプトは次のようになりますが、プロンプトはモードによって変化します。FXOS CLI の使用方法の詳細については、FXOS のドキュメントを参照してください。

```
Firepower-module2>
Firepower-module2#
```

# 構文の書式

コマンド構文の説明には、次の表記法を使用しています。

| 表記法 | 説明 |
|---|---|
| **command** | **Command** テキストは、記載されているとおりに入力するコマンドおよびキーワードを示しています。 |
| *variable* | *Variable* テキストは、ユーザーが値を指定する引数です。 |
| [x] | 角カッコの中の要素は、省略可能です（キーワードや引数）。 |
| [x \| y] | いずれか1つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。 |
| {x \| y} | 必ずいずれか 1 つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。 |
| [x {y \| z}] | 省略可能または必須の要素内に、さらに省略可能または必須の選択肢を含める場合は、角カッコや波カッコを入れ子にして示しています。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。 |

# コマンドの入力

コンソールポートまたは SSH セッションを使用して CLI にログインすると、次のコマンドプロンプトが表示されます。

```
>
```

コマンドを実行するには、プロンプトでコマンドを入力して Enter キーを押します。その他の機能には次のものがあります。

- コマンド履歴のスクロール：上下矢印キーを使用すると、すでに入力したコマンドをスクロールできます。履歴でコマンドを再入力、または編集して再入力できます。
- コマンドの完成：部分的な文字列を入力してコマンドまたはキーワードを完成させるには、スペースキーまたは Tab キーを押します。コマンドを完成させるには、部分的な文字列が 1 つのコマンドまたはキーワードに一致する必要があります。
- コマンドの省略：通常の CLI では、コマンドを省略できません。完全なコマンド文字列を入力する必要があります。ただし診断 CLI では、ほとんどのコマンドは、コマンド固有の最少の文字列に短縮できます。たとえば、**show version** の代わりに **show ver** を入力できます。
- コマンド出力の停止：コマンドが大量の出力を生成する場合は、q キーを押すと出力を終了できます。
- 長時間実行コマンドの停止：コマンドが十分な速度で出力を返さず、別のコマンドを試すことにした場合は、Ctrl+C を押します。

# show コマンド出力のフィルタリング

出力をフィルタリングコマンドにパイピングすると、**show** コマンドの出力をフィルタリングできます。出力のパイピングはすべての **show** コマンドで使用できますが、大量のテキストを生成するコマンドを処理する場合に最も役立ちます。

フィルタリング機能を使用するには、次の形式を使用します。この場合、show コマンドの後の縦棒 | はパイプ文字であり、コマンドに含まれ、構文の説明の一部ではありません。フィルタリングオプションはコマンドの | 文字の後に入力します。

**show** *command* | {**grep** | **include** | **exclude** | **begin**} 正規表現

### フィルタリングコマンド

次のフィルタリングコマンドを使用できます。

- **grep**：パターンと一致する行のみを表示します。
- **include**：パターンと一致する行のみを表示します。
- **exclude**：パターンと一致するすべての行を除外し、その他のすべての行を表示します。
- **begin**：パターンを含む最初の行を検索し、その行と後続のすべての行を表示します。

***regular_expression***

通常は単純なテキスト文字列である正規表現です。式を一重引用符または二重引用符で囲まないでください。式の一部と見なされます。また、末尾のスペースは式に含まれます。

次に、**show access-list** コマンドの出力を変更して、inside1_2 インターフェイスに適用されるルールだけを表示する例を示します。

```
> show access-list | include inside1_2
access-list NGFW_ONBOX_ACL line 3 advanced trust ip ifc inside1_2 any ifc inside1_3 any
 rule-id 268435458
event-log both (hitcnt=0) 0x2c7f5801
access-list NGFW_ONBOX_ACL line 4 advanced trust ip ifc inside1_2 any ifc inside1_4 any
 rule-id 268435458
event-log both (hitcnt=0) 0xf170c15b
access-list NGFW_ONBOX_ACL line 5 advanced trust ip ifc inside1_2 any ifc inside1_5 any
 rule-id 268435458
event-log both (hitcnt=0) 0xce627c77
access-list NGFW_ONBOX_ACL line 6 advanced trust ip ifc inside1_2 any ifc inside1_6 any
 rule-id 268435458
event-log both (hitcnt=0) 0xe37dcdd2
access-list NGFW_ONBOX_ACL line 7 advanced trust ip ifc inside1_2 any ifc inside1_7 any
 rule-id 268435458
event-log both (hitcnt=0) 0x65347856
access-list NGFW_ONBOX_ACL line 8 advanced trust ip ifc inside1_2 any ifc inside1_8 any
 rule-id 268435458
event-log both (hitcnt=0) 0x6d622775
access-list NGFW_ONBOX_ACL line 9 advanced trust ip ifc inside1_3 any ifc inside1_2 any
 rule-id 268435458
event-log both (hitcnt=0) 0xc1579ed7
```

```
access-list NGFW_ONBOX_ACL line 15 advanced trust ip ifc inside1_4 any ifc inside1_2 any
 rule-id 268435458
event-log both (hitcnt=0) 0x1d1a8032
access-list NGFW_ONBOX_ACL line 21 advanced trust ip ifc inside1_5 any ifc inside1_2 any
 rule-id 268435458
event-log both (hitcnt=0) 0xf508bbd8
access-list NGFW_ONBOX_ACL line 27 advanced trust ip ifc inside1_6 any ifc inside1_2 any
 rule-id 268435458
event-log both (hitcnt=0) 0xa6be4e58
access-list NGFW_ONBOX_ACL line 33 advanced trust ip ifc inside1_7 any ifc inside1_2 any
 rule-id 268435458
event-log both (hitcnt=0) 0x699725ea
access-list NGFW_ONBOX_ACL line 39 advanced trust ip ifc inside1_8 any ifc inside1_2 any
 rule-id 268435458
event-log both (hitcnt=0) 0xd2014e58
access-list NGFW_ONBOX_ACL line 47 advanced trust ip ifc inside1_2 any ifc outside any
rule-id 268435457
event-log both (hitcnt=0) 0xea5bdd6e
```

# コマンドのヘルプ

次のコマンドを入力すると、コマンドラインからヘルプ情報を利用できます。

- **?** ：すべてのコマンドのリストを表示します。
- command_name：コマンドのオプションを表示します。 **?** たとえば、**show ?** のようになります。
- string：文字列に一致するコマンドまたはキーワードを表示します。**?** たとえば、**n?** は、文字 n で始まるすべてのコマンドを表示します。
- command_name を使用して、コマンドのシンタックスと限定された使用法の情報を表示します。**help** ヘルプページがあるコマンドを表示するには、**help ?** と入力します。

# 第 I 部

# A ～ R コマンド

# a - clear e

# aaa-server active、fail

障害とマークされた AAA サーバーを再度アクティブにするには、**aaa-server active** コマンドを使用します。アクティブな AAA サーバーを障害とマークするには、**aaa-server fail** コマンドを使用します。

**aaa-server** *groupname* {**active** | **fail**} **host** *hostname*

## 構文の説明

| | |
|---|---|
| **active** | サーバーをアクティブ状態に設定します。 |
| **fail** | サーバーを障害状態に設定します。 |
| *groupname* | AAA サーバーグループまたはレルム名。 |
| **host** *hostname* | アクティブになっているサーバーの FQDN または IP アドレス。 |

## 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しないと、グループ内の障害が発生したサーバーは、グループ内のすべてのサーバーに障害が発生するまで障害状態のままになります。グループ内のすべてのサーバーに障害が発生した後に、サーバーはすべて再度アクティブにされます。**show aaa-server** コマンドの出力で、サーバーグループまたはレルム名、およびすべての AAA サーバーの情報を確認できます。

### 例

次に、group1 のサーバー 192.168.125.60 の状態を表示し、手動で再度アクティブにする例を示します。

```
> show aaa-server group1 host 192.68.125.60
Server Group: group1
Server Protocol: RADIUS
Server Address: 192.68.125.60
Server port: 1645
Server status: FAILED. Server disabled at 11:10:08 UTC Fri Aug...
>
> aaa-server group1 active host 192.168.125.60
>
> show aaa-server group1 host 192.68.125.60
Server Group: group1
Server Protocol: RADIUS
Server Address: 192.68.125.60
Server port: 1645
Server status: ACTIVE (admin initiated). Last Transaction at 11:40:09 UTC Fri Aug...
```

関連コマンド

| コマンド | 説明 |
| --- | --- |
| **clear aaa-server statistics** | AAA サーバー統計情報をクリアします。 |
| **show aaa-server** | AAA サーバー統計情報を表示します。 |
| **test aaa-server** | AAA サーバーの設定を確認します。 |

# app-agent heartbeat

脅威に対する防御 デバイスで実行されている app-agent（アプリケーション エージェント）のハートビートメッセージ間隔を設定するには、**app-agent heartbeat** コマンドを使用します。

**app-agent heartbeat** ［**interval** *milliseconds*］［**retry-count** *integer*］

## 構文の説明

| | |
|---|---|
| **interval** *milliseconds* | ハートビートメッセージの間隔をミリ秒単位で指定します。この間隔は 100 ミリ秒単位で調整できます。デフォルトは 1000 です。許可された範囲は、リリース 6.2.2 以降では 100 ー 6000 ですが、古いリリースでは 300 ー 6000 です。<br>連続的なハートビートメッセージの損失がこの再試行回数に達すると、システムの残りの部分への障害通知がトリガーされます。デフォルトの 1000 ミリ秒の場合、障害検出設定がアグレッシブになり、誤った障害検出が生じるリスクがあります。 |
| **retry-count** *integer* | 応答がない場合、またはアプリケーション エージェントがハートビートメッセージのエラー応答を受信した場合に、アプリケーションエージェントがハートビートメッセージを再試行する回数を指定します（3ー10回）。デフォルトは 3 です。 |

## コマンド デフォルト

間隔のデフォルト値は 1000 ミリ秒です。

デフォルトの再試行回数は 3 です。

## 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。 |
| 6.2.2 | 許可される間隔の範囲が 100 ー 6000 に変更されました。 |

## 使用上のガイドライン

脅威に対する防御 デバイスで実行されているアプリケーション エージェントの主な役割は、脅威に対する防御 モジュールと Firepower 2100、4100、および 9300 FXOS のシャーシ間の接続と通信です。

ハートビート通信チャネルは、FXOS シャーシと 脅威に対する防御 アプリケーション エージェント間のリンクの正常性をモニターする目的で使用されます。脅威に対する防御 アプリケーションは、一定の間隔で FXOS シャーシスーパーバイザに要求メッセージを送信し、FXOS シャーシスーパーバイザから適切な応答を受信するまで、設定された回数再試行します。

脅威に対する防御 アプリケーション エージェントと FXOS シャーシスーパーバイザ間のハートビートメカニズムも、ハードウェアバイパス機能の障害をモニターします。Firepower 2100、4100、9300 シリーズの特定のインターフェイスモジュールでは、ハードウェアバイパス機能を有効にできます。ハードウェアバイパスは、停電時にトラフィックがインラインインターフェ

イスペア間で流れ続けることを確認します。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。

### 例

次の例では、アプリケーション エージェントのハートビート間隔を 600 ミリ秒に、再試行回数を 6 回に設定します。

```
> app-agent heartbeat interval 600 retry-count 6
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show app-agent** | アプリケーション エージェントのステータスを表示します。 |
| **show inline-set** | インラインセット情報を表示します。 |
| **show interface** | インターフェイスステータス情報を表示します。 |

# asp inspect-dp egress-optimization

出力最適化を有効にするには、**asp inspect-dp egress-optimization** コマンドを使用します。出力最適化をディセーブルにするには、このコマンドの **no** 形式を使用します。

出力最適化は、選択された IPS トラフィックを対象としたパフォーマンス機能です。この機能は、すべての Threat Defense プラットフォームでデフォルトで有効になっています。

（注） この機能は有効のままにしておくことが強く推奨されます。Cisco TAC から指示された場合にのみ無効にしてください。

**asp inspect-dp egress-optimization**
**no asp inspect-dp egress-optimization**

## コマンド デフォルト

出力最適化はデフォルトで有効になっています。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.4 | このコマンドが導入されました。 |

## 使用上のガイドライン

出力最適化は、パフォーマンスを向上させるため、常に有効化することが意図されています。トラブルシューティングを目的として Cisco TAC からアドバイスがあった場合のみ、出力最適化を無効化します。

### 例

次に、出力最適化を有効にする例を示します。

```
> asp inspect-dp egress-optimization
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show conn state egress_optimization** | 出力最適化の対象となるフローに関する情報を表示します。このコマンドは、Cisco TAC のアドバイスに従って使用します。 |
| **show asp inspect-dp egress-optimization** | 出力最適化に関連する統計情報を表示します。 |
| **clear asp inspect-dp egress-optimization** | 出力最適化に関連する統計情報をクリアします。 |

# asp load-balance per-packet

複数のコアのロードバランシング動作をパケットごとに変更するには、**asp load-balance per-packet** コマンドを使用します。デフォルトのロード バランシング メカニズムを復元するには、このコマンドの **no** 形式を使用します。

**asp load-balance per-packet**
**no asp load-balance per-packet**

## コマンド デフォルト

パケット単位のロードバランシングはデフォルトで無効になっています。

## 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

ロード バランサのジョブは、パケットを CPU コアに配布し、パケットの順序を維持することです。デフォルトでは、接続は一度に1つのコアでしか処理できません。この動作により、使用中のインターフェイス/RXリングの数がコアの数に比べて少ない場合、コアは十分に活用されません。たとえば、脅威に対する防御 デバイスで 2 つのギガビット イーサネット インターフェイスのみを使用している場合は、2つのコアのみが使用されます。（10ギガビットイーサネット インターフェイスには 4 つの RX リングと、1 つの RX リングとしてギガビット イーサネット インターフェイスがあります）。パケット単位のロード バランシングを有効にして、より多くのコアを使用できるようにすることで、ロード バランサを最適化することができます。

デフォルトのロードバランシング動作では、多数のインターフェイスが使用されている場合にシステム全体のパフォーマンスが最適化され、パケット単位のロードバランサでは、アクティブなインターフェイスの数が少ない場合にシステム全体のパフォーマンスが最適化されます。

パケット単位のロードバランシングを有効にすると、1つのコアがインターフェイスからのパケットを処理する場合に、別のコアが同じインターフェイスからの次のパケットを受信して処理できます。したがって、すべてのコアが同じインターフェイスからのパケットを同時に処理することが可能です。

パケット単位のロード バランシングにより、次の場合にパフォーマンスが向上します。

- システムがパケットをドロップする
- **show cpu** コマンドで、CPU 使用率が 100% を大きく下回っていることが示されている。CPU 使用率は、使用されているコアの数を示す良い指標です。たとえば、8 コアシステムで、2 つのコアが使用されている場合、**show cpu** は 25% を示します。4 コアの場合は 50%、6 コアの場合は 75% を示します。
- 使用中のインターフェイスの数が少ない

（注） 通常、脅威に対する防御 に 64 未満の同時フローがある場合、パケット単位のロードバランシングを有効にすると、そのメリットよりもオーバーヘッドが大きくなります。

### 例

次に、デフォルトのロード バランシング動作を変更する例を示します。

```
> asp load-balance per-packet
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear asp load-balance history** | パケットごとの ASP ロードバランシングの履歴統計情報をクリアし、リセットします。OK |
| **show asp load-balance** | ロード バランサのキュー サイズのヒストグラムを表示します。OK |

# asp packet-profile

脅威に対する防御デバイスによるネットワークトラフィックの処理方法に関する統計を取得するには、**asp packet-profile** コマンドを使用します。パケットプロファイリングを無効にするには、このコマンドの no 形式を使用します。

高速セキュリティパス（ASP）プロセスは、プレフィルタポリシーによって高速パス処理されたパケット数、大規模なフローとしてオフロードされたパケット数、アクセス制御（Snort）によって完全に評価されたパケット数を判断します。

**asp packet-profile**
**no asp packet-profile**

## コマンド デフォルト

パケットプロファイリングは、デフォルトでは有効になっています。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.5 | このコマンドが導入されました。 |

## 使用上のガイドライン

パケットプロファイリングは、常に有効にすることが意図されていますが、統計情報の収集や追加的な計算が原因で CPU 使用率が高くなっている場合は、無効にできます。

### 例

次に、パケットプロファイリングを有効にする例を示します。

```
> asp packet-profile
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show asp packet-profile** | データプレーンのみ、またはデータプレーンと Snort を通過し、ハードウェアにオフロードされたパケットの統計情報を表示します。 |
| **clear asp packet-profile** | パケットプロファイリング関連の統計情報をクリアします。 |

# asp rule-engine transactional-commit

ルールエンジンのトランザクション コミット モデルを有効または無効にするには、**asp rule-engine transactional-commit** コマンドを使用します。

**asp rule-engine transactional-commit** *option*
**asp rule-engine transactional-commit** *option*

## 構文の説明

| | |
|---|---|
| *option* | 選択したポリシー用のルール エンジンのトランザクション コミット モデルをイネーブルにします。次のオプションがあります。<br>• **access-group**：グローバルに、またはインターフェイスに適用されるアクセスルール。<br>• **nat**：ネットワークアドレス変換ルール。 |

## コマンド デフォルト

デフォルトでは、トランザクション コミット モデルはディセーブルになっています。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.6 | このコマンドが導入されました。 |

## 使用上のガイドライン

デフォルトでは、ルール ベースのポリシー（アクセス ルールなど）を変更した場合、変更はただちに有効になります。ただし、この即時性にはパフォーマンスにわずかなコストがかかります。パフォーマンスコストは、1 秒あたりの接続数が多い環境で大量のルールリストがある場合に顕著です。たとえば、デバイスが 1 秒あたり 18,000 の接続を処理しながら、25,000 のルールがあるポリシーを変更する場合などです。

パフォーマンスに影響するのは、ルール検索を高速化するためにルール エンジンがルールをコンパイルするためです。デフォルトでは、新しいルールを適用できるように、接続試行を評価するときに未コンパイルのルールも検索されます。新しいルールはコンパイルされていないため、検索に時間がかかります。

ルール変更を実装するときにルール エンジンがトランザクション モデルを使用するように、この動作を変更できます。これにより、新しいルールがコンパイルされ、使用できるようになるまで、引き続き古いルールが使用されます。トランザクション モデルを使用すると、ルールのコンパイル中、パフォーマンスは低下しないはずです。次の表は、その動作の違いを明確にします。

| モデル | コンパイル前 | コンパイル中 | コンパイル後 |
|---|---|---|---|
| デフォルト | 古いルールと照合します。 | 新しいルールと照合します。<br>（接続数/秒が削減されます） | 新しいルールと照合します。 |

| モデル | コンパイル前 | コンパイル中 | コンパイル後 |
|---|---|---|---|
| トランザクション | 古いルールと照合します。 | 古いルールと照合します。<br>（接続数/秒は影響を受けません） | 新しいルールと照合します。 |

トランザクションモデルの他のメリットには、アクセスグループで使用されるインターフェイス上の ACL を置き換えるときに、古い ACL を削除して新しいポリシーを適用するまでの時間差が生じないことがあります。これにより、動作中に許容可能な接続がドロップされる確率が減少します。

**ヒント** ルール タイプのトランザクション モデルをイネーブルにした場合、コンパイルの先頭と末尾をマークする syslog メッセージが存在します。これらのメッセージには、780001 以降の番号が付けられます。

**例**

次に、アクセス グループのトランザクション コミット モデルをイネーブルにする例を示します。

```
> asp rule-engine transactional-commit access-group
```

# blocks

ブロック診断（**show blocks** コマンドで表示）に追加のメモリを割り当てるには、**blocks** コマンドを使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

**blocks queue history enable** ［*memory_size*］
**no blocks queue history enable** ［*memory_size*］

## 構文の説明

| | |
|---|---|
| *memory_size* | （任意）ダイナミックな値を適用するのではなく、ブロック診断用のメモリ サイズをバイト単位で設定します。この値が空きメモリよりも大きい場合は、エラー メッセージが表示され、値は受け入れられません。この値が空きメモリの 50% を超える場合は、警告メッセージが表示されますが、値は受け入れられます。 |

## コマンド デフォルト

ブロック診断の追跡に割り当てられるデフォルト メモリは、2136 バイトです。

## 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

現在割り当てられているメモリを表示するには、**show blocks queue history** コマンドを入力します。

脅威に対する防御 デバイスをリロードすると、メモリ割り当てがデフォルトに戻ります。

割り当てられるメモリ量は最大 150 KB ですが、空きメモリの 50% を超えることはありません。必要に応じて、メモリ サイズを手動で指定できます。

### 例

次に、ブロック診断用のメモリ サイズを増やす例を示します。

```
> blocks queue history enable
```

次に、メモリ サイズを 3000 バイトに増やす例を示します。

```
> blocks queue history enable 3000
```

次に、メモリ サイズを 3000 バイトに増やすことを試みるものの、この値が使用可能な空きメモリを超えている例を示します。

```
> blocks queue history enable 3000
ERROR: memory size exceeds current free memory
```

次に、メモリ サイズを 3000 バイトに増やすものの、この値が空きメモリの 50% を超えている例を示します。

```
> blocks queue history enable 3000
WARNING: memory size exceeds 50% of current free memory
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear blocks** | システム バッファの統計情報をクリアします。 |
| **show blocks** | システム バッファの使用状況を表示します。 |

# capture

パケットスニッフィングおよびネットワーク障害の切り分けのためにパケットキャプチャ機能を有効にするには、**capture** コマンドを使用します。パケットキャプチャ機能をディセーブルにするには、このコマンドの no 形式を使用します。

ネットワークトラフィックをキャプチャします。

**capture** *capture_name* [ **type** { **asp-drop** [ **all** | *drop-code* ] | **raw-data** | **isakmp** [ **ikev1** | **ikev2** ] | **inline-tag** [ *tag* ] }] { **interface** { *interface_name* | **data-plane | management-plane | cplane** } } [ **buffer** *buf_size* ] [ **file-size** *file_size* ] [ **ethernet-type** *type* ] [ **headers-only** ] [ **packet-length** *bytes* ] [ **circular-buffer** ] [ **trace** [ **trace-count** *number* ] [ **match** *protocol* { **host** *source_ip* | *source_ip mask* | **any4** | **any6** } [ *operator src_port* ] { **host** *dest_ip* | *dest_ip mask* | **any4** | **any6** } [ *operator dest_port* ] ]

クラスタ制御リンク トラフィックをキャプチャします。

**capture** *capture_name* **type lacp interface** *interface_id* [ **buffer** *buf_size* ] [ **packet-length** *bytes* ] [ **circular-buffer** ] [ **real-time** [ **dump** ] [ **detail** ] ]
**capture** *capture_name* **interface cluster** [ **buffer** *buf_size* ] [ **ethernet-type** *type* ] [ **packet-length** *bytes* ] [ **circular-buffer** ] [ **trace** [ **trace-count** *number* ] ] [ **real-time** [ **dump** ] [ **detail** ] ] [ **trace** ] [ **match** *protocol* { **host** *source_ip* | *source_ip mask* | **any4** | **any6** } [ *operator src_port* ] { **host** *dest_ip* | *dest_ip mask* | **any4** | **any6** } [ *operator dest_port* ] ]

クラスタ全体のパケットをキャプチャします。

**cluster exec capture** *capture_name* [ **persist** ] [ **include-decrypted** ]

キャプチャからパケットキャプチャまたはパラメータを削除します。キャプチャを完全に削除することが目的の場合は、パラメータを省略します。

**no capture** *capture_name* [ *arguments* ]

パケットキャプチャを削除せずに停止します。

**capture** *capture_name* **stop**

## 構文の説明

| | |
|---|---|
| **any4** | 単一の IP アドレスおよびマスクではなく、任意の IPv4 アドレスを指定します。 |
| **any6** | 単一の IP アドレスおよびマスクではなく、任意の IPv6 アドレスを指定します。 |
| **all** | 高速セキュリティ パスでドロップされるすべてのパケットをキャプチャします。 |

| | |
|---|---|
| **asp-drop** *drop-code* | （任意）高速セキュリティパスでドロップされるパケットをキャプチャします。drop-code は、高速セキュリティ パスでドロップされるトラフィックのタイプを指定します。drop-code のリストについては、CLI ヘルプを参照してください。このキーワードは、**packet-length**、**circular-buffer**、および **buffer** キーワードと一緒に入力できますが、**interface** または **ethernet-type** キーワードと一緒には入力できません。クラスタでは、ドロップされた、ユニット間の転送データ パケットもキャプチャされます。 |
| **buffer** *buf_size* | （任意）パケットの保存に使用するバッファのサイズをバイト単位で定義します。このバイト数のバッファがいっぱいになると、パケットキャプチャは停止します。クラスタ内で使用されるときは、これはユニットあたりのサイズです（全ユニットの合計ではありません）。サポートされる最大バッファサイズは 32 MB です。<br>バッファサイズとファイルサイズのオプションは同時に使用できません。 |
| *capture_name* | パケット キャプチャの名前を指定します。複数のトラフィックのタイプをキャプチャするには、複数の **capture** ステートメントで同じ名前を使用します。**show capture** コマンドを使用してキャプチャのコンフィギュレーションを表示すると、すべてのオプションが 1 行にまとめられます。 |
| **data-plane** | データプレーン インターフェイスでキャプチャされるパケットを指定します。 |
| **management-plane** | 管理インターフェイスでキャプチャされるパケットを指定します。 |
| **circular-buffer** | （任意）バッファがいっぱいになったとき、バッファを先頭から上書きします。 |
| **ethernet-type** *type* | （任意）キャプチャするイーサネット タイプを選択します。サポートされるイーサネット タイプには、8021Q、ARP、IP、IP6、IPX、LACP、PPPOED、PPPOES、RARP および VLAN などがあります。802.1Q タイプと VLAN タイプでは例外が発生します。802.1Q タグは自動的にスキップされ、照合には内部イーサネット タイプが使用されます。 |

| | |
|---|---|
| **file-size** *file-size* | （任意）**file-size** はディスク上のファイルにパケットをキャプチャするように指定します。<br><br>*file-size* は、キャプチャファイルのサイズを 32 MB から 10 GB の範囲で指定します。<br><br>キャプチャファイルは、フラッシュメモリ **(disk0:/)** に **capture_name.pcap** という名前で作成されます。<br><br>**file-size** が設定されると、ハードディスクメモリ（ファイル）を使用して、キャプチャバッファでキャプチャされたデータが書き込まれます。キャプチャされたデータは、ファイル名に基づいてディスクに保存されます。<br><br>バッファサイズとファイルサイズのオプションは同時に使用できません。 |
| **headers-only** | （任意）データなしでキャプチャするパケットのレイヤ2およびレイヤ3/4 ヘッダーを選択します。 |
| **host** *source_ip*, *dest_ip* | パケットの送信先または送信元ホストの単一の IP アドレスを指定します。 |
| **include-decrypted** | （オプション）ファイアウォールデバイスに入った時点で、通常のトラフィックと復号化されたトラフィックの両方を含む復号化された IPsec パケットをキャプチャします。また、SSL復号トラフィックのパケットもキャプチャします。ただし、パケットは VTI インターフェイスでのみ復号化された形式で表示されるため、このオプションは VTI トンネルには適用できません。暗号化マップ VPN のように外部ではありません。 |
| **inline-tag** *tag* | 特定の SGT 値のタグを指定するか、または未指定のままにしてすべての SGT 値のタグ付きパケットをキャプチャします。 |
| **interface** *interface_name* | パケットキャプチャを使用するインターフェイスの名前を設定します。**type asp-drop** を除いて、パケットをキャプチャするにはインターフェイスを設定する必要があります。複数の **capture** コマンドで同じ名前を使用して、複数のインターフェイスを設定できます。管理プレーン上のパケットをキャプチャするには、**interface** キーワードを使用し、インターフェイス名として「**asa_mgmt_plane**」を指定します。インターフェイス名として「**cluster**」を指定すると、クラスタ制御リンクインターフェイスのトラフィックをキャプチャできます。データインターフェイス上で Management Center アクセスを有効にした場合に内部バックプレーンインターフェイスでパケットをキャプチャするには、**nlp_int_tap** を指定します。キャプチャのタイプとして **lacp** が設定されている場合は、インターフェイス名は物理名です。 |
| **ikev1**, **ikev2** | IKEv1 または IKEv2 プロトコル情報だけをキャプチャします。 |

| | |
|---|---|
| **isakmp** | （オプション）VPN 接続の ISAKMP トラフィックをキャプチャします。ISAKMP サブシステムは、上位層プロトコルにアクセスできません。このキャプチャは、PCAP パーサーを満足させるために物理、IP、および UDP の各レイヤを 1 つにまとめた疑似キャプチャです。このピア アドレスは、SA 交換から取得され、IP レイヤに保存されます。 |
| **lacp** | （オプション）LACP トラフィックをキャプチャします。設定されている場合は、インターフェイス名は物理インターフェイス名です。 |
| *mask* | IP アドレスのサブネットマスク。たとえば、クラス C マスクの場合は 255.255.255.0 です。 |
| **match** *protocol* | 5 タプルが一致するパケットを指定し、キャプチャされるこれらのパケットのフィルタリングを許可します。1 行に最大 3 回このキーワードを使用できます。 |
| *operator src_port, dest_port* | （任意）送信元または宛先で使用されるポート番号を照合します。使用できる演算子は、次のとおりです。<br>• **lt**：小なり<br>• **gt**：大なり<br>• **eq**：等しい<br>• **neq**：等しくない<br>• **range**：範囲 |
| **packet-length** *bytes* | （任意）キャプチャ バッファに保存する各パケットの最大バイト数を設定します。 |
| persit | （オプション）クラスタユニットで永続的なパケットをキャプチャします。 |
| **raw-data** | （任意）着信パケットおよび発信パケットを 1 つ以上のインターフェイスでキャプチャします。 |
| **stop** | パケットキャプチャを削除せずに停止します。キャプチャを再開するには、このオプションを指定したこのコマンドの **no** 形式を使用します。 |
| **trace** *trace_count* | （任意）パケット トレース情報、およびキャプチャするパケット数をキャプチャします。このオプションをアクセス リストとともに使用すると、トレース パケットがデータ パスに挿入されるので、パケットが想定どおりに処理されているかどうかを判別できます。 |
| **type** | （任意）キャプチャされるデータのタイプを指定します。 |

## コマンド デフォルト

デフォルトの設定は次のとおりです。

- デフォルトの **type** は **raw-data** です。
- デフォルトの**buffer** サイズは 512 KB です。
- デフォルトのイーサネット タイプは IP パケットです。
- デフォルトの **packet-length** は 1518 バイトです。

## 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。 |
| 6.2.1 | このコマンドは、ボックス クラッシュ時にすべてのアクティブなキャプチャの内容をフラッシュまたはディスク上のファイルに保存するように更新されました。 |
| 6.2.3 | オプション asa_mgmt_plane および asa_dataplane の名前がそれぞれ **management-plane** および **data-plane** に変更されました。 |
| 6.2.3.x | IPv4 および IPv6 ネットワークトラフィックをそれぞれキャプチャするために、**any4** および **any6** オプションが導入されました。 |
| 6.3 | オプション［**file-size** *file-size*］を使用すると、ファイルサイズを MB 単位でキャプチャできます（32 ー 10000）。 |
| 6.7 | **interface nlp_int_tap** インターフェイス名は、データインターフェイス上で Management Center アクセスを有効にした場合に内部バックプレーン インターフェイスでパケットをキャプチャするために追加されました。 |

## 使用上のガイドライン

パケットキャプチャは、接続の問題のトラブルシューティングまたは不審なアクティビティのモニタリングを行うときに役立ちます。複数のキャプチャを作成できます。**capture** コマンドは、実行コンフィギュレーションには保存されません。また、ハイアベイラビリティ時にスタンバイユニットにコピーされません。

脅威に対する防御 デバイスでは、通過するすべての IP トラフィックを追跡でき、すべての管理トラフィック（SSH トラフィック、Telnet トラフィックなど）を含む、着信するすべての IP トラフィックをキャプチャできます。

脅威に対する防御のアーキテクチャは、パケット処理のための異なる3セットのプロセッサで構成されています。このアーキテクチャに起因して、キャプチャ機能の性能に一定の制限が加わります。通常は、脅威に対する防御デバイスのパケット転送機能の大部分が2個のフロントエンド ネットワーク プロセッサで処理され、アプリケーション インスペクションが必要なパケットに限り、コントロールプレーン汎用プロセッサに送信されます。パケットがセッション管理パス ネットワーク プロセッサに送信されるのは、高速パス プロセッサで処理されないセッションがある場合だけです。

脅威に対する防御デバイスによって転送またはドロップされるすべてのパケットがこの2つのフロントエンドネットワーク プロセッサを通るため、パケットキャプチャ機能はこれらのネットワークプロセッサに実装されています。したがって、該当するトラフィック インターフェイ

ス用の適切なキャプチャが設定されていれば、脅威に対する防御デバイスを通過するすべてのパケットをこれらのフロントエンドプロセッサでキャプチャできます。入力側では、インターフェイスに到着した時点でパケットがキャプチャされ、出力側では、ネットワークに送信される直前でパケットがキャプチャされます。

キャプチャされたデータを保存するため、パケットキャプチャはキャプチャされたデータをその場で自動的に物理ストレージに書き込むので、**copy** コマンドを使用する必要がありません。キャプチャサイズは最大 10 GB までサポートされます。100 MB を超えるキャプチャは自動的に圧縮されます。

### キャプチャの保存

脅威に対する防御デバイス上のすべてのアクティブなキャプチャの内容は、ボックスがクラッシュしたときに保存されます。トラブルシューティングプロセスの一部としてキャプチャをアクティブ化する場合は、次の点に注意する必要があります。

- 使用するキャプチャバッファのサイズ、およびフラッシュまたはディスクに十分なスペースがあるかどうか。
- キャプチャされたパケットがクラッシュ前の最新のものになるように、キャプチャ バッファはすべての使用例で円形としてマークする必要があります。

アクティブなキャプチャの内容を保存するファイルの名前は、次の形式となります。

*[<context_name>.]<capture_name>.pcap*

*context_name* は、マルチコンテキストモードでキャプチャがアクティブになっているユーザーコンテキストの名前を示します。シングル コンテキスト モードでは、context_name は適用されません。

*capture_name* は、アクティブ化されたキャプチャの名前を示します。

キャプチャの保存は、コンソールまたはクラッシュ ダンプの前に行われます。これにより、33 MB のキャプチャ バッファでクラッシュのダウンタイムが約 5 秒増加します。キャプチャしたコンテンツをファイルにコピーするのは簡単なプロセスなので、ネストされたクラッシュのリスクは最小限です。

### キャプチャの表示

パケットキャプチャを表示するには、**show capture** *name* コマンドを使用します。キャプチャをファイルに保存するには、**copy capture** コマンドを使用します。パケット キャプチャ情報を Web ブラウザで表示するには、**https://***FTP-ip-address***/***admin***/capture/***capture_name*[**/pcap**] コマンドを使用します。**pcap** キーワードを指定すると、libpcap 形式のファイルが Web ブラウザにダウンロードされ、Web ブラウザを使用してこのファイルを保存できます（libcap ファイルは、TCPDUMP または Ethereal で表示できます）。

バッファの内容を TFTP サーバーに ASCII 形式でコピーする場合、パケットの詳細および 16 進ダンプは表示されず、ヘッダーだけが表示されます。詳細および 16 進ダンプを表示するには、バッファを PCAP 形式で転送し、TCPDUMP または Ethereal で読み取る必要があります。

### キャプチャの削除

キーワードを指定せずに **no capture** を入力すると、キャプチャが削除されます。キャプチャを保持するには、**interface** キーワードを指定します。キャプチャは指定したインターフェイスから分離されて保持されます。

### クラスタ

**capture** コマンドの前に **cluster exec** を指定すると、あるユニットで **capture** コマンドを発行し、そのコマンドを他のすべてのユニットで同時に実行できます。クラスタ全体のキャプチャを実行した後、同じキャプチャファイルをクラスタ内のすべてのユニットから同時に TFTP サーバーにコピーするには、マスターユニットで **cluster exec copy** コマンドを入力します。

**cluster exec capture** *capture_name arguments*

**cluster exec copy /pcap capture:** *cap_name* **tftp://***location/path/filename***.pcap**

複数の PCAP ファイル（各ユニットから 1 つずつ）が TFTP サーバーにコピーされます。宛先のキャプチャ ファイル名には自動的にユニット名が付加され、filename_A.pcap、filename_B.pcap などとなります。この例では、A と B がクラスタ ユニット名です。

（注） ファイル名の末尾にユニット名を追加すると、別の宛先名が生成されます。

### 制限事項

次に、キャプチャ機能の制限の一部を示します。制限の大部分は、本質的に分散的な脅威に対する防御 のアーキテクチャと、脅威に対する防御 デバイスで使用するハードウェアアクセラレータによるものです。

- インライン SGT タグ付きパケットの場合、キャプチャされたパケットに含まれている追加 CMD ヘッダーを、PCAP ビューアが認識しないことがあります。
- パケット内の 802.1Q タグが、設定されたサブインターフェイスのものと異なる場合、そのようなパケットはキャプチャされません。パケットは名前付きインターフェイスに関連付けられていないため、無視されます。
- 受信側インターフェイスがないためグローバルインターフェイスがない場合、バックプレーン上で送信されるパケットは、制御パケットとして扱われます。これらのパケットはアクセス リスト チェックをバイパスし、常にキャプチャされます。
- 特定の asp-drop をキャプチャする場合に適切な理由を表示するには、show capture コマンドを使用します。ただし、show capture コマンドは、すべての asp-drop をキャプチャする場合は適切な理由を表示しません。

file-size オプションを使用したパケットキャプチャ機能には、次の制限があります。

- Firepower 4100/9300 シリーズのみに適用されます。
- 既存のキャプチャには、ファイルサイズオプションは追加できません。

- **copy** コマンドはサポートされていません。
- リアルタイム、トレース、リニア、および循環バッファはサポートされていません。
- ファイルサイズオプションを使用したキャプチャの数を増やすと、システムのパフォーマンスが低下します。
- システムの負荷が高いと、パケットキャプチャのデータが失われます。

### 例

パケットをキャプチャするには、次のコマンドを入力します。

```
> capture captest interface inside
> capture captest interface outside
```

Web ブラウザで、発行した「captest」という名前の **capture** コマンドの内容を次の場所に表示できます。

```
https://171.69.38.95/admin/capture/captest
```

libpcap ファイル（Web ブラウザが使用）をローカルマシンにダウンロードするには、次のコマンドを入力します。

```
https://171.69.38.95/capture/http/pcap
```

次に、脅威に対する防御 デバイスがクラッシュしたときにシングルモードでパケットをキャプチャする例を示します。

```
> capture 789 interface inside
```

キャプチャ「789」のコンテンツは、*789.pcap* ファイルとして保存されます。

次に、脅威に対する防御 がクラッシュしたときにマルチモードでパケットをキャプチャする例を示します。

```
>capture 624 interface inside
```

管理コンテキスト内のキャプチャ「624」のコンテンツは、*admin.624.pcap* ファイルとして保存されます。

次に、ARP パケットをキャプチャする例を示します。

```
> capture arp ethernet-type arp interface outside
```

### クラスタリングでのキャプチャ

クラスタ内のすべてのユニットでのキャプチャをイネーブルにするには、これらの各コマンドの前に cluster exec キーワードを追加します。

次の例では、クラスタリング環境の LACP キャプチャを作成する方法を示します。

```
> capture lacp type lacp interface gigabitEthernet0/0
```

次の例では、クラスタリング リンクでの制御パス パケットのキャプチャを作成する方法を示します。

```
> capture cp interface cluster match udp any eq 49495 any
> capture cp interface cluster match udp any any eq 49495
```

次の例では、クラスタを通過するデータ パス トラフィックをキャプチャする方法を示します。

```
> capture abc interface inside match tcp host 1.1.1.1 host 2.2.2.2 eq www
> capture abc interface inside match dup host 1.1.1.1 any
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear capture** | キャプチャ バッファをクリアします。 |
| **copy capture** | キャプチャ ファイルをサーバーにコピーします。 |
| **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。 |

# capture-traffic

脅威に対する防御インターフェイスを通過するパケットを代行受信してキャプチャするには、**capture-traffic** コマンドを使用します。指定されたオプションのリストの整数式に一致する、指定された脅威に対する防御ドメイン上のトラフィックをキャプチャできます（管理インターフェイス（br1）またはトラフィック インターフェイス）。

**capture-traffic**

ドメインと TCP ダンプオプションの入力が求められます。

## 構文の説明

| | |
|---|---|
| ドメイン | トラフィックをキャプチャするドメインを指定します。<br>• 0：br1。管理インターフェイスからのトラフィックをキャプチャします。<br>• 1：ルータ。設定されたデータインターフェイスからのトラフィックをキャプチャします。 |
| **-A** | 各パケット（リンクレベルヘッダーを除く）を ASCII で出力します。Web ページのキャプチャに便利です。 |
| **-B** | オペレーティングシステムのキャプチャバッファサイズを buffer_size に設定します。 |
| **-c** | カウントパケットを受信すると終了します。 |
| **-C** | raw パケットを savefile に書き込む前に、ファイルが現在 file_size よりも大きいかどうかを確認し、大きい場合は現在の savefile を閉じて新しいファイルを開きます。最初の savefile の後の savefile には、-w フラグの後に 1 から始まる数字が続く、指定された名前が付けられます。file_size の単位は、100 万バイト（1,048,576 バイトではなく 1,000,000 バイト）です。 |
| **-d** | コンパイル済みのパケット照合コードを人間が読める形式で標準出力にダンプし、停止します。 |
| **-dd** | パケット照合コードを C プログラムフラグメントとしてダンプします。 |
| **-ddd** | パケット照合コードを 10 進数（先頭に count）としてダンプします。 |

| | |
|---|---|
| **-D** | システムで使用でき、tcpdump がパケットをキャプチャできるネットワークインターフェイスのリストを出力します。ネットワークインターフェイスごとに、番号とインターフェイス名が表示され、その後にインターフェイスの説明が続く場合もあります。インターフェイス名または番号に-iフラグを付けることで、キャプチャするインターフェイスを指定できます。<br><br>これは、リストするコマンドを持たないシステム（Windows システム、または ifconfig -a がない UNIX システム）で役立ちます。この番号は、インターフェイス名がやや複雑な文字列である Windows 2000 以降のシステムで役立ちます。<br><br>tcapdump が pcap_findaclldevs() 関数を持たない古いバージョンの libpcap で構築されている場合、-D フラグはサポートされません。 |
| **-e** | 各ダンプ行にリンクレベルヘッダーを出力します。 |
| **-E** | addr にアドレス指定され、Security Parameter Index 値である spiを含む IPsec ESP パケットを復号化するには、spi@ipaddr algo:secret を使用します。この組み合わせは、カンマまたは改行で区切って繰り返すことができます。 |
| **-f** | 「外部」IPv4 アドレスを記号ではなく数値で出力します（このオプションは、Sun の NIS サーバーがローカル以外のインターネット番号を変換し続けて大抵ハングアップするという深刻な損傷を回避するためのもので、ます）。<br><br>「外部」IPv4 アドレスのテストは、キャプチャが実行されているインターフェイスの IPv4 アドレスとネットマスクを使用して実行されます。<br><br>キャプチャが行われているインターフェイスにアドレスまたはネットマスクがないことが理由で、または（複数のインターフェイス上でキャプチャできる Linux の「任意」のインターフェイスでキャプチャが行われていることが理由で、そのアドレスまたはネットマスクが使用できない場合は、このオプションは正しく機能しません。 |
| **-F** | フィルタ式への入力としてファイルを使用します。コマンドラインで指定された追加の式は無視されます。 |
| **-G** | 指定した場合は、-w オプションで指定したダンプファイルを rotate_seconds 秒ごとにローテーションします。<br><br>savefile の名前は -w で指定され、strftime(3) で定義された時刻形式が含まれます。時刻形式が指定されていない場合、新しいファイルごとに前のファイルが上書きされます。<br><br>-C オプションと組み合わせて使用すると、ファイル名は ‘file<count>’ の形式になります。 |
| **-I** | インターフェイスを「モニターモード」にします。これは IEEE 802.11 Wi-Fi インターフェイスでのみサポートされ、一部のオペレーティングシステムでのみサポートされます。 |

| | |
|---|---|
| **-K** | TCP チェックサムの検証を試みないでください。<br>これは、ハードウェアで TCP チェックサム計算を実行するインターフェイスには便利ですが、それ以外の場合はすべての発信 TCP チェックサムが不良としてフラグ付けされます。 |
| **-l** | stdout 行をバッファリングします。キャプチャ中にデータを表示する場合に便利です。たとえば、「'tcpdump -l \| tee dat」や「tcpdump -l > dat & tail -f dat」などです。 |
| **-L** | インターフェイスと出口の既知のデータリンクタイプを一覧表示します。 |
| **-m** | ファイルモジュールから SMI MIB モジュール定義をロードします。<br>このオプションを複数回使用すると、複数の MIB モジュールを tcpdump にロードすることができます。 |
| **-M** | TCP-MD5 オプション（RFC 2385）がある場合、TCP セグメントで検出されたダイジェストを検証するための共有秘密として秘密を使用します。 |
| **-n** | アドレス（ホストアドレス、ポート番号など）を名前に変換しません。 |
| **-N** | ホスト名のドメイン名修飾を出力しません。<br>たとえば、このフラグを指定すると、tcpdump は「nic.ddn.mil」ではなく「nic」を出力します。 |
| **-O** | パケット照合コードオプティマイザを実行しません。これは、オプティマイザのバグが疑われる場合にのみ役立ちます。 |
| **-p** | インターフェイスを無差別モードに入れません。インターフェイスは他の理由で無差別モードになる可能性があることに注意してください。そのため、「-p」は「ether host {local-hw-addr} or ether broadcast」の省略形として使用できません。 |
| **-q** | クイック出力。出力されるプロトコル情報が少ないため、出力行が短くなります。 |
| **-R** | ESP/AH パケットが古い仕様（RFC1825 ー RFC1829）に基づいていると仮定します。指定した場合、tcpdump はリプレイ防止フィールドを出力しません。<br>ESP/AH 仕様にプロトコル バージョン フィールドがないため、tcpdump は ESP/AH プロトコルのバージョンを推測できません。 |
| **-r** | ファイル（-w オプションを使用して作成したもの）からパケットを読み取ります。ファイルが「-」の場合、標準入力が使用されます。 |
| **-S** | 相対 TCP シーケンス番号ではなく、絶対 TCP シーケンス番号を出力します。 |

| | |
|---|---|
| **-s** | デフォルトの 68 ではなく、パケットそれぞれのデータの snaplen バイトを取得します（SunOS の NIT では、実際の最小値は 96 です）。IP、ICMP、TCP、および UDP では 68 バイトで十分ですが、ネームサーバーおよび NFS パケットからプロトコル情報が切り捨てられる場合があります（以下を参照）。限定的なスナップショットが原因で切り捨てられたパケットは、出力に「[|proto]」と表示されます。proto は、切り捨てが発生したプロトコルレベルの名前です。<br><br>スナップショットを大きくすると、パケットの処理にかかる時間が長くなり、パケットバッファリングの量が減少することに注意してください。これにより、パケットが失われる可能性があります。必要なプロトコル情報をキャプチャできる最小数に snaplen を制限する必要があります。snaplen を 0 に設定すると、パケット全体をキャッチするのに必要な長さを使用することを意味します。 |
| **-T** | 「式」によって選択されたパケットを強制的に指定されたタイプに変換します。現在知られているタイプは、aodv（アドホックオンデマンド距離ベクトルプロトコル）、cnfp（Cisco NetFlow プロトコル）、rpc（リモートプロシージャコール）、rtp（リアルタイム アプリケーション プロトコル）、rtcp（リアルタイム アプリケーション制御プロトコル）、 snmp（Simple Network Management Protocol）、tftp（Trivial File Transfer Protocol）、vat（Visual Audio Tool）、wb（Distributed White Board）です。 |
| **-t** | 各ダンプ行にタイムスタンプを出力しません。 |
| **-tt** | 各ダンプ行にフォーマットされていないタイムスタンプを出力します。 |
| **-ttt** | 各ダンプ行の現在の行と前の行の間の差分（マイクロ秒の解像度）を出力します。 |
| **-tttt** | 各ダンプ行にデフォルト形式のタイムスタンプと日付を出力します。 |
| **-ttttt** | 各ダンプ行の現在の行と最初の行の間の差分（マイクロ秒の解像度）を出力します。 |
| **-u** | 復号されていない NFS ハンドルを出力します。 |
| **-U** | 出力を -w オプション「packet-buffered」で保存します。つまり、出力バッファがいっぱいになったときのみではなく、各パケットが保存されるたびに出力ファイルに書き込まれます。<br><br>tcapdump が pcap_dump_flush() 関数を持たない古いバージョンの libpcap で構築されている場合、-U フラグはサポートされません。 |

| | |
|---|---|
| **-v** | 解析および出力時に、（もう少し）詳細な出力を生成します。たとえば、IPパケットの存続時間、ID、全長とオプションが表示されます。また、IPおよびICMPヘッダーチェックサムの検証などの、追加のパケット整合性チェックが使用可能です。<br><br>-w オプションを使用してファイルに書き込む場合、キャプチャされたパケット数を 10 秒ごとに報告します。 |
| **-vv** | さらに詳細な出力。たとえば、NFS応答パケットからの追加フィールドが出力され、SMB パケットは完全にデコードされます。 |
| **-vvv** | さらに詳細な出力。たとえば、telnet SB... SE オプションはすべて出力されます。-X Telnet オプションは 16 進数でも出力されます。 |
| **-w** | raw パケットを解析して出力するのではなく、ファイルに書き込みます。後で -r オプションを使用して出力できます。ファイルが「-」の場合、標準出力が使用されます。 |
| **-W** | -C オプションと組み合わせて使用すると、作成されるファイルの数が指定された数に制限され、ファイルの書き込みが最初から開始されるため、「回転」バッファが作成されます。さらに、最大数のファイルをサポートするのに十分な数の先行 0 をファイル名に付けることで、ファイルを正しくソートできるようにします。 |
| **-x** | 解析および出力時に、各パケットのヘッダーの出力に加えて、各パケットのデータ（リンクレベルヘッダーを差し引いたもの）を 16 進数で出力します。パケット全体または snaplen バイトの小さい方が出力されます。これはリンク層パケット全体であるため、パディングを行うリンク層について（たとえば、イーサネット）、上位層のパケットが必要なパディングよりも短い場合、パディングバイトも出力されます。 |
| **-xx** | 解析および出力時に、各パケットのヘッダーの出力に加えて、各パケットのデータを、リンクレベルヘッダーを含めて 16 進数で出力します。 |
| **-X** | 解析および出力時に、各パケットのヘッダーの出力に加えて、各パケットのデータ（リンク レベル ヘッダーを差し引いたもの）を 16 進数と ASCII で出力します。<br><br>これは、新しいプロトコルの分析に非常に便利です。 |
| **-XX** | 解析および出力時に、各パケットのヘッダーの出力に加えて、各パケットのデータを、リンクレベルヘッダーを含めて 16 進数と ASCII で出力します。 |
| **-y** | パケットをキャプチャするときに使用するデータリンクタイプを datalinktype に設定します。 |
| **-Z** | （ルートであれば）権限をドロップし、ユーザー ID とグループ ID をユーザーのプライマリ グループのユーザーおよびグループ ID に変更します。 |

## 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

デフォルトでは、**capture-traffic** コマンドは代行受信するパケットごとに 1 行のテキストを生成します。各行には、タイムスタンプ、プロトコル名、送信元および宛先アドレス（IP パケットの場合は IP アドレスであり、他のプロトコルの場合は、明示的に要求されない限り、**capture-traffic** は識別子を出力しません（**-e** コマンドラインの説明を参照））、および TCP シーケンス番号、フラグ、ARP/ICMP コマンドなどの情報が含まれます。

（注） **pcap** ファイル（**capture-traffic** コマンドまたは **debug daq** コマンドの出力）には、受信したパケットの未変換の詳細が表示されます。**Connection Events** リスト（Management Center）には、ポリシーで実際に適用された変換済みパケットの詳細が表示されます。

キャプチャを停止するには、Control+C を入力します。**-w** *outputfile* オプションを使用すると、パケットキャプチャはそのファイル名で /var/common/ に保存されます。それ以外の場合は、ディスプレイに書き込まれます。

### 例

次に、管理インターフェイスからトラフィックをキャプチャする例を示します。

```
> capture-traffic
Please choose domain to capture traffic from:
  0 - br1
  1 - Router
Selection? 0
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
-v
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show traffic** | トラフィック統計情報を表示します。 |
| **show interface** | インターフェイスのステータス情報を表示します。 |

# clear aaa-server statistics

AAA サーバーの統計情報をリセットするには、**clear aaa-server statistics** コマンドを使用します。

**clear aaa-server statistics** ［**LOCAL** | *groupname* ［**host** *hostname*］ | **protocol** *protocol*］

## 構文の説明

| | |
|---|---|
| *groupname* | （任意）グループ内のサーバーの統計情報をクリアします。 |
| **host** *hostname* | （任意）グループ内の特定のサーバーの統計情報をクリアします。 |
| **LOCAL** | （任意）LOCAL ユーザー データベースの統計情報をクリアします。 |
| **protocol** *protocol* | （任意）指定するプロトコルのサーバーの統計情報をクリアします。使用可能なプロトコルを確認するには、? を入力します。 |

## コマンド デフォルト

すべてのグループのすべての AAA サーバーの統計情報を削除します。

## 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。 |

### 例

次に、すべてのサーバー グループの AAA 統計情報をリセットする例を示します。

```
> clear aaa-server statistics
```

次に、サーバー グループ全体の AAA 統計情報をリセットする例を示します。

```
> clear aaa-server statistics svrgrp1
```

次に、グループ内の特定のサーバーの AAA 統計情報をリセットする例を示します。

```
> clear aaa-server statistics svrgrp1 host 10.2.3.4
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show aaa-server** | AAA サーバー統計情報を表示します。 |

# clear access-list

アクセスリストカウンタをクリアするには、clear access-list コマンドを使用します。

**clear access-list** *id*

## 構文の説明

| | |
|---|---|
| *id* | アクセス リストの名前。 |

## 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

**clear access-list** コマンドを入力する際には、カウンタをクリアするアクセスリストの id を指定する必要があります。ACL のリストを表示するには、**show access-list** コマンドを使用します。

### 例

次に、特定のアクセス リスト カウンタをクリアする例を示します。

```
> clear access-list inbound
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show access-list** | アクセス リスト エントリを番号で表示します。 |
| **show running-config access-list** | 適応型セキュリティアプライアンスで実行中のアクセス リスト コンフィギュレーションを表示します。 |

# clear arp

ダイナミック ARP エントリまたは ARP 統計情報をクリアするには、**clear arp** コマンドを使用します。

**clear arp** ［**statistics** | *interface_name*］

## 構文の説明

| | |
|---|---|
| **statistics** | ARP 統計情報をクリアします。 |
| *interface_name* | 指定したインターフェイスの統計情報をクリアします。 |

## 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、すべての ARP 統計情報をクリアする例を示します。

```
> clear arp statistics
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show arp statistics** | ARP 統計情報を表示します。 |
| **show running-config arp** | ARP タイムアウトの現在のコンフィギュレーションを表示します。 |

# clear asp

高速セキュリティパス（ASP）の統計情報をクリアするには、**clear asp** コマンドを使用します。

**clear asp** { **cluster counter** | **dispatch** | **drop** [ **flow** | **frame** ] | **event dp-cp** | **inspect-dp ack-passthrough** | **inspect-dp egress-optimization** | **inspect-dp snort** { **counters** [ **instance** *number* [ **queue** *number* ] ] | **queue-exhaustion** [ **snapshot** *number* ] } | **load-balance history** | **overhead** | **packet-profile** | **table** [ **arp** | **classify** | **filter** [ **access-list** *acl_name* ] ] }

## 構文の説明

| | |
|---|---|
| **access-list** *acl_name* | 指定したアクセス リストのヒット カウンタだけをクリアします。 |
| **arp** | ASP ARP テーブルのみでヒット カウンタをクリアします。 |
| **classify** | ASP classify テーブルのみでヒット カウンタをクリアします。 |
| **cluster counter** | クラスタ カウンタをクリアします。 |
| **counters** | データパスインスペクションの Snort カウンタをクリアします。 |
| **dispatch** | ディスパッチの統計情報をクリアします。 |
| **event** | データ パスからコントロール プレーンへのイベントの統計情報をクリアします。 |
| **filter** | ASP フィルタテーブルのヒットカウンタのみをクリアします。 |
| **flow** | ドロップされたフロー統計をクリアします。 |
| **frame** | ドロップされたフレーム/パケット統計をクリアします。 |
| **inspect-dp ack-passthrough** | Snortインスペクションをバイパスした空のTCP ACKパケットのカウンタをクリアします。 |
| **inspect-dp egress-optimization** | 出力最適化の統計情報をクリアします。 |
| **inspect-dp snort** | データパスインスペクションの Snort 統計情報をクリアします。 |
| **instance** *number* | インスタンス ID でカウンタをクリアします。 |
| **load-balance history** | パケット単位の ASP ロード バランシングの履歴をクリアし、自動切り替えが発生した回数をリセットします。 |
| **overhead** | すべての ASP マルチプロセッサ オーバーヘッドの統計情報をクリアします。 |
| **packet-profile** | パケットプロファイルの統計情報をクリアします。 |

| | |
|---|---|
| **queue** *number* | インスタンス ID とキュー ID でカウンタをクリアします。 |
| **queue-exhaustion** | データ パス インスペクションの Snort キュー スナップショットをクリアします。 |
| **snapshot** *number* | スナップショット ID でキューの枯渇をクリアします。 |
| **table** | ASP ARP テーブルおよび ASP 分類テーブルのヒット カウンタをクリアします。 |

## 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。 |
| 6.4 | **clear asp inspect-dp egress-optimization** コマンドが導入されました。 |
| 6.5 | **packet-profile** キーワードが追加されました。 |
| 7.0 | **inspect-dp ack-passthrough** キーワードが追加されました。 |

### 例

ディスパッチの統計情報をクリアする例を次に示します。

```
> clear asp dispatch
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show asp** | ASP 統計情報を表示します。 |

# clear bfd

双方向フォワーディング検出（BFD）カウンタをクリアするには、**clear bfd counters** コマンドを使用します。

**clear bfd counters** ［**ld** *local_discr* | *interface_name* | **ipv4** *ip_address* | **ipv6** *ip_address*］

## 構文の説明

| | |
|---|---|
| **ld** *local_discr* | （任意）指定したローカル識別子の BFD カウンタをクリアします（1 - 4294967295）。 |
| *interface_name* | （任意）指定したインターフェイスの BFD カウンタをクリアします。 |
| **ipv4** *ip_address* | （任意）指定したネイバー IPv6 アドレスの BFD カウンタをクリアします。 |
| **ipv6** *ip_address* | （任意）指定したネイバー IPv6 アドレスの BFD カウンタをクリアします。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

### 例

次に、すべての BFD カウンタをクリアする例を示します。

```
> clear bfd counters
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show bfd** | ドロップされたパケット、ネイバー、およびマップエントリを含む BFD プロトコル情報を表示します。 |

# clear bgp

ハードまたはソフト再構成を使用してボーダー ゲートウェイ プロトコル（BGP）接続をリセットするには、**clear bgp** コマンドを使用します。

**clear bgp** {[***** | **external** ] [**ipv4 unicast** [*as_number* | *neighbor_address* | **table-map**] | **ipv6 unicast** [*as_number* | *neighbor_address*]] [**soft**] [**in** | **out**] | *as_number* [**soft**] [**in** | **out**] | *neighbor_address* [**soft**] [**in** | **out**] | **table-map**}

## 構文の説明

| | |
|---|---|
| ***** | 現在のすべてのBGPセッションをリセットすることを指定します。 |
| *as_number* | （任意）すべての BGP ピア セッションがリセットされる自律システムの番号。 |
| **external** | 外部のすべてのBGPセッションをリセットすることを指定します。 |
| **in** | （オプション）インバウンド再構成を開始します。**in** と **out** のどちらのキーワードも指定しない場合は、インバウンドとアウトバウンドの両方のセッションがリセットされます。 |
| **ipv4 unicast** | IPv4 アドレス ファミリ セッションのハードまたはソフト再構成を使用して BGP 接続をリセットします。 |
| **ipv6 unicast** | IPv6 アドレス ファミリ セッションのハードまたはソフト再構成を使用して BGP 接続をリセットします。 |
| *neighbor_address* | （任意）指定された BGP ネイバーのみをリセットすることを指定します。この引数の値には、IPv4 アドレスまたは IPv6 アドレスを指定できます。 |
| **out** | （オプション）インバウンド再構成またはアウトバウンド再構成を開始します。**in** と **out** のどちらのキーワードも指定しない場合は、インバウンドとアウトバウンドの両方のセッションがリセットされます。 |
| **soft** | （任意）低速ピアのステータスを強制的にクリアして、元のアップデート グループに移します。 |
| **table-map** | BGP ルーティング テーブルの table-map 設定情報をクリアします。このコマンドを使用して、BGP ポリシー アカウンティング機能で設定されたトラフィック インデックス情報をクリアできます。 |

## 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

**clear bgp** コマンドを使用して、ハードリセットまたはソフト再構成を開始できます。ハードリセットは、指定されたピアリング セッションを切断して再構築し、BGP ルーティング テーブルを再構築します。ソフト再構成は、保存されたプレフィックス情報を使用し、既存のピアリング セッションを切断せずに BGP ルーティング テーブルの再構成とアクティブ化を行います。ソフト再構成では、保存されているアップデート情報が使用されます。アップデートを保存するために追加のメモリが必要になりますが、ネットワークを中断せずに、新しい BGP ポリシーを適用することができます。ソフト再構成は、インバウンドセッション、またはアウトバウンド セッションに対して設定できます。

### 例

次の例では、すべての BGP セッションが、リセットされます。

```
> clear bgp *
```

次の例では、ネイバー 10.100.0.1 とのインバウンド セッションに対してソフト再構成が開始され、アウトバウンド セッションは影響を受けません。

```
> clear bgp 10.100.0.1 soft in
```

次の例では、ルート リフレッシュ機能が BGP ネイバー ルータでイネーブルになっており、ネイバー 172.16.10.2 とのインバウンドセッションに対してソフト再構成が開始され、アウトバウンド セッションは影響を受けません。

```
> clear bgp 172.16.10.2 in
```

次の例では、自律システム番号 35700 のすべてのルータとのセッションに対してハード リセットが開始されます。

```
> clear bgp 35700
```

次の例では、すべてのインバウンド eBGP ピアリング セッションに対してソフト再構成が設定されます。

```
> clear bgp external soft in
```

次の例では、すべてのアウトバウンド アドレス ファミリ IPv4 マルチキャスト eBGP ピアリング セッションがクリアされます。

```
> clear bgp external ipv4 multicast out
```

次の例では、自律システム 65400 の IPv4 ユニキャスト アドレス ファミリ セッションで BGP ネイバーのインバウンド セッションに対してソフト再構成が開始され、アウトバウンド セッションは影響を受けません。

```
> clear bgp ipv4 unicast 65400 soft in
```

次の例では、asplain 表記の 4 バイトの自律システム番号 65538 の IPv4 ユニキャスト アドレス ファミリ セッションで BGP ネイバーに対してハード リセットが開始されます。

```
> clear bgp ipv4 unicast 65538
```

次の例では、asdot 表記の 4 バイトの自律システム番号 1.2 の IPv4 ユニキャスト アドレス ファミリ セッションで BGP ネイバーに対してハード リセットが開始されます。

```
> clear bgp ipv4 unicast 1.2
```

次の例は、IPv4 ユニキャスト ピアリング セッションのテーブル マップをクリアします。

```
> clear bgp ipv4 unicast table-map
```

# clear blocks

枯渇状態や履歴情報などのパケットバッファカウンタをリセットするには、**clear blocks** コマンドを使用します。

**clear blocks** ［**exhaustion** ｛**history** ｜ **snapshot**｝ ｜ **export-failed** ｜ **queue** ［**history** ［**core-local** ［*number*］］］］

## 構文の説明

| | |
|---|---|
| **core-local** [*number*] | （任意）すべてのコア、またはコア番号を指定する場合は特定のコアに対し、アプリケーションによってキューに入れられたシステムバッファをクリアします。 |
| **exhaustion** | （任意）枯渇状態をクリアします。 |
| **export-failed** | （任意）エクスポート失敗カウンタをクリアします。 |
| **history** | （任意）履歴をクリアします。 |
| **queue** | （任意）キューに入れられたブロックをクリアします。 |
| **snapshot** | （任意）スナップショット情報をクリアします。 |

## 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

最低水準点カウンタを各プール内で現在使用可能なブロックにリセットします。また、このコマンドは、前回のバッファ割り当ての失敗時に保存された履歴情報をクリアします。

### 例

次に、ブロックをクリアする例を示します。

```
> clear blocks
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **blocks** | ブロック診断に割り当てるメモリを増やします。 |
| **show blocks** | システム バッファの使用状況を表示します。 |

# clear capture

キャプチャバッファをクリアするには、**clear capture** コマンドを使用します。

**clear capture** {**/all** | *capture_name*}

## 構文の説明

| | |
|---|---|
| **/all** | すべてのインターフェイス上のパケットをクリアします。 |
| *capture_name* | パケット キャプチャの名前を指定します。 |

## 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。 |

### 例

次に、キャプチャバッファ「example」のキャプチャバッファをクリアする例を示します。

```
> clear capture example
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **capture** | パケット スニッフィングおよびネットワーク障害の切り分けのためにパケット キャプチャ機能をイネーブルにします。 |
| **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。 |

# clear clns

コネクションレスモードネットワーク プロトコル（CLNP）情報をクリアするには、**clear clns** コマンドを使用します。

**clear clns** {**is-neighbors** | **neighbors** | **traffic**}

## 構文の説明

| | |
|---|---|
| **is-neighbors** | 中間システムのネイバールートをクリアします。 |
| **neighbors** | すべての CLNS ネイバールートをクリアします。 |
| **traffic** | CLNS プロトコル統計情報をクリアします。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

### 例

次に、すべての CLNS ネイバールートをクリアする例を示します。

```
> clear clns neighbors
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show clns** | コネクションレスモードネットワーク プロトコル（CLNP）ネットワーク情報を表示します。 |

# clear cluster info

クラスタの統計情報をクリアするには、**clear cluster info** コマンドを使用します。

**clear cluster info** {**flow-mobility counters** | **health details** | **trace** | **transport**}

## 構文の説明

| | |
|---|---|
| **flow-mobility counters** | クラスタ フローモビリティ カウンタをクリアします。 |
| **health details** | クラスタ ヘルス情報をクリアします。 |
| **trace** | クラスタ イベント トレース情報をクリアします。 |
| **transport** | クラスタ転送統計情報をクリアします。 |

## 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

クラスタ統計情報を表示するには、show cluster info コマンドを使用します。

### 例

次に、クラスタ イベント トレース情報をクリアする例を示します。

```
> clear cluster info trace
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show cluster info** | クラスタ統計情報を表示します。 |

# clear configure key chain

設定されているキーチェーンを削除するには、**clear configure key chain** コマンドを使用します。

**clear configure key chain***key-chain-name*

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.4 | このコマンドが導入されました。 |

## 使用上のガイドライン

**clear configure key chain** コマンドを使用して、設定されているキーチェーンを削除します。

### 例

次に、設定されているキーチェーンを削除する例を示します。

```
> clear configure key chain CHAIN1
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **key chain** | OSPFv2 認証用のキーチェーンを設定します。 |
| **show key chain** | 設定されているキーチェーンを表示します。 |
| **show running key chain** | 現在アクティブなキーチェーンの詳細を表示します。 |

# clear conn

特定の接続または複数の接続をクリアするには、**clear conn** コマンドを使用します。

**clear conn** ［ **vrf** ｛ *name* ｜ **global** ｝］ ｛ **all** ｜ **protocol** ｛ **tcp** ｜ **udp** ｜ **sctp** ｝ ｜ **address** *ip* ［ **-** *ip* ］ ［ *netmask mask* ］ ｜ **port** *port* ［ **-** *port* ］ ｜ **inline-set** *name* ｜ **security-group** ｛ **name** ｜ **tag** ｝ *attribute* ｝ ｜ **user** ［ *domain_nickname* **** ］ *user_name* ｜ **user-group** ［ *domain_nickname* **** ］ *user_group_name* ］ ｜ **zone** ［ *zone_name* ］ ［ **data-rate** ］ ｝

## 構文の説明

| | |
|---|---|
| **address** *ip*[**-***ip*] | 指定された送信元または宛先の IP アドレス（IPv4 または IPv6）との接続をクリアします。範囲を指定するには、IP アドレスをダッシュ（-）で区切ります。例：10.1.1.1-10.1.1.5 |
| **all** | to-the-box 接続を含む、すべての接続をクリアします。all キーワードを指定しない場合は、through-the-box 接続だけがクリアされます。 |
| **inline-set** *name* | 指定したインラインセットに一致する接続をクリアします。 |
| **netmask** *mask* | （任意）指定された IP アドレスで使用するサブネットマスクを指定します。 |
| **port** *port*[**-***port*] | 指定された送信元ポートまたは宛先ポートとの接続をクリアします。範囲を指定するには、ポート番号をダッシュ（-）で区切ります。例：1000-2000 |
| **protocol** {**tcp** \| **udp** \| **sctp**} | 指定したプロトコルが設定されている接続をクリアします。 |
| **security-group** {**name** \| **tag**} *attribute* | 指定したセキュリティグループ属性が設定されている接続をクリアします。 |
| **user** [*domain_nickname*****] *user_name* | 指定したユーザーに属する接続をクリアします。*domain_nickname* 引数を含めない場合、システムはデフォルトドメイン内のユーザーの接続をクリアします。 |
| **user-group** [*domain_nickname*****] *user_group_name*] | 指定したユーザーグループに属する接続をクリアします。*domain_nickname* 引数を含めない場合、システムはデフォルトドメイン内のユーザーグループの接続をクリアします。 |
| **zone** [*zone_name*] | セキュリティゾーンに属する接続をクリアします。 |
| ［**vrf** ｛*name* ｜ **global**｝］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。コマンドをグローバル仮想ルータに限定するには、**vrf global** を指定します。このキーワードを省略すると、コマンドはすべての仮想ルータに適用されます。 |

| | |
|---|---|
| **data-rate** | （任意）保存されている現在の最大データレートをクリアします。 |

## 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。 |
| 6.6 | **vrf** および **data-rate** キーワードが追加されました。 |

## 使用上のガイドライン

コンフィギュレーションに対してセキュリティポリシーの変更を加えた場合は、すべての新しい接続で新しいセキュリティポリシーが使用されます。既存の接続では、その接続が確立された時点で設定されていたポリシーの使用が続行されます。すべての接続で新しいポリシーが確実に使用されるようにするには、**clear conn** コマンドを使用して、現在の接続を切断し、新しいポリシーを使用して再接続できるようにする必要があります。または、ホスト単位で接続をクリアするための **clear local-host** コマンドを使用したり、ダイナミック NAT を使用する接続用の **clear xlate** コマンドを使用したりすることもできます。

セカンダリ接続を許可するためのピンホールをデバイスが作成している場合は、これが **show conn** コマンドの出力に不完全な接続として表示されます。この不完全な接続をクリアするには、**clear conn** コマンドを使用します。

（注） このコマンドは、管理インターフェイスへの接続をクリアしません。データインターフェイスまたは診断インターフェイスへの管理接続のみをクリアできます。

### 例

すべての接続を表示して、10.10.10.108 からの管理接続をクリアする例を次に示します。

```
> show conn all
TCP mgmt 10.10.10.108:4168 NP Identity Ifc 10.0.8.112:22, idle 0:00:00,
bytes 3084, flags UOB
> clear conn address 10.10.10.108
```

次の例では、拡張メモリに保存されている接続の最大データレートをクリアする方法について示します。

```
> clear conn data-rate
Released conn extension memory for 10 connection(s)
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear local-host** | 特定のローカル ホストまたはすべてのローカル ホストによるすべての接続をクリアします。 |

| コマンド | 説明 |
| --- | --- |
| **clear xlate** | ダイナミック NAT セッションおよび NAT を使用しているすべての接続をクリアします。 |
| **show conn** | 接続情報を表示します。 |
| **show local-host** | ローカル ホストのネットワーク状態を表示します。 |
| **show xlate** | NAT セッションを表示します。 |

# clear console-output

現在キャプチャされているコンソール出力を削除するには、**clear console-output** コマンドを使用します。

**clear console-output**

## 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、現在キャプチャされているコンソール出力を削除する例を示します。

```
> clear console-output
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show console-output** | キャプチャされているコンソール出力を表示します。 |
| **show running-config console timeout** | デバイスに対するコンソール接続のアイドルタイムアウトを表示します。 |

# clear counters

プロトコルスタックカウンタをクリアするには、**clear counters** コマンドを使用します。

**clear counters** ［**all** | **summary** | **top** *n*］［**detail**］［**protocol** *protocol_name* ［*counter_name*］］［**threshold** *n*］

## 構文の説明

| | |
|---|---|
| **all** | （任意）すべてのフィルタ詳細をクリアします。 |
| *counter_name* | （任意）名前でカウンタを指定します。使用可能なカウンタ名を表示するには、**show counters protocol** コマンドを使用します。 |
| **detail** | （任意）カウンタの詳細情報をクリアします。 |
| **protocol** *protocol_name* | （任意）指定したプロトコルのカウンタをクリアします。 |
| **summary** | （任意）カウンタの要約をクリアします。 |
| **threshold** *n* | （任意）指定されたしきい値以上になっているカウンタをクリアします。指定できる範囲は 1 ～ 4294967295 です。 |
| **top** *n* | （任意）指定されたしきい値以上になっているカウンタをクリアします。指定できる範囲は 1 ～ 4294967295 です。 |

## コマンド デフォルト

**clear counters summary detail** コマンドはデフォルトです。

## 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、プロトコル スタック カウンタをクリアする例を示します。

```
> clear counters
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show counters** | プロトコル スタック カウンタを表示します。 |

# clear cpu profile

CPU プロファイリングの統計情報をクリアするには、**clear cpu** コマンドを使用します。

**clear cpu profile**

## 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、クラッシュ ファイルを削除する例を示します。

```
> clear cpu profile
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show cpu** | CPU に関する情報を表示します。 |
| **show cpu profile** | CPU プロファイリング データを表示します。 |

# clear crashinfo

フラッシュメモリ内のクラッシュファイルの内容を削除するには、**clear crashinfo** コマンドを使用します。

**clear crashinfo** ［**module** {**0** | **1**}］

## 構文の説明

| | |
|---|---|
| **module** {**0** | **1**} | （任意）スロット 0 または 1 のモジュールのクラッシュ ファイルをクリアします。 |

## 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、クラッシュ ファイルを削除する例を示します。

```
> clear crashinfo
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **crashinfo force** | システムを強制的にクラッシュさせます。 |
| **crashinfo test** | フラッシュメモリ内のファイルにクラッシュ情報を保存できるかどうかをテストします。 |
| **show crashinfo** | フラッシュ メモリに格納されているクラッシュ ファイルの内容を表示します。 |

# clear crypto accelerator statistics

クリプトアクセラレータ MIB からグローバルおよびアクセラレータ固有の統計情報をクリアするには、**clear crypto accelerator statistics** コマンドを使用します。

**clear crypto accelerator statistics**

## 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、グローバル コンフィギュレーション モードで、クリプト アクセラレータの統計情報を表示する例を示します。

```
> clear crypto accelerator statistics
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear crypto protocol statistics** | 暗号アクセラレータ MIB にあるプロトコル固有の統計情報をクリアします。 |
| **show crypto accelerator statistics** | 暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報を表示します。 |
| **show crypto protocol statistics** | 暗号アクセラレータ MIB からプロトコル固有の統計情報を表示します。 |

# clear crypto ca crls

指定したトラストポイントに関連付けられたすべての CRL の CRL キャッシュをクリアするか、trustpool に関連付けられたすべての CRL をキャッシュからクリアするか、またはすべての CRL の CRL キャッシュをクリアするには、**clear crypto ca crls** コマンドを使用します。

**clear crypto ca crls** ［**trustpool** | **trustpoint** *trust_point_name*］

## 構文の説明

| | |
|---|---|
| **trustpoint** *trust_point_name* | トラストポイントの名前。名前を指定しない場合、このコマンドはシステム上のキャッシュされた CRL をすべてクリアします。trustpointname を指定せず trustpoint キーワードを指定した場合、コマンドは失敗します。 |
| **trustpool** | trustpool 内の証明書に関連付けられた CRL にのみアクションが適用されることを示します。 |

## 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、デバイスからすべての trustpool CRL をクリアする例、trustpoint123 に関連付けられたすべての CRL をクリアする例、およびすべてのキャッシュされた CRL を削除する例を個別に示します。

```
> clear crypto ca crl trustpool
> clear crypto ca crl trustpoint trustpoint123
> clear crypto ca crl
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show crypto ca crl** | キャッシュされたすべての CRL、または指定したトラストポイントのキャッシュされた CRL を表示します。 |

# clear crypto ca trustpool

trustpool からすべての証明書を削除するには、**clear crypto ca trustpool** コマンドを使用します。

**clear crypto ca trustpool noconfirm**

## 構文の説明

| | |
|---|---|
| **noconfirm** | ユーザー確認プロンプトを抑制し、コマンドが要求どおりに処理されます。 |

## 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、すべての証明書をクリアする例を示します。

```
> clear crypto ca trustpool
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **crypto ca trustpool export** | PKI trustpool を構成する証明書をエクスポートします。 |
| **crypto ca trustpool import** | PKI trustpool を構成する証明書をインポートします。 |
| **crypto ca trustpool remove** | 指定された 1 つの証明書を trustpool から削除します。 |

# clear crypto ikev1

IPsec IKEv2 SA または統計情報を削除するには、**clear crypto ikev1** コマンドを使用します。

**clear crypto ikev1** {**sa** [*ip_address* ] | **stats**}

## 構文の説明

| | |
|---|---|
| **sa** *ip_address* | SA をクリアします。すべての IKEv1 SA をクリアするには、IP アドレスを指定せずにこのオプションを使用します。それ以外の場合は、クリアする SA の IPv4 アドレスまたは IPv6 アドレスを指定します。 |
| **stats** | IKEv1 統計情報をクリアします。 |

## 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、脅威に対する防御 デバイスからすべての IPsec IKEv1 の統計を削除する例を示します。

```
> clear crypto ikev1 stats
>
```

次に、10.86.1.1 のピア IP アドレスを持つ SA を削除する例を示します。

```
> clear crypto ikev1 sa 10.86.1.1
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipsec sa** | カウンタ、エントリ、マップ名、ピア IP アドレス、ホスト名などの IPSec SA に関する情報を表示します。 |
| **show running-config crypto** | IPsec、クリプト マップ、ダイナミック クリプト マップ、ISAKMP など、暗号コンフィギュレーション全体を表示します。 |

# clear crypto ikev2

IPsec IKEv2 SA または統計情報を削除するには、**clear crypto ikev2** コマンドを使用します。

**clear crypto ikev2** {**sa** [*ip_address* ] | **stats**}

## 構文の説明

| | |
|---|---|
| **sa** *ip_address* | SA をクリアします。すべての IKEv2 SA をクリアするには、IP アドレスを指定せずにこのオプションを使用します。それ以外の場合は、クリアする SA の IPv4 アドレスまたは IPv6 アドレスを指定します。 |
| **stats** | IKEv2 統計情報をクリアします。 |

## 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、脅威に対する防御 デバイスからすべての IPsec IKEv2 の統計を削除する例を示します。

```
> clear crypto ikev2 stats
>
```

次に、10.86.1.1 のピア IP アドレスを持つ SA を削除する例を示します。

```
> clear crypto ikev2 sa 10.86.1.1
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipsec sa** | カウンタ、エントリ、マップ名、ピア IP アドレス、ホスト名などの IPSec SA に関する情報を表示します。 |
| **show running-config crypto** | IPsec、クリプト マップ、ダイナミック クリプト マップ、ISAKMP など、暗号コンフィギュレーション全体を表示します。 |

# clear crypto ipsec sa

IPsec SA のカウンタ、エントリ、クリプトマップ、またはピア接続を削除するには、**clear crypto ipsec sa** コマンドを使用します。

**clear crypto ipsec sa** ［**counters** | **entry** *ip_address* {**esp** | **ah**} *spi* | **inactive** | **map** *map_name* | **peer** *ip_address*］

## 構文の説明

| | |
|---|---|
| **ah** | 認証ヘッダー。 |
| **counters** | 各 SA 統計情報のすべての IPsec をクリアします。 |
| **entry** *ip_address* | 指定した IP アドレス、ホスト名、プロトコル、および SPI 値に一致するトンネルを削除します。 |
| **esp** | 暗号化セキュリティ プロトコル。 |
| **inactive** | すべての非アクティブな IPsec SA をクリアします。 |
| **map** *map_name* | マップ名で識別される、指定したクリプトマップに関連付けられているすべてのトンネルを削除します。 |
| **peer** *ip_address* | 指定したホスト名または IP アドレスで識別されるピアへのすべての IPsec SA を削除します。 |
| *spi* | セキュリティ パラメータ インデックス（16 進数）を指定します。受信 SPI である必要があります。このコマンドは、送信 SPI ではサポートされていません。 |

## 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

すべての IPsec SA をクリアするには、このコマンドを引数なしで使用します。

### 例

次に、脅威に対する防御 からすべての IPsec SA を削除する例を示します。

```
> clear crypto ipsec sa
>
```

次に、10.86.1.1 のピア IP アドレスを持つ SA を削除する例を示します。

```
> clear crypto ipsec sa peer 10.86.1.1
```

関連コマンド

| Command | 説明 |
|---|---|
| **show ipsec sa** | カウンタ、エントリ、マップ名、ピア IP アドレス、ホスト名などの IPSec SA に関する情報を表示します。 |
| **show running-config crypto** | IPsec、クリプト マップ、ダイナミック クリプト マップ、ISAKMP など、暗号コンフィギュレーション全体を表示します。 |

# clear crypto isakmp

ISAKMP SA または統計情報をクリアするには、**clear crypto isakmp** コマンドを使用します。

**clear crypto isakmp** ［**sa** | **stats**］

## 構文の説明

| | |
|---|---|
| **sa** | IKEv1 および IKEv2 SA をクリアします。 |
| **stats** | IKEv1 および IKEv2 統計情報をクリアします。 |

## 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

すべての ISAKMP 運用データをクリアするには、このコマンドを引数なしで使用します。

### 例

次に、すべての ISAKMP SA を削除する例を示します。

```
> clear crypto isakmp sa
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show isakmp** | ISAKMP 運用データに関する情報を表示します。 |
| **show running-config crypto** | IPsec、クリプト マップ、ダイナミック クリプト マップ、ISAKMP など、暗号コンフィギュレーション全体を表示します。 |

# clear crypto protocol statistics

クリプトアクセラレータ MIB にあるプロトコル固有の統計情報をクリアするには、**clear crypto protocol statistics** コマンドを使用します。

**clear crypto protocol statistics** *protocol*

## 構文の説明

| | |
|---|---|
| *protocol* | 統計情報をクリアするプロトコルの名前を指定します。プロトコルの選択肢は次のとおりです。<br>• **all**：現在サポートされているすべてのプロトコル。<br>• **ikev1**：インターネット キー エクスチェンジ（IKE）バージョン 1。<br>• **ikev2**：インターネット キー エクスチェンジ（IKE）バージョン 2。<br>• **ipsec**：IP セキュリティ（IPsec）フェーズ 2 プロトコル。<br>• **other**：新規プロトコル用に予約済み。<br>• **srtp**：セキュア RTP（SRTP）プロトコル。<br>• **ssh**：セキュアシェル（SSH）プロトコル。<br>• **ssl**：セキュアソケットレイヤ（SSL）プロトコル。 |

## 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、すべての暗号化アクセラレータ統計情報をクリアする例を示します。

```
> clear crypto protocol statistics all
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear crypto accelerator statistics** | 暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報をクリアします。 |
| **show crypto accelerator statistics** | 暗号アクセラレータ MIB からグローバルおよびアクセラレータ固有の統計情報を表示します。 |

| Command | 説明 |
| --- | --- |
| **show crypto protocol statistics** | クリプト アクセラレータ MIB のプロトコル固有の統計情報を表示します。 |

# clear crypto ssl

SSL 情報をクリアするには、**clear crypto ssl** コマンドを使用します。

**clear crypto ssl** {**cache** [**all**] | **errors** | **mib** | **objects**}

## 構文の説明

| | |
|---|---|
| **cache** | SSLセッションキャッシュ内の期限切れセッションをクリアします。 |
| **all** | （任意）SSL セッション キャッシュ内のすべてのセッションおよび統計情報をクリアします。 |
| **errors** | SSL エラーをクリアします。 |
| **mib** | SSL MIB 統計情報をクリアします。 |
| **objects** | SSL オブジェクト統計情報をクリアします。 |

## 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、すべての SSL キャッシュ セッションおよび統計情報をクリアする例を示します。

```
> clear crypto ssl cache all
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show crypto ssl** | SSL 情報を表示します。 |

# clear dhcpd

DHCP サーバーのバインディングおよび統計情報をクリアするには、**clear dhcpd** コマンドを使用します。

**clear dhcpd** {**binding** [**all** | *ip_address* ] | **statistics**}

## 構文の説明

| | |
|---|---|
| **all** | （任意）すべての dhcpd バインディングをクリアします。 |
| **binding** | クライアント アドレスのすべてのバインディングをクリアします。 |
| *ip_address* | （任意）指定した IP アドレスのバインディングをクリアします。 |
| **statistics** | 統計情報カウンタをクリアします。 |

## 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、dhcpd 統計情報をクリアする例を示します。

```
> clear dhcpd statistics
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show dhcpd** | DHCP のバインディング、統計情報、または状態情報を表示します。 |

# clear dhcprelay statistics

DHCP リレー統計情報カウンタをクリアするには、**clear dhcprelay statistics** コマンドを使用します。

**clear dhcprelay statistics**

## 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、DHCP リレー統計情報をクリアする例を示します。

```
> clear dhcprelay statistics
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show dhcprelay statistics** | DHCP リレー エージェントの統計情報を表示します。 |
| **show running-config dhcprelay** | DHCP リレー エージェントの現在のコンフィギュレーションを表示します。 |

# clear dns

完全修飾ドメイン名（FQDN）ホストに関連付けられた IP アドレスをクリアするには、DNS 要求によって解決されているため、**clear dns** コマンドを使用します。

**clear dns** ［ **host** *fqdn_name* ］ ［ **ipcache** ［ **counters** ］］

## 構文の説明

| | |
|---|---|
| **host** *fqdn_name* | （任意）IPアドレスをクリアする完全修飾ドメイン名を指定します。ホストを指定しない場合、すべての DNS 解決がクリアされます。 |
| **ipcache** ［**counters**］ | ダイレクト インターネット アクセスのポリシーベースのルーティングで使用される DNS スヌーピングを通じて取得した IP キャッシュからすべてのエントリがクリアされます。<br>キャッシュ内のエントリを削除せずにそれらのヒットカウントをすべてリセットするだけの場合は、**counters** を指定します。 |

## 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。 |
| 7.1 | **ipcache** ［**counters**］キーワードが追加されました。 |

### 例

次に、指定した FQDN ホストに関連付けられた IP アドレスをクリアする例を示します。

```
> clear dns host www.example.com
```

次に、IP キャッシュをクリアする例を示します。IP キャッシュを削除すると、システムはネットワーク サービス オブジェクトおよびオブジェクトグループ内のドメイン名の新しい DNS クエリを使用してキャッシュを再度設定します。DNS クエリが完了するまで、ドメイン名宛てのトラフィックは、クリアされたIPキャッシュエントリのドメイン名を含むネットワークサービス グループに分類されなくなります。

```
> clear dns ip-cache
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show dns hosts** | 特定のホストの DNS 解決を表示します。 |

# clear dns-hosts cache

DNS キャッシュをクリアするには、**clear dns-hosts cache** コマンドを使用します。

**clear dns-hosts cache**

## 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、DNS キャッシュをクリアする例を示します。

```
> clear dns-hosts cache
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show dns-hosts** | DNS キャッシュを表示します。 |

# clear efd-throttle

スロットルされたエレファントフローからスロットルをクリアし、Snort インスペクションをバイパスするには、**clear efd-throttle** コマンドを使用します。

**clear efd-throttle** { *IPv4_address* | *IPv6_address/prefix* | **all bypass** | **any** { *source_port* { *destination_IPv4_address* | *destination_IPv6_address/prefix* | **any** } | **any** { *destination_IPv4_address* | *destination_IPv6_address/prefix* | **any** { *destination_port* { **tcp bypass** | **udp bypass** } | **any** { **tcp bypass** | **udp bypass** } } } } }

## 構文の説明

| | |
|---|---|
| *IPv4_address* | 指定した IPv4 アドレス（5 タプル）のスロットルされたエレファントフローをクリアします。 |
| *IPv6_address/prefix* | 指定した IPv6 アドレスのスロットルされたエレファントフローをクリアします。 |
| **all** | スロットルをクリアし、すべてのエレファントフローを検査します。 |
| **bypass** | （任意）スロットルをクリアし、すべてのエレファントフローの Snort インスペクションをバイパスします。 |
| **any** | • 送信元アドレスとマスク 0.0.0.0 0.0.0.0 と ::/0 の省略形として使用します。<br>• 任意の送信元ポートまたは宛先ポートに使用します。 |
| *source_port* | 指定した送信先ポートとの接続のスロットルをクリアします。 |
| *destination_port* | 指定した宛先ポートとの接続のスロットルをクリアします。 |
| **tcp** | TCP 接続のスロットルのみをクリアします。 |
| **udp** | UDP 接続のスロットルのみをクリアします。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2 | このコマンドが導入されました。 |

### 例

次に、スロットルされたエレファントフローのスロットルをクリアし、そのフローで Snort インスペクションを続行する例を示します。

```
> clear efd-throttle 172.16.77.0 255.255.255.0 1234 172.16.4.0 255.255.255.0 80 tcp
```

次に、スロットルされたエレファントフローのスロットルをクリアし、そのフローの Snort インスペクションをバイパスする例を示します。

```
> clear efd-throttle 172.16.77.0 255.255.255.0 1234 172.16.4.0 255.255.255.0 80 tcp
bypass
```

次に、スロットルされたすべてのエレファントフローのスロットルをクリアし、それらのすべてのフローで Snort インスペクションを続行する例を示します。

```
> clear efd-throttle all
```

次に、スロットルされたすべてのエレファントフローのスロットルをクリアし、それらのすべてのフローの Snort インスペクションをバイパスする例を示します。

```
> clear efd-throttle all bypass
```

# clear eigrp events

EIGRP イベントログをクリアするには、**clear eigrp events** コマンドを使用します。

**clear eigrp** ［*as_number*］ **events**

## 構文の説明

| | |
|---|---|
| *as_number* | （任意）イベント ログをクリアする EIGRP プロセスの自律システム番号を指定します。デバイスでサポートされる EIGRP ルーティング プロセスは 1 つのみであるため、自律システム番号（プロセス ID）を指定する必要はありません。 |

## 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

**show eigrp events** コマンドを使用して、EIGRP イベントログを表示できます。

### 例

次に、EIGRP イベント ログをクリアする例を示します。

```
> clear eigrp events
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show eigrp events** | EIGRP イベント ログを表示します。 |

# clear eigrp neighbors

EIGRP ネイバーテーブルからエントリを削除するには、**clear eigrp neighbors** コマンドを使用します。

**clear eigrp** ［*as_number*］ **neighbors** ［*ip_addr* | *if_name*］［**soft**］

## 構文の説明

| | |
|---|---|
| *as_number* | （任意）ネイバー エントリを削除する EIGRP プロセスの自律システム番号を指定します。デバイスでサポートされる EIGRP ルーティング プロセスは 1 つだけなので、自律システム番号（AS）（プロセス ID）を指定する必要はありません。 |
| *if_name* | （任意）インターフェイスの名前。インターフェイス名を指定すると、このインターフェイスを介して学習されたすべてのネイバーテーブル エントリが削除されます。 |
| *ip_addr* | （任意）ネイバー テーブルから削除するネイバーの IP アドレス。 |
| **soft** | デバイスは、隣接関係をリセットすることなくネイバーと再同期されます。 |

## コマンド デフォルト

ネイバー IP アドレスまたはインターフェイス名を指定しない場合は、すべてのダイナミック エントリがネイバー テーブルから削除されます。

## 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

**clear eigrp neighbors** コマンドでは、手動で定義されたネイバーはネイバーテーブルから削除されません。ダイナミックに検出されたネイバーだけが削除されます。

**show eigrp neighbors** コマンドを使用して、EIGRP ネイバーテーブルを表示できます。

### 例

次に、EIGRP ネイバー テーブルからすべてのエントリを削除する例を示します。

```
> clear eigrp neighbors
```

次に、「outside」という名前のインターフェイスを介して学習されたすべてのエントリを EIGRP ネイバー テーブルから削除する例を示します。

```
> clear eigrp neighbors outside
```

関連コマンド

| Command | 説明 |
| --- | --- |
| **show eigrp neighbors** | EIGRP ネイバー テーブルを表示します。 |

# clear eigrp topology

EIGRP トポロジテーブルからエントリを削除するには、**clear eigrp topology** コマンドを使用します。

**clear eigrp** ［*as_number*］ **topology** *ip_addr* ［*mask*］

## 構文の説明

| | |
|---|---|
| *as_number* | （任意）EIGRP プロセスの自律システム番号を指定します。デバイスでサポートされる EIGRP ルーティングプロセスは 1 つだけなので、自律システム番号（AS）（プロセス ID）を指定する必要はありません。 |
| *ip_addr* | トポロジ テーブルからクリアする IP アドレス。 |
| *mask* | （任意）*ip-addr* 引数に適用するネットワーク マスク。 |

## 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、EIGRP トポロジ テーブルから既存の EIGRP エントリをクリアします。**show eigrp topology** コマンドを使用して、トポロジ ーブルのエントリを表示できます。

### 例

次に、EIGRP トポロジテーブルから 192.168.1.0 ネットワークのエントリを削除する例を示します。

```
> clear eigrp topology 192.168.1.0 255.255.255.0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show eigrp topology** | EIGRP トポロジ テーブルを表示します。 |

# clear f - clear z

# clear facility-alarm output

ISA 3000 で出力リレーの電源を切って、LED のアラーム状態をクリアするには、**clear facility-alarm output** コマンドを使用します。

**clear facility-alarm output**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | 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、出力リレーの電源を切り、出力 LED のアラーム状態をクリアします。これにより、外部アラームがオフになります。ただし、このコマンドを実行しても、外部アラームをトリガーしたアラーム条件は修正されません。問題を解決する必要があります。現在のアラーム条件を確認するには、**show facility-alarm status** コマンドを使用します。

### 例

次に、出力リレーの電源を切り、出力 LED のアラーム状態をクリアする例を示します。

```
> clear facility-alarm output
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show alarm settings** | すべてのグローバル アラーム設定を表示します。 |
| **show environment alarm-contact** | 入力アラーム コンタクトのステータスを表示します。 |
| **show facility-alarm** | トリガーされたアラームのステータス情報を表示します。 |

# clear failover statistics

高可用性統計情報カウンタをクリアするには、**clear failover statistics** コマンドを使用します。

**clear failover statistics**

## 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 failover statistics** コマンドで表示される統計情報、および **show failover** コマンド出力の Stateful Failover Logical Update Statistics セクションのカウンタをクリアします。

### 例

次に、高可用性統計情報カウンタをクリアする例を示します。

```
> clear failover statistics
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show failover** | 高可用性構成および動作統計に関する情報を表示します。 |

# clear flow-export counters

NetFlow 統計情報とエラーデータのランタイムカウンタを 0 にリセットするには、**clear flow-export counters** コマンドを使用します。

**clear flow-export counters**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

### 例

次に、NetFlow のランタイム カウンタをリセットする例を示します。

```
> clear flow-export counters
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show flow-export counters** | NetFlow のすべてのランタイム カウンタを表示します。 |

# clear flow-offload

オフロードされたフローのカウンタと統計情報をクリアするには、**clear flow-offload** コマンドを使用します。

このコマンドは Firepower 4100/9300 シャーシ の 脅威に対する防御で使用できます。

**clear flow-offload statistics**

## 構文の説明

| | |
|---|---|
| **statistics** | すべてのオフロードされたフローの統計情報をゼロにリセットします。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

### 例

次に、すべてのフローカウンタをクリアする例を示します。

```
> clear flow-offload statistics
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show flow-offload** | ダイナミック フロー オフロード カウンタ、統計情報、および情報を表示します。 |
| **configure flow-offload** | ダイナミック フロー オフロードを有効または無効にします。 |

# clear flow-offload-ipsec

IPsec フローオフロードに関する情報をクリアするには、**clear flow-offload-ipsec** コマンドを使用します。

**clear flow-offload-ipsec statistics**

## 構文の説明

| | |
|---|---|
| **statistics** | IPsec フローオフロード関連の統計をクリアします。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2 | このコマンドが導入されました。 |

### 例

次に、すべての IPsec フローオフロード統計をクリアする例を示します。

```
> clear flow-offload-ipsec statistics
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show flow-offload-ipsec** | IPsec フローオフロード統計および情報を表示します。 |

# clear fragment

IP フラグメント再構成モジュールの動作データをクリアするには、**clear fragment** コマンドを入力します。

**clear fragment** {**queue** | **statistics** [*interface_name*]}

## 構文の説明

| | |
|---|---|
| **queue** | IP フラグメント再構築キューをクリアします。 |
| **statistics** *interface_name* | IP フラグメント再構築統計情報をクリアします。必要に応じて、そのインターフェイスの統計情報のみをクリアするインターフェイス名を指定できます。指定しない場合、すべてのインターフェイスの統計情報がクリアされます。 |

## 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

このコマンドは、現在キューに入っている再構築待機中のフラグメント（**queue** キーワードが入力されている場合）、またはすべての IP フラグメント再構築統計情報（**statistics** キーワードが入力されている場合）のいずれかをクリアします。統計情報は、再構築に成功したフラグメントチェーンの数、再構築に失敗したチェーンの数、および最大サイズの超過によってバッファ オーバーフローが発生した回数を示すカウンタです。

### 例

次に、IP フラグメント再構成モジュールの運用データをクリアする例を示します。

```
> clear fragment queue
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show fragment** | IP フラグメント再構成モジュールの動作データを表示します。 |
| **show running-config fragment** | IP フラグメント再構成コンフィギュレーションを表示します。 |

# clear gc

ガベージコレクション（GC）プロセスの統計情報を表示するには、**clear gc** コマンドを使用します。

**clear gc**

## 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、GC プロセスの統計情報を削除する例を示します。

```
> clear gc
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show gc** | GC のプロセスの統計情報を表示します。 |

# clear igmp

すべてのIGMPカウンタ、グループキャッシュ、およびトラフィックをクリアするには、**clear igmp** コマンドを使用します。

**clear igmp** {**counters** ［*if_name*］ | **group** ［**interface** *name*］ | **traffic**}

## 構文の説明

| | |
|---|---|
| **counters** [*if_name*] | IGMP統計カウンタをクリアします。必要に応じて、インターフェイス名を指定して、該当インターフェイスのカウンタだけをクリアできます。 |
| **group** [**interface** *name*] | IGMPグループキャッシュエントリを削除します。必要に応じて、インターフェイス名を指定して、該当インターフェイスにのみ関連付けられているグループを削除できます。<br>このコマンドは、スタティックに設定されたグループをクリアしません。 |
| **traffic** | トラフィックカウンタをクリアします。 |

## 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、IGMP 統計情報カウンタをクリアする例を示します。

```
> clear igmp counters
```

次に、検出されたすべての IGMP グループを IGMP グループ キャッシュからクリアする例を示します。

```
> clear igmp group
```

次に、IGMP 統計情報トラフィック カウンタをクリアする例を示します。

```
> clear igmp traffic
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show igmp** | IGMP 情報を表示します。 |

# clear ikev1

IPsec IKEv2 SA または統計情報を削除するには、**clear ikev1** コマンドを使用します。

**clear ikev1** {**sa** [*ip_address* ] | **stats**}

## 構文の説明

| | |
|---|---|
| **sa** *ip_address* | SA をクリアします。すべての IKEv1 SA をクリアするには、IP アドレスを指定せずにこのオプションを使用します。それ以外の場合は、クリアする SA の IPv4 アドレスまたは IPv6 アドレスを指定します。 |
| **stats** | IKEv1 統計情報をクリアします。 |

## 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、脅威に対する防御 デバイスからすべての IPsec IKEv1 の統計を削除する例を示します。

```
> clear ikev1 stats
>
```

次に、10.86.1.1 のピア IP アドレスを持つ SA を削除する例を示します。

```
> clear ikev1 sa 10.86.1.1
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipsec sa** | カウンタ、エントリ、マップ名、ピア IP アドレス、ホスト名などの IPSec SA に関する情報を表示します。 |
| **show running-config crypto** | IPsec、クリプト マップ、ダイナミック クリプト マップ、ISAKMP など、暗号コンフィギュレーション全体を表示します。 |

# clear ikev2

IPsec IKEv2 SA または統計情報を削除するには、**clear ikev2** コマンドを使用します。

**clear ikev2** {**sa** [*ip_address* ] | **stats**}

## 構文の説明

| | |
|---|---|
| **sa** *ip_address* | SA をクリアします。すべての IKEv2 SA をクリアするには、IP アドレスを指定せずにこのオプションを使用します。それ以外の場合は、クリアする SA の IPv4 アドレスまたは IPv6 アドレスを指定します。 |
| **stats** | IKEv2 統計情報をクリアします。 |

## 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、脅威に対する防御 デバイスからすべての IPsec IKEv2 の統計を削除する例を示します。

```
> clear ikev2 stats
>
```

次に、10.86.1.1 のピア IP アドレスを持つ SA を削除する例を示します。

```
> clear ikev2 sa 10.86.1.1
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipsec sa** | カウンタ、エントリ、マップ名、ピア IP アドレス、ホスト名などの IPSec SA に関する情報を表示します。 |
| **show running-config crypto** | IPsec、クリプト マップ、ダイナミック クリプト マップ、ISAKMP など、暗号コンフィギュレーション全体を表示します。 |

# clear interface

IP インターフェイスの統計情報を消去するには、**clear interface** コマンドを使用します。

**clear interface** [*physical_interface*[**.***subinterface*] | *interface_name*]

## 構文の説明

| | |
|---|---|
| *interface_name* | （任意）インターフェイス名を指定します。 |
| *physical_interface* | （任意）**gigabit**ethernet0/1 などのインターフェイス ID を指定します。 |
| サブインターフェイス | （任意）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。 |

## コマンド デフォルト

デフォルトでは、このコマンドはすべてのインターフェイス統計情報をクリアします。

## 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、すべてのインターフェイス統計情報をクリアする例を示します。

```
> clear interface
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show interface** | インターフェイスの実行時ステータスと統計情報を表示します。 |
| **show running-config interface** | インターフェイスの設定を表示します。 |

# clear ip

特定のレガシー機能の統計情報をクリアするには、**clear ip** コマンドを使用します。

**clear ip** ｛**audit count** ［**global**］ | **verify statistics**｝［**interface** *interface_name*］

## 構文の説明

| | |
|---|---|
| **audit count**［**global**］ | 監査ポリシーのシグニチャ一致カウントをクリアします。**interface** キーワードを指定しない場合、すべての署名のカウントがグローバルにクリアされます。必要に応じて、このことを明示的に指定する **global** キーワードを含めることができます（global と interface の両方は指定できません）。 |
| **interface** *interface_name* | （任意）指定されたインターフェイスの統計情報のみクリアします。 |
| **verify statistics** | ユニキャスト リバース パス フォワーディング（RPF）でドロップされたパケットの数をクリアします。 |

## 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

通常、これらの機能は有効になっていないため、クリアする統計情報はありません。

### 例

次に、すべてのインターフェイスの IP 監査数をクリアする例を示します。

```
> clear ip audit count
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ip audit count** | ユニキャスト RPF 統計情報を表示します。 |
| **show ip verify statistics** | ユニキャスト RPF 統計情報を表示します。 |
| **show running-config ip audit name** | **ip audit name** コマンドの設定を表示します。**name** に加えて、**interface** と **signature** の設定を確認できます。 |
| **show running-config ip verify reverse-path** | **ip verify reverse-path** の設定を表示します。 |

# clear ipsec sa

IPsec SA のカウンタ、エントリ、クリプトマップ、またはピア接続を削除するには、**clear ipsec sa** コマンドを使用します。

**clear ipsec sa** ［**counters** | **entry** *ip_address* {**esp** | **ah**} *spi* | **inactive** | **map** *map_name* | **peer** *ip_address*］

## 構文の説明

| | |
|---|---|
| **ah** | 認証ヘッダー。 |
| **counters** | 各 SA 統計情報のすべての IPsec をクリアします。 |
| **entry** *ip_address* | 指定した IP アドレス、ホスト名、プロトコル、および SPI 値に一致するトンネルを削除します。 |
| **esp** | 暗号化セキュリティ プロトコル。 |
| **inactive** | すべての非アクティブな IPsec SA をクリアします。 |
| **map** *map_name* | マップ名で識別される、指定したクリプト マップに関連付けられているすべてのトンネルを削除します。 |
| **peer** *ip_address* | 指定したホスト名または IP アドレスで識別されるピアへのすべての IPsec SA を削除します。 |
| *spi* | セキュリティ パラメータ インデックス（16 進数）を指定します。受信 SPI である必要があります。このコマンドは、送信 SPI ではサポートされていません。 |

## 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

すべての IPsec SA をクリアするには、このコマンドを引数なしで使用します。

### 例

次に、グローバル コンフィギュレーション モードで、脅威に対する防御 からすべての IPsec SA を削除する例を示します。

```
> clear ipsec sa
>
```

次に、グローバル コンフィギュレーション モードで、10.86.1.1 のピア IP アドレスを持つ SA を削除する例を示します。

```
> clear ipsec sa peer 10.86.1.1
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipsec sa** | カウンタ、エントリ、マップ名、ピア IP アドレス、ホスト名などの IPsec SA に関する情報を表示します。 |
| **show running-config crypto** | IPsec、クリプト マップ、ダイナミック クリプト マップ、ISAKMP など、暗号コンフィギュレーション全体を表示します。 |

# clear ipv6 dhcp

DHCPv6 の統計情報をクリアするには、**clear ipv6 dhcp** コマンドを使用します。

**clear ipv6 dhcp** {**client** [**pd**] | **interface** *interface_name* | **server**} **statistics**

## 構文の説明

| | |
|---|---|
| **client** [**pd**] | DHCPv6 クライアントの統計情報をクリアします。プレフィックス委任クライアントの統計情報をクリアするには、**pd** キーワードを追加します。 |
| **interface** *interface_name* | 指定したインターフェイスの DHCPv6 統計情報をクリアします。 |
| **server** | DHCPv6 サーバーの統計情報をクリアします。 |

## 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。 |

### 例

次に、DHCPv6 クライアントの統計情報をクリアする例を示します。

```
> clear ipv6 dhcp client statistics
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipv6 dhcp** | DHCPv6 の統計情報を表示します。 |

# clear ipv6 dhcprelay

IPv6 DHCP リレー バインディング エントリおよび統計情報をクリアするには、**clear ipv6 dhcprelay** コマンドを使用します。

**clear ipv6 dhcprelay** {**binding** [*ip_address* ] | **statistics**}

## 構文の説明

| | |
|---|---|
| **binding** | IPv6 DHCP リレー バインディング エントリをクリアします。 |
| *ip_address* | （オプション）DHCP リレー バインディングの IPv6 アドレスを指定します。IP アドレスを指定した場合、その IP アドレスに関連付けられたリレー バインディング エントリだけがクリアされます。 |
| **statistics** | IPv6 DHCP リレー エージェントの統計情報をクリアします。 |

## 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、IPv6 DHCP リレー バインディングの統計情報データをクリアする例を示します。

```
> clear ipv6 dhcprelay binding
>
```

次に、IPv6 DHCP リレー エージェントの統計情報データをクリアする例を示します。

```
> clear ipv6 dhcprelay statistics
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipv6 dhcprelay binding** | リレー エージェントによって作成されたリレー バインディング エントリを表示します。 |
| **show ipv6 dhcprelay statistics** | IPv6 DHCP リレー エージェントの情報を表示します。 |

# clear ipv6 mld traffic

IPv6 マルチキャストリスナー検出（MLD）トラフィックカウンタをクリアして、リセットするには、**clear ipv6 mld traffic** コマンドを使用します。

**clear ipv6 mld traffic**

## 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、IPv6 MLD のトラフィック カウンタをクリアする例を示します。

```
> clear ipv6 mld traffic
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipv6 mld traffic** | IPv6 MLD トラフィックカウンタを表示します。 |

# clear ipv6 neighbors

IPv6 ネイバー探索キャッシュをクリアするには、**clear ipv6 neighbors** コマンドを使用します。

**clear ipv6 neighbors**

## 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、検出されたすべての IPv6 ネイバーをキャッシュから削除します。スタティック エントリは削除しません。

### 例

次に、IPv6 ネイバー探索キャッシュのすべてのエントリ（スタティック エントリは除く）を削除する例を示します。

```
> clear ipv6 neighbors
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipv6 neighbor** | IPv6 ネイバー キャッシュ情報を表示します。 |

# clear ipv6 ospf

OSPFv3 ルーティングパラメータをクリアするには、**clear ipv6 ospf** コマンドを使用します。

**clear ipv6** ［*process_id*］［**counters**］［**events**］［**force-spf**］［**process**］［**redistribution**］［**traffic**］

## 構文の説明

| | |
|---|---|
| **counters** | OSPF プロセス カウンタをリセットします。 |
| **events** | OSPF イベント ログをクリアします。 |
| **force-ospf** | OSPF プロセスの SPF をクリアします。 |
| **process** | OSPFv3 プロセスをリセットします。 |
| *process_id* | プロセス ID の番号をクリアします。有効値の範囲は 1 ～ 65535 です。 |
| **redistribution** | OSPFv3 ルート再配布をクリアします。 |
| **traffic** | トラフィック関連の統計情報をクリアします。 |

## 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、すべての OSPFv3 ルート再配布をクリアする例を示します。

```
> clear ipv6 ospf redistribution
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show running-config ipv6 router** | OSPFv3 プロセスの実行コンフィギュレーションを表示します。 |

# clear ipv6 prefix-list

ルーティング IPv6 プレフィックスリストをクリアするには、**clear ipv6 prefix-list** コマンドを使用します。

**clear ipv6 prefix-list** ［*name*］

## 構文の説明

| | |
|---|---|
| *name* | 名前付き IPv6 プレフィックスリストをクリアします。 |

## 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、list1 IPv6 プレフィックス リストをクリアする例を示します。

```
> clear ipv6 prefix-list list1
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show running-config ipv6 prefix-list** | IPv6 プレフィックス リストの実行コンフィギュレーションを表示します。 |

# clear ipv6 route

IPv6 ルーティング テーブルからルートを削除するには、clear ipv6 route コマンドを使用します。

**clear ipv6 route** ［**management-only**］｛**all** | *ipv6-prefix/prefix-length*｝

## 構文の説明

| | |
|---|---|
| **management-only** | IPv6 管理ルーティング テーブルのみをクリアします。 |
| *ipv6-prefix/prefix-length* | IPv6 プレフィックス用のルーテッドをクリアします。 |
| **all** | すべての IPv6 ルートをクリアします。 |

## 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

**clear ipv6 route** コマンドは、IPv6 固有である点を除いて、**clear ip route** コマンドに似ています。

宛先ごとの最大伝送ユニット（MTU）キャッシュもクリアされます。

### 例

次に、2001:0DB8::/35 用の IPv6 ルートを削除する例を示します。

```
> clear ipv6 route 2001:0DB8::/35
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipv6 route** | IPv6 ルートを表示します。 |

# clear ipv6 traffic

IPv6 トラフィックカウンタをリセットするには、**clear ipv6 traffic** コマンドを使用します。

**clear ipv6 traffic**

## 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

このコマンドを使用すると、**show ipv6 traffic** コマンドの出力内のカウンタをリセットします。

### 例

次に、IPv6 トラフィック カウンタをリセットする例を示します。

```
> clear ipv6 traffic
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipv6 traffic** | IPv6 トラフィックの統計情報を表示します。 |

# clear isakmp

ISAKMP SA または統計情報をクリアするには、**clear isakmp** コマンドを使用します。

**clear isakmp** ［**sa** | **stats**］

## 構文の説明

| | |
|---|---|
| **sa** | （任意）IKEv1 SA および IKEv2 SA をクリアします。 |
| **stats** | （任意）IKEv1 および IKEv2 統計情報をクリアします。 |

## 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

すべての ISAKMP 運用データをクリアするには、このコマンドを引数なしで使用します。

### 例

次に、すべての ISAKMP SA を削除する例を示します。

```
> clear isakmp sa
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show isakmp** | ISAKMP 運用データに関する情報を表示します。 |
| **show running-config crypto** | IPsec、クリプト マップ、ダイナミック クリプト マップ、ISAKMP など、暗号コンフィギュレーション全体を表示します。 |

# clear isis

IS-IS データ構造をクリアするには、**clear isis** コマンドを使用します。

**clear isis** {***** | **lspfull** | **rib redistribution** [**level-1** | **level-2**] [*network_prefix*] [*network_mask*]}

## 構文の説明

| | |
|---|---|
| ***** | すべての IS-IS データ構造をクリアします。 |
| **level-1** | （任意）再配布キャッシュから、レベル 1 IS-IS 再配布プレフィックスをクリアします。 |
| **level-2** | （任意）再配布キャッシュから、レベル 2 IS-IS 再配布プレフィックスをクリアします。 |
| **lspfull** | IS-IS LSPFULL 状態をクリアします。 |
| *network_mask* | （任意）RIB からクリアするネットワーク プレフィックスのネットワーク マスクのネットワーク ID を A.B.C.D 形式で表したもの。プレフィックスに対するネットワーク マスクを指定しなかった場合、ネットワーク マスクには、プレフィックスのメジャー ネットが使用されます。 |
| *network_prefix* | （任意）再配布ルーティング情報ベース（RIB）からクリアするネットワーク プレフィックスのネットワーク ID を A.B.C.D 形式で表したもの。プレフィックスに対するネットワーク マスクを指定しなかった場合、ネットワーク マスクには、プレフィックスのメジャー ネットが使用されます。 |
| **rib redistribution** | IS-IS 再配布キャッシュ内のプレフィックスをクリアします。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

## 使用上のガイドライン

再配布されたルートが多すぎて、リンクステート PDU（LSP）がいっぱいになってしまった場合は、問題の解決後、**clear isis lspfull** コマンドを使用して、この状態をクリアします。

**clear isis rib** コマンドは、Cisco Technical Assistance Center の担当者がソフトウェアエラーの後で実行を依頼したときに、トラブルシューティングのためにだけ使用することをお勧めします。

### 例

次に、LSPFULL 状態をクリアする例を示します。

```
> clear isis lspfull
```

次に、IP ローカル再配布キャッシュからネットワーク プレフィックス 10.1.0.0 をクリアする例を示します。

```
> clear isis rib redistribution 10.1.0.0 255.255.0.0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show clns** | CLNS 固有の情報を表示します。 |
| **show isis** | IS-IS の情報を表示します。 |
| **show route isis** | IS-IS ルートを表示します。 |

# clear kernel cgroup-controller

カーネルの cgroup コントローラの統計情報をクリアするには、**clear kernel cgroup-controller** コマンドを使用します。

**clear kernel cgroup-controller** ［**cpu** | **memory**］

## 構文の説明

| | |
|---|---|
| **cpu** | （任意）cpu/cpuacct コントローラの統計情報をクリアします。 |
| **memory** | （任意）メモリコントローラの統計情報をクリアします。 |

## 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、cgroup コントローラの統計情報をクリアする例を示します。

```
> clear kernel cgroup-controller
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show kernel cgroup-controller** | cgroup コントローラの統計情報を表示します。 |

# clear lacp

EtherChannel LACP ポートチャネルの統計情報をクリアするには、**clear lacp** コマンドを使用します。

**clear lacp** ［*channel_group_number*］

## 構文の説明

| | |
|---|---|
| *channel_group_number* | （オプション）1 ー 48 の番号ごとに、チャネルグループ情報をクリアします。 |

## コマンド デフォルト

チャネル番号を指定しないと、すべてのポートチャネルの統計情報がクリアされます。

## 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、ポートチャネル統計情報をクリアする例を示します。

```
> clear lacp 12
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show lacp** | ポート チャネルの情報を表示します。 |

# clear lisp eid

LISP EID テーブルをクリアするには、**clear list eid** コマンドを使用します。

**clear lisp eid** ［*ip_address* ］

## 構文の説明

| | |
|---|---|
| *ip_address* | 指定した IP アドレスを EID テーブルから削除します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.2 | このコマンドが導入されました。 |

## 使用上のガイドライン

デバイスは、EID とサイト ID を関連付ける EID テーブルを保持します。**clear lisp eid** コマンドは、テーブルの EID エントリをクリアします。

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear cluster info flow-mobility counters** | フロー モビリティ カウンタをクリアします。 |
| **show cluster info flow-mobility counters** | フロー モビリティ カウンタを表示します。 |
| **show conn** | LISP フロー モビリティの対象となるトラフィックを表示します。 |
| **show lisp eid** | EID テーブルを表示します。 |

# clear local-host （廃止）

接続制限や初期接続制限など、クライアントごとのランタイム状態を再初期化するには、**clear local-host** コマンドを使用します。

**clear local-host** ［*hostname* | *ip_address*］［**all**］［**zone**］

## 構文の説明

| | |
|---|---|
| **all** | （任意）to-the-box トラフィックを含む、すべての接続をクリアします。**all** キーワードを指定しない場合は、through-the-box トラフィックだけがクリアされます。 |
| *hostname* または *ip_address* | （任意）ローカルホスト名か、IPv4 または IPv6 アドレスを指定します。 |
| **zone** | （任意）トラフィックゾーンのすべての接続をクリアします。 |

## コマンド デフォルト

すべての through-the-box 実行時状態をクリアします。

## 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。 |
| 7.0 | このコマンドは廃止されました。ローカルアドレスへの接続をクリアするには、**clear conn address** コマンドを使用します。 |

## 使用上のガイドライン

コンフィギュレーションに対してセキュリティポリシーの変更を加えた場合は、すべての新しい接続で新しいセキュリティポリシーが使用されます。既存の接続では、その接続が確立された時点で設定されていたポリシーの使用が続行されます。すべての接続で新しいポリシーが確実に使用されるようにするには、**clear local-host** コマンドを使用して、現在の接続を切断し、新しいポリシーを使用して再接続できるようにする必要があります。または、さらにきめ細かく接続をクリアするための **clear conn** コマンドや、ダイナミック NAT を使用する接続用の **clear xlate** コマンドを使用できます。

**clear local-host** コマンドは、ホストライセンス制限からホストを解放します。ライセンス制限にカウントされているホストの数は、**show local-host** コマンドを入力して確認できます。

### 例

次に、10.1.1.15 のホストのランタイム状態および関連する接続をクリアする例を示します。

```
> clear local-host 10.1.1.15
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear conn** | あらゆる状態の接続を切断します。 |
| **clear xlate** | ダイナミック NAT セッションおよび NAT を使用しているすべての接続をクリアします。 |
| **show local-host** | ローカル ホストのネットワーク状態を表示します。 |

# clear logging

ロギングバッファをクリアするには、**clear logging** コマンドを使用します。

**clear logging** {**buffer** | **counter** *option* | **queue bufferwrap** | **unified-client**}

## 構文の説明

| | |
|---|---|
| **buffer** | 内部ロギングバッファをクリアします。 |
| **counter** *[接続先（Destination）]* | 指定されたロギングの宛先に対するカウンタと統計情報をクリアします。すべてのロギングの宛先に関する統計情報をクリアするには、**all** を指定します。または、次のいずれかの宛先を指定して、アクションをその 1 つの宛先に制限できます。**buffer**、**console**、**mail**、**monitor**、**trap**。 |
| **queue bufferwrap** | 保存されている FTP およびフラッシュ ロギング バッファ キューをクリアします。 |
| **unified-client** | 統合ロギングクライアント、loggerD からロギング統計情報をクリアします。 |

## 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。 |
| 6.3 | **unified-client** キーワードが追加されました。 |
| 6.6 | **counter** キーワードが追加されました。 |

### 例

次の例では、ログ バッファの内容をクリアする方法を示します。

```
> clear logging buffer
```

次に、保存されているログ バッファの内容をクリアする例を示します。

```
> clear logging queue bufferwrap
```

次に、loggerD サービスの統計情報をクリアする例を示します。

```
> clear logging unified-client
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **logging savelog** | 任意のフラッシュファイル名を指定します。 |

| Command | 説明 |
| --- | --- |
| **show logging** | ロギング情報を表示します。 |

# clear mac-address-table

ダイナミック MAC アドレステーブルエントリをクリアするには、**clear mac-address-table** コマンドを使用します。

**clear mac-address-table** ［*interface_name*］

## 構文の説明

| | |
|---|---|
| *interface_name* | （任意）選択したインターフェイスの MAC アドレス テーブル エントリをクリアします。 |

## 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、ダイナミック MAC アドレス テーブルのエントリをクリアする例を示します。

```
> clear mac-address-table
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show mac-address-table** | MAC アドレス テーブルのエントリを表示します。 |

# clear memory

メモリツールのキューと統計情報をクリアするには、**clear memory** コマンドを使用します。

**clear memory** {**delayed-free-poisoner** | **profile** [**peak**] | **tracking**}

## 構文の説明

| | |
|---|---|
| **delayed-free-poisoner** | delayed free-memory poisoner ツールのキューで保持されているすべてのメモリを検証せずにシステムに戻し、関連する統計情報カウンタをクリアします。この機能を有効にするには、**memory delayed-free-poisoner enable** コマンドを使用します。 |
| **profile** [**peak**] | メモリ プロファイリング機能によって保持されるメモリ バッファをクリアします。ピークメモリバッファの内容をクリアするには、任意の **peak** キーワードを含めます。<br>プロファイルバッファをクリアする前に、メモリプロファイリングを停止するには、**no memory profile enable** コマンドを使用します。 |
| **tracking** | **memory tracking enable** コマンドによって収集されたメモリトラッキング情報をクリアします。 |

## 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、delayed free-memory poisoner ツールのキューと統計情報をクリアする例を示します。

```
> clear memory delayed-free-poisoner
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **memory** | さまざまなメモリツールを有効にします。 |
| **show memory delayed-free-poisoner** | delayed free-memory poisoner ツールのキューの使用状況に関する要約を表示します。 |
| **show memory profile** | メモリプロファイリングの結果を表示します。 |
| **show memory tracking** | メモリトラッキングの結果を表示します。 |

# clear mfib counters

マルチキャスト転送情報ベース（MFIB）ルートパケットカウンタをクリアするには、**clear mfib counters** コマンドを使用します。

**clear mfib** {**cluster-stats** | **counters** [*source_or_group* [*source*]]}

## 構文の説明

| | |
|---|---|
| **cluster-stats** | MFIB クラスタ同期統計情報をクリアします。 |
| **count** | MFIB ルートおよびパケットカウントデータをクリアします。**count** コマンドを引数なしで使用した場合、すべてのルートのルートカウンタがクリアされます。 |
| *source_or_group* [*group*] | （任意）送信元またはグループの IPv4、IPv6、または名前。両方を指定する場合は、最初に送信元を指定します。送信元アドレスはユニキャストアドレスです。 |

## 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、すべての MFIB ルータ パケット カウンタをクリアする例を示します。

```
> clear mfib counters
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show mfib** | MFIB ルートおよびパケット カウント データを表示します。 |

# clear nat counters

NAT ポリシーカウンタをクリアするには、clear nat counters コマンドを使用します。

**clear nat counters** ［**interface** *name*］［*ip_addr mask* ｜ ｛**object** ｜ **object-group**｝ *name*］［**translated** ［**interface** *name*］［*ip_addr mask* ｜ ｛**object** ｜ **object-group**｝ *name*］］］

## 構文の説明

| | |
|---|---|
| **interface** *name* | （任意）送信元または宛先（変換済み）インターフェイスを指定します。 |
| *ip_addr mask* | （オプション）IP アドレスおよびサブネット マスクを指定します。 |
| **object** *name* | （任意）ネットワーク オブジェクトまたはサービス オブジェクトを指定します。 |
| **object-group** *name* | （任意）ネットワーク オブジェクト グループを指定します。 |
| **translated** | （オプション）変換されたパラメータを指定します。 |

## 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。 |

### 例

次に、NAT ポリシー カウンタをクリアする例を示します。

```
> clear nat counters
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show nat** | プロトコル スタック カウンタを表示します。 |

# clear object

ネットワークサービス オブジェクトのヒットカウントをクリアするには、**clear object** コマンドを使用します。

**clear object** ［ **id** *object_name* | **network-service** ］

## 構文の説明

| | |
|---|---|
| **id** *name* | （オプション）指定したネットワークサービス オブジェクトのカウンタをクリアします。大文字と小文字が区別されます。たとえば、「object-name」は「Object-Name」と一致しません。 |
| **network-service** | （オプション）すべてのネットワークサービス オブジェクトのカウンタをクリアします。このアクションは、コマンドでパラメータを指定しない場合と同じです。 |

## コマンド デフォルト

パラメータを指定しない場合、すべてのオブジェクトのヒットカウントがクリアされます。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1 | このコマンドが導入されました。 |

### 例

次に、すべてのオブジェクトのヒットカウントをクリアする例を示します。

```
> clear object
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show object** | ネットワークサービス オブジェクトとそのヒットカウントを表示します。 |

# clear object-group

ネットワーク オブジェクト グループまたはネットワークサービスオブジェクト グループにあるオブジェクトのヒットカウントをクリアするには、**show object-group** コマンドを使用します。

**clear object-group** ［ *object_group_name* ］

## 構文の説明

| | |
|---|---|
| *object_group_name* | カウンタをクリアするオブジェクトグループの名前。名前を指定しない場合、すべてのオブジェクトグループのカウンタがクリアされます。 |

## 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。 |
| 7.1 | ネットワークサービス オブジェクトで動作するようにコマンドが拡張されました。 |

### 例

次に、「Anet」というオブジェクトグループのヒットカウントをクリアする例を示します。

```
> clear object-group Anet
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show object-group** | オブジェクトグループの情報を表示します。 |

# clear ospf

OSPF プロセス情報をクリアするには、**clear ospf** コマンドを使用します。

**clear ospf** ［**vrf** *name* | **all**］ {**counters** ［**neighbor** *interface*］ | **events** | **force-spf** | **process /noconfirm** | **redistribution** | **traffic**}

## 構文の説明

| | |
|---|---|
| **counters** | OSPF カウンタをクリアします。 |
| **neighbor** *interface* | （任意）ネイバーの統計情報のみクリアします。 |
| **events** | OSPF イベント ログをクリアします。 |
| **force-spf** | 増分 SPF 統計情報をクリアします。 |
| **process /noconfirm** | OSPF ルーティング プロセスを再起動します。 |
| **redistribution** | OSPF 経路再配布統計情報を消去します。 |
| **traffic** | OSPF トラフィック関連の統計情報をクリアします。 |
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |

## 使用上のガイドライン

このコマンドは、設定のいずれの部分も削除せず、統計情報のみクリアします。

### 例

次に、すべての OSPF ネイバーカウンタをクリアする例を示します。

```
> clear ospf counters
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ospf** | 実行コンフィギュレーションのすべての OSPF 情報を表示します。 |

# clear packet-debugs

デバッグログをデータベースから削除するには、**clear packet-debugs** コマンドを使用します。

**clear packet-debugs**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.4 | このコマンドが導入されました。 |
| 6.5 | このコマンドは、**clear packet debugs** から **clear packet-debugs** に変更されました。 |

## 使用上のガイドライン

データベースからすべてのデバッグログを削除するには、**clear packet-debugs** コマンドを使用します。

### 例

次に、デバッグログデータベースに保存されているすべてのデバッグログを削除する例を示します。

```
> clear packet-debugs
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **debug packet-start** | データベースへのデバッグログの書き込みを開始します。 |

# clear packet-tracer

永続的なパケットトレーサを削除するには、**clear packet-tracer** コマンドを使用します。

**clear packet-tracer**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

## 使用上のガイドライン

永続的なパケットトレーサは、**packet-tracer** コマンドで **persist** キーワードを使用して設定します。

### 例

次に、すべての永続的なパケットトレーサを削除する例を示します。

```
> clear packet-tracer
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **packet-tracer** | パケットトレーサを設定します。 |

# clear path-monitoring

インターフェイスのパスモニタリング設定をクリアするには、**clear path-monitoring** コマンドを使用します。

**clear path-monitoring** ［ **interface** *name* ］

## 構文の説明

| | |
|---|---|
| **Interface** *name* | 指定されたインターフェイスで設定されたパスモニタリング設定を削除します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2 | このコマンドが導入されました。 |

### 例

次に、outside1 インターフェイスのパスモニタリング設定をクリアする例を示します。

```
> clear path-montoring outside1
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show path-monitoring** | パスモニタリングメトリック情報を表示します。 |

# clear pclu

PC の統計情報をクリアするには、**clear pclu** コマンドを使用します。

**clear pclu**

## 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、PC 情報をクリアする例を示します。

```
> clear pclu
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show pclu** | PCLU 情報を表示します。 |

# clear pim

PIM トラフィックのカウンタとマッピングをクリアするには、**clear pim** コマンドを使用します。

**clear pim** {**counters** | **group-map** [*rp-address*] | **reset** | **topology** [*group*]}

## 構文の説明

| | |
|---|---|
| **counters** | PIM トラフィック カウンタをクリアします。 |
| **group-map** [*rp-address*] | グループからランデブーポイント（RP）へのマッピングエントリを RPマッピングキャッシュから削除します。必要に応じて、ランデブーポイントの名前を指定して、その RP のエントリのみをクリアすることもできます。次のいずれかの名前を使用できます。<br>• ドメインネームシステム（DNS）ホストテーブルで定義されている RP の名前。<br>• RP の IP アドレス。これは、4 分割ドット付き 10 進表記のマルチキャスト IP アドレスです。 |
| **reset** | リセット時の MRIB 同期を必須にします。トポロジ テーブルのすべての情報がクリアされ、MRIB 接続がリセットされます。このオプションを使用して、PIM トポロジテーブルと MRIB データベース間の状態を同期することもできます。 |
| **topology** [*group*] | PIM トポロジテーブルから既存の PIM ルートをクリアします。IGMP ローカル メンバーシップなど、MRIB テーブルから取得した情報は保持されます。必要に応じて、トポロジテーブルから削除するマルチキャストグループのアドレスまたは名前を指定できます。次のいずれかの名前を使用できます。<br>• DNS ホストテーブルで定義されているマルチキャストグループの名前。<br>• マルチキャストグループの IPv4 または IPV6 アドレス。 |

## 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、PIM トラフィック カウンタをクリアする例を示します。

```
> clear pim counters
```

次に、RP アドレス 23.23.23.2 のグループから RP へのマッピングのエントリを削除する例を示します。

```
> show pim group-map

Group Range         Proto Client Groups RP address      Info
224.0.1.39/32*      DM    static 0      0.0.0.0
224.0.1.40/32*      DM    static 0      0.0.0.0
224.0.0.0/24*       L-Localstatic 1      0.0.0.0
232.0.0.0/8*        SSM   config 0      0.0.0.0
224.0.0.0/4*        SM    config 0      9.9.9.9         RPF: ,0.0.0.0
224.0.0.0/4         SM    BSR    0      23.23.23.2      RPF: Gi0/3,23.23.23.2
> clear pim group-map 23.23.23.2
> show pim group-map
Group Range         Proto Client Groups RP address      Info
224.0.1.39/32*      DM    static 0      0.0.0.0
224.0.1.40/32*      DM    static 0      0.0.0.0
224.0.0.0/24*       L-Localstatic 1      0.0.0.0
232.0.0.0/8*        SSM   config 0      0.0.0.0
224.0.0.0/4*        SM    config 0      9.9.9.9         RPF: ,0.0.0.0
224.0.0.0/4         SM    static 0      0.0.0.0         RPF: ,0.0.0.0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show pim** | PIM トラフィックの情報を表示します。 |

# clear prefix-list

プレフィックスリストのエントリのヒットカウントをリセットするには、**clear prefix-list** コマンドを使用します。

**clear prefix-list** ［*prefix_list_name*］

## 構文の説明

| | |
|---|---|
| *prefix_list_name* | （任意）ヒットカウントをクリアするプレフィックスリストの名前。 |

## 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、first_list という名前のリストからプレフィックスリスト情報をクリアする例を示します。

```
> clear prefix-list first_list
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show prefix-list** | プレフィックス リストまたはプレフィックス リスト エントリに関する情報を表示します。 |

# clear priority-queue statistics

特定のインターフェイス、またはすべての設定済みインターフェイスに関する priority-queue statistics のカウンタをクリアするには、**clear priority-queue statistics** コマンドを使用します。

**clear priority-queue statistics** *interface_name*

## 構文の説明

| | |
|---|---|
| *interface_name* | （任意）指定されたインターフェイスの priority-queue statistics をクリアします。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

### 例

次に、すべてのインターフェイスの priority-queue statistics をクリアする例を示します。

```
> clear priority-queue statistics
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show priority-queue statistics** | 指定したインターフェイスまたはすべてのインターフェイスのプライオリティ キュー統計情報を表示します。 |

# clear process

脅威に対する防御 デバイスで実行されている特定のプロセスの統計をクリアするには、clear process コマンドを使用します。

**clear process** {**cpu-hog** | **internals**}

## 構文の説明

| | |
|---|---|
| **cpu-hog** | 高 CPU 負荷統計情報をクリアします。 |
| **internals** | プロセス内部統計情報をクリアします。 |

## 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、高 CPU 負荷統計情報をクリアする例を示します。

```
> clear process cpu-hog
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **cpu hog granular-detection** | リアルタイム高 CPU 負荷検出情報をトリガーします。 |
| **show processes** | 脅威に対する防御 で動作しているプロセスのリストを表示します。 |

# clear resource usage

リソース使用状況の統計情報をクリアするには、**clear resource usage** コマンドを使用します。

**clear resource usage** ［**detail** ｜ **resource** ｛［**rate**］ *resource_name* ｜ **all**｝］

## 構文の説明

| | |
|---|---|
| **detail** | すべてのリソース使用状況の詳細をクリアします。 |
| **resource** [**rate**] *resource_name* | 特定のリソースの使用状況をクリアします。すべてのリソースを対象にするには、**all**（デフォルト）を指定します。リソース使用状況のレートをクリアする場合は、**rate** を指定します。rate で測定されるリソースには、**conns**、**inspects**、および **syslogs** があります。これらのリソースの種類を指定する場合は、**rate** キーワードを指定する必要があります。conns リソースは、同時接続としても測定されます。1 秒あたりの接続を表示するには、**rate** キーワードのみを使用します。<br>リソースには、次のタイプがあります。<br>• **Conns**：任意の 2 つのホスト間の TCP または UDP 接続（1 つのホストと他の複数ホストとの間の接続を含む）。<br>• **Hosts**：デバイスを介して接続できるホスト。<br>• **IPSec**：デバイスを介して接続する IPSec 管理トンネル。<br>• **Mac-addresses**：MAC アドレステーブルで許可される MAC アドレス数。<br>• **Routes**：ルーティング テーブル エントリ。<br>• **SSH**：SSH セッション。<br>• **Storage**：ストレージサイズ制限（MB 単位）。<br>• **Telnet**：Telnet セッション。<br>• **VPN**：VPN リソース。<br>• **Xlates**：NAT 変換。 |

## コマンド デフォルト

デフォルトのリソース名は **all** で、すべてのリソースタイプがクリアされます。

## 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、システム全体の使用状況の統計情報をクリアする例を示します。

```
> clear resource usage resource all
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show resource types** | リソース タイプのリストを表示します。 |
| **show resource usage** | デバイスのリソース使用状況を表示します。 |

# clear route

ダイナミックに学習されたルートをルーティングテーブルから削除するには、**clear route** コマンドを使用します。

**clear route** ［ **vrf** *name* | **all** ］ ［ **management-only** ］ ［ **all** | *ip_address* ［ *ip_mask_or_prefix* ］］

## 構文の説明

| | |
|---|---|
| **all** | 学習したすべてのルートを削除するように指定します。 |
| *ip_address mask_or_prefix* | 削除するルートの IPv4 または IPv6 宛先アドレスとマスクまたはプレフィックス。ルートを指定しない場合、動的に学習されたすべてのルートが削除されます。 |
| **management-only** | （オプション）管理ルーティングテーブルをクリアします。宛先アドレスを指定して、特定の管理ルートをクリアできます。 |
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |
| 7.1 | バージョン 7.1 以降では、ユニットがハイアベイラビリティ グループまたはクラスタの一部である場合、このコマンドはアクティブユニットまたは制御ユニットにのみ使用できます。HA グループまたはクラスタのすべてのユニットのルートがクリアされます。以前のリリースでは、コマンドを実行したユニットのルートのみがクリアされます。 |

### 例

次に、すべてのダイナミックに学習されたルートを削除する例を示します。

```
> clear route
```

関連コマンド

| Command | 説明 |
| --- | --- |
| **show route** | ルート情報を表示します。 |

# clear rule hits

アクセスコントロールポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報をクリアし、ゼロにリセットするには、**clear rule hits** コマンドを使用します。

**clear rule hits** ［*id*］

## 構文の説明

| | |
|---|---|
| *id* | （オプション）ルールの ID。この引数を含めると、指定したルールのルールヒット情報のみがクリアされます。<br>ルール ID を識別するには、**show access-list** コマンドを使用します。 |

## コマンド デフォルト

ルールIDを指定しない場合、すべてのルールのルールヒット情報がクリアされ、ゼロにリセットされます。

（注） このアクションは元に戻せないため、このコマンドの使用には注意が必要です。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.4 | このコマンドが導入されました。 |

## 使用上のガイドライン

ルールヒット情報は、アクセスコントロールルールとプレフィルタルールのみを対象としています。

### 例

すべてのルールヒット情報をクリアする例を次に示します。

```
> clear rule hits
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show rule hits** | アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報を表示します。 |
| **show cluster rule hits** | クラスタ内のすべてのノードから、アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報をクリアし、ゼロにリセットします。 |
| **cluster exec show rule hits** | クラスタの各ノードから、アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報を分離形式で表示します。 |

| Command | 説明 |
| --- | --- |
| **cluster exec clear rule hits** | クラスタ内のすべてのノードから、アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報をクリアし、ゼロにリセットします。 |

# clear service-policy

有効になっているポリシーの動作データまたは統計情報をクリアするには、**clear service-policy** コマンドを使用します。

**clear service-policy** ［**global** | **interface** *intf* | **shape** | **user-statistics**］

## 構文の説明

| | |
|---|---|
| **global** | （任意）グローバル サービス ポリシーの統計情報をクリアします。 |
| **interface** *intf* | （任意）特定のインターフェイスのサービス ポリシーの統計情報をクリアします。 |
| **shape** | （任意）シェイプポリシーの統計情報をクリアします。 |
| **user-statistics** | （オプション）ユーザー統計情報のグローバル カウンタはクリアしますが、ユーザーごとの統計情報はクリアしません。この機能は 脅威に対する防御 ではサポートされていません。 |

## コマンド デフォルト

デフォルトでは、このコマンドは、すべてのイネーブルなサービス ポリシーのすべての統計情報をクリアします。

## 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

一部のインスペクションエンジンでは、統計情報を選択してクリアできます。**clear service-policy inspect** コマンドを参照してください。

### 例

次に、外部インターフェイスのサービス ポリシー統計情報をクリアする方法の例を示します。

```
> clear service-policy interface outside
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear service-policy inspect** | GTP、M3UA、およびRADIUS検査エンジンのサービスポリシーの統計情報をクリアします。 |
| **show service-policy** | サービス ポリシーを表示します。 |
| **show running-config service-policy** | 実行コンフィギュレーションに設定されているサービス ポリシーを表示します。 |

# clear service-policy inspect gtp

GTP インスペクションの統計情報をクリアするには、**clear service-policy inspect gtp** コマンドを使用します。

**clear service-policy inspect gtp** {**pdp-context** {**all** | **apn** *ap_name* | **imsi** *IMSI_value* | **ms-addr** *IP_address* | **tid** *tunnel_ID* | **version** *version_num*} | **requests** [**map** *name* | **version** *version_num*] | **statistics** [*IP_address*]}

## 構文の説明

| | |
|---|---|
| **pdp-context** {**all** \| **apn** *ap_name* \| **imsi** *IMSI_value* \| **ms-addr** *IP_address* \| **tid** *tunnel_ID* \| **version** *version_num*} | パケット データ プロトコル（PDP）またはベアラー コンテキスト情報をクリアします。次のキーワードを使用して、クリアするコンテキストを指定できます。<br>• **all**：すべてのコンテキストをクリアします。<br>• **apn** *ap_name*：指定されたアクセスポイント名のコンテキストをクリアします。<br>• **imsi** *IMSI_value*：指定された IMSI 16 進数のコンテキストをクリアします。<br>• **ms-addr** *IP_address*：指定されたモバイルサブスクライバ（MS）の IP アドレスのコンテキストをクリアします。<br>• **tid** *tunnel_ID*：指定された GTP トンネル ID（16 進数）のコンテキストをクリアします。<br>• **version** *version_num*：指定された GTP バージョン（0 ～ 255）のコンテキストをクリアします。 |
| **requests** [**map** *name* \| **version** *version_num*] | GTP 要求をクリアします。次のパラメータを使用して、クリアする要求を任意で制限できます。<br>• **map** *name*：指定された GTP インスペクション ポリシー マップに関連付けられている要求をクリアします。<br>• **version** *version_num*：指定された GTP バージョン（0 ～ 255）の要求をクリアします。 |
| **statistics** [*IP_address*] | **inspect gtp** コマンドの GTP 統計情報をクリアします。エンドポイントのアドレスを指定すると、特定のエンドポイントの統計情報をクリアできます。 |

## 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。 |

### 例

次に、GTP 統計情報をクリアする例を示します。

```
> clear service-policy inspect gtp statistics
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show service-policy inspect gtp** | GTP 統計情報を表示します。 |

# clear service-policy inspect m3ua

M3UA インスペクションの統計情報をクリアするには、**clear service-policy inspect m3ua** コマンドを使用します。

**clear service-policy inspect m3ua** {**drops** | **endpoint** [*ip_address* ]}

## 構文の説明

| | |
|---|---|
| **drops** | M3UA ドロップの統計情報をクリアします。 |
| **endpoint** [*ip_address*] | M3UAエンドポイントの統計情報をクリアします。必要に応じて、エンドポイントの IP アドレスを指定して、そのエンドポイントの統計情報のみをクリアできます。 |

## 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

このコマンドを使用して、M3UAインスペクションの統計情報をクリアします。統計情報を表示するには、このコマンドの **show** バージョンを使用します。

### 例

次に、M3UA エンドポイントの統計情報をクリアする例を示します。

```
> clear service-policy inspect m3ua endpoint
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show service-policy inspect m3ua** | M3UA 統計情報を表示します。 |

# clear service-policy inspect radius-accounting

RADIUS アカウンティングユーザーをクリアするには、**clear service-policy inspect radius-accounting** コマンドを使用します。

**clear service-policy inspect radius-accounting users** {**all** | *ip_address* | *policy_map*}

## 構文の説明

| | |
|---|---|
| **all** | すべてのユーザーをクリアします。 |
| *ip_address* | この IP アドレスのユーザーをクリアします。 |
| *policy_map* | このポリシーマップに関連付けられているユーザーをクリアします。 |

## 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、すべての RADIUS アカウンティング ユーザーをクリアする例を示します。

```
> clear service-policy inspect radius-accounting users all
```

# clear shun

現在有効になっているすべての shun を無効にして、shun 統計情報をクリアするには、**clear shun** コマンドを使用します。

**clear shun** ［**statistics**］

## 構文の説明

| | |
|---|---|
| **statistics** | （任意）インターフェイス カウンタだけをクリアします。 |

## 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、現在イネーブルになっているすべての shun をディセーブルにして、shun 統計情報をクリアする例を示します。

```
> clear shun
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **shun** | 新規接続を抑制し、既存のすべての接続からのパケットを不許可にすることにより、攻撃元ホストへのダイナミック応答をイネーブルにします。 |
| **show shun** | 回避についての情報を表示します。 |

# clear snmp-server statistics

SNMP サーバー統計情報（SNMP パケットの入力カウンタと出力カウンタ）をクリアするには、**clear snmp-server statistics** コマンドを使用します。

**clear snmp-server statistics**

## 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、SNMP サーバー統計情報をクリアする例を示します。

```
> clear snmp-server statistics
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show snmp-server statistics** | SNMP サーバー コンフィギュレーション情報を表示します。 |

# clear snort statistics

Snort 統計情報（パケットカウンタ、フローカウンタ、およびイベントカウンタ）をクリアするには、**clear snort statistics** コマンドを使用します。

**clear snort statistics**

## 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、Snort 統計情報をクリアする例を示します。

```
> clear snort statistics
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show snort statistics** | Snort サービス コンフィギュレーションに関する情報を表示します。 |

# clear snort tls-offload

SSL ハードウェア アクセラレーション（接続、暗号化、暗号解読）に関連した Snort 統計情報をクリアするには、**clear snort tls-offload** コマンドを使用します。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。このコマンドは、SSL ハードウェア アクセラレーションをサポートする次の管理対象デバイスでのみ使用できます。

- Threat Defense を搭載した Firepower 2100
- を搭載した Firepower 4100/9300 Threat Defense

  Firepower 4100/9300 Threat Defense コンテナインスタンスでの TLS 暗号化アクセラレーションのサポートの詳細については、『*FXOS Configuration Guide*』を参照してください。

仮想アプライアンス上および上記以外のハードウェアでの TLS 暗号化アクセラレーション はサポートされていません。

**clear snort tls-offload [proxy | tracker]**

## 構文の説明

| | |
|---|---|
| **proxy** | （オプション）プロキシの統計情報のみをクリアします。 |
| **tracker** | （オプション）トラッカーの統計情報のみをクリアします。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.2.3 | このコマンドが導入されました。 |

次に、プロキシの統計情報をクリアする例を示します。

```
> clear snort tls-offload proxy
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show snort tls-offload** | すべての Snort プロセスの統計情報を表示します。 |
| **debug snort tls-offload** | すべての Snort プロセスの全タイプのエラーデバッグメッセージを表示します。 |

# clear ssl

デバッグ目的で SSL 情報をクリアするには、**clear ssl** コマンドを使用します。

**clear ssl** {**cache** [**all**] | **errors** | **mib** | **objects**}

## 構文の説明

| | |
|---|---|
| **cache** [**all**] | SSL セッション キャッシュ内の期限切れセッションをクリアします。SSL セッションキャッシュ内のすべてのセッションおよび統計情報をクリアするには、任意の **all** キーワードを追加します。 |
| **errors** | ssl エラーをクリアします。 |
| **mib** | SSL MIB 統計情報をクリアします。 |
| **objects** | SSL オブジェクト統計情報をクリアします。 |

## 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

AnyConnect 機能に影響するため、DTLS キャッシュがクリアされることはありません。

### 例

次に、SSL キャッシュをクリアし、SSL セッション キャッシュ内のすべてのセッションおよび統計情報をクリアする例を示します。

```
> clear ssl cache
SSL session cache cleared: 2
No SSL VPNLB session cache
No SSLDEV session cache
DLTS caches are not cleared
> clear ssl cache all
Clearing all sessions and statistics
SSL session cache cleared: 5
No SSL VPNLB session cache
No SSLDEV session cache
DLTS caches are not cleared
```

# clear sunrpc-server active

Sun RPC アプリケーション インスペクションによって開けられたピンホールをクリアするには、**clear sunrpc-server active** コマンドを使用します。

**clear sunrpc-server active**

## 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

Sun RPC アプリケーション インスペクションによって開けられた、NFS や NIS などのサービス トラフィックがデバイスを通過できるようにするピンホールをクリアするには、**clear sunrpc-server active** コマンドを使用します。

### 例

次に、SunRPC サービス テーブルをクリアする例を示します。

```
> clear sunrpc-server active
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show sunrpc-server active** | アクティブな Sun RPC サービスに関する情報を表示します。 |

# clear threat-detection rate

脅威検出レート統計情報をゼロにリセットするには、**clear threat-detection rate** コマンドを使用します。

**clear threat-detection rate**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

### 例

```
> clear threat-detection rate
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show threat-detection rate** | 脅威検出レート統計情報を表示します。 |

# clear threat-detection scanning-threat

スキャン脅威検出によって識別された攻撃者およびターゲットに関する情報を削除するには、**clear threat-detection scanning-threat** コマンドを使用します。

**clear threat-detection scanning-threat** ［**attacker** ［*ip_address* ［*mask*］］ | **target** ［*ip_address* ［*mask*］］］

## 構文の説明

| | |
|---|---|
| **attacker** [*ip_address* [*mask*]] | （オプション）攻撃者のみをクリアします。IPアドレスとオプションのマスクを指定して、単一の攻撃者をクリアできます。 |
| **target** [*ip_address* [*mask*]] | （オプション）ターゲットのみをクリアします。IP アドレスとオプションのマスクを指定して、1 つのターゲットをクリアできます。 |

## コマンド デフォルト

すべての攻撃者とターゲットがクリアされます。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

### 例

次の例では、現在のスキャンの脅威を表示してからクリアします。

```
> show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0
    192.168.1.249
   Latest Attacker Host & Subnet List:
    192.168.10.234
    192.168.10.0
    192.168.10.2
    192.168.10.3
    192.168.10.4
    192.168.10.5
    192.168.10.6
    192.168.10.7
    192.168.10.8
    192.168.10.9
> clear threat-detection scanning-threat
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show threat-detection scanning-threat** | スキャンする脅威の攻撃者とターゲットを表示します。 |

# clear threat-detection shun

攻撃者を自動的に回避するようにスキャン脅威検出を設定した場合は、**clear threat-detection shun** コマンドを使用して自動回避リストからホストを削除できます。**clear shun** コマンドを使用して、手動で回避されたホストの回避を停止します。

**clear threat-detection shun** ［*ip_address* ［*mask*］］

## 構文の説明

| | |
|---|---|
| *ip_address* [*mask*] | （任意）特定の IP アドレスの回避を解除します。サブネットマスクはオプションです。 |

## コマンド デフォルト

すべての回避された攻撃者が解放されます。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

### 例

次に、回避リストを表示し、ホスト 10.1.1.6 を解放する例を示します。

```
> show threat-detection shun
Shunned Host List:
10.1.1.6
198.1.6.7
> clear threat-detection shun 10.1.1.6
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show threat-detection shun** | 自動的に回避されたホストを表示します。 |

# clear threat-detection statistics

脅威検出統計情報をゼロにリセットするには、**clear threat-detection statistics** コマンドを使用します。

**clear threat-detection statistics** ［**tcp-intercept**］

## 構文の説明

| | |
|---|---|
| **tcp-intercept** | （任意）TCP 代行受信の統計情報をクリアします。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

### 例

脅威検出統計情報をクリアする例を次に示します。

```
> clear threat-detection statistics
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show threat-detection statistics** | 脅威検出統計情報を表示します。 |

# clear traffic

送信アクティビティおよび受信アクティビティのカウンタをリセットするには、**clear traffic** コマンドを使用します。

**clear traffic**

## 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

**clear traffic** コマンドは、**show traffic** コマンドで表示される送信アクティビティと受信アクティビティのカウンタをリセットします。これらのカウンタは、最後に clear traffic コマンドが入力されてから、またはデバイスがオンラインになってから、各インターフェイスを通過したパケット数およびバイト数を示します。また、秒数は、デバイスが最後にリブートされてからオンラインである継続時間を示します。

### 例

次に、**clear traffic** コマンドの例を示します。

```
> clear traffic
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show traffic** | 送信アクティビティおよび受信アクティビティのカウンタを表示します。 |

# clear vpn-sessiondb statistics

VPN セッションの統計情報をクリアするには、**clear vpn-sessiondb statistics** コマンドを使用します。

**clear vpn-sessiondb statistics** {**all** | **anyconnect** | **failover** | **global** | **index** *number* | **ipaddress** *IP_address* | **l2l** | **name** *username* | **ospfv3** | **protocol** *protocol* | **ra-ikev1-ipsec** | **ra-ikev2-ipsec** | **tunnel-group** *name* | **vpn-lb** | **webvpn**}

## 構文の説明

| | |
|---|---|
| **all** | すべてのセッションの統計情報をクリアします。 |
| **anyconnect** | AnyConnect VPN クライアント セッションの統計情報をクリアします。 |
| **failover** | フェールオーバー IPsec セッションの統計情報をクリアします。 |
| **global** | グローバル セッション データの統計情報をクリアします。 |
| **index** *index_number* | インデックス番号を指定して単一のセッションの統計情報をクリアします。**show vpn-sessiondb detail** コマンドの出力には、セッションごとにインデックス番号が表示されます。 |
| **ipaddress** *IP_address* | 指定した IP アドレスのセッションの統計情報をクリアします。 |
| **l2l** | VPN LAN-to-LAN セッションの統計情報をクリアします。 |
| **protocol** *protocol* | 特定のプロトコルの統計情報をクリアします。プロトコルのリストを表示するには、「?」と入力します。 |
| **ra-ikev1-ipsec** | IPsec IKEv1 セッションの統計情報をクリアします。 |
| **ra-ikev2-ipsec** | IPsec IKEv2 セッションの統計情報をクリアします。 |
| **tunnel-group** *groupname* | 指定したトンネル グループ（接続プロファイル）のセッションの統計情報をクリアします。 |
| **vpn-lb** | VPN ロードバランシング管理セッションの統計情報をクリアします。 |
| **webvpn** | クライアントレス SSL VPN セッションの統計情報をクリアします。 |

## 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、すべての VPN セッションの統計情報をクリアする例を示します。

```
> clear vpn-sessiondb statistics all
INFO: Number of sessions cleared : 20
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show vpn-sessiondb** | VPN セッションに関する情報を表示します。 |

# clear wccp

Web Cache Communication Protocol（WCCP）情報をリセットするには、**clear wccp** コマンドを使用します。

**clear wccp** ［**web-cache** | *service_number*］

## 構文の説明

| | |
|---|---|
| **web-cache** | Web キャッシュ サービスを指定します。 |
| *service-number* | ダイナミック サービスID。このサービスの定義は、キャッシュによって示されます。ダイナミック サービス番号は 0 ～ 254 の範囲で指定できます。 |

## 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。 |

### 例

次に、Web キャッシュ サービスの WCCP 情報をリセットする例を示します。

```
> clear wccp web-cache
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show wccp** | WCCP コンフィギュレーションを表示します。 |

# clear webvpn statistics

リモートアクセス VPN の統計情報をクリアするには、**clear webvpn statistics** コマンドを使用します。

**clear webvpn statistics**

## 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。 |

### 例

次に、リモートアクセス VPN の統計情報をクリアする例を示します。

```
> clear webvpn statistics
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show webvpn** | リモートアクセス VPN に関する情報を表示します。 |

# clear xlate

現在のダイナミック NAT 変換および接続情報をクリアするには、**clear xlate** コマンドを使用します。

**clear xlate** ［**global** *ip1*［*-ip2*］［**netmask** *mask*］］［**local** *ip1*［*-ip2*］［**netmask** *mask*］］［**gport** *port1*［*-port2*］］［**lport** *port1*［*-port2*］］［**interface** *if_name*］［**type** *type*］

## 構文の説明

| | |
|---|---|
| **global** *ip1*[*-ip2*] | （任意）グローバル IP アドレスまたはアドレスの範囲を指定して、アクティブな変換をクリアします。 |
| **gport** *port1*[*-port2*] | （任意）グローバル ポートまたはポートの範囲を指定して、アクティブな変換をクリアします。 |
| **interface** *if_name* | （任意）アクティブな変換をインターフェイス別に表示します。 |
| **local** *ip1*[*-ip2*] | （任意）ローカル IP アドレスまたはアドレスの範囲を指定して、アクティブな変換をクリアします。 |
| **lport** *port1*[*-port2*] | （任意）ローカル ポートまたはポートの範囲を指定して、アクティブな変換をクリアします。 |
| **netmask** *mask* | （任意）グローバル IP アドレスまたはローカル IP アドレスを限定するネットワークマスクまたは IPv6 プレフィックスを指定します。 |
| **type** *type* | （任意）タイプを指定して、アクティブな変換をクリアします。次のタイプのいずれかを入力できます。<br>• **dynamic**：ダイナミック変換を指定します。<br>• **portmap**：PAT グローバル変換を指定します。<br>• **static**：スタティック変換を指定します。<br>• **twice-nat**：手動 NAT 変換を指定します。 |

## 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

**clear xlate** コマンドは、変換スロットの内容をクリアします（「xlate」は変換スロットを意味します）。変換スロットは、キーの変更が行われた後でも存続できます。NAT ルールを追加、変更、または削除した後は、必ず **clear xlate** コマンドを使用します。

xlate は、NAT または PAT セッションについて記述します。これらのセッションは、**show xlate detail** コマンドで表示できます。

xlate には、スタティックとダイナミックという 2 つのタイプがあります。スタティック xlate は、スタティック NAT ルールを使用して作成される永続的な xlate です。**clear xlate** コマンドでは、スタティックエントリは消去されません。スタティック xlate は、スタティック NAT ルールを設定から削除することによってのみ削除できます。設定からスタティックルールを削除しても、スタティックルールを使用する既存の接続はトラフィックを引き続き転送できます。これらの接続を非アクティブにするには、**clear local-host** コマンドか **clear conn** コマンドを使用します。

ダイナミック xlate は、トラフィック処理で必要に応じて作成される xlate です。**clear xlate** コマンドを実行すると、ダイナミック xlate および関連した接続が削除されます。**clear local-host** または **clear conn** コマンドを使用して、xlate および関連した接続を消去することもできます。設定から NAT ルールを削除した場合、ダイナミック xlate および関連した接続がアクティブのまま残る場合があります。これらの接続を削除するには、**clear xlate** コマンドを使用します。

### 例

次に、現在の変換および接続スロット情報をクリアする例を示します。

```
> clear xlate global
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear local-host** | ローカル ホストのネットワーク情報をクリアします。 |
| **show conn** | すべてのアクティブ接続を表示します。 |
| **show local-host** | ローカル ホスト ネットワーク情報を表示します。 |
| **show xlate** | 現在の変換情報を表示します。 |

# clf - cz

# cluster disable

ユニットでクラスタリングを無効にするには、**cluster disable** コマンドを使用します。

**cluster disable**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.5 | 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、クラスタからクラスタユニットを手動で削除できます。このコマンドではクラスタリング設定は変更されないため、後で **cluster enable** コマンドを使用してクラスタに再追加できます。

### 例

次に、ユニットのクラスタリングを無効にする例を示します。

```
> cluster disable
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **cluster enable** | クラスタリングをイネーブルにします。 |
| **cluster master unit** | 新しいユニットをクラスタのマスターユニットとして設定します。 |
| **cluster remove unit** | ユニットをクラスタから削除します。 |
| **show cluster info** | クラスタ情報を表示します。 |
| **cluster exec** | すべてのクラスタ メンバーにコマンドを送信します。 |

# cluster enable

ユニットでクラスタリングを有効にするには、**cluster enable** コマンドを使用します。

**cluster enable**

## 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

最初にイネーブルにしたユニットについては、マスターユニット選定が発生します。最初のユニットは、その時点でクラスタの唯一のメンバーであるため、そのユニットがマスターユニットになります。この期間中にコンフィギュレーション変更を実行しないでください。

### 例

次に、ユニットでクラスタリングを有効にする例を示します。

```
> cluster enable
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **cluster disable** | クラスタリングをディセーブルにします。 |
| **cluster master unit** | 新しいユニットをクラスタのマスターユニットとして設定します。 |
| **cluster remove unit** | ユニットをクラスタから削除します。 |
| **show cluster info** | クラスタ情報を表示します。 |
| **cluster exec** | すべてのクラスタ メンバーにコマンドを送信します。 |

# cluster exec

クラスタ内のすべてのユニット、または特定のメンバーに対してコマンドを実行するには、**cluster exec** コマンドを使用します。

**cluster exec** ［**unit** *unit_name*］ *command*

## 構文の説明

| | |
|---|---|
| **unit** *unit_name* | （オプション）特定のユニットに対してコマンドを実行します。メンバー名を表示するには、**cluster exec unit ?** コマンドを入力するか（現在のユニットを除くすべての名前を表示する場合）、**show cluster info** コマンドを入力します。 |
| *command* | 実行するコマンドを指定します。 |

## 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

**show** コマンドをすべてのメンバーに送信すると、すべての出力が収集されて現在のユニットのコンソールに表示されます。**capture** や **copy** などのその他のコマンドも、クラスタ全体での実行を活用できます。

### 例

同じキャプチャ ファイルをクラスタ内のすべてのユニットから同時に TFTP サーバーにコピーするには、マスター ユニットで次のコマンドを入力します。

```
> cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

複数の PCAP ファイル（各ユニットから 1 つずつ）が TFTP サーバーにコピーされます。宛先のキャプチャファイル名には、capture1_device1.pcap、capture1_device2.pcap などのようにユニット名が自動的に付加されます、この例では、device1 と device2 がクラスタユニット名です。

次の例では、**cluster exec show port-channel** summary コマンドの出力に、クラスタの各メンバーの EtherChannel 情報が表示されています。

```
> cluster exec show port-channel summary
primary(LOCAL):*************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster  Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP       Yes  Gi0/0(P)
2         Po2             LACP       Yes  Gi0/1(P)
 secondary:*********************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster   Ports
```

```
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP       Yes   Gi0/0(P)
2         Po2             LACP       Yes   Gi0/1(P)
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **cluster enable** | ユニットでクラスタリングを有効にします。 |
| **cluster master unit** | 新しいユニットをクラスタのマスターユニットとして設定します。 |
| **cluster remove unit** | ユニットをクラスタから削除します。 |
| **show cluster info** | クラスタ情報を表示します。 |
| **cluster exec** | すべてのクラスタ メンバーにコマンドを送信します。 |

# cluster exec clear rule hits

クラスタ内のすべてのノードから、アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報をクリアし、ゼロにリセットするには、**cluster exec clear rule hits** コマンドを使用します。

**cluster exec clear rule hits** ［*id*］

## 構文の説明

| | |
|---|---|
| *id* | （オプション）ルールの ID。この引数を含めると、指定したルールのルールヒット情報のみがクリアされます。<br>ルール ID を識別するには、**show access-list** コマンドを使用します。ただし、このコマンドの出力にすべてのルールが表示されているわけではありません。次の URL で REST API GET 操作をトリガーすると、すべてのルールとルールの ID を確認できます。<br>• `/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true`<br>• `/api/fmc_config/v1/domain/{domainUUID}/policy/prefilterpolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true` |

## コマンド デフォルト

ルール ID を指定しない場合、すべてのルールのルールヒット情報がクリアされ、ゼロにリセットされます。

（注） このアクションは元に戻せないため、このコマンドの使用には注意が必要です。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.4 | このコマンドが導入されました。 |

## 使用上のガイドライン

ルールヒット情報は、アクセスコントロールルールとプレフィルタルールのみを対象としています。

### 例

すべてのルールヒット情報をクリアする例を次に示します。

```
> cluster exec clear rule hits
```

関連コマンド

| Command | 説明 |
|---|---|
| **show cluster rule hits** | クラスタ内のすべてのノードから、アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報をクリアし、ゼロにリセットします。 |
| **cluster exec show rule hits** | クラスタの各ノードから、アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報を分離形式で表示します。 |
| **show rule hits** | アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報を表示します。 |
| **clear rule hits** | アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報をクリアし、ゼロにリセットします。 |

# cluster exec show rule hits

クラスタの各ノードから、アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報を分離形式で表示するには、**cluster exec show rule hits** コマンドを使用します。

**cluster exec show rule hits** ［*id* | **raw** | **gt** *#hit-count* | **lt** *#hit-count* | **range** *#hit-count1 #hit-count2*］

## 構文の説明

| | |
|---|---|
| *id* | （オプション）ルールの ID。この引数を含めると、表示される情報は指定されたルールに限定されます。<br>ルール ID を識別するには、**show access-list** コマンドを使用します。ただし、このコマンドの出力にすべてのルールが表示されているわけではありません。次の URL で REST API GET 操作をトリガーすると、すべてのルールとルールの ID を確認できます。<br>• `/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true`<br>• `/api/fmc_config/v1/domain/{domainUUID}/policy/prefilterpolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true` |
| **raw** | （任意）.csv 形式でルールヒット情報を表示します。 |
| **gt** *#hit-count* | （任意）ヒットカウントが #hit-count より大きいすべてのルールを表示します。 |
| **lt** *#hit-count* | （任意）ヒットカウントが #hit-count より小さいすべてのルールを表示します。 |
| **range** *#hit-count1 #hit-count2* | （任意）#hit-count1 と #hit-count2 の間のヒットカウントを持つすべてのルールを表示します。 |

## コマンド デフォルト

ルール ID を指定しない場合、すべてのルールのルールヒット情報が表示されます。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.4 | このコマンドが導入されました。 |

## 使用上のガイドライン

ルールヒット情報は、アクセスコントロールルールとプレフィルタルールのみを対象としています。

### 例

次に、クラスタの各ノードからのルールヒット情報を分離形式で表示する例を示します。

```
> cluster exec show rule hits
unit-1-1(LOCAL):*******************************************************

RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)

-------------------------------------------------------------------------------------
268435260            1                   06:55:17 Mar 8 2019     06:55:17 Mar 8 2019

268435261            1                   06:55:19 Mar 8 2019     06:55:19 Mar 8 2019


unit-1-3:*************************************************************

RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)

-------------------------------------------------------------------------------------
268435264            1                   06:54:43 Mar 8 2019     06:54:43 Mar 8 2019

268435265            1                   06:54:57 Mar 8 2019     06:54:57 Mar 8 2019


unit-1-2:*************************************************************

RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)

-------------------------------------------------------------------------------------
268435270            1                   06:54:53 Mar 8 2019     06:54:53 Mar 8 2019

268435271            1                   06:55:01 Mar 8 2019     06:55:01 Mar 8 2019
```

### 関連コマンド

| Command | 説明 |
|---|---|
| **cluster exec clear rule hits** | クラスタ内のすべてのノードから、アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報をクリアし、ゼロにリセットします。 |
| **show cluster rule hits** | クラスタのすべてのノードからアクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報を集約形式で表示します。 |
| **show rule hits** | アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報を表示します。 |
| **clear rule hits** | アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報をクリアし、ゼロにリセットします。 |

# cluster master unit

新しいユニットをデバイスクラスタのマスターユニットとして設定するには、**cluster master unit** コマンドを使用します。

**cluster master unit** *unit_name*

## 構文の説明

| | |
|---|---|
| *unit_name* | 新しいマスター ユニットとなるローカル ユニット名を指定します。メンバー名を表示するには、**cluster master unit ?** コマンドを入力するか（現在のユニットを除くすべての名前を表示する場合）、**show cluster info** コマンドを入力します。 |

## 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

メイン クラスタ IP アドレスへの再接続が必要になります。

### 例

次に、新しいマスターユニットとして **device2** を設定する例を示します。

```
> cluster master unit device2
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **cluster enable** | ユニットでクラスタリングを有効にします。 |
| **cluster exec** | すべてのクラスタ メンバーにコマンドを送信します。 |
| **cluster remove unit** | ユニットをクラスタから削除します。 |
| **show cluster info** | クラスタ情報を表示します。 |

# cluster remove unit

クラスタからユニットを削除するには、**cluster remove unit** コマンドを使用します。

**cluster remove unit** *unit_name*

## 構文の説明

| | |
|---|---|
| *unit_name* | クラスタから削除するローカルユニット名を指定します。メンバー名を表示するには、**cluster remove unit ?** または **show cluster info** コマンドを入力します。 |

## 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

ブートストラップ コンフィギュレーションは変更されず、マスター ユニットから最後に同期されたコンフィギュレーションもそのままであるので、コンフィギュレーションを失わずに後でそのユニットを再度追加できます。マスター ユニットを削除するためにスレーブ ユニットでこのコマンドを入力した場合は、新しいマスター ユニットが選定されます。

### 例

次に、ユニット名を確認してから、device2 をクラスタから削除する例を示します。

```
> cluster remove unit ?
Current active units in the cluster:
device2
> cluster remove unit device2
WARNING: Clustering will be disabled on unit device2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **cluster enable** | ユニットでクラスタリングを有効にします。 |
| **cluster exec** | すべてのクラスタ メンバーにコマンドを送信します。 |
| **cluster master unit** | 新しいユニットをクラスタのマスターユニットとして設定します。 |
| **show cluster info** | クラスタ情報を表示します。 |

# cluster reset-interface-mode

クラスタリングを無効にした後でクラスタユニットをスタンドアロンモードに変換するには、**cluster reset-interface-mode** コマンドを使用します。

**cluster reset-interface-mode**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | このコマンドが導入されました。 |

## 使用上のガイドライン

**cluster disable** コマンドを使用して、最初にクラスタリングを無効にする必要があります。この **cluster reset-interface-mode** コマンドは 脅威に対する防御 の設定をクリアし、論理デバイスを再起動します。4100 シリーズの FXOS では、論理デバイスもスタンドアロンタイプのデバイスに変換されます。ブートストラップ設定とインターフェイスの割り当ては維持されます。

### 例

次に、クラスタリングを無効にしてから、クラスタリング設定を削除する例を示します。

```
> cluster disable
> cluster reset-interface-mode

Broadcast message from root@firepower (Tue Apr 27 18:36:12 2021):

The system is going down for reboot NOW!
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **cluster enable** | ユニットでクラスタリングを有効にします。 |
| **cluster exec** | すべてのクラスタ メンバーにコマンドを送信します。 |
| **cluster master unit** | 新しいユニットをクラスタのマスターユニットとして設定します。 |
| **show cluster info** | クラスタ情報を表示します。 |

# configure cert-update auto-update

脅威に対する防御デバイスでのCA証明書の自動更新を有効または無効にするには、**configure cert-update auto-update** コマンドを使用します。

**configure cert-update auto-update** { **enable** | **disable** }

## 構文の説明

| | |
|---|---|
| **enable** | CA 証明書の自動更新を有効にします。 |
| **disable** | CA 証明書の自動更新を無効にします。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0.5 | このコマンドが導入されました。 |

## 使用上のガイドライン

デフォルトでは、バージョン 7.0.5 をインストールまたは 脅威に対する防御 をアップグレードすると、CA 証明書が自動的に更新されます。この機能を無効にするには、**disable** キーワードを使用します。CA バンドルの自動更新を再度有効にするには、**enable** キーワードを使用します。CA 証明書の自動更新を有効にすると、更新プロセスはシステムで定義された時刻に毎日実行されます。

### 例

次に、**configure cert-update auto-update** コマンドの出力例を示します。

```
> configure cert-update auto-update disable
Autoupdate is disabled
> configure cert-update auto-update enable
Autoupdate is enabled and set for every day at 12:18 UTC
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show cert-update** | CA 証明書の自動更新のステータスを表示します。 |
| **configure cert-update run-now** | CA 証明書の更新をすぐに試します。 |
| **configure cert-update test** | シスコのサーバーからの最新のCA証明書を使用して接続チェックを実行します。 |

# configure cert-update run-now

CA 証明書の自動更新をすぐに実行するには、**configure cert-update run-now** コマンドを使用します。

**configure cert-update run-now** ［ **force** ］

## 構文の説明

| | |
|---|---|
| **force** | 接続チェックが失敗した場合でも、CA 証明書の更新を実行します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0.5 | このコマンドが導入されました。 |

## 使用上のガイドライン

CA 証明書をすぐに更新する場合は、**configure cert-update run-now** を使用します。ただし、シスコのサーバーのうちの 1 つでも SSL 接続チェックが失敗した場合、プロセスは終了します。接続に失敗しても更新を続行するには、**force** キーワードを使用します。たとえば、ローカル CA バンドルには、スマートライセンス、AMP 登録、ThreatGrid サービスなどのいくつかのシスコ サービスにアクセスするための証明書があり、シスコのスマートライセンスサービスへの接続に失敗した場合も、**configure cert-update run-now force** コマンドを使用すると、証明書の更新プロセスが実行されます。

（注） IPv6 のみの展開では、一部のシスコのサーバーが IPv6 をサポートしていないため、CA 証明書の自動更新が失敗することがあります。このような場合は、**configure cert-update run-now force** コマンドを使用して CA 証明書を強制的に更新します。

### 例

次に、接続チェックが失敗した場合の **configure cert-update run-now** コマンドの出力例を示します。

```
> configure cert-update run-now
Certs failed some connection checks.
```

次に、接続チェックが成功し、ローカル CA バンドルが更新された場合の **configure cert-update run-now** コマンドの出力例を示します。

```
>configure cert-update run-now
Certs have been replaced or was already up to date.
```

次に、**configure cert-update run-now force** コマンドの出力例を示します。

```
> configure cert-update run-now force
Certs failed some connection checks, but replace has been forced.
```

関連コマンド

| Command | 説明 |
|---|---|
| **configure cert-update auto-update** | 毎日の CA 証明書の自動更新を有効または無効にします。 |
| **show cert-update** | CA 証明書の自動更新のステータスを表示します。 |
| **configure cert-update test** | シスコのサーバーからの最新のCA証明書を使用して接続チェックを実行します。 |

# configure cert-update test

ローカルシステムの CA 証明書が最新であることを確認し、古い場合は、新しい CA バンドルを使用してサーバーへの SSL 接続をテストするには、**configure cert-update test** コマンドを使用します。

**configure cert-update test**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0.5 | 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 **configure cert-update test** コマンドは、ローカルシステムの CA バンドルを（シスコのサーバーからの）最新の CA バンドルと比較します。CA バンドルが最新の場合はチェックは実行されず、次の例のセクションに示すようにテスト結果が表示されます。CA バンドルが古い場合、ダウンロードされた CA バンドルに対して接続チェックが実行され、次の例のセクションに示すように結果が表示されます。

### 例

次に、ローカル CA バンドルが最新の場合の **configure cert-update test** コマンドからの出力例を示します。

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

次に、ローカル CA バンドルが古く、ダウンロードしたバンドルの接続チェックが失敗した場合の **configure cert-update test** コマンドの出力例を示します。

```
> configure cert-update test
Test failed, not able to fully connect.
```

次に、ローカル CA バンドルが古く、ダウンロードされたバンドルの接続チェックが成功した場合、または CA バンドルがすでに最新の場合の **configure cert-update test** コマンドからの出力の例を示します。

```
> configure cert-update test
Test succeeded, certs can safely be updated or are already up to date.
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure cert-update auto-update** | 毎日の CA 証明書の自動更新を有効または無効にします。 |
| **show cert-update** | CA 証明書の自動更新のステータスを表示します。 |
| **configure cert-update run-now** | CA 証明書の更新をすぐに試します。 |

# configure coredump packet-engine

パケットエンジンのコアダンプ生成を有効または無効にするには、**configure coredump packet-engine** コマンドを使用します。

**configure coredump packet-engine** {**enable** | **disable**}

## 構文の説明

| | |
|---|---|
| **disable** | パケットエンジンのコアダンプ生成を無効にします。 |
| **enable** | パケットエンジンのコアダンプ生成を有効にします。 |

## 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

パケットエンジンのコアダンプ生成は、デフォルトで有効になっています。

このコマンドは、Firepower 2100 シリーズのみで使用できます。サポートされていないプラットフォームでこのコマンドを入力すると、次のメッセージが返されます。

```
This command is not available on this platform.
```

### 例

次の例では、パケットエンジンのコアダンプ生成を無効にします。

```
> configure coredump packet-engine disable
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show coredump** | パケットエンジンのコアダンプ生成の設定を表示します。 |

# configure disable-https-access

HTTPS アクセスリストをクリアし、すべての IP アドレスからの HTTPS 接続の試行を拒否するようにデバイスを設定するには、**configure disable-https-access** コマンドを使用します。

**configure disable-https-access**

## 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

このコマンドを使用して、デバイスへの HTTPS アクセスを無効にします。ローカルマネージャである Device Manager を使用する場合は、HTTPS アクセスが必要です。

デバイスがローカル管理の高可用性グループ内のユニットである場合、アクティブユニットが次に設定の更新を展開するときに変更が上書きされます。これがアクティブユニットの場合、展開中に変更がピアに伝播されます。

### 例

次に、任意のアドレスからの HTTPS 接続を拒否するようにデバイスを設定する例を示します。

```
> configure disable-https-access
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure https-access-list** | 指定した IP アドレスからの HTTPS 接続を受け入れるようにデバイスを設定します。 |
| **show https-access-list** | 現在の HTTPS アクセスリストを表示します。 |

# configure disable-ssh-access

SSH アクセスリストをクリアし、すべての IP アドレスからの SSH 接続の試行を拒否するようにデバイスを設定するには、**configure disable-ssh-access** コマンドを使用します。

**configure disable-ssh-access**

## 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

デバイスへの SSH アクセスを無効にするには、このコマンドを使用します。これにより、コンソールポート経由以外の CLI アクセスが防止されます。

デバイスがローカル管理の高可用性グループ内のユニットである場合、アクティブユニットが次に設定の更新を展開するときに変更が上書きされます。これがアクティブユニットの場合、展開中に変更がピアに伝播されます。

### 例

次に、任意のアドレスからの SSH 接続を拒否するようにデバイスを設定する例を示します。

```
> configure disable-ssh-access
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure ssh-access-list** | 指定した IP アドレスからの SSH 接続を受け入れるようにデバイスを設定します。 |
| **show ssh-access-list** | 現在の SSH アクセスリストを表示します。 |

# configure firewall

ファイアウォールモードをトランスペアレントモードまたはルーテッドモードに設定するには、**configure firewall** コマンドを使用します。

**configure firewall** {**routed** | **transparent**}

## 構文の説明

| | |
|---|---|
| **routed** | ファイアウォール モードをルーテッド ファイアウォール モードに設定します。 |
| **transparent** | ファイアウォール モードをトランスペアレント ファイアウォールに設定します。 |

## コマンド デフォルト

デフォルトでは、デバイスはルーテッドモードです。

## 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

トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように動作するレイヤ2ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。

多くのコマンドは両方のモードではサポートされていないため、モードを変更した場合は、デバイスによってコンフィギュレーションがクリアされます。設定済みのコンフィギュレーションがある場合は、モードを変更する前にコンフィギュレーションをバックアップしてください。新しいコンフィギュレーション作成時の参照としてこのバックアップを使用できます。

（注） Device Manager を使用している場合、トランスペアレント ファイアウォール モードに切り替えることはできません。ローカルマネージャを使用していて、トランスペアレントモードに変換する場合は、まず **configure manager delete** を使用してマネージャを削除し、トランスペアレントモードに変換してから、**configure manager add** を使用して Management Center を指定する必要があります。

### 例

次に、ファイアウォール モードをトランスペアレントに変更する例を示します。

```
> configure firewall transparent
```

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。 |
| **show firewall** | ファイアウォール モードを表示します。 |

# configure flow-offload

このコマンドは、特定のフロー（つまり、トラフィック）をハードウェアで処理することで、それらのフローの加速を有効または無効にします。フロー処理をハードウェアにオフロードすると、パフォーマンスが向上するため、デフォルトで有効になっています。

ダイナミック フロー オフロードは、Firepower 4100/9300 シャーシの 脅威に対する防御 でサポートされます。ダイナミック フロー オフロードでは、ハードウェアにオフロードされるトラフィックを選択できます。これは、脅威に対する防御 デバイスのソフトウェアや CPU で処理されないことを意味します。

**configure flow-offload dynamic whitelist {enable | disable}**

## 構文の説明

| | |
|---|---|
| **dynamic whitelist enable** | ダイナミックオフロードを有効にします。 |
| **dynamic whitelist disable** | ダイナミックオフロードを無効にします。 |

## コマンド デフォルト

デフォルトでは、イネーブルです。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

## 使用上のガイドライン

ダイナミック フロー オフロードのサポートと制限については、『*Management Center Configuration Guide*』の共通ルール特性に関する章を参照してください。

### 例

次に、動的オフロードの無効化の例を示します。

```
> configure flow-offload dynamic whitelist disable
```

次に、動的オフロードの有効化の例を示します。

```
> configure flow-offload dynamic whitelist enable
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show flow-offload** | ダイナミック フロー オフロード カウンタ、統計情報、および情報を表示します。 |
| **clear flow-offload** | ダイナミック フロー オフロードのフロー、カウンタ、または統計をクリアします。 |

# configure high-availability

デバイス間のハイアベイラビリティ設定（フェールオーバー）を無効化、一時停止、または再開するには、**configure high-availability** コマンドを使用します。

**configure high-availability** {**disable** [**clear-interfaces**] | **resume** | **suspend** [**clear-interfaces**]}

## 構文の説明

| | |
|---|---|
| **clear-interfaces** | （任意）ハイアベイラビリティが無効化または一時停止されると、インターフェイス設定をクリアします。 |
| **disable** | このデバイスとそのピア間のハイアベイラビリティ関係を解除します。<br>このオプションは、ローカルで管理されているデバイスでは使用できません。代わりに Device Manager を使用します。誤って無効化コマンドを使用した場合は、続けて BreakHAStatus リソースを使用して脅威に対する防御 API コールを実行し、アクションを完了する必要があります。 |
| **resume** | このデバイスとそのピアの間で一時的に中断されたハイアベイラビリティ設定を再開します。ユニットは、ピア ユニットとアクティブ/スタンバイ ステータスをネゴシエートします。無効にした設定は再開できません。 |
| **suspend** | このデバイスとそのピア間のハイアベイラビリティ設定を一時的に停止します。後で設定を再開できます。<br>アクティブ装置からハイ アベイラビリティを中断すると、アクティブ装置とスタンバイ装置の両方で設定が中断されます。スタンバイ装置から中断すると、スタンバイ装置でのみ中断されますが、アクティブ装置は中断されたユニットへのフェールオーバーを試みなくなります。 |

## 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

2つのデバイススタックをハイアベイラビリティペアとして設定できます。これはフェールオーバー設定とも呼ばれ、ペアの一方のデバイスに障害が発生した場合、もう一方のデバイスが引き継ぎます。

何らかの理由でデバイスマネージャの設定を更新できない場合は、**configure high-availability** コマンドを使用してハイアベイラビリティペアを管理できます。たとえば、ハイアベイラビリティペアに到達できない場合は、**configure high-availability disable** を使用して両方のハイアベイラビリティピアからフェールオーバー設定を削除できます。

フェールオーバー設定を一時的に停止して、後で再開することもできます。ユニットでHAを一時的に停止することは、次の場合に役立ちます。

- 両方のユニットがアクティブ-アクティブの状況で、フェールオーバー リンクでの通信を修復しても、問題が解決されない場合。
- アクティブユニットまたはスタンバイ ユニットをトラブルシューティングする間、ユニットのフェールオーバーを発生させたくない場合。
- スタンバイデバイスのソフトウェアアップグレードをインストール中のフェールオーバーを防ぎたい場合。

ハイ アベイラビリティを中断すると、デバイスのペアがフェールオーバー ユニットとして動作しなくなります。現在アクティブなデバイスはアクティブなままで、すべてのユーザ接続を処理します。ただし、フェールオーバー基準はモニタされなくなり、システムにより現在の擬似-スタンバイ デバイスにフェールオーバーされることはなくなります。スタンバイ デバイスの設定は保持されますが、非アクティブのままです。

HA の中断と HA の破棄の主な違いは、中断された HA デバイスではハイ アベイラビリティ設定が保持されることです。HA を破棄すると、この設定は消去されます。そのため、中断されたシステムでHA を再開するためのオプションがあります。これにより、既存の設定が有効になり、2 台のデバイスがフェールオーバー ペアとして再び機能します。

（注） ハイ アベイラビリティの中断は一時的な状態です。ユニットをリロードすると、ハイ アベイラビリティ設定が自動的に再開され、ピアとアクティブ/スタンバイ ステータスがネゴシエートされます。

**例**

次の例は、ハイアベイラビリティ設定を一時的に停止してから再開する方法を示しています。

```
> show failover
Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.7(0)74, Mate 9.7(0)74
Serial Number: Ours 9A41CKDXQJU, Mate 9A3MFP0H1CP
Last Failover at: 19:23:17 UTC Oct 26 2016
        This host: Primary - Active
                Active time: 776671 (sec)
                slot 0: empty
                  Interface outside (192.168.77.1): Normal (Waiting)
                  Interface inside (192.168.87.1): Normal (Waiting)
```

```
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
        Other host: Secondary - Standby Ready
                Active time: 53 (sec)
                  Interface outside (0.0.0.0): Normal (Waiting)
                  Interface inside (0.0.0.0): Normal (Waiting)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
(...Output truncated...)
> configure high-availability suspend
Please ensure that no deployment operation is in progress before suspending
high-availability.
Please enter 'YES' to continue if there is no deployment operation in progress and
'NO' if you wish to abort: Yes
Successfully suspended high-availability.
> show failover
Failover Off
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
> configure high-availability resume
Successfully resumed high-availablity.
> show failover
Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
Unit Enrollment Hold action is active, timeout in 1792 seconds
Version: Ours 9.7(0)74, Mate 9.7(0)74
Serial Number: Ours 9A41CKDXQJU, Mate Unknown
Last Failover at: 20:26:06 UTC Nov 4 2016
        This host: Primary - Active
                Active time: 778071 (sec)
                slot 0: empty
                  Interface outside (192.168.77.1): Normal (Waiting)
                  Interface inside (192.168.87.1): Normal (Waiting)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
        Other host: Secondary - App Sync
                Active time: 53 (sec)
                  Interface outside (0.0.0.0): Unknown (Waiting)
                  Interface inside (0.0.0.0): Unknown (Waiting)
                  Interface diagnostic (0.0.0.0): Unknown (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
(...Output truncated...)
```

関連コマンド

| Command | 説明 |
| --- | --- |
| **show failover** | フェールオーバー（ハイアベイラビリティ）設定を示します。 |
| **show high-availability config** | フェールオーバー（ハイアベイラビリティ）設定を示します。**show failover** と同じ出力を提供します。 |

# configure https-access-list

指定したIPアドレスからのHTTPS接続を受け入れるようにデバイスを設定するには、**configure https-access-list** コマンドを使用します。

**configure https-access-list** *address_list*

## 構文の説明

| | |
|---|---|
| *address_list* | ホストまたはネットワークのIPアドレスのカンマ区切りリスト（IPv4 Classless Inter-Domain Routing（CIDR）表記または IPv6 プレフィックス長表記）。たとえば、10.100.10.0/24 または 2001:DB8::/96 のように表記します。<br>すべてのIPv4ホストを指定するには、「0.0.0.0/0」と入力します。すべての IPv6 ホストを指定するには、「::/0」のように指定します。 |

## 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

サポートされているすべてのホストまたはネットワークを1つのコマンドに含める必要があります。このコマンドで指定されたアドレスは、HTTPS アクセスリストの現在の内容を上書きします。

HTTPSアクセスを許可するだけでは、ユーザーはローカルマネージャにログインできません。設定ソフトウェアへのアクセスは、ユーザー名とパスワードによって制御されます。

デバイスがローカル管理の高可用性グループ内のユニットである場合、アクティブユニットが次に設定の更新を展開するときに変更が上書きされます。これがアクティブユニットの場合、展開中に変更がピアに伝播されます。

### 例

次の例では、任意の IPv4 または IPv6 アドレスからの HTTPS 接続を受け入れるようにデバイスを設定します。

```
> configure https-access-list 0.0.0.0/0,::/0
The https access list was changed successfully.
> show https-access-list
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:https
ACCEPT     tcp      anywhere             anywhere             state NEW tcp dpt:https
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure disable-https-access** | HTTPS アクセスリストをクリアします。 |

| Command | 説明 |
| --- | --- |
| **show https-access-list** | HTTPS アクセスリストを表示します。 |

# configure identity-subnet-filter

ユーザーから IP へ、およびセキュリティグループタグ（SGT）から IP へのマッピングを ISE から受信するときに、サブネットを除外するには **configure identity-subnet-filter** コマンドを使用します。通常は、Snort アイデンティティ正常性モニターのメモリエラーを防ぐために、メモリの少ない管理対象デバイスに対してこれを行う必要があります。

**configure identity-subnet-filter** { **add** | **remove** } *subnet*

## 構文の説明

| | |
|---|---|
| **add** | 指定したサブネットを除外したサブネットのリストに追加します。 |
| **remove** | 指定したサブネットを除外したサブネットのリストから削除します。 |
| *subnet* | 追加または除外するサブネットを指定します。 |

## 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。 |

### 例

次の例では、管理インターフェイスの静的 IPv6 アドレスを設定します。

```
> configure identity-subnet-filter 192.0.2.0/24
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show identity-subnet-filter** | ユーザーと IP、および SGT と IP のマッピングから現在除外されているサブネットを表示します。 |

# configure inspection

デフォルトのアプリケーションプロトコル検査エンジンを有効または無効にするには、**configure inspection** コマンドを使用します。

**configure inspection** *protocol* {**enable** | **disable**}

## 構文の説明

| | |
|---|---|
| **disable** | 検査エンジンを無効にします。 |
| **enable** | 検査エンジンを有効にします。 |
| *protocol* | 有効または無効にする検査プロトコル。オプションのリストについては、「使用上のガイドライン」を参照してください。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.2 | このコマンドが導入されました。 |

## 使用上のガイドライン

デフォルトの検査エンジンは、シスコテクニカルサポートの指示がある場合、または関連するトラフィックタイプがネットワーク上で発生しないことが確実な場合にのみ無効にしてください。たとえば、検査対象のポートですべてのトラフィックをブロックする場合、そのポートの検査は安全に無効化できます。これらの検査は、すべてのデータインターフェイスに適用されます。

これらの検査エンジンは、Snort インスペクションとは別のものです。これらのエンジンは、次のサービスを提供します。

- ピンホールの作成：一部のアプリケーションプロトコルは、標準ポートまたはネゴシエートされたポートでセカンダリ TCP または UDP 接続を開きます。インスペクションでは、これらのセカンダリ ポートのピンホールが開くため、ユーザーはそれらを許可するアクセス コントロール ルールを作成する必要はありません。
- NAT の書き換え：プロトコルの一部としてのパケットデータ内のセカンダリ接続用の FTP 埋め込み型 IP アドレスおよびポートなどのプロトコル。エンドポイントのいずれかに関与する NAT 変換がある場合、インスペクション エンジンは、埋め込まれたアドレスおよびポートの NAT 変換を反映するようにパケット データを書き換えます。セカンダリ接続は NAT の書き換えがないと動作しません。NAT の制限については、デバイス（Management Center または Device Manager）の設定に使用するマネージャの設定ガイドの「NAT」の章を参照してください。
- プロトコルの強制：一部のインスペクションでは、検査対象プロトコルにある程度の RFC への準拠が強制されます。

次の検査エンジンは、無効にした後で有効にできます。現在有効になっている検査エンジンを確認するには、**show running-config policy-map** コマンドを使用し、**inspect** コマンドを探しま

す。各検査のデフォルトパラメータの詳細を表示するには、**show running-config all policy-map** コマンドを使用します。

- **dcerpc**：（TCP ポート 135）。分散型コンピューティング環境/リモートプロシージャコール。DCERPC 検査エンジンは、Endpoint Mapper（EPM）とウェルノウン TCP ポート 135 上のクライアントとの間のネイティブ TCP 通信を検査します。DCERPC に基づく Microsoft リモートプロシージャ コール（MSRPC）は、Microsoft 分散クライアントおよびサーバーアプリケーションで広く使用されているプロトコルであり、ソフトウェア クライアントがサーバー上のプログラムをリモートで実行できるようにします。検査は、ピンホールの作成および NAT サービスを提供します。

- **dns**：（UDP ポート 53）。Domain Name System（ドメイン ネーム システム）。DNS は UDP ポート 53 で検査されます。検査は、NAT サービスとプロトコルの適用を提供します。NAT ルールで NAT の書き換えオプションを使用するには、この検査エンジンを有効にする必要があります。NAT の書き換えは、IPv4 ネットワークと IPv6 ネットワーク（NAT64/46）間で NAT を実行するときに頻繁に必要になります。

- **esmtp**：（TCP ポート 25）。Extended Simple Mail Transfer Protocol。ESMTP インスペクションでは、スパム、フィッシング、不正形式メッセージ攻撃、バッファ オーバーフロー/アンダーフロー攻撃などの攻撃を検出します。また、アプリケーションセキュリティとプロトコル準拠により、正常な ESMTP メッセージだけを通し、送受信者およびメール中継のブロックも行います。検査中に適用される制御の詳細については、**show running-config all policy-map** コマンドを使用し、「policy-map type inspect esmtp _default_esmtp_map」行および後続のパラメータを探して確認してください。

  ESMTP アプリケーションインスペクションは、ユーザーが使用できるコマンドとサーバーが返送するメッセージを制御し、その数を減らします。また、NAT サービスとプロトコル準拠を提供します。ESMTP インスペクションは、次の 3 つの主要なタスクを実行します。

  - SMTP 要求を 7 つの基本 SMTP コマンドと 8 つの拡張コマンドに制限します。サポートされるコマンドは次のとおりです。

    拡張 SMTP：AUTH、EHLO、ETRN、HELP、SAML、SEND、SOML、STARTTLS、および VRFY。

    SMTP（RFC 821）：DATA、HELO、MAIL、NOOP、QUIT、RCPT、RSET。

  - SMTP コマンド応答シーケンスをモニターします。

  - 監査証跡を生成します。Syslog 監査記録 108002 は、メールアドレスに埋め込まれた無効な文字が置き換えられた場合に生成されます。詳細については、RFC 821 を参照してください。

- **ftp**：（TCP ポート 21）。File Transfer Protocol（ファイル転送プロトコル）。検査は、ピンホールおよび NAT サービスを提供します。

- **h323_h225**：（TCP ポート 1720、UDP ポート 1718）。H.323 インスペクションは RAS、H.225、H.245 をサポートし、埋め込まれた IP アドレスとポートをすべて変換する機能を備えています。また、ステートトラッキングとフィルタリングを実行します。H.323 イン

スペクションは、Cisco CallManager などの H.323 準拠のアプリケーションをサポートします。H.323 は、国際電気通信連合によって定義されている、LAN を介したマルチメディア会議用のプロトコル群です。デバイスは、H.323 v3 機能の同一コールシグナリングチャネルでの複数コールを含めて、H.323 をバージョン 6 までサポートします。

H.323 インスペクションの 2 つの主要機能は次のとおりです。

- H.225 と H.245 の両メッセージ内に埋め込まれている必要な IPv4 アドレスを NAT 処理します。H.323 メッセージは PER 符号化形式で符号化されているため、ASA では ASN.1 デコーダを使用して H.323 メッセージを復号化します。
- ネゴシエートされた H.245 と RTP/RTCP 接続をダイナミックに割り当てます。RAS を使用すると、H.225 接続もダイナミックに割り当てることができます。

- **h323_ras**：（UDP ポート 1718 ー 1719）。**h323_h225**についての説明を参照してください。この検査は、RAS シグナリング用です。
- **icmp**：（ICMP トラフィックのみ）。ICMP インスペクション エンジンを使用すると、ICMP トラフィックが「セッション」を持つようになるため、TCP トラフィックや UDP トラフィックのように検査することが可能になります。ICMP 検査エンジンを使用しない場合、ICMP にデバイスの通過を許可しない（アクセスコントロールルールでブロックする）ことをお勧めします。ステートフル インスペクションを実行しないと、ICMP がネットワーク攻撃に利用される可能性があります。ICMP インスペクション エンジンは、要求ごとに応答が 1 つだけであること、シーケンス番号が正しいことを確認します。検査は、NAT サービスも提供します。
- **icmp_error**：（ICMP トラフィックのみ）。ICMP エラーインスペクションを有効にすると、デバイスは NAT の設定に基づいて、ICMP エラーメッセージを送信する中間ホップ用の変換セッションを作成します。デバイスは、変換後の IP アドレスでパケットを上書きします。これは、デバイスを通過するトレースルートに意味のある情報を提供するために必要です。
- **ip-options**：（RSVP トラフィックのみ）。IP オプションインスペクションは、パケットヘッダーの [IP Options] フィールドの内容に基づいて許可する IP パケットを制御します。Router Alert オプションが設定されているパケットは許可されます。その他のオプションが設定されているパケットはドロップされます。
- **netbios**：（UDP 送信元ポート 137、138）。NetBIOS Name Server over IP。NetBIOS アプリケーション インスペクションでは、NetBIOS ネーム サービス（NBNS）パケットおよび NetBIOS データグラム サービス パケットに埋め込まれている IP アドレスで NAT を実行します。また、プロトコル準拠チェックを行って、さまざまなフィールドの数や長さの整合性を確認します。
- **rsh**：（TCP ポート 514）。RSH プロトコルは、TCP ポート 514 で RSH クライアントから RSH サーバーへの TCP 接続を使用します。クライアントとサーバーは、クライアントが STDERR 出力ストリームを受信する TCP ポート番号をネゴシエートします。RSH インスペクションは、必要に応じて、ピンホールを開き、ネゴシエートされたポート番号の NAT をサポートします。

- **rtsp**：（TCP ポート 554）。Real-time Streaming Protocol。RTSP 検査エンジンを使用することにより、デバイスはRTSPパケットを通過させることができます。RTSPは、RealAudio、RealNetworks、Apple QuickTime、RealPlayer、およびCisco IP/TV 接続によって使用されます。RTSP アプリケーションは、制御チャネルとしての TCP（例外的に UDP）とともに予約済みポート 554 を使用します。デバイスは、RFC 2326 に準拠して TCP だけをサポートします。このTCP制御チャネルは、クライアント上で設定されているトランスポートモードに応じて、音声/ビデオ トラフィックの送信に使用されるデータ チャネルのネゴシエーションに使用されます。サポートされているRDTトランスポートは、rtp/avp、rtp/avp/udp、x-real-rdt、x-real-rdt/udp、x-pn-tng/udp です。

- **sqlnet**：（TCPポート1521）。インスペクション エンジンは、SQL*Net バージョン1および2をサポートしていますが、形式は Transparent Network Substrate（TNS）のみです。インスペクションでは、表形式データ ストリーム（TDS）形式をサポートしていません。SQL*Net メッセージは、埋め込まれたアドレスとポートについてスキャンされ、必要に応じて NAT の書き換えが適用されます。

  SQL 制御 TCP ポート 1521 と同じポートで SQL データ転送が行われる場合は、SQL*Net のインスペクションをディセーブルにします。SQL*Netインスペクションがイネーブルになっていると、セキュリティ アプライアンスはプロキシとして機能し、クライアントのウィンドウ サイズを65000から約16000に減らすため、データ転送の問題が発生します。

- **sip**：（TCP/UDP ポート 5060）。セッション開始プロトコル。SIP は、インターネット会議、テレフォニー、プレゼンス、イベント通知、およびインスタントメッセージングに広く使用されているプロトコルです。テキストベースの性質とその柔軟性により、SIP ネットワークは数多くのセキュリティ脅威にさらされます。SIPアプリケーション インスペクションでは、メッセージヘッダーおよび本文のアドレス変換、ポートの動的なオープン、および基本的な健全性チェックが行われます。

- **skinny**：（TCP ポート 2000）。Skinny Client Control Protocol（SCCP）。SCCP（Skinny）アプリケーション インスペクションでは、パケット データ、ピンホールの動的開放に埋め込まれている IP アドレスとポート番号を変換します。また、追加のプロトコル準拠チェックと基本的なステート トラッキングも行います。

- **sunrpc**：（TCP/UDP ポート 111）。Sun RPC は、NFS および NIS で使用されます。Sun RPC サービスはどのポート上でも実行できます。サーバー上の Sun RPC サービスにアクセスしようとするクライアントは、そのサービスが実行されているポートを知る必要があります。そのためには、予約済みポート111でポートマッパープロセス（通常はrpcbind）に照会します。

  クライアントがサービスの Sun RPC プログラム番号を送信すると、ポート マッパー プロセスはサービスのポート番号を応答します。クライアントは、ポート マッパー プロセスによって特定されたポートを指定して、Sun RPC クエリーをサーバーに送信します。サーバーが応答すると、デバイスはこのパケットを代行受信し、そのポートで TCP と UDP の両方の初期接続を開きます。Sun RPC ペイロード情報の NAT または PAT はサポートされていません。

- **tftp**：（UDP ポート 69）。Trivial File Transfer Protocol。インスペクション エンジンは、TFTP 読み取り要求（RRQ）、書き込み要求（WRQ）、およびエラー通知（ERROR）を

検査し、必要に応じてダイナミックに接続と変換を作成し、TFTP クライアントとサーバーの間のファイル転送を許可します。

有効な読み取り要求（RRQ）または書き込み要求（WRQ）を受信すると、必要に応じて、ダイナミックなセカンダリ チャネルと PAT 変換が割り当てられます。このセカンダリ チャネルは、これ以降 TFTP によってファイル転送またはエラー通知用に使用されます。TFTP サーバーだけがセカンダリ チャネル経由のトラフィックを開始できます。また、TFTP クライアントとサーバーの間に存在できる不完全なセカンダリ チャネルは 1 つまでです。サーバーからのエラー通知があると、セカンダリ チャネルは閉じます。TFTP トラフィックのリダイレクトにスタティック PAT が使用されている場合は、TFTP インスペクションをイネーブルにする必要があります。

- **xdmcp**：（UDP ポート 177）。X Display Manager Control Protocol。XDMCP は、UDP ポート 177 を使用して X セッションをネゴシエートするプロトコルです。X セッションは確立時に TCP を使用します。XWindows セッションを正常にネゴシエートして開始するために、デバイスは、Xhosted コンピュータからの TCP 戻り接続を許可する必要があります。TCP ポート経由の戻り接続を許可するには、アクセスコントロールルールを使用します。

  XWindows セッション中、マネージャはウェルノウンポート 6000 | n 上でディスプレイ Xserver と通信します。次の端末設定を行うと、各ディスプレイは別々に Xserver と接続します。**setenv DISPLAY Xserver:***n*、ここで n はディスプレイ番号です。

  XDMCP が使用されている場合、デバイスが必要に応じて NAT を実行できる IP アドレスを使用して、ディスプレイがネゴシエートされます。XDCMP インスペクションでは、PAT はサポートされません。

### 例

次に、現在のインスペクション設定を表示し、XDMCP インスペクションを無効にする例を示します。検査エンジンは有効化または無効化できますが、デフォルトの動作を変更することはできません。たとえば、次の出力は、DNS/TCP インスペクションが無効になっていることを示しています。**configure inspection** コマンドを使用して、DNS インスペクションを TCP トラフィックに適用するように設定することはできません。

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
```

```
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect dcerpc
!
> configure inspection xdmcp disable
Building configuration...
Cryptochecksum: 46dbea1d 51c2089a fcc3e42f 3dafd2d5
12386 bytes copied in 0.160 secs
[OK]
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect dcerpc
  inspect ftp
!
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show running-config policy-map** | インスペクション設定を含む、サービスポリシーのポリシーマップを表示します。 |
| **show service-policy** | インスペクションの統計情報を含むサービスポリシー統計情報を表示します。 |

# configure log-events-to-ramdisk

RAM ディスクへの接続イベントのロギングを有効または無効にして、システムパフォーマンスを向上させ、ソリッドステートドライブ（SSD）への接続イベントの書き込みに伴うディスクの消耗を減らすには、**configure log-events-to-ramdisk** コマンドを使用します。

**configure log-events-to-ramdisk** {**enable** | **disable**}

## 構文の説明

| | |
|---|---|
| **enable** | RAM ディスクへの接続イベントロギングを有効にします。 |
| **disable** | RAM ディスクへの接続イベントロギングを無効にします。接続イベントは SSD に記録されます。 |

## コマンド デフォルト

この機能をサポートするプラットフォームでは、デフォルトで有効になっています。

## 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

接続イベントを記録するために使用する RAM ディスクと物理 SSD を切り替えるには、このコマンドを使用します。有効にすると、接続イベントは RAM ディスクに記録されます。無効にすると、接続イベントは SSD に記録されます。停電が発生すると、RAM ディスクに記録された接続イベントは失われます。

このコマンドは、すべてのデバイスタイプで使用できるわけではありません。サポートされていないプラットフォームでこのコマンドを入力すると、次のメッセージが返されます。

```
This command is not available on this platform.
```

### 例

次に、RAM ディスクへのロギングを無効にする例を示します。

```
> configure log-events-to-ramdisk disable
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show log-events-to-disk** | 現在のロギングステータスを表示します。 |
| **show disk-manager** | システムの各パート（サイロ、低水位、高水位など）のディスク使用率の詳細情報を表示します。 |

# configure manager add

Management Center または CDO、あるいはその両方からの接続、またはそれに対する接続を開始するようにデバイスを設定するには、**configure manager add** コマンドを使用します。

⚠

**注意** リモートマネージャを追加すると、設定が工場出荷時のデフォルトにリセットされます。

**configure manager add** { *hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE** } *regkey* [ *nat_id* ] [ *display_name* ]

## 構文の説明

| | |
|---|---|
| *hostname* | Management Center のホスト名を指定します。 |
| *IPv4_address* | Management Center の IPv4 アドレスを指定します。 |
| *IPv6_address* | Management Center の IPv6 アドレスを指定します。 |
| *display_name* | **show managers** コマンドでこのマネージャを表示するための表示名を指定します。このオプションは、CDO をプライマリマネージャおよび分析専用のオンプレミス Management Center として識別する場合に役立ちます。この引数を指定しない場合、ファイアウォールは以下のいずれかの方法を使用して表示名を自動生成します。<br>• *hostname* \| *IP_address*（**DONTRESOLVE** キーワードを使用しない場合）<br>• **manager-***timestamp* |
| **DONTRESOLVE** | Management Center が直接アドレス指定できない場合は、**DONTRESOLVE** を使用します。**DONTRESOLVE** を使用する場合は、*nat_id* が必要です。このデバイスを Management Center に追加する場合は、デバイスの IP アドレスと *nat_id* の両方を必ず指定してください。接続の片側で IP アドレスを指定し、両側で同じ一意の NAT ID を指定する必要があります。 |
| *regkey* | デバイスを Management Center へ登録するのに必要な、英数字の一意の登録キーを指定します。英数字とハイフン（-）を使用できます。 |
| *nat_id* | 一方が IP アドレスを指定しない場合に、Management Center とデバイス間の登録プロセス中に使用されるオプションの英数字文字列です。Management Center で同じ NAT ID を指定します。管理にデータインターフェイスを使用する場合は、登録用に脅威に対する防御 と Management Center の両方で NAT ID を指定する必要があります。 |

## 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。 |
| 7.2 | 複数のマネージャに対するサポート（プライマリクラウド配信型 Management Center（CDO）と分析専用のオンプレミス Management Center）が追加されました。 |

## 使用上のガイドライン

デバイスを Management Center に登録するには、一意の英数字登録キーが常に必要です。

通常は、両方の IP アドレスが必要となります。つまり、Management Center でデバイスの IP アドレスを指定し、デバイスで Management Center の IP アドレスを指定します。ただし、IP アドレスの 1 つのみがわかっている場合は、最初の通信用に信頼を確立して正しい登録キーを検索するために、接続の両側に一意の NAT ID を指定する必要もあります。Management Center の IP アドレスがわからない場合は、IP アドレスまたはホスト名の代わりに **DONTRESOLVE** キーワードを使用します。

（注） 管理にデータインターフェイスを使用する場合は、登録用に 脅威に対する防御と Management Center の両方で NAT ID を指定する必要があります。

IPv4 を使用して登録した Management Center とデバイスを IPv6 に変換する場合は、デバイスをいったん削除してから Management Center で再登録する必要があります。

Management Center からローカルの Device Manager に変更するには、**configure manager delete** コマンドを使用してから **configure manager local** コマンドを使用します。

（注） デバイスをある Management Center から別のものに移動したり、ローカルマネージャに変更したりする前に、現在の Management Center から削除してください。

### 例

```
> configure manager add DONTRESOLVE abc123 efg456
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure manager delete** | 管理側 Management Center を削除します。 |
| **configure manager edit** | 管理側 Management Center を編集します。 |
| **configure manager local** | ローカルマネージャを設定します。 |
| **show managers** | 現在のマネージャを表示します。 |

# configure manager delete

現在のマネージャを無効にして、ノーマネージャモードを開始するには、**configure manager delete** コマンドを使用します。

⚠

**注意** マネージャを削除すると、脅威に対する防御 設定が工場出荷時の初期状態にリセットされます。ただし、管理ブートストラップ設定は維持されます。

**configure manager delete** *identifier*

## 構文の説明

| | |
|---|---|
| *identifier* | 複数のマネージャが定義されている場合は、識別子（UUID ともいう。**show managers** コマンドを参照）を指定する必要があります。各マネージャ エントリを個別に削除します。 |

## 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。 |
| 6.3 | 高可用性モードのチェックが追加されました。 |
| 7.2 | 複数のマネージャが設定されている場合に備えて、*identifier* 変数が追加されました。 |

## 使用上のガイドライン

現在のデバイスマネージャを削除するには、このコマンドを使用します。デバイスはノーマネージャモードになり、リモートマネージャ（Management Center）を追加したり、ローカルマネージャ（Device Manager ）を使用したりすることができるようになります。このコマンドは、ローカル管理とリモート管理を切り替えるときや、リモートマネージャがアクティブでなくなったときに使用します。

デバイスが高可用性用に設定されている場合は、まず、デバイスマネージャ(可能な場合)または **configure high-availability disable** コマンドを使用して、高可用性設定を中断する必要があります。アクティブなユニットから HA を中断することをお勧めします

このコマンドの動作は、現在のマネージャによって異なります。

- Remote：Management Center に到達できません。Management Center がまだ 脅威に対する防御 と通信している場合は、最初に Management Center のインベントリからデバイスを削除します。その後、このコマンドを使用できます。
- Local：制限なし。すぐにノーマネージャモードに移行します。

### 例

次の例では、現在のマネージャを削除して、ノーマネージャモードを開始します。

```
> configure manager delete

If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in
Cisco Smart Software Manager.
Do you want to continue[yes/no]:yes

DHCP Server Disabled
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure manager add** | デバイスの管理側 Management Center を設定します。 |
| **configure manager local** | ローカルマネージャを設定します。 |
| **show managers** | 現在のマネージャを表示します。 |

# configure manager edit

脅威に対する防御 設定の Management Center IP アドレスを編集するには、**configure manager edit** コマンドを使用します。

**configure manager edit** *identifier* { **hostname** { *ip_address* | *hostname* } | **displayname** *display_name* }

## 構文の説明

| | |
|---|---|
| *identifier* | Management Center の識別子（UUID）を指定します。**show managers** コマンドを使用して識別子を表示するか（7.2 以降）、Management Center CLI **show version** コマンドから UUID を取得します。 |
| **hostname** {*ip_address* \| *hostname*} | ホスト名/IPアドレスを変更します。 |
| **displayname** *display_name* | 表示名を変更します。 |

## 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。 |
| 7.2 | **hostname** キーワードと **displayname** キーワードが追加されました。 |

## 使用上のガイドライン

Management Center の IP アドレスまたはホスト名を変更する場合は、設定が一致するようにデバイス CLI で値を変更する必要があります。ほとんどの場合、管理接続はデバイスの Management Center IP アドレスまたはホスト名を変更せずに再確立されますが、少なくともデバイスを Management Center に追加して NAT ID のみを指定した場合は、接続が再確立されるようにするために、このタスクを実行する必要があります。他の場合でも、Management Center IP アドレスまたはホスト名を最新の状態に維持して、ネットワークの復元力を高めることを推奨します。

Management Center が **DONTRESOLVE** と NAT ID によって最初に識別された場合、このコマンドを使用して値をホスト名または IP アドレスに変更できます。IP アドレスまたはホスト名を **DONTRESOLVE** に変更することはできません。

管理接続がダウンした後、再確立されます。**sftunnel-status** コマンドを使用して、接続の状態をモニターできます。

### 例

Management Center UUID は Management Center を明確に識別します。たとえば、Management Center 高可用性の場合は、脅威に対する防御 デバイスでアクティブな Management Center を指定する必要があります。

識別子を表示するには、**show managers** コマンドを入力します。

```
> show managers
Type                      : Manager
Host                      : 10.10.1.4
Display name              : 10.10.1.4
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
Management type           : Configuration
```

UUID を取得したら、脅威に対する防御 デバイスの IP アドレスを編集できます。次に例を示します。

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 10.10.5.1
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure manager delete** | 管理側 Management Center を削除します。 |
| **configure manager add** | Management Center を設定します。 |
| **show managers** | 現在のマネージャを表示します。 |

# configure manager local

ローカルマネージャである Device Manager を使用するようにデバイスを設定するには、**configure manager local** コマンドを使用します。

**configure manager local**

## 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

このコマンドを使用して、ローカルマネージャである Device Manager を有効にします。個別の Management Center を使用しない場合は、ローカルマネージャを使用します。ローカルマネージャを有効にすると、**http://***management_ip_address* でブラウザを使用して Device Manager を開くことができます。

（注） システムがデータベースを再初期化する必要があるため、コマンドの完了に最大 4 ー 6 分かかります。Please be patient.

ローカルマネージャは、6.5 以降のほとんどのプラットフォームで使用できます。使用しているプラットフォームで使用できない場合は、**configure manager add** コマンドを使用してリモートマネージャを設定します。

### 追加の制限事項

- ローカルマネージャに切り替える前に、デバイスを No Manager モードにする必要があります。No Manager モードを開始するには、**configure manager delete** コマンドを使用します。現在のマネージャを確認するには、**show managers** コマンドを使用します。
- デバイスはトランスペアレント ファイアウォール モードでは動作できません（**configure firewall** コマンドを参照）。ローカルマネージャはルーテッドモードのみをサポートします。

### 例

次に、ローカルマネージャを設定する例を示します。

```
> configure manager local
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure manager add** | デバイスの管理側 Management Center を設定します。 |

| Command | 説明 |
| --- | --- |
| **configure manager delete** | 管理側 Management Center を削除します。 |
| **show managers** | 現在のマネージャを表示します。 |

# configure mini-coredump

ミニコアダンプの生成を有効または無効にするには、**configure mini-coredump** コマンドを使用します。

**configure mini-coredump** { **enable** | **disable** }

## 構文の説明

| | |
|---|---|
| **enable** | ミニコアダンプの生成を有効にします。 |
| **disable** | ミニコアダンプの生成を無効にします。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | このコマンドが導入されました。 |

## 使用上のガイドライン

ミニコアダンプの生成はデフォルトで有効になっています。

Snort 3 プロセスは、そのマルチスレッドの性質により、巨大なコアファイルをダンプします。これらのダンプは、ハードディスクに書き込まれるまでに時間がかかります。コアが書き込まれて新しいプロセスが開始されるまで、Snort のトラフィック検査は中断されます。ミニコアダンプを作成すると、時間の遅延が回避されます。ミニコアダンプには、デバッグに役立つスタックとメモリ値の重要な詳細が含まれています。

### 例

次に、ミニコアダンプの生成を無効にする例を示します。

```
> configure mini-coredump disable
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show mini-coredump status** | ミニコアダンプの生成の設定を表示します。 |

# configure network dns searchdomains

DNS 検索ドメインのリストを設定するには、**configure network dns searchdomains** コマンドを使用します。

**configure network dns searchdomains** ［*dnslist*］

## 構文の説明

| | |
|---|---|
| *dnslist* | DNS 検索ドメインのカンマ区切りリストを指定します。 |

## 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

DNS検索ドメインの現在のリストを新しいリストに置き換えるには、このコマンドを使用します。これらのドメインは、コマンド（**ping system** など）に完全修飾ドメイン名を指定しない場合にホスト名に追加されます。ドメインは、管理インターフェイスまたは管理インターフェイスを経由するコマンドでのみ、使用されます。

デバイスがローカル管理の高可用性グループ内のユニットである場合、アクティブユニットが次に設定の更新を展開するときに変更が上書きされます。これがアクティブユニットの場合、展開中に変更がピアに伝播されます。

### 例

次の例では、新しい検索ドメインリストを設定し、完全修飾ホスト名ではないホスト名で ping を実行します。

```
> configure network dns searchdomains example.com
> show dns system
search example.com
nameserver 10.163.47.11
> ping system www
PING www.example.com (10.163.4.161) 56(84) bytes of data.
64 bytes from www.example.com (10.163.4.161): icmp_seq=1 ttl=242 time=8.01 ms
64 bytes from www.example.com (10.163.4.161): icmp_seq=2 ttl=242 time=16.7 ms
^C
--- origin-www.cisco.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 7.961/10.216/16.718/3.755 ms
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure network dns servers** | DNS サーバーを設定します。 |
| **show dns system** | 管理インターフェイスの現在の DNS 設定を表示します。 |

# configure network dns servers

管理インターフェイスの DNS サーバーを設定するには、**configure network dns servers** コマンドを使用します。

**configure nework dns servers** ［*dnslist*］

## 構文の説明

| | |
|---|---|
| *dnslist* | DNS サーバーのカンマ区切りリストを指定します。 |

## 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

DNS サーバーの現在のリストを新しいリストに置き換えるには、このコマンドを使用します。これらのサーバーは管理インターフェイスでのみ使用されます。データインターフェイスを通過するコマンドの完全修飾ドメイン名を解決することはできません。

バージョン 6.3 以降、ローカル管理デバイス限定で、データインターフェイスおよび管理インターフェイスが同じ DNS グループを使用している場合、そのグループがマネージャからの次の展開時に更新されます。これは、データインターフェイスで使用されている DNS グループにも変更が適用されることを意味します。管理インターフェイスの変更はすぐに反映されます。すべての DNS 変更は、このコマンドを使用するのではなく、ローカルマネージャから行うことを推奨します。

デバイスがローカル管理の高可用性グループ内のユニットである場合、アクティブユニットが次に設定の更新を展開するときに変更が上書きされます。これがアクティブユニットの場合、展開中に変更がピアに伝播されます。

### 例

次に、管理インターフェイスの DNS サーバーを設定する例を示します。

```
> configure network dns servers 10.163.47.11,10.124.1.10
> show dns system
search example.com
nameserver 10.163.47.11
nameserver 10.124.1.10
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure network dns searchdomains** | DNS 検索ドメインを設定します。 |
| **show dns system** | 管理インターフェイスの現在の DNS 設定を表示します。 |

# configure network hostname

デバイスの管理インターフェイスのホスト名を設定するには、**configure network hostname** コマンドを使用します。

**configure network hostname** *name*

## 構文の説明

| | |
|---|---|
| *name* | 新しいホスト名を指定します。 |

## 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

システムホスト名は複数の場所で定義されます。マネージャからホスト名を更新すると、システムはすべてのプロセスでホスト名を同期します。Device Manager（ローカルマネージャ）を使用しているときにこのコマンドを使用する場合は、すべてのシステムプロセスで同じ名前が使用されるように、Device Manager から変更を展開して更新を完了する必要があります。

### 例

次の例では、ホスト名を sfrocks に設定します。

```
> configure network hostname sfrocks
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show network** | 管理インターフェイスの設定を表示します。 |

# configure network http-proxy

管理インターフェイスの HTTP プロキシを設定するには、**configure network http-proxy** コマンドを使用します。

**configure network http-proxy**

## 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。 |
| 6.6 | このコマンドは、ローカル管理システムで機能するようになりました。 |

## 使用上のガイドライン

このコマンドを使用して、デバイスの HTTP プロキシアドレスを設定します。コマンド発行後に、HTTP プロキシのアドレスとポート、プロキシの認証が必要かどうかをユーザーは尋ねられます。認証が必要な場合はプロキシのユーザー名、プロキシのパスワード、およびプロキシのパスワードの確認を入力するよう要求されます。

### 例

次に、管理インターフェイスの HTTP プロキシを設定する例を示します。この例では、認証が設定されます。入力したパスワードは CLI に表示されません。

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure network http-proxy-disable** | HTTP プロキシ設定を無効化します。 |
| **show network** | 管理インターフェイスの設定を表示します。 |

# configure network http-proxy-disable

管理インターフェイスの HTTP プロキシを削除するには、**configure network http-proxy-disable** コマンドを使用します。

**configure network http-proxy-disable**

## 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、管理インターフェイスの HTTP プロキシを削除する例を示します。

```
> show network
(...Output Truncated...)
===============[ Proxy Information ]================
State                        : Enabled
HTTP Proxy                   : 10.100.10.10
Port                         : 80
Authentication               : Enabled
Username                     : proxyuser
> configure network http-proxy-disable
Are you sure that you wish to delete the current http-proxy configuration? (y/n): y
Configuration successfully deleted.
> show network
(...Output Truncated...)
===============[ Proxy Information ]================
State                        : Disabled
Authentication               : Disabled
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure network http-proxy** | HTTP プロキシを設定します。 |
| **show network** | 管理インターフェイスの設定を表示します。 |

# configure network ipv4 delete

デバイスの管理インターフェイスの IPv4 設定を無効にするには、**configure network ipv4 delete** コマンドを使用します。

**configure network ipv4 delete** ［*management_interface*］

## 構文の説明

| | |
|---|---|
| *management_ interface* | 管理インターフェイスを指定します。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、Firepower 4100 および 9300 シリーズ デバイスでのみサポートされます。他のプラットフォームではこのパラメータを指定しないでください。Firepower 4100 および 9300 の管理インターフェイス ID は、デフォルトの管理インターフェイスの場合は **management0**、任意のイベントインターフェイスの場合は **management1** です。 |

## 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

デバイスの管理インターフェイスの IPv4 設定を無効にするには、このコマンドを使用します。削除した IP アドレスに接続すると、デバイスへの接続が失われます。IPv4 アドレスを削除する前に、IPv6 アドレスが設定されていることを確認します。

IPv4 アドレスを変更するために設定を削除する必要はありません。IPv4 アドレッシングを維持しつつ、アドレスのみを変更する場合は、**configure network ipv4 manual** コマンドか **configure network ipv4 dhcp** コマンドを使用します。

### 例

次の例では、IPv4 アドレス設定を削除します。

```
> configure network ipv4 delete
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure network ipv4 dhcp** | DHCP サーバーからアドレスを取得するように IPv4 を設定します。 |
| **configure network ipv4 manual** | 静的 IP アドレスを使用して IPv4 を手動で設定します。 |

| Command | 説明 |
| --- | --- |
| **show network** | 管理インターフェイスの設定を表示します。 |

# configure network ipv4 dhcp

DHCP サーバーから IPv4 アドレスを取得するように管理インターフェイスを設定するには、**configure network ipv4 dhcp** コマンドを使用します。

**configure network ipv4 dhcp** ［*management_interface*］

## 構文の説明

| | |
|---|---|
| *management_ interface* | 管理インターフェイスを指定します。DHCP はデフォルトの管理インターフェイスでのみサポートされているため、この引数を使用する必要はありません。 |

## 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

このコマンドを使用して、デバイスの管理インターフェイスが DHCP サーバーから IPv4 設定を受信するように指定します。管理インターフェイスは DHCP サーバーと通信して、設定情報を取得します。

（注） **configure network management-data-interface** コマンドを使用して Management Center アクセス用のデータインターフェイスを設定している場合、管理インターフェイスの DHCP を使用することはできないため、IP アドレスを手動で設定する必要があります。これは、**data-interfaces** である必要があるデフォルトルートが DHCP サーバーから受信したルートで上書きされる可能性があるためです。管理インターフェイスを使用する予定がない場合でも、プライベートアドレスなどの IP アドレスを設定する必要があります。この IP アドレスは、トラフィックがデータインターフェイスに転送されるときに NAT 処理されます。

### 例

次の例では、DHCP を使用して IPv4 アドレスを取得するように管理インターフェイスを設定する方法を示します。

```
> configure network ipv4 dhcp
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure network ipv4 delete** | IPv4 ネットワーキングを無効にします。 |
| **configure network ipv4 manual** | IPv4 を手動で設定します。 |

| Command | 説明 |
| --- | --- |
| **show network** | 管理インターフェイスの設定を表示します。 |

# configure network ipv4 dhcp-dp-route

管理インターフェイスのデフォルト IP アドレス、ネットワークマスク、およびゲートウェイを復元するには、**configure network ipv4 dhcp-dp-route** コマンドを使用します。このコマンドでは、DNS サーバーなどの他のネットワーク設定は変更されません。

（注） このコマンドは、Secure Firewall Threat Defense Virtual（Threat Defense Virtual）、Firepower 4100/9300、または ISA 3000 ではサポートされていません。

**configure network ipv4 dhcp-dp-route**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.6 | このコマンドが導入されました。 |

## 使用上のガイドライン

いずれかのバージョンの IP アドレスを指定しなかった場合でも、このコマンドの IPv4 バージョンと IPv6 バージョンの両方を入力して、設定を工場出荷時のデフォルトに復元する必要があります。

### 例

次の例では、管理インターフェイスのデフォルト設定を復元します。

```
> configure network ipv4 dhcp-dp-route
Creating /etc/sf/sftunnel.conf with header line
Set up management0 as DHCP ipv4 client with the default route through data interfaces.
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure network ipv4 delete** | IPv4 ネットワーキングを無効にします。 |
| **configure network ipv4 dhcp** | DHCP 経由で IPv4 を設定します。 |
| **configure network ipv4 manual** | IPv4 を手動で設定します。 |
| **show network** | 管理インターフェイスの設定を表示します。 |

# configure network ipv4 dhcp-server-disable

管理インターフェイスで DHCP サーバーを無効にするには、**configure network ipv4 dhcp-server-disable** コマンドを使用します。

**configure network ipv4 dhcp-server-disable**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.2 | このコマンドが導入されました。 |

## 使用上のガイドライン

管理インターフェイスにアクティブなDHCPサーバーがある場合は、それを無効にできます。無効になっている場合、管理ネットワーク上のクライアントに静的アドレスを設定するか、ネットワーク上の別のデバイスをDHCPサーバーサービスを提供するデバイスとして設定する必要があります。

DHCPを使用してアドレスを取得するように管理IPアドレスを変更すると、DHCPサーバーは（有効な場合）自動的に無効になります。

### 例

次の例は、DHCP サーバーが有効になっているかどうかを確認してから、無効にする方法を示しています。

```
> show network-dhcp-server
DHCP Server Enabled
192.168.45.46-192.168.45.254
> configure network ipv4 dhcp-server-disable
DCHP Server Disabled
> show network-dhcp-server
DHCP Server Disabled
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure network ipv4 dhcp-server-enable** | 管理インターフェイスの DHCP サーバーを有効にします。 |
| **show dhcp-server** | 管理インターフェイスの DHCP サーバーのステータスを表示します。 |

# configure network ipv4 dhcp-server-enable

管理インターフェイスでオプションの DHCP サーバーを有効にするには、**configure network ipv4 dhcp-server-enable** コマンドを使用します。

**configure network ipv4 dhcp-server-enable** *start_ip_address end_ip_address*

## 構文の説明

| | |
|---|---|
| *start_ip_address*<br>*end_ip_address* | DHCP アドレスプールの開始および終了 IPv4 アドレスを指定します。管理インターフェイスは、DHCP クライアント要求を受信すると、このプールからアドレスを提供します。プールは、管理 IPv4 アドレスと同じサブネットにある必要があります。<br>DHCP アドレスプールにネットワークアドレス、管理アドレス、またはブロードキャストアドレスを含めないでください。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.2 | このコマンドが導入されました。 |

## 使用上のガイドライン

管理インターフェイスの手動（静的）IPv4 アドレスを設定する場合は、管理ネットワーク上のエンドポイントにアドレスを提供するように DHCP サーバーを設定できます。

サーバーを有効にする前に、管理ネットワーク上に他の DHCP サーバーがないことを確認します。ネットワークごとに最大 1 台の DHCP サーバーを設定できます。1 台を超えると、予測できない結果が生じることがあります。

（注） このコマンドは、Threat Defense Virtual デバイスではサポートされません。

### 例

次に、DHCP サーバーを設定し、そのステータスを表示する例を示します。

```
> configure network ipv4 dhcp-server-enable 192.168.45.46 192.168.45.254
DHCP Server Enabled
> show network-dhcp-server
DHCP Server Enabled
192.168.45.46-192.168.45.254
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure network ipv4 dhcp-server-disable** | 管理インターフェイスの DHCP サーバーを無効にします。 |

| Command | 説明 |
| --- | --- |
| **show dhcp-server** | 管理インターフェイスの DHCP サーバーのステータスを表示します。 |

# configure network ipv4 manual

管理インターフェイスで静的 IPv4 アドレスを設定するには、**configure network ipv4 manual** コマンドを使用します。

**configure network ipv4 manual** *ipaddr netmask gw* ［*management_interface*］

## 構文の説明

| | |
|---|---|
| *ipaddr* | IP アドレスを指定します。 |
| *netmask* | サブネット マスクを指定します。 |
| *gw* | デフォルトゲートウェイの IPv4 アドレスを指定します。<br><br>管理ネットワーク上の明示的なゲートウェイではなく、ゲートウェイとしてデバイス上のデータインターフェイスを使用する **data-interfaces** を指定するオプションがあります。管理用物理インターフェイスを別の管理ネットワークに接続したくない場合は、データインターフェイスを使用します。Management Center データインターフェイスの管理については、**configure network management-data-interface** コマンドを参照してください。<br><br>このコマンド内の gw は、デバイスのデフォルトルートを作成するために使用されることに注意してください。イベント専用インターフェイスを設定する場合は、コマンドの一部として gw を入力する必要があります。ただし、このエントリは、指定した値にデフォルトルートを設定するだけで、イベントインターフェイスの個別のスタティックルートは作成しません。管理インターフェイスとは異なるネットワークでイベント専用インターフェイスを使用している場合は、管理インターフェイスとともに使用するように gw を設定し、**configure network static-routes** コマンドを使用してイベント専用インターフェイス用に別のスタティックルートを作成することを推奨します。 |
| *management_ interface* | 管理インターフェイスを指定します。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、Firepower 4100 および 9300 シリーズ デバイスでのみサポートされます。他のプラットフォームではこのパラメータを指定しないでください。Firepower 4100 および 9300 の管理インターフェイス ID は、デフォルトの管理インターフェイスの場合は **management0**、任意のイベントインターフェイスの場合は **management1** です。 |

## 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。 |

| リリース | 変更内容 |
|---|---|
| 6.2 | ゲートウェイの **data-interfaces** キーワードが追加されました。 |
| 6.7 | **data-interfaces** キーワードがデータインターフェイスでの Management Center 管理に使用できるようになりました。 |

## 使用上のガイドライン

**configure network management-data-interface** コマンドを使用して Management Center アクセス用のデータインターフェイスを設定する場合は、手動 IP アドレス（IPv4 または IPv6）を設定する必要があります。管理インターフェイスを使用する予定がない場合でも、プライベートアドレスなどの IP アドレスを設定する必要があります。この IP アドレスは、トラフィックがデータインターフェイスに転送されるときに NAT 処理されます。data-interfaces である必要があるデフォルトルートは、DHCPサーバーから受信したルートで上書きされる可能性があるため、DHCP（デフォルト）は使用できません。

### 例

次の例では、管理インターフェイスで静的 IPv4 アドレスを設定します。

```
> configure network ipv4 manual 10.123.1.10 255.255.0.0 10.123.1.1
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure network ipv4 delete** | IPv4 ネットワーキングを無効にします。 |
| **configure network ipv4 dhcp** | DHCP 経由で IPv4 を設定します。 |
| **show network** | 管理インターフェイスの設定を表示します。 |

# configure network ipv6 delete

デバイスの管理インターフェイスの IPv6 設定を無効にするには、**configure network ipv4 delete** コマンドを使用します。

**configure network ipv6 delete** ［*management_interface*］

## 構文の説明

| | |
|---|---|
| *management_ interface* | 管理インターフェイスを指定します。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、Firepower 4100 および 9300 シリーズ デバイスでのみサポートされます。他のプラットフォームではこのパラメータを指定しないでください。Firepower 4100 および 9300 の管理インターフェイス ID は、デフォルトの管理インターフェイスの場合は **management0**、任意のイベントインターフェイスの場合は **management1** です。 |

## 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

このコマンドを使用して、デバイスの管理インターフェイスの IPv6 設定を無効にします。削除する IP アドレスに接続している場合、デバイスへの接続が失われます。IPv6 アドレスを削除する前に、IPv4 アドレスが設定されていることを確認します。

IPv6 アドレスを変更するために設定を削除する必要はありません。IPv6 アドレッシングを維持しつつ、アドレスのみを変更する場合は、**configure network ipv6** {**manual** | **dhcp** | **router**} コマンドを使用します。

### 例

次の例では、IPv6 アドレス設定を削除します。

```
> configure network ipv6 delete
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure network ipv6 dhcp** | DHCP 経由で IPv6 を設定します。 |
| **configure network ipv6 manual** | IPv6 を手動で設定します。 |

| Command | 説明 |
| --- | --- |
| **configure network ipv6 router** | ルータ経由で IPv6 を設定します。 |
| **show network** | 管理インターフェイスの設定を表示します。 |

# configure network ipv6 destination-unreachable

管理インターフェイスで IPv6 を使用しているときに ICMPv6 宛先到達不能パケットを有効または無効にするには、**configure network ipv6 destination-unreachable** コマンドを使用します。

**configure network ipv6 destination-unreachable** {**enable** | **disable**}

## 構文の説明

| | |
|---|---|
| **enable** | 宛先到達不能パケットを有効にします。この設定は、デフォルトです。 |
| **disable** | 宛先到達不能パケットを無効にします。 |

## コマンド デフォルト

デフォルトでは、イネーブルです。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.4.0 | コマンドが追加されました。 |

## 使用上のガイドライン

これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。

### 例

次に、宛先到達不能メッセージを無効にする例を示します。

```
> configure network ipv6 destination-unreachable disable
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure network ipv6 delete** | IPv6 ネットワーキングを無効にします。 |
| **configure network ipv6 echo-reply** | エコー応答パケットを有効または無効にします。 |
| **configure network ipv6 manual** | IPv6 を手動で設定します。 |
| **configure network ipv6 router** | ルータ経由で IPv6 を設定します。 |
| **show network** | 管理インターフェイスの設定を表示します。 |

# configure network ipv6 dhcp

DHCP サーバーから IPv6 アドレスを取得するように管理インターフェイスを設定するには、**configure network ipv6 dhcp** コマンドを使用します。

**configure network ipv6 dhcp** ［*management_interface*］

## 構文の説明

| | |
|---|---|
| *management_ interface* | 管理インターフェイスを指定します。DHCPはデフォルトの管理インターフェイスでのみサポートされているため、この引数を使用する必要はありません。 |

## 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

このコマンドを使用して、デバイスの管理インターフェイスが DHCP サーバーから IPv6 設定を受信するように指定します。管理インターフェイスはDHCPサーバーと通信して、設定情報を取得します。

（注） **configure network management-data-interface** コマンドを使用して Management Center アクセス用のデータインターフェイスを設定している場合、管理インターフェイスのDHCPを使用することはできないため、IP アドレスを手動で設定する必要があります。これは、**data-interfaces** である必要があるデフォルトルートがDHCPサーバーから受信したルートで上書きされる可能性があるためです。管理インターフェイスを使用する予定がない場合でも、プライベートアドレスなどの IP アドレスを設定する必要があります。この IP アドレスは、トラフィックがデータインターフェイスに転送されるときに NAT 処理されます。

### 例

次の例では、DHCP を使用して IPv6 アドレスを取得するように管理インターフェイスを設定する方法を示します。

```
> configure network ipv6 dhcp
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure network ipv6 delete** | IPv6 ネットワーキングを無効にします。 |
| **configure network ipv6 manual** | IPv6 を手動で設定します。 |

| Command | 説明 |
| --- | --- |
| **configure network ipv6 router** | ルータ経由で IPv6 を設定します。 |
| **show network** | 管理インターフェイスの設定を表示します。 |

# configure network ipv6 dhcp-dp-route

管理インターフェイスのデフォルト IP アドレス、ネットワークマスク、およびゲートウェイを復元するには、**configure network ipv6 dhcp-dp-route** コマンドを使用します。このコマンドでは、DNS サーバーなどの他のネットワーク設定は変更されません。

（注） このコマンドは、Threat Defense Virtual、Firepower 4100/9300、または ISA 3000 ではサポートされていません。

**configure network ipv6 dhcp-dp-route**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.6 | このコマンドが導入されました。 |

## 使用上のガイドライン

いずれかのバージョンの IP アドレスを指定しなかった場合でも、このコマンドの IPv4 バージョンと IPv6 バージョンの両方を入力して、設定を工場出荷時のデフォルトに復元する必要があります。

### 例

次の例では、管理インターフェイスのデフォルト設定を復元します。

```
> configure network ipv6 dhcp-dp-route
Set up management0 as DHCP ipv6 client with the default route through data interfaces.
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure network ipv6 delete** | IPv6 ネットワーキングを無効にします。 |
| **configure network ipv6 dhcp** | DHCP 経由で IPv6 を設定します。 |
| **configure network ipv6 manual** | IPv6 を手動で設定します。 |
| **show network** | 管理インターフェイスの設定を表示します。 |

# configure network ipv6 echo-reply

管理インターフェイスで IPv6 を使用しているときに ICMPv6 エコー応答パケットを有効または無効にするには、**configure network ipv6 echo-reply** コマンドを使用します。

**configure network ipv6 echo-reply** {**enable** | **disable**}

## 構文の説明

| | |
|---|---|
| **enable** | エコー応答パケットを有効にします。この設定は、デフォルトです。 |
| **disable** | エコー応答パケットを無効にします。 |

## コマンド デフォルト

デフォルトでは、イネーブルです。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.4.0 | コマンドが追加されました。 |

## 使用上のガイドライン

これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。エコー応答パケットを無効にすると、デバイスの管理インターフェイスにテスト目的で IPv6 ping を使用できなくなります。

### 例

次の例では、エコー応答メッセージを無効にします。

```
> configure network ipv6 echo-reply disable
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure network ipv6 delete** | IPv6 ネットワーキングを無効にします。 |
| **configure network ipv6 destination-unreachable** | 宛先到達不能パケットを有効または無効にします。 |
| **configure network ipv6 manual** | IPv6 を手動で設定します。 |
| **configure network ipv6 router** | ルータ経由で IPv6 を設定します。 |
| **show network** | 管理インターフェイスの設定を表示します。 |

# configure network ipv6 manual

管理インターフェイスで静的 IPv6 アドレスを設定するには、**configure network ipv6 manual** コマンドを使用します。

**configure network ipv6 manual** *ip6addr ip6prefix* ［*ip6gw*］［*management_interface*］

## 構文の説明

| | |
|---|---|
| *ip6addr* | IP アドレスを指定します。 |
| *ip6prefix* | プレフィックス長を指定します。 |
| *ip6gw* | デフォルトゲートウェイの IPv6 アドレスを指定します。<br>管理ネットワーク上の明示的なゲートウェイではなく、ゲートウェイとしてデバイス上のデータインターフェイスを使用する **data-interfaces** を指定するオプションがあります。管理用物理インターフェイスを別の管理ネットワークに接続したくない場合は、データインターフェイスを使用します。Management Center データインターフェイスの管理については、**configure network management-data-interface** コマンドを参照してください。<br>このコマンド内の ip6gw は、デバイスのデフォルトルートを作成するために使用されることに注意してください。イベント専用インターフェイスを設定する場合は、コマンドの一部として ip6gw を入力する必要があります。ただし、このエントリは、指定した値にデフォルトルートを設定するだけで、イベントインターフェイスの個別のスタティックルートは作成しません。管理インターフェイスとは異なるネットワークでイベント専用インターフェイスを使用している場合は、管理インターフェイスとともに使用するように ip6gw を設定し、**configure network static-routes** コマンドを使用してイベント専用インターフェイス用に別のスタティックルートを作成することを推奨します。 |
| *management_ interface* | 管理インターフェイスを指定します。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、Firepower 4100 および 9300 シリーズ デバイスでのみサポートされます。他のプラットフォームではこのパラメータを指定しないでください。Firepower 4100 および 9300 の管理インターフェイス ID は、デフォルトの管理インターフェイスの場合は **management0**、任意のイベントインターフェイスの場合は **management1** です。 |

## 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。 |
| 6.2 | ゲートウェイの **data-interfaces** キーワードが追加されました。 |
| 6.7 | **data-interfaces** キーワードがデータインターフェイスでの Management Center 管理に使用できるようになりました。 |

## 使用上のガイドライン

**configure network management-data-interface** コマンドを使用して Management Center アクセス用のデータインターフェイスを設定する場合は、手動 IP アドレス（IPv4 または IPv6）を設定する必要があります。管理インターフェイスを使用する予定がない場合でも、プライベートアドレスなどの IP アドレスを設定する必要があります。この IP アドレスは、トラフィックがデータインターフェイスに転送されるときに NAT 処理されます。data-interfaces である必要があるデフォルトルートは、DHCP サーバーから受信したルートで上書きされる可能性があるため、DHCP（デフォルト）は使用できません。

### 例

次の例では、管理インターフェイスの静的 IPv6 アドレスを設定します。

```
> configure network ipv6 manual 2001:DB8:3ffe:1900:4545:3:200:f8ff:fe21:67cf 64
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure network ipv6 delete** | IPv6 ネットワーキングを無効にします。 |
| **configure network ipv6 dhcp** | DHCP 経由で IPv6 を設定します。 |
| **configure network ipv6 router** | ルータ経由で IPv6 を設定します。 |
| **show network** | 管理インターフェイスの設定を表示します。 |

# configure network ipv6 router

ステートレス自動設定を使用してルータからIPv6アドレスを取得するように管理インターフェイスを設定するには、**configure network ipv6 router** コマンドを使用します。

**configure network ipv6 router** ［*management_interface*］

## 構文の説明

| | |
|---|---|
| *management_ interface* | 管理インターフェイスを指定します。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、Firepower 4100 および 9300 シリーズ デバイスでのみサポートされます。他のプラットフォームではこのパラメータを指定しないでください。Firepower 4100 および 9300 の管理インターフェイス ID は、デフォルトの管理インターフェイスの場合は **management0**、任意のイベントインターフェイスの場合は **management1** です。 |

## 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

このコマンドを使用して、デバイスの管理インターフェイスがルータから IPv6 の設定を受信するように指定します。管理インターフェイスは IPv6 ルータと通信して、設定情報を取得します。

### 例

次に、ステートレス自動設定を使用してルータからIPv6アドレスを受信するように管理インターフェイスを設定する例を示します。

```
> configure network ipv6 router
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure network ipv6 delete** | IPv6 ネットワーキングを無効にします。 |
| **configure network ipv6 dhcp** | DHCP 経由で IPv6 を設定します。 |
| **configure network ipv6 manual** | IPv6 を手動で設定します。 |

| Command | 説明 |
| --- | --- |
| **show network** | 管理インターフェイスの設定を表示します。 |

# configure network management-data-interface

管理インターフェイスの代わりにデータインターフェイスを Management Center の管理用に設定するには、**configure network management-data-interface** コマンドを使用します。

**configure network managament-data-interface** [ { **ipv4** { **dhcp** | [ **manual** *ip_address netmask* ] [ **default-gw** *gateway_ip* ] } | **ipv6** { **manual** *ip_address prefix* ] [ **default-gw** *gateway_ip* ] } | **ddns update-url https://** *username* **:** *password* **@** *provider-domain* **/** *path* **?hostname=<h>&myip=<a>** | **nameif** *name* | **client** *ip_address mask-or-prefix* | } **interface** *id* | **disable** ]

## 構文の説明

| | |
|---|---|
| **ipv4** | IP アドレスに IPv4 を指定します。 |
| **ipv6** | IP アドレスに IPv6 を指定します。 |
| **dhcp** | IPv4 アドレスの DHCP を指定します。 |
| **manual** *ip_address netmask-or-prefix* | 手動 IP アドレスとネットマスクまたはプレフィックスを指定します。 |
| **default-gw** *gateway_ip* | デフォルトゲートウェイのアドレスを指定します。CLI でセカンダリインターフェイスを編集する場合、ゲートウェイを設定したり、デフォルトルートを変更したりすることはできません。このインターフェイスのスタティックルートは Management Center でしか編集できません。 |
| **ddns update-url** [illegible] | DDNS Web タイプ更新 URL を指定します。DDNS プロバイダーから提供されたユーザー名とパスワードを指定します。正しいパスについては、DDNS プロバイダーに確認してください。<br><br>疑問符（?）文字を入力する前に、キーボードの Ctrl キーと v キーを一緒に押します。これにより、? がソフトウェアでヘルプ照会と解釈されなくなり、? を入力できます。<br><br>これらのキーワードは引数のように見えますが、URL の最後にこのテキストをそのまま入力する必要があります。脅威に対する防御は、DDNS 更新を送信するときに、<h> と <a> フィールドを自動的にホスト名と IP アドレスに置き換えます。 |
| **nameif** *name* | インターフェイス名を設定します。 |
| **client** *ip_address* | 特定のネットワーク上の Management Center へのデータ インターフェイス アクセスを制限します。引数を指定せずに **configure network managament-data-interface** コマンドを入力した場合、このキーワードはウィザードの一部ではないことに注意してください。 |

| | |
|---|---|
| **interface** *id* | Management Center 管理アクセスに使用するデータインターフェイス ID を指定します。Management Center アクセスには、データインターフェイス 1 つのみを指定できます。 |
| **disable** | データインターフェイスで Management Center 管理アクセスを無効にします。 |

## 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。 |
| 7.3 | Management Center にセカンダリ管理インターフェイスを追加した後は、このコマンドを使用して CLI でその設定の一部を編集できます。 |

## 使用上のガイドライン

最初にこのコマンドを設定するときに引数を指定しない場合は、データインターフェイスの基本的なネットワーク設定を行うためのウィザードが表示されます。

（注） このコマンドを使用する場合は、コンソールポートを使用する必要があります。管理インターフェイスに SSH を使用すると、接続が切断され、コンソールポートに再接続する必要が生じる場合があります。SSH の詳細な使用方法については、次を参照してください。

Management Center でセカンダリ管理インターフェイスを設定する場合、このコマンドを使用して編集できます。CLI でセカンダリインターフェイスを手動で追加することはできません。Management Center を使用する必要があります。

このコマンドの使用については、次の詳細を参照してください。

- データインターフェイスを管理に使用する場合、元の管理インターフェイスは DHCP を使用できません。初期セットアップ時に IP アドレスを手動で設定しなかった場合は、**configure network** {**ipv4** | **ipv6**} **manual** コマンドを使用して設定できるようになりました。管理インターフェイス ゲートウェイを **data-interfaces** に設定しなかった場合は、ここでこのコマンドで設定します。
- データインターフェイスからの Management Center アクセスには、次の制限があります。
  - マネージャアクセスを有効にできるのは、1 つの物理的なデータインターフェイスのみです。サブインターフェイスと EtherChannel は使用できません。冗長性を目的として、Management Center の単一のセカンダリインターフェイスでマネージャアクセスを有効にすることもできます。
  - このインターフェイスは管理専用にできません。
  - ルーテッドインターフェイスを使用するルーテッドファイアウォールモードのみです。
  - PPPoE はサポートされていません。ISP で PPPoE が必要な場合は、PPPoE をサポートするルータを Threat Defense と WAN モデムの間に配置する必要があります。

- インターフェイスを配置する必要があるのはグローバル VRF のみです。
- SSH はデータインターフェイスではデフォルトで有効になっていないため、後で Management Center を使用して SSH を有効にする必要があります。また、管理インターフェイス ゲートウェイがデータインターフェイスに変更されるため、**configure network static-routes** コマンドを使用して管理インターフェイス用の静的ルートを追加しない限り、リモートネットワークから管理インターフェイスに SSH 接続することはできません。Amazon Web Services の Threat Defense Virtual の場合、コンソールポートは使用できないため、管理インターフェイスへの SSH アクセスを維持する必要があります。設定を続行する前に、管理用の静的ルートを追加します。または、マネージャアクセス用のデータインターフェイスを設定する前に、すべての CLI 構成（**configure manager add** コマンドを含む）を終了してから接続を切断します。
- 管理インターフェイスとイベント専用インターフェイスを別々に使用することはできません。
- ハイアベイラビリティはサポートされません。この場合、管理インターフェイスを使用する必要があります。
- クラスタリングはサポートされません。この場合、管理インターフェイスを使用する必要があります。

- 脅威に対する防御 を Management Center に追加すると、Management Center はインターフェイス設定（インターフェイス名と IP アドレス、ゲートウェイへの静的ルート、DNS サーバー、DDNS サーバーなど）を検出して維持します。DNS サーバー設定の詳細については、次を参照してください。Management Center では、後で Management Center アクセスインターフェイス設定を変更できますが、脅威に対する防御 または Management Center が管理接続による再確立を妨げるような変更を加えないようにしてください。管理接続が中断された場合、脅威に対する防御 には以前の展開を復元する **configure policy rollback** コマンドが含まれます。
- DDNS サーバー更新の URL を設定すると、脅威に対する防御 は Cisco Trusted Root CA バンドルからすべての主要 CA の証明書を自動的に追加するため、脅威に対する防御 は HTTPS 接続の DDNS サーバー証明書を検証できます。脅威に対する防御 は、DynDNS リモート API 仕様（https://help.dyn.com/remote-access-api/）を使用するすべての DDNS サーバーをサポートします。
- このコマンドは、「データ」インターフェイス DNS サーバーを設定します。セットアップスクリプトで（または **configure network dns servers** コマンドを使用して）設定した管理 DNS サーバーは、管理トラフィックに使用されます。データ DNS サーバーは、DDNS（設定されている場合）またはこのインターフェイスに適用されるセキュリティポリシーに使用されます。

  Management Center では、この 脅威に対する防御 に割り当てるプラットフォーム設定ポリシーでデータインターフェイス DNS サーバーが設定されます。Management Center に 脅威に対する防御 を追加すると、ローカル設定が維持され、DNS サーバーはプラットフォーム設定ポリシーに追加されません。ただし、DNS 設定を含む 脅威に対する防御 に後でプ

ラットフォーム設定ポリシーを割り当てると、その設定によってローカル設定が上書きされます。Management Center と 脅威に対する防御 を同期させるには、この設定に一致するように DNS プラットフォーム設定をアクティブに設定することをお勧めします。

また、ローカル DNS サーバーは、DNS サーバーが初期登録で検出された場合にのみ Management Center で保持されます。たとえば、管理インターフェイスを使用してデバイスを登録し、後で **configure network management-data-interface** コマンドを使用してデータインターフェイスを設定した場合、脅威に対する防御設定と一致するように、DNS サーバーを含むすべての設定を Management Center で手動で設定する必要があります。

- 管理インターフェイスは、脅威に対する防御 を Management Center に登録した後に、管理インターフェイスまたは別のデータインターフェイスのいずれかに変更できます。
- セットアップウィザードで設定した FQDN がこのインターフェイスに使用されます。
- コマンドの一部としてデバイス設定全体をクリアできます。このオプションはリカバリシナリオで使用できますが、初期セットアップや通常の操作には使用しないでください。
- データ管理を無効にするには、**configure network management-data-interface disable** コマンドを入力します。

### 例

次に、DHCP を使用して Ethernet1/1 を Management Center 管理インターフェイスとして設定する例を示します。

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to
change the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

次に、手動 IP アドレスを使用して Ethernet1/1 を Management Center 管理インターフェイスとして設定する例を示します。

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
```

```
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to
change the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure network ipv4 manual** | 手動 IPv4 IP アドレスを使用して管理インターフェイスを設定します。 |
| **configure network ipv6 manual** | 手動 IPv6 IP アドレスを使用して管理インターフェイスを設定します。 |
| **configure policy rollback** | 管理接続が中断された場合に、以前の展開を復元します。 |
| **show network** | 管理インターフェイスの設定を表示します。 |

# configure network management-interface

Firepower 4100 または 9300 シリーズ デバイスでイベントと管理トラフィックを分離するために複数の管理インターフェイスを設定するには、**configure network management-interface** コマンドを使用します。脅威に対する防御 では、Firepower 4100 シリーズと 9300 シリーズのデバイスでのみ複数の管理インターフェイスが使用できます。このコマンドを使用して、Management Center 通信に使用する MTU ポートと TCP ポートを設定することもできます。

**configure network management-interface** { [ **disable** | **disable-event-channel** | **disable-management-channel** | **enable** | **enable-event-channel** | **enable-management-channel** ] *interface_id* ] | **tcpport** *number* | **mtu-event-channel** [ *bytes* ] | **mtu-management-channel** [ *bytes* ] }

## 構文の説明

| | |
|---|---|
| **disable** | 指定した管理インターフェイスを無効にします。 |
| **disable-event-channel** | 指定したインターフェイスのイベント トラフィック チャネルを無効にします。 |
| **disable-management-channel** | 指定したインターフェイスの管理チャネルを無効にします。 |
| **enable** | 指定した管理インターフェイスを有効にします。 |
| **enable-event-channel** | 指定したインターフェイスのイベント トラフィック チャネルを有効にします。 |
| **enable-management-channel** | 指定したインターフェイスの管理チャネルを有効にします。 |
| *interface_id* | 有効または無効にする管理インターフェイスを指定します（**management0** または **management1**）。management0 および management1 は、物理インターフェイス ID に関係のない、これらのインターフェイスの内部名です。 |
| **tcpport** *number* | Management Center との通信に使用する TCP ポートを設定します。デフォルトは 8305 です。デフォルトを変更する場合は、SSH（22）または HTTPS（443）ポートを指定しないでください。数値を 1024 以上（65535 まで）の高い範囲に維持します。このコマンドは、**configure network management-port** コマンドと同等です。 |
| **mtu-event-channel** [*bytes*] | イベントインターフェイスの MTU を、IPv4 を有効にした場合は 64 ー 9000、IPv6 を有効にした場合は 1280 ー 9000 の間で設定します（バイト単位）。IPv4 と IPv6 の両方を有効にした場合、最小値は 1280 です。*bytes* を入力しない場合、値の入力を求められます。このコマンドは、**configure network mtu** コマンドと同等です。 |

| | |
|---|---|
| **mtu-management-channel** [*bytes*] | 管理インターフェイスの MTU を、IPv4 を有効にした場合は 64 ー 1500、IPv6 を有効にした場合は 1280 ー 1500 の間で設定します（バイト単位）。IPv4 と IPv6 の両方を有効にした場合、最小値は 1280 です。*bytes* を入力しない場合、値の入力を求められます。このコマンドは、**configure network mtu** コマンドと同等です。<br>（注） MTU を非常に低い値に設定すると、Device Manager のパフォーマンスに影響を及ぼす可能性があります。 |

## コマンド デフォルト

management0 インターフェイスが有効になり、イベントトラフィックと管理トラフィックの両方に使用されます。 management1 は無効です。

デフォルトの TCP ポートは 8305 です。

デフォルトの MTU は管理インターフェイスでもイベントインターフェイスでも 1500 です。

## 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。 |
| 6.6 | **mtu-event-channel** キーワードと **mtu-management-channel** キーワードが追加されました。 |

## 使用上のガイドライン

デバイスを管理する場合、Management Center 管理インターフェイスには 2 つの別個のトラフィック チャネルがあります。管理トラフィック チャネルはすべての内部トラフィック（デバイスの管理に固有のデバイス間トラフィックなど）を伝送し、イベント トラフィック チャネルはすべてイベント トラフィック（Web イベントなど）を伝送します。必要に応じて、Management Center で個別のイベント専用インターフェイスを設定し、イベントトラフィックを処理することもできます（Management Center Web インターフェースで、この設定が実行されていることを確認してください）。イベント専用インターフェイスは 1 つだけ設定できます。イベントトラフィックは大量の帯域幅を使用する可能性があるので、管理トラフィックからイベント トラフィックを分離することで、Management Center のパフォーマンスを向上させることができます。

Firepower 4100 シリーズと 9300 シリーズのデバイスでは、論理デバイスに割り当てる mgmt タイプのインターフェイスは、脅威に対する防御 アプリケーションでデフォルトの management0 インターフェイスとして指定されます。このインターフェイスには、デフォルトで管理チャンネルとイベントチャンネルの両方が含まれています。Management Center で別のイベントインターフェイスを設定した場合は、Firepower 4100 または 9300 デバイスで、脅威に対する防御論理デバイスに eventing-type インターフェイスを割り当てることで分離を活用することができます。このインターフェイスは、management1 インターフェイスとして指定されます。可能であれば、デバイス イベント インターフェイスと Management Center イベント インターフェイスの間で、イベント トラフィックが送信されます。イベント ネットワークがダウンすると、イベント トラフィックは、デフォルトの管理インターフェイスに戻ります。可能な場合には別

個のイベントインターフェイスが使用されますが、管理インターフェイスが常にバックアップとなります。

Management Center イベント専用インターフェイスは管理チャネルのトラフィックを受け入れることができないので、デバイス イベント インターフェイスで管理チャネルを単に無効にしてください。必要に応じて、管理インターフェイスのイベントを無効にすることができます。いずれの場合も、デバイスは、イベントのみのインターフェイス上でイベントを送信しようとします。そのインターフェイスがダウンしていた場合は、イベントチャネルが無効になっていても、管理インターフェイス上でイベントを送信します。

イベントインターフェイスを論理デバイスに割り当てても、このインターフェイスは有効になっておらず、ネットワーク設定も設定されていません。脅威に対する防御 CLI にアクセスし、**configure network management-interface** コマンドを使用して有効にする必要があります。次に、**configure network** {**ipv4** | **ipv6**} **manual** コマンドを使用して管理インターフェイスのアドレスを設定します。

### 例

次の例では、management1 を有効にし、管理チャネルを無効にします。デフォルトでは、両方のチャネルが有効になっています。

```
> configure network management-interface enable management1
> configure network management-interface disable-management-channel management1
>
```

次の例では、Management Center との通信に使用するポートを変更します。

```
> configure network management-interface tcpport 8306
Management port changed to 8306.
```

次の例では、イベントインターフェイスの MTU を 9000 に設定します。

```
> configure network management-interface mtu-event-channel 9000
MTU set successfully to 9000 from 1500 for management1
Refreshing Network Config...
Interface management1 speed is set to '10000baseT/Full'
>
```

次の例では、CLI プロンプトを使用して、管理インターフェイスの MTU を 1400 に設定します。

```
> configure network management-interface mtu-management-channel
Do you want to change the MTU [1500] for management0 interface?(Yes/No): Yes
Enter the new value for MTU [1500]> 1400
MTU set successfully to 1400 from 1500 for management0
Refreshing Network Config...
Interface management0 speed is set to '10000baseT/Full'
>
```

関連コマンド

| Command | 説明 |
| --- | --- |
| **configure network mtu** | 管理インターフェイスまたはイベントインターフェイスの MTU を設定します。 |
| **configure network static-routes ipv4/ipv6** | 管理インターフェイスのスタティックルートを設定します。 |
| **show network** | 管理インターフェイスの設定を表示します。 |

# configure network management-port

Management Center との通信に使用する TCP ポートを設定するには、**configure network management-port** コマンドを使用します。

**configure network management-port** *number*

## 構文の説明

| | |
|---|---|
| *number* | Management Center との通信に使用する TCP ポートを設定します。デフォルトは 8305 です。デフォルトを変更する場合は、SSH（22）または HTTPS（443）ポートを指定しないでください。数値を 1024 以上（65535 まで）の高い範囲に維持します。 |

## 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

Management Center への管理接続に使用するポートを変更するには、このコマンドを使用します。このコマンドを使用しても、ローカルマネージャである Device Manager で使用されるポートが変更されることはありません。このコマンドは、**configure network management-interface tcpport** コマンドと同等です。両方のコマンドを使用する必要はありません。

### 例

次の例では、Management Center との通信に使用するポートを変更します。

```
> configure network management-port 8306
Management port changed to 8306.
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure network ipv4** | 管理インターフェイスの IPv4 アドレスを設定します。 |
| **configure network ipv6** | 管理インターフェイスの IPv6 アドレスを設定します。 |
| **show network** | 管理インターフェイスの設定を表示します。 |

# configure network mtu

管理インターフェイスまたはイベントインターフェイスの MTU を設定するには、**configure network mtu** コマンドを使用します。

**configure network mtu** ［ *interface_id* ］［ *bytes* ］

## 構文の説明

| | |
|---|---|
| *bytes* | （任意）MTU をバイト単位で設定します。管理インターフェイスでは、IPv4 を有効にした場合は 64ー1500、IPv6 を有効にした場合は 1280ー1500 の値を指定できます。<br>イベントインターフェイスでは、IPv4 を有効にした場合は 64ー9000、IPv6 を有効にした場合は 1280ー9000 です。<br>IPv4 と IPv6 の両方を有効にした場合、最小値は 1280 です。*bytes* を入力しない場合、値の入力を求められます。<br>（注） MTU を非常に低い値に設定すると、Device Manager のパフォーマンスに影響を及ぼす可能性があります。 |
| *interface_id* | （任意）MTU を設定するインターフェイス ID を指定します。プラットフォームに応じて使用可能なインターフェイス ID（management0、management1、br1、eth0など）を表示するには、**show network** コマンドを使用します。インターフェイスを指定しない場合は、管理インターフェイスが使用されます。 |

## コマンド デフォルト

デフォルトの MTU は管理インターフェイスでもイベントインターフェイスでも 1500 です。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.6 | 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、**configure network management-interface mtu-event-channel** および **configure network management-interface mtu-management-channel** コマンドと同等です。両方のコマンドを使用する必要はありません。

### 例

次の例では、イベントインターフェイス management1 の MTU を 8192 に設定します。

```
> configure network mtu 8192 management1
MTU set successfully to 8192 from 1500 for management1
Refreshing Network Config...
NetworkSettings::refreshNetworkConfig MTU value at start 8192

Interface management1 speed is set to '10000baseT/Full'
NetworkSettings::refreshNetworkConfig MTU value at end 8192
```

```
>
```

次の例では、CLI プロンプトを使用して、管理インターフェイスの MTU を 1400 に設定します。

```
> configure network mtu
Do you want to change the MTU [1500] for management0 interface?(Yes/No): Yes
Enter the new value for MTU [1500]> 1400
MTU set successfully to 1400 from 1500 for management0
Refreshing Network Config...
Interface management0 speed is set to '10000baseT/Full'
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure network ipv4** | 管理インターフェイスの IPv4 アドレスを設定します。 |
| **configure network ipv6** | 管理インターフェイスの IPv6 アドレスを設定します。 |
| **configure network management-interface** | 管理インターフェイスまたはイベントインターフェイスの MTU を設定します。 |
| **show network** | 管理インターフェイスの設定を表示します。 |

# configure network speed

管理インターフェイスまたはデータインターフェイスの速度を設定するには、**configure network speed** コマンドを使用します。

（注） このコマンドは、Cisco Secure Firewall 3100 でのみサポートされています。

**configure network speed** { *speed* | **sfp-detect** [ *interface_id* ]

## 構文の説明

| | |
|---|---|
| *interface_id* | （任意）速度を設定するインターフェイス ID を指定します。デフォルトは management0 です。 |
| **sfp-detect** | インストールされている SFP モジュールの速度を検出し、適切な速度を使用します。この設定は、デフォルトです。デュプレックスは常に全二重で、自動ネゴシエーションは常に有効です。このオプションは、後でネットワークモジュールを別のモデルに変更し、速度を自動的に更新する場合に便利です。 |
| *speed* | 特定の速度に速度を設定します。使用できる速度は、インターフェイスによって異なります。 |

## コマンド デフォルト

デフォルトの速度は **sfp-detect** です。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1 | このコマンドは、Cisco Secure Firewall 3100 に導入されました。 |

## 使用上のガイドライン

SFP 機能に関係なく、速度を特定の速度に設定する場合を除き、デフォルトの **sfp-detect** を使用することをお勧めします。

### 例

次に、管理インターフェイスである management0 の速度を 1gbps に設定する例を示します。

```
> configure network speed 1gbps
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure network ipv4** | 管理インターフェイスの IPv4 アドレスを設定します。 |

| Command | 説明 |
|---|---|
| **configure network ipv6** | 管理インターフェイスの IPv6 アドレスを設定します。 |
| **configure network management-interface** | 管理インターフェイスまたはイベントインターフェイスの MTU を設定します。 |
| **show network** | 管理インターフェイスの設定を表示します。 |

# configure network static-routes

スタティックルートを追加または削除するには、**configure network static-routes** コマンドを使用します。

**configure network static-routes** {**ipv4** | **ipv6**} {**add** *interface destination netmask_or_prefix gateway* | **delete**}

## 構文の説明

| | |
|---|---|
| **add** | 管理インターフェイスのスタティックルートを追加します。 |
| **delete** | 管理インターフェイスのスタティックルートを削除します。削除するルートを選択するように求められます。 |
| *interface* | 管理インターフェイスの ID。モデルの管理インターフェイス ID を表示するには、**show network** コマンドを使用します。 |
| **ipv4** | IPv4 管理アドレスのスタティックルートを追加または削除します。 |
| **ipv6** | IPv6 管理アドレスのスタティックルートを追加または削除します。 |
| *destination* | 追加または削除する宛先 IP アドレス（必要に応じて IPv4 形式または IPv6 形式）。たとえば、10.100.10.10 または 2001:db8::201 のように表示されます。 |
| *netmask_or_prefix* | IPv4 のネットワークアドレスマスク、または IPv6 のプレフィックス。IPv4 ネットマスクは、ドット付き 10 進形式にする必要があります（255.255.255.0 など）。IPv6 プレフィックスは、96 などの標準プレフィックス番号です。 |
| *gateway* | 追加または削除するゲートウェイアドレス（必要に応じて IPv4 形式または IPv6 形式）。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.0.1 | このコマンドが導入されました。 |

## 使用上のガイドライン

**configure network management-interface** コマンドを使用してイベント専用インターフェイスを設定する際、そのインターフェイスが管理インターフェイスとは別のネットワーク上に存在する場合は、スタティックルートを設定する必要があります。スタティックルートは、through-the-box トラフィック（データインターフェイス上のトラフィック）には影響しません。スタティックルートがない場合、すべての管理トラフィックは、デフォルト管理インターフェイスのゲートウェイとして指定されたデフォルトルートを使用します。通常、単一の管理インターフェイスを使用する場合、またはイベント専用インターフェイスが同じネットワーク上にある場合、スタティックルートは必要ありません。

（注） デフォルトルートの場合は、このコマンドを使用しないでください。デフォルト管理インターフェイスに対して **configure network ipv4** コマンドまたは **ipv6** コマンドを使用する場合は、デフォルト ルート ゲートウェイの IP アドレスしか変更できません。

**例**

次の例では、**10.115.24.0** の宛先アドレス、**255.255.255.0** のネットワークアドレスマスク、および **10.115.9.2** のゲートウェイアドレスを使用して、管理インターフェイス **management1** の IPv4 スタティックルートを追加します。

```
> configure network static-routes ipv4 add management1 10.115.24.0 255.255.255.0 10.115.9.2
```

次の例では、**2001:db8::201** の宛先アドレス、**64** の IPv6 プレフィックス長、および **2001:db8::3657** のゲートウェイアドレスを使用して、管理インターフェイス **management1** の IPv6 スタティックルートを追加します。

```
> configure network static-routes ipv6 add management1 2001:db8::201 64 2001:db8::3657
```

次の例は、スタティックルートを削除する方法を示しています。

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                 : management1
Destination               : 10.1.1.0
Gateway                   : 192.168.0.254
Netmask                   : 255.255.255.0
> configure network static-routes ipv4 delete
Please select which IPv4 Static Route to delete:
1) management1:   dest 10.1.1.0          nmask 255.255.255.0     gw 192.168.0.254
Please enter number of route to delete: 1
Interface:    management1
Destination:  10.1.1.0
Netmask:      255.255.255.0
Gateway:      192.168.0.254
Are you sure that you want to delete this route?  (y/n) [n]: y
Configuration updated successfully
> show network-static-routes
No static routes currently configured.
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure network management-interface** | 複数の管理インターフェイスを設定します。 |
| **configure network static-routes ipv4** | 管理インターフェイスの IPv4 スタティックルートを追加または削除します。 |

| Command | 説明 |
| --- | --- |
| **show network-static-routes** | 管理インターフェイス用に設定されたスタティックルートを表示します。 |

# configure password

現在ログインしているユーザーアカウントのパスワードを変更するには、**configure password** コマンドを使用します。

**configure password**

## 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

このコマンドを使用すると、現在のユーザーはCLIでパスワードを変更できます。コマンドを発行すると、CLIは現在の（古い）パスワードを入力するようユーザーに要求し、その後で新しいパスワードを2回入力するよう要求します。

### 例

次の例では、現在のユーザーアカウントのパスワードを変更します。

```
> configure password
Enter current password: oldpassword
Enter new password: newpassword
Confirm new password: newpassword
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure user add** | CLI アクセス用のユーザーアカウントを追加します。 |

# configure policy rollback

脅威に対する防御 の設定 last-deployed に展開した設定にロールバックするには、**configure policy rollback** コマンドを使用します。

**configure policy rollback**

## 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。 |
| 7.2 | ロールバックは高可用性でサポートされています。 |

## 使用上のガイドライン

Management Center の管理に 脅威に対する防御 でデータインターフェイスを使用し（**configure network management-data-interface** を参照）、ネットワーク接続に影響する Management Center からの設定変更を展開する場合、脅威に対する防御 の設定を last-deployed 設定にロールバックするため、管理接続を復元できます。その後、ネットワーク接続が維持されるように Management Center で構成設定を調整し、再展開できます。ロールバック機能は、接続が失われていない場合でも使用でき、このトラブルシューティングの状況以外でも使用できます。

次のガイドラインを参照してください。

- 前回の展開のみ 脅威に対する防御 でローカルに使用できます。さらに以前の展開にロールバックすることはできません。
- ロールバックは Management Center 7.2 以降は高可用性でサポートされています。
- ロールバックは、クラスタリング展開ではサポートされていません。
- ロールバックは、Management Center で設定できる設定にのみ影響します。たとえば、ロールバックは、脅威に対する防御 CLI でのみ設定できる専用管理インターフェイスに関連するローカル構成には影響しません。**configure network management-data-interface** コマンドを使用した最後の Management Center 展開後にデータインターフェイス設定を変更し、rollback コマンドを使用すると、それらの設定は保持されないことに注意してください。最後に展開された Management Center 設定にロールバックされます。
- UCAPL/CC モードはロールバックできません。
- 以前の展開中に更新されたアウトオブバンド SCEP 証明書データはロールバックできません。
- ロールバック中に、現在の設定がクリアされるため、接続がドロップされます。

ロールバック後、脅威に対する防御 はロールバックが正常に完了したことを Management Center に通知します。Management Center では、設定がロールバックされたことを示すバナーが展開画面に表示されます。

ロールバックが失敗した場合、一般的な展開の問題についてhttps://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.htmlを参照して

ください。場合によっては、Management Center 管理アクセスの復元後にロールバックが失敗することがあります。この場合、Management Center 設定の問題を解決して、Management Center から再展開できます。

### 例

次に、最後に展開された設定をロールバックする例を示します。

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
.....................
.....................
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure network management-data-interface** | Management Center 管理用のデータインターフェイスを設定します。 |

# configure raid

RAID 内で SSD を管理するには、**configure raid** コマンドを使用します。

（注） このコマンドは、Cisco Secure Firewall 3100 でのみサポートされています。

**configure raid** ｛ **add** ｜ **remove** ｜ **remove-secure** ｝ **local-disk** ｛ **1** ｜ **2** ｝ ［ *psid* ］

## 構文の説明

| | |
|---|---|
| **add** | SSD を RAID に追加します。新しい SSD と RAID の同期が完了するまでに数時間かかることがありますが、その間、ファイアウォールは完全に動作します。再起動もでき、電源投入後に同期は続行されます。 |
| *psid* | 以前に別のシステムで使用されていて、まだロックされている SSD を追加する場合は、*psid* と入力します。*psid* は SSD の背面に貼られたラベルに印刷されています。または、システムを再起動し、SSD を再フォーマットして RAID に追加できます。 |
| **remove** | SSD を RAID から取り外し、データをそのまま保持します。 |
| **remove-secure** | SSD を RAID から取り外し、自己暗号化ディスク機能を無効にして、SSD を安全に消去します。 |
| **local-disk** ｛**1** ｜ **2**｝ | SSD（disk1 または disk2）を指定します。 |

## コマンド デフォルト

SSD が 2 つある場合、起動時に RAID が形成されます。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1 | このコマンドは、Cisco Secure Firewall 3100 に導入されました。 |

## 使用上のガイドライン

ファイアウォールの電源が入っている状態で Threat Defense CLI で次のタスクを実行できます。

- SSD の 1 つをホットスワップする：SSD に障害がある場合は、交換できます。SSD が 1 つしかない場合、ファイアウォールの電源がオンになっている間 SSD は取り外せません。
- SSD の 1 つを取り外す：SSD が 2 つある場合は、1 つを取り外すことができます。
- 2 つ目の SSD を追加する：SSD が 1 つの場合は、2 つ目の SSD を追加して RAID を形成できます。

⚠

**注意** この手順を使用して、SSD を RAID から削除する前に SSD を取り外さないでください。データが失われる可能性があります。

**例**

次に、RAID から disk2 が削除され、安全に消去される例を示します。

```
> configure raid remove-secure local-disk 2
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show raid** | RAID ステータスを表示します。 |
| **show ssd** | SSD ステータスを表示します。 |

# configure snort

Snort 検査エンジンの高度な動作を設定するには、**configure snort** コマンドを使用します。

**configure snort preserve-connection** {**enable** | **disable**}

## 構文の説明

| | |
|---|---|
| **preserve-connection** {**enable** \| **disable**} | Snort プロセスがダウンした場合に、ルーテッドインターフェイスとトランスペアレントインターフェイスで既存の TCP/UDP 接続を維持するかどうかを指定します。このオプションはデフォルトでは有効になっていますが、無効化できます。コマンドを有効にした場合、すでに許可されている接続は確立されたままですが、Snort が再び使用可能になるまで新しい接続を確立できません。無効化した場合、Snort がダウンすると、新規または既存のすべての接続がドロップされます。<br><br>ICMP ping などの非 TCP/UDP 接続は維持されません。<br><br>現在の設定を表示するには、**show running-config snort** コマンドを使用します。実行コンフィギュレーション全体を表示する場合、**snort preserve-connection** コマンドの **no** 形式を使用すると、この機能が無効であることが示されます。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.2.0.2、6.2.3 | このコマンドが導入されました。ただし、**preserve-connection disable** は Device Manager（ローカル管理）ではサポートされていないため、設定を展開するたびに接続の維持が再度有効になります。<br><br>このコマンドは、脅威に対する防御 または Management Center でバージョン 6.2.1、6.2.2、6.2.2.x、または 6.2.0.2 以前のバージョンが実行されている場合には使用できません。この場合、コマンドが無効になっているかのようにデバイスが動作するため、Snort がダウンするとすべての新規および既存の接続がドロップされます。 |

## 使用上のガイドライン

**preserve-connection** を有効にすると、Snort がダウンしても、既存の接続は確立されたままになります。Snort が使用可能になると、これらの確立された接続は Snort 検査をバイパスし続けます。Snort 検査が必要な新しい接続は、Snort が再び使用可能になるまでドロップされます。

### 例

次の例では、**preserve-connection** を無効化します。

```
> configure snort preserve-connection disable
```

関連コマンド

| コマンド | 説明 |
|---|---|
| **show conn** | 接続を表示します。 |
| **show conn detail** | 接続の詳細に Snort 検査情報を含めます。 |
| **show conn detail long** | 長い形式の接続の詳細に Snort 検査情報を含めます。 |

# configure ssh-access-list

指定した IP アドレスからの SSH 接続を受け入れるようにデバイスを設定するには、**configure ssh-access-list** コマンドを使用します。

**configure ssh-access-list** *address_list*

## 構文の説明

| | |
|---|---|
| *address_list* | ホストまたはネットワークの IP アドレスのカンマ区切りリスト（IPv4 Classless Inter-Domain Routing（CIDR）表記または IPv6 プレフィックス長表記）。たとえば、10.100.10.0/24 または 2001:DB8::/96 のように表記します。<br>すべての IPv4 ホストを指定するには、「0.0.0.0/0」と入力します。すべての IPv6 ホストを指定するには、「::/0」のように指定します。 |

## 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

サポートされているすべてのホストまたはネットワークを 1 つのコマンドに含める必要があります。このコマンドで指定したアドレスで、SSH アクセスリストの現在の内容が上書きされます。

SSH アクセスを許可するだけでは、ユーザーはローカルマネージャにログインできません。設定ソフトウェアへのアクセスは、ユーザー名とパスワードによって制御されます。

現在 CLI にログインしている IP アドレスを除外すると、接続が切断されます。CLI に再度アクセスするには、IP アドレスを変更する必要があります。

デバイスがローカル管理の高可用性グループ内のユニットである場合、アクティブユニットが次に設定の更新を展開するときに変更が上書きされます。これがアクティブユニットの場合、展開中に変更がピアに伝播されます。

### 例

次の例では、任意の IPv4 または IPv6 アドレスからの SSH 接続を受け入れるようにデバイスを設定します。

```
> configure ssh-access-list 0.0.0.0/0,::/0
The ssh access list was changed successfully.
> show ssh-access-list
ACCEPT     tcp  --  anywhere            anywhere            state NEW tcp dpt:ssh
ACCEPT     tcp      anywhere            anywhere            state NEW tcp dpt:ssh
```

関連コマンド

| Command | 説明 |
| --- | --- |
| **configure disable-ssh-access** | SSH アクセスリストをクリアします。 |
| **show ssh-access-list** | SSH アクセスリストを表示します。 |

# configure ssl-protocol

クライアントがデバイスへの HTTPS 接続で使用できる SSL プロトコルを設定するには、ローカルマネージャを使用するときに **configure ssl-protocol** コマンドを使用します。

**configure ssl-protocol** {*protocol_list* | **default**}

## 構文の説明

| | |
|---|---|
| **default** | デフォルトの SSL プロトコルリストを有効にします。**TLSv1.1**、**TLSv1.2**。 |
| *protocol_list* | 次のいずれかのプロトコルを指定するカンマ区切りリスト。**TLSv1**、**TLSv1.1**、**TLSv1.2**、**SSLv3**。 |

## コマンド デフォルト

デフォルト設定は **TLSv1.1**、**TLSv1.2** です。

## 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

このコマンドは、クライアントがデバイスへの HTTPS Web アクセスに使用できるプロトコルを設定します。これは、ローカルマネージャである Device Manager で使用されます。リモートマネージャでは使用できません。

（注） このコマンドを使用して、デバイスとの通信に現在使用しているプロトコルを無効にすると、接続が失われます。

### 例

次の例では、HTTPS 接続のすべての SSL プロトコルを受け入れるようにデバイスを設定します。

```
> show ssl-protocol
The supported ssl protocols are TLSv1.1 TLSv1.2
> configure ssl-protocol TLSv1,TLSv1.1,TLSv1.2,SSLv3
The following ssl protocols are now enabled:  TLSv1 TLSv1.1 TLSv1.2 SSLv3
> show ssl-protocol
The supported ssl protocols are  TLSv1 TLSv1.1 TLSv1.2 SSLv3
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ssl-protocol** | 現在設定されている SSL プロトコルを表示します。 |

# configure tcp-randomization

TCP シーケンス番号のランダム化を無効にするには、**configure tcp-randomization** コマンドを使用します。

**configure tcp-randomization** {**enable** | **disable**}

## 構文の説明

| | |
|---|---|
| **enable** | 着信パケットと発信パケットの TCP シーケンス番号をランダムに変更して、攻撃者が次のパケットのシーケンス番号を予測できないようにします。 |
| **disable** | 着信パケットと発信パケットの TCP シーケンス番号を変更しないでください。 |

## コマンド デフォルト

シーケンス番号のランダム化は、デフォルトで有効になっています。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.2 | このコマンドが導入されました。 |

## 使用上のガイドライン

個々の TCP 接続には 2 つの初期シーケンス番号（ISN）があり、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバーで生成されます。脅威に対する防御デバイスは、着信と発信の両方向で通過する TCP SYN の ISN をランダム化します。

保護対象のホストの ISN をランダム化することにより、攻撃者が新しい接続に使用される次の ISN を予測して新しいセッションをハイジャックするのを阻止します。

たとえば、データがスクランブルされるため、必要に応じて TCP 初期シーケンス番号ランダム化をディセーブルにすることができます。たとえば、連続番号が付いた TCP パケットに依存するソフトウェアテストツール、ソフトウェア製品、またはハードウェアデバイスを使用しているとします。TCP ランダム化設定を変更すると、デバイス上のすべてのインターフェイスとすべてのトラフィックに影響します。特定のインターフェイスまたはトラフィッククラスを指定して変更することはできません。

TCP シーケンス番号のランダム化は、ランダム化による特定の問題が発生した場合にのみ無効にする必要があります。

（注） Device Manager を使用している場合は、TCP シーケンス番号のランダム化を無効にできますが、Device Manager から設定を展開するたびに、この機能は再度有効になります。TCP シーケンス番号のランダム化を無効のままにしておく場合は、展開が完了するたびにコマンドを再入力する必要があります。

### 例

次の例では、TCP シーケンス番号のランダム化が無効になります。

```
> configure tcp-randomization disable
```

TCP シーケンス番号のランダム化が現在有効かそれとも無効かを確認するには、**set connection random-sequence-number disable** コマンドの実行コンフィギュレーションを調べます。このコマンドは global_policy ポリシーマップに含まれるため、**show running-config policy-map** コマンドを使用して設定の表示を制限できます。**set connection random-sequence-number** コマンドが設定に表示されない場合は、TCP シーケンス番号のランダム化が有効になっています。

たとえば、次の例では TCP シーケンス番号のランダム化が無効になっています（関連するコマンドが強調表示されています）。

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
 class tcp
  set connection random-sequence-number disable
!
```

次の例では、**set connection random-sequence-number** コマンドが global_policy ポリシーマップに含まれていないため、TCP シーケンス番号のランダム化が有効になっていることがわかります。

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
```

```
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
```

# configure unlock_time

失敗したログインの最大数を超えたためにユーザーアカウントがロックされた後、自動的にロック解除されるまでの時間を設定するには、**configure unlock_time** コマンドを使用します。このコマンドは、CC/UCAPL コンプライアンスモードのみで動作します。

**configure unlock_time** *number*

## 構文の説明

| | |
|---|---|
| *number* | ロック解除時間を分単位で指定します。値の範囲は 1 ー 9999 です。 |

## コマンド デフォルト

CC/UCAPL モードで実行している場合、デフォルトのロック解除時間は 30 分です。

CC/UCAPL モードで実行していない場合、ユーザーアカウントは、**configure user unlock** コマンドを使用してロック解除するまでロックされたままになります。自動ロック解除時間は設定できません。

## 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

CC/UCAPL コンプライアンスモードで実行している場合は、ロックアウトされたユーザーのグローバルロック解除時間を設定できます。設定された時間が経過すると、ユーザーアカウントの最大ログイン試行失敗回数を超えた特定のユーザーのアカウントはロック解除され、ユーザーは再試行できるようになります。ログイン試行の失敗が許可される最大回数を設定するには、**configure user maxfailedlogins** コマンドを使用します。

ロック解除時間を設定した場合でも、**configure user unlock** コマンドを使用してユーザーアカウントをいつでもロック解除できます。ユーザーは、ロック解除時間が経過するまで待つ必要はありません。

### 例

次の例では、ロック解除時間を 60 分に設定します。

```
> configure unlock_time 60
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure user add** | 新しいユーザーを追加します。 |
| **configure user maxfailedlogins** | ユーザーがログインで失敗できる最大回数を設定します。 |
| **configure user unlock** | 指定したユーザーのアカウントのロックを解除します。 |

| Command | 説明 |
| --- | --- |
| **show user** | ユーザーアカウントを表示します。 |

# configure user access

既存ユーザーのアクセス認証レベルを変更するには、**configure user access** コマンドを使用します。

**configure user access** ユーザー名 {**basic** | **config**}

## 構文の説明

| | |
|---|---|
| *username* | 既存ユーザーの名前を指定します。 |
| **basic** | ユーザーに基本的なアクセス権を付与します。ユーザーはコンフィギュレーション コマンドを入力することはできません。 |
| **config** | ユーザーにコンフィギュレーション アクセス権を付与します。すべてのコマンドの管理者権限がユーザーに与えられます。 |

## 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

ユーザーアカウントを作成するときに、ユーザーのアクセス権を指定します。**configure user access** コマンドを使用して、指定したユーザーのアクセスレベルを変更します。このコマンドは、該当ユーザーが次にログインするときに有効になります。

### 例

次の例では、ユーザー jdoe のアクセス権を Basic に変更します。

```
> configure user access jdoe basic
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure user add** | 新しいユーザーを追加します。 |
| **show user** | ユーザーアカウントとアクセス権を表示します。 |

# configure user add

CLI アクセス用の新しいユーザーアカウントを作成するには、**configure user add** コマンドを使用します。

**configure user add** ユーザー名 {**basic** | **config**}

## 構文の説明

| | |
|---|---|
| *username* | 既存ユーザーの名前を指定します。 |
| **basic** | ユーザーに基本的なアクセス権を付与します。ユーザーはコンフィギュレーション コマンドを入力することはできません。 |
| **config** | ユーザーにコンフィギュレーション アクセス権を付与します。すべてのコマンドの管理者権限がユーザーに与えられます。 |

## 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

指定した名前、アクセスレベル、およびパスワードで新しいユーザーを作成するには、このコマンドを使用します。このコマンドは、パスワードを要求するコマンドプロンプトを表示します。他のすべてのアカウントプロパティは、デフォルトのプロパティで設定されます。

### 例

次の例では、config アクセス権を使用して、joecool という名前のユーザ アカウントを追加します。パスワードは入力時に非表示となります。

```
> configure user add joecool config
Enter new password for user joecool: newpassword
Confirm new password for user joecool: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
joecool           1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure user access** | ユーザーアクセスレベルを設定します。 |
| **configure user aging** | ユーザーパスワードのエージングを設定します。 |
| **configure user delete** | 指定したユーザーを削除します。 |
| **configure user disable** | 指定したユーザーを無効にします。 |

| Command | 説明 |
|---|---|
| **configure user enable** | 指定したユーザーを有効にします。 |
| **configure user forcereset** | 指定したユーザーのパスワードを強制的にリセットします。 |
| **configure user maxfailedlogins** | 指定したユーザーのログイン失敗の最大回数を設定します。 |
| **configure user password** | 指定したユーザーのパスワードを設定します。 |
| **configure user strengthcheck** | 指定したユーザーのパスワードの強度チェック要件を設定します。 |
| **configure user unlock** | 指定したユーザーのアカウントのロックを解除します。 |
| **show user** | ユーザーアカウントを表示します。 |

# configure user aging

ユーザーのパスワードの有効期限を設定するには、**configure user aging** コマンドを使用します。

**configure user aging** *username max_days warn_days* ［ *grace_period* ］

## 構文の説明

| | |
|---|---|
| *username* | ユーザーの名前を指定します。管理者ユーザーのエージング設定は変更できません。 |
| *max_days* | パスワードの最大有効日数を指定します。有効範囲は1 ～ 9999 です。 |
| *warn_days* | パスワードの有効期限が切れる前に、ユーザーによるパスワード変更が猶予される日数を指定します。有効範囲は 1 ー 9999 ですが、最大日数未満にする必要があります。 |
| *grace_period* | （任意、FXOS プラットフォームのみ。）パスワードの有効期限が切れた後、ユーザーが引き続きパスワードを変更できる日数を指定します。FXOS 以外のプラットフォームでは、パラメータは受け入れられますが、**show user** 出力には猶予期間が無効であることが示されます。 |

## 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。 |
| 7.0 | *grace_period* パラメータが追加されました。 |

### 例

次に、ユーザーのパスワードを 100日後に期限切れになるように設定し、パスワードの有効期限の 30 日前にユーザーに警告を開始する例を示します。show user の出力で、[Exp ]列と [Warn] 列の数値を確認します。

```
> configure user aging jdoe 100 30
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
jdoe              1001  Local Config  Enabled    No    100   30  Dis   No   5
```

次に、パスワードを 180 日後に期限切れになるように設定し、期限切れになる 7 日前にユーザーへの警告を開始し、7 日の猶予期間を含める例を示します。

```
> configure user aging joeuser 180 7 7
> show user
Login          UID   Auth Access  Enabled Reset   Exp   Warn    Grace  MinL Str Lock Max
admin          100  Local Config  Enabled    No  10000     7  Disabled    8 Ena   No N/A
extuser        501 Remote Config Disabled   N/A  99999     7  Disabled    1 Dis   No N/A
```

```
joeuser       1000  Local Config  Enabled   Yes    180     7         7    8 Dis   No
5
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure user add** | 新しいユーザーを追加します。 |
| **configure user forcereset** | 指定したユーザーのパスワードを強制的にリセットします。 |
| **configure user password** | 指定したユーザーのパスワードを設定します。 |
| **show user** | ユーザーアカウントを表示します。 |

# configure user delete

ユーザーアカウントを削除するには、**configure user delete** コマンドを使用します。

**configure user delete** ユーザー名

## 構文の説明

| | |
|---|---|
| *username* | ユーザーの名前を指定します。admin ユーザーは削除できません。 |

## 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

次の例では、ユーザーアカウントを削除します。

```
> configure user delete jdoe
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure user add** | 新しいユーザーを追加します。 |
| **configure user disable** | ユーザーアカウントを削除せずに無効にします。 |
| **show user** | ユーザーアカウントを表示します。 |

# configure user disable

ユーザーアカウントを削除せずに無効にするには、**configure user disable** コマンドを使用します。

**configure user disable** ユーザー名

## 構文の説明

| | |
|---|---|
| *username* | ユーザーの名前を指定します。**admin** ユーザーを無効にすることはできません。 |

## 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

ユーザーアカウントを削除せずに無効にするには、このコマンドを使用します。無効なユーザーはログインできません。無効なユーザーアカウントを再度有効にするには、**configure user enable** コマンドを使用します。

### 例

次の例では、ユーザーアカウントを無効にします。

```
> configure user disable jdoe
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
jdoe              1001  Local Config Disabled    No    100   30  Dis   No   5
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure user add** | 新しいユーザーを追加します。 |
| **configure user delete** | 指定したユーザーを削除します。 |
| **configure user enable** | 指定したユーザーを有効にします。 |
| **configure user unlock** | 指定したユーザーのアカウントのロックを解除します。 |
| **show user** | ユーザーアカウントを表示します。 |

# configure user enable

以前に無効にしたユーザーを有効にするには、**configure user enable** コマンドを使用します。

**configure user enable** ユーザー名

## 構文の説明

| | |
|---|---|
| *username* | ユーザーの名前を指定します。 |

## 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

ユーザーを有効にしてログインを許可するには、このコマンドを使用します。

### 例

次の例では、無効なユーザーアカウントを有効にします。**show user**[Enabled] 列が変更されたことに注意してください。

```
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
jdoe              1001  Local Config Disabled    No    100   30  Dis   No   5
> configure user enable jdoe
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
jdoe              1001  Local Config  Enabled    No    100   30  Dis   No   5
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure user add** | 新しいユーザーを追加します。 |
| **configure user disable** | 指定したユーザーを無効にします。 |
| **configure user forcereset** | 指定したユーザーのパスワードを強制的にリセットします。 |
| **configure user unlock** | 指定したユーザーのアカウントのロックを解除します。 |
| **show user** | ユーザーアカウントを表示します。 |

# configure user forcereset

ユーザーが次にログインするときにパスワードの変更を強制するには、**configure user forcereset** コマンドを使用します。

**configure user forcereset** ユーザー名

## 構文の説明

| | |
|---|---|
| *username* | ユーザーの名前を指定します。 |

## 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

ユーザーが次にログインするときにパスワードの変更を強制するには、このコマンドを使用します。ユーザーがログインしてパスワードを変更すると、強度のチェックが自動的に有効になります。

### 例

次の例では、ユーザーが次にログインするときにパスワードのリセットを強制します。

```
> configure user forcereset jdoe
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure user password** | 指定したユーザーのパスワードを設定します。 |
| **configure user strengthcheck** | 指定したユーザーのパスワードの強度チェック要件を設定します。 |
| **show user** | ユーザーアカウントを表示します。 |

# configure user maxfailedlogins

ユーザーの連続ログイン失敗回数の最大数を設定するには、**configure user maxfailedlogins** コマンドを使用します。

**configure user maxfailedlogins** *username number*

## 構文の説明

| | |
|---|---|
| *username* | ユーザーの名前を指定します。 |
| *number* | 連続ログイン失敗回数の最大数を 1 ー 9999 の範囲で指定します。 |

## コマンド デフォルト

デフォルトの動作や値はありません。ただし、新しいアカウントの作成時は、連続ログイン失敗回数のデフォルトの最大数は 5 です。

## 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。 |
| 6.2.2 | CC/UCAPL コンプライアンスモードで実行している場合は、**admin** ユーザーのログイン試行失敗回数の最大数も設定できます。 |

## 使用上のガイドライン

このコマンドを使用して、指定したユーザーのアカウントがロックされるまでの連続ログイン失敗回数の最大数を設定します。ユーザーアカウントがロックされた場合は、**configure user unlock** コマンドを使用してロックを解除します。

### 例

次の例では、連続ログイン失敗回数の最大数を 3 に設定します。

```
> configure user maxfailedlogins jdoe 3
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure user add** | 新しいユーザーを追加します。 |
| **configure user password** | 指定したユーザーのパスワードを設定します。 |
| **configure user unlock** | 指定したユーザーのアカウントのロックを解除します。 |
| **show user** | ユーザーアカウントを表示します。 |

# configure user minpasswdlen

ユーザーパスワードの最小長を指定するには、**configure user minpasswdlen** コマンドを使用します。

**configure user minpasswdlen** *username number*

## 構文の説明

| | |
|---|---|
| *username* | ユーザーの名前を指定します。 |
| *number* | パスワードの最小長を 1 ～ 127 の間で指定します。 |

## コマンド デフォルト

パスワードの最小長はありません。

## 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。 |
| 6.2.2 | **admin** ユーザーのパスワードの最小長を設定できるようになりました。 |

## 使用上のガイドライン

指定したユーザーのパスワードの最小長を設定するには、このコマンドを使用します。ユーザーアカウントの現在のパスワードの入力が求められます。最小長が現在のパスワードの長さよりも長い場合は、新しいパスワードを設定するように求められます。

### 例

次の例では、パスワードの最小長を8文字に設定します。この例では、現在のパスワードが新しい最小長よりも短いため、新しいパスワードを設定する必要があります。

```
> configure user minpasswdlen jdoe 8
Setting minimum password length to 8
Enter current password: <enter old password>
Enter new password for user jdoe: <enter new password>
Confirm new password for user jdoe: <enter new password>

Setting Minimum password length succeeded
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure user add** | 新しいユーザーを追加します。 |
| **show user** | ユーザーアカウントを表示します。 |

# configure user password

別のユーザーアカウントのパスワードを指定するには、**configure user password** コマンドを使用します。

**configure user password** ユーザー名

## 構文の説明

| | |
|---|---|
| *username* | ユーザーの名前を指定します。 |

## 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

指定したユーザーのパスワードを設定するには、このコマンドを使用します。このコマンドでは、ユーザーのパスワードを入力するよう要求されます。自分のパスワードを変更するには、このコマンドの代わりに **configure password** コマンドを使用します。

### 例

次の例では、別のユーザーのアカウントにパスワードを設定します。パスワードは入力時に非表示となります。

```
> configure user password jdoe
Enter new password for user jdoe: newpassword
Confirm new password for user jdoe: newpassword
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure password** | 現在ログインしているユーザーのパスワードを変更します。 |
| **configure user add** | 新しいユーザーを追加します。 |
| **configure user aging** | ユーザーパスワードのエージングを設定します。 |
| **configure user forcereset** | 指定したユーザーのパスワードを強制的にリセットします。 |
| **configure user maxfailedlogins** | 指定したユーザーのログイン失敗の最大回数を設定します。 |
| **configure user strengthcheck** | 指定したユーザーのパスワードの強度チェック要件を設定します。 |
| **show user** | ユーザーアカウントを表示します。 |

# configure user strengthcheck

ユーザーのパスワードに対する強度の要件を有効または無効にするには、**configure user strengthcheck** コマンドを使用します。

**configure user strengthcheck** ユーザー名 {**enable** | **disable**}

## 構文の説明

| | |
|---|---|
| *username* | ユーザーの名前を指定します。 |
| **enable** | 指定したユーザーのパスワードの要件を設定します。 |
| **disable** | 指定したユーザーのパスワードの要件を削除します。 |

## 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

このコマンドを使用して、パスワードの変更時にユーザーに対して特定のパスワード基準を満たすように要求する、強度チェックを有効または無効にします。ユーザーパスワードの有効期限が切れた場合、または **configure user forcereset** コマンドを使用した場合は、ユーザーが次にログインしたときにこの要件が自動的に有効になります。

### 例

次の例では、ユーザーアカウントの強度チェックを有効にします。

```
> configure user strengthcheck jdoe enable
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure user add** | 新しいユーザーを追加します。 |
| **configure user forcereset** | 指定したユーザーのパスワードを強制的にリセットします。 |
| **configure user maxfailedlogins** | 指定したユーザーのログイン失敗の最大回数を設定します。 |
| **configure user password** | 指定したユーザーのパスワードを設定します。 |
| **configure user unlock** | 指定したユーザーのアカウントのロックを解除します。 |
| **show user** | ユーザーアカウントを表示します。 |

# configure user unlock

ログイン失敗の最大数を超過したユーザーアカウントのロックを解除するには、**configure user unlock** コマンドを使用します。

**configure user unlock** ユーザー名

## 構文の説明

| | |
|---|---|
| *username* | ユーザーの名前を指定します。 |

## 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。 |

### 例

次の例では、ユーザーアカウントのロックを解除します。

```
> configure user unlock jdoe
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure user add** | 新しいユーザーを追加します。 |
| **configure user maxfailedlogins** | 指定したユーザーのログイン失敗の最大回数を設定します。 |
| **show user** | ユーザーアカウントを表示します。 |

# conn data-rate

負荷の大きいデータを渡すデバイス上の接続を表示するには、**conn data-rate** コマンドを使用します。このコマンドには、フローごとのデータレートが既存の接続情報とともに表示されます。データレート別に接続の収集を無効にするには、このコマンドの **no** 形式を使用します。

**conn data-rate**

**no conn data-rate**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.6 | このコマンドが導入されました。 |

## 使用上のガイドライン

**conn data-rate** コマンドは、デバイスの全体的な負荷の最も大きな部分を占めている可能性のある接続やユーザーを特定する際に特に役立ちます。

有効にすると、**conn data-rate** 機能によって、すべての接続に関する次の 2 つの統計情報が追跡されます。

- 接続の順方向および逆方向の現在の（1 秒）データレート。
- 接続の順方向および逆方向の最大（1 秒）データレート。

### 例

次の例では、接続データレート収集を有効にする方法、この機能が有効になっていることを確認する方法、およびデータレートを表示する方法を示します。

```
> conn data-rate
> show conn data-rate
Connection data rate tracking is currently enabled.
Use 'show conn detail' to see the data rates of active connections.

> show conn detail

TCP outside: 198.51.100.1/46994 NP Identity Ifc: 203.0.113.1/22,
flags UOB , idle 0s, uptime 9m24s, timeout 1h0m, bytes 68627
Initiator: 198.51.100.1, Responder: 203.0.113.1
data-rate forward/reverse
current rate: 1194/0 bytes/sec <-----------------current data rate for forward/reverse
flows
max rate: 2520/0 bytes/sec <----------------max data rate for forward/reverse flows
time since last max 0:08:54/NA <----------------time since last max data rate for
forward/reverse flows
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show conn data-rate** | 接続データレートトラッキングの現在の状態を表示します。 |

| Command | 説明 |
| --- | --- |
| **show conn detail** | データレート値によってフィルタ処理された接続を表示します。 |
| **clear conn data-rate** | 現在の最大データレート値をクリアします。 |

# connect fxos

FXOS Service Manager CLI モードを開始するには、**connect fxos** コマンドを使用します。

**connect fxos**

## 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

FXOS は、Firepower 2100、4100、および 9300 シリーズ デバイスの基盤となるソフトウェアです。

### 例

次に、脅威に対する防御 CLI で起動したときに FXOS CLI を開始する例を示します。? と入力し、FXOS で使用可能なコマンドを確認します。

```
> connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2015, Cisco Systems, Inc. All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license.

(...remaining copyrights omitted...)

kp-fpr2100-2#
```

次に、（**connect ftd** FXOS コマンドを使用して）最初に FXOS CLI から 脅威に対する防御 CLI を開始した場合の動作の例を示します。

```
> connect fxos
You came from FXOS Service Manager. Please enter 'exit' to go back.
```

# copy

フラッシュメモリに、またはフラッシュメモリからファイルをコピーするには、**copy** コマンドを使用します。

**copy** [ **/noconfirm** | **/noverify** ] [ *interface_name* ] { **/pcap capture:/** [ *buffer_name* ] | *src_url* | **running-config** | **startup-config** } *dest_url*

## 構文の説明

| | |
|---|---|
| **/noverify** | （オプション）開発キー署名済みイメージをコピーするときに署名検証をスキップします。 |
| **/noconfirm** | （オプション）確認のプロンプトを表示しないでファイルをコピーします。 |
| *interface_name* | （任意）ファイルをコピーするインターフェイス名を指定します。インターフェイスを指定しない場合、脅威に対する防御 はデータルーティングテーブルを確認します。データルーティングテーブルの一部ではない**管理**インターフェイスまたはその他の管理専用インターフェイスを使用するには、このオプションを使用して指定する必要があります。 |
| **/pcap capture:/** [ *buffer_name*] | 指定したバッファから **capture** コマンドの raw パケットキャプチャダンプをコピーします。 |
| **running-config** | システム メモリに格納されている実行コンフィギュレーションを指定します。 |
| **startup-config** | フラッシュ メモリに格納されているスタートアップ コンフィギュレーションを指定します。スタートアップコンフィギュレーションは、フラッシュメモリ内の隠しファイルになっています。 |

| | |
|---|---|
| *src-url*<br>*dest-url* | コピー元のファイル（コピーするファイル）とコピー先のファイル（コピーで作成するファイル）を指定します。2つのリモートロケーション間でコピーすることはできないため、コピー元のファイルがローカルの場合に、コピー先のファイルはローカルまたはリモートになります。コピー元のファイルがリモートの場合、コピー先のファイルはローカルである必要があります。ファイルの場所には次の URL シンタックスを使用します。<br>• **disk0:/**[[*path/*]*filename*] または **flash:/**[[*path/*]*filename*]：**flash** と **disk0** はどちらも内部フラッシュ メモリを示します。どちらのオプションを使用してもかまいません。<br>• **disk***n***:/**[[*path/*]*filename*]：オプションの外部フラッシュドライブを示します。*n* でドライブ番号を指定します。<br>• **smb:/**[[*path/*]*filename*]：サーバー メッセージブロック、UNIX サーバーのローカル ファイル システムを示します。<br>• **ftp://**[[*user*[**:***password*]@] *server*[:*port*]/[*path/*] *filename*[**;type=***xx*]]：**type** は次のいずれかのキーワードになります。**ap**（ASCII パッシブモード）、**an**（ASCII 通常モード）、**ip**（デフォルト：バイナリパッシブモード）、**in**（バイナリ通常モード）。<br>• **http**[**s**]**://**[[*user*[**:***password*] **@**]*server*[:*port*]/[*path/*]*filename*]<br>• **scp://**[[*user*[:*password*]@] *server*[/*path*]/*filename*[**;int=***interface_name*]]：SCP サーバーを示します。**;int=***interface* オプションを指定すると、ルートルックアップがバイパスされ、常に指定したインターフェイスを使用してセキュアコピー（SCP）サーバーに接続するようになります。<br>• **system:/**[[*path/*]*filename*]：システムメモリを表します。<br>• **tftp://**[[*user*[**:***password*]@] *server*[:*port*] /[*path/*]*filename*[**;int=***interface_name*]]：TFTP サーバーを示します。パス名にスペースを含めることはできません。**;int=***interface* オプションを指定すると、ルート ルックアップをバイパスし、常に指定したインターフェイスを使用して TFTP サーバーに接続するようになります。<br>• **cluster_trace:** ：cluster_trace ファイルシステムを示します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1 | インターフェイスを指定しない場合、脅威に対する防御はデータルーティングテーブルを確認します。管理ルーティングテーブルへのフォールバックはありません。以前は、デフォルトのルックアップは、データルーティングテーブルへのフォールバックを備えた管理ルーティングテーブルでした。管理インターフェイスと診断インターフェイスの統合により、管理ルーティングテーブルは自動的に使用されなくなりました。使用する場合は、管理インターフェイスを指定する必要があります。 |
| 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

クラスタ全体のキャプチャを実行後、マスターユニットで次のコマンドを入力して、クラスタ内のすべてのユニットから同じキャプチャ ファイルを TFTP サーバーに同時にコピーできます。

**cluster exec copy /noconfirm /pcap capture:***cap_name* **tftp://***location***/***path***/***filename***.pcap**

複数の PCAP ファイル（各ユニットから 1 つずつ）が TFTP サーバーにコピーされます。宛先のキャプチャ ファイル名には自動的にユニット名が付加され、filename_A.pcap、filename_B.pcap などとなります。ここで、A および B はクラスタ ユニット名です。

（注） ファイル名の末尾にユニット名を追加すると、別の宛先名が生成されます。

### 例

次に、インストールログのコピーを作成する例を示します。

```
> copy /noconfirm flash:/install.log flash:/install.save.log
Copy in progress...CC
INFO: No digital signature found
150498 bytes copied in 0.20 secs
```

次に、システム実行スペースでファイルをディスクから TFTP サーバーにコピーする例を示します。

```
> copy /noconfirm disk0:/install.log
tftp://10.7.0.80/install.log
```

次に、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。

```
> copy /noconfirm running-config tftp://10.7.0.80/firepower/device1.cfg
```

次に、開発キー署名済みイメージを検証せずにコピーする例を示します。

```
> copy /noverify /noconfirm lfbff.SSA exa_lfbff.SSA
Source filename [lfbff.SSA]?
Destination filename [exa_lfbff.SSA]?
Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Writing file disk0:/exa_lfbff.SSA...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Digital Signature was not verified
124125968 bytes copied in 61.740 secs (2034851 bytes/sec)
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **write net** | 実行コンフィギュレーションを TFTP サーバーにコピーします。 |

# cpu hog granular-detection

リアルタイムの占有検出を行い、短期間での CPU 占有しきい値を設定するには、**cpu hog granular-detection** コマンドを使用します。

**cpu hog granular-detection** ［**count** *number*］［**threshold** *value*］

## 構文の説明

| | |
|---|---|
| **count** *number* | 実行されるコード実行割り込みの数を指定します。値は 1 ～ 10000000 です。デフォルト値および推奨値は 1000 です。 |
| **threshold** *value* | 範囲は 1 ～ 100 です。設定されていない場合はデフォルトが使用されます。デフォルトはプラットフォームによって異なります。 |

## コマンド デフォルト

デフォルトの **count** は 1000 です。デフォルトの **threshold** は、プラットフォームによって異なります。

## 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

**cpu hog granular-detection** コマンドでは、現在のコード実行に 10 ミリ秒ごとに割り込み、割り込みの総数がカウントされます。割り込みによって CPU 占有がチェックされます。存在する場合は、ログに記録されます。このコマンドによって、データ パスでの CPU 占有検出の精度が低下します。

各スケジューラ ベースの占有は、最大 5 つの割り込みベースの占有エントリに関連付けられます。各エントリには最大 3 つのトレースバックが含まれる場合があります。割り込みベースの占有は上書きできません。空き領域がない場合は、新しい占有が廃棄されます。スケジューラ ベースの占有は、LRU ポリシーに従って引き続き再利用され、関連付けられている割り込みベースの占有はそのときにクリアされます。

### 例

次に、CPU 占有検出をトリガーする例を示します。

```
> cpu hog granular-detection count 1000 threshold 10
Average time spent on 1000 detections is 10 seconds, and it may take longer
under heavy traffic.
Please leave time for it to finish and use show process cpu-hog to check results.
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show processes cpu-hog** | CPU を占有しているプロセスを表示します。 |
| **clear process cpu-hog** | CPU を占有しているプロセスをクリアします。 |

# cpu profile activate

CPU プロファイリングを開始するには、**cpu profile activate** コマンドを使用します。

**cpu profile activate** ［*n_samples* ［**sample-process** *process_name*］［**trigger cpu-usage** *cpu%* ［*process_name*］］］

## 構文の説明

| | |
|---|---|
| *n_samples* | サンプル数 *n* を保存するためのメモリを割り当てます。有効値は 1 ～ 100,000 です。 |
| **sample-process** *process_name* | 特定のプロセスのみをサンプリングします。 |
| **trigger cpu-usage** *cpu%* [*process_name*] | グローバルな CPU 使用率である 5 秒を超えるまでプロファイラを開始しないようにし、CPU 使用率がこの値を下回った場合はプロファイラを停止します。<br>プロセス名を指定すると、プロセスの 5 秒間の CPU 使用率がトリガーとして使用されます。 |

## コマンド デフォルト

*n_samples* のデフォルト値は 1000 です。

*cpu%* のデフォルト値は 0 です。

## 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

CPU プロファイラは、CPU 使用率が高いプロセスの特定に役立ちます。CPU のプロファイリングでは、タイマー割り込みが発生したときに CPU で動作していたプロセスのアドレスをキャプチャします。このプロファイリングは、CPU の負荷に関係なく、10 ミリ秒ごとに発生します。たとえば、5000 のサンプルを取得する場合、プロファイリングが完了するまで正確に 50 秒かかります。CPU プロファイラが使用する CPU 時間が比較的少ない場合は、サンプルの収集に時間がかかります。CPU プロファイル レコードは、別のバッファでサンプリングされます。

**show cpu profile** コマンドを **cpu profile activate** コマンドとともに使用して、ユーザーが収集できる情報、および TAC が CPU の問題のトラブルシューティングに使用できる情報を表示します。**show cpu profile dump** コマンドの出力は、16 進形式で表示されます。

CPU プロファイラが開始条件の発生を待機している場合、**show cpu profile** コマンドは次の出力を表示します。

```
CPU profiling started: 12:45:57.209 UTC Wed Nov 14 2012
CPU Profiling waiting on starting condition.
Core 0: 0 out of 10 samples collected.
Core 1: 0 out of 10 samples collected.
Core 2: 0 out of 10 samples collected.
```

```
Core 3: 0 out of 10 samples collected.
CP
0 out of 10 samples collected.
```

### 例

次の例では、プロファイラをアクティブ化して、デフォルトである1000個のサンプルを格納するように指示します。次に、**show cpu profile** コマンドは、プロファイリングが進行中であることを示します。いくらかの時間が経過してから、次の**show cpu profile** コマンドは、プロファイリングが完了したことを示します。最後に、**show cpu profile dump** コマンドを使用して結果を取得します。出力をコピーし、シスコテクニカルサポートに提出します。完全な出力を得るには、SSH セッションをログに記録する必要があります。

```
> cpu profile activate
Activated CPU profiling for 1000 samples.
Use "show cpu profile" to display the progress or "show cpu profile dump" to interrupt
profiling and display the incomplete results.
> show cpu profile
CPU profiling started: 16:13:48.279 UTC Thu Oct 20 2016
CPU profiling currently in progress:
    Core 0: 501 out of 1000 samples collected.
    CP: 586 out of 1000 samples collected.
Use "show cpu profile dump" to see the results after it is complete or to interrupt
profiling and display the incomplete results.
> show cpu profile
CPU profiling started: 16:13:48.279 UTC Thu Oct 20 2016
CPU Profiling has stopped.
    Core 0 done with 1000 samples
    CP done with 1000 samples
Use "show cpu profile dump" to see the results.
> show cpu profile dump
(...output omitted...)
```

### 関連コマンド

| Command | 説明 |
|---|---|
| **show cpu profile** | CPU プロファイリングの進行状況を表示します。 |
| **show cpu profile dump** | プロファイリングに関して、完了していない結果または完了した結果を表示します。 |

# cpu profile dump

CPU プロファイリングの結果をテキストファイルに保存するには、**cpu profile dump** コマンドを使用します。

**cpu profile dump** *dest_url*

## 構文の説明

*dest_url*

- **disk0:/**[[*path/*]*filename*] または **flash:/**[[*path/*]*filename*]：**flash** と **disk0** はどちらも内部フラッシュ メモリを示します。いずれのオプションも使用できます。
- **disk***n***:/**[[*path/*]*filename*]：オプションの外部フラッシュドライブを示します。*n* でドライブ番号を指定します。
- **smb:/**[[*path/*]*filename*]：UNIX サーバーのローカルファイルシステムを示します。サーバー メッセージ ブロック ファイル システム プロトコルは、データをパッケージ化し、他のシステムと情報を交換するために、LAN マネージャおよび類似のネットワーク システムで使用されます。
- **ftp://**[[*user*[**:***password*]@] *server*[:*port*]/[*path/*] *filename*[**;type=***xx*]]：**type** は次のいずれかのキーワードになります。**ap**（ASCII パッシブモード）、**an**（ASCII 通常モード）、**ip**（デフォルト：バイナリパッシブモード）、**in**（バイナリ通常モード）。
- **http**[**s**]**://**[[*user*[**:***password*] **@**]*server*[:*port*]/[*path/*]*filename*]
- **scp://**[[*user*[:*password*]@] *server*[/*path*]/*filename*[**;int=***interface_name*]]：**;int=***interface* オプションを指定すると、ルート ルックアップがバイパスされ、常に指定したインターフェイスを使用してセキュア コピー（SCP）サーバーに接続するようになります。
- **tftp://**[[*user*[**:***password*]@] *server*[:*port*] /[*path/*]*filename*[**;int=***interface_name*]]：パス名にスペースを含めることはできません。**;int=***interface* オプションを指定すると、ルート ルックアップをバイパスし、常に指定したインターフェイスを使用して TFTP サーバーに接続するようになります。
- **cluster:**：クラスタファイルシステムを示します。

## 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

**CPU profile dump** コマンドは、CPU プロファイラの出力を、指定されたテキストファイルに 16 進数形式で書き込みます。

### 例

次に、最新の CPU プロファイルダンプを cpudump.txt という名前のファイルに保存する例を示します。

```
> cpu profile dump disk0:/cpudump.txt
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show cpu profile dump** | プロファイリングに関して、完了していない結果または完了した結果を表示します。 |

# crashinfo force

デバイスを強制的にクラッシュさせるには、**crashinfo force** コマンドを使用します。

**crashinfo force /noconfirm** {**page-fault** | **watchdog** | **process** *process_ID*}

## 構文の説明

| | |
|---|---|
| **page-fault** | ページフォールトを利用して、デバイスを強制的にクラッシュさせます。 |
| **watchdog** | ウォッチドッグを利用して、デバイスを強制的にクラッシュさせます。 |
| **process** *process_ID* | process_ID で指定されたプロセスを強制的にクラッシュさせます。プロセス ID を表示するには、**show kernel process** コマンドを使用します。 |

## コマンド デフォルト

デフォルトでは、デバイスはフラッシュメモリにクラッシュ情報ファイルを保存します。

## 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

**crashinfo force** コマンドを使用して、クラッシュ出力の生成をテストできます。クラッシュ出力では、本物のクラッシュを、**crashinfo force page-fault** コマンドまたは **crashinfo force watchdog** コマンドによって発生したクラッシュと区別できません。これは、これらのコマンドによって実際にクラッシュが発生しているためです。デバイスは、クラッシュのダンプが完了するとリロードします。

注意：実稼働環境では **crashinfo force** コマンドを使用しないでください。**crashinfo force** コマンドはデバイスをクラッシュさせて、強制的にリロードを実行します。

### 例

次に、ページフォールトにより強制的にクラッシュを実行する例を示します。

```
> crashinfo force /noconfirm page-fault
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear crashinfo** | クラッシュ情報ファイルの内容をクリアします。 |
| **crashinfo test** | デバイスでフラッシュメモリ内のファイルにクラッシュ情報を保存できるかどうかをテストします。 |
| **show crashinfo** | クラッシュ情報ファイルの内容を表示します。 |

# crashinfo test

フラッシュメモリのファイルにクラッシュ情報を保存するデバイスの機能をテストするには、**crashinfo test** コマンドを使用します。

**crashinfo test**

## 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

**crashinfo test** コマンドを入力してもデバイスはクラッシュしません。フラッシュ メモリ内に以前のクラッシュ情報ファイルがすでに存在する場合、そのファイルは上書きされます。

### 例

次に、クラッシュ情報ファイル テストの出力例を示します。

```
> crashinfo test
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear crashinfo** | クラッシュ情報ファイルの内容をクリアします。 |
| **crashinfo force** | デバイスを強制的にクラッシュさせます。 |
| **show crashinfo** | クラッシュ情報ファイルの内容を表示します。 |

# crypto ca trustpool export

PKI trustpool を構成する証明書をエクスポートするには、**crypto ca trustpool export** コマンドを使用します。

**crypto ca trustpool export** *filename*

## 構文の説明

| | |
|---|---|
| *filename* | エクスポートされた trustpool 証明書を保存するファイル。 |

## 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、アクティブな trustpool の内容全体を、指定されたファイルパスに pem コード形式でコピーします。

### 例

```
> crypto ca trustpool export disk0:/exportfile.pem
Trustpool certificates exported to disk0:/exportfile.pem
>
> more exportfile.pem
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEb
MBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDAdTYWxmb3JkMRow
GAYDVQQKDBFDb21vZG8gQ0EgTGltaXRlZDEhMB8GA1UEAwwYQUFBIENlcnRpZmlj
YXRlIFNlcnZpY2VzMB4XDTA0MDEwMTAwMDAwMFoXDTI4MTIzMTIzNTk1OVowezEL
MAkGA1UEBhMCR0IxGzAZBgNVBAgMEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4GA1UE
<More>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **crypto ca trustpool import** | PKI trustpool を構成する証明書をインポートします。 |
| **crypto ca trustpool remove** | 1 つの証明書を PKI trustpool から削除します。 |
| **show crypto ca trustpool** | PKI trustpool を表示します。 |

# crypto ca trustpool import

PKI trustpool を構成する証明書をインポートするには、**crypto ca trustpool import** コマンドを使用します。

**crypto ca trustpool import** ［**clean**］ **url** *url* **noconfirm** ［**signature-required**］
**crypto ca trustpool import** ［**clean**］ **default noconfirm**

## 構文の説明

| | |
|---|---|
| **clean** | インポート前にダウンロードされたすべての trustpool 証明書を削除します。 |
| **default** | デバイスのデフォルトの信頼できる CA リストに戻します。 |
| **noconfirm** | すべてのインタラクティブ プロンプトを抑制します。 |
| **signature-required** | 署名されたファイルのみを受け入れることを指定します。**signature-required** キーワードが含まれている場合に、シグネチャが存在しないかまたは確認できないと、インポートが失敗します。 |

| | |
|---|---|
| **url** *url* | インポートする trustpool ファイルの場所を指定します。<br>• **disk0:/**[[*path/*]*filename*]：内部フラッシュメモリを示します。<br>• **disk***n***:/**[[*path/*]*filename*]：オプションの外部フラッシュドライブを示します。*n* でドライブ番号を指定します。<br>• **smb:/**[[*path/*]*filename*]：UNIX サーバーのローカルファイルシステムを示します。サーバー メッセージ ブロック ファイル システム プロトコルは、データをパッケージ化し、他のシステムと情報を交換するために、LAN マネージャおよび類似のネットワーク システムで使用されます。<br>• **ftp://**[[*user*[**:***password*]@] *server*[:*port*]/[*path/*] *filename*[**;type=***xx*]]：**type** は次のいずれかのキーワードになります。**ap**（ASCII パッシブモード）、**an**（ASCII 通常モード）、**ip**（デフォルト：バイナリパッシブモード）、**in**（バイナリ通常モード）。<br>• **http**[**s**]**://**[[*user*[**:***password*] **@**]*server*[:*port*]/[*path/*]*filename*]<br>• **scp://**[[*user*[:*password*]@] *server*[/*path*]/*filename*[**;int=***interface_name*]]：**;int=***interface* オプションを指定すると、ルート ルックアップがバイパスされ、常に指定したインターフェイスを使用してセキュア コピー（SCP）サーバーに接続するようになります。<br>• **tftp://**[[*user*[**:***password*]@] *server*[:*port*] /[*path/*]*filename*[**;int=***interface_name*]]：パス名にスペースを含めることはできません。**;int=***interface* オプションを指定すると、ルート ルックアップをバイパスし、常に指定したインターフェイスを使用して TFTP サーバーに接続するようになります。 |

## 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

このコマンドを使用すると、trustpool バンドルを cisco.com からダウンロードするときに、ファイルのシグネチャを検証できます。バンドルを他のソースからダウンロードする場合や、シグネチャをサポートしていない形式でダウンロードする場合は、有効なシグネチャは必須ではありません。ユーザーにはシグネチャのステータスが通知され、バンドルを受け入れるかどうかを選択できます。

表示される可能性のあるインタラクティブな警告は、次のとおりです。

- 無効なシグネチャを持つシスコ バンドル形式
- シスコ以外のバンドル形式
- 有効なシグネチャを持つシスコ バンドル形式

（注） ファイルのシグネチャを確認できない場合は、その他の方法によって正規のファイルであることを確認していない限り、証明書をインストールしないでください。

### 例

次に、デフォルトの trustpool を復元する例を示します。

```
> crypto ca trustpool import clean default noconfirm
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **crypto ca trustpool export** | PKI trustpool を構成する証明書をエクスポートします。 |
| **crypto ca trustpool remove** | 1 つの証明書を PKI trustpool から削除します。 |
| **show crypto ca trustpool** | PKI trustpool を表示します。 |

# crypto ca trustpool remove

PKI trustpool から指定した 1 つの証明書を削除するには、**crypto ca trustpool remove** コマンドを使用します。

**crypto ca trustpool remove** *cert_fingerprint* ［**noconfirm**］

## 構文の説明

| | |
|---|---|
| *cert_fingerprint* | 証明書フィンガープリントは 16 進数です。 |
| **noconfirm** | すべてのインタラクティブプロンプトを抑制するには、このキーワードを指定します。 |

## 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。 |

### 例

次に、証明書を削除する例を示します。

```
> crypto ca trustpool remove 497904b0eb8719ac47b0bc11519b74d0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear crypto ca trustpool** | trustpool からすべての証明書を削除します。 |
| **crypto ca trustpool export** | PKI trustpool を構成する証明書をエクスポートします。 |
| **crypto ca trustpool import** | PKI trustpool を構成する証明書をインポートします。 |
| **show crypto ca trustpool** | PKI trustpool を表示します。 |

# d - r

# debug

特定の機能のデバッグ メッセージを表示するには、**debug** コマンドを使用します。デバッグ メッセージの表示を無効にするには、このコマンドの **no** 形式を使用します。すべてのデバッグ コマンドをオフにするには、**no debug all** を使用します。

**debug** *feature* ［*subfeature*］［*level*］
**no debug** *feature* ［*subfeature*］

## 構文の説明

| | |
|---|---|
| *feature* | デバッグをイネーブル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、**debug ?** 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 メッセージをイネーブルにできます。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 デフォルト

デフォルトのデバッグ レベルは 1 です。

## 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。 |
| 7.2 | このコマンドは、パスモニタリングのデバッグを含めるように変更されました。 |

## 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、DNS デバッグを有効にし、診断 CLI でメッセージを生成するアクションを実行します。デバッグメッセージは、「ERROR: % Invalid Hostname」というメッセージに続いて開始されます。Enter を押してプロンプトを表示します。次の例で、これらのデバッグメッセージが **show console-output** のディスプレイにどのように表示されるかを示します。

```
> debug dns
debug dns enabled at level 1.

> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower# ping www.example.com
                ^
ERROR: % Invalid Hostname
firepower# DNS: get global group DefaultDNS handle 1fa0b047
DNS: Resolve request for 'www.example.com' group DefaultDNS
DNS: No interfaces enabled
DNS: get global group DefaultDNS handle 1fa0b047
DNS: Resolve request for 'www.example.com' group DefaultDNS
DNS: No interfaces enabled

firepower# (press Ctrl+a, then d, to return to the regular CLI.)

Console connection detached.
> show console-output
... (output redacted)...
Message #75 : DNS: get global group DefaultDNS handle 1fa0b047
Message #76 : DNS: Resolve request for 'www.cisco.com' group DefaultDNS
Message #77 : DNS: No interfaces enabled
Message #78 : DNS: get global group DefaultDNS handle 1fa0b047
Message #79 : DNS: Resolve request for 'www.cisco.com' group DefaultDNS
Message #80 : DNS: No interfaces enabled
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show debug** | 現在アクティブなデバッグ設定を示します。 |
| **undebug** | ある機能のデバッグを無効にします。このコマンドは **no debug** の同意語です。 |

# debug packet-condition

デバッグする必要があるフローにフィルタを適用するには、**debug packet-condition** コマンドを使用します。フローのフィルタを削除するには、このコマンドの **no** 形式を使用します。フローのすべてのフィルタをオフにする場合、**no debug packet-condition** を使用します。

**debug packet-condition** [ **position** *<line>* ] **match** *<proto> {any|any4|any6|host <ip>|<ipv4>|<ipv4_mask>|<ipv6>/<prefixlen>}* [ *<src_operator> <ports> {any|any4|any6|host <ip>|<ipv4>|<ipv4_mask>|<ipv6>/<prefixlen>}* ] [ *<dest_operator> <ports>* ] [ *<icmp_type>* | *<icmp6_type>* ] [ *connection <connection-id>* ] [ *unidirectional* ]

## 構文の説明

| | |
|---|---|
| **position** *<line>* | 既存のフィルタのリストでフィルタを配置する位置を指定します。<br>*<line>* は番号を示します。 |
| **match***<proto> {any|any4|any6|host <ip>|<ipv4>|<ipv4_mask>|<ipv6>/<prefixlen>}* | フィルタの一致条件を指定します。<br>*<proto>* はプロトコルを示します。<br>*{any|any4|any6|host <ip>|<ipv4>|<ipv4_mask>|<ipv6>/<prefixlen>}* は IP アドレスオプションを示します。 |
| *<src_operator><port> {any|any4|any6|host <ip>|<ipv4>|<ipv4_mask>|<ipv6>/<prefixlen>}* | （オプション）送信元のポートまたは IP アドレスを指定します。 |
| *<dest_operator><port> {any|any4|any6|host <ip>|<ipv4>|<ipv4_mask>|<ipv6>/<prefixlen>}* | （オプション）宛先のポートまたはIPアドレスの詳細を指定します。 |
| *<icmp_type>|<icmp6_type>* | （オプション）接続の ICMP のタイプを指定します。 |
| *connection <connection-id>* | （オプション）進行中の接続の接続 ID を指定します。 |
| *unidirectional* | （オプション）指定した方向のパケットに対してのみデバッグを実行することを指定します。変数が指定されていない場合、デフォルトの動作は双方向であり、トラフィックは接続の順方向と逆方向の両方のフローと照合されます。 |

## コマンド デフォルト

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.4 | このコマンドが導入されました。 |

| リリース | 変更内容 |
|---|---|
| 6.5 | **debug packet condition** コマンドが **debug packet-condition** に変更されました。 |
| 6.6 | 進行中の接続をサポートするようにコマンド **debug packet-condition** が強化されました。 |

## 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

次に、デバッグする必要があるフローにフィルタを設定する方法の例を示します。

```
> debug packet-condition position 7 match tcp 1.2.3.0 255.255.255.0 any4
> debug packet-condition match tcp 1.2.3.0 255.255.255.0 eq www any4 unidirectional
> debug packet-condition match connection 70856531
> no debug packet-condition match tcp 1.2.3.0 255.255.255 eq www unidirectional
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **debug packet-start** | デバッグログデータベースへの接続を開き、データベースへのデバッグログの書き込みを開始します。 |
| **debug packet-stop** | デバッグログデータベースへの接続を閉じ、データベースへのデバッグログの書き込みを停止します。 |

# debug packet-module

デバッグメッセージを送信する各モジュールのレベルを設定するには、**debug packet-module** コマンドを使用します。レベルは 0（緊急）ー 7（デバッグ）の範囲で設定できます。レベルを設定すると、シビラティ（重大度）が同等以上のすべてのメッセージがログに記録されます。現在、サポートされているのは、DAQ、PDTS、ACL、およびSnortモジュールのみです。

**debug packet-module** [ **acl** | **all** | **daq** | **pdts** | **snort-engine** | **snort-fileprocessor** | **snort-firewall** ] < *0* ～ *7* >

## 構文の説明

| | |
|---|---|
| **acl** | パケット処理パスのアクセス コントロール ポリシーを選択します。 |
| **all** | パケット処理パスのすべてのモジュールを選択します。 |
| **daq** | パケット処理パスの DAQ 情報を選択します。 |
| **pdts** | パケット処理パスの PDTS（Snort へのデータプレーン送信/受信キュー）通信を選択します。 |
| **snort-engine** | パケット処理パスの Snort 情報を選択します。 |
| **snort-fileprocessor** | パケット処理パスの Snort ファイルプロセッサ情報を選択します。 |
| **snort-firewall** | パケット処理パスの Snort ファイアウォール情報を選択します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.4 | このコマンドが導入されました。 |
| 6.5 | **debug packet** コマンドが **debug packet-module** に変更されました。 |

## 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

次に、パケット処理パスの DAQ 情報にレベルを設定する例を示します。

```
> debug packet daq 6
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **debug packet-start** | デバッグログデータベースへの接続を開き、データベースへのデバッグログの書き込みを開始します。 |
| **debug packet-stop** | デバッグログデータベースへの接続を閉じ、データベースへのデバッグログの書き込みを停止します。 |

# debug packet-module trace

モジュールレベルのパケットトレースを有効にするには、**debug packet-module trace** コマンドを使用します。

**debug packet-module trace**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.6 | 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

次に、モジュールレベルのパケットトレースを有効にする例を示します。

```
> debug packet-module trace
```

次に、**debug packet-module trace** コマンドの出力例を示します。

```
ID          | Details                                                                  | Time
(ns)
----------- --------------------------------------------------------------------
------------------------------
6525759     | TCP        74.125.24.156      : 443   -> 192.168.0.31      : 58280 |
19-02-2020 06:48:43.050675868
```

さらに、次のコマンドを使用して、パケットの詳細を取得できます。

```
> show packet debugs module trace packet-id 6525759

Module: tcp-normalizer
Entry Time: 19-02-2020 06:48:43.050675868(ns)
****************************************
Module: translate
Entry Time: 19-02-2020 06:48:43.050684452(ns)
****************************************
Module: inspect_snort
Entry Time: 19-02-2020 06:48:43.050688028(ns)
****************************************
Module: pdts
Entry Time: 19-02-2020 06:48:43.050691843(ns)
```

```
****************************************
Module: pdts
Entry Time: 19-02-2020 06:48:43.051417112(ns)
****************************************
Module: pdts
Entry Time: 19-02-2020 06:48:43.051421642(ns)
****************************************
Module: tcp-normalizer
Entry Time: 19-02-2020 06:48:43.051424980(ns)
****************************************
Module: adjacency
Entry Time: 19-02-2020 06:48:43.051438331(ns)
****************************************
Module: fragment
Entry Time: 19-02-2020 06:48:43.051442861(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750763893(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750815391(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750831365(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750843286(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750889778(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750911474(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750942230(ns)
****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.750986576(ns)
****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.750999689(ns)
****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.751020193(ns)
****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.751051425(ns)
****************************************
Module: snort_firewall
Entry Time: 19-02-2020 06:48:43.751075029(ns)
****************************************
Module: snort_firewall
Entry Time: 19-02-2020 06:48:43.751084804(ns)
****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.751099348(ns)
****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.751118421(ns)
****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.751137018(ns)
****************************************
```

```
Module: daq
Entry Time: 19-02-2020 06:48:43.751152753(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.751164197(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.751177072(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.751186609(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.751203775(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.751224517(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.751236677(ns)
****************************************
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show packet debugs module trace** | 各モジュールから収集されたすべてのデバッグトレースのリストを表示します。 |
| **debug packet-start** | デバッグログデータベースへの接続を開き、データベースへのデバッグログの書き込みを開始します。 |
| **debug packet-stop** | デバッグログデータベースへの接続を閉じ、データベースへのデバッグログの書き込みを停止します。 |

# debug packet-start

パケットのデバッグを開始し、デバッグログデータベースへのデバッグログの書き込みを開始するには、**debug packet-start** コマンドを使用します。

**debug packet-start**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.4 | このコマンドが導入されました。 |
| 6.5 | このコマンドは、**debug packet start** から **debug packet-start** に変更されました。 |

## 使用上のガイドライン

**debug packet-start** は、デバッグログデータベースへの接続を開きます。このコマンドが呼び出されない限り、デバッグログはデータベースに書き込まれません。

### 例

次に、パケットのデバッグを開始する例を示します。

```
> debug packet-start
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **debug packet-stop** | デバッグログデータベースへの接続を閉じ、データベースへのデバッグログの書き込みを停止します。 |

# debug packet-stop

パケットのデバッグを停止し、デバッグログデータベースへのデバッグログの書き込みを停止するには、**debug packet-stop** コマンドを使用します。

**debug packet-stop**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.4 | このコマンドが導入されました。 |
| 6.5 | このコマンドは、**debug packet stop** から **debug packet-stop** に変更されました。 |

## 使用上のガイドライン

**debug packet-stop** は、デバッグログデータベースへの接続を閉じます。

### 例

次に、パケットのデバッグを停止する例を示します。

```
> debug packet-stop
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **debug packet-start** | デバッグログデータベースへの接続を開き、データベースへのデバッグログの書き込みを開始します。 |

# delete

フラッシュメモリからファイルを削除するには、**delete** コマンドを使用します。

**delete /noconfirm** ［**/recursive**］［**/replicate**］［**disk0:** | **disk***n***:** | **flash:**］［*path/*］*filename*

## 構文の説明

| | |
|---|---|
| **/noconfirm** | 確認のためのプロンプトを表示しません。 |
| **/recursive** | （任意）すべてのサブディレクトリの指定されたファイルを再帰的に削除します。 |
| **/replicate** | （オプション）スタンバイ ユニットの指定されたファイルを削除します。 |
| **disk0:** | （オプション）内部のフラッシュ メモリを指定します。 |
| **disk***n***:** | （任意）オプションの外部フラッシュドライブを示します。n でドライブ番号を指定します。通常は disk1 です。 |
| *filename* | 削除するファイルの名前を指定します。 |
| **flash:** | （オプション）内部のフラッシュ メモリを指定します。このキーワードは **disk0** と同じです。 |
| *path/* | （任意）ファイルのパスに指定します。 |

## コマンド デフォルト

ディレクトリを指定しない場合、ディレクトリはデフォルトで現在の作業ディレクトリになります。

## 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

パスを指定しない場合は、現在の作業ディレクトリからファイルが削除されます。ファイルの削除では、ワイルドカードがサポートされています。

### 例

次に、現在の作業ディレクトリから test.cfg という名前のファイルを削除する例を示します。

```
> delete /noconfirm test.cfg
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **cd** | 現在の作業ディレクトリから、指定したディレクトリに変更します。 |
| **dir** | 現在のディレクトリ内のファイルを一覧表示します。 |
| **rmdir** | ファイルまたはディレクトリを削除します。 |

# dig

完全修飾ドメイン名の IP アドレスを検索するには、**dig** コマンドを使用します。

**dig** *hostname*

## 構文の説明

| | |
|---|---|
| *hostname* | IP アドレスを検索するホストの完全修飾ドメイン名。たとえば、www.example.com などです。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1 | このコマンドが導入されました。このコマンドは、**nslookup** コマンドに置き換えられました。 |

## 使用上のガイドライン

完全修飾ドメイン名を許可するコマンドの中には、管理インターフェイス用に設定されたDNSサーバーを使用して完全修飾ドメイン名からIPアドレスを検索できないものがあります。データインターフェイスを通過するコマンド用にDNSサーバーが設定されていない場合は、**dig** コマンドを使用して IP アドレスを特定し、そのコマンドで IP アドレスを使用します。

**dig** コマンドは、管理インターフェイスでのみ機能し、管理インターフェイス用に設定されたDNSサーバーから情報を返します。データインターフェイスにさまざまなサーバーを設定する場合、データインターフェイスを通過するコマンドで FQDN を使用すると、異なる IP アドレスが返されたり、それらの DNS サーバーが名前を解決できない場合は IP アドレスがまったく返されないことがあります。

### 例

次に、FQDN www.example.com の IP アドレスを検索する例を示します。このアドレスは、出力の ANSWER セクションで強調表示されます。出力の末尾近くにある SERVER 表示は、解決を返した DNS サーバーの IP アドレスを示しています（この例の IP アドレスはサニタイズされています）。

ヘッダーの NOERROR ステータスは、要求が成功したことを示しています。その他の値はエラーを表します。たとえば、NXDOMAIN は、応答側の DNS サーバーにドメイン名が存在しないことを意味します。Linux の dig コマンドの出力の読み取りの詳細については、インターネットを検索してください。

```
> dig www.example.com
; <<>> DiG 9.11.4 <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14008
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
; COOKIE: 88335c9f3dc2ca124e36b5eb60db9067b6cae4de2ea5bffb (good)
```

```
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        0       IN      A       93.184.216.34
;; AUTHORITY SECTION:
example.com.            58911   IN      NS      a.iana-servers.net.
example.com.            58911   IN      NS      b.iana-servers.net.

;; ADDITIONAL SECTION:
a.iana-servers.net.     0       IN      A       199.43.135.53

;; Query time: 12 msec
;; SERVER: 10.163.47.11#53(10.163.47.11)
;; WHEN: Tue Jun 29 21:28:07 UTC 2021
;; MSG SIZE  rcvd: 152
```

# dir

ディレクトリの内容を表示するには、dir コマンドを使用します。

**dir** ［**/all**］［**all-filesystems**］［**/recursive**］［ **disk0:** | **disk***n***:** | **flash:** | **system:**］［*path*］［*filename*］

## 構文の説明

| | |
|---|---|
| **/all** | （任意）すべてのファイルを表示します。 |
| **/recursive** | （任意）ディレクトリの内容を再帰的に表示します。 |
| **all-filesystems** | （任意）すべてのファイル システムのファイルを表示します。 |
| **disk0:** | （任意）内部フラッシュメモリを指定し、続けてコロンを入力します。 |
| **disk***n***:** | （任意）オプションの外部フラッシュドライブを示します。*n* でドライブ番号を指定します。通常は disk1 です。 |
| **flash:** | （任意）デフォルト フラッシュ パーティションのディレクトリの内容を表示します。 |
| *path* | （任意）特定のパスを指定します。 |
| *filename* | （任意）ファイルの名前を指定します。 |
| **system:** | （任意）ファイル システムのディレクトリの内容を表示します。 |

## コマンド デフォルト

ディレクトリを指定しない場合、ディレクトリはデフォルトで現在の作業ディレクトリになります。

## 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、ディレクトリの内容を表示する例を示します。

```
> dir
Directory of disk0:/
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **cd** | 現在の作業ディレクトリから、指定したディレクトリに変更します。 |
| **pwd** | 現在の作業ディレクトリを表示します。 |
| **mkdir** | ディレクトリを作成します。 |
| **rmdir** | ディレクトリを削除します。 |

# dns update

DNS ポーリングタイマーの有効期限を待機せずに、指定されたホスト名を解決する DNS ルックアップを開始するには、**dns update** コマンドを使用します。

**dns update** ［**host** *fqdn_name*］［**timeout seconds** *number*］

## 構文の説明

| | |
|---|---|
| **host** *fqdn_name* | DNS アップデートを実行するホストの完全修飾ドメイン名を指定します。 |
| **timeout seconds** *number* | ルックアップ動作のタイムアウトを秒単位で指定します（3 ～ 30）。デフォルトは 30 です。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | 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、DNS ポーリング タイマーの有効期限を待機しないで、指定されたホスト名を解決する DNS ルックアップをすぐに開始します。ホスト名を指定せずに DNS 更新を実行すると、アクセス制御ルールで使用されるすべての名前（アクティブ化済みと認識される）が解決されます。コマンドの実行が終了すると、システムのコマンドプロンプトに「Done」と表示され、syslog メッセージが生成されます。

### 例

次の例では、アクセス制御ルールで使用されるすべての FQDN の DNS 更新を実行します。

```
> dns update
INFO: update dns process started
> [Done]
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear dns** | FQDN ネットワークオブジェクトの DNS 解決を削除します。 |
| **show dns** | FQDN ネットワークオブジェクトの DNS 解決を表示します。 |

# eotool コマンド

**eotool** コマンドは、Cisco Technical Assistance Center の指示の下でのみ使用してください。

# exit

CLI を終了するには、**exit** コマンドを使用します。

**exit**

## 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

通常の CLI では、**exit** および **logout** コマンドの動作は同じであり、デバイスとの SSH セッションを閉じます。

エキスパートモードの場合、**exit** を実行するとエキスパートモードが終了し、通常の CLI に戻ります。

診断 CLI（**system support diagnostic-cli**）を使用している場合、**exit** コマンドを実行すると特権 EXEC モードからユーザー EXEC モードに戻ります。

### 例

次に、**exit** コマンドを使用して CLI への SSH 接続を閉じる例を示します。

```
> exit
```

次に、**exit** コマンドを使用して、診断 CLI の特権 EXEC モード（プロンプトで **#** 記号で表される）からユーザー EXEC モードに戻る例を示します。ログオフメッセージは無視できます。CLI セッションはアクティブなままです。

```
firepower# exit
Logoff
Type help or '?' for a list of available commands.
firepower>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **logout** | CLI セッションからログオフします。 |

# expert

一部の手順で必要となるエキスパートモードを開始するには、**expert** コマンドを使用します。

**expert**

## 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

マニュアルの手順で求められた場合、または Cisco Technical Assistance Center から求められた場合のみ、エキスパートモードを使用します。

⚠

**注意** エキスパートモードでコマンドを実行しても、結果が Device Manager に反映されない場合があります。意図しない結果を避けるために、エキスパートモードでのみ記載されたコマンド、またはシスコテクニカルサポートから指示されたコマンドを使用してください。

### 例

次の例は、エキスパートモードを開始および終了する方法を示しています。エキスパートモードのプロンプトには、username@hostname 情報が表示されます。

```
> expert
admin@firepower:~$
admin@firepower:~$ exit
logout
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **exit** | エキスパートモードを終了します。 |

# failover active

スタンバイデバイスをアクティブ状態に切り替えるには、**failover active** コマンドを使用します。アクティブデバイスをスタンバイに切り替えるには、このコマンドの **no** 形式を使用します。

**failover active**
**no failover active**

## 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

スタンバイユニットからのフェールオーバー切り替えを開始するには **failover active** コマンドを使用し、アクティブユニットからのフェールオーバー切り替えを開始するには **no failover active** コマンドを使用します。この機能を使用して、障害が発生したユニットを稼働させたり、メンテナンスのためにアクティブ ユニットをオフラインにしたりできます。ステートフル フェールオーバーを使用していない場合、すべてのアクティブ接続がドロップされるため、クライアントはフェールオーバーの発生後、接続を再確立する必要があります。

### 例

次に、スタンバイユニットをアクティブに切り替える例を示します。

```
> failover active
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **failover reset** | デバイスを障害発生状態からスタンバイに移行します。 |

# failover exec

フェールオーバーペアの特定のユニットでコマンドを実行するには、 **failover exec** コマンドを使用します。

**failover exec** {**active** | **standby** | **mate**} *cmd_string*

## 構文の説明

| | |
|---|---|
| **active** | コマンドをフェールオーバーペアのアクティブユニットに対して実行することを指定します。 |
| *cmd_string* | 実行するコマンド。サポートされているコマンドについては、CLIのヘルプを参照してください。 |
| **mate** | コマンドをフェールオーバー ピアに対して実行することを指定します。 |
| **standby** | コマンドをフェールオーバーペアのスタンバイユニットに対して実行することを指定します。 |

## 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

**failover exec** コマンドを使用して、フェールオーバーペアの特定のユニットにコマンドを送信できます。

コマンドの出力は現在の端末セッションに表示されるため、**failover exec** コマンドを使用し、ピア装置で **show** コマンドを発行して、その結果を現在の端末で確認できます。

ピア装置でコマンドを実行するには、ローカル装置でコマンドを実行できるだけの十分な権限を持っている必要があります。

### 制限事項

- コマンドの完成およびコンテキストヘルプは、*cmd_string* 引数のコマンドでは使用できません。
- **debug**（**undebug**）コマンドを **failover exec** コマンドと一緒に使用することはできません。
- スタンバイ装置が故障状態の場合、故障の原因がサービス カードの不具合であれば、**failover exec** コマンドからのコマンドは受信できます。それ以外の場合、リモート コマンドの実行は失敗します。
- **failover exec mate failover exec mate** コマンドのような、再帰的な **failover exec** コマンドは入力できません。
- ユーザーの入力または確認が必要なコマンドでは、**/nonconfirm** オプションを使用する必要があります。

### 例

次に、**failover exec** コマンドを使用して、フェールオーバーピアのフェールオーバー設定を表示する例を示します。コマンドはアクティブユニットであるプライマリ ユニットで実行されるため、セカンダリのスタンバイ ユニットの情報が表示されます。

```
> failover exec mate show running-config failover
failover
failover lan interface failover GigabitEthernet0/3
failover polltime unit 1 holdtime 3
failover polltime interface 3 holdtime 15
failover link failover GigabitEthernet0/3
failover interface ip failover 10.0.5.1 255.255.255.0 standby 10.0.5.2
```

次に、**failover exec** コマンドを使用して、**show interface** コマンドをスタンバイユニットに送信する例を示します。

```
> failover exec standby show interface
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
      MAC address 000b.fcf8.c290, MTU 1500
      IP address 192.168.5.111, subnet mask 255.255.255.0
      216 packets input, 27030 bytes, 0 no buffer
      Received 2 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      284 packets output, 32124 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "outside":
      215 packets input, 23096 bytes
      284 packets output, 26976 bytes
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  23 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  24 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(10 Mbps)
      MAC address 000b.fcf8.c291, MTU 1500
      IP address 192.168.0.11, subnet mask 255.255.255.0
      214 packets input, 26902 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      215 packets output, 27028 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "inside":
      214 packets input, 23050 bytes
      215 packets output, 23140 bytes
```

```
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  21 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  21 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/2 "failover", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
      Description: LAN/STATE Failover Interface
      MAC address 000b.fcf8.c293, MTU 1500
      IP address 10.0.5.2, subnet mask 255.255.255.0
      1991 packets input, 408734 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      1835 packets output, 254114 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/2) software (0/0)
  Traffic Statistics for "failover":
      1913 packets input, 345310 bytes
      1755 packets output, 212452 bytes
      0 packets dropped
      1 minute input rate 1 pkts/sec,  319 bytes/sec
      1 minute output rate 1 pkts/sec,  194 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 1 pkts/sec,  318 bytes/sec
      5 minute output rate 1 pkts/sec,  192 bytes/sec
      5 minute drop rate, 0 pkts/sec
...
```

次に、ピアユニットに対して不正なコマンドを発行したときにエラーメッセージが返され、そのエラー メッセージが表示される例を示します。

```
> failover exec mate bad command
bad command
  ^
ERROR: % Invalid input detected at '^' marker.
```

次に、フェールオーバーが無効になっている場合に **failover exec** コマンドを使用すると返されるエラーメッセージの例を示します。

```
> failover exec mate show failover
ERROR: Cannot execute command on mate because failover is disabled
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **debug fover** | フェールオーバー関連のデバッグ メッセージを表示します。 |
| **debug xml** | **failover exec** コマンドによって使用される XML パーサーのデバッグ メッセージを表示します。 |
| **show failover exec** | **failover exec** コマンドモードを表示します。 |

# failover reload-standby

スタンバイユニットを強制的にリブートするには、**failover reload-standby** コマンドを使用します。

**failover reload-standby**

## 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

フェールオーバー ユニットが同期化されないときにこのコマンドを使用します。スタンバイユニットが再起動し、起動終了後にアクティブ ユニットと再同期化されます。

### 例

次に、アクティブユニットで **failover reload-standby** コマンドを使用して、スタンバイユニットを強制的にリブートする例を示します。

```
> failover reload-standby
```

# failover reset

障害が発生したデバイスを障害のない状態に復元するには、**failover reset** コマンドを入力します。

**failover reset**

## 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

**failover reset** コマンドを使用すると、障害が発生したユニットを、障害が発生していない状態にすることができます。**failover reset** コマンドはいずれのユニットでも入力できますが、常にアクティブユニットでコマンドを入力することを推奨します。アクティブユニットで **failover reset** コマンドを入力すると、スタンバイユニットが障害の発生していない状態に復元されます。

**show failover** コマンドを使用することにより、ユニットのフェールオーバーステータスを表示できます。

### 例

次に、障害が発生したユニットを障害が発生していない状態に変更する例を示します。

```
> failover reset
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show failover** | 装置のフェールオーバー ステータスに関する情報を表示します。 |

# file copy

FTP 経由で common ディレクトリからリモートホストにファイルを転送するには、**file copy** コマンドを使用します。

**file copy** *host_name user_id path filename_1* ［*filename_2 ... filename_n*］

## 構文の説明

| | |
|---|---|
| *host_name* | ターゲットリモートホストの名前または IP アドレスを指定します。 |
| *user_id* | リモートホストのユーザーを指定します。 |
| *path* | リモートホストの宛先パスを指定します。 |
| *filename_1* ～ *filename_n* | common ディレクトリから転送するファイルの名前を指定します。複数のファイル名を指定する場合は、空白で区切る必要があります。この引数では、ワイルドカードがサポートされます。 |

## コマンド デフォルト

このコマンドは、システムがトラブルシューティング ファイルを書き込む common ディレクトリからのみファイルを転送します。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.0.1 | このコマンドが導入されました。 |

### 例

この例では、common ディレクトリ内のすべてのファイルをユーザー **jdoe** 経由でアクセスするリモートホスト **sentinel** 上の **/pub** ディレクトリに転送します。

```
> file copy sentinel jdoe /pub *
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **file list** | common ディレクトリ内のファイルを一覧表示します。 |
| **file delete** | common ディレクトリからファイルを削除します。 |
| **file secure-copy** | SCP 経由で common ディレクトリのファイルを転送します。 |

# file delete

common ディレクトリからファイルを消去するには、**file delete** コマンドを使用します。

**file delete** *filename_1* ［*filename_2* **...** *filename_n*］

## 構文の説明

| | |
|---|---|
| *filename_1* ～ *filename_n* | common ディレクトリから削除するファイルの名前を指定します。複数のファイル名を指定する場合は、空白で区切る必要があります。この引数では、ワイルドカードがサポートされます。 |

## コマンド デフォルト

このコマンドは、システムがトラブルシューティング ファイルを書き込む common ディレクトリ内のファイルに対してのみ動作します。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.0.1 | このコマンドが導入されました。 |

### 例

この例では、単一のファイルを削除します。

```
> file delete 10.83.170.31-43235986-2363-11e6-b278-aff0a43948fe-troubleshoot.tar.gz
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **file list** | common ディレクトリ内のファイルを一覧表示します。 |
| **file copy** | FTP 経由で common ディレクトリのファイルを転送します。 |
| **file secure-copy** | SCP 経由で common ディレクトリのファイルを転送します。 |

# file list

common ディレクトリ内のファイルを一覧表示するには、**file list** コマンドを使用します。

**file list** ［*filename_1 ... filename_n*］

## 構文の説明

| | |
|---|---|
| *filename_1* ～ *filename_n* | common ディレクトリから一覧表示するファイルの名前を指定します。複数のファイル名を指定する場合は、空白で区切る必要があります。この引数では、ワイルドカードがサポートされます。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.0.1 | 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、システムがトラブルシューティング ファイルを書き込む common ディレクトリ内のファイルのみを一覧表示します。ファイル名を指定しない場合は、common ディレクトリ内のすべてのファイルがリストされます。

### 例

次に、common ディレクトリの内容を表示する例を示します。

```
> file list
May 26 17:46       137474048 /core_1464284811_rackham-sfr.cisco.com_diskmanager_11.21145
Jun 27 20:36        1464696832 /core_1467059810_rackham-sfr.cisco.com_lina_6.21293
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **file copy** | FTP 経由で common ディレクトリのファイルを転送します。 |
| **file delete** | common ディレクトリからファイルを削除します。 |
| **file secure-copy** | SCP 経由で common ディレクトリのファイルを転送します。 |

# file secure-copy

SCP経由でcommonディレクトリからリモートホストにファイルを転送するには、**file secure-copy** コマンドを使用します。

**file secure-copy** *host_name user_id path filename_1* ［*filename_2 ... filename_n*］

## 構文の説明

| | |
|---|---|
| *host_name* | ターゲットリモートホストの名前または IP アドレスを指定します。 |
| *user_id* | リモートホストのユーザーを指定します。 |
| *path* | リモートホストの宛先パスを指定します。 |
| *filename_1* ～ *filename_n* | common ディレクトリから転送するファイルの名前を指定します。複数のファイル名を指定する場合は、空白で区切る必要があります。この引数では、ワイルドカードがサポートされます。 |

## コマンド デフォルト

このコマンドは、システムがトラブルシューティング ファイルを書き込むcommonディレクトリからのみファイルを転送します。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.0.1 | このコマンドが導入されました。 |

### 例

この例では、common ディレクトリ内のすべてのファイルをユーザー **jdoe** 経由でアクセスするリモートホスト **101.123.31.1** 上の **/tmp** ディレクトリに転送します。

```
> file secure-copy 101.123.31.1 jdoe /tmp *
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **file copy** | FTP 経由で common ディレクトリのファイルを転送します。 |
| **file delete** | common ディレクトリからファイルを削除します。 |
| **file list** | common ディレクトリ内のファイルを一覧表示します。 |

# fsck

ファイルシステムのチェックを実行して破損を修復するには、**fsck** コマンドを使用します。

**fsck /noconfirm disk*n*:**

## 構文の説明

| | |
|---|---|
| **disk*n*:** | フラッシュメモリドライブを指定します。*n* はドライブ番号です。 |
| **/noconfirm** | コマンドがプロンプトなしで実行されるように指定します。このキーワードは必須です。 |

## 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

**fsck** コマンドは、ファイルシステムに破損がないかどうかをチェックし、破損があった場合には修復を試みます。より恒久的な手順を試みる前に、このコマンドを使用します。

FSCK ユーティリティで（電源障害や異常なシャットダウンなどによる）ディスクの破損箇所が修復される場合、FSCKxxx.REC という名前のリカバリファイルが作成されます。これらのファイルには、FSCK 実行時に回復されたファイルの一部またはファイル全体が含まれています。まれに、データを回復するためにこれらのファイルを調べる必要がある場合があります。通常、これらのファイルは必要なく、安全に削除できます。

（注） FSCK ユーティリティは起動時に自動的に実行されるため、手動で **fsck** コマンドを入力していない場合でもこれらのリカバリファイルが存在する場合があります。

### 例

次に、フラッシュ メモリのファイル システムをチェックする例を示します。

```
> fsck /noconfirm disk0:
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **delete** | ユーザーに表示されるすべてのファイルを削除します。 |
| **erase** | すべてのファイルを削除し、フラッシュ メモリをフォーマットします。 |
| **format** | ファイルシステムをフォーマットします。 |

# help

特定のコマンドのヘルプ情報を表示するには、**help** コマンドを使用します。

**help** {*command* | **?**}

## 構文の説明

| | |
|---|---|
| **?** | ヘルプを使用できるすべてのコマンドを表示します。 |
| *command* | CLI ヘルプを表示するコマンドを指定します。 |

## 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

**help** コマンドを使用すると、一部のコマンドのヘルプ情報が表示されます。**help** コマンドの後にコマンド名を入力することによって、個々のコマンドのヘルプを参照できます。コマンド名を指定せずに代わりに **?** を入力すると、ヘルプがあるすべてのコマンドがリストされます。

コマンドの一部を入力した後に ? を入力してヘルプを表示することもできます。これにより、コマンド文字列内のその場所で有効なパラメータが表示されます。

### 例

次に、**traceroute** コマンドのヘルプを表示する例を示します。

```
> help traceroute
USAGE:
        traceroute <destination> [source <src_address|src_intf>]
                   [numeric] [timeout <time>] [ttl <min-ttl> <max-ttl>]
                   [probe <probes>] [port <port-value>] [use-icmp]
DESCRIPTION:
traceroute      Print the route packets take to a network host
SYNTAX:
destination     Address or hostname of destination
src_address     Source address used in the outgoing probe packets
src_intf        Interface through which the destination is accessible
numeric         Do not resolve addresses to hostnames
time            The time in seconds to wait for a response to a probe
min-ttl         Minimum time-to-live value used in probe packets
max-ttl         Maximum time-to-live value used in probe packets
probes          The number of probes to send for each TTL value
port-value      Base UDP destination port used in probes
use-icmp        Use ICMP probes instead of UDP probes
```

# history

現在のセッションのコマンドライン履歴を表示するには、**history** コマンドを使用します。

**history** *limit*

## 構文の説明

| | |
|---|---|
| *limit* | エントリ数の履歴リストのサイズ。サイズを無制限に設定するには、つまり履歴全体を表示するには、「0」を入力します。 |

## 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

上矢印を使用して、過去のコマンドをスクロールすることもできます。

履歴ビューには、コマンドが入力された順序のシーケンス番号が含まれます。

### 例

このコマンドの出力例を次に示します。

```
> history 0
   48  show environment
   49  show network-static-routes
   50  show network
   51  show running-config
   52  show service-policy
   53  show ntp
   54  show cpu
   55  show memory
   56  history 0
>
```

# logging savelog

ログバッファをフラッシュメモリに保存するには、**logging savelog** コマンドを使用します。

**logging savelog** ［*savefile*］

## 構文の説明

| | |
|---|---|
| *savefile* | （オプション）保存されたログのファイル名。ファイル名を指定しない場合は、次に示すように、ログファイルはデフォルトのタイムスタンプフォーマットを使用して保存されます。<br><br>`LOG-YYYY-MM-DD-HHMMSS.TXT`<br><br>*YYYY* は年、*MM* は月、*DD* は日付、*HHMMSS* は時間、分、および秒で示された時刻です。 |

## 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

ログ バッファをフラッシュ メモリに保存する前に、バッファへのロギングをイネーブルにする必要があります。イネーブルにしないと、ログ バッファのデータはフラッシュ メモリに保存されません。ただし、設定されたロギングバッファサイズが 2MB を超える場合、内部ログバッファはフラッシュメモリに書き込まれません。Management Center（リモート）または Device Manager （ローカル）を使用してバッファロギングを設定します。

（注） **logging savelog** コマンドによってバッファはクリアされません。バッファをクリアするには、**clear logging buffer** コマンドを使用します。

### 例

次に、latest-logfile.txt というファイル名で、ログバッファをフラッシュメモリに保存する例を示します。

```
> logging savelog latest-logfile.txt
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear logging buffer** | ログ バッファが保持している syslog メッセージをすべて消去します。 |

| Command | 説明 |
| --- | --- |
| **copy** | TFTP サーバーまたは FTP サーバーを使用して、ファイルをある場所から別の場所にコピーします。 |
| **delete** | 保存されたログ ファイルなどのファイルをディスク パーティションから削除します。 |

# logout

CLI を終了するには、**logout** コマンドを使用します。

**logout**

## 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

**logout** コマンドを使用すると、デバイスからログアウトして CLI セッションを終了できます。**exit** コマンドを使用することもできます。

### 例

次に、デバイスからログアウトする方法の例を示します。

```
> logout
```

# memory caller-address

コールトレースまたは発信元 PC 用にプログラムメモリの特定の範囲を設定して、メモリの問題を容易に特定できるようにするには、**memory caller-address** コマンドを使用します。発信元 PC は、メモリ割り当てプリミティブを呼び出したプログラムのアドレスです。アドレス範囲を削除するには、このコマンドの no 形式を使用します。

**memory caller-address** *startPC endPC*
**no memory caller-address**

## 構文の説明

| | |
|---|---|
| *endPC* | メモリ ブロックの終了アドレス範囲を指定します。 |
| *startPC* | メモリ ブロックの開始アドレス範囲を指定します。 |

## コマンド デフォルト

メモリを追跡できるように、実際の発信元 PC が記録されます。

## 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

メモリの問題を特定のメモリブロックに限定するには、**memory caller-address** コマンドを使用します。

場合によっては、メモリ割り当てプリミティブの実際の発信元 PC が、プログラムの多くの場所で使用されている既知のライブラリ関数であることがあります。プログラムの個々の場所を特定するには、そのライブラリ関数の開始プログラム アドレスおよび終了プログラム アドレスを設定し、それによってライブラリ関数の呼び出し元のプログラムアドレスを記録します。

（注） 発信元アドレスの追跡を有効にすると、デバイスのパフォーマンスが一時的に低下することがあります。

### 例

次に、**memory caller-address** コマンドで設定したアドレスの範囲、および **show memory caller-address** コマンドによる表示結果の例を示します。

```
> memory caller-address 0x00109d5c 0x00109e08
> memory caller-address 0x009b0ef0 0x009b0f14
> memory caller-address 0x00cf211c 0x00cf4464
> show memory caller-address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **memory profile enable** | メモリ使用状況（メモリ プロファイリング）のモニタリングをイネーブルにします。 |
| **memory profile text** | プロファイルするメモリのテキスト範囲を設定します。 |
| **show memory** | 物理メモリの最大量とオペレーティング システムで現在使用可能な空きメモリ量について要約を表示します。 |
| **show memory binsize** | 特定のバイナリ サイズに割り当てられているチャンクの要約情報を表示します。 |
| **show memory profile** | デバイスのメモリ使用状況（プロファイリング）に関する情報を表示します。 |
| **show memory caller-address** | デバイスに設定されているアドレスの範囲を表示します。 |

# memory delayed-free-poisoner

**memory delayed-free-poisoner** コマンドを使用して、delayed free-memory poisoner ツールのパラメータを設定します。delayed free-memory poisoner ツールを有効にするには、**memory delayed-free-poisoner enable** コマンドを使用します。delayed free-memory poisoner ツールを無効にするには、このコマンドの **no** 形式を使用します。delayed free-memory poisoner ツールを使用すると、アプリケーションによってメモリが解放された後、解放メモリの変化をモニターできます。

**memory delayed-free-poisoner** {**enable** | **desired-fragment-count** *frag_count* | **desired-fragment-size** *frag-size* | **threshold** *heap_use_percent* | **validate** | **watchdog-percent** *watchdog_limit*}
**no memory delayed-free-poisoner enable**

## 構文の説明

| | |
|---|---|
| **enable** | delayed free-memory poisoner ツールの操作を開始します。 |
| **desired-fragment-count** *frag_count* | poisonerのキューに保持するメモリフラグメントの数を設定します。有効な値の範囲は 0 ー 8192 です。デフォルトは 16 です。 |
| **desired-fragment-size** *frag-size* | poisoner のキューに保持する連続した空きメモリフラグメントのサイズをバイト単位で設定します。有効な値の範囲は 0 ー 268435456 です。デフォルトは 102400 です。 |
| **threshold** *heap_use_percent* | poisoner のキューからメモリが解放されるシステムメモリ使用率のパーセンテージしきい値を 0 ー 100 の範囲で設定します。デフォルトは 100 です。 |
| **validate** | delayed free-memory poisoner キュー内の全要素の検証を強制実行します。 |
| **watchdog-percent** *watchdog_limit* | ウォッチドッグ制限をウォッチドッグしきい値（15秒）のパーセンテージとして設定します。値の範囲は 10 ～ 100 です。デフォルトは 50 です。 |

## コマンド デフォルト

**memory delayed-free-poisoner enable** コマンドはデフォルトでは無効になっています。

デフォルトの **desired-fragment-count** は 16 です。

デフォルトの **desire-fragment-size** は 102400 です。

デフォルトの **watchdog-percent** は 50 です。

## 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

delayed free-memory poisoner ツールをイネーブルにすると、メモリ使用状況およびシステム パフォーマンスに大きな影響を及ぼします。このコマンドは、Cisco Technical Assistance Center の指示の下でのみ使用してください。システムの使用率が高い間は、実働環境では実行しないでください。

このツールを有効にすると、デバイスで実行されているアプリケーションによるメモリ解放要求が FIFO キューに書き込まれます。要求が poisoner のキューに書き込まれるたびに、それに伴うメモリバイトのうち、下位メモリ管理には必要ないバイトが、値 0xcc で書き込まれて「改ざん」されます。

メモリ解放要求は、システムの空きメモリプールにある量よりも多くのメモリがアプリケーションで必要になるまで、キューに残ります。より多くのメモリが必要になると、poisoner はキュー内の少なくとも **desired-fragment-count** メモリバッファの **desired-fragment-size** バイトをシークし、そのメモリをキューからプルして検証します。**desired-fragment-size** と **desired-fragment-count** の値を変更することで、poisoner が大量のメモリ要求を処理するのにかかる時間を調整できます。

メモリに変更がない場合、メモリはシステムの空きメモリプールに返され、poisoner は最初に要求を行ったアプリケーションからのメモリ要求を再発行します。このプロセスは、要求元のアプリケーションに対して十分なメモリが解放されるまで繰り返されます。

改ざんされたメモリに変更があった場合、システムは強制的にクラッシュし、クラッシュの原因を確認するために使用できる診断出力を生成します。

delayed free poisoner には、プロセスの過剰なリソース使用を防ぐためのウォッチドッグメカニズムが含まれています。ウォッチドッグしきい値は 15 秒で、その間 CPU を放棄せずにプロセスが継続的に実行されると、poisoner はシステムを強制的にクラッシュさせます。

ウォッチドッグの動作は、ウォッチドッグ制限を設定することで調整できます。ウォッチドッグ制限は 15 秒のウォッチドッグしきい値の割合を示します。デフォルトは 50% です。したがって、delayed free poisoner がアクティブな場合、デフォルトでは、プロセスが CPU を放棄せずに 7.5 秒間連続して実行されると、そのプロセスからの追加のメモリ割り当て要求は、プロセスが再スケジュールされるまで失敗します。この動作は、ウォッチドッグ制限の値を変更することで調整できます。

過剰なメモリフラグメンテーションを防止し、システム CPU の負荷を軽減するために、poisoner がメモリをキューからシステムメモリプールに自動的に解放する空きメモリ使用率のパーセンテージ **threshold** を設定できます。（デフォルトでは、poisoner はシステムメモリが使い果たされるまでメモリをキューから解放しません）。

delayed free-memory poisoner ツールは、定期的にキューのすべての要素を自動的に検証します。**memory delayed-free-poisoner validate** コマンドを使用して手動で検証を開始することもできます。要素に予期しない値が含まれている場合、システムは強制的にクラッシュし、クラッシュの原因を突き止めるための診断出力を作成します。予期しない値が存在しない場合、要素はキューに残り、ツールによって正常に処理されます。**memory delayed-free-poisoner validate** コマンドを実行しても、キュー内のメモリはシステムメモリプールに返されません。

このコマンドの **no** 形式を実行すると、キュー内の要求で参照されるすべてのメモリが検証されずに空きメモリプールに返され、すべての統計カウンタがクリアされます。

### 例

次に、delayed free-memory poisoner ツールをイネーブルにする例を示します。

```
> memory delayed-free-poisoner enable
```

次に、delayed free-memory poisoner ツールが不正なメモリ再利用を検出した場合の出力例を示します。

```
delayed-free-poisoner validate failed because a
        data signature is invalid at delayfree.c:328.
    heap region:    0x025b1cac-0x025b1d63 (184 bytes)
    memory address: 0x025b1cb4
    byte offset:    8
    allocated by:   0x0060b812
    freed by:       0x0060ae15
Dumping 80 bytes of memory from 0x025b1c88 to 0x025b1cd7
025b1c80:                         ef cd 1c a1 e1 00 00 00  |          ........
025b1c90: 23 01 1c a1 b8 00 00 00 15 ae 60 00 68 ba 5e 02  |  #.........`.h.^.
025b1ca0: 88 1f 5b 02 12 b8 60 00 00 00 00 00 6c 26 5b 02  |  ..[...`.....l&[.
025b1cb0: 8e a5 ea 10 ff ff ff ff cc cc cc cc cc cc cc cc  |  ................
025b1cc0: cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc  |  ................
025b1cd0: cc cc cc cc cc cc cc cc                         |  ........
An internal error occurred.  Specifically, a programming assertion was
violated.  Copy the error message exactly as it appears, and get the
output of the show version command and the contents of the configuration
file.  Then call your technical support representative.
assertion "0" failed: file "delayfree.c", line 191
```

次の表では、出力の重要な部分について説明されています。

**表 *1:* 不正なメモリ使用に関する出力の説明**

| フィールド | 説明 |
|---|---|
| heap region | 要求元のアプリケーションが使用できるメモリ領域のアドレス領域およびサイズ。これは、要求されたサイズと同じ値ではなく、メモリ要求が行われたときにシステムがメモリを配分できるように小さくなることがあります。 |
| memory address | 障害が検出されたメモリの位置。 |
| byte offset | バイトオフセットはヒープ領域の先頭を基準にしており、このアドレスから始まるデータ構造を保持するためにフィールドが変更された場合には、バイトオフセットを使用してそのフィールドを見つけることができます。値が0か、またはヒープ領域バイトカウントよりも大きい値である場合は、問題が下位ヒープパッケージの予期しない値であることを示している可能性があります。 |
| allocated by/freed by | この特定のメモリ領域に関して実施された最後の malloc/calloc/realloc および解放要求の命令アドレス。 |

| フィールド | 説明 |
|---|---|
| Dumping... | 検出された障害がヒープ メモリ領域の先頭にどれだけ近いかに応じて、1 つまたは 2 つのメモリ領域のダンプ。システム ヒープ ヘッダーに続く 8 バイトは、このツールがさまざまなシステム ヘッダー値のハッシュとキュー リンクを保持するために使用するメモリです。システム ヒープ トレーラが検出されるまでの領域内のそれ以外のバイトは、0xcc に設定する必要があります。 |

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear memory delayed-free-poisoner** | delayed free-memory poisoner ツールのキューおよび統計情報をクリアします。 |
| **show memory delayed-free-poisoner** | delayed free-memory poisoner ツールのキューの使用状況に関する要約を表示します。 |

# memory logging

メモリロギングを有効にするには、**memory logging** コマンドを使用します。メモリロギングを無効にするには、このコマンドの **no** 形式を使用します。

**memory logging 1024-4194304** ［**wrap** ［**size** ［**1-2147483647**］ | **process** *process-name* ］
**no memory logging**

## 構文の説明

| | |
|---|---|
| **1024-4194304** | メモリ ロギング バッファのロギング エントリの数を指定します。指定する必要がある引数はこれだけです。 |
| **process** *process-name* | モニター対象のプロセスを指定します。<br>（注） Checkheaps プロセスは、非標準の方法でメモリ アロケータを使用するため、プロセスとして完全に無視されます。 |
| **size 1-2147483647** | モニターするサイズおよびエントリ数を指定します。 |
| **wrap** | バッファのラップ時にバッファを保存します。保存できるのは一度だけです。複数回ラップされると上書きされる可能性があります。バッファがラップすると、そのデータの保存をイネーブルにするトリガーがイベント マネージャに送信されます。 |

## 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

メモリ ロギング パラメータを変更するには、それをディセーブルにしてから、再度イネーブルにします。**show memory logging** コマンドを使用してログを表示します。

### 例

次に、メモリ ロギングをイネーブルにする例を示します。

```
> memory logging 202980
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show memory logging** | メモリ ロギングの結果を表示します。 |

# memory profile enable

メモリ使用状況（メモリプロファイリング）のモニタリングを有効にするには、**memory profile enable** コマンドを使用します。メモリプロファイルリングを無効にするには、このコマンドの **no** 形式を使用します。

**memory profile enable** ［**peak** *peak_value*］
**no memory profile enable** ［**peak** *peak_value*］

## 構文の説明

| | |
|---|---|
| **peak** *peak_value* | メモリ使用状況のスナップショットを使用率ピーク バッファに保存するメモリ使用状況しきい値を指定します。このバッファの内容を後で分析して、システムのピーク時のメモリ ニーズを判断できます。 |

## コマンド デフォルト

デフォルトでは、メモリ プロファイリングはディセーブルになっています。

## 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

メモリプロファイリングを有効にする前に、**memory profile text** コマンドを使用して、プロファイリングするメモリのテキスト範囲を設定する必要があります。

**clear memory profile** コマンドを入力するまで、一部のメモリはプロファイリングシステムによって保持されます。**show memory profile status** コマンドの出力を参照してください。

（注） メモリプロファイリングをイネーブルにすると、デバイスのパフォーマンスが一時的に低下する場合があります。

### 例

次に、メモリ プロファイリングをイネーブルにする例を示します。

```
> memory profile enable
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **memory profile text** | プロファイルするメモリのテキスト範囲を設定します。 |
| **show memory profile** | デバイスのメモリ使用状況（プロファイリング）に関する情報を表示します。 |

# memory profile text

プロファイリングするメモリのプログラムテキスト範囲を設定するには、**memory profile text** コマンドを使用します。無効にするには、このコマンドの no 形式を使用します。

**memory profile text** {*startPC endPC* | **all**} *resolution*
**no memory profile text** {*startPC endPC* | **all**} *resolution*

## 構文の説明

| | |
|---|---|
| **all** | メモリ ブロックのテキスト範囲全体を指定します。 |
| *endPC* | メモリ ブロックの終了テキスト範囲を指定します。 |
| *resolution* | ソーステキスト領域のトレースの精度を 1 ー 44582263 の範囲で設定する必要があります。 |
| *startPC* | メモリ ブロックの開始テキスト範囲を指定します。 |

## 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

テキスト範囲が小さい場合、精度を「4」にすると、命令への呼び出しが正常に追跡されます。テキスト範囲が大きい場合、精度を粗くしても初回通過には十分であり、範囲は次回の通過でさらに小さな領域にまで絞り込むことができます。

メモリプロファイリングを開始するには、**memory profile text** コマンドでテキスト範囲を入力した後、続けて **memory profile enable** コマンドを入力する必要があります。デフォルトでは、メモリプロファイリングはディセーブルになっています。

（注） メモリプロファイリングをイネーブルにすると、デバイスのパフォーマンスが一時的に低下する場合があります。

### 例

次に、精度を 100 にして、プロファイリングするメモリのテキスト範囲を設定する例を示します。

```
> memory profile text all 100
```

次に、メモリ プロファイリングのテキスト範囲のコンフィギュレーションおよびステータス（OFF）を表示する例を示します。

```
> show memory profile status
```

```
InUse profiling: OFF
Peak profiling: OFF
Memory used by profile buffers: 0 bytes
Profile:
0x00007efc3e0227a8-0x00007efc40aa1f8e(00000100)
```

（注） メモリプロファイリングを開始するには、**memory profile enable** コマンドを入力する必要があります。デフォルトでは、メモリ プロファイリングはディセーブルになっています。

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear memory profile** | メモリ プロファイリング機能によって保持されているバッファをクリアします。 |
| **memory profile enable** | メモリ使用状況（メモリ プロファイリング）のモニタリングをイネーブルにします。 |
| **show memory profile** | デバイスのメモリ使用状況（プロファイリング）に関する情報を表示します。 |

# memory tracking

ヒープメモリ要求の追跡を有効にするには、**memory tracking** コマンドを使用します。メモリ追跡を無効にするには、このコマンドの **no** 形式を使用します。

**memory tracking** {**enable** | **allocates-by-threshold** *min_allocates* | **bytes-threshold** *min_bytes* | **filter-from-address-pool** *address*}
**no memory tracking enable**

## 構文の説明

| | |
|---|---|
| **enable** | メモリの追跡を有効にします。 |
| **allocates-by-threshold** *min_allocates* | 発信者のアドレスプールのエントリには、少なくともこの数の割り当てコールを含める必要があります（0 ー 4294967295）。 |
| **bytes-threshold** *min_bytes* | 発信者のアドレスプールのエントリは、少なくともこのバイト数のメモリを消費する必要があります（0 ー 4294967295）。 |
| **filter-from-address-pool** *address* | このアドレスのアドレスプールのエントリを除外します。アドレスを決定するには、最初にトラッキングを有効にしてから、show memory tracking address を使用します。「memory tracking address pool」リストで「allocated by」アドレスを探します。たとえば、次のように表示されます。<br>...allocated by 0x00007efc3f80e508<br>次を使用して除外できます。<br>**filter-from-address-pool 0x00007efc3f80e508** |

## 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、ヒープ メモリ要求の追跡をイネーブルにする例を示します。

```
> memory tracking enable
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear memory tracking** | 現在収集されているすべての情報をクリアします。 |
| **show memory tracking** | メモリトラッキングの結果を表示します。 |

# more

ファイルの内容を表示するには、**more** コマンドを使用します。

**more** [**/ascii** | **/binary** | **/ebcdic** | **disk0:** | **disk1:** | **flash:** | **ftp:** | **http:** | **https:** | **tftp:** ] *filename*

## 構文の説明

| | |
|---|---|
| **/ascii** | （任意）バイナリ ファイルをバイナリ モード、ASCII ファイルをバイナリ モードで表示します。 |
| **/binary** | （任意）任意のファイルをバイナリ モードで表示します。 |
| **/ebcdic** | （任意）バイナリ ファイルを EBCDIC で表示します。 |
| **disk0:** | （任意）内部フラッシュメモリ上のファイルを表示します。 |
| **disk1:** | （任意）外部フラッシュメモリカード上のファイルを表示します。 |
| *filename* | 表示するファイルの名前を指定します。 |
| **flash:** | （任意）内部フラッシュメモリを指定し、続けてコロンを入力します。ASA 5500 シリーズの適応型セキュリティアプライアンスでは、**flash** キーワードは **disk0** のエイリアスです。 |
| **ftp:** | （任意）FTP サーバー上のファイルを表示します。 |
| **http:** | （任意）Web サイト上のファイルを表示します。 |
| **https:** | （任意）セキュアな Web サイト上のファイルを表示します。 |
| **tftp:** | （任意）TFTP サーバー上のファイルを表示します。 |

## コマンド デフォルト

ASCII モード。

## 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

**system support view-files** コマンドは、ログファイルを検索および表示するための優れたオプションです。

### 例

次に、「test.cfg」というローカル ファイルの内容を表示する例を示します。

```
> more test.cfg
: Saved
```

```
: Written by enable_15 at 10:04:01 Apr 14 2005
XXX Version X.X(X)
nameif vlan300 outside security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
ciscoasa test
fixup protocol ftp 21
fixup protocol h323 H225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list deny-flow-max 4096
access-list alert-interval 300
access-list 100 extended permit icmp any any
access-list 100 extended permit ip any any
pager lines 24
icmp permit any outside
mtu outside 1500
ip address outside 172.29.145.35 255.255.0.0
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
!
interface outside
!
route outside 0.0.0.0 0.0.0.0 172.29.145.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
snmp-server host outside 128.107.128.179
snmp-server location my_context, USA
snmp-server contact admin@example.com
snmp-server community public
no snmp-server enable traps
floodguard enable
fragment size 200 outside
no sysopt route dnat
telnet timeout 5
ssh timeout 5
terminal width 511
gdb enable
mgcp command-queue 0
Cryptochecksum:00000000000000000000000000000000
: end
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **cd** | 指定されたディレクトリに変更します。 |
| **pwd** | 現在の作業ディレクトリを表示します。 |

| Command | 説明 |
| --- | --- |
| **system support view-files** | ログファイルの内容を検索して表示します。 |

# nslookup（非推奨）

完全修飾ドメイン名の IP アドレスを検索する、または IP アドレスの完全修飾ドメイン名を検索するには、**nslookup** コマンドを使用します。

**nslookup** {*hostname* | *ip_address*}

## 構文の説明

| | |
|---|---|
| *hostname* | IP アドレスを検索するホストの完全修飾ドメイン名。たとえば、www.example.com などです。 |
| *ip_address* | 完全修飾ドメイン名を検索するホストの IP アドレス。 |

## 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。 |
| 6.6 | このコマンドは機能しなくなり、廃止されました。 |
| 7.1 | このコマンドが削除され、**dig** コマンドに置き換えられました。 |

## 使用上のガイドライン

完全修飾ドメイン名を許可するコマンドの中には、管理インターフェイス用に設定された DNS サーバーを使用して完全修飾ドメイン名から IP アドレスを検索できないものがあります。データインターフェイスを通過するコマンド用に DNS サーバーが設定されていない場合は、**nslookup** コマンドを使用して IP アドレスを特定し、そのコマンドで IP アドレスを使用します。

**nslookup** コマンドは、特定の IP アドレスの完全修飾ドメイン名を判断する場合にも役立ちます。

### 例

次に、www.cisco.com の IP アドレスを検索する例を示します。最初の [Server] および [Address] 情報には、DNS サーバー（完全修飾ドメイン名の場合もあります）、IP アドレス、およびポートが表示されます（この例では偽のアドレスを使用しています）。その後の情報は、入力した名前の正規の（実際の）ホスト名と IP アドレスを示します。

```
> nslookup www.cisco.com
Server:         10.102.6.247
Address:        10.102.6.247#53

www.cisco.com   canonical name = origin-www.cisco.com.
Name:   origin-www.cisco.com
Address: 173.37.145.84
```

次の例は、逆引き参照を実行し、IP アドレスのホスト名を決定する方法を示しています。最初の情報は、使用されている DNS サーバーに関するものです。マッピングされたホスト名が **name =** フィールドに示されます。

```
> nslookup 173.37.145.84
Server:         10.102.6.247
Address:        10.102.6.247#53

84.145.37.173.in-addr.arpa      name = www2.cisco.com.
```

# packet-tracer

ファイアウォールルールをテストする 5 つのタプルを指定して、トラブルシューティング用にパケットトレーシングを有効にするには、**packet-tracer** コマンドを使用します。ここでは、わかりやすいように、ICMP、TCP、および IP の各パケットのモデリング別に構文を示します。複数のパケットを再生し、 **pcap** キーワードを使用して完全なワークフローをトレースできます。

**packet-tracer input** *ifc_name* **icmp** {*sip* | **user** *username*} *type code* [*ident*] {*dip* | **fqdn** *fqdn-string*} [**detailed**] [**xml**]
**packet-tracer input** *ifc_name* {**tcp** | **udp**} {*sip* | **user** *username*} *sport* {*dip* | **fqdn** *fqdn-string*} *dport* [**detailed**] [**xml**]
**packet-tracer input** *ifc_name* **rawip** {*sip* | **user** *username*} *protocol* {*dip* | **fqdn** *fqdn-string*} [**detailed**] [**xml**]
**packet-tracer input** *ifc_name* **pcap** *pcap_filename* [ **bypass-checks** | **decrypted** | **detailed** | **persist** | **transmit** | **xml** | **json** | **force** ]

## 構文の説明

| | |
|---|---|
| **bypass-checks** | （任意）シミュレートされたパケットのセキュリティチェックをバイパスします。 |
| **decrypted** | （任意）シミュレートされたパケットを、復号された IPSec/SSL VPN と見なします。 |
| *code* | ICMP パケット トレースの ICMP コードを指定します。 |
| **detailed** | （オプション）トレース結果の詳細な情報を表示します。 |
| *dip* | パケット トレースの宛先アドレス（IPv4 または IPv6）を指定します。 |
| *dport* | TCP/UDP/SCTP パケット トレースの宛先ポートを指定します。 |
| **fqdn** *fqdn-string* | ホストの完全修飾ドメイン名を指定します。IPv4 の FQDN のみがサポートされます。 |
| **force** | 既存の pcap トレースを削除し、新しい pcap ファイルを実行します。 |
| **icmp** | 使用するプロトコルとして ICMP を指定します。 |
| *ident* | （任意）ICMP パケット トレースの ICMP ID を指定します。 |
| **inline-tag** *tag* | レイヤ 2 CMD ヘッダーに埋め込まれているセキュリティ グループ タグの値を指定します。有効な値の範囲は 0 ～ 65533 です。 |
| **input** *ifc_name* | パケットをトレースする送信元インターフェイス名を指定します。 |
| **json** | （任意）トレース結果を JSON 形式で表示します。 |
| **pcap** | pcap を入力として指定します。 |

| | |
|---|---|
| *pcap_filename* | トレース用のパケットを含む pcap ファイル名。 |
| *protocol* | raw IP パケット トレーシングのプロトコル番号（0 ～ 255）を指定します。 |
| **persist** | （任意）長期間のトレースを有効にし、クラスタでのトレースも有効にします。 |
| **rawip** | 使用するプロトコルとして raw IP を指定します。 |
| *sip* | パケット トレースの送信元アドレス（IPv4 または IPv6）を指定します。 |
| *sport* | TCP/UDP/SCTP パケット トレースの送信元ポートを指定します。 |
| **tcp** | 使用するプロトコルとして TCP を指定します。 |
| **transmit** | （任意）シミュレートされたパケットがデバイスから送信できるようにします。 |
| *type* | ICMP パケット トレースの ICMP タイプを指定します。 |
| **udp** | 使用するプロトコルとして UDP を指定します。 |
| **user** *username* | 送信元 IP アドレスとしてユーザーを指定する場合に domain\user の形式でユーザー アイデンティティを指定します。ユーザーに対して最後にマッピングされたアドレス（複数ある場合）がトレースに使用されます。 |
| **xml** | （オプション）トレース結果を XML 形式で表示します。 |

## 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。 |
| 6.6 | 出力が強化され、パケットのルーティング中にパケットを許可/拒否する特定の理由を提供するようになりました。 |
| 7.1 | トレースの入力として pcap ファイルを使用できるように、packet-tracer コマンドが拡張されました。 |

## 使用上のガイドライン

パケットのキャプチャに加えて、脅威に対する防御デバイスを介してパケットの寿命をトレースして、想定どおりに動作しているかどうかを確認できます。**packet-tracer** コマンドを使用すると、次の操作を実行できます。

- 実働ネットワークにおけるすべてのパケット ドロップをデバッグします。
- コンフィギュレーションが意図したとおりに機能しているかを確認する。

- パケットに適用可能なすべてのルール、およびルールが追加される原因となったCLI行を表示する。
- データ パス内でのパケット変化を時系列で表示する。
- データ パスにトレーサ パケットを挿入する。

**packet-tracer** コマンドは、パケットに関する詳細情報と、脅威に対する防御 デバイスによるパケットの処理方法を表示します。コンフィギュレーションからのコマンドが原因でパケットがドロップしたのではない場合、**packet-tracer** コマンドにより、原因に関する詳細な情報が読みやすい形式で表示されます。たとえば、ヘッダーの検証が無効なためパケットがドロップされた場合、「packet dropped due to bad ip header (reason)」メッセージが表示されます。

**packet-tracer** が単一のパケットを注入してトレースしている間、**pcap** キーワードにより、パケットトレーサは複数のパケット（最大100パケット）を再生し、フロー全体をトレースできます。pcap ファイルを入力として提供し、さらに分析するために XML または JSON 形式で結果を取得できます。トレース出力をクリアするには、**clear packet-tracer** の **pcap trace** サブコマンドを使用します。トレースの進行中は、トレース出力を使用できません。

### 例

次に、入力として pcap ファイルを使用してパケットトレーサを実行する例を示します。

```
> packet-tracer input inside pcap http_get.pcap detailed xml
```

次に、既存の pcap トレースバッファをクリアし、入力として pcap ファイルを提供することにより、パケットトレーサを実行する例を示します。

```
> packet-tracer input inside pcap http_get.pcap force
```

次に、HTTP ポート 10.100.10.10 から 10.100.11.11 への TCP パケットをトレースする例を示します。暗黙の拒否アクセス ルールによってパケットがドロップされることを示す結果が表示されます。

```
> packet-tracer input outside tcp 10.100.10.10 80 10.100.11.11 80
Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.86.116.1 using egress ifc  outside
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:
Result:
input-interface: outside
input-status: up
```

```
input-line-status: up
output-interface: NP Identity Ifc
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

次の例では、ネクストホップのARPエントリが含まれる直接接続されたホストでTCPパケットを追跡します。

```
firepower(config)# packet-tracer input inside tcp 192.168.100.100 12345 192.168.102.102
 80 detailed
Phase: 1
Type: ROUTE-LOOKUP
Subtype: No ECMP load balancing
Result: ALLOW
Config:
Additional Information:
Destination is locally connected. No ECMP load balancing.
Found next-hop 192.168.102.102 using egress ifc  outside(vrfid:0)

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group TEST global
access-list TEST advanced trust ip any any
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a8aa5e90, priority=12, domain=permit, trust
hits=17, user_data=0x2ae29aabc100, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=34, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a8488800, priority=0, domain=inspect-ip-options, deny=true
hits=22, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=inside(vrfid:0), output_ifc=any
```

```
Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=36, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a893e230, priority=0, domain=inspect-ip-options, deny=true
hits=10, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside(vrfid:0), output_ifc=any

Phase: 7
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 21, packet dispatched to next module
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Module information for reverse flow ...
snp_fp_inspect_ip_options
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Phase: 8
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.102.102 using egress ifc  outside(vrfid:0)

Phase: 9
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
```

```
Additional Information:
found adjacency entry for next-hop 192.168.102.102 on interface  outside
Adjacency :Active
mac address 0aaa.0bbb.00cc hits 5 reference 1

Result:
input-interface: inside(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: allow
```

次の例では、ネクストホップに対する有効なARPエントリがないためにドロップされたTCPパケットを追跡します。ドロップされた理由では、ARPテーブルをチェックするためのヒントも提供されています。

```
<Displays same phases as in the previous example till Phase 8>

Result:
input-interface: inside(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Drop-reason: (no-v4-adjacency) No valid V4 adjacency. Check ARP table (show arp) has
entry for nexthop., Drop-location: frame snp_fp_adj_process_cb:200 flow (NA)/NA
```

次の例では、NAT と到達可能なネクストホップを使用した準最適ルーティングのパケットトレーサを示しています。

```
firepower(config)# sh run route
route inside 0.0.0.0 0.0.0.0 192.168.100.100 1
route outside 0.0.0.0 0.0.0.0 192.168.102.102 10

firepower(config)# sh nat detail
Manual NAT Policies (Section 1)
1 (outside) to (dmz) source static src_real src_mapped  destination static dest_real
dest_mapped
translate_hits = 3, untranslate_hits = 3
Source - Origin: 9.9.9.0/24, Translated: 10.10.10.0/24
Destination - Origin: 192.168.104.0/24, Translated: 192.168.104.0/24
firepower(config)# packet-tracer input dmz tcp 192.168.104.104 12345 10.10.10.10 80
detailed

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (outside,dmz) source static src_real src_mapped destination static dest_real
dest_mapped
Additional Information:
NAT divert to egress interface outside(vrfid:0)
Untranslate 10.10.10.10/80 to 9.9.9.10/80

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
```

```
Config:
access-group TEST global
access-list TEST advanced trust ip any any
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a8aa5e90, priority=12, domain=permit, trust
hits=20, user_data=0x2ae29aabc100, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (outside,dmz) source static src_real src_mapped destination static dest_real
dest_mapped
Additional Information:
Static translate 192.168.104.104/12345 to 192.168.104.104/12345
Forward Flow based lookup yields rule:
in  id=0x2ae2a8aa4ff0, priority=6, domain=nat, deny=false
hits=4, user_data=0x2ae2a8a9d690, cs_id=0x0, flags=0x0, protocol=0
src ip/id=192.168.104.0, mask=255.255.255.0, port=0, tag=any
dst ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
input_ifc=dmz(vrfid:0), output_ifc=outside(vrfid:0)

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=40, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a89de1b0, priority=0, domain=inspect-ip-options, deny=true
hits=4, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=dmz(vrfid:0), output_ifc=any

Phase: 6
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (outside,dmz) source static src_real src_mapped destination static dest_real
dest_mapped
Additional Information:
Forward Flow based lookup yields rule:
out id=0x2ae2a8aa53d0, priority=6, domain=nat-reverse, deny=false
hits=5, user_data=0x2ae2a8a9d580, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
```

```
src ip/id=192.168.104.0, mask=255.255.255.0, port=0, tag=any
dst ip/id=9.9.9.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
input_ifc=dmz(vrfid:0), output_ifc=outside(vrfid:0)

Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=42, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a893e230, priority=0, domain=inspect-ip-options, deny=true
hits=13, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside(vrfid:0), output_ifc=any

Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 24, packet dispatched to next module
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Module information for reverse flow ...
snp_fp_inspect_ip_options
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Phase: 10
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.100.100 using egress ifc  inside(vrfid:0)

Phase: 11
```

```
Type: SUBOPTIMAL-LOOKUP
Subtype: suboptimal next-hop
Result: ALLOW
Config:
Additional Information:
Input route lookup returned ifc  inside is not same as existing ifc  outside
Doing adjacency lookup lookup on existing ifc outside

Phase: 12
Type: NEXTHOP-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Lookup Nexthop on interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.102.102 using egress ifc  outside(vrfid:0)

Phase: 13
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for Next-hop 192.168.102.102 on interface  outside
Adjacency :Active
mac address 0aaa.0bbb.00cc hits 5 reference 1

Result:
input-interface: dmz(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: allow
```

次の例では、NAT を使用した準最適ルーティングのパケットトレーサを示しています。ここでは、到達不能なネクストホップが原因でパケットがドロップされます。

```
firepower(config)# sh run route
route inside 0.0.0.0 0.0.0.0 192.168.100.100 1

firepower(config)# sh nat detail
Manual NAT Policies (Section 1)
1 (outside) to (dmz) source static src_real src_mapped  destination static dest_real
dest_mapped
translate_hits = 3, untranslate_hits = 3
Source - Origin: 9.9.9.0/24, Translated: 10.10.10.0/24
Destination - Origin: 192.168.104.0/24, Translated: 192.168.104.0/24


<Displays same phases as in the previous example till Phase 11>

Result:
input-interface: dmz(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Drop-reason: (no-adjacency) No valid adjacency, Drop-location: frame
snp_fp_adjacency_internal:5890 flow (NA)/NA
```

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。 |
| **show packet-tracer** | PCAP ファイルに対して最後に実行されたパケットトレーサのトレースバッファ出力を表示します。 |

# perfmon

コンソールにパフォーマンス情報を表示するには、**perfmon** コマンドを使用します。

**perfmon** {**verbose** | **interval***seconds* | **settings**}

## 構文の説明

| | |
|---|---|
| **verbose** | パフォーマンスモニター情報をコンソールに表示します。デフォルトでは、perfmon settings で「quiet」と表示される情報は表示されません。<br>診断 CLI で **perfmon verbose** をオフにする必要があります。 |
| **interval** *seconds* | コンソールでパフォーマンス表示がリフレッシュされるまでの秒数を指定します。 |
| **settings** | 間隔、および perfmon が quiet と verbose のどちらであるかを表示します。 |

## コマンド デフォルト

デフォルトの間隔は、120 秒です。

## 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

**perfmon** コマンドを使用すると、デバイスのパフォーマンスをモニターできます。**show perfmon** コマンドを使用すると、情報がすぐに表示されます。

**perfmon verbose** コマンドを使用すると、間隔ごとにコンソールに情報が表示されます。

情報は、コンソールポートで CLI に実際に接続している場合、または診断 CLI（**system support diagnostic-cli**）を使用している場合のみ自動的に表示されます。別のポートで CLI（管理インターフェイスを含む）を使用している場合は、**show console-output** コマンドを使用して自動的に生成された情報を表示します。または、このコマンドを使用せず、**show perfmon** コマンドを直接使用します。

このコマンドは、診断 CLI でのみ使用することを推奨します。

（注） 通常の CLI から **verbose** をオフにすることはできません。代わりに、診断 CLI で特権 EXEC モードからオフにする必要があります。「例」の項を参照してください。

## 例

次に、パフォーマンスモニター統計情報を 120 秒間隔でコンソールに表示する例を示します。出力の「Fixup」統計情報は、関連するプロトコル検査エンジンを指しています。

```
> perfmon verbose
> perfmon settings
interval: 120 (seconds)
verbose
> show console-output
...
Message #109 :
Message #110 : PERFMON STATS:                      Current      Average
Message #111 : Xlates                                0/s          0/s
Message #112 : Connections                           0/s          0/s
Message #113 : TCP Conns                             0/s          0/s
Message #114 : UDP Conns                             0/s          0/s
Message #115 : URL Access                            0/s          0/s
Message #116 : URL Server Req                        0/s          0/s
Message #117 : TCP Fixup                             0/s          0/s
Message #118 : TCP Intercept Established Conns       0/s          0/s
Message #119 : TCP Intercept Attempts                0/s          0/s
Message #120 : TCP Embryonic Conns Timeout           0/s          0/s
Message #121 : FTP Fixup                             0/s          0/s
Message #122 : AAA Authen                            0/s          0/s
Message #123 : AAA Author                            0/s          0/s
Message #124 : AAA Account                           0/s          0/s
Message #125 : HTTP Fixup                            0/s          0/s
Message #126 :
...
```

次に、冗長モードをオフにする例を示します。これは、診断 CLI から行う必要があります。

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower> enable
Password: <Press return, do not enter a password>

firepower# perfmon quiet
firepower# perfmon settings
interval: 120 (seconds)
quiet
firepower# <Press Ctrl+a, d>

Console connection detached.
> perfmon settings
interval: 120 (seconds)
quiet
```

関連コマンド

| Command | 説明 |
| --- | --- |
| **show perfmon** | パフォーマンス情報を表示します。 |

# pigtail コマンド

**pigtail** コマンドは、Cisco Technical Assistance Center の指示の下でのみ使用してください。

書き込まれたログを表示する場合は、**pigtail** の代わりに **tail-logs** コマンドを使用します。

⚠

**注意** ディスク使用率が高くなる可能性があるため、pigtail プロセスを実行中のままにしないでください。このプロセスがポリシーの展開中に実行されていると、展開の妨げになる可能性があります。pigtail プロセスを停止する方法については、Cisco Technical Assistance Center にお問い合わせください。

# ping

指定したインターフェイスから IP アドレスへの接続をテストするには、**ping** コマンドを使用します。使用できるパラメータは、通常の ICMP ベースの ping、TCP の ping、および「システム」の ping とで異なります。また、システムの ping は管理インターフェイスから実行されますが、他のタイプの ping はデータインターフェイスを通過します。テストでは、必ず正しいタイプの ping を使用してください。

**ping** ［**interface** *if_name* | **vrf** *name*］ *host* ［**repeat** *count*］［**timeout** *seconds*］［**data** *pattern*］［**size** *bytes*］［**validate**］
**ping tcp** ［**interface** *if_name* | **vrf** *name*］ *host port* ［**repeat** *count*］［**timeout** *seconds*］［**source** *host port*］
**ping system** *host*

## 構文の説明

| | |
|---|---|
| **data** *pattern* | （オプション、ICMP のみ）16 ビットデータ パターン（16 進数形式、0 ～ FFFF）を指定します。デフォルトは 0xabcd です。 |
| *host* | ping の送信先ホストの IPv4 アドレスまたは名前を指定します。ICMP ping の場合は、IPv6 アドレスも指定できます。IPv6 は、TCP またはシステム ping ではサポートされていません。<br><br>ping が www.example.com などの完全修飾ドメイン名を使用できるかどうかは、名前を解決する DNS サーバーの可用性に依存します。システム ping は管理インターフェイスに DNS サーバーを使用しますが、他のタイプの ping は管理 DNS サーバーを使用しません。 システム以外のホスト名の ping が機能するには、データインターフェイスの DNS を設定する必要があります。<br><br>**ping** がホスト名を解決できない場合、**nslookup** を使用して名前に関連付けられた IP アドレスを特定し、IP アドレスで ping を実行します。 |
| **interface** *if_name* | （オプション）ICMP の場合、これはホストがアクセス可能なインターフェイス名です。指定しない場合、host は IP アドレスに解決され、宛先インターフェイスを決定するためにルーティング テーブルが参照されます。TCP の場合は、送信元からの SYN パケットの送信に使用する入力インターフェイスを指定します。<br><br>Virtual Routing and Forwarding（VRF）が有効なときに **interface** キーワードを指定すると、ping は指定されたインターフェイスの仮想ルーティングテーブルを使用します。 |
| *port* | （TCP のみ）ping を送信するホストの TCP ポート番号（1 ～ 65535）を指定します。 |
| **repeat** *count* | （任意）ping 要求を繰り返す回数を指定します。デフォルトは 5 分です。 |

| | |
|---|---|
| **size** *bytes* | （オプション、ICMP のみ）データグラム サイズ（バイト単位）を指定します。デフォルトは 100 です。 |
| **source** *host port* | （オプション、TCP のみ）ping の送信元の特定の IP アドレスおよびポートを指定します（特定のポートを指定しない場合は port = 0 を使用します）。 |
| **system** | 管理インターフェイスを通じてホストに ping を実行します。データインターフェイスを介した ping とは違い、システム ping のデフォルト数はありません。ping は Ctrl+c を使用して停止するまで続けられます。 |
| **tcp** | （オプション）TCP での接続をテストします（デフォルトは ICMP です）。TCP ping では、SYN パケットを送信し、宛先から SYN-ACK パケットが返されると成功と見なします。TCP ping は同時に複数実行することもできます。 |
| **timeout** *seconds* | （オプション）タイムアウト間隔（秒数）を指定します。デフォルト値は 2 秒です。 |
| **validate** | （オプション、ICMP のみ）応答データを検証します。 |
| **vrf** *name* | （任意）Virtual Routing and Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、仮想ルータの名前を指定して、使用する仮想ルーティングテーブルを選択できます。このキーワードは、**interface** キーワードと同時に使用することはできません。<br><br>Virtual Routing and Forwarding（VRF）が有効なときに **interface** キーワードを指定すると、ping は指定されたインターフェイスの仮想ルーティングテーブルを使用します。 |

## 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。 |
| 6.6 | **vrf** キーワードが追加されました。 |

## 使用上のガイドライン

**ping** コマンドを使用すると、デバイスが接続可能かどうか、またはホストがネットワークで使用可能かどうかを判断できます。

通常の ICMP ベースの ping を使用する場合、それらのパケットの送信を禁止する ICMP ルールがないことを確認してください（ICMP ルールを使用していなければ、すべての ICMP トラフィックが許可されます）。

TCP ping を使用する場合は、指定したポートでの TCP トラフィックの送受信がアクセス ポリシーで許可されている必要があります。

このコンフィギュレーションは、**ping** コマンドで生成されたメッセージに対して、デバイスが応答したり受け入れたりするために必要です。**ping** コマンドの出力は、応答が受け入れられた

かどうかを示します。ホストが応答しない場合は、**ping** コマンドを入力すると、次のようなメッセージが表示されます。

```
> ping 10.1.1.1
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

デバイスがネットワークに接続していて、トラフィックを送受信していることを確認するには、**show interface** コマンドを使用します。指定されたインターフェイスの名前は、ping の送信元アドレスとして使用されます。

### 例

次に、データインターフェイスを介してIPアドレスにアクセスできるかどうかを判断する例を示します。インターフェイスが指定されていないため、アドレスへの到達方法を判断するためにルーティングテーブルが使用されます。

```
> ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

次の例では、TCP ping を使用して、データインターフェイスを介してホストにアクセス可能かどうかを判断します。

```
> ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

> ping tcp 10.0.0.1 21 source 192.168.1.1 2002 repeat 10
Type escape sequence to abort.
Sending 10 TCP SYN requests to 10.0.0.1 port 21
from 192.168.1.1 starting port 2002, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/2/2 ms
```

次の例では、システム ping を実行して、管理インターフェイスから www.cisco.com にアクセスできるかどうかを判断します。ping を停止するには、Ctrl+c を使用する必要があります（出力では ^C で示されます）。

```
> ping system www.cisco.com
PING origin-www.cisco.COM (72.163.4.161) 56(84) bytes of data.
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=1 ttl=242 time=10.6 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=2 ttl=242 time=8.13 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=3 ttl=242 time=8.51 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=4 ttl=242 time=8.40 ms
^C
--- origin-www.cisco.COM ping statistics ---
```

```
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 8.139/8.927/10.650/1.003 ms
>
```

次の例では、redという名前の仮想ルータのルーティングテーブルを使用して、アドレスに ping を実行します。

```
> ping vrf red 2002::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/20 ms
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **nslookup** | ホスト名または IP アドレスの DNS ルックアップを実行します。 |
| **show interface** | インターフェイス コンフィギュレーションに関する情報を表示します。 |

# pmtool コマンド

**pmtool** コマンドは、Cisco Technical Assistance Center の指示の下でのみ使用してください。

# reboot

デバイスをリブートするには、**reboot** コマンドを使用します。

**reboot**

## 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

```
> reboot
This command will reboot the system. Continue?
Please enter 'YES' or 'NO': yes

Broadcast message from root@firepower

The system is going down for reboot NOW!
...
```

# redundant-interface

アクティブにする冗長インターフェイスのメンバーインターフェイスを設定するには、**redundant-interface** コマンドを使用します。

**redundant-interface redundant** *number* **active-member** *physical_interface*

## 構文の説明

| | |
|---|---|
| **active-member** *physical_interface* | アクティブ メンバーを設定します。使用可能な物理インターフェイス名（GigabitEthernet0/0 など）を表示するには、show interface コマンドを使用します。両方のメンバー インターフェイスが同じ物理タイプである必要があります。 |
| **redundant** *number* | 冗長インターフェイス ID（**redundant 1** など）を指定します。番号は 1 ー 8 です。 |

## コマンド デフォルト

デフォルトで、コンフィギュレーション内の最初のメンバーインターフェイスが使用可能な場合、そのインターフェイスがアクティブ インターフェイスとなります。

## 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

Device Manager に冗長インターフェイスを作成します。冗長インターフェイスを作成する場合は、プライマリインターフェイスを指定します。このコマンドを使用して、実行時にアクティブになるインターフェイスを変更します。

どのインターフェイスがアクティブであるかを表示するには、次のコマンドを入力します。

**show interface redundant***number* **detail | grep Member**

次に例を示します。

```
> show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

### 例

次の例では、redundant1 インターフェイスのアクティブインターフェイスを変更します。

```
> show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2

> redundant-interface redundant 1 active-member gigabitethernet0/2
```

関連コマンド

| Command | 説明 |
| --- | --- |
| **clear interface** | **show interface** コマンドのカウンタをクリアします。 |
| **show interface** | インターフェイスの実行時ステータスと統計情報を表示します。 |

# restore

Secure Firewall Management Centerによって管理されている Secure Firewall Threat Defense デバイスからローカルにバックアップされた設定を復元するには、**restore** コマンドを使用します。リモートの場所に保存されたバックアップを復元するには、バックアップファイルの場所とユーザー名に対して追加パラメータを指定します。

**restore remote-manager-backup** [ *backup tar-file* | **location** [*scp-hostname username filepath backup tar-file*] ]

## 構文の説明

| | |
|---|---|
| **remote-manager-backup** *backup tar-file* | Secure Firewall Management Center によって作成されたローカルバックアップを復元します。ローカル バックアップ ファイルが Secure Firewall Threat Defense デバイスに保存されます。 |
| **remote-manager-backup location** *scp-hostname username filepath backup tar-file* | Secure Firewall Management Center によって作成されたリモートバックアップを復元します。リモートバックアップは、ユーザーが設定した場所に保存され、SCP サーバーからアクセスできます。また、ホスト名、ユーザー名、およびファイルパスによって識別されます。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

## 使用上のガイドライン

**restore** コマンドは、新しい/交換用 Secure Firewall Threat Defense の Secure Firewall Threat Defense システムファイル、Snort DB テーブル、および LINA 実行コンフィギュレーションを復元します。また、**restore** コマンドを使用すると、実際の復元操作を実行する前に、Secure Firewall Threat Defense デバイス上の既存の LINA 実行コンフィギュレーションが削除されます。これにより、Secure Firewall Threat Defense デバイスはバックアップが実行された時点で存在する設定のみを保持します。復元操作が成功すると、交換用デバイスのシリアル番号を除くすべてのデバイス設定が交換されます。

復元操作により、元のデバイスに割り当てられた汎用一意識別子（UUID）を使用して、交換用/新規 Secure Firewall Threat Defense デバイスと元の Secure Firewall Management Center デバイスとの接続が再確立されます。復元が正常に完了すると、Secure Firewall Management Center はデバイスのすべてのポリシーを期限切れとしてマークし、デバイスの交換手順が完了したときに、交換用 Secure Firewall Threat Defense に影響する可能性のある Secure Firewall Management Center の設定変更が展開されるようにします。これにより、新しい Secure Firewall Threat Defense および Secure Firewall Management Center 設定が同期されます。

### 例

次に、ローカルバックアップファイルからの復元操作の例を示します。

```
> restore remote-manager-backup 10.10.1.168_PRIMARY_20180614055906.tar
```

次に、リモートバックアップファイルからの復元操作の例を示します。

```
>restore remote-manager-backup location 10.106.140.100 admin /Volume/home/admin
10.10.1.168_PRIMARY_20180614055906.tar
```

# 第 II 部

# S コマンド

# sa - show a

# sftunnel-status

デバイスと管理側 Management Center 間の接続（トンネル）のステータスを表示するには、**sftunnel-status** コマンドを使用します。

**sftunnel-status**

## 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

デバイスと管理側 Management Center 間の接続（トンネル）のステータスを表示するには、**sftunnel-status** コマンドを使用します。ローカルマネージャである Device Manager を使用している場合、このコマンドを実行しても情報は表示されません。

ステータス情報には、次のセクションが含まれます。

- [SFTUNNEL Status]：接続が確立された時刻、および接続で使用される管理インターフェイスに関する情報。
- [RUN STATUS]：IP アドレス、暗号化、および登録ステータス情報。
- [PEER INFO]：Management Center とこのデバイスへの接続に関する情報。このセクションには、ID、正常性イベント、RPC、NTP、IDS、マルウェアルックアップ、CSM_CCM（デバイスの設定に使用）、eStreamer、UE チャネル、および FSTREAM など、さまざまなサービスのためにシステム間で送信される可能性がある複数のタイプのメッセージの統計ブロックも含まれます。
- [RPC status]。

### 例

次に、**sftunnel-status** コマンドの出力例を示します。

```
> sftunnel-status

SFTUNNEL Start Time: Tue Oct 11 21:44:44 2016
        Both IPv4 and IPv6 connectivity is supported
        Broadcast count = 2
        Reserved SSL connections: 0
        Management Interfaces: 1
        br1 (control events) 10.83.57.37,2001:420:2710:2556:1:0:0:37

**********************

**RUN STATUS****10.83.57.41*************
        Cipher used = AES256-GCM-SHA384 (strength:256 bits)
        ChannelA Connected: Yes, Interface br1
        Cipher used = AES256-GCM-SHA384 (strength:256 bits)
        ChannelB Connected: Yes, Interface br1
        Registration: Completed.
```

```
        IPv4 Connection to peer '10.83.57.41' Start Time: Tue Oct 11 21:46:00 2016

PEER INFO:
        sw_version 6.2.0
        sw_build 2007
        Management Interfaces: 1
        eth0 (control events) 10.83.57.41,2001:420:2710:2556:1:0:0:41
        Peer channel Channel-A is valid  type (CONTROL), using 'br1',
connected to '10.83.57.41' via '10.83.57.37'
        Peer channel Channel-B is valid  type (EVENT), using 'br1',
connected to '10.83.57.41' via '10.83.57.37'

        TOTAL TRANSMITTED MESSAGES <3> for Identity service
        RECEIVED MESSAGES <2> for Identity service
        SEND MESSAGES <1> for Identity service
        HALT REQUEST SEND COUNTER <0> for Identity service
        STORED MESSAGES for Identity service (service 0/peer 0)
        STATE <Process messages> for Identity service
        REQUESTED FOR REMOTE <Process messages> for Identity service
        REQUESTED FROM REMOTE <Process messages> for Identity service

        TOTAL TRANSMITTED MESSAGES <2760> for Health Events service
        RECEIVED MESSAGES <1380> for Health Events service
        SEND MESSAGES <1380> for Health Events service
        HALT REQUEST SEND COUNTER <0> for Health Events service
        STORED MESSAGES for Health service (service 0/peer 0)
        STATE <Process messages> for Health Events service
        REQUESTED FOR REMOTE <Process messages> for Health Events service
        REQUESTED FROM REMOTE <Process messages> for Health Events service

        TOTAL TRANSMITTED MESSAGES <656> for RPC service
        RECEIVED MESSAGES <328> for RPC service
        SEND MESSAGES <328> for RPC service
        HALT REQUEST SEND COUNTER <0> for RPC service
        STORED MESSAGES for RPC service (service 0/peer 0)
        STATE <Process messages> for RPC service
        REQUESTED FOR REMOTE <Process messages> for RPC service
        REQUESTED FROM REMOTE <Process messages> for RPC service

        TOTAL TRANSMITTED MESSAGES <25131> for IP(NTP) service
        RECEIVED MESSAGES <13532> for IP(NTP) service
        SEND MESSAGES <11599> for IP(NTP) service
        HALT REQUEST SEND COUNTER <0> for IP(NTP) service
        STORED MESSAGES for IP(NTP) service (service 0/peer 0)
        STATE <Process messages> for IP(NTP) service
        REQUESTED FOR REMOTE <Process messages> for IP(NTP) service
        REQUESTED FROM REMOTE <Process messages> for IP(NTP) service

        TOTAL TRANSMITTED MESSAGES <2890> for IDS Events service
        RECEIVED MESSAGES <1445> for service IDS Events service
        SEND MESSAGES <1445> for IDS Events service
        HALT REQUEST SEND COUNTER <0> for IDS Events service
        STORED MESSAGES for IDS Events service (service 0/peer 0)
        STATE <Process messages> for IDS Events service
        REQUESTED FOR REMOTE <Process messages> for IDS Events service
        REQUESTED FROM REMOTE <Process messages> for IDS Events service

        TOTAL TRANSMITTED MESSAGES <4> for Malware Lookup Service service
        RECEIVED MESSAGES <1> for Malware Lookup Service) service
        SEND MESSAGES <3> for Malware Lookup Service service
        HALT REQUEST SEND COUNTER <0> for Malware Lookup Service service
        STORED MESSAGES for Malware Lookup Service service (service 0/peer 0)
        STATE <Process messages> for Malware Lookup Service service
        REQUESTED FOR REMOTE <Process messages> for Malware Lookup Service) service
```

```
        REQUESTED FROM REMOTE <Process messages> for Malware Lookup Service service

        TOTAL TRANSMITTED MESSAGES <372> for CSM_CCM service
        RECEIVED MESSAGES <186> for CSM_CCM service
        SEND MESSAGES <186> for CSM_CCM service
        HALT REQUEST SEND COUNTER <0> for CSM_CCM service
        STORED MESSAGES for CSM_CCM (service 0/peer 0)
        STATE <Process messages> for CSM_CCM service
        REQUESTED FOR REMOTE <Process messages> for CSM_CCM service
        REQUESTED FROM REMOTE <Process messages> for CSM_CCM service

        TOTAL TRANSMITTED MESSAGES <2907> for EStreamer Events service
        RECEIVED MESSAGES <1453> for service EStreamer Events service
        SEND MESSAGES <1454> for EStreamer Events service
        HALT REQUEST SEND COUNTER <0> for EStreamer Events service
        STORED MESSAGES for EStreamer Events service (service 0/peer 0)
        STATE <Process messages> for EStreamer Events service
        REQUESTED FOR REMOTE <Process messages> for EStreamer Events service
        REQUESTED FROM REMOTE <Process messages> for EStreamer Events service

        Priority UE Channel 1 service

        TOTAL TRANSMITTED MESSAGES <2930> for UE Channel service
        RECEIVED MESSAGES <11> for UE Channel service
        SEND MESSAGES <2919> for UE Channel service
        HALT REQUEST SEND COUNTER <0> for UE Channel service
        STORED MESSAGES for UE Channel service (service 0/peer 0)
        STATE <Process messages> for UE Channel service
        REQUESTED FOR REMOTE <Process messages> for UE Channel service
        REQUESTED FROM REMOTE <Process messages> for UE Channel service

        Priority UE Channel 0 service

        TOTAL TRANSMITTED MESSAGES <2942> for UE Channel service
        RECEIVED MESSAGES <11> for UE Channel service
        SEND MESSAGES <2931> for UE Channel service
        HALT REQUEST SEND COUNTER <0> for UE Channel service
        STORED MESSAGES for UE Channel service (service 0/peer 0)
        STATE <Process messages> for UE Channel service
        REQUESTED FOR REMOTE <Process messages> for UE Channel service
        REQUESTED FROM REMOTE <Process messages> for UE Channel service

        TOTAL TRANSMITTED MESSAGES <29286> for FSTREAM service
        RECEIVED MESSAGES <14648> for FSTREAM service
        SEND MESSAGES <14638> for FSTREAM service

        Heartbeat Send Time:     Wed Oct 12 21:58:31 2016
        Heartbeat Received Time: Wed Oct 12 21:59:48 2016

**********************

**RPC STATUS****10.83.57.41*************
  'ip' => '10.83.57.41',
  'uuid' => 'c03cb3c2-8fe2-11e6-bce8-8c278d49b0dd',
  'ipv6' => '2001:420:2710:2556:1:0:0:41',
  'name' => '10.83.57.41',
  'active' => '1',
  'uuid_gw' => '',
  'last_changed' => 'Tue Oct 11 19:32:20 2016'

Check routes:
```

関連コマンド

| Command | 説明 |
| --- | --- |
| **configure manager add** | リモートマネージャである Management Center を追加します。 |

# sftunnel-status-brief

デバイスと管理側 Management Center の間の接続（トンネル）の簡単なステータスを表示するには、**sftunnel-status-brief** コマンドを使用します。

**sftunnel-status-brief**

## 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。 |

## 使用上のガイドライン

管理接続のステータスを表示するには、**sftunnel-status-brief** コマンドを入力します。**sftunnel-status** を使用して、より完全な情報を表示することもできます。

### 例

ダウン状態の接続の出力例を次に示します。ピアチャネルの「接続先」情報やハートビート情報が表示されていません。

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

アップ状態の接続の出力例を次に示します。ピアチャネルとハートビート情報が表示されています。

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **sftunnel-status** | 管理トンネルステータスの詳細表示を表示します。 |

# show aaa-server

AAA サーバーの統計情報を表示するには、**show aaa-server** コマンドを使用します。

**show aaa-server** ［ **LOCAL** | *groupname* ［**host** *hostname*］ | **protocol** *protocol*］

## 構文の説明

| | |
|---|---|
| *groupname* | （オプション）グループ内のサーバーの統計情報を表示します。 |
| **host** *hostname* | （オプション）グループ内の特定のサーバーの統計情報を表示します。 |
| **LOCAL** | （オプション）ローカルユーザーデータベースの統計情報を表示します。 |
| **protocol** *protocol* | （オプション）指定したプロトコル（**ldap** または **radius**）のサーバーの統計情報を表示します。 |

## コマンド デフォルト

デフォルトで、すべての AAA サーバー統計情報が表示されます。

## 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

次の表に、**show aaa-server** コマンド出力のフィールドの説明を示します。

| フィールド | 説明 |
|---|---|
| Server Group | サーバーグループ名。 |
| Server Protocol | サーバーグループのサーバープロトコル。 |
| Server Address | AAA サーバーの IP アドレス。 |
| Server port | システムおよび AAA サーバーによって使用される通信ポート。 |

| フィールド | 説明 |
|---|---|
| Server status | サーバーのステータス。ステータスの後に「(admin initiated)」と表示されている場合、このサーバーは、**aaa-server active** または **aaa-server fail** コマンドを使用して手動で障害発生状態にされたか、または再アクティブ化されています。値は次のとおりです。<br>• ACTIVE：システムはこの AAA サーバーと通信します。<br>• FAILED：システムはこの AAA サーバーと通信できません。この状態になったサーバーは、設定されているポリシーに応じて一定期間この状態のままとなった後、再アクティブ化されます。<br>最終トランザクション日時を次のいずれかの形式で示します。<br>• `Last Transaction success at` *`time timezone date`*<br>• `Last Transaction failure at` *`time timezone date`*<br>• `Last Transaction at Unknown`（デバイスがサーバーとまだ通信していない場合） |
| Number of pending requests | 現在進行中の要求数。 |
| Average round trip time | サーバーとのトランザクションを完了するまでにかかる平均時間。 |
| Number of authentication requests | システムによって送信された認証要求数。タイムアウト後の再送信は、この値には含まれません。 |
| Number of authorization requests | 認可要求数。この値は、コマンド認可、コンピュータを通過するトラフィックの認可、トンネルグループでイネーブルにされた WebVPN および IPsec 認可機能が原因の認可要求を指します。タイムアウト後の再送信は、この値には含まれません。 |
| Number of accounting requests | アカウンティング要求数。タイムアウト後の再送信は、この値には含まれません。 |
| Number of retransmissions | 内部タイムアウト後にメッセージが再送信された回数。この値は、RADIUS サーバー（UDP）にのみ適用されます。 |
| Number of accepts | 成功した認証要求数。 |
| Number of rejects | 拒否された要求数。この値には、エラー状態、および実際にクレデンシャルが AAA サーバーから拒否された場合の両方が含まれます。 |
| Number of challenges | 最初にユーザー名とパスワードの情報を受信した後に、AAA サーバーがユーザーに対して追加の情報を要求した回数。 |
| Number of malformed responses | この値には特に意味はありません。 |

| フィールド | 説明 |
|---|---|
| Number of bad authenticators | この値は、RADIUS にのみ適用されます。<br>RADIUSパケット内の「authenticator」文字列が破損した回数（まれ）、またはシステム上の共有秘密キーが RADIUS サーバー上のものと一致しない回数。この問題を修正するには、正しいサーバー キーを入力します。 |
| タイムアウトの回数 | システムが、AAA サーバーが応答しない、または動作が不正であることを検出し、オフラインであると見なした回数。 |
| Number of unrecognized responses | 認識できない応答またはサポートしていない応答をシステムが AAA サーバーから受信した回数。たとえば、サーバーからの RADIUS パケット コードが不明なタイプ（既知の「access-accept」、「access-reject」、「access-challenge」または「accounting-response」以外のタイプ）である場合です。通常、これは、サーバーからのRADIUS応答パケットが破損していることを意味していますが、まれなケースです。 |

### 例

次に、グループ内の特定のサーバーの AAA 統計情報を表示する例を示します。

```
> show aaa-server group1 host 192.68.125.60
Server Group: group1
Server Protocol: RADIUS
Server Address: 192.68.125.60
Server port: 1645
Server status: ACTIVE. Last transaction (success) at 11:10:08 UTC Fri Aug 22
Number of pending requests 20
Average round trip time 4ms
Number of authentication requests 20
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 1
Number of accepts 16
Number of rejects 4
Number of challenges 5
Number of malformed responses 0
Number of bad authenticators 0
Number of timeouts 0
Number of unrecognized responses 0
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear aaa-server statistics** | AAA サーバー統計情報をクリアします。 |

# show access-control-config

アクセス コントロール ポリシーに関する要約情報を表示するには、**show access-control-config** コマンドを使用します。

**show access-control-config**

## 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

このコマンドを実行すると、各アクセスコントロールルールの特性を含む、アクセス コントロール ポリシーの概要が表示されます。出力には、アクセス コントロール ポリシーの名前と説明、デフォルトのアクション、セキュリティ インテリジェンス ポリシー、およびアクセスコントロールルールのセットと各アクセスコントロールルールに関する情報が表示されます。また、参照されたSSLポリシー、ネットワーク分析ポリシー、侵入ポリシー、およびファイルポリシーの名前、侵入変数セットのデータ、ロギング設定、およびポリシーレベルのパフォーマンス、前処理、一般設定などのその他の詳細設定も表示されます。

情報には、送信元と宛先のポートデータ（ICMP エントリのタイプとコードを含む）および各アクセスコントロールルールに一致した接続数（ヒット数）など、ポリシー関連の接続情報が含まれます。

情報には、URL フィルタリングのブロックアクションおよびインタラクティブ ブロック アクションに使用される HTML も表示されます。

Device Manager （ローカルマネージャ）を使用している場合、サポートされていない機能はデフォルト設定の表示になるか、または空の表示になります。Management Center を使用している場合は、マネージャを使用してこれらの設定を調整できます。CLI を使用して、この出力に表示されているルールやオプションを設定することはできません。マネージャを使用する必要があります。

### 例

次に、ローカルマネージャである Device Manager を使用して管理されるデバイスのアクセス制御の設定例を示します。

```
> show access-control-config

===============[ NGFW-Access-Policy ]===============
Description               :
=================[ Default Action ]=================
Default Action            : Block
Logging Configuration
    DC                    : Enabled
    Beginning             : Disabled
    End                   : Disabled
Rule Hits                 : 0
Variable Set              : Default-Set
```

```
===[ Security Intelligence - Network Whitelist ]====
===[ Security Intelligence - Network Blacklist ]====
Logging Configuration     : Disabled
    DC                    : Disabled

=====[ Security Intelligence - URL Whitelist ]======
=====[ Security Intelligence - URL Blacklist ]======
Logging Configuration     : Disabled
    DC                    : Disabled

=======[ Security Intelligence - DNS Policy ]=======
    Name                  : Default DNS Policy

======[ Rule Set: admin_category (Built-in) ]=======

=====[ Rule Set: standard_category (Built-in) ]=====

------------[ Rule: Inside_Inside_Rule ]------------
    Action                : Fast-path

    Source Zones          : inside_zone
    Destination Zones     : inside_zone
    Users
    URLs
    Logging Configuration
      DC                  : Enabled
      Beginning           : Enabled
      End                 : Enabled
      Files               : Disabled
    Safe Search           : No
    Rule Hits             : 0
    Variable Set          : Default-Set

-----------[ Rule: Inside_Outside_Rule ]------------
    Action                : Fast-path

    Source Zones          : inside_zone
    Destination Zones     : outside_zone
    Users
    URLs
    Logging Configuration
      DC                  : Enabled
      Beginning           : Enabled
      End                 : Enabled
      Files               : Disabled
    Safe Search           : No
    Rule Hits             : 0
    Variable Set          : Default-Set

=======[ Rule Set: root_category (Built-in) ]=======

===============[ Advanced Settings ]================
General Settings
  Maximum URL Length                  : 1024
  Interactive Block Bypass Timeout    : 600
  Do not retry URL cache miss lookup  : No
  Inspect Traffic During Apply        : Yes
Network Analysis and Intrusion Policies
  Initial Intrusion Policy            : Balanced Security and Connectivity
  Initial Variable Set                : Default-Set
  Default Network Analysis Policy     : Balanced Security and Connectivity
Files and Malware Settings
  File Type Inspect Limit             : 1460
```

```
  Cloud Lookup Timeout                : 2
  Minimum File Capture Size           : 6144
  Maximum File Capture Size           : 1048576
  Min Dynamic Analysis Size           : 15360
  Max Dynamic Analysis Size           : 2097152
  Malware Detection Limit             : 10485760
Transport/Network Layer Preprocessor Settings
  Detection Settings
    Ignore VLAN Tracking Connections  : No
  Maximum Active Responses            : No Maximum
  Minimum Response Seconds            : No Minimum
  Session Termination Log Threshold   : 1048576
Detection Enhancement Settings
  Adaptive Profile                    : Disabled
Performance Settings
  Event Queue
    Maximum Queued Events             : 5
    Disable Reassembled Content Checks: False
  Performance Statistics
    Sample time (seconds)             : 300
    Minimum number of packets         : 10000
    Summary                           : False
    Log Session/Protocol Distribution : False
  Regular Expression Limits
    Match Recursion Limit             : Default
    Match Limit                       : Default
  Rule Processing Configuration
    Logged Events                     : 5
    Maximum Queued Events             : 8
    Events Ordered By                 : Content Length
Intelligent Application Bypass Settings
    State                                        : Off
Latency-Based Performance Settings
  Packet Handling                     : Disabled

============[ HTTP Block Response HTML ]============
HTTP/1.1 403 Forbidden
Connection: close
Content-Length: 506
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<title>Access Denied</title>
<style type="text/css">body {margin:0;font-family:verdana,sans-serif;} h1 {margin:0;pa
dding:12px 25px;background-color:#343434;color:#ddd} p {margin:12px 25px;} strong {col
or:#E0042D;}</style>
</head>
<body>
<h1>Access Denied</h1>
<p>
<strong>You are attempting to access a forbidden site.</strong><br/><br/>
Consult your system administrator for details.
</p>
</body>
</html>
```

関連コマンド

| Command | 説明 |
| --- | --- |
| **show access-list** | アクセスコントロールリスト（ACL）の内容を表示します。 |

# show access-list

アクセスリストのルールおよびヒットカウンタを表示するには、**show access-list** コマンドを使用します。

**show access-list** ［ *id* ［ *ip_address* | **brief** | **numeric** ］ | **element-count** ］

## 構文の説明

| | |
|---|---|
| *id* | （任意）表示をこの 1 つのアクセスリストに制限する既存のアクセスリストの名前。 |
| *ip_address* | （任意）このアドレスを持つルールに表示を制限する送信元 IPv4 または IPv6 アドレス。 |
| **brief** | （任意）アクセスリスト ID、ヒットカウント、および最終ルールヒットのタイムスタンプをすべて 16 進形式で表示します。 |
| **numeric** | （任意）ACL 名を指定すると、ポートが名前ではなく数値で表示されます。たとえば、www ではなく 80 と表示されます。 |
| **element-count** | （任意）システムで定義されているすべてのアクセスリストのアクセス コントロール エントリの総数を表示します。 |

## 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。 |
| 6.6 | **numeric** および **element-count** キーワードが追加されました。 |
| 7.1 | オブジェクトグループの検索が有効になっている場合は、**element-count** の出力にオブジェクトグループの内訳も含まれます。 |

## 使用上のガイドライン

アクセス コントロール ポリシーの一部の要素は、拡張アクセスコントロールリスト（ACL）エントリとして構成されます。可能な場合、レイヤ 3 基準に基づいてトラフィックをブロックするアクセスコントロールルールが ACL の拒否ルールになります。信頼アクセスコントロールルールと一致する信頼 ACL ルールが表示されることもあります。

ただし、アクセスコントロールルールで検査が要求されている場合、ルールアクションがブロックの場合でも、ACL エントリは実際にトラフィックを許可します。この許可されたトラフィックは、最終的に不要なトラフィックをブロックできる Snort などの検査エンジンに渡されます。

したがって、**show access-list** に示されている低レベル ACL ルールとデバイスのアクセス コントロール ポリシー ルールの間に 1 対 1 の関係はありません。高度な ACL を使用すると、システムは早期にトラフィックのドロップや信頼の決定を下すことができるため、検査を必要としない接続をできる限り迅速に通過させたり、ドロップしたりできます。

（注） アクセス制御のルールとプレフィルタのルールのヒットカウント情報を表示することが目的の場合は、このコマンドの代わりに **show rule hits** コマンドを使用します。

ACLは、ルートマップやサービスポリシーの一致基準など、他の目的にも使用できます。標準および拡張 ACL は、これらの目的で使用されます。

1つのコマンドに複数のアクセス リスト識別子を入力することによって、一度に複数のアクセス リストを表示できます。

**brief** キーワードを指定して、アクセス リスト ヒット カウント、ID、およびタイムスタンプ情報を 16 進形式で表示できます。16 進形式で表示されるコンフィギュレーション ID は、3 列に表示され、Syslog 106023 および 106100 で使用されるものと同じ ID です。

アクセス リストが最近変更された場合、リストは出力から除外されます。この場合は、メッセージにそのことが示されます。

（注） 出力には、ACL に含まれる要素の数が表示されます。この番号は、必ずしも ACL 内のアクセス コントロール エントリ (ACE) の数と同じではありません。たとえば、アドレス範囲をもつネットワーク オブジェクトを使用する場合、システムは追加の要素を作成することがありますが、これらの追加要素は出力に含まれません。

### クラスタリングのガイドライン

クラスタリングを使用する場合、トラフィックが単一のユニットで受信された場合でも、クラスタリングのダイレクタロジックにより、その他のユニットに ACL のヒットカウントが表示される場合があります。これは予期された動作です。クライアントから直接パケットを受信しなかったユニットは、所有者要求に応じてクラスタ制御リンクを介して転送されたパケットを受信することがあるため、ユニットはパケットを受信ユニットに戻す前に ACL をチェックすることがあります。このため、トラフィックがユニットを通過しなかった場合でも ACL ヒット カウントが増分されます。

### 例

次に、**show access-list** コマンドの出力例を示します。Device Manager （ローカルまたは「オンボックス」マネージャ）を使用している場合、アクセス コントロール ポリシー用に生成された高度なアクセスリストが表示されます。注釈はシステムによって生成され、アクセス コントロールエントリ（ACE）を理解するのに役立ちます。注釈には関連ルールの名前が表示され、その後にルールから生成されたACEが表示されます。次の例では、注釈が強調表示されています。

```
> show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list NGFW_ONBOX_ACL; 50 elements; name hash: 0xf5cc3f88
access-list NGFW_ONBOX_ACL line 1 remark rule-id 268435458: ACCESS POLICY:
```

```
NGFW_Access_Policy
access-list NGFW_ONBOX_ACL line 2 remark rule-id 268435458: L5 RULE: Inside_Inside_Rule
access-list NGFW_ONBOX_ACL line 3 advanced trust ip ifc inside1_2 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x2c7f5801
access-list NGFW_ONBOX_ACL line 4 advanced trust ip ifc inside1_2 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xf170c15b
access-list NGFW_ONBOX_ACL line 5 advanced trust ip ifc inside1_2 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0xce627c77
access-list NGFW_ONBOX_ACL line 6 advanced trust ip ifc inside1_2 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0xe37dcdd2
access-list NGFW_ONBOX_ACL line 7 advanced trust ip ifc inside1_2 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x65347856
access-list NGFW_ONBOX_ACL line 8 advanced trust ip ifc inside1_2 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0x6d622775
access-list NGFW_ONBOX_ACL line 9 advanced trust ip ifc inside1_3 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0xc1579ed7
access-list NGFW_ONBOX_ACL line 10 advanced trust ip ifc inside1_3 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0x40968b8f
access-list NGFW_ONBOX_ACL line 11 advanced trust ip ifc inside1_3 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0xc5a178c1
access-list NGFW_ONBOX_ACL line 12 advanced trust ip ifc inside1_3 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0xdbc1560f
access-list NGFW_ONBOX_ACL line 13 advanced trust ip ifc inside1_3 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x3571535c
access-list NGFW_ONBOX_ACL line 14 advanced trust ip ifc inside1_3 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0xc4a66c0a
access-list NGFW_ONBOX_ACL line 15 advanced trust ip ifc inside1_4 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0x1d1a8032
access-list NGFW_ONBOX_ACL line 16 advanced trust ip ifc inside1_4 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x8f7bbcdf
access-list NGFW_ONBOX_ACL line 17 advanced trust ip ifc inside1_4 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0xe616991f
access-list NGFW_ONBOX_ACL line 18 advanced trust ip ifc inside1_4 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0x4db9d2aa
access-list NGFW_ONBOX_ACL line 19 advanced trust ip ifc inside1_4 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0xf8a88db4
access-list NGFW_ONBOX_ACL line 20 advanced trust ip ifc inside1_4 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0x1d3b5b80
access-list NGFW_ONBOX_ACL line 21 advanced trust ip ifc inside1_5 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0xf508bbd8
access-list NGFW_ONBOX_ACL line 22 advanced trust ip ifc inside1_5 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x7084f3fc
access-list NGFW_ONBOX_ACL line 23 advanced trust ip ifc inside1_5 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xd989f9aa
access-list NGFW_ONBOX_ACL line 24 advanced trust ip ifc inside1_5 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0xd5aa77f5
access-list NGFW_ONBOX_ACL line 25 advanced trust ip ifc inside1_5 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x4a7648b2
access-list NGFW_ONBOX_ACL line 26 advanced trust ip ifc inside1_5 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0x118ef4b4
access-list NGFW_ONBOX_ACL line 27 advanced trust ip ifc inside1_6 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0xa6be4e58
access-list NGFW_ONBOX_ACL line 28 advanced trust ip ifc inside1_6 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0xda17cb9e
access-list NGFW_ONBOX_ACL line 29 advanced trust ip ifc inside1_6 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xc6bfe6b7
access-list NGFW_ONBOX_ACL line 30 advanced trust ip ifc inside1_6 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0x5fe085c3
access-list NGFW_ONBOX_ACL line 31 advanced trust ip ifc inside1_6 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x4574192b
access-list NGFW_ONBOX_ACL line 32 advanced trust ip ifc inside1_6 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0x36203c1e
access-list NGFW_ONBOX_ACL line 33 advanced trust ip ifc inside1_7 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0x699725ea
```

```
access-list NGFW_ONBOX_ACL line 34 advanced trust ip ifc inside1_7 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x36a1e6a1
access-list NGFW_ONBOX_ACL line 35 advanced trust ip ifc inside1_7 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xe415bb76
access-list NGFW_ONBOX_ACL line 36 advanced trust ip ifc inside1_7 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0x18ebff70
access-list NGFW_ONBOX_ACL line 37 advanced trust ip ifc inside1_7 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0xf9bfd690
access-list NGFW_ONBOX_ACL line 38 advanced trust ip ifc inside1_7 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0xf08a88b4
access-list NGFW_ONBOX_ACL line 39 advanced trust ip ifc inside1_8 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0xd2014e58
access-list NGFW_ONBOX_ACL line 40 advanced trust ip ifc inside1_8 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x952c7254
access-list NGFW_ONBOX_ACL line 41 advanced trust ip ifc inside1_8 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xfc38a46f
access-list NGFW_ONBOX_ACL line 42 advanced trust ip ifc inside1_8 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0x3f878e23
access-list NGFW_ONBOX_ACL line 43 advanced trust ip ifc inside1_8 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0x48e852ce
access-list NGFW_ONBOX_ACL line 44 advanced trust ip ifc inside1_8 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x83c65e52
access-list NGFW_ONBOX_ACL line 45 remark rule-id 268435457: ACCESS POLICY:
NGFW_Access_Policy
access-list NGFW_ONBOX_ACL line 46 remark rule-id 268435457: L5 RULE: Inside_Outside_Rule
access-list NGFW_ONBOX_ACL line 47 advanced trust ip ifc inside1_2 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0xea5bdd6e
access-list NGFW_ONBOX_ACL line 48 advanced trust ip ifc inside1_3 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0xd7461ffc
access-list NGFW_ONBOX_ACL line 49 advanced trust ip ifc inside1_4 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0x6e13508e
access-list NGFW_ONBOX_ACL line 50 advanced trust ip ifc inside1_5 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0xfe1fcdd6
access-list NGFW_ONBOX_ACL line 51 advanced trust ip ifc inside1_6 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0xa4dba9a8
access-list NGFW_ONBOX_ACL line 52 advanced trust ip ifc inside1_7 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0x2cfd43cd
access-list NGFW_ONBOX_ACL line 53 advanced trust ip ifc inside1_8 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0xc3c3fafb
access-list NGFW_ONBOX_ACL line 54 remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy
access-list NGFW_ONBOX_ACL line 55 remark rule-id 1: L5 RULE: DefaultActionRule
access-list NGFW_ONBOX_ACL line 56 advanced deny ip any any rule-id 1 (hitcnt=0)
0x84953cae
>
```

次に、16 進形式で指定されたアクセス ポリシー（ヒット カウントがゼロではない ACE）に関する簡単な情報の例を示します。最初の 2 列には、ID が 16 進形式で表示され、3 番めの列にはヒット カウントがリストされ、4 番めの列には、タイムスタンプ値が 16 進形式で表示されます。ヒット カウントの値は、トラフィックがルールにヒットした回数を表します。タイムスタンプ値は、最終ヒットの時刻を報告します。ヒット カウントがゼロの場合、情報は表示されません。

次に、Telnet トラフィックが通過する際の **show access-list brief** コマンドの出力例を示します。

```
> show access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
7b1c1660 44ae5901 00000001 4a68ab51
```

次に、SSH トラフィックが通過する際の **show access-list brief** コマンドの出力例を示します。

```
> show access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
7b1c1660 44ae5901 00000001 4a68ab51
3666f922 44ae5901 00000001 4a68ab66
```

次に、システムで定義されているすべてのアクセスリストのアクセスコントロールエントリの総数である要素カウントの例を示します。アクセスグループとして割り当てられているアクセスリストの場合、アクセスをグローバルに、またはインターフェイス上で制御するために、（実行コンフィギュレーションの **object-group-search access-control** コマンドで表される）オブジェクトグループ検索を有効にすることで要素カウントを減らすことができます。オブジェクトグループ検索をイネーブルにすると、ネットワークオブジェクトがアクセスコントロールエントリで使用されます。それ以外の場合、オブジェクトはそのオブジェクトに含まれる個々の IP アドレスに展開され、送信元/宛先アドレスのペアごとに個別のエントリが書き込まれます。したがって、5 つの IP アドレスを持つ送信元ネットワークオブジェクトと 6 つのアドレスを持つ宛先オブジェクトを使用する単一のルールは、1 つではなく 30 の要素（5 x 6 エントリ）に展開されます。要素カウントが多いほど、アクセスリストが大きくなり、パフォーマンスに影響を与える可能性が高くなります。

```
> show access-list element-count
Total number of access-list elements: 33934
```

7.1 以降では、オブジェクトグループ検索を有効にしている場合、ルールに含まれるオブジェクトグループの数（OBJGRP）、送信元オブジェクト（SRC OBJ）と宛先オブジェクト（DST OBJ）の数、および追加されたグループと削除されたグループの数に関する追加情報が提供されます。

```
> show access-list element-count
Total number of access-list elements: 892

OBJGRP      SRC OG      DST OG      ADD OG      DEL OG
842         842         842         842         0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear access-list** | アクセス リスト カウンタをクリアします。 |
| **show running-config access-list** | 現在実行しているアクセス リスト コンフィギュレーションを表示します。 |

# show alarm settings

ISA 3000 で各タイプのアラームの構成を表示するには、**show alarm settings** コマンドを使用します。

**show alarm settings**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

### 例

次に、**show alarm settings** コマンドの出力例を示します。

```
> show alarm settings

Power Supply
         Alarm                   Disabled
         Relay                   Disabled
         Notifies                Disabled
         Syslog                  Disabled
Temperature-Primary
         Alarm                   Enabled
         Thresholds              MAX: 92C                MIN: -40C
         Relay                   Enabled
         Notifies                Enabled
         Syslog                  Enabled
Temperature-Secondary
         Alarm                   Disabled
         Threshold
         Relay                   Disabled
         Notifies                Disabled
         Syslog                  Disabled
Input-Alarm 1
         Alarm                   Enabled
         Relay                   Disabled
         Notifies                Disabled
         Syslog                  Enabled
Input-Alarm 2
         Alarm                   Enabled
         Relay                   Disabled
         Notifies                Disabled
         Syslog                  Enabled
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear facility-alarm output** | 出力リレーの電源を切り、LED のアラーム状態をクリアします。 |
| **show environment alarm-contact** | 入力アラーム コンタクトのステータスを表示します。 |

| Command | 説明 |
| --- | --- |
| **show facility-alarm** | トリガーされたアラームのステータス情報を表示します。 |

# show allocate-core

CPU コアの割り当て方法に関する情報を表示するには、**show allocate-core** コマンドを使用します。

**show allocate-core** { **lina-cpu-percentage** | **lina-mem-percentage** | **profile state** }

## 構文の説明

| | |
|---|---|
| **lina-cpu-percentage** | Lina プロセスに割り当てられた CPU コアの割合を示します。残りのコアは Snort プロセスに割り当てられます。 |
| **lina-mem-percentage** | Lina プロセスに割り当てられたシステムメモリの割合を示します。残りのメモリは Snort プロセスに割り当てられます。 |
| **profile** | デバイスで現在動作しているコア割り当てプロファイルを表示します。 |
| **state** | コア割り当てプロセスが有効になっているか無効になっているかを示します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.3 | このコマンドが追加されました。 |

## 使用上のガイドライン

管理ソフトウェアから CPU コア割り当てプロファイルを割り当てることができます。このコマンドを使用して、デバイスで実行されているプロファイルを表示および確認します。可能なプロファイルは次のとおりです。

- default：Lina プロセスと Snort プロセスのコア割り当てのデフォルトスキーム。正確な割り当ては、ハードウェアプラットフォームによって異なります。他のオプションを使用して、割合を決定します。
- ips-heavy：IPS の負荷が高いユースケース用に、より多くの CPU を Snort に割り当てます。30% を Lina、70% を Snort に割り当てます。
- vpn-heavy-prefilter-fastpath：VPN トラフィックを高速パスするプレフィルタポリシーも設定するときに、VPN 負荷の高いユースケース用により多くの CPU を Lina に割り当てます。90% を Lina、10% を Snort に割り当てます。
- vpn-heavy-with-inspection：VPN トラフィックを高速パス処理するプレフィルタポリシーを設定せず、その代わりにアクセス コントロール ポリシーでトラフィックを検査する場合、VPN の多いユースケース用により多くの CPU を Lina に割り当てます。60% を Lina、40% を Snort に割り当てます。

### 例

次に、Lina CPU とメモリの割合、プロファイル、およびコア割り当ての状態を表示する例を示します。

```
> show allocate-core lina-cpu-percentage

Lina CPU percentage is set to : 48
> show allocate-core lina-mem-percentage

Lina memory percentage is set to : 50
> show allocate-core profile

Core allocation profile is set to : default
> show allocate-core state
Core allocation is disabled
```

# show app-agent heartbeat

アプリケーション エージェントのステータスを表示するには、**show app-agent heartbeat** コマンドを使用します。

**show app-agent heartbeat**

## 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

アプリケーションエージェントのハートビート通信チャネルは、FXOS シャーシのスーパーバイザと 脅威に対する防御 のアプリケーション エージェント間のリンクの正常性をモニタリングする目的で使用されます。これは、Firepower 4100 または 9300 シリーズ デバイスでハードウェアバイパスを設定する場合に使用されます。脅威に対する防御 ソフトウェアを実行する他のデバイスモデルでは使用されません。

**show app-agent heartbeat** コマンドを使用して、アプリケーション エージェントのハートビート通信チャネルのステータスを表示します。

### 例

次に、アプリケーション エージェントのハートビートステータスの例を示します。

```
> show app-agent heartbeat
appagent heartbeat timer 1 retry-count 3
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **app-agent** | アプリケーション エージェントをハードウェアバイパス用に設定します。 |

# show arp

ARP テーブルを表示するには、**show arp** コマンドを使用します。

**show arp**

## 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

表示出力には、ダイナミック、スタティック、およびプロキシARPエントリが表示されます。ダイナミックARPエントリには、ARPエントリの秒単位のエージングが含まれています。エージングの代わりに、スタティックARPエントリにはダッシュ（-）が、プロキシARPエントリには「alias」という状態が含まれています。

ARPテーブルには、システム通信に使用されるnlp_int_tapなどの内部インターフェイスのエントリを含めることができます。

### 例

次に、**show arp** コマンドの出力例を示します。1 つめのエントリは、2 秒間エージングされているダイナミック エントリです。2 つめのエントリはスタティック エントリ、3 つめのエントリはプロキシ ARP のエントリです。

```
> show arp
        outside 10.86.194.61 0011.2094.1d2b 2
        outside 10.86.194.1 001a.300c.8000 -
        outside 10.86.195.2 00d0.02a8.440a alias
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear arp statistics** | ARP 統計情報をクリアします。 |
| **show arp statistics** | ARP 統計情報を表示します。 |
| **show running-config all arp** | ARP タイムアウトの現在のコンフィギュレーションを表示します。 |

# show arp-inspection

各インターフェイスの ARP インスペクション設定を表示するには、**show arp-inspection** コマンドを使用します。

**show arp-inspection**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.1 | このコマンドが追加されました。 |
| 6.2 | ルーテッド モードのサポートが追加されました。 |

### 例

次に、**show arp-inspection** コマンドの出力例を示します。

```
> show arp-inspection
interface                arp-inspection         miss
-------------------------------------------------------
inside1                  enabled                flood
outside                  disabled                -
```

miss 列には、ARP インスペクションがイネーブルの場合に一致しないパケットに対して実行するデフォルトのアクション（「flood」または「no-flood」）が表示されます。

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear arp statistics** | ARP 統計情報をクリアします。 |
| **show arp statistics** | ARP 統計情報を表示します。 |
| **show running-config all arp** | ARP タイムアウトの現在のコンフィギュレーションを表示します。 |

# show arp statistics

ARP 統計情報を表示するには、**show arp statistics** コマンドを使用します。

**show arp statistics**

## 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、**show arp statistics** コマンドの出力例を示します。

```
> show arp statistics
        Number of ARP entries:
        ASA : 6
        Dropped blocks in ARP: 6
        Maximum Queued blocks: 3
        Queued blocks: 1
        Interface collision ARPs Received: 5
        ARP-defense Gratuitous ARPS sent: 4
        Total ARP retries: 15
        Unresolved hosts: 1
        Maximum Unresolved hosts: 2
```

次の表で各フィールドについて説明します。

表 *2 : show arp statistics* のフィールド（続き）

| フィールド | 説明 |
|---|---|
| Number of ARP entries | ARP テーブル エントリの合計数。 |
| Dropped blocks in ARP | IP アドレスが対応するハードウェア アドレスに解決されている間にドロップされたブロック数。 |
| Maximum queued blocks | IP アドレスの解決を待機している間に ARP モジュールにキューイングされた最大ブロック数。 |
| Queued blocks | 現在 ARP モジュールにキューイングされているブロック数。 |
| Interface collision ARPs received | すべてのインターフェイスで受信された、インターフェイスの IP アドレスと同じ IP アドレスから送信された ARP パケット数。 |
| ARP-defense gratuitous ARPs sent | ARP-Defense メカニズムの一環としてデバイスによって送信された Gratuitous ARP の数。 |

| フィールド | 説明 |
|---|---|
| Total ARP retries | 最初の ARP 要求への応答でアドレスが解決されなかった場合に ARP モジュールによって送信される ARP 要求の合計数。 |
| Unresolved hosts | 現在も ARP モジュールによって ARP 要求が送信されている未解決のホスト数。 |
| Maximum unresolved hosts | 最後のクリア後、またはデバイスの起動後に、ARP モジュールに存在した未解決ホストの最大数。 |

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear arp statistics** | ARP 統計情報をクリアします。 |
| **show arp** | ARP テーブルを表示します。 |
| **show running-config all arp** | ARP タイムアウトの現在のコンフィギュレーションを表示します。 |

# show as-path-access-list

現在のすべての自律システム（AS）パスアクセスリストの内容を表示するには、**show as-path-access-list** コマンドを使用します。

**show as-path-access-list** ［*number*］

## 構文の説明

| | |
|---|---|
| *number* | （オプション）AS パスアクセスリスト番号を指定します。有効な値は、1 ～ 500 です。 |

## コマンド デフォルト

*number* 引数を指定しない場合、コマンド出力には、すべての AS パスアクセスリストの内容が表示されます。

## 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、**show as-path-access-list** コマンドの出力例を示します。

```
> show as-path-access-list
 AS path access list 1

 AS path access list 2
```

# show asp cluster counter

クラスタリング環境のグローバル情報またはコンテキストに固有の情報をデバッグするには、**show asp cluster counter** コマンドを使用します。

**show asp cluster counter**

## 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

**show asp cluster counter** コマンドは、グローバル DP カウンタおよびコンテキストに固有の DP カウンタを表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。この情報はデバッグの目的でのみ使用されます。また、情報の出力は変更される可能性があります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

### 例

次に、**show asp cluster counter** コマンドの出力例を示します。

```
> show asp cluster counter
Global dp-counters:
Context specific dp-counters:
MCAST_FP_TO_SP                  361136
MCAST_SP_TOTAL                  361136
MCAST_SP_PKTS                   143327
MCAST_SP_PKTS_TO_CP             143327
MCAST_FP_CHK_FAIL_NO_HANDLE     217809
MCAST_FP_CHK_FAIL_NO_ACCEPT_IFC 81192
MCAST_FP_CHK_FAIL_NO_FP_FWD     62135
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show asp drop** | ドロップされたパケットの高速セキュリティ パス カウンタを示します。 |

# show asp dispatch

パフォーマンス問題の診断に役立つ、デバイスのロードバランス ASP ディスパッチャの統計情報を表示するには、**show asp dispatch** コマンドを使用します。このコマンドは、ハイブリッドポーリング/割り込みモードの Threat Defense Virtual デバイスでのみ使用できます。

**show asp dispatch**

## 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、**show asp dispatch** コマンドの出力例を示します。

```
> show asp dispatch
==== Lina DP thread dispatch stats - CORE 0 ====
Dispatch loop count        :          92260212
Dispatch C2C poll count    :                 2
CP scheduler busy          :          14936242
CP scheduler idle          :          77323971
RX ring busy               :           1513632
Async lock global q busy   :            809481
Global timer q busy        :           1958684
SNP flow bulk sync busy    :               174
Purg process busy          :              2838
Block attempts             :          44594355
Maximum timeout specified  :          10000000
Minimum timeout specified  :           1572864
Average timeout specified  :           9999994
Waken up with OK status    :           2476791
Waken up with timeout      :          42117564
Sleep interrupted          :             85753
Number of interrupts       :           2492566
Number of RX interrupts    :           1454442
Number of TX interrupts    :           2492566
Enable interrupt ok        :         174566236
Disable interrupt ok       :         174231423
Maximum elapsed time       :          54082257
Minimum elapsed time       :              6165
Average elapsed time       :           9658532
Message pipe stats         :

Last clearing of asp dispatch: Never

==== Lina DP thread home-ring/interface list - CORE 0 ====
Interface Internal-Data0/0: port-id 0 irq 10 fd 37
Interface GigabitEthernet0/0: port-id 256 irq 5 fd 38
Interface GigabitEthernet0/1: port-id 512 irq 9 fd 39
Interface GigabitEthernet0/2: port-id 768 irq 11 fd 40
>
```

# show asp drop

高速セキュリティパスでドロップされたパケットまたは接続をデバッグするには、**show asp drop** コマンドを使用します。

**show asp drop** ［**flow** ［*flow_drop_reason*］ | **frame** ［*frame_drop_reason*］］

## 構文の説明

| | |
|---|---|
| **flow** [*flow_drop_reason*] | （任意）ドロップされたフロー（接続）を表示します。必要に応じて、特定の理由を指定できます。考えられるフローのドロップ理由のリストを表示するには、? を使用します。 |
| **frame** [*frame_drop_reason*] | （任意）ドロップされたパケットを表示します。必要に応じて、特定の理由を指定できます。考えられるフレームのドロップ理由のリストを表示するには、? 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

**show asp drop** コマンドは、高速セキュリティパスによってドロップされたパケットまたは接続を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。この情報はデバッグの目的でのみ使用されます。また、情報の出力は変更される可能性があります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

考えられるドロップの理由については、
https://www.cisco.com/c/ja_jp/td/docs/security/asa/asa-command-reference/show_asp_drop/show_asp_drop.html
にある『show asp drop コマンドの使用方法』を参照してください。

### 例

次に、**show asp drop** コマンドの出力例を示します。タイムスタンプは、カウンタが最後にクリアされた時間を示しています。

```
> show asp drop

Frame drop:
  Flow is denied by configured rule (acl-drop)                          3
  Dst MAC L2 Lookup Failed (dst-l2_lookup-fail)                      4110
  L2 Src/Dst same LAN port (l2_same-lan-port)                         760
  Expired flow (flow-expired)                                           1

Last clearing: Never

Flow drop:
  Flow is denied by access rule (acl-drop)                             24
  NAT failed (nat-failed)                                           28739
  NAT reverse path failed (nat-rpf-failed)                          22266
  Inspection failure (inspect-fail)                                 19433
```

```
Last clearing: 17:02:12 UTC Jan 17 2012 by enable_15
```

# show asp event

データパスまたは制御パスのイベントキューをデバッグするには、**show asp event** コマンドを使用します。

**show asp event {dp-cp | cp-dp}**

## 構文の説明

| | |
|---|---|
| **dp-cp** | ASPデータパスからコントロールプレーンに送信されたイベントを表示します。 |
| **cp-dp** | コントロールプレーンから ASP データパスに送信されたイベントを表示します。 |

## 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

**show asp event** コマンドは、データパスおよび制御パスの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステムデバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

### 例

次に、**show asp event dp-cp** コマンドの出力例を示します。

```
> show asp event dp-cp
DP-CP EVENT QUEUE                    QUEUE-LEN  HIGH-WATER
Punt Event Queue                             0           0
Routing Event Queue                          0           0
Identity-Traffic Event Queue                 0           1
PTP-Traffic Event Queue                      0           0
General Event Queue                          0           0
Syslog Event Queue                           0           0
Non-Blocking Event Queue                     0           8
Midpath High Event Queue                     0           0
Midpath Norm Event Queue                     0           0
Crypto Event Queue                           0         146
HA Event Queue                               0           0
Threat-Detection Event Queue                 0           0
SCP Event Queue                              0           0
ARP Event Queue                              0           1
IDFW Event Queue                             0           0
CXSC Event Queue                             0           0
BFD Event Queue                              0           0

EVENT-TYPE          ALLOC ALLOC-FAIL ENQUEUED ENQ-FAIL  RETIRED 15SEC-RATE
crypto-msg            810          0      810        0      810          0
arp-in              17288          0    17288        0    17288          0
identity-traffic        2          0        2        0        2          0
scheduler             239          0      239        0      239          0
```

# show asp inspect-dp ack-passthrough

Snort インスペクションをバイパスする空の ACK パケットに関連する統計を表示するには、**show asp inspect-dp ack-passthrough** コマンドを使用します。

**show asp inspect-dp ack-passthrough**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | このコマンドが導入されました。 |

## 使用上のガイドライン

これらの統計をリセットするには、**clear asp inspect-dp ack-passthrough** コマンドを使用します。

### 例

次に出力例を示します。情報には、ACK パススルーが有効かどうかと次の統計が含まれます。

- バイパスされた ACK パケット：検査のために Snort へ転送されなかった空の ACK パケットの数。
- 送信されたメタ ACK：Snort に送信された後続のデータパケットにピギーバックされた空の ACK の数。同じ方向の後続のデータパケットがより高いシーケンス番号の ACK を持っている場合、以前に保存された空の ACK 情報は必要なく、含まれていないため、この数はバイパスされたパケットの数よりも少ないことがあります。

```
> show asp inspect-dp ack-passthrough

Current running state: Enabled

Packet Statistics:
 ACK packets bypassed                    506
 Meta ACK sent                           506
>
```

# show asp inspect-dp egress-optimization

出力最適化（パフォーマンスを向上させる機能）に関する統計情報を表示します。このコマンドは、Cisco TAC のアドバイスに従って使用します。

**show asp inspect-dp egress optimization**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.4 | このコマンドが導入されました。 |

## 使用上のガイドライン

**show asp inspect-dp egress-optimization** コマンドは、出力最適化（パフォーマンスを向上させる機能）の対象となる接続についての情報を表示します。出力には、次の情報が表示されます。

- [Current running state]：出力最適化が有効か無効か。
- フロー（フローは 1 つ以上のパケットで構成されます）：
  - [Current]：現在出力最適化の対象となっているフローの数。
  - [Maximum]：検査エンジンが最後に再起動された後、または出力最適化統計情報がクリアされてからの、出力最適化の対象となるフローの合計数。
- パケット：
  - [Processed]：処理されたパケットの合計数。
  - [Excepted]：最初は出力最適化の対象と判断されたが、その後に出力最適化の対象外と判断されたパケットの数。

### 例

次に、**show asp inspect-dp egress-optimization** コマンドの出力例を示します。

```
> show asp inspect-dp egress-optimization
Current running state: Enabled
Flow:
  current: 1, maximum: 3
  snort-unreachable: 0, snort-unsupported-header: 1, snort-unsupported-verdict: 2
Packet:
  processed: 5
  excepted: 0
```

関連コマンド

| コマンド | 説明 |
| --- | --- |
| **clear asp inspect-dp egress-optimization** | 出力最適化の統計情報をクリアします。 |
| **show conn state egress_optimization** | 出力最適化の対象となるフローに関する情報を表示します。このコマンドは、Cisco TAC のアドバイスに従って使用します。 |

# show asp inspect-dp snapshot

PDTS（Snort へのデータプレーン送信/受信キュー）リングのスナップショットを表示するには、**show asp inspect-dp snapshot** コマンドを使用します。

**show asp inspect-dp snapshot** {**config** | **instance** *instance_id* **queue** *queue_id*}

## 構文の説明

| | |
|---|---|
| **config** | PDTS スナップショットのグローバル コンフィギュレーションを表示します。 |
| **instance** *instance_id* | 指定した PDTS コンシューマインスタンス ID のスナップショットを表示します。値は 0 ～ 2147483647 です。 |
| **queue** *queue_id* | PDTS リングの指定されたデータパス送信キュー ID のスナップショットを表示します。値は 0 ～ 2147483647 です。 |

## 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

**show asp inspect-dp snapshot** コマンドは、PDTS リングスナップショット機能のグローバル コンフィギュレーションを表示します。出力には、次の情報が表示されます。

- Max snapshots：許可される自動スナップショットの最大数。
- Current in use：これまでに保存されたスナップショットの数。
- Interval：同じ PDTS リングで 2 つのスナップショットが許可される期間を指定する時間間隔。
- Auto Snapshot：自動 PDTS スナップショット機能が有効か無効かを表示します。

### 例

次に、**show asp inspect-dp snapshot config** コマンドの出力例を示します。

```
> show asp inspect-dp snapshot config
Max snapshots  Current in use  Interval (min)  Auto Snapshot
-------------  --------------  --------------  -------------
2              0               5               OFF
```

次に、**show asp inspect-dp snapshot instance** コマンドの出力例を示します。

```
> show asp inspect-dp snapshot instance 2 queue 1
0 packet captured
0 packet shown
```

# show asp inspect-dp snort

すべての Snort インスタンスのステータスを表示するには、**show asp inspect-dp snort** コマンドを使用します。

**show asp inspect-dp snort [instance** *instance_id***]**

## 構文の説明

| | |
|---|---|
| **instance** *instance_id* | 特定の Snort インスタンスのステータスを表示します。値は 0 ～ 2147483647 です。 |

## 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

このコマンドは、すべての Snort インスタンスのステータスを表示します。出力には、次の情報が表示されます。

- Id：Snort インスタンス ID。
- Pid：Snort インスタンスプロセス ID。
- Cpu-Usage：Snort インスタンス ID の CPU 使用状況。合計およびユーザー/システム別に出力されます。**注**：このフィールドは、Firepower 2100 シリーズでは表示されません。
- Conns：現在 Snort インスタンスが保持している接続の数。
- Segs/Pkts：Snort インスタンスによって現在処理されているセグメントまたはパケットの数。
- Status：Snort インスタンスのステータス。

### 例

次に、**show asp inspect-dp snort** コマンドの出力例を示します。

```
> show asp inspect-dp snort

SNORT Inspect Instance Status Info

Id Pid       Cpu-Usage    Conns      Segs/Pkts  Status
           tot (usr | sys)
-- ----- ---------------- ---------- ---------- ----------
0  9188    0% (  0%|  0%)   0          0        READY
1  9187    0% (  0%|  0%)   0          0        READY
2  9186    0% (  0%|  0%)   0          0        READY
```

次に、Firepower 2010 での **show asp inspect-dp snort** コマンドの出力例を示します。

```
> show asp inspect-dp snort

SNORT Inspect Instance Status Info

Id Pid   Conns      Segs/Pkts  Status
-- ----- ---------- ---------- ----------
0  30080  40           0        READY
1  30081  14           0        READY
2  30079  20           0        READY
```

# show asp inspect-dp snort counters

Snort インスタンスの PDTS 関連 raw カウンタを表示するには、**show asp inspect-dp snort counters** コマンドを使用します。

**show asp inspect-dp snort counters [instance** *instance_id***] [queues] [rate] [debug] [zeros]**

## 構文の説明

| | |
|---|---|
| **instance** *instance_id* | 特定の Snort インスタンスのカウンタを表示します。値は 0 ～ 2147483647 です。 |
| **queues** | キュー情報を詳細に表示します。インスタンスの各プロデューサキューは個別に表示されます。インスタンスのキュー情報は集約されません。 |
| **rate** | カウンタのスナップショットを 5 秒間取得して 1 秒に平均化し、カウンタの変化率を示します。 |
| **debug** | 他の方法では表示されない特定のデバッグカウンタが表示されます。 |
| **zeros** | ゼロカウンタを含むすべてのカウンタが表示されます。 |

## コマンド デフォルト

インスタンスを指定しない場合は、すべてのインスタンスが表示されます。

## 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

このコマンドは、Snort インスタンスの PDTS 関連 raw カウンタを表示します。出力には、次の情報が表示されます。

- Id：Snort インスタンス ID。「All」は集約されたすべての Snort インスタンスを意味します。
- QId：Lina 送信キュー ID。これは Lina スレッドの数に対応します。「All」はすべてのキューが集約されることを意味します。
- Type：カウンタのタイプ。データカウンタ、エラーカウンタ、デバッグカウンタなど。
- Name：カウンタの名前。
- Value：カウンタの判読可能な値。
- Raw-Value：カウンタの raw 値。

カウンタ名：

- Tx Bytes：Lina が Snort インスタンスに送信したバイト数。
- Tx Segs：Lina が Snort インスタンスに送信したフレーム/セグメントの数。

- Rx Bytes：Lina が Snort インスタンスから受信したバイト数。
- Rx Segs：Lina が Snort インスタンスから受信したフレーム/セグメントの数。
- NewConns：Snort インスタンスに送信された接続の数。
- RxQ-Wakeup
- TxQ-Wakeup
- TxQ-LB-Dynamic：PDTS ダイナミック ロード バランシングが開始された回数。
- TxQ-Data-Hi-Thresh：Lina の送信キューの上限しきい値に達した回数。
- RxQ-Full：Lina の受信キューがいっぱいになった回数。
- TxQ-Full：Lina の送信キューがいっぱいになった回数。
- TxQ-Data-Limit：Lina の送信キューのデータ制限に達した回数。
- TxQ-LB-Failed：PDTS ダイナミック ロード バランシングに失敗した回数。
- TxQ-Unavail：Lina の送信キューが使用できなかった回数。
- TxQ-Not-Ready：Lina の送信キューの準備ができていなかった回数。
- TxQ-Suspended：Lina の送信キューが中断された回数。
- RxQ-Unavail：Lina の受信キューが使用できなかった回数。
- RxQ-Not-Ready：Lina の受信キューの準備ができていなかった回数。
- RxQ-Suspended：Lina の受信キューが中断された回数。

### 例

次に、**show asp inspect-dp snort counters** コマンドの出力例を示します。

```
> show asp inspect-dp snort counters summary instance 5 debug zeros
SNORT Inspect Instance Counters
Id   QId    Type    Name                              Value      Raw-Value
--   ----   ----    ----                              ---------  ----------
5    All    data    Tx Bytes                           3.3 GB   (3549197468)
5    All    data    Tx Segs                            4.7 M    (4671722)
5    All    data    Rx Bytes                           3.3 GB   (3495936190)
5    All    data    Rx Segs                            4.7 M    (4677344)
5    All    data    NewConns                           11.1 K   (11103)
5    All    debug   RxQ-Wakeup                         0        (0)
5    All    debug   TxQ-Wakeup                         4.7 M    (4655982)
5    All    warn    TxQ-LB-Dynamic                     0        (0)
5    All    warn    TxQ-Data-Hi-Thresh                 0        (0)
5    All    drop    RxQ-Full                           0        (0)
5    All    drop    TxQ-Full                           0        (0)
5    All    drop    TxQ-Data-Limit                     0        (0)
5    All    drop    TxQ-LB-Failed                      0        (0)
5    All    err     TxQ-Unavail                        0        (0)
5    All    err     TxQ-Not-Ready                      0        (0)
5    All    err     TxQ-Suspended                      0        (0)
```

```
5    All    err     RxQ-Unavail                    0        (0)
5    All    err     RxQ-Not-Ready                  0        (0)
5    All    err     RxQ-Suspended                  0        (0)
```

# show asp inspect-dp snort counters summary

Snort インスタンスの PDTS 関連カウンタを表示するには、**show asp inspect-dp snort counters summary** コマンドを使用します。カウンタは各インスタンスに集約されます。

**show asp inspect-dp snort counters summary [instance** *instance_id***] [queues] [rate]**

## 構文の説明

| | |
|---|---|
| **instance** *instance_id* | 特定の Snort インスタンスのカウンタを表示します。値は 0 ～ 2147483647 です。 |
| **queues** | キュー情報を詳細に表示します。インスタンスの各プロデューサキューは個別に表示されます。インスタンスのキュー情報は集約されません。 |
| **rate** | カウンタの 1 秒間の平均増加数を表示します。現在、1 秒間の平均は、コマンドの最後の呼び出しと現在の呼び出しの間の差分増加に基づいています。これは、差分増加が 1 秒間に 1 回サンプリングされた 5 秒間の移動平均に基づくように変更されます。 |

## コマンド デフォルト

インスタンスを指定しない場合は、すべてのインスタンスが表示されます。

## 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

このコマンドは、Snort インスタンスの PDTS 関連カウンタを表示します。出力には、次の情報が表示されます。

- Id：Snort インスタンス ID。「All」は集約されたすべての Snort インスタンスを意味します。
- QId：Lina 送信キュー ID。これは Lina スレッドの数に対応します。「All」はすべてのキューが集約されることを意味します。
- TxBytes：Lina が Snort インスタンスに送信した合計バイト数。
- TxFrames：Lina が Snort インスタンスに送信したフレーム/セグメントの合計数。
- RxBytes：Lina が Snort インスタンスから受信した合計バイト数。
- RxFrames：Lina が Snort インスタンスから受信したフレーム/セグメントの合計数。
- Conns：Snort インスタンスによって処理された接続の合計数。

### 例

次に、**show asp inspect-dp snort counters summary** コマンドの出力例を示します。

```
> show asp inspect-dp snort counters summary instance 2
SNORT Inspect Instance Counter Summary
Id   QId  TxBytes    TxFrames   RxBytes    RxFrames   Conns
--   ---- ---------- ---------- ---------- ---------- -----
2    All    0          0          0          0          0
```

# show asp inspect-dp snort queues

すべてのキューを同じインスタンスに集約するすべての Snort インスタンス（プロセス）のキュー情報を表示するには、**show asp inspect-dp snort queues** コマンドを使用します。

**show asp inspect-dp snort queues [instance** *instance_id***] [detail] [debug]**

## 構文の説明

| | |
|---|---|
| **instance** *instance_id* | 特定の Snort インスタンスのキューを表示します。値は 0 ～ 2147483647 です。 |
| **detail** | キュー情報を詳細に表示します。インスタンスの各プロデューサキューは個別に表示されます。インスタンスのキュー情報は集約されません。 |
| **debug** | 追加のデバッグ情報も表示されます。 |

## コマンド デフォルト

インスタンスを指定しない場合は、すべてのインスタンスが表示されます。

## 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

このコマンドは、すべてのキューを同じインスタンスに集約するすべての Snort インスタンス（プロセス）のキュー情報を表示します。出力には次の情報が表示されます。

- Id：Snort インスタンス ID。「All」は集約されたすべての Snort インスタンスを意味します。
- QId：Lina 送信キュー ID。これは Lina スレッドの数に対応します。「All」はすべてのキューが集約されることを意味します。
- Rx Queue：Lina の受信キュー。「Used」はデータ量を示し、「util」はキュー使用率を示し、「state」は共有メモリの状態を示します。
- TxQ：Lina の送信キュー。「Used」はデータ量を示し、「util」はキュー使用率を示し、「state」は共有メモリの状態を示します。

Counters:

- RxQ-Size：Lina の受信キューサイズ。
- TxQ-Size：Lina の送信キューサイズ。
- TxQ-Data-Limit：送信キューのデータ制限。このしきい値を超えると、データパケットはドロップされます。パーセンテージは、送信キューのしきい値を示します。

- TxQ-Data-Hi-Thresh：送信キューの高しきい値。このしきい値を超えると、PDTS 動的ロードバランシングが開始され、他の Snort インスタンスへのフローのバランシングが試行されます。

### 例

次に、**show asp inspect-dp snort queues** コマンドの出力例を示します。

```
> show asp inspect-dp snort counters summary instance 2
SNORT Inspect Instance Queue Configuration

RxQ-Size:              1   MB
TxQ-Size:            128   KB
TxQ-Data-Limit:      102.4 KB   (80%)
TxQ-Data-Hi-Thresh:   35.8 KB   (28%)

Id QId  RxQ         RxQ    TxQ         TxQ
        (used)      (util) (used)      (util)
-- ---- ---------- ------ ---------- ------
0  All    0        0%       0        0%
1  All    0        0%       0        0%
2  All    0        0%       0        0%
```

# show asp inspect-dp snort queue-exhaustion

Snort キューの枯渇が発生した場合の自動スナップショットを表示するには、**show asp inspect-dp snort queue-exhaustion** コマンドを使用します。

**show asp inspect-dp snort queue-exhaustion** ［**snapshot** *snapshot_id*］［**export** *location*］

## 構文の説明

| | |
|---|---|
| **snapshot** *snapshot_id* | このオプションは、キュー枯渇についての情報を出力する特定のスナップショットを指定します。値は 1 ー 24 の範囲で指定します。 |
| **export** *location* | スナップショットの内容は、オフボックス分析のために、指定された場所の pcap ファイルにエクスポートされます。 |

## 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

**show asp inspect-dp snort queue-exhaustion** コマンドは、Snort キューが枯渇したときに取得されたスナップショットの内容を表示します。選択したスナップショットの内容が表示されます。この出力は、**show capture** コマンドの出力に似ています。

### 例

次に、**show asp inspect-dp snort queue-exhaustion** コマンドの出力例を示します。

```
> show asp inspect-dp snort queue-exhaustion snapshot 1
102 packets captured
   1: 13:52:36.266343       10.100.26.6.80 > 192.168.26.6.45858: .
693143043:693144411(1368) ack 1996534769 win 235 <nop,nop,timestamp 25172833 64977907>
   2: 13:52:36.266343       10.100.26.6.80 > 192.168.26.6.45858: .
693144411:693145779(1368) ack 1996534769 win 235 <nop,nop,timestamp 25172833 64977907>
   3: 13:52:36.266343       10.100.26.6.80 > 192.168.26.6.45858: .
693145779:693147147(1368) ack 1996534769 win 235 <nop,nop,timestamp 25172838 64977912>
   4: 13:52:36.266343       10.100.26.6.80 > 192.168.26.6.45858: .
693147147:693148515(1368) ack 1996534769 win 235 <nop,nop,timestamp 25172838 64977912>
   5: 13:52:36.266343       10.100.26.6.80 > 192.168.26.6.45858: .
693153987:693155355(1368) ack 1996534769 win 235 <nop,nop,timestamp 25172858 64977932>
   6: 13:52:36.266343       10.100.26.6.80 > 192.168.26.6.45858: .
(...output truncated...)
```

# show asp load-balance

ロードバランサのキューサイズのヒストグラムを表示するには、**show asp load-balance** コマンドを使用します。

**show asp load-balance** ［**detail**］

## 構文の説明

| | |
|---|---|
| **detail** | （任意）サンプルで使用されているハッシュバケットに関する詳細情報を表示します。 |

## 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

**show asp load-balance** コマンドは、問題のトラブルシューティングに役立つ場合があります。通常、パケットはインターフェイス受信リングからプルした同じコアによって処理されます。ただし、別のコアが受信したパケットと同じ接続をすでに処理している場合、パケットは、そのコアにキューイングされます。このキューイングによって、他のコアがアイドル状態であっても、ロードバランサ キューが大きくなることがあります。詳細については、**asp load-balance per-packet** コマンドを参照してください。

### 例

次に、**show asp load-balance** コマンドの出力例を示します。X 軸は異なるキューにキューイングされているパケットの数を表します。Y 軸は、パケットがキューイングされているロード バランサのハッシュ バケットを表します（ヒストグラム バケットを示すヒストグラムのバケットと混同しないでください）。キューを持つハッシュバケットの正確な数を確認するには、**detail** キーワードを使用します。

```
> show asp load-balance
Histogram of 'ASP load balancer queue sizes'
  64 buckets sampling from 1 to 65 (1 per bucket)
  6 samples within range (average=23)
                    ASP load balancer queue sizes
  100 +
      |
      |
      |
S     |
a     |
m     |
p     |
l  10 +
e     |
s     |
      |
      |
      |                              #
      |   # #                        # #           #
```

```
|   # #                    # #           #
+---------+---------+---------+---------+---------+---------+----
          10        20        30        40        50        60
                    # of queued jobs per queue
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **asp load-balance per-packet** | マルチコア ASA モデルのコア ロード バランシング方式を変更します。 |

# show asp multiprocessor accelerated- features

高速セキュリティ パス マルチプロセッサ アクセラレーションをデバッグするには、**show asp multiprocessor accelerated-features** コマンドを使用します。

**show asp multiprocessor accelerated-features**

## 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

**show asp multiprocessor accelerated-features** コマンドを実行すると、マルチプロセッサの高速化機能のリストが表示されます。このリストは、パフォーマンス上の問題をトラブルシューティングするのに役立ちます。

### 例

次に、**show asp multiprocessor accelerated-features** コマンドの出力例を示します。

```
> show asp multiprocessor accelerated-features
MultiProcessor accelerated feature list:
        Access Lists
        DNS Guard
        Failover Stateful Updates
        Flow Operations(create, update, and tear-down)
        Inspect HTTP URL Logging
        Inspect HTTP (AIC)
        Inspect IPSec Pass through
        Inspect ICMP and ICMP error
        Inspect RTP/RTCP
        IP Audit
        IP Fragmentation & Re-assembly
        IPSec data-path
        MPF L2-L4 Classify
        Multicast forwarding
        NAT/PAT
        Netflow using UDP transport
        Non-AIC Inspect DNS
        Packet Capture
        QOS
        Resource Management
        Routing Lookup
        Shun
        SSL data-path
        Syslogging using UDP transport
        TCP Intercept
        TCP Security Engine
        TCP Transport
        Threat Detection
        Unicast RPF
        WCCP Re-direct
Above list applies to routed, transparent, single and multi mode.
```

# show asp overhead

スピンロックおよび非同期損失の統計情報を追跡および表示するには、**show asp overhead** コマンドを使用します。

**show asp overhead** ［**sort-by-average**］［**sort-by-file**］

## 構文の説明

| | |
|---|---|
| **sort-by-average** | コールごとの平均サイクル数で結果をソートします。 |
| **sort-by-file** | ファイル名で結果をソートします。 |

## 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、**show asp overhead** コマンドの出力例を示します。

```
> show asp overhead
0.0% of available CPU cycles were lost to Multiprocessor overhead
        since last the MP overhead statistics were last cleared
              File Name Line Function Call             Avg         Cycles      %
----------------------- ---- ----------------------  -----  -------------  -----
```

# show asp packet-profile

プレフィルタポリシーによって高速パス処理されたパケット数、大規模なフローとしてオフロードされたパケット数、アクセス制御（Snort）によって完全に評価されたパケット数などを表示するには、**show asp packet-profile** コマンドを使用します。

**show asp packet-profile [data-path offload snort]**

## 構文の説明

| | |
|---|---|
| **data-path** | データ プレーン パケット プロファイルのカウンタを表示します。 |
| **offload** | ハードウェア オフロード パケット プロファイルのカウンタを表示します。 |
| **snort** | Snort パケットプロファイルのカウンタを表示します。 |

## コマンド デフォルト

インスタンスを指定しない場合は、すべてのインスタンスが表示されます。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.5 | このコマンドが導入されました。 |

## 使用上のガイドライン

脅威に対する防御デバイスを通過する各パケットは、設定されているアクセスポリシー、Snort の判定、およびフローオフロードサポートなどのハードウェア機能に応じて、さまざまな処理段階を経由します。

グローバルカウンタは、これらの統計情報を追跡するために使用され、各セッションの終了時に更新されます。これらのグローバルカウンタは収集され、ヒストグラムの形式で表示されます。任意の時点で、デバイスのブートアップ時または最後の再起動以降にシステムによって処理された累積パケットカウンタがヒストグラムに表示されます。

### 例

次に、**show asp packet-profile** コマンドの出力例を示します。

```
> show asp packet-profile
Current config state: Enabled

Packets Processed
==================

        hw-dynamic-offload                :                    0
        hw-static-offload                 :                    0
        data-path-trust                   :              1419636
        data-path-snort                   :              3522634
        data-path-snort-bypass-allowedlist :               144496
        data-path-snort-bypass-blockedlist :                    0
        data-path-snort-busy-failopen     :                    0
        data-path-snort-down-failopen     :                   10
```

```
                data-path-snort-pre-allowedlist-distribution
                --------------------------------------------

                        Packets         :    Connections
                        [0-3]           :              0
                        [4-7]           :           6202
                        [8-15]          :          10950
                        [16-31]         :           2487
                        [32-63]         :             85
                        [64-127]        :              0
                        [128-255]       :              0
                        [256-511]       :              0
                        [512-1023]      :              0
                        [1024 and above]:              0

                data-path-snort-pre-blockedlist-distribution
                --------------------------------------------

                        Packets         :    Connections
                        [0-3]           :              0
                        [4-7]           :              0
                        [8-15]          :              0
                        [16-31]         :              0
                        [32-63]         :              0
                        [64-127]        :              0
                        [128-255]       :              0
                        [256-511]       :              0
                        [512-1023]      :              0
                        [1024 and above]:              0

                data-path-snort-post-allowedlist-distribution
                ---------------------------------------------

                        Packets         :    Connections
                        [0-3]           :              0
                        [4-7]           :              0
                        [8-15]          :              0
                        [16-31]         :              0
                        [32-63]         :              0
                        [64-127]        :              0
                        [128-255]       :              0
                        [256-511]       :              0
                        [512-1023]      :              0
                        [1024 and above]:              0

                offload-post-allowedlist-distribution
                ---------------------------------------------

                        Packets         :    Connections
                        [0-3]           :              0
                        [4-7]           :              0
                        [8-15]          :              0
                        [16-31]         :              0
                        [32-63]         :              0
                        [64-127]        :              0
                        [128-255]       :              0
                        [256-511]       :              0
                        [512-1023]      :              0
                        [1024 and above]:              0
>
>
```

# show asp rule-engine

tmatch コンパイルプロセスのステータスを確認するには、**show asp rule-engine** コマンドを使用します。

**show asp rule-engine**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1 | このコマンドが導入されました。 |

### 例

次に、アクセスグループとして使用されるアクセスリストのコンパイルが進行中か完了しているのかを確認する例を示します。コンパイル時間は、アクセスリストのサイズによって異なります。時間ステータスの Start（開始）と Completed（完了）は、バッチプロセスであり、モジュールに固有ではないため、すべてのルールに共通です。ほとんどのモジュール要素数がテーブルに表示されます。ステータスには、NAT ルール、ルート、オブジェクト、およびインターフェイスのコンパイルも表示されます。

```
> show asp rule-engine

Rule compilation Status:   Completed
Duration(ms):              421
Start Time:                18:58:34 UTC Apr 7 2021
Last Completed Time:       18:58:44 UTC Apr 7 2021
ACL Commit Mode:           MANUAL
Object Group Search:       DISABLED
Transitional Commit Model: DISABLED

Module    |  Insert   |  Remove   |  Current   |

 NAT      |        90  |        60  |         30  |
 ROUTE    |       107  |        40  |         67  |
 IFC      |        30  |        22  |          8  |
 ACL      |      1446  |       970  |        476  |
```

# show asp table arp

高速セキュリティパスの ARP テーブルをデバッグするには、**show asp table arp** コマンドを使用します。

**show asp table arp** ［**interface** *interface_name*］［**address** *ip_address* ［**netmask** *mask*］］

## 構文の説明

| | |
|---|---|
| **address** *ip_address* | （任意）ARP テーブル エントリを表示する IP アドレスを指定します。 |
| **interface** *interface_name* | （任意）ARPテーブルを表示する特定のインターフェイスを指定します。 |
| **netmask** *mask* | （任意）IP アドレスのサブネット マスクを設定します。 |

## 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

**show arp** コマンドがコントロールプレーンの内容を表示するのに対して、**show asp table arp** コマンドは高速セキュリティパスの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステムデバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

### 例

次に、**show asp table arp** コマンドの出力例を示します。

```
> show asp table arp
Context: single_vf, Interface: inside
  10.86.194.50                            Active   000f.66ce.5d46 hits 0
  10.86.194.1                             Active   00b0.64ea.91a2 hits 638
  10.86.194.172                           Active   0001.03cf.9e79 hits 0
  10.86.194.204                           Active   000f.66ce.5d3c hits 0
  10.86.194.188                           Active   000f.904b.80d7 hits 0
Context: single_vf, Interface: identity
  ::                                      Active   0000.0000.0000 hits 0
  0.0.0.0                                 Active   0000.0000.0000 hits 50208
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show arp** | ARP テーブルを表示します。 |
| **show arp statistics** | ARP 統計情報を表示します。 |

# show asp table classify

高速セキュリティパスの分類子テーブルをデバッグするには、**show asp table classify** コマンドを使用します。

**show asp table classify** ［**interface** *interface_name*］［**crypto** | **domain** *domain_name*］［**hits**］［**match** *regexp*］

## 構文の説明

| | |
|---|---|
| **crypto** | （任意）暗号、暗号解除、および IPSec トンネル フロー ドメインのみを表示します。 |
| **domain** *domain_name* | （任意）特定の分類子ドメインのエントリを表示します。使用可能なドメインのリストについては、CLI のヘルプを参照してください。 |
| **hits** | （オプション）0 以外のヒット値を持つ分類子エントリを表示します。 |
| **interface** *interface_name* | （任意）分類子テーブルを表示する特定のインターフェイスを指定します。 |
| **match** *regexp* | （オプション）正規表現に一致する分類子エントリを表示します。正規表現にスペースが含まれる場合、引用符を使用します。 |

## 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

**show asp table classify** コマンドは、高速セキュリティパスの分類子の内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。分類子は、着信パケットのプロパティ（プロトコル、送信元アドレス、宛先アドレスなど）を検査して、各パケットを適切な分類ルールと対応付けます。それぞれのルールには、パケットのドロップや通過の許可など、どのタイプのアクションを実行するかを規定した分類ドメインのラベルが付けられます。表示される情報はデバッグの目的でのみ使用されます。また、出力は変更される可能性があります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

### 例

次に、**show asp table classify** コマンドの出力例を示します。

```
> show asp table classify
Interface test:
No. of aborted compiles for input action table 0x33b3d70: 29
in  id=0x36f3800, priority=10, domain=punt, deny=false
        hits=0, user_data=0x0, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip=10.86.194.60, mask=255.255.255.255, port=0, tag=any
```

```
in  id=0x33d3508, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
in  id=0x33d3978, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=53, tag=any
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
...
```

次に、**show asp table classify hits** コマンドの出力例を示します。ヒットカウンタの最後のクリアに関するレコードが示されています。

```
Interface mgmt:
in id=0x494cd88, priority=210, domain=permit, deny=true
       hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,

        mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
        dscp=0x0
in id=0x494d1b8, priority=112, domain=permit, deny=false
        hits=1, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=1 src ip=0.0.0.0,
        mask=0.0.0.0, port=0 dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0

Interface inside:
in id=0x48f1580, priority=210, domain=permit, deny=true
       hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,

        mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
        dscp=0x0
in id=0x48f09e0, priority=1, domain=permit, deny=false
        hits=101, user_data=0x0, cs_id=0x0, l3_type=0x608 src mac=0000.0000.0000,
        mask=0000.0000.0000 dst mac=0000.0000.0000, mask=0000.0000.0000
Interface outside:
in id=0x48c0970, priority=210, domain=permit, deny=true
        hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,

       mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0, dscp=0x0
```

次に、レイヤ 2 情報を含む **show asp table classify hits** コマンドの出力例を示します。

```
Input Table
in  id=0x7fff2de10ae0, priority=120, domain=permit, deny=false
    hits=4, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=1
    src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, icmp-code=0, dscp=0x0
    input_ifc=LAN-SEGMENT, output_ifc=identity in  id=0x7fff2de135c0, priority=0,
domain=inspect-ip-options, deny=true
    hits=41, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
    input_ifc=LAN-SEGMENT, output_ifc=any
...

Output Table:

L2 - Output Table:

L2 - Input Table:
in  id=0x7fff2de0e080, priority=1, domain=permit, deny=false
```

```
    hits=30, user_data=0x0, cs_id=0x0, l3_type=0x608
    src mac=0000.0000.0000, mask=0000.0000.0000
    dst mac=0000.0000.0000, mask=0000.0000.0000
    input_ifc=LAN-SEGMENT, output_ifc=any
in  id=0x7fff2de0e580, priority=1, domain=permit, deny=false
    hits=382, user_data=0x0, cs_id=0x0, l3_type=0x8
    src mac=0000.0000.0000, mask=0000.0000.0000
    dst mac=0000.0000.0000, mask=0100.0000.0000
    input_ifc=LAN-SEGMENT, output_ifc=any
in  id=0x7fff2de0e800, priority=1, domain=permit, deny=false
    hits=312, user_data=0x0, cs_id=0x0, l3_type=0x8
    src mac=0000.0000.0000, mask=0000.0000.0000
    dst mac=ffff.ffff.ffff, mask=ffff.ffff.ffff
    input_ifc=LAN-SEGMENT, output_ifc=any
```

# show asp table cluster chash-table

クラスタリングのために高速セキュリティパスの cHash テーブルをデバッグするには、**show asp table cluster chash-table** コマンドを使用します。

**show asp table cluster chash-table**

## 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

**show asp table cluster chash-table** コマンドは、高速セキュリティパスの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステムデバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

### 例

次に、**show asp table cluster chash-table** コマンドの出力例を示します。

```
> show asp table cluster chash-table
Cluster current chash table:

00003333
21001200
22000033
02222223
33331111
21110000
00133103
22222223
30000102
11222222
23222331
00002223
(...output truncated...)
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show asp cluster counter** | クラスタ データパス カウンタ情報を表示します。 |

# show asp table interfaces

高速セキュリティパスのインターフェイステーブルをデバッグするには、**show asp table interfaces** コマンドを使用します。

**show asp table interfaces**

## 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

**show asp table interfaces** コマンドは、高速セキュリティパスのインターフェイステーブルの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

### 例

次に、**show asp table interfaces** コマンドの出力例を示します。

```
> show asp table interfaces
** Flags: 0x0001-DHCP, 0x0002-VMAC, 0x0010-Ident Ifc, 0x0020-HDB Initd,
   0x0040-RPF Enabled
Soft-np interface 'dmz' is up
    context single_vf, nicnum 0, mtu 1500
        vlan 300, Not shared, seclvl 50
        0 packets input, 1 packets output
        flags 0x20
Soft-np interface 'foo' is down
    context single_vf, nicnum 2, mtu 1500
        vlan <None>, Not shared, seclvl 0
        0 packets input, 0 packets output
        flags 0x20
Soft-np interface 'outside' is down
    context single_vf, nicnum 1, mtu 1500
        vlan <None>, Not shared, seclvl 50
        0 packets input, 0 packets output
        flags 0x20
Soft-np interface 'inside' is up
    context single_vf, nicnum 0, mtu 1500
        vlan <None>, Not shared, seclvl 100
        680277 packets input, 92501 packets output
        flags 0x20
...
```

# show asp table network-service

高速セキュリティパスのネットワークサービス オブジェクト テーブルをデバッグするには、**show asp table network-service** コマンドを使用します。

**show asp table network-service**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1 | このコマンドが導入されました。 |

### 例

次に、ネットワークサービス オブジェクト テーブルを表示する例を示します。

```
> show asp table network-service
Per-Context Category NSG:
        subnet=0.0.0.0/0, branch_id=214491, branch_name=connect.facebook.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=214491, branch_name=connect.facebook.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=370809, branch_name=facebook.com.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=370809, branch_name=facebook.com.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=490321, branch_name=fbcdn.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=490321, branch_name=fbcdn.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=548791, branch_name=fbcdn-photos-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=548791, branch_name=fbcdn-photos-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=681143, branch_name=fbcdn-photos-e-a.akamaihd.net.,

ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=681143, branch_name=fbcdn-photos-e-a.akamaihd.net.,

ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=840741, branch_name=fbcdn-photos-b-a.akamaihd.net.,

ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=840741, branch_name=fbcdn-photos-b-a.akamaihd.net.,

ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1014669, branch_name=fbstatic-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1014669, branch_name=fbstatic-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1098051, branch_name=fbexternal-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1098051, branch_name=fbexternal-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1217875, branch_name=fbcdn-profile-a.akamaihd.net.,

ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
```

```
        subnet=0.0.0.0/0, branch_id=1217875, branch_name=fbcdn-profile-a.akamaihd.net.,

ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
       subnet=0.0.0.0/0, branch_id=1379985, branch_name=fbcdn-creative-a.akamaihd.net.,

ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
       subnet=0.0.0.0/0, branch_id=1379985, branch_name=fbcdn-creative-a.akamaihd.net.,

ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1524617, branch_name=channel.facebook.com.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1524617, branch_name=channel.facebook.com.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1683343, branch_name=fbcdn-dragon-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1683343, branch_name=fbcdn-dragon-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1782703, branch_name=contentcache-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1782703, branch_name=contentcache-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1868733, branch_name=facebook.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1868733, branch_name=facebook.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=2068293, branch_name=plus.google.com.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=2068293, branch_name=plus.google.com.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=2176667, branch_name=instagram.com.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=2176667, branch_name=instagram.com.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=2317259, branch_name=linkedin.com.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=2317259, branch_name=linkedin.com.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
```

# show asp table routing

高速セキュリティパスのルーティングテーブルをデバッグするには、**show asp table routing** コマンドを使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

**show asp table routing** ［**vrf** *name* | **all**］ ［**management-only**］［**input** | **output**］［**address** *ip_address* ［**netmask** *mask*］ | **interface** *interface_name*］

## 構文の説明

| | |
|---|---|
| **address** *ip_address* | ルーティング エントリを表示する IP アドレスを設定します。IPv6 アドレスの場合は、スラッシュ（/）に続けてプレフィックス（0～128）を入力し、サブネット マスクを含めることができます。たとえば、「fe80::2e0:b6ff:fe01:3b7a/128」のように入力します。 |
| **input** | 入力ルート テーブルにあるエントリを表示します。 |
| **interface** *interface_name* | （任意）ルーティング テーブルを表示する特定のインターフェイスを指定します。 |
| **netmask** *mask* | IPv4 アドレスの場合は、サブネット マスクを指定します。 |
| **output** | 出力ルート テーブルにあるエントリを表示します。 |
| **management-only** | 管理ルーティング テーブル内のナンバー ポータビリティ ルートを表示します。 |
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してビューを特定の仮想ルータに制限できます。すべての仮想ルータのルーティングテーブルを表示するには、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータのルーティングテーブルを表示します。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |

## 使用上のガイドライン

**show asp table routing** コマンドは、高速セキュリティパスのルーティングテーブルの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。management-only キーワードは、管理ルーティング テーブル内のナンバー ポータビリティ ルートを表示します。

### 例

次に、**show asp table routing** コマンドの出力例を示します。

```
> show asp table routing

in   255.255.255.255 255.255.255.255 identity
in   224.0.0.9       255.255.255.255 identity
in   10.86.194.60    255.255.255.255 identity
in   10.86.195.255   255.255.255.255 identity
in   10.86.194.0     255.255.255.255 identity
in   209.165.202.159 255.255.255.255 identity
in   209.165.202.255 255.255.255.255 identity
in   209.165.201.30  255.255.255.255 identity
in   209.165.201.0   255.255.255.255 identity
in   10.86.194.0     255.255.254.0   inside
in   224.0.0.0       240.0.0.0       identity
in   0.0.0.0         0.0.0.0         inside
out  255.255.255.255 255.255.255.255 foo
out  224.0.0.0       240.0.0.0       foo
out  255.255.255.255 255.255.255.255 test
out  224.0.0.0       240.0.0.0       test
out  255.255.255.255 255.255.255.255 inside
out  10.86.194.0     255.255.254.0   inside
out  224.0.0.0       240.0.0.0       inside
out  0.0.0.0         0.0.0.0         via 10.86.194.1, inside
out  0.0.0.0         0.0.0.0         via 0.0.0.0, identity
out  ::              ::              via 0.0.0.0, identity
```

次の例は、alpha という名前の仮想ルータのルーティングテーブルを示しています。

```
> show asp table routing vrf alpha
Routing table for vrf alpha
route table timestamp: 3916283895
in   1.1.1.1         255.255.255.255 identity
in   1.1.1.0         255.255.255.0   i1
out  255.255.255.255 255.255.255.255 i1
out  1.1.1.1         255.255.255.255 i1
out  1.1.1.0         255.255.255.0   i1
out  224.0.0.0       240.0.0.0       i1
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show route** | コントロール プレーン内のルーティング テーブルを表示します。 |

# show asp table socket

高速セキュリティパスのソケット情報をデバッグするには、**show asp table socket** コマンドを使用します。

**show asp table socket** ［*handle*］［**stats**］

## 構文の説明

| | |
|---|---|
| *handle* | ソケットの長さを指定します。 |
| **stats** | 高速セキュリティパスのソケットテーブルの統計情報を表示します。 |

## 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

**show asp table socket** コマンドは、高速セキュリティ スのソケット情報を表示します。この情報は、高速セキュリティパスのソケットにおける問題のトラブルシューティングに役立つ場合があります。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

### 例

次に、**show asp table socket** コマンドの出力例を示します。

```
Protocol  Socket    Local Address              Foreign Address         State
TCP       00012bac  10.86.194.224:23           0.0.0.0:*               LISTEN
TCP       0001c124  10.86.194.224:22           0.0.0.0:*               LISTEN
SSL       00023b84  10.86.194.224:443          0.0.0.0:*               LISTEN
SSL       0002d01c  192.168.1.1:443            0.0.0.0:*               LISTEN
DTLS      00032b1c  10.86.194.224:443          0.0.0.0:*               LISTEN
SSL       0003a3d4  0.0.0.0:443                0.0.0.0:*               LISTEN
DTLS      00046074  0.0.0.0:443                0.0.0.0:*               LISTEN
TCP       02c08aec  10.86.194.224:22           171.69.137.139:4190     ESTAB
```

次に、**show asp table socket stats** コマンドの出力例を示します。

```
TCP Statistics:
  Rcvd:
     total 14794
     checksum errors 0
     no port 0
  Sent:
     total 0
UDP Statistics:
  Rcvd:
     total 0
     checksum errors 0
  Sent:
     total 0
```

```
     copied 0
NP SSL System Stats:
  Handshake Started: 33
  Handshake Complete: 33
  SSL Open: 4
  SSL Close: 117
  SSL Server: 58
  SSL Server Verify: 0
  SSL Client: 0
```

TCP/UDP 統計情報は、送受信したパケットのうち、デバイスで実行またはリッスンしているサービス（Telnet、SSH、HTTPS など）に転送されるパケットの数を示すパケットカウンタです。チェックサムエラーは、計算されたパケットチェックサムがパケットに保存されているチェックサム値と一致しなかった（つまり、パケットが破損した）ため、ドロップされたパケットの数です。NP SSL 統計情報は、受信した各タイプのメッセージの数を示します。ほとんどが、SSL サーバーまたは SSL クライアントインスタンスへの新しい SSL 接続の開始と終了を示します。

## 関連コマンド

| Command | 説明 |
|---|---|
| **show asp table vpn-context** | 高速セキュリティ パスの VPN コンテキスト テーブルを表示します。 |

# show asp table vpn-context

高速セキュリティパスの VPN コンテキストテーブルをデバッグするには、**show asp table vpn-context** コマンドを使用します。

**show asp table vpn-context** ［**detail**］

## 構文の説明

| | |
|---|---|
| **detail** | （任意）VPN コンテキスト テーブルに関する追加の詳細情報を表示します。 |

## 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

**show asp table vpn-context** コマンドは、高速セキュリティ スの VPN コンテキストの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

### 例

次に、**show asp table vpn-context** コマンドの出力例を示します。

```
> show asp table vpn-context
VPN ID=0058070576, DECR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058193920, ENCR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058168568, DECR+ESP, UP, pk=0000299627, rk=0000000061, gc=2
VPN ID=0058161168, ENCR+ESP, UP, pk=0000305043, rk=0000000061, gc=1
VPN ID=0058153728, DECR+ESP, UP, pk=0000271432, rk=0000000061, gc=2
VPN ID=0058150440, ENCR+ESP, UP, pk=0000285328, rk=0000000061, gc=1
VPN ID=0058102088, DECR+ESP, UP, pk=0000268550, rk=0000000061, gc=2
VPN ID=0058134088, ENCR+ESP, UP, pk=0000274673, rk=0000000061, gc=1
VPN ID=0058103216, DECR+ESP, UP, pk=0000252854, rk=0000000061, gc=2
...
```

次に、PRESERVE フラグで示されているように固定の IPsec トンネルフロー機能が有効になっている場合の **show asp table vpn-context** コマンドの出力例を示します。

```
> show asp table vpn-context
VPN CTX=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=0000000000,
rk=0000000000, gc=0
VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000,
rk=0000000000, gc=0
```

次に、**show asp table vpn-context detail** コマンドの出力例を示します。固定の IPsec トンネルフロー機能が有効になっている場合、フラグにはPRESERVEフラグが含まれます。

```
> show asp table vpn-context detail

VPN Ctx  = 0058070576 [0x03761630]
State    = UP
Flags    = DECR+ESP
SA       = 0x037928F0
SPI      = 0xEA0F21F0
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0

VPN Ctx  = 0058193920 [0x0377F800]
State    = UP
Flags    = ENCR+ESP
SA       = 0x037B4B70
SPI      = 0x900FDC32
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
...
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show asp drop** | ドロップされたパケットの高速セキュリティ パス カウンタを示します。 |

# show asp table zone

高速セキュリティパスのゾーンテーブルをデバッグするには、**show asp table zone** コマンドを使用します。

**show asp table zone**

## 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

**show asp table zone** コマンドは、高速セキュリティパスの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステムデバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

### 例

次に、**show asp table zone** コマンドの出力例を示します。この例では、is-154 という名前のゾーンは実際にはインラインセットであり、トラフィックゾーンではありません。

```
> show asp table zone
Zone: krjones-passive-security-zone id: 48947
    Security-level: 0
    Context       : single_vf
    Zone member(s):
      passive                       GigabitEthernet0/0

Zone: passive_default_context_0 id: 1
    Security-level: 0
    Context       : single_vf
    Zone member(s):

Zone: is-154 id: 34309
    Security-level: 0
    Context       : single_vf
    Zone member(s):
      out                           GigabitEthernet0/2
      in                            GigabitEthernet0/1
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show inline-set** | インラインセットを表示します。 |
| **show zone** | トラフィックゾーンを表示します。 |

# show audit-log

システムの監査ログを表示するには、**show audit-log** コマンドを使用します。

**show audit-log**

## 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

このコマンドでは、監査ログが時系列の逆順に表示され、最も新しい監査ログイベントが最初に示されます。

イベントには、システムの更新、権限の問題、設定の変更、ポリシーアプリケーションなどが含まれます。この情報は、Management Center によってリモート管理されるデバイスのみで使用できます。ローカル管理システムの監査ログは空になっています。

### 例

次の例は、監査ログを示しています。

```
> show audit-log
Audit Log Output:
 time                    :  1476223151 (Tue Oct 11 21:59:11 2016)
 event_type              :  notify
 subsystem               :  Task Queue
 actor                   :  System
 message                 :  Successful task completion : Clam update synchronization
from firepower
 result                  :  Success
 action_source_ip        :  localhost
 action_destination_ip   :  localhost
-------------------------------------------------------------
 time                    :  1476222646 (Tue Oct 11 21:50:46 2016)
 event_type              :  notify
 subsystem               :  Task Queue
 actor                   :  System
 message                 :  Successful task completion : Apply AMP Dynamic Analysis C
onfiguration from firepower
 result                  :  Success
 action_source_ip        :  localhost
 action_destination_ip   :  localhost
-------------------------------------------------------------
 time                    :  1476222564 (Tue Oct 11 21:49:24 2016)
 event_type              :  notify
 subsystem               :  Task Queue
 actor                   :  System
 message                 :  Successful task completion : Apply Initial_Health_Policy
2016-10-11 18:54:59 from firepower
 result                  :  Success
 action_source_ip        :  localhost
 action_destination_ip   :  localhost
-------------------------------------------------------------
 time                    :  1476222563 (Tue Oct 11 21:49:23 2016)
```

```
 event_type             :  notify
 subsystem              :  Health > Health Policy > Apply > Initial_Health_Policy 20
16-10-11 18:54:59 > firepower
 actor                  :  admin
 message                :  Apply
 result                 :  Success
 action_source_ip       :  127.0.0.1
 action_destination_ip  :  localhost
-------------------------------------------------------------
 time                   :  1476222508 (Tue Oct 11 21:48:28 2016)
 event_type             :  notify
 subsystem              :  Task Queue
 actor                  :  System
 message                :  Successful task completion : Registration '10.83.57.41'
 result                 :  Success
 action_source_ip       :  localhost
 action_destination_ip  :  localhost
-------------------------------------------------------------
 time                   :  1476222473 (Tue Oct 11 21:47:53 2016)
 event_type             :  Restart
 subsystem              :  NTP Configuration changed
 actor                  :  Default User
 message                :  Restart
 result                 :  Success
 action_source_ip       :  Default User IP
 action_destination_ip  :  Default Target IP
-------------------------------------------------------------
```

# show b

- show bridge-group （531 ページ）

# show banner

設定されているバナーメッセージを表示するには、**show banner** コマンドを入力します。

**show banner** ［**login**］

## 構文の説明

| | |
|---|---|
| **login** | パスワードログインプロンプト用に設定されたバナーを表示します。 |

## 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

```
> show banner
```

# show bfd drops

BFD でドロップされたパケットの数を表示するには、**show bfd drops** コマンドを使用します。

**show bfd drops**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

### 例

次に、BFD でドロップされたパケットを表示する例を示します。

```
> show bfd drops
BFD Drop Statistics
                         IPV4 IPV6 IPV4-M IPV6-M
Invalid TTL              0    0    0      0
BFD Not Configured       0    0    0      0
No BFD Adjacency         0    0    0      0
Invalid Header Bits      0    0    0      0
Invalid Discriminator    0    0    0      0
Session AdminDown        0    0    0      0
Authen invalid BFD ver   0    0    0      0
Authen invalid len       0    0    0      0
Authen invalid seq       0    0    0      0
Authen failed            0    0    0      0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear bfd counters** | BFD カウンタをクリアします。 |
| **show bfd map** | 設定済みの BFD マップを表示します。 |
| **show bfd neighbors** | 既存の BFD 隣接関係の詳細なリストを表示します。 |
| **show bfd summary** | BFD のサマリー情報を表示します。 |

# show bfd map

設定された BFD マップを表示するには、**show bfd map** コマンドを使用します。

**show bfd map**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

### 例

次に、BFD マップを表示する例を示します。

```
> show bfd map
Destination: 40.40.40.2/24
 Source: 50.50.50.2/24
 Template: mh
 Authentication(Type): sha-1
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear bfd counters** | BFD カウンタをクリアします。 |
| **show bfd drops** | BFD でドロップされたパケットの数を表示します。 |
| **show bfd neighbors** | 既存の BFD 隣接関係の詳細なリストを表示します。 |
| **show bfd summary** | BFD のサマリー情報を表示します。 |

# show bfd neighbors

既存の BFD 隣接関係の行単位のリストを表示するには、**show bfd neighbors** コマンドを使用します。

**show bfd neighbors** ［**client bgp**］［**ipv4** ［*ip_address*］ | **ipv6** ［*ipv6_address*］ | **multihop-ipv4** ［*ip_address*］ | **multihop-ipv6** ［*ipv6_address*］］［**inactive**］［**detail**］

## 構文の説明

| | |
|---|---|
| **client bgp** | （オプション）BGP クライアントのネイバーを表示します。 |
| **ipv4** [ip_address] | （オプション）シングルホップ IPv4 ネイバーを表示します。必要に応じて、特定のネイバーアドレスを指定できます。 |
| **ipv6** [*ipv6_address*] | （オプション）シングルホップ IPv6 ネイバーを表示します。必要に応じて、特定のネイバーアドレスを指定できます。 |
| **multihop-ipv4** [*ip_address*] | （オプション）マルチホップ IPv4 ネイバーを表示します。必要に応じて、特定のネイバーアドレスを指定できます。 |
| **multihop-ipv6** [*ipv6_address*] | （オプション）マルチホップ IPv6 ネイバーを表示します。必要に応じて、特定のネイバーアドレスを指定できます。 |
| **inactive** | （オプション）非アクティブな隣接関係を表示します。 |
| **detail** | （オプション）各ネイバーのすべての BFD プロトコル パラメータおよびタイマーを表示します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

### 例

次に、BFD ネイバーを表示する例を示します。

```
> show bfd neighbors
OurAddr     NeighAddr    LD/RD  RH     Holdown(mult)     State Int
172.16.10.1 172.16.10.2  1/6    1      260 (3 )          Up    Fa0/1
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear bfd counters** | BFD カウンタをクリアします。 |
| **show bfd drops** | BFD でドロップされたパケットの数を表示します。 |
| **show bfd map** | 設定済みの BFD マップを表示します。 |

| Command | 説明 |
| --- | --- |
| **show bfd summary** | BFD のサマリー情報を表示します。 |

# show bfd summary

BFD の要約情報を表示するには、**show bfd summary** コマンドを使用します。

**show bfd summary** ［**client** | **session**］

## 構文の説明

| | |
|---|---|
| **client** | （オプション）クライアントの BFD サマリーを表示します。 |
| **session** | （オプション）セッションの BFD サマリーを表示します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | 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して、BFD、BFD クライアント、または BFD セッションのサマリー情報を表示できます。BFD クライアントがピアとのセッションを開始すると、BFD は定期的に BFD 制御パケットをピアに送信します。次のセッションの状態に関する情報が、このコマンドの出力に含まれます。

- Up：別の BFD インターフェイスが BFD 制御パケットに確認応答すると、セッションはアップ状態に移行します。
- Down：データ パスで障害が生じ、BFD が設定された時間内に制御パケットを受信しない場合は、セッションとデータ パスがダウンとして宣言されます。セッションがダウンした場合は、BFD クライアントがトラフィックを再ルーティングするために必要なアクションを実行できるように、BFD が BFD クライアントに通知します。

### 例

次に、BFD サマリーを表示する例を示します。

```
> show bfd summary
         Session         Up      Down
Total    1               1       0

> show bfd summary session
Protocol Session     Up  Down
IPV4     1           1     0
Total    1           1     0

> show bfd summary client
Client   Session      Up     Down
BGP      1            1      0
EIGRP    1            1      0
Total    2            2      0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear bfd counters** | BFD カウンタをクリアします。 |
| **show bfd drops** | BFD でドロップされたパケットの数を表示します。 |
| **show bfd map** | 設定済みの BFD マップを表示します。 |
| **show bfd neighbors** | 既存の BFD 隣接関係の詳細なリストを表示します。 |

# show bgp

ボーダー ゲートウェイ プロトコル（BGP）ルーティングテーブル内のエントリを表示するには、**show bgp** コマンドを使用します。

**show bgp** ［**vrf** *name* | **all**］ ［*ip-address* ［*mask* ［**longer-prefixes** ［**injected**］ | **shorter-prefixes** ［*length*］ | **bestpath** | **multipaths** | **subnets**］ | **bestpath** | **multipaths**］ | **all** | **prefix-list** *name* | **pending-prefixes** | **route-map** *name*］］

## 構文の説明

| | |
|---|---|
| *ip-address* | （任意）BGPルーティングテーブル内の表示するネットワークを指定します。 |
| *mask* | （オプション）指定したネットワークの一部であるホストをフィルタリングまたは照合するためのマスク。 |
| **longer-prefixes** | （オプション）指定したルートと、より限定的なすべてのルートを表示します。 |
| **injected** | （オプション）BGP ルーティング テーブルに注入された、より限定的なプレフィックスを表示します。 |
| **shorter-prefixes** | （オプション）指定したルートと、より限定的でないすべてのルートを表示します。 |
| *length* | （オプション）プレフィックス長。この引数の値は、0 ～ 32 の数値です。 |
| **bestpath** | （オプション）このプレフィックスの最適パスを表示します。 |
| **multipaths** | （オプション）このプレフィックスのマルチパスを表示します。 |
| **subnets** | （オプション）指定したプレフィックスのサブネット ルートを表示します。 |
| **all** | （オプション）BGPルーティングテーブルのすべてのアドレスファミリ情報を表示します。 |
| **prefix-list** *name* | （オプション）指定したプレフィックスリストに基づいて出力をフィルタリングします。 |
| **pending-prefixes** | （オプション）BGPルーティングテーブルからの削除が保留されているプレフィックスを表示します。 |
| **route-map** *name* | （オプション）指定したルートマップに基づいて出力をフィルタリングします。 |

| | |
|---|---|
| ［**vrf** *name* ｜ **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* ｜ **all**］ キーワードが追加されました。 |

## 使用上のガイドライン

**show bgp** コマンドは、BGP ルーティングテーブルの内容を表示するために使用します。出力は、特定のプレフィックスのエントリ、特定のプレフィックス長のエントリ、および、プレフィックスリスト、ルートマップ、または条件付きアドバタイズメントを介して注入されたプレフィックスのエントリを表示するようにフィルタリングできます。

### 例

次に、BGP ルーティング テーブルの出力例を示します。

```
> show bgp
BGP table version is 22, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.1/32      0.0.0.0                  0         32768 i
*>i10.2.2.2/32      172.16.1.2               0    100      0 i
*bi10.9.9.9/32      192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                           0 10 10 i
* i172.16.1.0/24    172.16.1.2               0    100      0 i
*>                  0.0.0.0                  0         32768 i
*> 192.168.1.0      0.0.0.0                  0         32768 i
*>i192.168.3.0      172.16.1.2               0    100      0 i
*bi192.168.9.0      192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                           0 10 10 i
*bi192.168.13.0     192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                           0 10 10 i
```

次の表では、各フィールドについて説明されています。

**表 *3 : show bgp* のフィールド**

| フィールド | 説明 |
|---|---|
| BGP table version | テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。 |

| フィールド | 説明 |
|---|---|
| local router ID | ルータの IP アドレス |
| Status codes | テーブルエントリのステータス。テーブルの各行の最初にステータスが表示されます。次のいずれかの値を指定できます。<br>• s：テーブルエントリが抑制されます。<br>• d：テーブルエントリがダンプニングされています。<br>• h：テーブルエントリの履歴です。<br>• *：テーブルエントリが有効です。<br>• >：テーブルエントリがそのネットワークで使用するための最良エントリです。<br>• i：テーブルエントリが内部 BGP（iBGP）セッションを経由して学習されます。<br>• r：テーブルエントリは RIB 障害です。<br>• S：テーブルエントリは失効しています。<br>• m：テーブルエントリには、そのネットワークで使用するためのマルチパスが含まれています。<br>• b：テーブルエントリには、そのネットワークで使用するためのバックアップ パスが含まれています。<br>• x：テーブルエントリには、ネットワークで使用するための最適外部ルートが含まれています。 |
| Origin codes | エントリの作成元。作成元のコードはテーブルの各行の終わりにあります。次のいずれかの値を指定できます。<br>• i：内部ゲートウェイプロトコル（IGP）から発信され、アドバタイズされたエントリ。<br>• e：エクステリア ゲートウェイ プロトコル（EGP）から発信されたエントリ。<br>• ?：パスの発信元はクリアされません。通常、これは IGP から BGP に再配信されるルータです。 |
| Network | ネットワークエンティティの IP アドレス |
| Next Hop | パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、ルータにこのネットワークへの非 BGP ルートがあることを示します。 |

| フィールド | 説明 |
|---|---|
| Metric | 表示されている場合は相互自律システムメトリック。 |
| LocPrf | ローカル プリファレンス値。デフォルト値は 100 です。 |
| Weight | 自律システム フィルタを介して設定されたルートの重み。 |
| Path | 宛先ネットワークへの自律システムパス。パス内の各自律システムに対して、このフィールド内に 1 エントリを含めることができます。 |
| (stale) | 指定した自律システムの次のパスがグレースフルリスタートプロセス中に「stale」とマークされたことを示します。 |

次に、BGP ルーティングテーブルの 192.168.1.0 エントリに関する情報の出力例を示します。

```
> show bgp 192.168.1.0
BGP routing table entry for 192.168.1.0/24, version 22
Paths: (2 available, best #2, table default)
  Additional-path
  Advertised to update-groups:
     3
  10 10
    192.168.3.2 from 172.16.1.2 (10.2.2.2)
      Origin IGP, metric 0, localpref 100, valid, internal, backup/repair
  10 10
    192.168.1.2 from 192.168.1.2 (10.3.3.3)
      Origin IGP, localpref 100, valid, external, best , recursive-via-connected
```

次に、BGP ルーティングテーブルの 10.3.3.3 255.255.255.255 エントリに関する情報の出力例を示します。

```
> show bgp 10.3.3.3 255.255.255.255

BGP routing table entry for 10.3.3.3/32, version 35
Paths: (3 available, best #2, table default)
Multipath: eBGP
Flag: 0x860
  Advertised to update-groups:
     1
  200
    10.71.8.165 from 10.71.8.165 (192.168.0.102)
      Origin incomplete, localpref 100, valid, external, backup/repair
      Only allowed to recurse through connected route
  200
    10.71.11.165 from 10.71.11.165 (192.168.0.102)
      Origin incomplete, localpref 100, weight 100, valid, external, best
      Only allowed to recurse through connected route
  200
    10.71.10.165 from 10.71.10.165 (192.168.0.104)
      Origin incomplete, localpref 100, valid, external,
      Only allowed to recurse through connected route
```

次の表では、各フィールドについて説明されています。

表 *4 : show bgp*（*4* バイト自律システム番号）のフィールド

| フィールド | 説明 |
|---|---|
| BGP routing table entry for | ルーティングテーブルエントリの IP アドレスまたはネットワーク番号。 |
| version | テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。 |
| Paths | 使用可能なパスの数、およびインストールされた最適パスの数。最適パスが IP ルーティングテーブルに登録されている場合、この行に「Default-IP-Routing-Table」と表示されます。 |
| Multipath | このフィールドは、マルチパスロードシェアリングがイネーブルの場合に表示されます。このフィールドは、マルチパスが iBGP と eBGP のどちらであるかを示します。 |
| Advertised to update-groups | アドバタイズメントが処理される各アップデートグループの数。 |
| Origin | エントリの作成元。送信元は IGP、EGP、incomplete のいずれかになります。この行には、設定されたメトリック（メトリックが設定されていない場合は 0）、ローカルプリファレンス値（100 がデフォルト）、およびルートのステータスとタイプ（内部、外部、マルチパス、最適）が表示されます。 |
| Extended Community | このフィールドは、ルートが拡張コミュニティ属性を伝送する場合に表示されます。この行には、属性コードが表示されます。拡張コミュニティに関する情報は後続の行に表示されます。 |

次に、**all** キーワードを指定した **show bgp** コマンドの出力例を示します。設定されたすべてのアドレスファミリに関する情報が表示されます。

```
> show bgp all

For address family: IPv4 Unicast   *****
BGP table version is 27, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      0.0.0.0                  0         32768 ?
*> 10.13.13.0/24    0.0.0.0                  0         32768 ?
*> 10.15.15.0/24    0.0.0.0                  0         32768 ?
*>i10.18.18.0/24    172.16.14.105         1388  91351      0 100 e
*>i10.100.0.0/16    172.16.14.107          262    272      0 1 2 3 i
*>i10.100.0.0/16    172.16.14.105         1388  91351      0 100 e
*>i10.101.0.0/16    172.16.14.105         1388  91351      0 100 e
*>i10.103.0.0/16    172.16.14.101         1388    173    173 100 e
*>i10.104.0.0/16    172.16.14.101         1388    173    173 100 e
*>i10.100.0.0/16    172.16.14.106         2219  20889      0 53285 33299 51178 47751 e
*>i10.101.0.0/16    172.16.14.106         2219  20889      0 53285 33299 51178 47751 e
```

```
*  10.100.0.0/16    172.16.14.109         2309             0 200 300 e
*>                  172.16.14.108         1388             0 100 e
*  10.101.0.0/16    172.16.14.109         2309             0 200 300 e
*>                  172.16.14.108         1388             0 100 e
*> 10.102.0.0/16    172.16.14.108         1388             0 100 e
*> 172.16.14.0/24   0.0.0.0                  0         32768 ?
*> 192.168.5.0      0.0.0.0                  0         32768 ?
*> 10.80.0.0/16     172.16.14.108         1388             0 50 e
*> 10.80.0.0/16     172.16.14.108         1388             0 50 e
```

次に、**longer-prefixes** キーワードを指定した **show bgp** コマンドの出力例を示します。

```
> show bgp 10.92.0.0 255.255.0.0 longer-prefixes

BGP table version is 1738, local router ID is 192.168.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop          Metric LocPrf Weight Path
*> 10.92.0.0         10.92.72.30         8896         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.1.0         10.92.72.30         8796         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.11.0        10.92.72.30        42482         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.14.0        10.92.72.30         8796         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.15.0        10.92.72.30         8696         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.16.0        10.92.72.30         1400         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.17.0        10.92.72.30         1400         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.18.0        10.92.72.30         8876         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.19.0        10.92.72.30         8876         32768 ?
*                    10.92.72.30                          0 109 108 ?
```

次に、**shorter-prefixes** キーワードを指定した **show bgp** コマンドの出力例を示します。8 ビットプレフィックス長を指定しています。

```
> show bgp 172.16.0.0/16 shorter-prefixes 8
*> 172.16.0.0         10.0.0.2                               0 ?
*                     10.0.0.2                 0             0 200 ?
```

次に、**prefix-list** キーワードを指定した **show bgp** コマンドの出力例を示します。

```
> show bgp prefix-list ROUTE

BGP table version is 39, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      10.0.0.2                               0 ?
*                   10.0.0.2                 0             0 200 ?
```

次に、**route-map** キーワードを指定した **show bgp** コマンドの出力例を示します。

```
> show bgp route-map LEARNED_PATH

BGP table version is 40, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      10.0.0.2                             0 ?
*                   10.0.0.2                 0           0 200 ?
```

# show bgp cidr-only

Classless Inter-Domain Routing（CIDR）を使用したルートを表示するには、**show bgp cidr-only** コマンドを使用します。

**show bgp cidr-only** ［**vrf** *name* | **all**］

## 構文の説明

| | |
|---|---|
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |

### 例

次に、**show bgp cidr-only** コマンドの出力例を示します。出力の説明については、**show bgp** コマンドを参照してください。

```
> show bgp cidr-only

BGP table version is 220, local router ID is 172.16.73.131
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 192.168.0.0/8    172.16.72.24                         0 1878 ?
*> 172.16.0.0/16    172.16.72.30                         0 108 ?
```

# show bgp community

指定された BGP コミュニティに属するルートを表示するには、**show bgp community** コマンドを使用します。

**show bgp community** ［**vrf** *name* | **all**］ ［*community-number*］［**exact-match**］［**no-advertise**］［**no-export**］

## 構文の説明

| | |
|---|---|
| *community-number* | （オプション）有効な値は 1 ～ 4294967295 のコミュニティ番号、または AA:NN（自律システムのコミュニティ番号:2 バイトの番号）です。 |
| **exact-match** | （オプション）完全一致を持つルートだけを表示します。 |
| **no-advertise** | （オプション）ピアにアドバタイズされないルートだけを表示します（ウェルノウン コミュニティ）。 |
| **no-export** | （オプション）ローカル自律システムの外部にエクスポートされていないルートだけを表示します（ウェルノウン コミュニティ）。 |
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |

### 例

次に、**show bgp community** コマンドの出力例を示します。出力の説明については、**show bgp** コマンドを参照してください。

```
> show bgp community 111:12345
BGP table version is 10, local router ID is 224.0.0.10
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 172.16.2.2/32    10.43.222.2           0             0 222 ?
*> 10.0.0.0         10.43.222.2           0             0 222 ?
*> 10.43.0.0        10.43.222.2           0             0 222 ?
*> 10.43.44.44/32   10.43.222.2           0             0 222 ?
```

```
*  10.43.222.0/24   10.43.222.2           0             0 222 i
*> 172.17.240.0/21  10.43.222.2           0             0 222 ?
*> 192.168.212.0    10.43.222.2           0             0 222 i
*> 172.31.1.0       10.43.222.2           0             0 222 ?
```

# show bgp community-list

ボーダー ゲートウェイ プロトコル（BGP）コミュニティリストによって許可されたルートを表示するには、**show bgp community-list** コマンドを使用します。

**show bgp community-list** ［**vrf** *name* | **all**］ {*community-list-number* | *community-list-name* ［**exact-match**］}

## 構文の説明

| | |
|---|---|
| *community-list-number* | 1 ～ 500 の範囲の標準または拡張コミュニティ リスト番号。 |
| *community-list-name* | コミュニティ リストの名前。コミュニティ リストの名前は、standard または expanded になります。 |
| **exact-match** | （オプション）完全一致を持つルートだけを表示します。 |
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |

### 例

次に、**show bgp community-list** の出力例を示します。出力の説明については、**show bgp** コマンドを参照してください。

```
> show bgp community-list 20
BGP table version is 716977, local router ID is 192.168.32.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

  Network          Next Hop          Metric LocPrf Weight Path
* i10.3.0.0         10.0.22.1             0    100      0 1800 1239 ?
*>i                 10.0.16.1             0    100      0 1800 1239 ?
* i10.6.0.0         10.0.22.1             0    100      0 1800 690 568 ?
*>i                 10.0.16.1             0    100      0 1800 690 568 ?
* i10.7.0.0         10.0.22.1             0    100      0 1800 701 35 ?
*>i                 10.0.16.1             0    100      0 1800 701 35 ?
*                   10.92.72.24                         0 1878 704 701 35 ?
* i10.8.0.0         10.0.22.1             0    100      0 1800 690 560 ?
*>i                 10.0.16.1             0    100      0 1800 690 560 ?
*                   10.92.72.24                         0 1878 704 701 560 ?
```

```
* i10.13.0.0        10.0.22.1            0    100      0 1800 690 200 ?
*>i                 10.0.16.1            0    100      0 1800 690 200 ?
*                   10.92.72.24                        0 1878 704 701 200 ?
* i10.15.0.0        10.0.22.1            0    100      0 1800 174 ?
*>i                 10.0.16.1            0    100      0 1800 174 ?
* i10.16.0.0        10.0.22.1            0    100      0 1800 701 i
*>i                 10.0.16.1            0    100      0 1800 701 i
*                   10.92.72.24                        0 1878 704 701 i
```

# show bgp filter-list

指定したフィルタリストと一致するルートを表示するには、**show bgp filter-list** コマンドを使用します。

**show bgp filter-list** ［**vrf** *name* | **all**］ *access-list-name*

## 構文の説明

| | |
|---|---|
| *access-list-name* | 自律システム パス アクセス リストの名前。有効な値は、1 ～ 500 です。 |
| ［**vrf** *name* \| **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* \| **all**］ キーワードが追加されました。 |

### 例

次に、**show bgp filter-list** コマンドの出力例を示します。出力の説明については、**show bgp** コマンドを参照してください。

```
> show bgp filter-list filter-list-acl
BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*  172.16.0.0       172.16.72.30                           0 109 108 ?
*  172.16.1.0       172.16.72.30                           0 109 108 ?
*  172.16.11.0      172.16.72.30                           0 109 108 ?
*  172.16.14.0      172.16.72.30                           0 109 108 ?
*  172.16.15.0      172.16.72.30                           0 109 108 ?
*  172.16.16.0      172.16.72.30                           0 109 108 ?
*  172.16.17.0      172.16.72.30                           0 109 108 ?
*  172.16.18.0      172.16.72.30                           0 109 108 ?
*  172.16.19.0      172.16.72.30                           0 109 108 ?
*  172.16.24.0      172.16.72.30                           0 109 108 ?
*  172.16.29.0      172.16.72.30                           0 109 108 ?
*  172.16.30.0      172.16.72.30                           0 109 108 ?
*  172.16.33.0      172.16.72.30                           0 109 108 ?
*  172.16.35.0      172.16.72.30                           0 109 108 ?
*  172.16.36.0      172.16.72.30                           0 109 108 ?
*  172.16.37.0      172.16.72.30                           0 109 108 ?
```

```
*  172.16.38.0      172.16.72.30                    0 109 108 ?
*  172.16.39.0      172.16.72.30                    0 109 108 ?
```

# show bgp injected-paths

ボーダー ゲートウェイ プロトコル（BGP）ルーティングテーブルに注入されたすべてのパスを表示するには、**show bgp injected-paths** コマンドを使用します。

**show bgp injected-paths** ［**vrf** *name* | **all**］

## 構文の説明

| | |
|---|---|
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |

### 例

次に、**show bgp injected-paths** コマンドの出力例を示します。出力の説明については、**show bgp** コマンドを参照してください。

```
> show bgp injected-paths
BGP table version is 11, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 172.16.0.0       10.0.0.2                             0 ?
*> 172.17.0.0/16    10.0.0.2                             0 ?
```

# show bgp ipv4 unicast

IP バージョン 4（IPv4）ボーダー ゲートウェイ プロトコル（BGP）ルーティングテーブル内のエントリを表示するには、**show bgp ipv4 unicast** コマンドを使用します。

**show bgp ipv4 unicast** ［**vrf** *name* | **all**］ ［**cidr-only**］

## 構文の説明

| | |
|---|---|
| **unicast** | IPv4 ユニキャスト アドレス プレフィックスを指定します。 |
| **cidr-only** | （オプション）不自然なネットマスクを持つルートを表示します。 |
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |

### 例

次に、**show bgp ipv4 unicast** コマンドの出力例を示します。出力の説明については、**show bgp** コマンドを参照してください。

```
> show bgp ipv4 unicast
 BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/24    172.16.10.1              0             0  300 i
*> 10.10.20.0/24    172.16.10.1              0             0  300 i
*  10.20.10.0/24    172.16.10.1              0             0  300 i
```

# show bgp ipv6 unicast

IPv6 ボーダー ゲートウェイ プロトコル（BGP）ルーティングテーブル内のエントリを表示するには、**show bgp ipv6** コマンドを使用します。

**show bgp ipv6 unicast** ［**vrf** *name* | **all**］ ［*ipv6-prefix/prefix-length*］［**longer-prefixes**］［**labels**］

## 構文の説明

| | |
|---|---|
| **unicast** | IPv6 ユニキャスト アドレス プレフィックスを指定します。 |
| *ipv6-prefix* | （オプション）IPv6 ネットワーク番号。IPv6 BGP ルーティング テーブル内の特定のネットワークを表示するために入力します。<br>この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。 |
| */prefix-length* | （オプション）IPv6プレフィックスの長さ。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。 |
| **longer-prefixes** | （オプション）ルートと、より限定的なルートを表示します。 |
| **labels** | （オプション）アドレスファミリごとに、このネイバーに適用されるポリシーを表示します。 |
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |

### 例

次に、**show bgp ipv6 unicast** コマンドの出力例を示します。ここでは、プレフィックス 3FFE:500::/24 に関する情報を示しています。出力の説明については、**show bgp** コマンドを参照してください。

```
> show bgp ipv6 unicast 3FFE:500::/24
BGP routing table entry for 3FFE:500::/24, version 19421
```

```
Paths: (6 available, best #1)
  293 3425 2500
    3FFE:700:20:1::11 from 3FFE:700:20:1::11 (192.168.2.27)
      Origin IGP, localpref 100, valid, external, best
  4554 293 3425 2500
    3FFE:C00:E:4::2 from 3FFE:C00:E:4::2 (192.168.1.1)
      Origin IGP, metric 1, localpref 100, valid, external
  33 293 3425 2500
    3FFE:C00:E:5::2 from 3FFE:C00:E:5::2 (209.165.18.254)
      Origin IGP, localpref 100, valid, external
  6175 7580 2500
    3FFE:C00:E:1::2 from 3FFE:C00:E:1::2 (209.165.223.204)
      Origin IGP, localpref 100, valid, external
1849 4697 2500, (suppressed due to dampening)
    3FFE:1100:0:CC00::1 from 3FFE:1100:0:CC00::1 (172.31.38.102)
      Origin IGP, localpref 100, valid, external
237 10566 4697 2500
    3FFE:C00:E:B::2 from 3FFE:C00:E:B::2 (172.31.0.3)
      Origin IGP, localpref 100, valid, external
> show bgp ipv6 unicast
BGP table version is 28, local router ID is 172.10.10.1
Status codes:s suppressed, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*>i4004::/64        ::FFFF:172.11.11.1
                                             0    100      0 ?
* i                 ::FFFF:172.30.30.1
                                             0    100      0 ?
```

# show bgp ipv4/ipv6 unicast community

IPv4 または IPv6 ボーダー ゲートウェイ プロトコル（BGP）ルーティングテーブル内のエントリを表示するには、それぞれ **show bgp ipv4 unicast community** または **show bgp ipv6 unicast community** コマンドを使用します。

**show bgp** ［**vrf** *name* ｜ **all**］ ｛**ipv4** ｜ **ipv6**｝ **unicast community** ［*community-number*］ ［**exact-match**］［**local-as** ｜ **no-advertise** ｜ **no-export**］

## 構文の説明

| | |
|---|---|
| **unicast** | IPv4 または IPv6 ユニキャスト アドレス プレフィックスを指定します。 |
| *community-number* | （オプション）有効な値は 1 ～ 4294967295 のコミュニティ番号、または AA:NN（自律システムのコミュニティ番号:2 バイトの番号）です。 |
| **exact-match** | （オプション）完全一致を持つルートだけを表示します。 |
| **local-as** | （オプション）ローカル自律システム外に送信されないルートだけを表示します（ウェルノウン コミュニティ）。 |
| **no-advertise** | （オプション）ピアにアドバタイズされないルートだけを表示します（ウェルノウン コミュニティ）。 |
| **no-export** | （オプション）ローカル自律システムの外部にエクスポートされていないルートだけを表示します（ウェルノウン コミュニティ）。 |
| ［**vrf** *name* ｜ **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* ｜ **all**］ キーワードが追加されました。 |

### 例

次に、**show bgp ipv6 unicast community** コマンドの出力例を示します。出力の説明については、**show bgp** コマンドを参照してください。

```
BGP table version is 69, local router ID is 10.2.64.5
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete
      Network               Next Hop              Metric LocPrf Weight Path
*> 2001:0DB8:0:1::1/64       ::                                       0 32768 i
*> 2001:0DB8:0:1:1::/80      ::                                       0 32768 ?
*> 2001:0DB8:0:2::/64        2001:0DB8:0:3::2                            0 2 i
*> 2001:0DB8:0:2:1::/80      2001:0DB8:0:3::2                            0 2 ?
* 2001:0DB8:0:3::1/64        2001:0DB8:0:3::2                            0 2 ?
*>                        ::                                         0 32768 ?
*> 2001:0DB8:0:4::/64        2001:0DB8:0:3::2                            0 2 ?
*> 2001:0DB8:0:5::1/64       ::                                       0 32768 ?
*> 2001:0DB8:0:6::/64        2000:0:0:3::2                            0 2 3 i
*> 2010::/64                 ::                                       0 32768 ?
*> 2020::/64                 ::                                       0 32768 ?
*> 2030::/64                 ::                                       0 32768 ?
*> 2040::/64                 ::                                       0 32768 ?
*> 2050::/64                 ::                                       0 32768 ?
```

# show bgp ipv4/ipv6 unicast community-list

IPv4 または IPv6 ボーダー ゲートウェイ プロトコル（BGP）コミュニティリストで許可されているルートを表示するには、それぞれ **show bgp ipv4 unicast community-list** または **show bgp ipv6 unicast community-list** コマンド使用します。

**show bgp** ［**vrf** *name* | **all**］ {**ipv4** | **ipv6**} **unicast community-list** {*number* | *name*} ［**exact-match**］

## 構文の説明

| | |
|---|---|
| **unicast** | IPv4 または IPv6 ユニキャスト アドレス プレフィックスを指定します。 |
| *number* | 1 ～ 199 の範囲のコミュニティ リスト番号。 |
| *name* | コミュニティ リストの名前。 |
| **exact-match** | （オプション）完全一致を持つルートだけを表示します。 |
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |

### 例

次に、コミュニティリスト番号 3 に対する **show bgp ipv6 unicast community-list** コマンドの出力例を示します。出力の説明については、**show bgp** コマンドを参照してください。

```
> show bgp ipv6 unicast community-list 3
BGP table version is 14, local router ID is 10.2.64.6
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete

    Network                Next Hop            Metric LocPrf Weight Path
*> 2001:0DB8:0:1::/64      2001:0DB8:0:3::1                         0 1 i
*> 2001:0DB8:0:1:1::/80    2001:0DB8:0:3::1                         0 1 i
*> 2001:0DB8:0:2::1/64     ::                                   0 32768 i
*> 2001:0DB8:0:2:1::/80    ::                                   0 32768 ?
* 2001:0DB8:0:3::2/64      2001:0DB8:0:3::1                         0 1 ?
```

```
*>                        ::                                    0 32768 ?
*> 2001:0DB8:0:4::2/64      ::                                    0 32768 ?
*> 2001:0DB8:0:5::/64       2001:0DB8:0:3::1                         0 1 ?
*> 2010::/64                2001:0DB8:0:3::1                         0 1 ?
*> 2020::/64                2001:0DB8:0:3::1                         0 1 ?
*> 2030::/64                2001:0DB8:0:3::1                         0 1 ?
*> 2040::/64                2001:0DB8:0:3::1                         0 1 ?
*> 2050::/64                2001:0DB8:0:3::1                         0 1 ?
```

# show bgp ipv4/ ipv6 unicast neighbors

ネイバーへの IPv4 または IPv6 ボーダー ゲートウェイ プロトコル（BGP）接続に関する情報を表示するには、**show bgp ipv4 unicast neighbors** または **show bgp ipv6 neighbors** コマンドを使用します。

**show bgp** ［**vrf** *name* | **all**］ {**ipv4** | **ipv6**} **unicast neighbors** ［*ip-address*］［**received-routes** | **routes** | **advertised-routes** | **paths** *regular-expression*］

## 構文の説明

| | |
|---|---|
| **unicast** | IPv4 または IPv6 ユニキャスト アドレス プレフィックスを指定します。 |
| *ip-address* | （任意）IPv4 または IPv6 BGP スピーキングネイバーのアドレス。この引数を省略した場合、すべての IPv4 または IPv6 ネイバーが表示されます。<br>IPv6 アドレスは、RFC 2373 に記述されている形式、つまり、コロン区切りの 16 ビット値を使用して16 進数で指定する必要があります。 |
| **received-routes** | （オプション）指定したネイバーから受信したすべてのルートを表示します。 |
| **routes** | （オプション）受信され、受け入れられるすべてのルートを表示します。これは received-routes キーワードの出力のサブセットです。 |
| **advertised-routes** | （オプション）ネイバーにアドバタイズされているネットワーキング デバイスのすべてのルートを表示します。 |
| **paths** *regular-expression* | （オプション）受信したパスの照合に使用される正規表現。 |
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |

### 例

次に、**show bgp ipv6 unicast neighbors** コマンドの出力例を示します。

```
> show bgp ipv6 unicast neighbors
BGP neighbor is 3FFE:700:20:1::11,  remote AS 65003, external link
  BGP version 4, remote router ID 192.168.2.27
  BGP state = Established, up for 13:40:17
  Last read 00:00:09, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 31306 messages, 20 notifications, 0 in queue
  Sent 14298 messages, 1 notifications, 0 in queue
  Default minimum time between advertisement runs is 30 seconds
 For address family: IPv6 Unicast
  BGP table version 21880, neighbor version 21880
  Index 1, Offset 0, Mask 0x2
  Route refresh request: received 0, sent 0
  Community attribute sent to this neighbor
  Outbound path policy configured
  Incoming update prefix filter list is bgp-in
  Outgoing update prefix filter list is aggregate
  Route map for outgoing advertisements is uni-out
  77 accepted prefixes consume 4928 bytes
  Prefix advertised 4303, suppressed 0, withdrawn 1328
  Number of NLRIs in the update sent: max 1, min 0
  1 history paths consume 64 bytes
  Connections established 22; dropped 21
  Last reset 13:47:05, due to BGP Notification sent, hold time expired
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 3FFE:700:20:1::12, Local port: 55345
Foreign host: 3FFE:700:20:1::11, Foreign port: 179
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x1A0D543C):
Timer          Starts    Wakeups            Next
Retrans          1218          5             0x0
TimeWait            0          0             0x0
AckHold          3327       3051             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
iss: 1805423033  snduna: 1805489354  sndnxt: 1805489354     sndwnd:  15531
irs:  821333727  rcvnxt:  821591465  rcvwnd:      15547  delrcvwnd:    837
SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, nagle
Datagrams (max data segment is 1420 bytes):
Rcvd: 4252 (out of order: 0), with data: 3328, total data bytes: 257737
Sent: 4445 (retransmit: 5), with data: 4445, total data bytes: 244128
```

次の表で、この出力に表示される重要なフィールドを説明します。

**表 *5 : show bgp ipv4/ ipv6 unicast neighbors* のフィールド**

| フィールド | 説明 |
|---|---|
| BGP neighbor | BGP ネイバーの IP アドレスとその自律システム番号。ネイバーがルータと同じ自律システム内にある場合、これらの間のリンクは内部となり、そうでない場合は外部リンクと見なされます。 |

| フィールド | 説明 |
|---|---|
| remote AS | ネイバーの自律システム。 |
| internal link | このピアが内部ボーダー ゲートウェイ プロトコル（iBGP）ピアであることを示します。 |
| BGP version | リモートルータとの通信に使用されるBGPバージョン。ネイバーのルータ ID（IP アドレス）も指定されます。 |
| remote router ID | ピリオドで区切られた4つのオクテットとして記述される32ビット数（ドット付き 10 進表記）。 |
| BGP state | この BGP 接続の内部ステート。 |
| up for | ベースとなる TCP 接続が存在している時間。 |
| Last read | BGP がこのネイバーから最後にメッセージを読み取った時間。 |
| hold time | ピアからのメッセージ間の最大経過時間。 |
| keepalive interval | TCP 接続が維持されていることを確認できるように、キープアライブ パケットを送信する時間間隔。 |
| Neighbor capabilities | このネイバーからアドバタイズされ受信される BGP 機能。 |
| Route refresh | ルートリフレッシュ機能を使用してネイバーがダイナミック ソフト リセットをサポートすることを示します。 |
| Address family IPv6 Unicast | BGP ピアが IPv6 到達可能性情報を交換していることを示します。 |
| Received | このピアから受信した、キープアライブを含むBGPメッセージの合計数。 |
| 通知 | ピアから受信したエラーメッセージの数。 |
| Sent | このピアに送信された、キープアライブを含むBGPメッセージの合計数。 |
| 通知 | ルータがこのピアに送信したエラー メッセージの数。 |
| advertisement runs | 最小アドバタイズメント間隔の値。 |
| For address family | 後続のフィールドが参照するアドレスファミリ。 |
| BGP table version | テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。 |
| neighbor version | 送信済みのプレフィックスおよびこのネイバーに送信する必要があるプレフィックスを追跡するためにソフトウェアによって使用された番号。 |

| フィールド | 説明 |
|---|---|
| Route refresh request | このネイバーで送受信されるルート リフレッシュ要求の数。 |
| Community attribute（出力例になし） | neighbor send-community コマンドがこのネイバー用に設定されている場合に表示されます。 |
| Inbound path policy（出力例になし） | インバウンド フィルタ リストまたはルート マップが設定されているかどうかを示します。 |
| Outbound path policy（出力例になし） | アウトバウンドフィルタリスト、ルートマップ、または抑制マップが設定されているかどうかを示します。 |
| bgp-in（出力例になし） | IPv6 ユニキャスト アドレス ファミリのインバウンド アップデート プレフィックス フィルタ リストの名前。 |
| aggregate（出力例になし） | IPv6ユニキャストアドレスファミリのアウトバウンドアップデート プレフィックス フィルタ リストの名前。 |
| uni-out（出力例になし） | IPv6 ユニキャスト アドレス ファミリのアウトバウンド ルート マップの名前。 |
| accepted prefixes | 受け入れられたプレフィックスの数。 |
| Prefix advertised | アドバタイズされたプレフィックスの数。 |
| suppressed | 抑制されたプレフィックスの数。 |
| withdrawn | 取り消されたプレフィックスの数。 |
| history paths（出力例になし） | 履歴を記憶するために保持されるパス エントリの数。 |
| Connections established | ルータが TCP 接続を確立し、2 つのピアが相互に BGP 通信を行うことに同意した回数。 |
| dropped | 良好な接続に失敗したか、ダウンした回数。 |
| Last reset | このピアリング セッションが最後にリセットされてからの経過時間（時:分:秒形式）。 |
| Connection state | BGP ピアの状態。 |
| unread input bytes | 処理待ちのパケットのバイト数。 |
| Local host、Local port | ローカル ルータおよびポートのピア アドレス。 |
| Foreign host, Foreign port | ネイバーのピア アドレス。 |
| Event Timers | 各タイマーの開始とウェイク アップの回数を表示する表。 |

| フィールド | 説明 |
|---|---|
| snduna | ローカル ホストが送信したものの、確認応答を受信していない最後の送信シーケンス番号。 |
| sndnxt | ローカル ホストが次に送信するシーケンス番号。 |
| sndwnd | リモート ホストの TCP ウィンドウ サイズ。 |
| irs | 最初の受信シーケンス番号。 |
| rcvnxt | ローカル ホストが確認応答した最後の受信シーケンス番号。 |
| rcvwnd | ローカル ホストの TCP ウィンドウ サイズ。 |
| delrecvwnd | 遅延受信ウィンドウ：ローカルホストによって接続から読み取られ、ホストがリモートホストにアドバタイズした受信ウィンドウから削除されていないデータ。このフィールドの値は、フルサイズのパケットより大きくなるまで次第に増加し、それに達した時点で、rcvwnd フィールドに適用されます。 |
| SRTT | 計算されたスムーズ ラウンドトリップ タイムアウト（ミリ秒単位）。 |
| RTTO | ラウンドトリップ タイムアウト（ミリ秒単位）。 |
| RTV | ラウンドトリップ時間の差異（ミリ秒単位）。 |
| KRTT | Karn アルゴリズムを使用した新しいラウンドトリップ タイムアウト（ミリ秒単位）。このフィールドは、再送信されたパケットのラウンドトリップ時間を個別に追跡します。 |
| minRTT | 計算に組み込み値を使用して記録された最小ラウンドトリップ タイムアウト（ミリ秒単位）。 |
| maxRTT | 記録された最大ラウンドトリップ タイムアウト（ミリ秒単位）。 |
| ACK hold | データを「ピギーバックする」ためにローカルホストが確認応答を遅延させる時間（ミリ秒単位）。 |
| Flags | BGP パケットの IP プレシデンス。 |
| Datagrams: Rcvd | ネイバーから受信したアップデート パケットの数。 |
| with data | データとともに受信したアップデート パケットの数。 |
| total data bytes | データのバイト総数。 |
| Sent | 送信されたアップデートパケットの数。 |
| with data | データとともに送信されたアップデート パケットの数。 |

| フィールド | 説明 |
|---|---|
| total data bytes | データのバイト総数。 |

次に、**advertised-routes** キーワードを指定した場合の **show bgp ipv6 unicast neighbors** コマンドの出力例を示します。出力の説明については、**show bgp** コマンドを参照してください。

```
> show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 advertised-routes
BGP table version is 21880, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 2001:200::/35    3FFE:700:20:1::11                       0 293 3425 2500 i
*> 2001:208::/35    3FFE:C00:E:B::2                         0 237 7610 i
*> 2001:218::/35    3FFE:C00:E:C::2                         0 3748 4697 i
```

次に、**routes** キーワードを指定した場合の **show bgp ipv6 unicast neighbors** コマンドの出力例を示します。

```
> show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 routes
BGP table version is 21885, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 2001:200::/35    3FFE:700:20:1::11                       0 293 3425 2500 i
*  2001:208::/35    3FFE:700:20:1::11                       0 293 7610 i
*  2001:218::/35    3FFE:700:20:1::11                       0 293 3425 4697 i
*  2001:230::/35    3FFE:700:20:1::11                       0 293 1275 3748 i
```

次に、**paths** キーワードを指定した場合の **show bgp ipv6 neighbors** コマンドの出力例を示します。

```
> show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 paths ^293
Address    Refcount Metric Path
0x6131D7DC        2      0 293 3425 2500 i
0x6132861C        2      0 293 7610 i
0x6131AD18        2      0 293 3425 4697 i
0x61324084        2      0 293 1275 3748 i
0x61320E0C        1      0 293 3425 2500 2497 i
0x61326928        1      0 293 3425 2513 i
0x61327BC0        2      0 293 i
0x61321758        1      0 293 145 i
0x61320BEC        1      0 293 3425 6509 i
0x6131AAF8        2      0 293 1849 2914 ?
0x61320FE8        1      0 293 1849 1273 209 i
0x613260A8        2      0 293 1849 i
0x6132586C        1      0 293 1849 5539 i
0x6131BBF8        2      0 293 1849 1103 i
0x6132344C        1      0 293 4554 1103 1849 1752 i
0x61324150        2      0 293 1275 559 i
0x6131E5AC        2      0 293 1849 786 i
0x613235E4        1      0 293 1849 1273 i
0x6131D028        1      0 293 4554 5539 8627 i
0x613279E4        1      0 293 1275 3748 4697 3257 i
```

```
0x61320328        1      0 293 1849 1273 790 i
0x6131EC0C        2      0 293 1275 5409 i
```

次の表で、この出力に表示される重要なフィールドを説明します。

**表 *6 : show bgp ipv6 neighbors paths* のフィールド**

| フィールド | 説明 |
|---|---|
| アドレス（Address） | パスが保存される内部アドレス。 |
| Refcount | そのパスを使用しているルートの数。 |
| メトリック | パスの Multi Exit Discriminator（MED）メトリック（BGP バージョン 2 および 3 のこのメトリック名は INTER_AS です）。 |
| Path | そのルートの自律システム パスと、そのルートの発信元コード。 |

次に、**show bgp ipv6 neighbors** コマンドの出力例を示します。ここでは、IPv6 アドレス 2000:0:0:4::2 の **received routes** を示しています。

```
> show bgp ipv6 unicast neighbors 2000:0:0:4::2 received-routes
BGP table version is 2443, local router ID is 192.168.0.2
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network               Next Hop           Metric LocPrf Weight Path
*> 2000:0:0:1::/64      2000:0:0:4::2                         0 2 1 i
*> 2000:0:0:2::/64      2000:0:0:4::2                         0 2 i
*> 2000:0:0:2:1::/80    2000:0:0:4::2                         0 2 ?
*> 2000:0:0:3::/64      2000:0:0:4::2                         0 2 ?
*  2000:0:0:4::1/64     2000:0:0:4::2                         0 2 ?
```

# show bgp ipv4/ ipv6 unicast paths

データベース内のすべての IPv4 または IPv6 ボーダー ゲートウェイ プロトコル（BGP）パスを表示するには、それぞれ **show bgp ipv4 unicast paths** または **show bgp ipv6 unicast paths** コマンドを使用します。

**show bgp** ［**vrf** *name* | **all**］ ｛**ipv4** | **ipv6**｝ **unicast paths** ［*regular-expression*］

## 構文の説明

| | |
|---|---|
| *regular-expression* | （オプション）受信したパスの照合に使用される正規表現。 |
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |

### 例

次に、**show bgp ipv6 unicast paths** コマンドの出力例を示します。

```
> show bgp ipv6 unicast paths
Address    Hash Refcount Metric Path
0x61322A78    0        2      0 i
0x6131C214    3        2      0 6346 8664 786 i
0x6131D600   13        1      0 3748 1275 8319 1273 209 i
0x613229F0   17        1      0 3748 1275 8319 12853 i
0x61324AE0   18        1      1 4554 3748 4697 5408 i
0x61326818   32        1      1 4554 5609 i
0x61324728   34        1      0 6346 8664 9009 ?
0x61323804   35        1      0 3748 1275 8319 i
0x61327918   35        1      0 237 2839 8664 ?
0x61320504   38        2      0 3748 4697 1752 i
0x61320988   41        2      0 1849 786 i
0x6132245C   46        1      0 6346 8664 4927 i
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *7: Show bgp ipv4/ ipv6 unicast path* のフィールド

| フィールド | 説明 |
|---|---|
| アドレス（Address） | パスが保存される内部アドレス。 |
| Refcount | そのパスを使用しているルートの数。 |
| メトリック | パスの Multi Exit Discriminator（MED）メトリック（BGP バージョン 2 および 3 のこのメトリック名は INTER_AS です）。 |
| Path | そのルートの自律システム パスと、そのルートの発信元コード。 |

# show bgp ipv4/ ipv6 unicast prefix-list

プレフィックスリストに一致するルートを表示するには、**show bgp ipv4 prefix-list** コマンドまたは **show bgp ipv6 prefix-list** コマンドを使用します。

**show bgp** ［**vrf** *name* ｜ **all**］ ｛**ipv4** ｜ **ipv6**｝ **unicast prefix-list** *name*

## 構文の説明

| | |
|---|---|
| **prefix-list** *name* | 指定したプレフィックスリスト。 |
| ［**vrf** *name* ｜ **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* ｜ **all**］ キーワードが追加されました。 |

### 例

次に、**show bgp ipv6 prefix-list** コマンドの出力例を示します。

```
> show bgp ipv6 unicast prefix-list pin
ipv6 prefix-list pin:
   count:4, range entries:3, sequences:5 - 20, refcount:2
   seq 5 permit 747::/16 (hit count:1, refcount:2)
   seq 10 permit 747:1::/32 ge 64 le 64 (hit count:2, refcount:2)
   seq 15 permit 747::/32 ge 33 (hit count:1, refcount:1)
   seq 20 permit 777::/16 le 124 (hit count:2, refcount:1)
The ipv6 prefix-list match the following prefixes:
   seq 5: matches the exact match 747::/16
   seq 10:first 32 bits in prefix must match with a prefixlen of /64
   seq 15:first 32 bits in prefix must match with any prefixlen up to /128
   seq 20:first 16 bits in prefix must match with any prefixlen up to /124
```

# show bgp ipv4/ ipv6 unicast regexp

自律システムパスの正規表現と一致する IPv4 または IPv6 ボーダー ゲートウェイ プロトコル（BGP）ルートを表示するには、**show bgp ipv4 regexp** または **show bgp ipv6 regexp** コマンドを使用します。

**show bgp** ［**vrf** *name* | **all**］ ｛**ipv4** | **ipv6**｝ **unicast regexp** *regular-expression*

## 構文の説明

| | |
|---|---|
| **regexp** *regular-expression* | BGP 自律システム パスと一致させるために使用される正規表現。 |
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |

### 例

次に、**show bgp ipv6 unicast regexp** コマンドの出力例を示します。ここでは、33 で始まるパスまたは 293 を含むパスを示しています。出力の説明については、**show bgp** コマンドを参照してください。

```
> show bgp ipv6 unicast regexp ^33|293
BGP table version is 69964, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  2001:200::/35    3FFE:C00:E:4::2          1             0 4554 293 3425 2500 i
*                   2001:0DB8:0:F004::1                    0 3320 293 3425 2500 i
*  2001:208::/35    3FFE:C00:E:4::2          1             0 4554 293 7610 i
*  2001:228::/35    3FFE:C00:E:F::2                        0 6389 1849 293 2713 i
*  3FFE::/24        3FFE:C00:E:5::2                        0 33 1849 4554 i
*  3FFE:100::/24    3FFE:C00:E:5::2                        0 33 1849 3263 i
*  3FFE:300::/24    3FFE:C00:E:5::2                        0 33 293 1275 1717 i
*                   3FFE:C00:E:F::2                        0 6389 1849 293 1275
```

# show bgp ipv4/ ipv6 unicast route-map

ルーティングテーブルにインストールできなかった IPv4 または IPv6 ボーダー ゲートウェイ プロトコル（BGP）ルートを表示するには、**show bgp ipv4 unicast route-map** または **show bgp ipv6 unicast route-map** コマンドを使用します。

**show bgp** ［**vrf** *name* ｜ **all**］ ｛**ipv4** ｜ **ipv6**｝ **unicast route-map** *name*

## 構文の説明

| | |
|---|---|
| **route-map** *name* | 照合のために指定したルート マップ。 |
| ［**vrf** *name* ｜ **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* ｜ **all**］ キーワードが追加されました。 |

### 例

次に、rmap という名前のルートマップに対する **show bgp ipv6 unicast route-map** コマンドの出力例を示します。出力の説明については、**show bgp** コマンドを参照してください。

```
> show bgp ipv6 unicast route-map rmap
BGP table version is 16, local router ID is 172.30.242.1
Status codes:s suppressed, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*>i12:12::/64       2001:0DB8:101::1         0    100     50 ?
*>i12:13::/64       2001:0DB8:101::1         0    100     50 ?
*>i12:14::/64       2001:0DB8:101::1         0    100     50 ?
*>i543::/64         2001:0DB8:101::1         0    100     50 ?
```

# show bgp ipv4/ ipv6 unicast summary

すべての IPv4 または IPv6 ボーダー ゲートウェイ プロトコル（BGP）接続のステータスを表示するには、それぞれ **how bgp ipv4 unicast summary** または **show bgp ipv6 unicast summary** コマンドを使用します。

**show bgp** ［**vrf** *name* | **all**］ {**ipv4** | **ipv6**} **unicast summary**

## 構文の説明

| | |
|---|---|
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |

### 例

次に、**show bgp ipv6 unicast summary** コマンドの出力例を示します。

```
> show bgp ipv6 unicast summary
BGP device identifier 172.30.4.4, local AS number 200
BGP table version is 1, main routing table version 1
Neighbor          V    AS  MsgRcvd  MsgSent   TblVer  InQ  OutQ  Up/Down   State/PfxRcd
2001:0DB8:101::2   4    200    6869     6882        0    0     0  06:25:24  Active
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *8 : show bgp ipv4/ ipv6 unicast summary* のフィールド

| フィールド | 説明 |
|---|---|
| BGP device identifier | ネットワーキング デバイスの IP アドレス。 |
| BGP table version | テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。 |
| main routing table version | メイン ルーティング テーブルに注入された BGP データベースの最後のバージョン。 |
| Neighbor | ネイバーの IPv6 アドレス。 |

| フィールド | 説明 |
|---|---|
| V | ネイバーに通知される BGP バージョン番号。 |
| AS | Autonomous System |
| MsgRcvd | ネイバーから受信された BGP メッセージ。 |
| MsgSent | ネイバーに送信された BGP メッセージ。 |
| TblVer | ネイバーに送信された BGP データベースの最後のバージョン。 |
| InQ | 処理を待機しているネイバーからのメッセージの数。 |
| OutQ | ネイバーへの送信を待機しているメッセージの数。 |
| Up/Down | BGP セッションが確立状態となったか、確立されていない場合は現在の状態になった時間の長さ。 |
| State/PfxRcd | BGP セッションの現在の状態/デバイスがネイバーから受信したプレフィックスの数。最大数（neighbor maximum-prefix コマンドで設定）に達すると、文字列「PfxRcd」がエントリに表示され、ネイバーがシャットダウンされて、接続がアイドルになります。<br>アイドル ステータスの（管理者）エントリは、接続が neighbor shutdown コマンドを使用してシャットダウンされたことを示します。 |

# show bgp neighbors

ネイバーへのボーダー ゲートウェイ プロトコル（BGP）および TCP 接続に関する情報を表示するには、show bgp neighbors コマンドを使用します。

**show bgp neighbors** ［**vrf** *name* | **all**］ ［**slow** | *ip-address* ［**advertised-routes** | **paths** ［*reg-exp*］ | **policy** ［**detail**］ | **received prefix-filter** | **received-routes** | **routes**］］

## 構文の説明

| | |
|---|---|
| **slow** | （オプション）ダイナミックに設定された低速ピアに関する情報を表示します。 |
| *ip-address* | （オプション）IPv4 ネイバーに関する情報を表示します。この引数を省略すると、すべてのネイバーに関する情報が表示されます。 |
| **advertised-routes** | （オプション）ネイバーにアドバタイズされたすべてのルートを表示します。 |
| **paths** [*reg-exp*] | （オプション）指定したネイバーから学習した自律システムパスを表示します。オプションの正規表現を使用して、出力をフィルタ処理できます。 |
| **policy** | （オプション）アドレスファミリごとに、このネイバーに適用されるポリシーを表示します。 |
| **detail** | （オプション）ルートマップ、プレフィックスリスト、コミュニティリスト、アクセスコントロールリスト（ACL）、自律システムパスフィルタリストなどの詳細なポリシー情報を表示します。 |
| **received prefix-filter** | （オプション）指定したネイバーから送信されたプレフィックス リスト（アウトバウンド ルート フィルタ（ORF））を表示します。 |
| **received-routes** | （オプション）指定したネイバーから受信したすべてのルートを表示します。 |
| **routes** | （オプション）受信され、受け入れられるすべてのルートを表示します。このキーワードを入力したときに表示される出力は、**received-routes** キーワードによって表示される出力のサブセットです。 |
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## コマンド デフォルト

このコマンドの出力には、すべてのネイバーの情報が表示されます。

## 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。 |
| 6.6 | [**vrf** *name* \| **all**] キーワードが追加されました。 |

## 使用上のガイドライン

**show bgp neighbors** コマンドを使用して、ネイバーセッションの BGP および TCP 接続情報を表示します。BGP の場合、これには詳細なネイバー属性、機能、パス、およびプレフィックス情報が含まれています。TCP の場合、これには BGP ネイバー セッション確立およびメンテナンスに関連した統計が含まれています。

アドバタイズされ、取り消されたプレフィックスの数に基づいて、プレフィックスアクティビティが表示されます。ポリシー拒否には、アドバタイズされたものの、その後、出力に表示されている機能または属性に基づいて無視されたルートの数が表示されます。

### 例

次に、10.108.50.2 の BGP ネイバーの出力例を示します。このネイバーは、内部 BGP（iBGP）ピアです。ルート更新とグレースフル リスタート機能をサポートしています。

```
> show bgp neighbors 10.108.50.2
BGP neighbor is 10.108.50.2,  remote AS 1, internal link
  BGP version 4, remote router ID 192.168.252.252
  BGP state = Established, up for 00:24:25
  Last read 00:00:24, last write 00:00:24, hold time is 180, keepalive interval is
   60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    MPLS Label capability: advertised and received
    Graceful Restart Capability: advertised
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  3          3
    Notifications:          0          0
    Updates:                0          0
    Keepalives:           113        112
    Route Refresh:          0          0
    Total:                116        115
  Default minimum time between advertisement runs is 5 seconds

 For address family: IPv4 Unicast
  BGP additional-paths computation is enabled
  BGP advertise-best-external is enabled
  BGP table version 1, neighbor version 1/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
                                 Sent       Rcvd
  Prefix activity:               ----       ----
```

```
    Prefixes Current:               0          0
    Prefixes Total:                 0          0
    Implicit Withdraw:              0          0
    Explicit Withdraw:              0          0
    Used as bestpath:             n/a          0
    Used as multipath:            n/a          0

                                  Outbound    Inbound
  Local Policy Denied Prefixes:   --------    -------
    Total:                               0          0

  Number of NLRIs in the update sent: max 0, min 0

  Connections established 3; dropped 2
  Last reset 00:24:26, due to Peer closed the session
External BGP neighbor may be up to 2 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 10.108.50.1, Local port: 179
Foreign host: 10.108.50.2, Foreign port: 42698

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x68B944):
Timer          Starts    Wakeups            Next
Retrans            27          0             0x0
TimeWait            0          0             0x0
AckHold            27         18             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss: 3915509457  snduna: 3915510016  sndnxt: 3915510016     sndwnd:  15826
irs:  233567076  rcvnxt:  233567616  rcvwnd:      15845  delrcvwnd:    539

SRTT: 292 ms, RTTO: 359 ms, RTV: 67 ms, KRTT: 0 ms
minRTT: 12 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value : 6

Datagrams (max data segment is 1460 bytes):
Rcvd: 38 (out of order: 0), with data: 27, total data bytes: 539
Sent: 45 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 08
```

次の表に、この出力で表示される重要なフィールドの説明を示します。アスタリスク文字（*）の後ろにあるフィールドは、カウンタが非ゼロ値の場合だけ表示されます。

**表 *9 : show bgp neighbors* のフィールド**

| フィールド | 説明 |
|---|---|
| BGP neighbor | BGP ネイバーの IP アドレスとその自律システム番号。 |
| remote AS | ネイバーの自律システム番号。 |
| local AS 300 no-prepend（出力には表示されない） | ローカルの自律システム番号が受信された外部ルートの先頭に付加されていないことを確認します。この出力は、自律システムを移行しているときのローカル自律システムの非表示をサポートします。 |

| フィールド | 説明 |
|---|---|
| internal link | iBGP ネイバーの場合「internal link」と表示されます。外部 BGP（eBGP）ネイバーの場合は「external link」と表示されます。 |
| BGP version | リモート ルータとの通信に使用される BGP バージョン。 |
| remote router ID | ネイバーの IP アドレス。 |
| BGP state | セッション ネゴシエーションの有限状態マシン（FSM）ステージ。 |
| up for | ベースとなる TCP 接続が存在している時間（hhmmss 形式）。 |
| Last read | BGP がこのネイバーから最後にメッセージを受信してからの時間（hhmmss 形式）。 |
| last write | BGP がこのネイバーに最後にメッセージを送信してからの時間（hhmmss 形式）。 |
| hold time | BGP がメッセージを受信せずにこのネイバーとセッションを維持した時間（秒数）。 |
| keepalive interval | キープアライブ メッセージがこのネイバーに転送される間隔（秒数）。 |
| Neighbor capabilities | このネイバーからアドバタイズされ受信される BGP 機能。2 つのルータ間で機能が正常に交換されている場合、「advertised and received」が表示されます。 |
| Route Refresh | ルート リフレッシュ機能のステータス。 |
| Graceful Restart Capability | グレースフル リスタート機能のステータス。 |
| Address family IPv4 Unicast | このネイバーの IP Version 4 ユニキャスト固有プロパティ。 |
| Message statistics | メッセージ タイプごとにまとめられた統計。 |
| InQ depth is | 入力キュー内のメッセージ数。 |
| OutQ depth is | 出力キュー内のメッセージ数。 |
| Sent | 送信されたメッセージの合計数。 |
| Received | 受信されたメッセージの合計数。 |
| Opens | 送受信されたオープンメッセージ数。 |
| 通知 | 送受信された通知（エラー）メッセージ数。 |
| Updates | 送受信されたアップデートメッセージ数。 |

| フィールド | 説明 |
|---|---|
| Keepalives | 送受信されたキープアライブメッセージ数。 |
| Route Refresh | 送受信されたルートリフレッシュ要求メッセージ数。 |
| Total | 送受信されたメッセージの合計数。 |
| Default minimum time between... | アドバタイズメント送信の間の時間（秒数）。 |
| For address family: | 後続のフィールドが参照するアドレスファミリ。 |
| BGP table version | テーブルの内部バージョン番号。この番号は、テーブルが変更されるたびに増分します。 |
| neighbor version | 送信済みのプレフィックスおよび送信する必要があるプレフィックスを追跡するためにソフトウェアによって使用された番号。 |
| update-group | このアドレス ファミリのアップデート グループ メンバーの数。 |
| Prefix activity | このアドレスファミリのプレフィックス統計。 |
| Prefixes current | このアドレス ファミリに対して受け入れられるプレフィックス数。 |
| Prefixes total | 受信されたプレフィックスの合計数。 |
| Implicit Withdraw | プレフィックスが取り消されて再アドバタイズされた回数。 |
| Explicit Withdraw | フィージブルでなくなったため、プレフィックスが取り消された回数。 |
| Used as bestpath | 最適パスとしてインストールされた受信プレフィックス数。 |
| Used as multipath | マルチパスとしてインストールされた受信プレフィックス数。 |
| * Saved（ソフト再構成） | ソフト再構成をサポートするネイバーで実行されたソフトリセットの数。このフィールドは、カウンタが非ゼロ値の場合のみ表示されます。 |
| * History paths | このフィールドは、カウンタが非ゼロ値の場合のみ表示されます。 |
| * Invalid paths | 無効なパスの数。このフィールドは、カウンタが非ゼロ値の場合のみ表示されます。 |
| Local Policy Denied Prefixes | ローカルポリシー設定が原因で拒否されたプレフィックス。カウンタは、インバウンドおよびアウトバウンドのポリシー拒否ごとに更新されます。この見出しの下のフィールドは、カウンタの値がゼロ以外である場合にだけ表示されます。 |
| * route-map | インバウンドおよびアウトバウンドのルートマップポリシー拒否を表示します。 |

| フィールド | 説明 |
|---|---|
| * filter-list | インバウンドおよびアウトバウンドのフィルタリストポリシー拒否を表示します。 |
| * prefix-list | インバウンドおよびアウトバウンドのプレフィックスリストポリシー拒否を表示します。 |
| * AS_PATH too long | アウトバウンドの AS パス長ポリシー拒否を表示します。 |
| * AS_PATH loop | アウトバウンドの AS パス ループ ポリシー拒否を表示します。 |
| * AS_PATH confed info | アウトバウンド コンフェデレーション ポリシー拒否を表示します。 |
| * AS_PATH contains AS 0 | 自律システム（AS）0 のアウトバウンド拒否を表示します。 |
| * NEXT_HOP Martian | アウトバウンドの Martian 拒否を表示します。 |
| * NEXT_HOP non-local | アウトバウンドの非ローカル ネクスト ホップ拒否を表示します。 |
| * NEXT_HOP is us | アウトバウンドのネクストホップ自身の拒否を表示します。 |
| * CLUSTER_LIST loop | アウトバウンドのクラスタリスト ループ拒否を表示します。 |
| * ORIGINATOR loop | ローカルで発信されたルートのアウトバウンド拒否を表示します。 |
| * unsuppress-map | 抑制マップによるインバウンド拒否を表示します。 |
| * advertise-map | アドバタイズ マップによるインバウンド拒否を表示します。 |
| * Well-known Community | ウェルノウン コミュニティのインバウンド拒否を表示します。 |
| * SOO loop | site-of-origin によるインバウンド拒否を表示します。 |
| * Bestpath from this peer | 最適パスがローカルルータから提供されたことによるインバウンド拒否を表示します。 |
| * Suppressed due to dampening | ネイバーまたはリンクがダンプニング状態であることによるインバウンド拒否を表示します。 |
| * Bestpath from iBGP peer | 最適パスが iBGP ネイバーから提供されたことによるインバウンド拒否を表示します。 |
| * Incorrect RIB for CE | CE ルータの RIB エラーによるインバウンド拒否を表示します。 |

| フィールド | 説明 |
|---|---|
| * BGP distribute-list | 配布リストによるインバウンド拒否を表示します。 |
| Number of NLRIs... | アップデート内のネットワーク層到達可能性属性の数。 |
| Connections established | TCP および BGP 接続が正常に確立した回数。 |
| dropped | 有効セッションに障害が発生したか停止した回数。 |
| Last reset | このピアリングセッションが最後にリセットされてからの時間。リセットがこの行に表示された理由。 |
| External BGP neighbor may be...（出力には表示されない） | BGP TTL セキュリティ チェックがイネーブルであることを示します。ローカルピアとリモートピアをまたぐことができるホップの最大数がこの行に表示されます。 |
| Connection state | BGP ピアの接続ステータス。 |
| Connection is ECN Disabled | 明示的輻輳通知のステータス（イネーブルまたはディセーブル）。 |
| Local host: 10.108.50.1, Local port: 179 | ローカル BGP スピーカーの IP アドレス。BGP ポート番号 179。 |
| Foreign host: 10.108.50.2, Foreign port: 42698 | ネイバーアドレスと BGP 宛先ポート番号。 |
| Enqueued packets for retransmit: | TCP によって再送信のためにキューに格納されたパケット。 |
| Event Timers | TCPイベントタイマー。起動およびウェイクアップのカウンタが提供されます（期限切れタイマー）。 |
| Retrans | パケットを再送信した回数。 |
| TimeWait | 再送信タイマーが期限切れになるまで待機する時間。 |
| AckHold | 確認応答ホールドタイマー |
| SendWnd | 伝送（送信）ウィンドウ。 |
| KeepAlive | キープアライブパケットの数。 |
| GiveUp | 確認応答がないためにパケットがドロップされた回数。 |
| PmtuAger | パス MTU ディスカバリ タイマー。 |

| フィールド | 説明 |
|---|---|
| DeadWait | デッドセグメントの有効期限タイマー。 |
| iss: | 初期パケット送信シーケンス番号。 |
| snduna | 確認応答されなかった最後の送信シーケンス番号。 |
| sndnxt: | 次に送信されるパケットのシーケンス番号。 |
| sndwnd: | リモートネイバーの TCP ウィンドウ サイズ。 |
| irs: | 初期パケット受信シーケンス番号。 |
| rcvnxt: | ローカルに確認応答された最後の受信シーケンス番号。 |
| rcvwnd: | ローカルホストの TCP ウィンドウサイズ。 |
| delrcvwnd: | 遅延受信ウィンドウ：ローカルホストによって接続から読み取られ、ホストがリモートホストにアドバタイズした受信ウィンドウから削除されていないデータ。このフィールドの値は、フルサイズのパケットより大きくなるまで次第に増加し、それに達した時点で、rcvwnd フィールドに適用されます。 |
| SRTT: | 計算されたスムーズ ラウンドトリップ タイムアウト。 |
| RTTO: | ラウンドトリップ タイムアウト。 |
| RTV: | ラウンドトリップ時間の差異。 |
| KRTT: | 新しいラウンドトリップ タイムアウト（Karn アルゴリズムを使用）。このフィールドは、再送信されたパケットのラウンドトリップ時間を個別に追跡します。 |
| minRTT: | 記録された最小ラウンドトリップ タイムアウト（計算に使用される組み込み値）。 |
| maxRTT: | 記録された最大ラウンドトリップ タイムアウト。 |
| ACK hold: | ローカルホストが追加データを伝送（ピギーバック）するために確認応答を遅らせる時間の長さ。 |
| IP Precedence value: | BGP パケットの IP プレシデンス。 |
| Datagrams | ネイバーから受信したアップデートパケットの数。 |
| Rcvd: | 受信パケット数。 |
| with data | データとともに送信されたアップデートパケットの数。 |
| total data bytes | 受信データの合計量（バイト）。 |

| フィールド | 説明 |
|---|---|
| Sent | 送信されたアップデートパケットの数。 |
| Second Congestion | 輻輳による再送信に要した秒数。 |
| Datagrams: Rcvd | ネイバーから受信したアップデートパケットの数。 |
| out of order: | シーケンスを外れて受信したパケットの数。 |
| with data | データとともに受信したアップデート パケットの数。 |
| Last reset | このピアリング セッションが最後にリセットされてからの経過時間。 |
| unread input bytes | 処理待ちのパケットのバイト数。 |
| retransmit | 再送信されたパケット数。 |
| fastretransmit | 再送信タイマーが期限切れになる前に、順序が不正なセグメントのために再送信された重複する確認応答の数。 |
| partialack | 部分的な確認応答（後続の確認応答がない、またはそれ以前の送信）のために再送信された回数。 |

次に、172.16.232.178 ネイバーのみにアドバタイズされたルートを表示する例を示します。出力の説明については、**show bgp** コマンドを参照してください。

```
> show bgp neighbors 172.16.232.178 advertised-routes
BGP table version is 27, local router ID is 172.16.232.181
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop          Metric LocPrf Weight Path
*>i10.0.0.0      172.16.232.179         0    100      0 ?
*> 10.20.2.0     10.0.0.0               0         32768 i
```

次に、**paths** キーワードを指定した **show bgp neighbors** コマンドの出力例を示します。

```
> show bgp neighbors 172.29.232.178 paths ^10
Address    Refcount Metric Path
0x60E577B0        2     40 10 ?
```

次の表では、各フィールドについて説明されています。

***表 10 : show bgp neighbors paths* のフィールド**

| フィールド | 説明 |
|---|---|
| アドレス（Address） | パスが保存される内部アドレス。 |
| Refcount | そのパスを使用しているルートの数。 |

| フィールド | 説明 |
|---|---|
| メトリック | パスの Multi Exit Discriminator（MED）メトリック（BGP バージョン 2 および 3 のこのメトリック名は INTER_AS です）。 |
| パス | そのルートの自律システム パスと、そのルートの発信元コード。 |

次の例は、10.0.0.0 ネットワークのすべてのルートをフィルタリングするプレフィックス リストが 192.168.20.72 ネイバーから受信されたことを示しています。

```
> show bgp neighbors 192.168.20.72 received prefix-filter
Address family:IPv4 Unicast
ip prefix-list 192.168.20.72:1 entries
   seq 5 deny 10.0.0.0/8 le 32
```

次の出力例に表示されているのは、192.168.1.2 にあるネイバーに適用されたポリシーです。ネイバー デバイスで設定されたポリシーが表示されます。

```
> show bgp neighbors 192.168.1.2 policy
Neighbor: 192.168.1.2, Address-Family: IPv4 Unicast
Locally configured policies:
 route-map ROUTE in
Inherited polices:
 prefix-list NO-MARKETING in
 route-map ROUTE in
 weight 300
 maximum-prefix 10000
```

次に、**show bgp neighbors** コマンドの出力例を示します。ここでは、BGP TCP パス最大伝送ユニット（MTU）ディスカバリが 172.16.1.2 にある BGP ネイバーに対して有効になっていることを確認します。

```
> show bgp neighbors 172.16.1.2
BGP neighbor is 172.16.1.2,  remote AS 45000, internal link
  BGP version 4, remote router ID 172.16.1.99
....
 For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5/0
...
  Address tracking is enabled, the RIB does have a route to 172.16.1.2
  Address tracking requires at least a /24 route to the peer
  Connections established 3; dropped 2
  Last reset 00:00:35, due to Router ID changed
  Transport(tcp) path-mtu-discovery is enabled
....
SRTT: 146 ms, RTTO: 1283 ms, RTV: 1137 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle, path mtu capable
```

# show bgp paths

データベース内のすべてのBGPパスを表示するには、**show bgp paths**コマンドを使用します。

**show bgp paths** ［**vrf** *name* | **all**］ ［*regexp*］

## 構文の説明

| | |
|---|---|
| *regexp* | BGP 自律システム パスと一致する正規表現。 |
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name*キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |

### 例

次に、**show bgp paths** コマンドの出力例を示します。

```
> show bgp paths
Address    Hash Refcount Metric Path
0x60E5742C    0        1      0 i
0x60E3D7AC    2        1      0 ?
0x60E5C6C0   11        3      0 10 ?
0x60E577B0   35        2     40 10 ?
```

次の表で各フィールドについて説明します。

**表 *11 : show bgp paths* のフィールド**

| フィールド | 説明 |
|---|---|
| アドレス（Address） | パスが保存される内部アドレス。 |
| Hash | パスが格納されているハッシュ バケット。 |
| Refcount | そのパスを使用しているルートの数。 |
| メトリック | パスの Multi Exit Discriminator（MED）メトリック（BGP バージョン 2 および 3 のこのメトリック名は INTER_AS です）。 |

| フィールド | 説明 |
| --- | --- |
| Path | そのルートの自律システム パスと、そのルートの発信元コード。 |

# show bgp prefix-list

プレフィックスリストまたはプレフィックスリストのエントリに関する情報を表示するには、**show bgp prefix-list** コマンドを使用します。

**show bgp prefix-list** ［**vrf** *name* ｜ **all**］ ［**detail** ｜ **summary**］［*prefix-list-name* ［**seq** *sequence-number* ｜ *network/length* ［**longer** ｜ **first-match**］］］

## 構文の説明

| | |
|---|---|
| **detail** ｜ **summary** | （オプション）すべてのプレフィックス リストに関する詳細情報または要約情報を表示します。 |
| **first-match** | （オプション）指定した network/length と一致する、指定したプレフィックス リストの最初のエントリを表示します。 |
| **longer** | （オプション）指定した network/length と一致するか、またはより限定的な、プレフィックス リストのすべてのエントリを表示します。 |
| *network/length* | （オプション）このネットワーク アドレスおよびネットマスク長（ビット単位）を使用する、指定したプレフィックス リストのすべてのエントリを表示します。 |
| *prefix-list-name* | （オプション）特定のプレフィックス リストのエントリを表示します。 |
| **seq** *sequence-number* | （オプション）指定したプレフィックス リストに指定したシーケンス番号があるプレフィックス リスト エントリだけを表示します。 |
| ［**vrf** *name* ｜ **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* ｜ **all**］ キーワードが追加されました。 |

### 例

次に、**show bgp prefix-list** コマンドの出力例を示します。ここでは、test という名前のプレフィックスリストの詳細を示しています。

```
> show bgp prefix-list detail test
ip prefix-list test:
Description: test-list
 count: 1, range entries: 0, sequences: 10 - 10, refcount: 3
 seq 10 permit 10.0.0.0/8 (hit count: 0, refcount: 1)
```

# show bgp regexp

自律システムパスの正規表現と一致するルートを表示するには、**show bgp regexp** コマンドを使用します。

**show bgp regexp** ［**vrf** *name* | **all**］ *regexp*

## 構文の説明

| | |
|---|---|
| *regexp* | BGP 自律システム パスと一致する正規表現。 |
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |

### 例

次に、**show bgp regexp** コマンドの出力例を示します。

```
> show bgp regexp 108$
BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
*  172.16.0.0       172.16.72.30                           0 109 108 ?
*  172.16.1.0       172.16.72.30                           0 109 108 ?
*  172.16.11.0      172.16.72.30                           0 109 108 ?
*  172.16.14.0      172.16.72.30                           0 109 108 ?
*  172.16.15.0      172.16.72.30                           0 109 108 ?
*  172.16.16.0      172.16.72.30                           0 109 108 ?
*  172.16.17.0      172.16.72.30                           0 109 108 ?
*  172.16.18.0      172.16.72.30                           0 109 108 ?
*  172.16.19.0      172.16.72.30                           0 109 108 ?
*  172.16.24.0      172.16.72.30                           0 109 108 ?
*  172.16.29.0      172.16.72.30                           0 109 108 ?
*  172.16.30.0      172.16.72.30                           0 109 108 ?
*  172.16.33.0      172.16.72.30                           0 109 108 ?
*  172.16.35.0      172.16.72.30                           0 109 108 ?
*  172.16.36.0      172.16.72.30                           0 109 108 ?
*  172.16.37.0      172.16.72.30                           0 109 108 ?
*  172.16.38.0      172.16.72.30                           0 109 108 ?
*  172.16.39.0      172.16.72.30                           0 109 108 ?
```

# show bgp rib-failure

ルーティング情報ベース（RIB）テーブルへの登録に失敗したボーダー ゲートウェイ プロトコル（BGP）ルートを表示するには、**show bgp rib-failure** コマンドを使用します。

**show bgp rib-failure** ［**vrf** *name* | **all**］

## 構文の説明

| | |
|---|---|
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |

### 例

次に、**show bgp rib-failure** コマンドの出力例を示します。

```
> show bgp rib-failure
Network           Next Hop                    RIB-failure   RIB-NH Matches
10.1.15.0/24      10.1.35.5          Higher admin distance             n/a
10.1.16.0/24      10.1.15.1          Higher admin distance             n/a
```

次の表では、各フィールドについて説明されています。

**表 *12 : show bgp rib-failure* のフィールド**

| フィールド | 説明 |
|---|---|
| ネットワーク | ネットワーク エンティティの IP アドレス。 |
| Next Hop | パケットを宛先ネットワークに転送するときに使用される次のシステムの IP アドレス。0.0.0.0 のエントリは、ルータにこのネットワークへの非 BGP ルートがあることを示します。 |
| RIB-failure | RIB 失敗の原因。アドミニストレイティブ ディスタンスが高いということは、スタティック ルートなど優れた（低い）アドミニストレーティブ ディスタンスを持つルートが IP ルーティング テーブルにすでにあることを意味します。 |

| フィールド | 説明 |
|---|---|
| RIB-NH Matches | より高いアドミニストレーティブ ディスタンスが RIB-failure 列に表示されていて、使用されているアドレスファミリに対して **bgp suppress-inactive** が設定されている場合にだけ適用されるルートステータス。次の 3 種類があります。<br>• [Yes]：RIB のルートに BGP ルートと同じネクスト ホップがあるか、またはネクスト ホップが BGP ネクスト ホップと同じ隣接に再帰することを意味します。<br>• [No]：RIB のネクスト ホップが BGP ルートのネクスト ホップとは別に再帰することを意味します。<br>• [n/a]：使用されているアドレスファミリに対して **bgp suppress-inactive** が設定されないことを意味します。 |

# show bgp summary

すべてのボーダー ゲートウェイ プロトコル（BGP）接続のステータスを表示するには、**show bgp summary** コマンドを使用します。

**show bgp summary** ［**vrf** *name* | **all**］

## 構文の説明

| | |
|---|---|
| ［**vrf** *name* \| **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* \| **all**］ キーワードが追加されました。 |

## 使用上のガイドライン

**show bgp summary** コマンドは、BGP ネイバーへのすべての接続に関する BGP パス、プレフィックス、および属性情報を表示するために使用します。

プレフィックスは、IP アドレスとネットワーク マスクです。これはネットワーク全体、ネットワークのサブセット、または単一のホストルートを表すことができます。パスは、所定の宛先へのルートです。デフォルトでは、BGP は宛先ごとに 1 つのパスだけをインストールします。マルチパス ルートが設定されている場合、BGP は各マルチパス ルートにパス エントリをインストールし、1 つのマルチパス ルートにのみ最適パスとマークされます。

BGP 属性とキャッシュ エントリは個別にも組み合わせても表示され、これは最適パス選択プロセスに影響を与えます。この出力のフィールドは、関連する BGP 機能が設定されているか、または属性が受信されたときに表示されます。メモリ使用量はバイト単位で表示されます。

### 例

次に、特権 EXEC モードでの **show bgp summary** コマンドからの出力例を示します。

```
> show bgp summary
BGP router identifier 172.16.1.1, local AS number 100
BGP table version is 199, main routing table version 199
37 network entries using 2850 bytes of memory
59 path entries using 5713 bytes of memory
18 BGP path attribute entries using 936 bytes of memory
2 multipath network entries and 4 multipath paths
10 BGP AS-PATH entries using 240 bytes of memory
7 BGP community entries using 168 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
```

```
90 BGP advertise-bit cache entries using 1784 bytes of memory
36 received paths for inbound soft reconfiguration
BGP using 34249 total bytes of memory
Dampening enabled. 4 history paths, 0 dampened paths
BGP activity 37/2849 prefixes, 60/1 paths, scan interval 15 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down State/PfxRcd
10.100.1.1      4   200      26      22      199    0    0 00:14:23 23
10.200.1.1      4   300      21      51      199    0    0 00:13:40 0
```

次の表で各フィールドについて説明します。

**表 *13 : show bgp summary* のフィールド**

| フィールド | 説明 |
|---|---|
| BGP router identifier | 優先度と可用性の順序で表示されたルータ ID、ループバックアドレス、または最上位 IP アドレス。 |
| BGP table version | BGP データベースの内部バージョン番号。 |
| main routing table version | メイン ルーティング テーブルに注入された BGP データベースの最後のバージョン。 |
| ...network entries | BGP データベースの一意のプレフィックス エントリの数。 |
| ...using ... bytes of memory | 同じ行のパス、プレフィックス、または属性のエントリのために消費されているメモリ量（バイト単位）。 |
| ...path entries using | BGP データベースのパス エントリの数。単一のパス エントリだけが特定の宛先にインストールされます。マルチパス ルートが設定されている場合、マルチパス ルートごとにパス エントリがインストールされます。 |
| ...multipath network entries using | 特定の宛先にインストールされているマルチパス エントリの数。 |
| * ...BGP path/bestpath attribute entries using | パスが最適パスとして選択されている一意の BGP 属性の組み合わせの数。 |
| * ...BGP rrinfo entries using | ORIGINATOR 属性と CLUSTER_LIST 属性の一意の組み合わせの数。 |
| ...BGP AS-PATH entries using | 一意の AS_PATH エントリの数。 |
| ...BGP community entries using | BGP コミュニティ属性の一意の組み合わせの数。 |
| *...BGP extended community entries using | 拡張コミュニティ属性の一意の組み合わせの数。 |

| フィールド | 説明 |
|---|---|
| BGP route-map cache entries using | BGP ルート マップの match 句と set 句の組み合わせの数。値が 0 の場合、ルート キャッシュが空であることを示します。 |
| ...BGP filter-list cache entries using | AS パス アクセス リストの permit ステートメントまたは deny ステートメントに一致するフィルタ リスト エントリの数。値が 0 の場合、フィルタ リスト キャッシュが空であることを示します。 |
| BGP advertise-bit cache entries using | アドバタイズされたビットフィールドエントリの数および関連するメモリ使用量。ビットフィールドエントリは、プレフィックスがピアにアドバタイズされるときに生成される情報（1 ビット）を表します。アドバタイズされたビットキャッシュは、必要に応じてダイナミックに作成されます。 |
| ...received paths for inbound soft reconfiguration | インバウンド ソフト再構成のために受信され保存されるパスの数。 |
| BGP using... | BGP プロセスによって使用されるメモリの総量（バイト単位）。 |
| Dampening enabled... | BGP ダンプニングがイネーブルであることを示します。この行には、累積ペナルティを伝送するパスの数およびダンプニングされたパスの数が表示されます。 |
| BGP activity... | パスまたはプレフィックスに対してメモリが割り当てられたか、または解放された回数を表示します。 |
| Neighbor | ネイバーの IP アドレス。 |
| V | ネイバーに通知される BGP バージョン番号。 |
| AS | 自律システム（AS）番号。 |
| MsgRcvd | ネイバーから受信されたメッセージ数。 |
| MsgSent | ネイバーに送信されたメッセージ数。 |
| TblVer | ネイバーに送信された BGP データベースの最終バージョン。 |
| InQ | ネイバーで処理するためにキューに格納されたメッセージ数。 |
| OutQ | ネイバーに送信するために、キューに格納されたメッセージ数。 |
| Up/Down | BGP セッションが確立状態となったか、確立状態ではない場合は現在の状態になった時間の長さ。 |

| フィールド | 説明 |
|---|---|
| State/PfxRcd | BGP セッションの現在の状態と、ネイバーまたはピア グループから受信されたプレフィックスの数。最大数に達すると、文字列「PfxRcd」がエントリに表示され、ネイバーがシャットダウンされて、接続がアイドルに設定されます。<br>アイドルステータスの（管理者）エントリは、接続がシャットダウンされたことを示します。 |

**show bgp summary** コマンドの次の出力は、BGP ネイバー 192.168.3.2 が、ダイナミックに作成されたもので、受信範囲グループ group192 のメンバであることを示します。この出力は、IP プレフィックス範囲 192.168.0.0/16 がグループ 192 という名前の受信範囲グループに定義されることも示します。

```
> show bgp summary
BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
*192.168.3.2    4 50000       2       2        0    0    0 00:00:37        0
* Dynamically created based on a listen range command
Dynamically created neighbors: 1/(200 max), Subnet ranges: 1

BGP peergroup group192 listen range group members:
  192.168.0.0/16
```

**show bgp summary** コマンドの次の出力は、4 バイトの異なる自律システム番号（65536 および 65550）の 2 つの BGP ネイバー（192.168.1.2 および 192.168.3.2）を示しています。ローカルな自律システム 65538 は、4 バイト自律システム番号でもあり、その番号はデフォルトの asplain 形式で表示されます。

```
> show bgp summary
BGP router identifier 172.17.1.99, local AS number 65538
BGP table version is 1, main routing table version 1
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4       65536       7       7        1    0    0 00:03:04      0
192.168.3.2     4       65550       4       4        1    0    0 00:00:15      0
```

**show bgp summary** コマンドの次の出力は同じ 2 つの BGP ネイバーを示していますが、4 バイト自律システム番号は asdot 表記法の形式で表示されます。

```
> show bgp summary
BGP router identifier 172.17.1.99, local AS number 1.2
BGP table version is 1, main routing table version 1
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4         1.0       9       9        1    0    0 00:04:13      0
192.168.3.2     4        1.14       6       6        1    0    0 00:01:24      0
```

# show bgp update-group

BGP アップデートグループに関する情報を表示するには、**show bgp update-group** コマンドを使用します。

**show bgp update-group** ［**vrf** *name* | **all**］ ［*index-group* | *ip-address*］［**summary**］

## 構文の説明

| | |
|---|---|
| *index-group* | （任意）対応するインデックス番号でグループタイプを更新します。アップデート グループのインデックス番号の範囲は 1 ～ 4294967295 です。 |
| *ip-address* | （任意）アップデートグループのメンバーである単一のネイバーの IP アドレス。 |
| **summary** | （任意）アップデートグループのメンバー情報のサマリーを表示します。出力をフィルタ処理することで、index-group または ip-address 引数を使用して単一のインデックスグループまたはピアの情報を表示することができます。 |
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |

## 使用上のガイドライン

このコマンドは、BGPアップデートグループに関する情報を表示するために使用します。BGP アウトバウンドポリシーが変更された場合、ルータは、1 分間のタイマー期限が切れた後で、アウトバウンド ソフト リセットをトリガーすることにより、自動的にアップデート グループ メンバーシップを再計算し、変更を適用します。この動作は、ネットワーク オペレータがミスを犯した場合に、コンフィギュレーションを変更する時間を与えるように設計されています。

### 例

次の **show bgp update-group** コマンドからの出力例には、すべてのネイバーに関するアップデートグループ情報が表示されます。

```
> show bgp update-group
BGP version 4 update-group 1, internal, Address Family: IPv4 Unicast
```

```
  BGP Update version : 0, messages 0/0
  Route map for outgoing advertisements is COST1
  Update messages formatted 0, replicated 0
  Number of NLRIs in the update sent: max 0, min 0
  Minimum time between advertisement runs is 5 seconds
  Has 1 member:
  10.4.9.21
BGP version 4 update-group 2, internal, Address Family: IPv4 Unicast
  BGP Update version : 0, messages 0/0
  Update messages formatted 0, replicated 0
  Number of NLRIs in the update sent: max 0, min 0
  Minimum time between advertisement runs is 5 seconds
  Has 2 members:
  10.4.9.5 10.4.9.8
```

次の表で各フィールドについて説明します。

**表 *14 : show bgp update-group* フィールド**

| フィールド | 説明 |
|---|---|
| BGP version | BGP バージョン。 |
| update-group | アップデートグループの番号とタイプ（内部または外部）。 |
| update messages formatted..., replicated... | フォーマットされ、複製されたアップデートメッセージの数。 |
| Number of NLRIs... | アップデートで送信された NLRI 情報。 |
| .Minimum time between... | 同じ行のパス、プレフィックス、または属性のエントリのために消費されているメモリ量（バイト単位）。 |
| ...path entries using | BGP データベースのパス エントリの数。単一のパス エントリだけが特定の宛先にインストールされます。マルチパス ルートが設定されている場合、マルチパス ルートごとにパス エントリがインストールされます。 |
| ...multipath network entries using | 特定の宛先にインストールされているマルチパス エントリの数。 |
| * ...BGP path/bestpath attribute entries using | パスが最適パスとして選択されている一意の BGP 属性の組み合わせの数。 |
| * ...BGP rrinfo entries using | ORIGINATOR 属性と CLUSTER_LIST 属性の一意の組み合わせの数。 |
| ...BGP AS-PATH entries using | 一意の AS_PATH エントリの数。 |
| ...BGP community entries using | BGP コミュニティ属性の一意の組み合わせの数。 |

| フィールド | 説明 |
|---|---|
| *...BGP extended community entries using | 拡張コミュニティ属性の一意の組み合わせの数。 |
| BGP route-map cache entries using | BGP ルート マップの match 句と set 句の組み合わせの数。値が 0 の場合、ルート キャッシュが空であることを示します。 |
| ...BGP filter-list cache entries using | AS パス アクセス リストの permit ステートメントまたは deny ステートメントに一致するフィルタ リスト エントリの数。値が 0 の場合、フィルタ リスト キャッシュが空であることを示します。 |
| BGP advertise-bit cache entries using | アドバタイズされたビットフィールドエントリの数および関連するメモリ使用量。ビットフィールドエントリは、プレフィックスがピアにアドバタイズされるときに生成される情報（1 ビット）を表します。アドバタイズされたビットキャッシュは、必要に応じてダイナミックに作成されます。 |
| ...received paths for inbound soft reconfiguration | インバウンド ソフト再構成のために受信され保存されるパスの数。 |
| BGP using... | BGP プロセスによって使用されるメモリの総量（バイト単位）。 |
| Dampening enabled... | BGP ダンプニングがイネーブルであることを示します。この行には、累積ペナルティを伝送するパスの数およびダンプニングされたパスの数が表示されます。 |
| BGP activity... | パスまたはプレフィックスに対してメモリが割り当てられたか、または解放された回数を表示します。 |
| Neighbor | ネイバーの IP アドレス。 |
| V | ネイバーに通知される BGP バージョン番号。 |
| AS | 自律システム（AS）番号。 |
| MsgRcvd | ネイバーから受信されたメッセージ数。 |
| MsgSent | ネイバーに送信されたメッセージ数。 |
| TblVer | ネイバーに送信された BGP データベースの最終バージョン。 |
| InQ | ネイバーで処理するためにキューに格納されたメッセージ数。 |
| OutQ | ネイバーに送信するために、キューに格納されたメッセージ数。 |
| Up/Down | BGP セッションが確立状態となったか、確立状態ではない場合は現在の状態になった時間の長さ。 |

| フィールド | 説明 |
| --- | --- |
| State/PfxRcd | BGP セッションの現在の状態と、ネイバーまたはピア グループから受信されたプレフィックスの数。最大数に達すると、文字列「PfxRcd」がエントリに表示され、ネイバーがシャットダウンされて、接続がアイドルに設定されます。<br>アイドルステータスの（管理者）エントリは、接続がシャットダウンされたことを示します。 |

# show blocks

システムバッファの使用率を表示するには、**show blocks** コマンドを使用します。

**show blocks** ［**core** | **export-failed** | **interface**］
**show blocks address** *hex* ［**diagnostics** | **dump** | **header** | **packet**］
**show blocks** ｛**all** | **assigned** | **free** | **old**｝［**core-local** ［*core-num*］［**diagnostics** | **dump** | **header** | **packet**］］
**show blocks exhaustion** ｛**history** ［**list** | *snapshot_num*］ | **snapshot**｝
**show blocks pool** *block-size*
**show blocks queue history** ［**core-local** ［*core-num*］］［**detail**］

## 構文の説明

| | |
|---|---|
| **address***hex* | （任意）このアドレスに対応するブロックを 16 進数形式で表示します。 |
| **all** | （任意）すべてのブロックを表示します。 |
| **assigned** | （任意）割り当て済みでアプリケーションによって使用されているブロックを表示します。 |
| **core** | （任意）コア固有のバッファを表示します。 |
| **core-local** [*core-num*] | （任意）すべてのコアのシステムバッファを表示します。コア番号（1 など）を指定して、特定のコアのバッファを表示することもできます。 |
| **detail** | （任意）一意のキュータイプごとに最初のブロックの一部（128 バイト）を表示します。 |
| **dump** | （任意）ヘッダーとパケットの情報を含め、ブロックの内容全体を表示します。dump と packet の相違点は、dump の場合、ヘッダーとパケットに関する追加情報が含まれることです。 |
| **diagnostics** | （任意）ブロックの診断を表示します。 |
| **exhaustion snapshot** | （オプション）取得されたスナップショットの最後の x 番号（x は現時点では 10）および最後のスナップショットのタイムスタンプを出力します。スナップショットが取得された後、5 分以上経過しないと別のスナップショットは取得されません。 |
| **exhaustion history** [**list** \| *snapshot_num*] | （任意）枯渇スナップショットの履歴を表示します。スナップショット番号を指定して情報を 1 つのスナップショットに制限したり、リストを使用してスナップショットの **list** を表示したりできます。 |
| **export-failed** | （任意）システム バッファ エクスポートの失敗カウンタを表示します。 |

| | |
|---|---|
| **free** | （任意）使用可能なブロックを表示します。 |
| **header** | （任意）ブロックのヘッダーを表示します。 |
| **interface** | （任意）インターフェイスに付加されているバッファを表示します。 |
| **old** | （任意）1分よりも前に割り当てられたブロックを表示します。 |
| **packet** | （任意）ブロックのヘッダーおよびパケットの内容を表示します。 |
| **pool** *block-size* | （任意）特定のサイズのブロックを表示します。 |
| **queue history** | （任意）脅威に対する防御 デバイスがブロックを使い果たしたときに、ブロックが割り当てられる位置を表示します。プール内のブロックが割り当てられることはありますが、ブロックがキューに割り当てられることはありません。この場合は、ブロックを割り当てたコードのアドレスが割り当て場所になります。 |

## 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。 |
| 7.0(1) | 失敗数を含むようにこのコマンドの出力が拡張されました。 |

## 使用上のガイドライン

**show blocks** コマンドは、脅威に対する防御 デバイスが過負荷になっているかどうかを判断する場合に役立ちます。このコマンドは、事前割り当て済みのシステムバッファの使用状況を表示します。トラフィックが 脅威に対する防御 デバイス経由で伝送されている限り、メモリがいっぱいになっている状態は問題にはなりません。**show conn** コマンドを使用すると、トラフィックが伝送されているかどうかを確認できます。トラフィックが伝送されておらず、かつメモリがいっぱいになっている場合は、問題がある可能性があります。この情報は、SNMP を使用して表示することもできます。

### 例

次に、**show blocks** コマンドの出力例を示します。

```
> show blocks
  SIZE    MAX    LOW    CNT    FAILED
     0   1450   1450   1450       0
     4    100     99     99       0
    80   1996   1992   1992       0
   256   4148   4135   4142       0
  1550   6274   6270   6272       0
  2048    100    100    100       0
  2560    164    164    164       0
  4096    100    100    100       0
  8192    100    100    100       0
  9344    100    100    100       0
```

```
16384     100     100     100        0
65536      16      16      16        0
```

次の表で各フィールドについて説明します。

**表 *15 : show blocks* のフィールド**

| フィールド | 説明 |
|---|---|
| SIZE | ブロック プールのサイズ（バイト単位）。それぞれのサイズは、特定のタイプを表しています。 |
| 0 | dupb ブロックで使用されます。 |
| 4 | DNS、ISAKMP、URL フィルタリング、uauth、TFTP、TCP モジュールなどのアプリケーションの既存ブロックを複製します。またこのサイズのブロックは、通常、パケットをドライバに送信するコードなどで使用されます。 |
| 80 | TCP 代行受信で確認応答パケットを生成するために、およびフェールオーバー hello メッセージに使用されます。 |
| 256 | ステートフル フェールオーバーの更新、syslog 処理、およびその他の TCP 機能に使用されます。<br><br>これらのブロックは、主にステートフル フェールオーバーのメッセージに使用されます。アクティブな 脅威に対する防御 デバイスは、パケットを生成してスタンバイ状態の 脅威に対する防御 デバイスに送信し、変換と接続のテーブルを更新します。接続が頻繁に作成または切断されるバースト トラフィックが発生すると、使用可能なブロックの数が 0 まで低下することがあります。この状況は、1 つ以上の接続がスタンバイ状態の 脅威に対する防御 デバイスに対して更新されなかったことを示しています。ステートフル フェールオーバー プロトコルは、不明な変換または接続を次回に捕捉します。256 バイトブロックの CNT カラムが長時間にわたって 0 またはその付近で停滞している場合は、脅威に対する防御 デバイスが処理している 1 秒あたりの接続数が非常に多いために、変換テーブルと接続テーブルの同期が取れている状態を 脅威に対する防御 デバイスが維持できない問題が発生します。<br><br>脅威に対する防御 デバイスから送信される syslog メッセージも 256 バイトブロックを使用しますが、256 バイトブロック プールが枯渇するような量が発行されることは通常ありません。CNT カラムの示す 256 バイト ブロックの数が 0 に近い場合は、Debugging（レベル 7）のログを syslog サーバーに記録していないことを確認してください。この情報は、脅威に対する防御 コンフィギュレーションの logging trap 行に示されています。ロギングは、デバッグのために詳細な情報が必要となる場合を除いて、Notification（レベル 5）以下に設定することを推奨します。 |

| フィールド | 説明 |
|---|---|
| 1550 | 脅威に対する防御 デバイスで処理するイーサネットパケットを格納するために使用されます。<br>パケットは、インターフェイスに入ると入力インターフェイス キューに配置され、次にオペレーティング システムに渡されてブロックに配置されます。デバイスは、パケットを許可するか拒否するかをセキュリティ ポリシーに基づいて決定し、パケットを発信インターフェイス上の出力キューに配置します。デバイスがトラフィック負荷に対応できていない場合は、使用可能なブロックの数が0付近で停滞します（このコマンドの出力の CNT 列に示されます）。CNT 列が 0 の場合、デバイスはより多くのブロックを割り当てようとします。このコマンドを実行すると、1550バイトブロックの最大数を8192より大きくすることができます。使用可能なブロックがなくなった場合、デバイスはパケットをドロップします。 |
| 2048 | 制御の更新に使用される制御フレームまたはガイド付きフレーム。 |
| 16384 | 64 ビット 66 MHz のギガビット イーサネット カード（i82543）にのみ使用されます。<br>イーサネット パケットの詳細については、1550 の説明を参照してください。 |
| MAX | 指定したバイト ブロックのプールで使用可能なブロックの最大数。起動時に、最大限のブロック数がメモリから切り分けられます。通常、ブロックの最大数は変化しません。例外は 256 バイトブロックおよび 1550 バイトブロックで、デバイスは必要に応じてより多くのブロックをダイナミックに作成できます。このコマンドを実行すると、1550バイトブロックの最大数を8192より大きくすることができます。 |
| LOW | 低基準値。この数は、デバイスの電源がオンになった時点、またはブロックが（**clear blocks** コマンドで）最後にクリアされた時点から、このサイズの使用可能なブロックが最も少なくなったときの数を示しています。LOW カラムが 0 である場合は、先行のイベントでメモリがいっぱいになったことを示します。 |
| CNT | 特定のサイズのブロック プールで現在使用可能なブロックの数。CNT カラムが 0 である場合は、メモリが現在いっぱいであることを意味します。 |

次に、**show blocks all** コマンドの出力例を示します。

```
> show blocks all
Class 0, size 4
     Block   allocd_by    freed_by data size  alloccnt  dup_cnt  oper location
0x01799940  0x00000000  0x00101603         0         0        0 alloc not_specified
0x01798e80  0x00000000  0x00101603         0         0        0 alloc not_specified
0x017983c0  0x00000000  0x00101603         0         0        0 alloc not_specified
...
    Found 1000 of 1000 blocks
    Displaying 1000 of 1000 blocks
```

次の表で各フィールドについて説明します。

**表 *16 : show blocks all* のフィールド**

| フィールド | 説明 |
|---|---|
| ブロック（Block） | ブロックのアドレス。 |
| allocd_by | ブロックを最後に使用したアプリケーションのプログラム アドレス（使用されていない場合は 0）。 |
| freed_by | ブロックを最後に解放したアプリケーションのプログラム アドレス。 |
| data size | ブロック内部のアプリケーション バッファまたはパケット データのサイズ。 |
| alloccnt | このブロックが作成されてから使用された回数。 |
| dup_cnt | このブロックに対する現時点での参照回数（このブロックが使用されている場合）。0 は 1 回の参照、1 は 2 回の参照を意味します。 |
| oper | ブロックに対して最後に実行された操作。alloc、get、put、free の 4 つのいずれかです。 |
| 場所 | ブロックを使用しているアプリケーション。または、ブロックを最後に割り当てたアプリケーションのプログラム アドレス（allocd_by フィールドと同じ）。 |

次に、**show blocks exhaustion history list** コマンドの出力例を示します。

```
> show blocks exhaustion history list
1 Snapshot created at 18:01:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out

2 Snapshot created at 18:02:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out

3 Snapshot created at 18:03:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out

4 Snapshot created at 18:04:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **blocks** | ブロック診断に割り当てられるメモリを増やします。 |
| **clear blocks** | システム バッファの統計情報をクリアします。 |
| **show conn** | アクティブな接続を表示します。 |

# show bootvar

ブートファイルとコンフィギュレーションのプロパティを表示するには、**show bootvar** コマンドを使用します。

**show bootvar**

## 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

BOOT 変数は、さまざまなデバイス上の起動イメージのリストを指定します。CONFIG_FILE 変数は、システム初期化中に使用されるコンフィギュレーション ファイルを指定します。

このコマンドの出力は、脅威に対する防御 にはおそらく意味がありません。

### 例

次に、脅威に対する防御 のブート変数を表示する例を示します。変数は空ですが、この例は機能しているシステムのものです。

```
> show bootvar
BOOT variable =
Current BOOT variable =
CONFIG_FILE variable =
Current CONFIG_FILE variable =
```

# show bridge-group

割り当てられたインターフェイス、MAC アドレス、IP アドレスなどブリッジグループ情報を表示するには、**show bridge-group** コマンドを使用します。

**show bridge-group** ［*bridge_group_number*］

## 構文の説明

| | |
|---|---|
| *bridge_group_number* | ブリッジグループ番号を 1 ～ 250 の整数で指定します。番号を指定しない場合、すべてのブリッジグループが表示されます。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.1 | このコマンドが追加されました。 |
| 6.2 | Integrated Routing and Bridging を使用している場合のルーテッド ファイアウォール モードのサポートが追加されました。 |

### 例

次に、**show bridge-group** コマンドの出力例を示します。

```
> show bridge-group
Static mac-address entries:  0 (in use), 16384 (max)
Dynamic mac-address entries: 0 (in use), 16384 (max)
 Bridge Group: 1
 Interfaces:
 GigabitEthernet1/2
 GigabitEthernet1/3
 GigabitEthernet1/4
 GigabitEthernet1/5
 GigabitEthernet1/6
 GigabitEthernet1/7
 GigabitEthernet1/8
 Management System IP Address:  192.168.1.1 255.255.255.0
 Management Current IP Address: 192.168.1.1 255.255.255.0
 Management IPv6 Global Unicast Address(es):
    2000:100::1, subnet is 2000:100::/64
 Static mac-address entries:  0
 Dynamic mac-address entries: 0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show running-config interface bvi** | ブリッジ グループ インターフェイス コンフィギュレーションを表示します。 |

# show c

# show capture

オプションを指定しないでキャプチャの設定を表示するには、**show capture** コマンドを使用します。

**show capture** ［*capture_name*］［**access-list** *access_list_name*］［**count** *number*］［**decode**］［**detail**］［**dump**］［**packet-number** *number*］［**trace**］

## 構文の説明

| | |
|---|---|
| **access-list** *access_list_name* | （任意）特定のアクセス リスト ID の IP フィールドまたはより高位のフィールドに基づいて、パケットに関する情報を表示します。 |
| *capture_name* | （オプション）パケット キャプチャの名前を指定します。 |
| **count** *number* | （任意）指定されたデータのパケット数を表示します。有効な値は 0 ～ 4294967295 です。 |
| **decode** | このオプションは、isakmp タイプのキャプチャがインターフェイスに適用されている場合に役立ちます。当該のインターフェイスを通過する ISAKMP データは、復号化の後にすべてキャプチャされ、フィールドをデコードした後にその他の情報とともに表示されます。 |
| **detail** | （任意）各パケットについて、プロトコル情報を追加表示します。 |
| **dump** | （オプション）データ リンク経由で転送されたパケットの 16 進ダンプを表示します。 |
| **packet-number** *number* | （任意）指定したパケット番号から表示を開始します。有効な値は 0 ～ 4294967295 です。 |
| **trace** | （任意）前述のように trace キーワードを使用してキャプチャが設定されている場合に使用される、各パケットの拡張トレース情報を表示します。また、インバウンド方向の各パケットのパケットトレーサの出力が表示されます。 |

## 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

キャプチャ名を指定した場合は、そのキャプチャのキャプチャバッファの内容が表示されます。

**dump** キーワードを指定しても、MAC 情報は 16 進ダンプに表示されません。

パケットのデコード出力は、パケットのプロトコルによって異なります。次の表の角カッコに囲まれている出力は、**detail** キーワードを指定した場合に表示されます。

表 *17*: パケット キャプチャの出力形式

| パケット タイプ | キャプチャの出力形式 |
|---|---|
| 802.1Q | *HH:MM:SS.ms* [ether-hdr] *VLAN-info encap-ether-packet* |
| 『ARP』 | *HH:MM:SS.ms* [ether-hdr] *arp-type arp-info* |
| IP/ICMP | *HH:MM:SS.ms* [ether-hdr] *ip-source* > *ip-destination:* icmp: *icmp-type icmp-code* [checksum-failure] |
| IP/UDP | *HH:MM:SS.ms* [ether-hdr] *src-addr.src-port dest-addr.dst-port:* [checksum-info] udp *payload-len* |
| IP/TCP | *HH:MM:SS.ms* [ether-hdr] *src-addr.src-port dest-addr.dst-port: tcp-flags* [header-check] [checksum-info] *sequence-number ack-number tcp-window urgent-info tcp-options* |
| IP/Other | *HH:MM:SS.ms* [ether-hdr] *src-addr dest-addr: ip-protocol ip-length* |
| Other | *HH:MM:SS.ms ether-hdr: hex-dump* |

脅威に対する防御デバイスが不正な形式の TCP ヘッダー付きのパケットを受信し、ASP ドロップの理由が invalid-tcp-hdr-length でそのパケットをドロップした場合、そのパケットを受信したインターフェイスでは **show capture** コマンドの出力にそれらのパケットは表示されません。

（注） ファイルサイズオプションを使用する場合：

- **show capture** ［*capture_name*］コマンドは、キャプチャされてスキップされたパケットの数を表示します。
- **show capture** コマンドは、キャプチャされたデータを KB および MB 単位で表示します。

### 例

次に、キャプチャのコンフィギュレーションを表示する例を示します。

```
> show capture
capture arp ethernet-type arp interface outside
capture http access-list http packet-length 74 interface inside
```

次に、ARP キャプチャによってキャプチャされたパケットを表示する例を示します。

```
> show capture arp
2 packets captured
19:12:23.478429 arp who-has 171.69.38.89 tell 171.69.38.10
19:12:26.784294 arp who-has 171.69.38.89 tell 171.69.38.10
2 packets shown
```

次に、クラスタリング環境の 1 つのユニットでキャプチャされたパケットを表示する例を示します。

```
> show capture
capture 1 cluster type raw-data interface primary interface cluster [Buffer Full - 524187
 bytes]
capture 2 type raw-data interface cluster [Capturing - 232354 bytes]
```

次に、クラスタリング環境のすべてのユニットでキャプチャされたパケットを表示する例を示します。

```
> cluster exec show capture
mycapture (LOCAL):--------------------------------------------------------------
capture 1 type raw-data interface primary [Buffer Full - 524187 bytes]
capture 2 type raw-data interface cluster [Capturing - 232354 bytes]

yourcapture:--------------------------------------------------------------------
capture 1 type raw-data interface primary [Capturing - 191484 bytes]
capture 2 type raw-data interface cluster [Capturing - 532354 bytes]
```

次に、SGT とイーサネット タギングがインターフェイスでイネーブルになっている場合にキャプチャされたパケットの例を示します。

```
> show capture my-inside-capture
1: 11:34:42.931012 INLINE-TAG 36 10.0.101.22 > 11.0.101.100: icmp: echo request
2: 11:34:42.931470 INLINE-TAG 48 11.0.101.100 > 10.0.101.22: icmp: echo reply
3: 11:34:43.932553 INLINE-TAG 36 10.0.101.22 > 11.0.101.100: icmp: echo request
4: 11.34.43.933164 INLINE-TAG 48 11.0.101.100 > 10.0.101.22: icmp: echo reply
```

SGT とイーサネット タギングがインターフェイスでイネーブルの場合、インターフェイスは引き続きタグ付きパケットまたはタグなしパケットを受信できます。この例は、出力に INLINE-TAG 36 があるタグ付きパケット用です。同じインターフェイスがタグなしパケットを受信した場合も、出力は変わりません（つまり、「INLINE-TAG 36」エントリは出力に含まれません）。

## 関連コマンド

| Command | 説明 |
|---|---|
| **capture** | パケット スニッフィングおよびネットワーク障害の切り分けのためにパケット キャプチャ機能をイネーブルにします。 |
| **clear capture** | キャプチャ バッファをクリアします。 |
| **copy capture** | キャプチャ ファイルをサーバーにコピーします。 |

# show cert-update

脅威に対する防御 デバイスの CA 証明書の自動更新のステータスを表示するには、**show cert-update** コマンドを使用します。

**show cert-update**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0.5 | このコマンドが導入されました。 |

### 例

次に、**show cert-update** コマンドの出力例を示します。

```
> show cert-update
Autoupdate is enabled and set for every day at 09:34 UTC
CA bundle was last modified 'Thu Sep 15 16:12:35 2022'
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure cert-update auto-update** | 毎日の CA 証明書の自動更新を有効または無効にします。 |
| **configure cert-update run-now** | CA 証明書の更新をすぐに試します。 |
| **configure cert-update test** | シスコのサーバーからの最新のCA証明書を使用して接続チェックを実行します。 |

# show checkheaps

チェックヒープ統計情報を表示するには、**show checkheaps** コマンドを使用します。チェックヒープは、ヒープ メモリ バッファの正常性およびコード領域の完全性を検証する定期的なプロセスです（ダイナミック メモリはシステム ヒープ メモリ領域から割り当てられます）。

**show checkheaps**

## 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、**show checkheaps** コマンドの出力例を示します。

```
> show checkheaps
Checkheaps stats from buffer validation runs
--------------------------------------------
Time elapsed since last run     : 42 secs
Duration of last run            : 0 millisecs
Number of buffers created       : 8082
Number of buffers allocated     : 7808
Number of buffers free          : 274
Total memory in use             : 43570344 bytes
Total memory in free buffers    : 87000 bytes
Total number of runs            : 310
```

# show checksum

設定のチェックサムを表示するには、**show checksum** コマンドを使用します。

**show checksum**

## 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

**show checksum** コマンドを使用すると、設定内容のデジタルサマリーとして機能する 4 つのグループの 16 進数を表示できます。このチェックサムが計算されるのは、コンフィギュレーションをフラッシュ メモリに格納するときのみです。

**show running-config** コマンドまたは **show checksum** コマンドの出力でチェックサムの前にドット（「.」）が表示された場合、この出力は、通常の設定の読み込みまたは書き込みモードのインジケータを示しています（脅威に対する防御 のフラッシュパーティションからの読み込みまたはフラッシュパーティションへの書き込み時）。「.」は、脅威に対する防御 デバイスが操作ですでに占有されているものの、「ハングアップ」しているわけではないことを示します。このメッセージは、「system processing, please wait」メッセージに似ています。

### 例

次に、コンフィギュレーションまたはチェックサムを表示する例を示します。

```
> show checksum
Cryptochecksum: 1a2833c0 129ac70b 1a88df85 650dbb81
```

# show chunkstat

チャンク統計情報を表示するには、**show chunkstat** コマンドを使用します。

**show chunkstat**

## 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、チャンクに関する統計情報を表示する例を示します。

```
> show chunkstat
Global chunk statistics: created 181, destroyed 34, siblings created 94, siblings destroyed
 34

Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01edb4cc, name "Managed Chunk Queue Elements", data start @ 01edbd24,
end @ 01eddc54
next: 01eddc8c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 499, elt size: 16, index first free 498
# chunks in use: 1, HWM of total used: 1, alignment: 0
Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01eddc8c, name "Registry Function List", data start @ 01eddea4, end @
01ede348
next: 01ede37c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 99, elt size: 12, index first free 42
# chunks in use: 57, HWM of total used: 57, alignment: 0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show counters** | プロトコル スタック カウンタを表示します。 |
| **show cpu** | CPU の使用状況に関する情報を表示します。 |

# show clns

IS-IS の Connectionless Network Service（CLNS）情報を表示するには、**show clns** コマンドを使用します。

**show clns** {**filter-set** [*name*] | **interface** [*interface_name*] | **is-neighbors** [*interface_name* [**detail**] | **neighbors** [**areas**] [*interface_name*] [**detail**] | **protocol** [*domain*] | **traffic**}

## 構文の説明

| | |
|---|---|
| **filter-set** [*name*] | CLNS フィルタ セットを表示します。必要に応じて、フィルタセットの名前を指定できます。 |
| **interface** [*interface_name*] | CLNS インターフェイスのステータスと設定を表示します。必要に応じて、出力を絞り込むインターフェイスの名前を指定できます。 |
| **is-neighbors** [*interface_name*] [**detail**] | IS ネイバー隣接関係を表示します。ネイバー エントリは、配置されているエリアに応じてソートされます。必要に応じて、出力を絞り込むインターフェイスの名前を指定できます。<br><br>**detail** を指定して、中継システムに関連付けられたエリアを含めます。そうでない場合は、サマリー表示が提供されます。 |
| **neighbors** [**areas**] [*interface_name*] [**detail**] | エンドシステム（ES）、中継システム（IS）、およびマルチトポロジ統合 Intermediate System-to-Intermediate System（M-ISIS）ネイバーを表示します。必要に応じて、出力を絞り込むインターフェイスの名前を指定できます。<br><br>CLNS マルチエリア隣接関係を表示するには、**areas** キーワードを含めます。<br><br>**detail** を指定して、中継システムに関連付けられたエリアを含めます。そうでない場合は、サマリー表示が提供されます。 |
| **protocol** [*domain*] | CLNS ルーティング プロトコル プロセス情報を表示します。少なくとも 2 つのルーティング プロセス、レベル 1 およびレベル 2 が常に存在し、さらに多い場合もあります。必要に応じて、CLNS ドメインの名前を指定して出力を絞り込むことができます。 |
| **traffic** | このルータが認識した CLNS パケットをリストします。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

## 例

次に、実行コンフィギュレーションで定義されているCLNSフィルタセットを表示し、**show clns filter-set** コマンドを使用して表示する例を示します。

```
> show running-config clns
clns filter-set US-OR-NORDUNET permit 47.0005...
clns filter-set US-OR-NORDUNET permit 47.0023...
clns filter-set LOCAL permit 49.0003
> show clns filter-set

CLNS filter set US-OR-NORDUNET
      permit 47.0005...
      permit 47.0023...
CLNS filter set LOCAL
      permit 49.0003...
```

次に、**show clns interface** コマンドの出力例を示します。[Routing Protocol: IS-IS] の下の情報には、レベル 1 とレベル 2 のメトリック、優先順位、回線 ID、アクティブなレベル 1 とレベル 2 の隣接関係の数など、Intermediate System-to-Intermediate System（IS-IS）に関する情報が表示されます。

```
> show clns interface
GigabitEthernet0/1 is up, line protocol is up
  Checksums enabled, MTU 1500
  ERPDUs enabled, min. interval 10 msec.
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 0 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1-2
    Interface number 0x0, local circuit ID 0x1
    Level-1 Metric: 10, Priority: 64, Circuit ID: c2.01
    DR ID: c2.01
    Level-1 IPv6 Metric: 10
    Number of active level-1 adjacencies: 3
    Level-2 Metric: 10, Priority: 64, Circuit ID: c2.01
    DR ID: c2.01
    Level-2 IPv6 Metric: 10
    Number of active level-2 adjacencies: 3
    Next IS-IS LAN Level-1 Hello in 1 seconds
    Next IS-IS LAN Level-2 Hello in 1 seconds
```

次に、**show clns neighbors** コマンドの出力例を示します。

```
> show clns neighbors

System Id      Interface   SNPA            State  Holdtime  Type Protocol
CSR7001        inside      000c.2921.ff44      Up          29   L1L2
CSR7002        inside      000c.2906.491c      Up          27   L1L2
```

次の表で、ネイバー出力の各フィールドについて説明します。

**表 *18* : ネイバー出力のフィールド**

| フィールド | 説明 |
|---|---|
| System Id | エリア内のシステムを識別する 6 バイト値。 |

| フィールド | 説明 |
|---|---|
| インターフェイス | システムの学習元インターフェイス名。 |
| SNPA | サブネットワーク ポイント オブ アタッチメント。これはデータ リンク アドレスです。 |
| 状態 | ES、IS、または M-ISIS の状態。<br>• Init：システムは IS で、IS-IS hello メッセージを待機しています。IS-IS は、ネイバーを隣接関係にないと見なします。<br>• Up：ES または IS が到達可能であると確信しています。 |
| Holdtime | この隣接関係エントリがタイムアウトするまでの秒数。 |
| タイプ | 隣接関係のタイプ。<br>• ES：エンドシステム隣接関係が、ES-IS プロトコルを介して検出されたか、または静的に設定されました。<br>• IS：ルータ隣接関係が、ES-IS プロトコルを介して検出されたか、または静的に設定されました。<br>• M-ISIS：ルータ隣接関係が、マルチトポロジ IS-IS プロトコルを介して検出されました。<br>• L1：レベル 1 ルーティングのみのルータ隣接関係。<br>• L1L2：レベル 1 およびレベル 2 ルーティングのルータ隣接関係。<br>• L2: 第 2 レベルのみのルータ隣接関係。 |
| Protocol | 隣接関係が学習されたプロトコル。有効なプロトコル ソースは、ES-IS、IS-IS、ISO IGRP、Static、DECnet、および M-ISIS です。 |

次に、**show clns neighbors detail** コマンドの出力例を示します。

```
> show clns neighbors detail

System Id      Interface   SNPA            State  Holdtime  Type Protocol
CSR7001        inside      000c.2921.ff44  Up          26   L1L2
  Area Address(es): 49.0001
  IP Address(es):  1.3.3.3*
  Uptime: 01:16:33
  NSF capable
  Interface name: inside
CSR7002        inside      000c.2906.491c  Up          27   L1L2
  Area Address(es): 49.0001
  IP Address(es):  20.3.3.3*
  Uptime: 01:16:33
  NSF capable
  Interface name: inside
```

次に、**show clns is-neighbors** コマンドの出力例を示します。

```
> show clns is-neighbors

System Id      Interface   State  Type Priority  Circuit Id         Format
CSR7001        inside      Up     L1L2 64/64    ciscoasa.01        Phase V
CSR7002        inside      Up     L1L2 64/64    ciscoasa.01        Phase V
```

次の表で、IS ネイバー出力の列について説明します。

**表 *19 : IS* ネイバー出力のフィールド**

| フィールド | 説明 |
|---|---|
| System Id | システムの ID 値。 |
| インターフェイス | ルータが検出されたインターフェイス。 |
| 状態 | 隣接状態。Up および Init が状態です。詳細については、**show clns neighbors** の説明を参照してください。 |
| タイプ | 隣接関係のタイプ：L1、L2、または L1L2。詳細については、**show clns neighbors** の説明を参照してください。 |
| プライオリティ | 関連ネイバーがアドバタイズしている IS-IS のプライオリティ。インターフェイスの指定 IS-IS ルータに対して最もプライオリティの高いネイバーが選ばれます。 |
| Circuit Id | インターフェイスにとって指定 IS-IS ルータが何であるかについてのネイバーの認識。 |
| 書式 | ネイバーがフェーズ V（OSI）隣接またはフェーズ IV（DECnet）隣接のいずれであるかを示すフォーマット。 |

次に、**show clns is-neighbors detail** コマンドの出力例を示します。

```
> show clns is-neighbors detail

System Id      Interface   State  Type Priority  Circuit Id         Format
CSR7001        inside      Up     L1L2 64/64    ciscoasa.01        Phase V
  Area Address(es): 49.0001
  IP Address(es):  1.3.3.3*
  Uptime: 00:12:49
  NSF capable
  Interface name: inside
CSR7002        inside      Up     L1L2 64/64    ciscoasa.01        Phase V
  Area Address(es): 49.0001
  IP Address(es):  20.3.3.3*
  Uptime: 00:12:50
  NSF capable
  Interface name: inside
```

次に、**show clns protocol** コマンドの出力例を示します。

```
> show clns protocol
```

```
IS-IS Router
  System Id: 0050.0500.5008.00  IS-Type: level-1-2
  Manual area address(es):
        49.0001
  Routing for area address(es):
        49.0001
  Interfaces supported by IS-IS:
        outside - IP
  Redistribute:
    static (on by default)
  Distance for L2 CLNS routes: 110
  RRR level: none
  Generate narrow metrics: level-1-2
  Accept narrow metrics:   level-1-2
  Generate wide metrics:   none
  Accept wide metrics:     none
```

次に、**show clns traffic** コマンドの出力例を示します。

```
> show clns traffic

CLNS:  Time since last clear: never
CLNS & ESIS Output: 0, Input: 8829
CLNS Local: 0, Forward: 0
CLNS Discards:
  Hdr Syntax: 0, Checksum: 0, Lifetime: 0, Output cngstn: 0
  No Route: 0, Discard Route: 0, Dst Unreachable 0, Encaps. Failed: 0
  NLP Unknown: 0, Not an IS: 0
CLNS Options: Packets 0, total 0 , bad 0, GQOS 0, cngstn exprncd 0
CLNS Segments:  Segmented: 0, Failed: 0
CLNS Broadcasts: sent: 0, rcvd: 0
Echos: Rcvd 0 requests, 0 replies
      Sent 0 requests, 0 replies
ESIS(sent/rcvd): ESHs: 0/0, ISHs: 0/0, RDs: 0/0, QCF: 0/0
Tunneling (sent/rcvd): IP: 0/0, IPv6: 0/0
Tunneling dropped (rcvd) IP/IPV6:  0
ISO-IGRP: Querys (sent/rcvd): 0/0 Updates (sent/rcvd): 0/0
ISO-IGRP: Router Hellos: (sent/rcvd): 0/0
ISO-IGRP Syntax Errors: 0

IS-IS: Time since last clear: never
IS-IS: Level-1 Hellos (sent/rcvd): 1928/1287
IS-IS: Level-2 Hellos (sent/rcvd): 1918/1283
IS-IS: PTP Hellos     (sent/rcvd): 0/0
IS-IS: Level-1 LSPs sourced (new/refresh): 7/13
IS-IS: Level-2 LSPs sourced (new/refresh): 7/14
IS-IS: Level-1 LSPs flooded (sent/rcvd): 97/2675
IS-IS: Level-2 LSPs flooded (sent/rcvd): 73/2628
IS-IS: LSP Retransmissions: 0
IS-IS: Level-1 CSNPs (sent/rcvd): 642/0
IS-IS: Level-2 CSNPs (sent/rcvd): 639/0
IS-IS: Level-1 PSNPs (sent/rcvd): 0/554
IS-IS: Level-2 PSNPs (sent/rcvd): 0/390
IS-IS: Level-1 DR Elections: 1
IS-IS: Level-2 DR Elections: 1
IS-IS: Level-1 SPF Calculations: 9
IS-IS: Level-2 SPF Calculations: 8
IS-IS: Level-1 Partial Route Calculations: 0
IS-IS: Level-2 Partial Route Calculations: 0
IS-IS: LSP checksum errors received: 0
IS-IS: Update process queue depth: 0/200
IS-IS: Update process packets dropped: 0
```

次の表で、トラフィック出力のフィールドについて説明します。

**表 *20*: トラフィック出力のフィールド**

| フィールド | 説明 |
|---|---|
| CLNS & ESIS Output | このルータが送信したパケットの合計数。 |
| 入力 | このルータが受信したパケットの合計数。 |
| CLNS Local | このルータによって生成されたパケット数。 |
| Forward | このルータが転送したパケット数。 |
| CLNS Discards | CLNS が廃棄したパケット数（廃棄理由ごとに分類されたもの）。 |
| CLNS Options | CLNS パケット内で見つかったオプション。 |
| CLNS Segments | セグメント化されたパケットの数と、パケットをセグメント化できなかったことによって発生した障害数。 |
| CLNS Broadcasts | 送受信された CLNS ブロードキャストの数。 |
| Echos | 受信されたエコー要求パケットとエコー応答パケットの数。このフィールドの後ろの行には、送信されたエコー要求パケットとエコー応答パケットの数をリストします。 |
| ESIS (sent/rcvd) | 送受信されたエンドシステム Hello（ESH）、中継システム Hello（ISH）、およびリダイレクトの数。 |
| ISO IGRP | 送受信された ISO Interior Gateway Routing Protocol（IGRP）のクエリーおよび更新の数。 |
| Router Hellos | 送受信された ISO IGRP ルータ hello パケットの数。 |
| IS-IS: Level-1 hellos (sent/rcvd) | 送受信されたレベル 1 IS-IS hello パケットの数。 |
| IS-IS: Level-2 hellos (sent/rcvd) | 送受信されたレベル 2 IS-IS hello パケットの数。 |
| IS-IS: PTP hellos (sent/rcvd) | シリアルリンクを通して送受信されたポイントツーポイントの IS-IS hello パケットの数。 |
| IS-IS: Level-1 LSPs (sent/rcvd) | 送受信されたレベル 1 のリンクステート プロトコル データ ユニット（PDU）の数。 |
| IS-IS: Level-2 LSPs (sent/rcvd) | 送受信されたレベル 2 のリンクステート PDU の数。 |
| IS-IS: Level-1 CSNPs (sent/rcvd) | 送受信されたレベル 1 Complete Sequence Number Packet（CSNP）の数。 |

| フィールド | 説明 |
|---|---|
| IS-IS: Level-2 CSNPs (sent/rcvd) | 送受信されたレベル 2 の CSNP の数。 |
| IS-IS: Level-1 PSNPs (sent/rcvd) | 送受信されたレベル 1 Partial Sequence Number Packet（PSNP）の数。 |
| IS-IS: Level-2 PSNPs (sent/rcvd) | 送受信されたレベル 2 の PSNP の数。 |
| IS-IS: Level-1 DR Elections | レベル 1 の指定ルータの選定が行われた回数。 |
| IS-IS: Level-2 DR Elections | レベル 2 の指定ルータの選定が行われた回数。 |
| IS-IS: Level-1 SPF Calculations | レベル 1 の最短パス優先（SPF）ツリーが計算された回数。 |
| IS-IS: Level-2 SPF Calculations | レベル 2 の SPF ツリーが計算された回数。 |

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear clns** | CLNS 固有の情報をクリアします。 |

# show cluster

クラスタ全体の集約データまたはその他の情報を表示するには、**show cluster** コマンドを使用します。

**show cluster { access-list** ［ *acl_name* ］ | **conn** ［ **count** ］ | **cpu** ［ **usage** ］ | **interface-mode** | **memory** | **resource usage** | **rule hits** ［ **raw** ］ | **service-policy** | **traffic** | **xlate count** }

## 構文の説明

| | |
|---|---|
| **access-list** [*acl_name*] | アクセス ポリシーのヒット カウンタを示します。特定の ACL のカウンタを表示するには、acl_name と入力します。 |
| **conn** [**count**] | 使用中の接続の、すべてのユニットでの合計数を表示します。**count** キーワードを入力すると、接続数だけが表示されます。 |
| **cpu** [**usage**] | CPU の使用率情報を表示します。 |
| **interface-mode** | クラスタ インターフェイス モードを表示します（spanned または individual）。 |
| **memory** | システム メモリ使用率などの情報を表示します。 |
| **resource usage** | システム リソースと使用状況を表示します。 |
| **rule hits** ［**raw**］ | アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報を表示します。**raw** キーワードを指定すると、データが .csv 形式で表示されます。 |
| **service-policy** | MPF サービス ポリシー統計情報を表示します。 |
| **traffic** | トラフィック統計情報を表示します。 |
| **xlate count** | 現在の変換情報を表示します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.4 | **rule hits** ［**raw**］キーワードが追加されました。 |
| 6.1 | このコマンドが導入されました。 |

### 例

次に、**show cluster access-list** コマンドの出力例を示します。

```
> show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
```

```
 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
  (hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0
  (hitcnt=0, 0, 0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
  (hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
  (hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
  (hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
  (hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
  (hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
  (hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
  (hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
  (hitcnt=429, 109, 107, 109, 104)0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
  (hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
  (hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
  (hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
  (hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
  (hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
  (hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

使用中の接続の、すべてのユニットでの合計数を表示するには、次のとおりに入力します。

```
> show cluster conn count
Usage Summary In Cluster:*********************************************
  200 in use (cluster-wide aggregated)
     cl2(LOCAL):**********************************************************
  100 in use, 100 most used
  cl1:*****************************************************************
  100 in use, 100 most used
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show cluster info** | クラスタ情報を表示します。 |

# show cluster history

クラスタのイベント履歴を表示するには、特権 EXEC モードで **show cluster history** コマンドを使用します。

**show cluster history** ［ **brief** ］［ **latest** ［ *number* ］ ］［ **reverse** ］［ **time** ［ *year month day* ］ *hh* **:** *mm* **:** *ss* ］

## 構文の説明

| | |
|---|---|
| **brief** | 一般イベントを除くクラスタ履歴を表示します。 |
| **latest** [*number*] | 最新のイベントを表示します。デフォルトでは、最新の 512 のイベントが表示されます。*number* を指定することでイベントの数を 1 ー 512 に制限できます。 |
| **reverse** | イベントを逆の順序で表示します。 |
| **time** [ *year month day*] *hh*:*mm*:*ss* | 指定された日時より前のイベントを表示します。 |

## コマンド デフォルト

デフォルトの動作や値はありません。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | **brief**、**latest**、**reverse**、**time** キーワードが追加されました。 |
| 6.6 | **show cluster history** コマンドは強化され、クラスタユニットがクラスタに参加できなかった理由、またはクラスタから離脱した理由に関するメッセージが追加されました。 |
| 6.1 | このコマンドが追加されました。 |

## 使用上のガイドライン

次に、 **show cluster history time** コマンドの出力例を示します。

```
> show cluster history time august 26 10:10:05
==========================================================================
From State            To State              Reason
==========================================================================

10:08:49 UTC Aug 26 2020
DISABLED              DISABLED              Disabled at startup


10:09:43 UTC Aug 26 2020
DISABLED              ELECTION              Enabled from CLI


10:10:01 UTC Aug 26 2020
ELECTION              ONCALL                Event: Cluster unit A state is MASTER
```

```
10:10:02 UTC Aug 26 2020
ONCALL                SLAVE_COLD            Slave proceeds with configuration sync

10:10:02 UTC Aug 26 2020
SLAVE_COLD            SLAVE_CONFIG          Client progression done

10:10:04 UTC Aug 26 2020
SLAVE_CONFIG          SLAVE_FILESYS         Configuration replication finished

10:10:05 UTC Aug 26 2020
SLAVE_FILESYS         SLAVE_BULK_SYNC       Client progression done
```

次に、**show cluster history brief** コマンドの出力例を示します。

```
> show cluster history brief
================================================================================
From State            To State              Reason
================================================================================
10:08:49 UTC Aug 26 2020
DISABLED              DISABLED              Disabled at startup

10:09:43 UTC Aug 26 2020
DISABLED              ELECTION              Enabled from CLI


10:10:02 UTC Aug 26 2020
ONCALL                SLAVE_COLD            Slave proceeds with configuration sync

10:10:02 UTC Aug 26 2020
SLAVE_COLD            SLAVE_CONFIG          Client progression done

10:10:04 UTC Aug 26 2020
SLAVE_CONFIG          SLAVE_FILESYS         Configuration replication finished

10:10:05 UTC Aug 26 2020
SLAVE_FILESYS         SLAVE_BULK_SYNC       Client progression done
```

次に、**show cluster history latest** コマンドの出力例を示します。

```
> show cluster history latest 3
================================================================================
From State            To State              Reason
================================================================================
10:10:05 UTC Aug 26 2020
SLAVE_FILESYS         SLAVE_BULK_SYNC       Client progression done

10:10:04 UTC Aug 26 2020
SLAVE_CONFIG          SLAVE_FILESYS         Configuration replication finished
```

```
10:10:02 UTC Aug 26 2020
SLAVE_COLD            SLAVE_CONFIG          Client progression done
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show cluster** | クラスタ全体の集約データおよびその他の情報を表示します。 |
| **show cluster info** | クラスタ情報を表示します。 |

# show cluster info

クラスタ情報を表示するには、**show cluster info** コマンドを使用します。

**show cluster info** [ **auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [ *options* ] | **health** | **incompatible-config** | **instance-type** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [ *options* ] | **transport** { **asp** | **cp** } ]

## 構文の説明

| | |
|---|---|
| **auto-join** | 時間遅延後にクラスタ ユニットがクラスタに自動的に再参加するかどうか、および障害状態（ライセンスの待機やシャーシのヘルスチェック障害など）がクリアされたかどうかを示します。ユニットが永続的に無効になっている場合、またはユニットがすでにクラスタ内にある場合、このコマンドでは出力が表示されません。 |
| **clients** | （オプション）登録クライアントのバージョンを表示します。 |
| **conn-distribution** | （オプション）クラスタ内の接続分布を表示します。 |
| **flow-mobility counters** | （オプション）EIDの移動やフロー オーナーの移動に関する情報を表示します。 |
| **goid** [*options*] | （オプション）グローバル オブジェクト ID データベースを示します。次のオプションがあります。<br>classmap<br>conn-set<br>hwidb<br>idfw-domain<br>idfw-group<br>interface<br>policymap<br>virtual-context |
| **health** | （オプション）ヘルス モニタリング情報を表示します。 |
| **incompatible-config** | （オプション）現在の実行コンフィギュレーションのクラスタリングと互換性のないコマンドを表示します。このコマンドは、クラスタリングをイネーブルにする前に役立ちます。 |
| **instance-type** | （任意）マルチインスタンス クラスタリングを使用する場合、クラスタメンバーごとのモジュールタイプとリソースサイズを表示します。 |
| **loadbalance** | （オプション）ロード バランシング情報を表示します。 |

| | |
|---|---|
| **old-members** | （オプション）クラスタの以前のメンバーを表示します。 |
| **packet-distribution** | （オプション）クラスタのパケット分布を表示します。 |
| **trace** [*options*] | （オプション）クラスタリング制御モジュール イベント トレースを表示します。次のオプションがあります。<br>• **latest** [*number*]：最新の number のイベントを表示します。number は 1 ～ 2147483647 の範囲です。デフォルトではすべてが表示されます。<br>• **level** *level*：レベル別にイベントをフィルタ処理します。レベルは、次のいずれかです。**all**、**critical**、**debug**、**informational**、または **warning**。<br>• **module** *module*：モジュール別にイベントをフィルタ処理します。モジュールは、次のいずれかです。**ccp**、**datapath**、**fsm**、**general**、**hc**、**license**、**rpc**、または **transport**。<br>• **time** {[*month day*] [*hh:mm:ss*]}：指定した時刻または日付より前のイベントを表示します。 |
| **transport** {**asp** \| **cp**} | （オプション）次のトランスポート関連の統計情報を表示します。<br>• **asp**：データプレーンのトランスポート統計情報。<br>• **cp**：コントロールプレーンのトランスポート統計情報。 |

## 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。 |
| 6.2.3 | **auto-join**キーワードが追加されました。 |
| 6.6 | 出力が拡張され、マルチインスタンス クラスタリングの特性が表示されるようになりました。クラスタメンバーごとのモジュールタイプとリソースサイズを表示するための **instance-type** キーワードも追加されました。 |

## 使用上のガイドライン

オプションを指定しない場合、**show cluster info** コマンドはクラスタの名前とステータス、クラスタメンバー、メンバーの状態など、一般的なクラスタ情報を表示します。

**clear cluster info** コマンドを使用して、統計情報をクリアします。

### 例

次に、**show cluster info** コマンドの出力例を示します。

```
> show cluster info
Cluster stbu: On
```

```
  This is "C" in state SLAVE
      ID        : 0
      Site ID : 1
      Version   : 6.2
      Serial No.: P3000000025
      CCL IP    : 10.0.0.3
      CCL MAC   : 000b.fcf8.c192
      Last join : 17:08:59 UTC Sep 26 2011
      Last leave: N/A
Other members in the cluster:
  Unit "D" in state SLAVE
      ID        : 1
      Site ID : 1
      Version   : 6.2
      Serial No.: P3000000001
      CCL IP    : 10.0.0.4
      CCL MAC   : 000b.fcf8.c162
      Last join : 19:13:11 UTC Sep 23 2011
      Last leave: N/A
  Unit "A" in state MASTER
      ID        : 2
      Site ID : 2
      Version   : 6.2
      Serial No.: JAB0815R0JY
      CCL IP    : 10.0.0.1
      CCL MAC   : 000f.f775.541e
      Last join : 19:13:20 UTC Sep 23 2011
      Last leave: N/A
  Unit "B" in state SLAVE
      ID        : 3
      Site ID : 2
      Version   : 6.2
      Serial No.: P3000000191
      CCL IP    : 10.0.0.2
      CCL MAC   : 000b.fcf8.c61e
      Last join : 19:13:50 UTC Sep 23 2011
      Last leave: 19:13:36 UTC Sep 23 2011
```

次に、マルチインスタンス クラスタリングを使用ている場合の **show cluster info** コマンドの出力例を示します

```
> show cluster info
Cluster MI: On
    Interface mode: spanned
    This is "unit-3-1" in state MASTER
        ID             : 0
        Site ID         : 1
        Version           : 6.6
        Serial No.        : FLM2123050F12T
        CCL IP             : 127.2.3.1
        CCL MAC   : a28e.6000.0012
        Module.
: FPR4K-SM-12
        Resource.
: 10 cores / 23876 MB RAM
        Last join          : 19:48:33 UTC Nov 13 2018
        Last leave: N/A
Other members in the cluster:
    Unit "unit-4-1" in state SLAVE
        ID               : 1
        Site ID           : 1
        Version           : 6.6
```

```
        Serial No.          : FLM212305ELPXW
        CCL IP              : 127.2.4.1
        CCL MAC     : a2f7.2000.0009
        Module
: FPR4K-SM-12
        Resource
: 6 cores / 14426 MB RAM
        Last join           : 20:29:55 UTC Nov 14 2018
        Last leave        : 19:07:53 UTC Nov 14 2018


Warning: Mixed module and / or mismatched resource profile size in cluster. System may
not run in an optimized state.
```

次に、マルチインスタンス クラスタリングを使用ている場合の **show cluster info instance-type** コマンドの出力例を示します。

```
> show cluster info instance-type

     Cluster Member     Module Type               CPU Cores        RAM (MB)
         unit-3-1       FPR4K-SM-12                 10              23876
         unit-4-1       FPR4K-SM-12                 6               14446

Warning: Mixed module type and / or mismatched resource profile in cluster. System may
not run in an optimized state.
```

次に、**show cluster info incompatible-config** コマンドの出力例を示します。

```
> show cluster info incompatible-config
INFO: Clustering is not compatible with following commands which given a
user's confirmation upon enabling clustering, can be removed automatically
from running-config.
policy-map global_policy
 class scansafe-http
  inspect scansafe http-map fail-close
policy-map global_policy
 class scansafe-https
  inspect scansafe https-map fail-close
INFO: No manually-correctable incompatible configuration is found.
```

次に、**show cluster info trace** コマンドの出力例を示します。

```
> show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at MASTER
```

次に、**show cluster info flow-mobility counters** コマンドの出力例を示します。

```
> show cluster info flow-mobility counters
EID movement notification received  : 0
EID movement notification processed : 0
Flow owner moving requested         : 0
```

**show cluster info auto-join** コマンドについては、次の出力を参照してください。

```
> show cluster info auto-join
Unit will try to join cluster in 253 seconds.
Quit reason: Received control message DISABLE

> show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Master has application down that slave has up.

> show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Chassis-blade health check failed.

> show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Service chain application became down.

> show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Unit is kicked out from cluster because of Application health check failure.


> show cluster info auto-join
Unit join is pending (waiting for the smart license entitlement: ent1)

> show cluster info auto-join
Unit join is pending (waiting for the smart license export control flag)
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show cluster** | クラスタ全体の集約データを表示します。 |

# show cluster rule hits

クラスタのすべてのノードから、アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報を集約形式で表示するには、**show cluster rule hits** コマンドを使用します。

**show cluster rule hits** ［**raw**］

## 構文の説明

| | |
|---|---|
| **raw** | （任意）.csv 形式でルールヒット情報を表示します。 |

## コマンド デフォルト

クラスタのすべてのノードから、すべてのルールのルールヒット情報を表示します。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.4 | このコマンドが導入されました。 |

## 使用上のガイドライン

ルールヒット情報は、アクセスコントロールルールとプレフィルタルールのみを対象としています。

### 例

次に、クラスタの各ノードからのルールヒット情報を分離形式で表示する例を示します。

```
> show cluster rule hits
RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)

--------------------------------------------------------------------------------
268435264            1                   06:54:44 Mar 8 2019     06:54:44 Mar 8 2019

268435265            1                   06:54:58 Mar 8 2019     06:54:58 Mar 8 2019

268435270            1                   06:54:53 Mar 8 2019     06:54:53 Mar 8 2019

268435271            1                   06:55:01 Mar 8 2019     06:55:01 Mar 8 2019

268435260            1                   06:55:17 Mar 8 2019     06:55:17 Mar 8 2019

268435261            1                   06:55:19 Mar 8 2019     06:55:19 Mar 8 2019
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **cluster exec show rule hits** | クラスタの各ノードから、アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報を分離形式で表示します。 |

| Command | 説明 |
| --- | --- |
| **cluster exec clear rule hits** | クラスタ内のすべてのノードから、アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報をクリアし、ゼロにリセットします。 |
| **show rule hits** | アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報を表示します。 |
| **clear rule hits** | アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報をクリアし、ゼロにリセットします。 |

# show community-list

特定のコミュニティリストによって許可されたルートを表示するには、**show community-list** コマンドを使用します。

**show community-list** ［*community_list_name*］

## 構文の説明

| | |
|---|---|
| *community_list_name* | （オプション）コミュニティリストの名前。 |

## 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、**show community-list** コマンドの出力例を示します。

```
> show community-list

Named Community expanded list comm2
    permit 10
Named Community standard list excomm1
    permit internet 100 no-export no-advertise
```

# show conn

指定した接続タイプの接続状態を表示するには、**show conn** コマンドを使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

**show conn** ［ **vrf** { *name* | **global** } ］ ［ **count** | ［ **all** ］ ［ **detail** ］ ［ **data-rate-filter** { **lt** | **eq** | **gt** } **value** } ］ ］ ［ **long** ］ ［ **state** *state_type* ］ ［ **flow-rule** ］ ［ **inline-set** ］ ［ **protocol** { **tcp** | **udp** | **sctp** } ］ ［ **address** *src_ip* ［ − *src_ip* ］ ［ **netmask** *mask* ］ ］ ［ **port** *src_port* ［ − *src_port* ］ ］ ［ **address** *dest_ip* ［ − *dest_ip* ］ ［ **netmask** *mask* ］ ］ ［ **port** *dest_port* ［ − *dest_port* ］ ］ ［ **state** *state_type* ］ ［ **zone** ［ *zone_name* ］ ］ ［ **data-rate** ］

## 構文の説明

| | |
|---|---|
| **address** {*src_ip* \| *dest_ip*} | （任意）指定した送信元または宛先 IPv4 アドレスあるいは IPv6 アドレスとの接続を表示します。範囲を指定するには、IP アドレスをダッシュ（-）で区切ります。たとえば、10.1.1.1-10.1.1.5 のように区切ります。 |
| **all** | （任意）通過トラフィックの接続に加えて、デバイスへの接続とデバイスからの接続を表示します。 |
| **count** | （任意）アクティブな接続の数を表示します。 |
| **detail** | （任意）変換タイプとインターフェイスの情報を含め、接続の詳細を表示します。 |
| **data-rate-filter {lt \| eq \| gt}***value* | （オプション）データレート値（1 秒あたりのバイト数）に基づいてフィルタリングされた接続を表示します。次に例を示します。<br>*data-rate-filter gt 123* |
| **flow-rule** | （任意）フロールールの接続を表示します。 |
| **inline-set** | （任意）インラインセットの接続を表示します。 |
| **long** | （任意）接続をロング フォーマットで表示します。 |
| **netmask** *mask* | （任意）指定された IP アドレスで使用するサブネット マスクを指定します。 |
| **port** {*src_port* \| *dest_port*} | （任意）指定した送信元ポートまたは宛先ポートとの接続を表示します。範囲を指定するには、ポート番号をダッシュ（-）で区切ります。たとえば、1000-2000 のように区切ります。 |
| **protocol** {**tcp \| udp \| sctp**} | （任意）接続プロトコルを指定します。 |
| **state** *state_type* | （任意）接続状態タイプを指定します。接続状態のタイプに使用できるキーワードについては、使用方法のセクションの表を参照してください。 |

| | |
|---|---|
| **zone** [*zone_name*] | （オプション）ゾーンの接続を表示します。**long** キーワードと **detail** キーワードは、接続が構築されたプライマリインターフェイスと、トラフィックの転送に使用される現在のインターフェイスを表示します。 |
| ［**vrf** {*name* \| **global**}］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。コマンドをグローバル仮想ルータに限定するには、**vrf global** を指定します。このキーワードを省略すると、コマンドはすべての仮想ルータに適用されます。 |
| **data-rate** | （オプション）データレート トラッキング ステータスが有効になっているか無効になっているかを表示します。 |

## コマンド デフォルト

デフォルトでは、すべての通過接続が表示されます。デバイスへの管理接続も表示するには、**all** キーワードを使用する必要があります。

## 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。 |
| 6.4 | **egress_optimization** 接続状態タイプが追加されました。 |
| 6.5 | デッド接続検出（DCD）イニシエータ/レスポンダプローブカウントが、DCD 対応接続に関する **show conn detail** の出力に追加されました。 |
| 6.6 | 次の変更が導入されました。<br>• **vrf** キーワードが追加されました。<br>接続データレート トラッキング ステータスが追加されました。<br>ユーザー指定のデータレート値によって接続をフィルタ処理するために、`show conn detail` コマンドに **data-rate-filter** キーワードが追加されました。<br>• **show conn detail** コマンド出力の **packet id** パラメータが **Connection lookup keyid** に変更されました。 |
| 6.7 | TCP フローが TLS サーバー証明書の取得に使用されることを示すため、コマンド出力に B フラグが追加されました。 |
| 7.2 | コマンド出力に対する N フラグが拡張され、エレファントフロー接続とそれらに対して実行されるアクションを示す 3、4、および 5 が含まれています。 |
| 7.3 | QUIC プロトコルの Q フラグが追加されました。 |

## 使用上のガイドライン

**show conn** コマンドは、アクティブな TCP 接続および UDP 接続の数を表示し、さまざまなタイプの接続に関する情報を提供します。接続のテーブル全体を参照するには、**show conn all** コマンドを使用します。このコマンドを使用して、特定の QoS ルール ID によってレート制限されているライブ接続を検索できます。

（注） 脅威に対する防御デバイスでセカンダリ接続できるようにピンホールを作成すると、**show conn** コマンドではこのピンホールが不完全な接続として表示されます。この不完全な接続をクリアするには、**clear conn** コマンドを使用します。

次の表に、**show conn state** コマンドを使用して指定できる接続タイプを示します。複数の接続タイプを指定する場合、キーワードの区切りにはカンマを使用します。ただし、スペースは必要ありません。次に、アップ状態の RPC 接続、H.323 接続、および SIP 接続に関する情報を表示する例を示します。

```
> show conn state up,rpc,h323,sip
```

表 *21* : 接続状態のタイプ

| キーワード | 表示される接続タイプ |
|---|---|
| **up** | アップ状態の接続 |
| **conn_inbound** | このキーワードは使用しないでください。インバウンド接続が正しく表示されません。 |
| **ctiqbe** | CTIQBE 接続 |
| **data_in** | 着信データ接続 |
| **data_out** | 発信データ接続 |
| **egress_optimization** | 出力最適化（パフォーマンスを向上させる機能）の対象となる接続についての情報を表示します。このコマンドは、Cisco TAC のアドバイスに従って使用します。このコマンドは、フラグ **F**（forward フローのみが出力最適化の対象）、**R**（reverse フローのみが対象）、または **FR**（forward フローと reverse フローの両方が対象）を使用します。 |
| **finin** | FIN 着信接続 |
| **finout** | FIN 発信接続 |
| **h225** | H.225 接続 |
| **h323** | H.323 接続 |
| **http_get** | HTTP get 接続 |

| キーワード | 表示される接続タイプ |
|---|---|
| **mgcp** | MGCP 接続 |
| **nojava** | Java アプレットへのアクセスを拒否する接続 |
| **rpc** | RPC 接続 |
| **service_module** | SSM によってスキャンされる接続 |
| **sip** | SIP 接続 |
| **skinny** | SCCP 接続 |
| **smtp_data** | SMTP メール データ接続 |
| **sqlnet_fixup_data** | SQL*Net データ インスペクション エンジン接続 |
| **tcp_embryonic** | TCP 初期接続 |
| **vpn_orphan** | 孤立した VPN トンネル フロー |

**detail** オプションを使用すると、次の表で定義されている接続フラグを使用して、変換タイプとインターフェイスに関する情報が表示されます。

**表 *22* : 接続フラグ**

| Flag | 説明 |
|---|---|
| a | SYN に対するイニシエータ ACK を待機 |
| A | SYN に対するレスポンダ ACK を待機 |
| b | TCP ステートバイパスまたは固定 |
| B | サーバー証明書の TCP プローブ |
| C | コンピュータ テレフォニー インターフェイス クイック バッファ エンコーディング（CTIQBE）メディア接続。 |
| c | 集中クラスタ |
| d | dump |
| D | DNS |

| Flag | 説明 |
|---|---|
| E | 外部バック接続。これは、内部ホストから開始されている必要があるセカンダリ データ接続です。たとえば、内部クライアントがPASVコマンドを発行し、外部サーバが受け入れた後、脅威に対する防御はFTPを使用してこのフラグが設定された外部バック接続を事前割り当てします。内部クライアントがサーバに接続しようとすると、脅威に対する防御 はこの接続試行を拒否します。外部サーバーだけが事前割り当て済みのセカンダリ接続を使用できます。 |
| e | 半分散 |
| f | イニシエータ FIN |
| F | レスポンダ FIN |
| g | メディア ゲートウェイ コントロール プロトコル（MGCP）接続 |
| G | group<br>Gフラグは、接続がグループの一部であることを示します。制御接続および関連するすべてのセカンダリ接続を指定するために、GRE および FTP Strict 検査によって設定されます。制御接続が切断されると、関連するすべてのセカンダリ接続も切断されます。 |
| h | H.225 |
| H | H.323 |
| i | 不完全な TCP 接続または UDP 接続 |
| I | イニシエータデータ |
| j | GTP データ |
| J | GTP |
| k | Skinny Client Control Protocol（SCCP）メディア接続 |
| K | GTP t3 応答 |
| L | カプセル化を解除する外部フロー |
| m | SIP メディア接続 |
| M | SMTP データ |
| n | GUP（Gatekeeper Update Protocol） |

| Flag | 説明 |
|---|---|
| N | Snort によって検査されます。<br>Snort がダウンした場合にシステムが接続を維持するように設定されている場合（デフォルトでは有効になっています）、N フラグには数値が含まれます。詳細については、**configure snort** コマンドを参照してください。<br>• 1：Snort がダウンした場合、この接続は維持されます。<br>• 2：Snort がダウンしましたが、この接続は維持されました。この接続は Snort によって検査されなくなります。<br>• 3：接続がエレファントフローに関連していることを示します。<br>• 4：エレファントフローの Snort インスペクションがバイパスされました。<br>• 5：エレファントフローに動的レート制限ポリシー（10% 削減）が適用されました。 |
| o | オフロードされたフロー。 |
| O | レスポンダデータ |
| p | パッセンジャフロー |
| P | 内部バック接続。これは、内部ホストから開始されている必要があるセカンダリデータ接続です。たとえば、内部クライアントが PORT コマンドを発行し、外部サーバーが受け入れた後、脅威に対する防御 デバイスは FTP を使用してこのフラグが設定された内部バック接続を事前割り当てします。外部サーバーがクライアントに接続しようとすると、デバイスはこの接続試行を拒否します。内部クライアントだけが事前割り当て済みのセカンダリ接続を使用できます。 |
| q | SQL*Net データ |
| Q | QUIC プロトコル。 |
| r | イニシエータが確認応答した FIN。このフラグは、イニシエータの FIN がレスポンダによって確認されたときに表示されます。 |
| R | レスポンダが確認応答した TCP 接続の FIN。このフラグは、レスポンダの FIN がイニシエータによって確認されたときに表示されます。 |
| R | UDP RPC.<br>**show conn** コマンド出力の各行は 1 つの接続（TCP または UDP）を表すため、1 行に 1 つの R フラグだけが存在します。 |
| t | SIP 一時接続。<br>UDP 接続の場合、値 t は接続が 1 分後にタイムアウトすることを示しています。 |

| Flag | 説明 |
|---|---|
| T | SIP 接続。<br>UDP 接続の場合、値 T は、**timeout sip** コマンドを使用して指定した値に従って接続がタイムアウトすることを示しています。 |
| U | up |
| v | M3UA 接続 |
| V | VPN の孤立 |
| W | WAAS |
| w | Firepower 9300 でのシャーシ間クラスタリングの場合、別のシャーシ上のバックアップオーナーでのフローを識別します。 |
| X | サービスモジュールにより検査 |
| × | 1 セッションあたり |
| y | クラスタリングの場合、バックアップスタブフローを識別します。 |
| あり | クラスタリングの場合、ディレクタスタブフローを識別します。 |
| z | クラスタリングの場合、フォワーダスタブフローを識別します。 |
| Z | ScanSafe リダイレクション |

（注） DNS サーバーを使用する接続の場合、**show conn** コマンドの出力で、接続の送信元ポートが DNS サーバーの IP アドレスに置き換えられることがあります。

複数の DNS セッションが同じ 2 つのホスト間で発生し、それらのセッションの 5 つのタプル（送信元/宛先 IP アドレス、送信元/宛先ポート、およびプロトコル）が同じものである場合、それらのセッションに対しては接続が 1 つだけ作成されます。DNS ID は *app_id* で追跡され、各 app_id のアイドル タイマーは独立して実行されます。

app_id の有効期限はそれぞれ独立して満了するため、正当な DNS 応答が 脅威に対する防御 デバイスを通過できるのは、限られた期間内だけであり、リソースの継続使用はできません。ただし、**show conn** コマンドを入力すると、DNS 接続のアイドルタイマーが新しい DNS セッションによってリセットされているように見えます。これは共有 DNS 接続の性質によるものであり、仕様です。

（注） 接続の非アクティブ期間（デフォルトは 1:00:00）中に TCP トラフィックがまったく発生しなかった場合は、接続が終了し、対応する接続フラグエントリも表示されなくなります。

LAN-to-LAN トンネルまたはネットワーク拡張モード トンネルがドロップし、回復しない場合は、孤立したトンネル フローが数多く発生します。このようなフローはトンネルのダウンによって切断されませんが、これらのフローを介して通過を試みるすべてのデータがドロップされます。**show conn** コマンドの出力では、このような孤立したフローを V フラグで示します。

バージョン 6.2.0.2 および 6.2.3 以降で **count** オプションを使用すると、次の表で定義されているステータスを使用して、接続数に関する情報が表示されます。

**表 *23 :* 接続状況（*Connection Status*）**

| ステータス（Status） | 説明 |
|---|---|
| enabled | 現在 preserve-connection が有効になっている接続数。 |
| in effect | 現在 preserve-connection が実行されている接続数。 |
| most enabled | 保持された接続の最大数。 |
| most in effect | 同時に保持された接続の最大数。 |

接続データレートトラッキング機能の現在の状態（有効または無効）を表示するには、**data-rate** キーワードを使用します。**data-rate filter** キーワードを使用して、データレート値（1 秒あたりのバイト数）を基に接続をフィルタ処理します。接続データをフィルタリングするには、比較演算子（より小さい、等しい、より大きい）を使用します。出力には、順方向と逆方向の両方のフローについて、アクティブな接続と 2 つのデータレート値（瞬時（1 秒）および最大データレート値）が表示されます。

## 例

次に、**show conn** コマンドの出力例を示します。次に、内部ホスト 10.1.1.15 から 10.10.49.10 の外部 Telnet サーバーへの TCP セッション接続の例を示します。B フラグが存在しないため、接続は内部から開始されています。「U」、「I」および「O」フラグは、接続がアクティブであり、着信データと発信データを受信したことを示します。

```
> show conn
54 in use, 123 most used
TCP out 10.10.49.10:23 in 10.1.1.15:1026 idle 0:00:22, bytes 1774, flags UIO
UDP out 10.10.49.10:31649 in 10.1.1.15:1028 idle 0:00:14, bytes 0, flags D-
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:5060, idle 0:00:24, bytes 1940435, flags
UTIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:5060, idle 0:00:42, bytes 2328346, flags
UTIOB
TCP dmz 10.10.10.51:50196 inside 192.168.1.22:2000, idle 0:00:04, bytes 31464, flags UIB
TCP dmz 10.10.10.51:52738 inside 192.168.1.21:2000, idle 0:00:09, bytes 129156, flags
UIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:0, idle 0:00:42, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):49736 inside 192.168.1.21:0, idle 0:01:32, bytes
0, flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:00:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:01:34, bytes
0, flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:02:24, bytes 0, flags Ti
```

```
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:03:34, bytes
0, flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:04:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:05:34, bytes
0, flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:06:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:07:34, bytes
0, flags Ti
```

次に、**show conn count** コマンドの出力例を示します。

```
> show conn count
30 in use, 3194964 most used
Cluster:
        fwd connections: 1 in use, 52 most used
        dir connections: 7 in use, 43826206 most used
        centralized connections: 0 in use, 15 most used
Inspect Snort:
        preserve-connection: 100 enabled, 80 in effect, 400 most enabled, 300 most in
effect
```

次に、**show conn detail** コマンドの出力例を示します。次に、外部ホスト 10.10.49.10 から内部ホスト 10.1.1.15 への UDP 接続の例を示します。D フラグは、DNS 接続であることを示しています。1028 は、接続上の DNS ID です。

```
> show conn detail
2 in use, 39 most used
Inspect Snort:
        preserve-connection: 2 enabled, 0 in effect, 39 most enabled, 0 most in effect
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,
       b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - initiator FIN, f - responder FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - decap tunnel, M - SMTP data, m - SIP media
       N - inspected by Snort (1 - preserve-connection enabled, 2 - preserve-connection
 in effect)
       n - GUP, O - responder data, o - offloaded,
       P - inside back connection, p - passenger flow
       q - SQL*Net data, R - initiator acknowledged FIN,
       R - UDP SUNRPC, r - responder acknowledged FIN,
       T - SIP, t - SIP transient, U - up,
       V - VPN orphan, v - M3UA W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow

TCP out: 151.101.128.134/443 in: 192.168.1.9/51570,
    flags UfrxIO N1, idle 39s, uptime 10m39s, timeout 10m0s, bytes 4698, xlate id
0x2b8a6ec9b140
  Initiator: 192.168.1.9, Responder: 151.101.128.134
  Connection lookup keyid: 23610071

TCP out: 151.101.120.134/443 in: 192.168.1.9/51568,
    flags UfrxIO N1, idle 39s, uptime 10m40s, timeout 10m0s, bytes 5564, xlate id
0x2b8a6ec9ad40
```

```
  Initiator: 192.168.1.9, Responder: 151.101.120.134
 Connection lookup keyid: 23388003
```

次に、**show conn** コマンドの出力例を示します。V フラグで示されているとおり、孤立したフローが存在します。

```
> show conn
16 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:21 idle 0:00:00, bytes 1048, flags UOVB
TCP out 192.168.110.251:21137 in 192.168.150.252:21 idle 0:00:00, bytes 1048, flags UIOB
```

孤立したフローがあるこのような接続へのレポートを制限するには、次の例で示すように、**show conn state** コマンドに **vpn_orphan** オプションを追加します。

```
> show conn state vpn_orphan
14 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:5013, idle 0:00:00, bytes 2841019, flags
 UOVB
```

クラスタリングの場合、接続フローをトラブルシュートするには、最初にすべてのユニットの接続を一覧表示します。一覧表示するには、マスターユニットで **cluster exec show conn** コマンドを入力します。ディレクタ（Y）、バックアップ（y）、およびフォワーダ（z）のフラグを持つフローを探します。次の例には、3 つのすべてのデバイスでの 172.18.124.187:22 から 192.168.103.131:44727 への SSH 接続が示されています。脅威に対する防御1 には z フラグがあり、この接続のフォワーダであることを表しています。脅威に対する防御3 には Y フラグがあり、この接続のディレクタであることを表しています。脅威に対する防御2 には特別なフラグはなく、これがオーナーであることを表しています。アウトバウンド方向では、この接続のパケットは 脅威に対する防御2 の内部インターフェイスに入り、外部インターフェイスから出ていきます。インバウンド方向では、この接続のパケットは 脅威に対する防御1 および 脅威に対する防御3 の外部インターフェイスに入り、クラスタ制御リンクを介して 脅威に対する防御2 に転送され、次に 脅威に対する防御2 の内部インターフェイスから出ていきます。

```
> cluster exec show conn
FTD1(LOCAL):**************************************************
18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727,
idle 0:00:00, bytes 37240828, flags z
FTD2:**************************************************
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727,
idle 0:00:00, bytes 37240828, flags UIO
FTD3:**************************************************
10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727,
idle 0:00:03, bytes 0, flags  Y
```

脅威に対する防御2 での show conn detail の出力は、最新のフォワーダが 脅威に対する防御1 であったことを示しています。

```
> show conn detail
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility,
       M - SMTP data, m - SIP media, n - GUP
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow
TCP outside: 172.18.124.187/22 inside: 192.168.103.131/44727,
    flags UIO , idle 0s, uptime 25s, timeout 1h0m, bytes 1036044,
cluster sent/rcvd bytes 0/1032983, cluster sent/rcvd total bytes 0/1080779, owners (1,255)
Traffic received at interface outside
        Locally received: 0 (0 byte/s)
        From most recent forwarder FTD1: 1032983 (41319 byte/s)
Traffic received at interface inside
        Locally received: 3061 (122 byte/s)
```

**detail** キーワードを使用すると、デッド接続検出（DCD）プローブの情報が表示されます。この情報は、発信側と応答側で接続がプローブされた頻度を示します。たとえば、DCD 対応接続の接続詳細は次のようになります。

```
TCP dmz: 10.5.4.11/5555 inside: 10.5.4.10/40299,
    flags UO , idle 1s, uptime 32m10s, timeout 1m0s, bytes 11828,
cluster sent/rcvd bytes 0/0, owners (0,255)
  Traffic received at interface dmz
        Locally received: 0 (0 byte/s)
  Traffic received at interface inside
        Locally received: 11828 (6 byte/s)
  Initiator: 10.5.4.10, Responder: 10.5.4.11
  DCD probes sent: Initiator 5, Responder 5
```

次の例では、接続データレートトラッキング機能のステータスを表示する方法について示します。

```
ciscoasa# show conn data-rate
Connection data rate tracking is currently enabled.
```

次の例では、指定したデータレートに基づいて接続をフィルタリングする方法について示します。

```
firepower# show conn detail data-rate-filter ?
eq  Enter this keyword to show conns with data-rate equal to specified value
gt  Enter this keyword to show conns with data-rate greater than specified value
lt Enter this keyword to show conns with data-rate less than specified value
firepower# show conn detail data-rate-filter gt ?
```

```
<0-4294967295> Specify the data rate value in bytes per second
firepower# show conn detail data-rate-filter gt 123 | grep max rate
max rate: 3223223/399628 bytes/sec
max rate: 3500123/403260 bytes/sec
```

B フラグを使用した **show conn** と **show conn detail** の出力例を次に示します。B フラグは、TCP フローを使用して TLS1.3 サーバー証明書を取得することを示します。TLS 1.3 証明書の要求がクライアントから 脅威に対する防御 接続に取得されると、TLS 1.3 サーバーと 脅威に対する防御 の間に別の接続が確立されます。結果として、脅威に対する防御 とクライアントの間に 1 つの接続が確立され、TLS 1.3 サーバーと 脅威に対する防御 の間には別の接続が確立されます。

```
>show conn
1 in use, 3 most used
Inspect Snort:
       preserve-connection: 1 enabled, 0 in effect, 1 most enabled, 0 most in effect
 TCP outside  33.33.33.2:80 inside  1.1.1.2:35226, idle 0:00:00, bytes 246324931, flags
 UIOBN1

> show conn detail
1 in use, 3 most used
Inspect Snort:
       preserve-connection: 1 enabled, 0 in effect, 1 most enabled, 0 most in effect
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,
       b - TCP state-bypass or nailed,
       B - TCP probe for server certificate
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - initiator FIN, f - responder FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - decap tunnel, M - SMTP data, m - SIP media
       N - inspected by Snort (1 - preserve-connection enabled, 2 - preserve-connection
 in effect)
       n - GUP, O - responder data, o - offloaded,
       P - inside back connection, p - passenger flow
       q - SQL*Net data, R - initiator acknowledged FIN,
       R - UDP SUNRPC, r - responder acknowledged FIN,
       T - SIP, t - SIP transient, U - up,
       V - VPN orphan, v - M3UA W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow

TCP outside: 33.33.33.2/80 inside: 1.1.1.2/35226,
    flags UIOBN1, idle 0s, uptime 12s, timeout 1h0m, bytes 698500915
  Initiator: 1.1.1.2, Responder: 33.33.33.2
  Connection lookup keyid: 865399
```

次に、**show conn detail** コマンドの出力例を示します。この例では N4 が表示され、エレファントフローに対する Snort インスペクションがバイパスされたことが示されています。

```
> show conn detail
0 in use, 19 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 1 most enabled, 0 most in effect
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,
       B - TCP probe for server certificate,
```

```
      b - TCP state-bypass or nailed,
      C - CTIQBE media, c - cluster centralized,
      D - DNS, d - dump, E - outside back connection, e - semi-distributed,
      F - initiator FIN, f - responder FIN,
      G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,
      i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
      k - Skinny media, L - decap tunnel, M - SMTP data, m - SIP media
      N - inspected by Snort (1 - preserve-connection enabled, 2 - preserve-connection
 in effect,
          3 - elephant-flow, 4 - elephant-flow bypassed, 5 - elephant-flow throttled)
      n - GUP, O - responder data, o - offloaded,
      P - inside back connection, p - passenger flow
      q - SQL*Net data, R - initiator acknowledged FIN,
      R - UDP SUNRPC, r - responder acknowledged FIN,
      T - SIP, t - SIP transient, U - up,
      V - VPN orphan, v - M3UA W - WAAS,
      w - secondary domain backup,
      X - inspected by service module,
      x - per session, Y - director stub flow, y - backup stub flow,
      Z - Scansafe redirection, z - forwarding stub flow

TCP outside_https: 172.16.4.1/80 inside_https: 172.16.77.1/38992,
    flags UIO N1N4, idle 0s, uptime 2m24s, timeout 1h0m, bytes 1891172595
  Initiator: 172.16.77.1, Responder: 172.16.4.1
  Connection lookup keyid: 1556755610
```

この例では出力に N5 が表示され、エレファントフローに動的なレート制限ポリシー（10% 削減）が適応されたことが示されています。

```
> show conn detail
0 in use, 19 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 1 most enabled, 0 most in effect
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,
       B - TCP probe for server certificate,
       b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - initiator FIN, f - responder FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - decap tunnel, M - SMTP data, m - SIP media
       N - inspected by Snort (1 - preserve-connection enabled, 2 - preserve-connection
 in effect,
          3 - elephant-flow, 4 - elephant-flow bypassed, 5 - elephant-flow throttled)
       n - GUP, O - responder data, o - offloaded,
       P - inside back connection, p - passenger flow
       q - SQL*Net data, R - initiator acknowledged FIN,
       R - UDP SUNRPC, r - responder acknowledged FIN,
       T - SIP, t - SIP transient, U - up,
       V - VPN orphan, v - M3UA W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow

TCP outside_https: 172.16.4.1/80 inside_https: 172.16.77.1/38822,
   flags UIO N1N5, qos-rule-id 20000, idle 0s, uptime 4m8s, timeout 1h0m, bytes 585732628

  Initiator: 172.16.77.1, Responder: 172.16.4.1
  Connection lookup keyid: 1933458538
```

関連コマンド

| コマンド | 説明 |
| --- | --- |
| **clear conn** | 接続をクリアします。 |
| **clear conn data-rate** | 保存されている現在の最大データレートをクリアします。 |

# show console-output

現在キャプチャされているコンソール出力を表示するには、**show console-output** コマンドを使用します。

**show console-output**

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、**show console-output** コマンドの出力例を示します。

```
> show console-output
Message #1 : Message #2 : Setting the offload CPU count to 0
Message #3 :
Compiled on Fri 20-May-16 13:36 PDT by builders
Message #4 :
Total NICs found: 14
Message #5 : i354 rev03 Gigabit Ethernet @ irq255 dev 20 index 08 MAC: e865.49b8.97f1
Message #6 : ivshmem rev03 Backplane Data Interface     @ index 09 MAC: 0000.0001.0002
Message #7 : en_vtun rev00 Backplane Control Interface  @ index 10 MAC: 0000.0001.0001
Message #8 : en_vtun rev00 Backplane Int-Mgmt Interface    @ index 11 MAC: 0000.0001.0003
Message #9 : en_vtun rev00 Backplane Ext-Mgmt Interface    @ index 12 MAC: 0000.0000.0000
Message #10 : en_vtun rev00 Backplane Tap Interface     @ index 13 MAC: 0000.0100.0001
Message #11 : Running Permanent Message
#12 : Activation Key: Message
#13 : 0x00000000 Message
#14 : 0x00000000 Message
#15 : 0x00000000 Message
#16 : 0x00000000 Message
#17 : 0x00000000 Message #18 :
Message #19 : The Running Activation Key is not valid, using default settings:
Message #20 :
(...output truncated...)
```

# show coredump

パケットエンジンのコアダンプ生成の設定を表示するには、**show coredump** コマンドを入力します。

**show coredump**

## 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

パケットエンジンのコアダンプ生成は、デフォルトで有効になっています。

このコマンドは、Firepower 2100 シリーズのみで使用できます。サポートされていないプラットフォームでこのコマンドを入力すると、次のメッセージが返されます。

```
This command is not available on this platform.
```

### 例

次に、パケットエンジンのコアダンプの生成が有効になっている例を示します。

```
> show coredump

Process Type: Coredump State:
packet-engine enabled
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure coredump packet-engine** | パケットエンジンのコアダンプ生成を有効または無効にします。 |

# show counters

プロトコルスタックカウンタを表示するには、**show counters** コマンドを使用します。

**show counters** ［**all** | **summary** | **top** *N*］［**description**］［**detail**］［**protocol** *protocol_name* ［**:***counter_name*］］［ **threshold** *N*］

## 構文の説明

| | |
|---|---|
| **all** | フィルタの詳細を表示します。 |
| *:counter_name* | カウンタを名前で指定します。 |
| **description** | さまざまなカウンタと説明を表示します。 |
| **detail** | 詳細なカウンタ情報を表示します。 |
| **protocol** *protocol_name* | 指定したプロトコルのカウンタを表示します。オプションのリストを表示するには、「?」と入力します。 |
| **summary** | カウンタの要約を表示します。 |
| **threshold** *N* | 指定したしきい値以上のカウンタのみを表示します。指定できる範囲は 1 ～ 4294967295 です。 |
| **top** *N* | 指定したしきい値以上のカウンタを表示します。指定できる範囲は1 ～ 4294967295 です。 |

## コマンド デフォルト

デフォルトは **show counters summary detail threshold 1** です。

## 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、デフォルトの情報を表示する例を示します。

```
> show counters
Protocol     Counter                                    Value   Context
IP           IN_PKTS                                   785064   Summary
IP           OUT_PKTS                                   19196   Summary
IP           OUT_DROP_DWN                              177099   Summary
IP           TO_ARP                                    785064   Summary
TCP          OUT_PKTS                                   38378   Summary
TCP          SESS_CTOD                                  19189   Summary
TCP          OUT_CLSD                                   19189   Summary
TCP          HASH_ADD                                   19189   Summary
TCP          SND_SYN                                    19189   Summary
SSLERR       BAD_SIGNATURE                                  3   Summary
SSLDEV       NEW_CTX                                        3   Summary
VPIF         BAD_VALUE                                    673   Summary
```

```
VPIF          NOT_FOUND                                 106843325    Summary
```

| Command | 説明 |
|---|---|
| **clear counters** | プロトコル スタック カウンタをクリアします。 |

# show cpu

CPU の使用状況についての情報を表示するには、**show cpu** コマンドを使用します。

**show cpu** ［**detailed** | **external** | **profile** ［**dump**］ | **system** ［*processor_num*］］
**show cpu core** ［**all** | *core_id*］
**show cpu usage** ［**detailed** | **core** ［**all** | *core_id*］ ］

## 構文の説明

| | |
|---|---|
| **core** [**all** \| *core_id*] | 各コアのCPU統計情報を表示します。すべてのコアを表示するか（デフォルト）、番号でコアを指定できます。デバイスで使用可能なコア番号を表示するには、パラメータなしでキーワードを使用します。コア番号は 0 から始まります。<br><br>**show cpu core** コマンドと **show cpu usage core** コマンドは、同じ情報を提供します。 |
| **detailed** | （オプション）CPU の内部使用に関する詳細な情報を表示します。 |
| **external** | （オプション）外部プロセスに関する CPU 使用状況を表示します。 |
| **profile** [**dump**] | （オプション）CPUプロファイリングデータを表示します。プロファイリングデータのダンプを表示するには、**dump** キーワードを含めます。 |
| **system** [*processor_num*] | （オプション）システム全体に関連した情報を表示します。必要に応じて、プロセッサ番号を指定して特定のプロセッサの情報を表示できます。CPU と呼ばれる使用可能なプロセッサの数を表示するには、キーワードを指定せずにこのコマンドを使用します。プロセッサ番号は 0 から始まります。したがって、出力に 8 つの CPU があることが示されている場合、システムに対して有効な数値は 0 ー 7 になります。 |
| **usage** | （任意）CPU使用状況を表示します。これがデフォルトのオプションです。 |

## 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

CPU 使用状況は、5 秒ごとの負荷の近似値を使用し、この概算値をさらに以降の 2 つの移動平均に適用することによって算出されます。

**show cpu profile dump** コマンドを **cpu profile activate** コマンドとともに使用して、CPU 問題のトラブルシューティング時に TAC が使用する情報を収集できます。**show cpu profile dump** コマンドの出力は、16 進形式で表示されます。

**detailed** ビューと **core** ビューでは、全体的な CPU 使用率が低いときにコアの使用率がゼロになっていることは珍しくありません。

Threat Defense Virtual の場合、**show cpu** コマンドは、VM に割り当てられた CPU の数が vCPU プラットフォームライセンスの制限に基づいて許可された制限内にあるかどうかも示します。ステータスは、Compliant、Noncompliant: Over-provisioned、または Noncompliant: Under-provisioned のいずれかになります。この情報は正確ではない可能性があります。

### 例

次に、CPU 使用状況を表示する例を示します。

```
> show cpu
CPU utilization for 5 seconds = 18%; 1 minute: 18%; 5 minutes: 18%
```

次に、CPU の使用状況に関する情報を表示する例を示します。

```
> show cpu detailed
Break down of per-core data path versus control point cpu usage:
Core         5 sec            1 min            5 min
Core 0       0.0 (0.0 + 0.0)  3.3 (0.0 + 3.3)  2.4 (0.0 + 2.4)
Current control point elapsed versus the maximum control point elapsed for:
      5 seconds = 99.0%; 1 minute: 99.8%; 5 minutes: 95.9%
CPU utilization of external processes for:
      5 seconds = 0.2%; 1 minute: 0.0%; 5 minutes: 0.0%
Total CPU utilization for:
      5 seconds = 0.2%; 1 minute: 3.3%; 5 minutes: 2.5%
```

（注） 「Current control point elapsed versus the maximum control point elapsed for」という文は、コントロール ポイントの現在の負荷が、定義された期間内に検出された最大負荷と比較されることを意味します。これは絶対値ではなく比率です。5 秒間隔に対して 99% という数値は、コントロール ポイントの現在の負荷が、その 5 秒間隔における最大負荷の 99% であることを意味します。負荷が常に増加し続ける場合、負荷は常に 100% になります。ただし、最大絶対値が定義されていないため、実際の CPU には引き続き多くの空き容量がある可能性があります。

次に、システムレベルの CPU 使用状況を表示する例を示します。最初の行の「(2 CPU)」という表示に注目してください。これはデバイス上のプロセッサの数です。

```
> show cpu system
Linux 3.10.62-ltsi-WR6.0.0.27_standard (ftd1.example.com)        10/20/16        _x86_64_    (2 CPU)

Time         CPU    %usr   %nice    %sys %iowait    %irq   %soft  %steal  %guest  %gnice   %idle
15:48:26     all   50.36    0.00   10.04    0.78    0.00    0.03    0.00    0.00    0.00   38.79
```

次の表で、**show cpu system** 出力の各フィールドについて説明します。

表 *24 : Show CPU System* のフィールド

| フィールド | 説明 |
|---|---|
| Time | 該当する数値が確認された時刻。 |
| CPU | プロセッサの数。 |
| %user | ユーザ レベル（アプリケーション）で実行中に生じたCPU使用率のパーセンテージ。 |
| %nice | 高い優先度で実行中に生じた CPU 使用率のパーセンテージ。 |
| %sys | システム レベル（カーネル）で実行中に生じたCPU使用率のパーセンテージ。これには、サービスの割り込みやsoftirqsで経過する時間は含まれません。softirq（ソフトウェアの割り込み）は、複数の CPU で同時に実行できる最大 32 個の列挙されたソフトウェア割り込みの 1 つです。 |
| %iowait | システムに未処理のディスク I/O 要求があったときに、CPU がアイドル状態だった時間の割合（パーセンテージ）。 |
| %irq | 割り込みを行うために CPU が費やした時間の割合（パーセンテージ）。 |
| %soft | softirqs を行うために CPU が費やした時間の割合（パーセンテージ）。 |
| %steal | ハイパーバイザが別の仮想プロセッサを実行しているときに、仮想CPUが強制的な待機で費やした時間の割合（パーセンテージ） |
| %guest | 仮想プロセッサを実行するために CPU が費やした時間の割合（パーセンテージ）。 |
| %gnice | 仮想プロセッサに高い優先度を付与するゲストレベルでの実行中に生じた CPU 使用率のパーセンテージ。 |
| %idle | CPU がアイドル状態で、システムに未処理のディスク I/O 要求がなかった時間の割合（パーセンテージ）。 |

次の例では、プロファイラをアクティブ化して、デフォルトである1000個のサンプルを格納するように指示します。次に、**show cpu profile** コマンドは、プロファイリングが進行中であることを示します。いくらかの時間が経過してから、次の**show cpu profile** コマンドは、プロファイリングが完了したことを示します。最後に、**show cpu profile dump** コマンドを使用して結果を取得します。出力をコピーし、シスコテクニカルサポートに提出します。完全な出力を得るには、SSH セッションをログに記録する必要があります。

```
> cpu profile activate
Activated CPU profiling for 1000 samples.
Use "show cpu profile" to display the progress or "show cpu profile dump" to interrupt
profiling and display the incomplete results.
> show cpu profile
CPU profiling started: 16:13:48.279 UTC Thu Oct 20 2016
```

```
CPU profiling currently in progress:
    Core 0: 501 out of 1000 samples collected.
    CP: 586 out of 1000 samples collected.
Use "show cpu profile dump" to see the results after it is complete or to interrupt
profiling and display the incomplete results.
> show cpu profile
CPU profiling started: 16:13:48.279 UTC Thu Oct 20 2016
CPU Profiling has stopped.
    Core 0 done with 1000 samples
    CP done with 1000 samples
Use "show cpu profile dump" to see the results.
> show cpu profile dump
(...output omitted...)
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear cpu profile** | CPU プロファイリングデータをクリアします。 |
| **cpu profile activate** | CPU プロファイリングをアクティベートします。 |
| **show counters** | プロトコル スタック カウンタを表示します。 |

# show crashinfo

フラッシュメモリに格納されたクラッシュファイルの内容を表示するには、**show crashinfo** コマンドを入力します。

**show crashinfo** ［**console** | **module** *number* | **save** | **webvpn** ［**detailed**］］

## 構文の説明

| | |
|---|---|
| **console** | （オプション）crashinfo コンソール出力のステータスを表示します。 |
| **module** *number* | （オプション）指定されたモジュールから取得したクラッシュ情報を表示します。モジュールは番号で示されます（例：1）。 |
| **save** | （オプション）クラッシュ情報をフラッシュメモリに保存するようにデバイスが設定されているかどうかを表示します。 |
| **webvpn** [**detailed**] | （任意）脅威に対する防御のクラッシュリカバリダンプを表示します。 |

## 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

クラッシュファイルがテストクラッシュから生成された（**crashinfo test** コマンドで生成された）場合、クラッシュファイルの最初の文字列は「:Saved_Test_Crash」であり、最後の文字列は「:End_Test_Crash」です。クラッシュファイルが実際のクラッシュから生成されたる場合、クラッシュファイルの最初の行の文字列は「:Saved_Crash」で、最後の文字列は「:End_Crash」です（これには、**crashinfo force page-fault** または **crashinfo force watchdog** コマンドの使用によるクラッシュが含まれます）。

FIPS 140-2 に準拠していることにより、キーやパスワードなどのクリティカル セキュリティ パラメータをクリプト境界（シャーシ）の外側に配布することが禁止されています。アサートまたはチェックヒープのエラーによってデバイスがクラッシュしたとき、コンソールにダンプされるスタック領域やメモリ領域には、機密データが含まれていることがあります。この出力は、FIPS モードでは表示されないようにする必要があります。

### 例

次に、crashinfo 情報がない場合の例を示します。

```
> show crashinfo
------------------ show crashinfo module 1 ------------------
INFO: This module has no crashinfo available.
```

次に、現在のクラッシュ情報コンフィギュレーションを表示する例を示します。

```
> show crashinfo save
```

```
crashinfo save enable
```

次に、crashinfo コンソール出力のステータスの例を示します。

```
> show crashinfo console
crashinfo console enable
```

次に、クラッシュ ファイルテストの出力例を示しますこのテストでは、脅威に対する防御デバイスは実際にはクラッシュしません。このテストで提供されるのは、シミュレートされたサンプルファイルです。

```
> crashinfo test
> show crashinfo
: Saved_Test_Crash
Thread Name: ci/console (Old pc 0x001a6ff5 ebp 0x00e88920)
Traceback:
0: 00323143
1: 0032321b
2: 0010885c
(...Remaining output truncated...)
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear crashinfo** | クラッシュ ファイルの内容を削除します。 |
| **crashinfo force** | 脅威に対する防御 デバイスを強制的にクラッシュさせます。 |
| **crashinfo test** | 脅威に対する防御デバイスでフラッシュメモリ内のファイルにクラッシュ情報を保存できるかどうかをテストします。 |

# show crypto accelerator load-balance

ハードウェア暗号化アクセラレータ MIB からのアクセラレータ固有のロードバランシング情報を表示するには、**show crypto accelerator load-balance** コマンドを使用します。

**show crypto accelerator load-balance** ［**ipsec** | **ssl** | **detail** ［**ipsec | ssl**］］

## 構文の説明

| | |
|---|---|
| **detail** | （任意）詳細情報を表示します。このオプションの後に、**ipsec** または **ssl** キーワードを含めることができます。 |
| **ipsec** | （任意）暗号化アクセラレータ IPSec ロードバランシングの詳細を表示します。 |
| **ssl** | （任意）暗号化アクセラレータ SSL ロードバランシングの詳細を表示します。 |

## 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、グローバルな暗号化アクセラレータのロードバランシング統計情報を表示する例を示します。

```
> show crypto accelerator load-balance

                 Crypto IPSEC Load Balancing Stats:
                 ==================================

Engine      Crypto Cores             IPSEC Sessions          Active Session
                                                             Distribution (%)
======     ==============      ============================   ================
  0        IPSEC 1, SSL 1      Total:     0  Active:     0          0.0%

Commands Completed       1 second         5 second         60 second
==================       ========         ========         =========
 Engine 0 (load)            0.0%             0.0%             0.0%

Encrypted Data           1 second         5 second         60 second
==================       ========         ========         =========
 Engine 0 (load)            0.0%             0.0%             0.0%

Decrypted Data           1 second         5 second         60 second
==================       ========         ========         =========
 Engine 0 (load)            0.0%             0.0%             0.0%

Engine 0 Per Core Load Balancing Stats:
=======================================

Commands Completed       1 second         5 second        60 second
==================       ========         ========         =========
```

```
 IPSec ring 0   (load)      0.0%             0.0%             0.0%

Encrypted Data           1 second         5 second         60 second
==================       ========         ========         =========
 IPSec ring 0   (load)      0.0%             0.0%             0.0%

Decrypted Data           1 second         5 second        60 second
==================       ========         ========         =========
 IPSec ring 0   (load)      0.0%             0.0%             0.0%

                  Crypto SSL Load Balancing Stats:
                  ================================

Engine      Crypto Cores             SSL Sessions             Active Session
                                                              Distribution (%)
======     ==============      ============================   ================
  0        IPSEC 1, SSL 1      Total:     0  Active:     0         0.0%

Commands Completed       1 second         5 second         60 second
==================       ========         ========         =========
 Engine 0 (load)            0.0%             0.0%             0.0%

Encrypted Data           1 second         5 second         60 second
==================       ========         ========         =========
 Engine 0 (load)            0.0%             0.0%             0.0%

Decrypted Data           1 second         5 second         60 second
==================       ========         ========         =========
 Engine 0 (load)            0.0%             0.0%             0.0%

Engine 0 Per Core Load Balancing Stats:
=======================================

Commands Completed       1 second         5 second        60 second
==================       ========         ========         =========
 Admin ring 0   (load)      0.0%             0.0%             0.0%

Encrypted Data           1 second         5 second         60 second
==================       ========         ========         =========
 Admin ring 0   (load)      0.0%             0.0%             0.0%

Decrypted Data           1 second         5 second        60 second
==================       ========         ========         =========
 Admin ring 0   (load)      0.0%             0.0%             0.0%
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear crypto accelerator statistics** | 暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報をクリアします。 |
| **clear crypto protocol statistics** | 暗号アクセラレータ MIB にあるプロトコル固有の統計情報をクリアします。 |
| **show crypto protocol statistics** | 暗号アクセラレータ MIB からプロトコル固有の統計情報を表示します。 |

# show crypto accelerator statistics

ハードウェア クリプト アクセラレータ MIB からグローバルおよびアクセラレータ固有の統計情報を表示するには、**show crypto accelerator statistics** コマンドを使用します。

**show crypto accelerator statistics**

## 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

出力統計情報は、次のように定義されます。

Accelerator 0 はソフトウェア ベースの暗号エンジンの統計情報を示します。

Accelerator 1 はハードウェア ベースの暗号エンジンの統計情報を示します。

RSA 統計情報には、デフォルトでソフトウェアで実行される、2048 ビット キーの RSA 処理が表示されます。つまり、2048 ビット キーがある場合、IKE/SSL VPN は、IPsec/SSL ネゴシエーション フェーズ中にソフトウェアで RSA 処理を実行します。実際の IPsec/SSL トラフィックは、引き続きハードウェアを使用して処理されます。これにより、同時に開始された同時セッションが数多くある場合、CPUの高使用となります。このため、RSAキー処理が複数発生し、CPU の高使用となる可能性があります。このようにして CPU の高使用状態となった場合は、1024 ビット キーを使用して、ハードウェアで RSA キー処理を実行する必要があります。このためには、アイデンティティ証明書を再度登録する必要があります。リリース 8.3(2) 以降では、5510 から 5550 のプラットフォームで crypto engine large-mod-accel コマンドを使用して、ハードウェアでこれらの処理を実行することもできます。

2048 ビットの RSA キーを使用しており、ソフトウェアで RSA 処理が実行されている場合は、CPU プロファイリングを使用して、CPU の高使用状況の原因となっている関数を特定できます。通常、bn_* 関数と BN_* 関数は RSA に使用される大規模なデータ セットでの数学的処理であり、ソフトウェアでの RSA 処理中に CPU の使用状況を確認する場合に最も役立ちます。次に例を示します。

```
@@@@@@@@@@@@@@@@@@@@.............................. 36.50% : _bn_mul_add_words
@@@@@@@@@@..................................... 19.75% : _bn_sqr_comba8
```

Diffie-Hellman 統計情報には、ソフトウェアで 1024 より大きいモジュラス サイズの暗号処理が実行されたことが表示されます（DH5（Diffie-Hellman グループ 5 が 1536 を使用しています）など）。この場合、2048 ビット キー証明書はソフトウェアで処理されます。このため、数多くのセッションが実行されるときに CPU の高使用状況となります。

DSA 統計情報には、2 つのフェーズでのキー生成が表示されます。最初のフェーズは、アルゴリズム パラメータの選択です。このパラメータは、システムの他のユーザーと共有することがあります。2 番めのフェーズは、1 人のユーザー用の秘密キーと公開キーの算出です。

SSL 統計情報には、ハードウェア クリプト アクセラレータへの SSL トランザクションで使用される、プロセッサ集約的な公開キーの暗号化アルゴリズムに関するレコードが表示されます。

RNG 統計情報には、キーとして使用する同じ乱数のセットを自動的に生成できる送信元とレシーバに関するレコードが表示されます。

### 例

次に、グローバルなクリプトアクセラレータの統計情報を表示する例を示します。

```
> show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
[Capacity]
   Supports hardware crypto: True
   Supports modular hardware crypto: False
   Max accelerators: 1
   Max crypto throughput: 100 Mbps
   Max crypto connections: 750
[Global Statistics]
   Number of active accelerators: 1
   Number of non-operational accelerators: 0
   Input packets: 700
   Input bytes: 753488
   Output packets: 700
   Output error packets: 0
   Output bytes: 767496
[Accelerator 0]
   Status: Active
   Software crypto engine
   Slot: 0
   Active time: 167 seconds
   Total crypto transforms: 7
   Total dropped packets: 0
   [Input statistics]
      Input packets: 0
      Input bytes: 0
      Input hashed packets: 0
      Input hashed bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [Output statistics]
      Output packets: 0
      Output bad packets: 0
      Output bytes: 0
      Output hashed packets: 0
      Output hashed bytes: 0
      Encrypted packets: 0
      Encrypted bytes: 0
   [Diffie-Hellman statistics]
      Keys generated: 0
      Secret keys derived: 0
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
      Encrypted packets: 0
      Encrypted bytes: 0
```

```
      Decrypted packets: 0
      Decrypted bytes: 0
   [DSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 98
      Random number request failures: 0
[Accelerator 1]
   Status: Active
   Encryption hardware device : Cisco ASA-55x0 on-board accelerator
(revision 0x0)
                            Boot microcode   : CNlite-MC-Boot-Cisco-1.2
                            SSL/IKE microcode: CNlite-MC-IPSEC-Admin-3.03
                            IPsec microcode  : CNlite-MC-IPSECm-MAIN-2.03
   Slot: 1
   Active time: 170 seconds
   Total crypto transforms: 1534
   Total dropped packets: 0
   [Input statistics]
      Input packets: 700
      Input bytes: 753544
      Input hashed packets: 700
      Input hashed bytes: 736400
      Decrypted packets: 700
      Decrypted bytes: 719944
   [Output statistics]
      Output packets: 700
      Output bad packets: 0
      Output bytes: 767552
      Output hashed packets: 700
      Output hashed bytes: 744800
      Encrypted packets: 700
      Encrypted bytes: 728352
   [Diffie-Hellman statistics]
      Keys generated: 97
      Secret keys derived: 1
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
      Encrypted packets: 0
      Encrypted bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [DSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 1
      Random number request failures: 0
```

次の表は出力について示しています。

| 出力 | 説明 |
|---|---|
| Capacity | このセクションは、脅威に対する防御デバイスがサポートできる暗号化アクセラレーションに関連しています。 |
| Supports hardware crypto | （True/False）脅威に対する防御 デバイスはハードウェア暗号化アクセラレーションをサポートできます。 |
| Supports modular hardware crypto | （True/False）サポートされている任意のハードウェア クリプト アクセラレータを個別のプラグイン カードまたはモジュールとして挿入できます。 |
| Max accelerators | 脅威に対する防御デバイスでサポートされるハードウェア暗号化アクセラレータの最大数。 |
| Mac crypto throughput | デバイスの最大定格 VPN スループット。 |
| Max crypto connections | デバイスのサポート対象 VPN トンネルの最大数。 |
| Global Statistics | このセクションは、デバイスの複合ハードウェア クリプト アクセラレータに関連しています。 |
| Number of active accelerators | アクティブなハードウェア アクセラレータの数。アクティブなハードウェア アクセラレータが初期化されており、crypto コマンドの処理に使用可能です。 |
| Number of non-operational accelerators | 非アクティブなハードウェア アクセラレータの数。非アクティブなハードウェア アクセラレータが検出されました。初期化が完了していないか、障害が発生して使用できなくなっています。 |
| Input packets | すべてのハードウェア クリプト アクセラレータで処理される着信パケットの数。 |
| Input bytes | 処理される着信パケット内のデータのバイト数。 |
| Output packets | すべてのハードウェア クリプト アクセラレータで処理される発信パケットの数。 |
| Output error packets | エラーが検出された、すべてのハードウェア暗号アクセラレータで処理される発信パケットの数。 |
| Output bytes | 処理される発信パケット内のデータのバイト数。 |

| 出力 | 説明 |
|---|---|
| Accelerator 0 | 各セクションは、クリプト アクセラレータに関連しています。最初のセクション（Accelerator 0）は、常に、ソフトウェア クリプト エンジンです。ハードウェア アクセラレータではありませんが、脅威に対する防御はこのソフトウェア クリプト エンジンを使用して、特定のクリプト タスクを実行します。ここには、その統計情報が表示されます。Accelerators 1 以上は、常に、ハードウェア クリプト アクセラレータです。 |
| Status（ステータス） | アクセラレータのステータス。アクセラレータが初期化されているか、アクティブか、あるいは失敗したかを示します。 |
| Software crypto engine | アクセラレータのタイプとファームウェアバージョン（該当する場合）。 |
| スロット | アクセラレータのスロット番号（該当する場合）。 |
| Active time | アクセラレータがアクティブ状態であった時間の長さ。 |
| Total crypto transforms | アクセラレータによって実行された crypto コマンドの合計数。 |
| Total dropped packets | エラーのためアクセラレータによってドロップされたパケットの合計数。 |
| Input statistics | このセクションは、アクセラレータで処理された入力トラフィックに関連しています。入力トラフィックは、複合か認証、またはその両方を行う必要がある暗号文と見なされます。 |
| Input packets | アクセラレータによって処理された入力パケットの数。 |
| Input bytes | アクセラレータによって処理された入力バイト数。 |
| Input hashed packets | アクセラレータがハッシュを実行したパケットの数。 |
| Input hashed bytes | アクセラレータがハッシュを実行したバイト数。 |
| Decrypted packets | アクセラレータが対称復号化を実行したパケットの数。 |
| Decrypted bytes | アクセラレータが対称復号化を実行したバイト数。 |
| Output statistics | このセクションは、アクセラレータで処理された出力トラフィックに関連しています。入力トラフィックは、暗号化かハッシュ、またはその両方を実行する必要があるクリアテキストと見なされます。 |
| Output packets | アクセラレータによって処理された出力パケットの数。 |

| 出力 | 説明 |
|---|---|
| Output bad packets | エラーが検出された、アクセラレータで処理された出力パケットの数。 |
| Output bytes | アクセラレータによって処理された出力バイト数。 |
| Output hashed packets | アクセラレータが出力ハッシュを実行したパケットの数。 |
| Output hashed bytes | アクセラレータが出力ハッシュを実行したバイト数。 |
| Encyrpted packets | アクセラレータが対称暗号化を実行したパケットの数。 |
| Encyrpted bytes | アクセラレータが対称暗号化を実行したバイト数。 |
| Diffie-Hellman statistics | このセクションは、Diffie-Hellman のキー交換処理に関連しています。 |
| Keys generated | アクセラレータによって生成された Diffie-Hellman キー セットの数。 |
| Secret keys derived | アクセラレータによって生成された Diffie-Hellman 共有秘密の数。 |
| RSA statistics | このセクションは、RSA 暗号処理に関連しています。 |
| Keys generated | アクセラレータによって生成された RSA キー セットの数。 |
| Signatures | アクセラレータによって実行された RSA シグニチャ処理の数。 |
| Verifications | アクセラレータによって実行された RSA シグニチャ確認の数。 |
| Encrypted packets | アクセラレータが RSA 暗号化を実行したパケットの数。 |
| Decrypted packets | アクセラレータが RSA 復号化を実行したパケットの数。 |
| Decrypted bytes | アクセラレータが RSA 復号化を実行したデータのバイト数。 |
| DSA statistics | このセクションは、DSA 処理に関連しています。DSA はバージョン 8.2 以上ではサポートされないため、この統計情報は表示されません。 |
| Keys generated | アクセラレータによって生成された DSA キー セットの数。 |
| Signatures | アクセラレータによって実行された DSA シグニチャ処理の数。 |
| Verifications | アクセラレータによって実行された DSA シグニチャ確認の数。 |

| 出力 | 説明 |
|---|---|
| SSL statistics | このセクションは、SSL レコード処理に関連しています。 |
| Outbound records | アクセラレータによって暗号化され、認証されたSSLレコードの数。 |
| Inbound records | アクセラレータによって復号化され、認証されたSSLレコードの数。 |
| RNG statistics | このセクションは、乱数生成に関連しています。 |
| Random number requests | アクセラレータに対する乱数の要求の数。 |
| Random number request failures | アクセラレータに対する乱数要求のうち、失敗した要求の数。 |

IPsecフローオフロードをサポートするプラットフォームでは、出力にはオフロードフローの統計が表示されますが、グローバルカウンタには、デバイス上のすべてのアクセラレータエンジンのオフロードフローと非オフロードフローの合計が表示されます。

```
> show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
[Capability]
   Supports hardware crypto: True
   Supported TLS Offload Mode: HARDWARE
   Supports modular hardware crypto: False
   Max accelerators: 3
   Max crypto throughput: 3000 Mbps
   Max crypto connections: 3000
[Global Statistics]
   Number of active accelerators: 2
   Number of non-operational accelerators: 0
   Input packets: 108
   Input bytes: 138912
   Output packets: 118
   Output error packets: 0
   Output bytes: 142329

[Accelerator 0]
   Status: OK
   Software crypto engine
   Slot: 0
   Active time: 489 seconds
   Total crypto transforms: 2770
   Total dropped packets: 0
   [Input statistics]
      Input packets: 0
      Input bytes: 19232
      Input hashed packets: 0
      Input hashed bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 19232
   [Output statistics]
      Output packets: 0
```

```
      Output bad packets: 0
      Output bytes: 18784
      Output hashed packets: 0
      Output hashed bytes: 0
      Encrypted packets: 0
      Encrypted bytes: 18784
   [Diffie-Hellman statistics]
      Keys generated: 0
      Secret keys derived: 0
   [RSA statistics]
      Keys generated: 1
      Signatures: 1
      Verifications: 1
      Encrypted packets: 1
      Encrypted bytes: 28
      Decrypted packets: 1
      Decrypted bytes: 256
   [ECDSA statistics]
      Keys generated: 13
      Signatures: 12
      Verifications: 15
   [EDDSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 0
      Random number request failures: 0
   [HMAC statistics]
      HMAC requests: 54

[Accelerator 1]
   Status: OK
   Encryption hardware device : Cisco ASA Crypto on-board accelerator (revision 0x1)
                              AE microcode        : CNN5x-MC-AE-MAIN-0007
                              SE SSL microcode    : CNN5x-MC-SE-SSL-0018
   Slot: 1
   Active time: 497 seconds
   Total crypto transforms: 2910
   Total dropped packets: 0
   [Input statistics]
      Input packets: 4
      Input bytes: 13056
      Input hashed packets: 0
      Input hashed bytes: 0
      Decrypted packets: 4
      Decrypted bytes: 6528
   [Output statistics]
      Output packets: 14
      Output bad packets: 0
      Output bytes: 20786
      Output hashed packets: 0
      Output hashed bytes: 0
      Encrypted packets: 14
      Encrypted bytes: 10393
   [Offloaded Input statistics]
      Input packets: 106
      Input bytes: 115328
      Input hashed packets: 0
      Input hashed bytes: 0
      Decrypted packets: 107
```

```
   Decrypted bytes: 112992
[Offloaded Output statistics]
   Output packets: 107
   Output bytes: 116416
   Output hashed packets: 0
   Output hashed bytes: 0
   Encrypted packets: 107
   Encrypted bytes: 112992
Total dropped packets: 0
[Diffie-Hellman statistics]
   Keys generated: 194
   Secret keys derived: 1
[RSA statistics]
   Keys generated: 0
   Signatures: 2
   Verifications: 1
   Encrypted packets: 3
   Encrypted bytes: 162
   Decrypted packets: 2
   Decrypted bytes: 512
[ECDSA statistics]
   Keys generated: 0
   Signatures: 0
   Verifications: 0
[EDDSA statistics]
   Keys generated: 0
   Signatures: 0
   Verifications: 0
[SSL statistics]
   Outbound records: 14
   Inbound records: 4
[RNG statistics]
   Random number requests: 34
   Random number request failures: 0
[HMAC statistics]
   HMAC requests: 26
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear crypto accelerator statistics** | 暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報をクリアします。 |
| **clear crypto protocol statistics** | 暗号アクセラレータ MIB にあるプロトコル固有の統計情報をクリアします。 |
| **show crypto protocol statistics** | 暗号アクセラレータ MIB からプロトコル固有の統計情報を表示します。 |

# show crypto accelerator usage

このコマンドを使用すると、すべてのコアにおける TLS 暗号化アクセラレーション コア使用率と平均使用率を表示できます。このコマンドは、すべてのハードウェア プラットフォームで使用できるわけではありません。

TLS 暗号化アクセラレーション のガイドラインと制限事項については、『*Management Center Configuration Guide*』を参照してください。

**show crypto accelerator usage** [ **detail** ]

## 構文の説明

| | |
|---|---|
| **detail** | （オプション）管理対象デバイスに Threat Defenseコンテナインスタンス がある場合に役立つ、詳細情報を表示します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.6 | このコマンドが導入されました。 |

## 使用上のガイドライン

各コアのコア使用率と平均使用率を表示します。ハードウェアモデルによっては、このコマンドを使用できない場合や、異なる統計情報が表示される場合があります。

### 例

次に、TLS 暗号化アクセラレーション のコア使用率を表示する例を示します。

```
> show crypto accelerator usage
Crypto engine 0: 64 ADMIN SE cores, utilization 18.8%
Crypto engine 1: 64 ADMIN SE cores, utilization 17.2%
Total 128 ADMIN SE cores, utilization18%
Crypto engine 0: 64 ADMIN AE cores, utilization 0%
Crypto engine 1: 64 ADMIN AE cores, utilization 0%
Total 128 ADMIN AE cores, utilization0%
```

次に、詳細な使用状況情報を表示する例を示します。

```
 show crypto accelerator usage detail
Crypto engine 0: 64 IPSec/SSL crypto cores, utilization 18.8%
Crypto engine 1: 64 IPSec/SSL crypto cores, utilization 17.2%
Total 128 IPSec/SSL cryto cores, utilization 18%
Crypto engine 0: 64 Asymmetric crypto cores, utilization 0%
Crypto engine 1: 64 Asymmetric crypto cores, utilization 0%
Total 128 Asymmetric crypto cores, utilization 0%
```

# show crypto ca certificates

特定のトラストポイントに関連した証明書、またはシステムにインストールされたすべての証明書を表示するには、**show crypto ca certificates** コマンドを使用します。

**show crypto ca certificates** ［*trustpointname*］

## 構文の説明

| | |
|---|---|
| *trustpointname* | （任意）トラストポイントの名前。名前を指定しない場合は、 脅威に対する防御 デバイスにインストールされているすべての証明書が表示されます。 |

## 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、**show crypto ca certificates** コマンドの出力例を示します。

```
>show crypto ca certificates tp1
CA Certificate
    Status: Available
    Certificate Serial Number 2957A3FF296EF854FD0D6732FE25B45
    Certificate Usage: Signature
    Issuer:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST - massachusetts
        C = US
        EA = a@b.con
   Subject:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST = massachusetts
        C = US
        EA = example.com
   CRL Distribution Point
        ldap://w2kadvancedsrv/CertEnroll/ms-root-sha-06-2004.crl
   Validity Date:
        start date: 14:11:40 UTC Jun 26 2004
        end date: 14:01:30 UTC Jun 4 2022
   Associated Trustpoints: tp2 tp1
```

# show crypto ca crls

キャッシュされたすべての証明書失効リスト（CRL）を表示、または指定したトラストポイントにキャッシュされたすべての CRL を表示するには、**show crypto ca crl** コマンドを使用します。

**show crypto ca crls** ［**trustpool** | **trustpoint** *trustpointname*］

## 構文の説明

| | |
|---|---|
| **trustpoint** *trustpointname* | （任意）トラストポイントの名前。名前を指定しない場合は、脅威に対する防御 デバイスにキャッシュされているすべての CRL が表示されます。 |
| **trustpool** | すべての trustpool 関連の CRL を表示します。 |

## 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、**show crypto ca crl** コマンドの出力例を示します。

```
> show crypto ca crl trustpoint tp1
CRL Issuer Name:
    cn=ms-sub1-ca-5-2004,ou=Franklin DevTest,o=Cisco
Systems,l=Franklin,st=MA,c=US,ea=user@example.com
    LastUpdate: 19:45:53 UTC Dec 24 2004
    NextUpdate: 08:05:53 UTC Jan 1 2005
    Retrieved from CRL Distribution Point:
      http://win2k-ad2.frk-ms-pki.cisco.com/CertEnroll/ms-sub1-ca-5-2004.crl
    Associated Trustpoints: tp1
```

# show crypto ca trustpoints

CA トラストポイントを表示するには、**show crypto ca trustpoints** コマンドを使用します。

**show crypto ca trustpoints** ［*trustpoint_name*］

**構文の説明**

| | |
|---|---|
| *trustpoint_name* | （任意）表示するトラストポイントの名前。 |

**コマンド デフォルト**

トラストポイントを指定しない場合は、すべてのトラストポイントが表示されます。

**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、CA トラストポイントを表示する例を示します。

```
> show crypto ca trustpoints
Trustpoint ftd-self:
    Configured for self-signed certificate generation.
```

# show crypto ca trustpool

trustpool を構成する証明書を表示するには、**show crypto ca trustpool** コマンドを使用します。

**show crypto ca trustpool** ［**detail** | **policy**］

## 構文の説明

| | |
|---|---|
| **detail** | （オプション）証明書の詳細を表示します。 |
| **policy** | （オプション）設定された trustpool ポリシーを表示します。 |

## コマンド デフォルト

このコマンドは、すべての trustpool を省略形式で表示します。**detail** オプションを指定した場合は、追加の情報が含まれます。

## 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

**show crypto ca trustpool** コマンドの出力には、各証明書のフィンガープリントの値が含まれます。これらの値は削除操作で必要です。

### 例

次に、trustpool 内の証明書を表示する方法の例を示します。

```
> show crypto ca trustpool
CA Certificate
Status: Available
Certificate Serial Number: 6c386c409f4ff4944154635da520ed4c
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA1 with RSA Encryption
Issuer Name: cn=bxb2008-root
dc=bdb2008
dc=mycompany
dc=com
Subject Name:
cn=bxb2008-root
dc=bxb2008
dc=cisco
dc=com
Validity Date:
start date:17:21:06 EST Jan 14 2009
end date:17:31:06 EST Jan 14 2024
CA Certificate
Status: Available
Certificate Serial Number: 58d1c756000000000059
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA1 with RSA Encryption
Issuer Name:
cn=bxb2008-root
dc=bxb2008
```

```
dc=mycompany
dc=com
Subject Name:
cn=BXB2008SUB1-CA
dc=bxb2008
dc=cisco
dc=com
OCSP AIA:
URL: http://bxb2008-1.bxb2008.mycompany.com/ocsp
CRL Distribution Points:
(1) http://bxb2008-1.bxb2008.mycompany.com/CertEnroll/bxb2008-root.crl
Validity Date:
start date:11:54:34 EST May 18 2009
end date:12:04:34 EST May 18 2011
```

次に、trustpool ポリシーを表示する方法の例を示します。

```
> show crypto ca trustpool policy
800 trustpool certificates installed
Trustpool auto import statistics:
 Last import result: SUCCESS
 Next scheduled import at 22:00:00 Tues Jul 21 2015
Trustpool Policy
Trustpool revocation checking is disabled
CRL cache time: 123 seconds
CRL next update field: required and forced
Automatic import of trustpool certificates is enabled
Automatic import URL: http://www.thawte.com
Download time: 22:00:00
Policy overrides:
map: map1
match:issuer-name eq cn=Mycompany Manufacturing CA
match:issuer-name eq cn=Mycompany CA
action:skip revocation-check
map: map2
match: issuer-name eq cn=mycompany Manufacturing CA
match: issuer-name eq cn=mycompany CA2
action: allowed expired certificates
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear crypto ca trustpool** | trustpool からすべての証明書を削除します。 |

# show crypto debug-condition

IPsec および ISAKMP のデバッグメッセージに関して、現在設定されているフィルタ、一致しない状態、およびエラー状態を表示するには、グローバル コンフィギュレーション モードで **show crypto debug-condition** コマンドを使用します。

**show crypto debug-condition**

## 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、フィルタリング条件を表示する例を示します。

```
> show crypto debug-condition
Crypto conditional debug is turned ON
IKE debug context unmatched flag:  OFF
IPsec debug context unmatched flag:  ON
IKE peer IP address filters:
1.1.1.0/24   2.2.2.2
IKE user name filters:
my_user
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **debug crypto condition** | IPsec および ISAKMP デバッグ メッセージのフィルタリング条件を設定します。 |
| **debug crypto condition error** | フィルタリング条件が指定されているかどうかのデバッグ メッセージを表示します。 |
| **debug crypto condition unmatched** | フィルタリングに十分なコンテキスト情報が含まれていない IPsec および ISAKMP のデバッグ メッセージを表示します。 |

# show crypto ikev1

インターネット キー エクスチェンジ バージョン 1（IKEv1）に関する情報を表示するには、**show crypto ikev1** コマンドを使用します。

**show crypto ikev1** {**ipsec-over-tcp** | **sa** [**detail**] | **stats**}

## 構文の説明

| | |
|---|---|
| **ipsec-over-tcp** | IPSec over TCP データを表示します。 |
| **sa** [**detail**] | IKEv1 ランタイム セキュリティ アソシエーション（SA）データベースに関する情報を表示します。SA データベースに関する詳細出力を表示するには、**detail** キーワードを含めます。 |
| **stats** | IKEv1 統計情報を表示します。 |

## 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、SA データベースに関する詳細情報を表示する例を示します。detail キーワードを含めない場合、IKE Peer、Type、Dir、Rky、および State 列だけが表示されます。

```
> show crypto ikev1 sa detail
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
```

次に、IPSec over TCP データを表示する例を示します。

```
> show crypto ikev1 ipsec-over-tcp
Global IKEv1 IPSec over TCP Statistics
--------------------------------
Embryonic connections: 0
Active connections: 0
Previous connections: 0
Inbound packets: 0
Inbound dropped packets: 0
Outbound packets: 0
Outbound dropped packets: 0
RST packets: 0
```

```
Recevied ACK heart-beat packets: 0
Bad headers: 0
Bad trailers: 0
Timer failures: 0
Checksum errors: 0
Internal errors: 0
```

次に、グローバル IKEv1 統計情報を表示する例を示します。

```
> show crypto ikev1 stats
Global IKEv1 Statistics
  Active Tunnels:              0
  Previous Tunnels:            0
  In Octets:                   0
  In Packets:                  0
  In Drop Packets:             0
  In Notifys:                  0
  In P2 Exchanges:             0
  In P2 Exchange Invalids:     0
  In P2 Exchange Rejects:      0
  In P2 Sa Delete Requests:    0
  Out Octets:                  0
  Out Packets:                 0
  Out Drop Packets:            0
  Out Notifys:                 0
  Out P2 Exchanges:            0
  Out P2 Exchange Invalids:    0
  Out P2 Exchange Rejects:     0
  Out P2 Sa Delete Requests:   0
  Initiator Tunnels:           0
  Initiator Fails:             0
  Responder Fails:             0
  System Capacity Fails:       0
  Auth Fails:                  0
  Decrypt Fails:               0
  Hash Valid Fails:            0
  No Sa Fails:                 0

IKEV1 Call Admission Statistics
  Max In-Negotiation SAs:                 50
  In-Negotiation SAs:                      0
  In-Negotiation SAs Highwater:            0
  In-Negotiation SAs Rejected:             0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show crypto ikev2 sa** | IKEv2 ランタイム SA データベースを表示します。 |
| **show running-config crypto isakmp** | アクティブな ISAKMP コンフィギュレーションをすべて表示します。 |

# show crypto ikev2

インターネット キー エクスチェンジ バージョン 2（IKEv2）に関する情報を表示するには、**show crypto ikev2** コマンドを使用します。

**show crypto ikev2** {**sa** [**detail**] | **stats**}

## 構文の説明

| | |
|---|---|
| **sa** [**detail**] | IKEv2 ランタイム セキュリティ アソシエーション（SA）データベースに関する情報を表示します。SA データベースに関する詳細出力を表示するには、**detail** キーワードを含めます。 |
| **stats** | IKEv2 統計情報を表示します。 |

## 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、SA データベースに関する詳細情報を表示する例を示します。

```
> show crypto ikev2 sa detail
IKEv2 SAs:
Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id            Local             Remote              Status   Role
671069399            10.0.0.0/500      10.255.255.255/500  READY    INITIATOR
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:20, Auth sign: PSK, Auth verify:
PSK
      Life/Active Time: 86400/188 sec
      Session-id: 1
      Status Description: Negotiation done
      Local spi: 80173A0373C2D403       Remote spi: AE8AEFA1B97DBB22
      Local id: asa
      Remote id: asa1
      Local req mess id: 8              Remote req mess id: 7
      Local next mess id: 8             Remote next mess id: 7
      Local req queued: 8               Remote req queued: 7
      Local window: 1                   Remote window: 1
      DPD configured for 10 seconds, retry 2
      NAT-T is not detected
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x242a3da5/0xe6262034
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-GCM, keysize: 128, esp_hmac: N/A
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

次に、IKEv2 統計情報を表示する例を示します。

```
> show crypto ikev2 stats
```

```
Global IKEv2 Statistics
  Active Tunnels:                          0
  Previous Tunnels:                        0
  In Octets:                               0
  In Packets:                              0
  In Drop Packets:                         0
  In Drop Fragments:                       0
  In Notifys:                              0
  In P2 Exchange:                          0
  In P2 Exchange Invalids:                 0
  In P2 Exchange Rejects:                  0
  In IPSEC Delete:                         0
  In IKE Delete:                           0
  Out Octets:                              0
  Out Packets:                             0
  Out Drop Packets:                        0
  Out Drop Fragments:                      0
  Out Notifys:                             0
  Out P2 Exchange:                         0
  Out P2 Exchange Invalids:                0
  Out P2 Exchange Rejects:                 0
  Out IPSEC Delete:                        0
  Out IKE Delete:                          0
  SAs Locally Initiated:                   0
  SAs Locally Initiated Failed:            0
  SAs Remotely Initiated:                  0
  SAs Remotely Initiated Failed:           0
  System Capacity Failures:                0
  Authentication Failures:                 0
  Decrypt Failures:                        0
  Hash Failures:                           0
  Invalid SPI:                             0
  In Configs:                              0
  Out Configs:                             0
  In Configs Rejects:                      0
  Out Configs Rejects:                     0
  Previous Tunnels:                        0
  Previous Tunnels Wraps:                  0
  In DPD Messages:                         0
  Out DPD Messages:                        0
  Out NAT Keepalives:                      0
  IKE Rekey Locally Initiated:             0
  IKE Rekey Remotely Initiated:            0
  CHILD Rekey Locally Initiated:           0
  CHILD Rekey Remotely Initiated:          0

IKEV2 Call Admission Statistics
  Max Active SAs:                   No Limit
  Max In-Negotiation SAs:                250
  Cookie Challenge Threshold:          Never
  Active SAs:                              0
  In-Negotiation SAs:                      0
  Incoming Requests:                       0
  Incoming Requests Accepted:              0
  Incoming Requests Rejected:              0
  Outgoing Requests:                       0
  Outgoing Requests Accepted:              0
  Outgoing Requests Rejected:              0
  Rejected Requests:                       0
  Rejected Over Max SA limit:              0
  Rejected Low Resources:                  0
  Rejected Reboot In Progress:             0
  Cookie Challenges:                       0
```

```
Cookie Challenges Passed:                0
Cookie Challenges Failed:                0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show crypto ikev1 sa** | IKEv1 ランタイム SA データベースを表示します。 |
| **show running-config crypto isakmp** | アクティブなISAKMPコンフィギュレーションをすべて表示します。 |

# show crypto ipsec df-bit

指定されたインターフェイスの IPsec パケットの IPsec do-not-fragment（DF ビット）ポリシーを表示するには、**show crypto ipsec df-bit** コマンドを使用します。同じ意味を持つ **show ipsec df-bit** コマンドも使用できます。

**show crypto ipsec df-bit** *interface*

## 構文の説明

| | |
|---|---|
| *interface* | インターフェイス名を指定します。 |

## 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

d f ビットの設定によって、カプセル化されたヘッダーの do-not-fragment（DF）ビットのシステムによる処理方法が決まります。IP ヘッダー内の DF ビットにより、デバイスがパケットをフラグメント化できるかどうかが決定されます。この設定に基づき、システムは暗号の適用時に外側の IPsec ヘッダーに対するクリアテキスト パケットの DF ビットの設定をクリアするか、設定するか、コピーするかのいずれかを実行します。

### 例

次に、inside というインターフェイスの IPsec DF ビット ポリシーを表示する例を示します。

```
> show crypto ipsec df-bit inside
df-bit inside copy
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show crypto ipsec fragmentation** | IPsec パケットのフラグメンテーション ポリシーを表示します。 |

# show crypto ipsec fragmentation

IPsec パケットのフラグメンテーション ポリシーを表示するには、**show crypto ipsec fragmentation** コマンドを使用します。同じ意味を持つ **show ipsec fragmentation** コマンドも使用できます。

**show crypto ipsec fragmentation** *interface*

## 構文の説明

| | |
|---|---|
| *interface* | インターフェイス名を指定します。 |

## 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

VPN に対するパケットを暗号化する際、システムはパケット長をアウトバウンドインターフェイスの MTU と比較します。パケットの暗号化が MTU を超える場合は、パケットをフラグメント化する必要があります。このコマンドは、パケットを暗号化した後（after-encryption）、または暗号化する前（before-encryption）にシステムがパケットをフラグメント化するかどうかを表示します。暗号化前のパケットのフラグメント化は、事前フラグメント化とも呼ばれ、暗号化パフォーマンス全体を向上させるため、システムのデフォルト動作になっています。

### 例

次に、inside というインターフェイスの IPsec フラグメンテーション ポリシーを表示する例を示します。

```
> show crypto ipsec fragmentation inside
fragmentation inside before-encryption
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show crypto ipsec df-bit** | 指定したインターフェイスの DF ビット ポリシーを表示します。 |

# show crypto ipsec policy

OSPFv3 に設定されている IPsec セキュアソケット API（SS API）セキュリティポリシーを表示するには、**show crypto ipsec policy** コマンドを使用します。このコマンドの代替形式である **show ipsec policy** を使用することもできます。

**show crypto ipsec policy**

## 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、OSPFv3 認証と暗号方式ポリシーを表示する例を示します。

```
> show crypto ipsec policy
Crypto IPsec client security policy data

Policy name:      OSPFv3-1-256
Policy refcount:  1
Policy flags:     0x00000000
SA handles:       sess 268382208 (0xfff3000) / in 55017 (0xd6e9) / out 90369 (0x16101)
Inbound  ESP SPI:        256 (0x100)
Outbound ESP SPI:        256 (0x100)
Inbound  ESP Auth Key:   1234567890123456789012345678901234567890
Outbound ESP Auth Key:   1234567890123456789012345678901234567890
Inbound  ESP Cipher Key: 12345678901234567890123456789012
Outbound ESP Cipher Key: 12345678901234567890123456789012
Transform set:    esp-aes esp-sha-hmac
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipv6 ospf interface** | OSPFv3 インターフェイスに関する情報を表示します。 |
| **show crypto sockets** | セキュアなソケット情報を表示します。 |

# show crypto ipsec sa

IPsec SA のリストを表示するには、**show crypto ipsec sa** コマンドを使用します。このコマンドの代替形式である **show ipsec sa** を使用することもできます。

**show crypto ipsec sa** ［**assigned-address** | **entry** | **identity** | **inactive** | **map** *map-name* | **peer** *peer-addr* | **spi** | **summary** | **user**］［**detail**］

## 構文の説明

| | |
|---|---|
| **assigned-address** | （オプション）割り当てられたアドレスの IPsec SA を表示します。 |
| **detail** | （任意）表示されているものに対する詳細なエラー情報を表示します。 |
| **entry** | （オプション）IPsec SA をピア アドレスの順に表示します。 |
| **identity** | （オプション）IPsec SA を ID の順に表示します。ESP は含まれません。これは簡略化された形式です。 |
| **inactive** | （オプション）非アクティブな IPsec SA を表示します。 |
| **map** *map-name* | （オプション）指定されたクリプトマップの IPsec SA を表示します。 |
| **peer** *peer-addr* | （オプション）指定されたピア IP アドレスの IPsec SA を表示します。 |
| **spi** | （オプション）SPI の IPsec SA を表示します。 |
| **summary** | （オプション）IPsec SA の概要をタイプ別に表示します。 |
| **user** | （オプション）ユーザーの IPsec SA を表示します。 |

## 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、OSPFv3 として識別されるトンネルを含む IPsec SA を表示する例を示します。

```
> show crypto ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
```

```
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
    #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
    #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
    #send errors: 0, #recv errors: 0

    local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21

    path mtu 1500, ipsec overhead 60, media mtu 1500
    current outbound spi: DC15BF68

  inbound esp sas:
    spi: 0x1E8246FC (511854332)
       transform: esp-3des esp-md5-hmac
       in use settings ={L2L, Transport, Manual key, (OSPFv3), }
       slot: 0, conn_id: 3, crypto-map: def
       sa timing: remaining key lifetime (sec): 548
       IV size: 8 bytes
       replay detection support: Y
  outbound esp sas:
    spi: 0xDC15BF68 (3692412776)
       transform: esp-3des esp-md5-hmac
       in use settings ={L2L, Transport, Manual key, (OSPFv3), }
       slot: 0, conn_id: 3, crypto-map: def
       sa timing: remaining key lifetime (sec): 548
       IV size: 8 bytes
       replay detection support: Y

  Crypto map tag: def, local addr: 10.132.0.17

    local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

（注） IPSec SA ポリシーに、フラグメンテーションは IPsec 処理の前に発生すると明記されている場合、フラグメンテーション統計情報は、フラグメンテーション前の統計情報です。SA ポリシーに、フラグメンテーションは IPsec 処理の後に発生すると明記されている場合、フラグメンテーション後の統計情報が表示されます。

次に、def という名前のクリプトマップの IPsec SA を表示する例を示します。

```
> show crypto ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
```

```
    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
```

次に、キーワード **entry** に関する IPsec SA の例を示します。

```
> show crypto ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
```

```
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
```

```
         replay detection support: Y
```

次に、キーワード **entry detail** を使用した IPsec SA の例を示します。

```
> show crypto ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
```

```
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
```

次に、キーワード **identity** を使用した IPsec SA の例を示します。

```
> show crypto ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
```

```
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

次に、キーワード **identity** および **detail** を使用した IPsec SA の例を示します。

```
> show crypto ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
      #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear isakmp sa** | IKE ランタイム SA データベースをクリアします。 |

| Command | 説明 |
| --- | --- |
| **show running-config isakmp** | アクティブなISAKMP コンフィギュレーションをすべて表示します。 |

# show crypto ipsec stats

IPSec 統計情報のリストを表示するには、**show crypto ipsec stats** コマンドを使用します。

**show crypto ipsec stats**

## 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、IPSec 統計情報を表示する例を示します。

```
> show crypto ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
    Encryption failures: 0
 Fragmentation successes: 3
  Pre-fragmentation successes:2
  Post-fragmentation successes: 1
 Fragmentation failures: 2
  Pre-fragmentation failures:1
  Post-fragmentation failures: 1
 Fragments created: 10
 PMTUs sent: 1
 PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear ipsec sa** | 指定されたパラメータに基づいて、IPsec SA またはカウンタをクリアします。 |
| **show ipsec sa** | 指定されたパラメータに基づいて IPsec SA を表示します。 |
| **show ipsec sa summary** | IPsec SA の要約を表示します。 |

# show crypto isakmp

IKEv1 と IKEv2 の両方の ISAKMP 情報を表示するには、**show crypto isakmp** コマンドを使用します。

**show crypto isakmp** {**sa** [**detail**] | **stats**}

## 構文の説明

| | |
|---|---|
| **sa** [**detail**] | ランタイム セキュリティ アソシエーション（SA）データベースに関する情報を表示します。SA データベースに関する詳細出力を表示するには、**detail** キーワードを含めます。 |
| **stats** | IKEv1 および IKEv2 統計情報を表示します。 |

## 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

**show crypto isakmp** コマンドは、同等の **show crypto ikev1** および **show crypto ikev2** コマンドの出力を組み合わせたものです。

次に、SA 情報を読む際のヒントを示します。

- Rky は No または Yes です。Yes の場合は、キー再生成が発生しており、キー再生成が完了するまで、2 番目に一致する SA は異なる状態になります。
- Role はイニシエータまたはレスポンダの状態です。これは SA のステートマシンの現在の状態を示します。
- State：トンネルがアップしデータが受け渡しされている場合、値は MM_ACTIVE または AM_ACTIVE のいずれかになります。

### 例

次に、SA データベースに関する詳細情報を表示する例を示します。

```
> show crypto isakmp sa detail

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
```

次の例では ISAKMP 統計情報が表示されます。IKEv1 と IKEv2 は別々に表示されます。

```
> show crypto isakmp stats

Global IKEv1 Statistics
  Active Tunnels:              136
  Previous Tunnels:            0
  In Octets:                   0
  In Packets:                  0
  In Drop Packets:             0
  In Notifys:                  0
  In P2 Exchanges:             0
  In P2 Exchange Invalids:     0
  In P2 Exchange Rejects:      0
  In P2 Sa Delete Requests:    0
  Out Octets:               1344
  Out Packets:                 8
  Out Drop Packets:            0
  Out Notifys:                 0
  Out P2 Exchanges:            0
  Out P2 Exchange Invalids:    0
  Out P2 Exchange Rejects:     0
  Out P2 Sa Delete Requests:   0
  Initiator Tunnels:           2
  Initiator Fails:             2
  Responder Fails:             0
  System Capacity Fails:       0
  Auth Fails:                  0
  Decrypt Fails:               0
  Hash Valid Fails:            0
  No Sa Fails:                 0

IKEV1 Call Admission Statistics
  Max In-Negotiation SAs:                50
  In-Negotiation SAs:                     0
  In-Negotiation SAs Highwater:           0
  In-Negotiation SAs Rejected:            0
In Drop Packets: 925

Global IKEv2 Statistics
  Active Tunnels:                        132
  Previous Tunnels:                      132
  In Octets:                             195471
  In Packets:                            1854
  In Drop Packets:                       925
  In Drop Fragments:                     0
  In Notifys:                            0
  In P2 Exchange:                        132
  In P2 Exchange Invalids:               0
  In P2 Exchange Rejects:                0
  In IPSEC Delete:                       0
  In IKE Delete:                         0
  Out Octets:                            119029
  Out Packets:                           796
  Out Drop Packets:                      0
  Out Drop Fragments:                    0
  Out Notifys:                           264
  Out P2 Exchange:                       0
Out P2 Exchange Invalids:              0
  Out P2 Exchange Rejects:               0
  Out IPSEC Delete:                      0
  Out IKE Delete:                        0
```

```
  SAs Locally Initiated:                    0
  SAs Locally Initiated Failed:             0
  SAs Remotely Initiated:                   0
  SAs Remotely Initiated Failed:            0
  System Capacity Failures:                 0
  Authentication Failures:                  0
  Decrypt Failures:                         0
  Hash Failures:                            0
  Invalid SPI:                              0
  In Configs:                               0
  Out Configs:                              0
  In Configs Rejects:                       0
  Out Configs Rejects:                      0
  Previous Tunnels:                         0
  Previous Tunnels Wraps:                   0
  In DPD Messages:                          0
  Out DPD Messages:                         0
  Out NAT Keepalives:                       0
  IKE Rekey Locally Initiated:              0
  IKE Rekey Remotely Initiated:             0
  CHILD Rekey Locally Initiated:            0
  CHILD Rekey Remotely Initiated:           0

IKEV2 Call Admission Statistics
  Max Active SAs:                     No Limit
  Max In-Negotiation SAs:                  300
  Cookie Challenge Threshold:              150
  Active SAs:                                0
  In-Negotiation SAs:                        0
  Incoming Requests:                         0
  Incoming Requests Accepted:                0
  Incoming Requests Rejected:                0
  Outgoing Requests:                         0
  Outgoing Requests Accepted:                0
  Outgoing Requests Rejected:                0
  Rejected Requests:                         0
  Rejected Over Max SA limit:                0
  Rejected Low Resources:                    0
  Rejected Reboot In Progress:               0
  Cookie Challenges:                         0
  Cookie Challenges Passed:                  0
  Cookie Challenges Failed:                  0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear crypto isakmp sa** | IKE ランタイム SA データベースをクリアします。 |
| **show running-config crypto isakmp** | アクティブなISAKMPコンフィギュレーションをすべて表示します。 |

# show crypto key mypubkey

ECDSA キーまたは RSA キーのキー名、使用法、および楕円曲線サイズを表示するには、**show crypto key mypubkey** コマンドを使用します。

**show crypto key mypubkey** {**ecdsa** | **rsa**}

## 構文の説明

| | |
|---|---|
| **ecdsa** | ECDSA 公開キーを表示します。 |
| **rsa** | RSA 公開キーを表示します。 |

## 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、RSA 公開キーを表示する例を示します。

```
> show crypto key mypubkey rsa
Key pair was generated at: 18:19:26 UTC May 26 2016
Key name: <Default-RSA-Key>
 Usage: General Purpose Key
 Modulus Size (bits): 1024
 Key Data:

  30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00c0bf77
  d651ead6 fca31c72 12064272 36f699b9 e971e198 1503ba6b f0112b63 97252a26
  38827d83 cd71863e b8962da5 bb905a47 666452a1 9eb1a36e dd8aab00 0e4493f1
  4422bf09 4bcfcb95 a83d38a9 7b9caba6 83c9b5b2 cff251f8 a0422a68 3690c9e5
  0cbbe83b 1a8b2460 1f83b43b a9b06912 7cc9f7f9 f596b81e e2a7bde7 8f020301
  0001
>
```

# show crypto protocol statistics

クリプトアクセラレータ MIB のプロトコル固有の統計情報を表示するには、**show crypto protocol statistics** コマンドを使用します。

**show crypto protocol statistics** *protocol*

## 構文の説明

| | |
|---|---|
| *protocol* | 統計情報を表示するプロトコルの名前を指定します。プロトコルの選択肢は次のとおりです。<br>**ikev1**：インターネット キー エクスチェンジ バージョン 1。<br>**ikev2**：インターネット キー エクスチェンジ バージョン 2。<br>**ipsec**：IP セキュリティフェーズ 2 プロトコル。<br>**ssl**：セキュアソケットレイヤ。<br>**ssh**：セキュアシェルプロトコル。<br>**srtp**：Secure Real-time Transport Protocol。<br>**other**：新規プロトコル用に予約済み。<br>**all**：現在サポートされているすべてのプロトコル。 |

## 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、すべてのプロトコルのクリプトアクセラレータ統計情報を表示する例を示します。

```
> show crypto protocol statistics all
[IKEv1 statistics]
   Encrypt packet requests: 46
   Encapsulate packet requests: 46
   Decrypt packet requests: 40
   Decapsulate packet requests: 40
   HMAC calculation requests: 91
   SA creation requests: 1
   SA rekey requests: 3
   SA deletion requests: 3
   Next phase key allocation requests: 2
   Random number generation requests: 0
   Failed requests: 0
[IKEv2 statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
```

```
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[IPsec statistics]
   Encrypt packet requests: 700
   Encapsulate packet requests: 700
   Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSH statistics are not supported]
[SRTP statistics are not supported]
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0
>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear crypto accelerator statistics** | 暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報をクリアします。 |
| **clear crypto protocol statistics** | 暗号アクセラレータ MIB にあるプロトコル固有の統計情報をクリアします。 |
| **show crypto accelerator statistics** | 暗号アクセラレータ MIB からグローバルおよびアクセラレータ固有の統計情報を表示します。 |

# show crypto sockets

暗号セキュアソケット情報を表示するには、**show crypto sockets** コマンドを使用します。

**show crypto sockets**

## 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、暗号セキュアソケット情報を表示する例を示します。

```
> show crypto sockets
Number of Crypto Socket connections 1

       Gi0/1  Peers: (local): 2001:1::1
                     (remote): ::
              Local Ident (addr/plen/port/prot): (2001:1::1/64/0/89)
              Remote Ident (addr/plen/port/prot): (::/0/0/89)
              IPsec Profile: "CSSU-UTF"
              Socket State: Open
              Client: "CSSU_App(UTF)" (Client State: Active)

       Crypto Sockets in Listen state:
```

次の表で、**show crypto sockets** コマンド出力のフィールドについて説明します。

| フィールド | 説明 |
|---|---|
| Number of Crypto Socket connections | システム内の暗号ソケットの数。 |
| Socket State | この状態は、アクティブな IPsec セキュリティ アソシエーション（SA）が存在することを意味する Open か、またはアクティブな IPsec SA が存在しないことを意味する Closed のどちらかです。 |
| クライアント | アプリケーションの名前とその状態。 |
| Flags | このフィールドが「shared」になっている場合、ソケットは複数のトンネル インターフェイスで共有されます。 |
| Crypto Sockets in Listen state | 暗号 IPsec プロファイルの名前。 |

関連コマンド

| Command | 説明 |
| --- | --- |
| **show crypto ipsec policy** | 暗号セキュア ソケット API でインストールされたポリシー情報を表示します。 |

# show crypto ssl

脅威に対する防御 デバイス上のアクティブな SSL セッションに関する情報を表示するには、**show crypto ssl** コマンドを使用します。

**show crypto ssl** ［**cache** | **ciphers** | **errors** ［**trace**］ | **mib** ［**64**］ | **objects**］

## 構文の説明

| | |
|---|---|
| **cache** | （オプション）SSLセッションキャッシュの統計情報を表示します。 |
| **ciphers** | （オプション）使用可能な SSL 暗号を表示します。 |
| **errors** | （オプション）SSL エラーを表示します。 |
| **trace** | （オプション）SSL エラートレース情報を表示します。 |
| **mib** | （オプション）SSL MIB の統計情報を表示します。 |
| **64** | （オプション）SSL MIB 64-bit カウンタの統計情報を表示します。 |
| **objects** | （オプション）SSL オブジェクトの統計情報を表示します。 |

## 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

このコマンドは、現在の SSLv3 以上のセッションに関する情報を表示します。情報には、有効になっている暗号の順序、無効化された暗号、使用されている SSL トラストポイント、証明書認証が有効かどうかが含まれます。

### 例

次に、**show ssl** コマンドの出力例を示します。

```
> show crypto ssl

Accept connections using SSLv3 or greater and negotiate to TLSv1 or greater
Start connections using TLSv1 and negotiate to TLSv1 or greater
SSL DH Group: group2 (1024-bit modulus)
SSL ECDH Group: group19 (256-bit EC)

SSL trust-points:
  Self-signed (RSA 2048 bits RSA-SHA256) certificate available
  Self-signed (EC 256 bits ecdsa-with-SHA256) certificate available
Certificate authentication is not enabled
```

SSL セッションキャッシュの統計情報を表示するには、**show crypto ssl cache** コマンドを使用します。

```
> show crypto ssl cache

SSL session cache statistics:
  Maximum cache size:          100    Current cache size:           0
  Cache hits:                    0    Cache misses:                 0
  Cache timeouts:                0    Cache full:                   0
  Accept attempts:               0    Accepts successful:           0
  Accept renegotiates:           0
  Connect attempts:              0    Connects successful:          0
  Connect renegotiates:          0
SSL VPNLB session cache statistics:
  Maximum cache size:           10    Current cache size:           0
  Cache hits:                    0    Cache misses:                 0
  Cache timeouts:                0    Cache full:                   0
  Accept attempts:               0    Accepts successful:           0
  Accept renegotiates:           0
  Connect attempts:              0    Connects successful:          0
  Connect renegotiates:          0
SSLDEV session cache statistics:
  Maximum cache size:           20    Current cache size:           0
  Cache hits:                    0    Cache misses:                 0
  Cache timeouts:                0    Cache full:                   0
  Accept attempts:               0    Accepts successful:           0
  Accept renegotiates:           0
  Connect attempts:              0    Connects successful:          0
  Connect renegotiates:          0
DTLS session cache statistics:
  Maximum cache size:          100    Current cache size:           0
  Cache hits:                    0    Cache misses:                 0
  Cache timeouts:                0    Cache full:                   0
  Accept attempts:               0    Accepts successful:           0
  Accept renegotiates:           0
  Connect attempts:              0    Connects successful:          0
  Connect renegotiates:          0
```

SSL 暗号リストを表示するには、**show crypto ssl cipher** コマンドを使用します。

```
> show crypto ssl cipher

Current cipher configuration:
default (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
```

```
  DES-CBC3-SHA
tlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1.1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1.2 (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
dtlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
```

# show ctiqbe

脅威に対する防御 デバイスで確立された CTIQBE セッションに関する情報を表示するには、**show ctiqbe** コマンドを使用します。

**show ctiqbe**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.2 | このコマンドが導入されました。 |

### 例

次の条件における **show ctiqbe** コマンドの出力例を示します。デバイスでセットアップされているアクティブ CTIQBE セッションは 1 つだけです。そのセッションは、ローカル アドレス 10.0.0.99 の内部 CTI デバイス（たとえば、Cisco IP SoftPhone）と 172.29.1.77 の外部 Cisco CallManager の間で確立されています。ここで、TCP ポート 2748 は、Cisco CallManager です。このセッションのハートビート間隔は 120 秒です。

```
> show ctiqbe

Total: 1
        LOCAL            FOREIGN          STATE   HEARTBEAT
-----------------------------------------------------------------
1       10.0.0.99/1117  172.29.1.77/2748        1       120
        ---------------------------------------------
        RTP/RTCP: PAT xlates: mapped to 172.29.1.99(1028 - 1029)
        ---------------------------------------------
        MEDIA: Device ID 27     Call ID 0
               Foreign 172.29.1.99      (1028 - 1029)
               Local   172.29.1.88      (26822 - 26823)
        ---------------------------------------------
```

CTI デバイスは、すでに CallManager に登録されています。デバイスの内部アドレスおよび RTP 受信ポートは 172.29.1.99 の UDP ポート 1028 に PAT 変換されています。RTCP 受信ポートは UDP 1029 に PAT 変換されています。

「RTP/RTCP: PAT xlates:」で始まる行は、内部 CTI デバイスが外部 CallManager に登録され、CTI デバイスのアドレスとポートがその外部インターフェイスに PAT 変換されている場合に限り表示されます。この行は、CallManager が内部インターフェイス上に位置する場合、または内部 CTI デバイスのアドレスとポートが、CallManager が使用しているのと同じ外部インターフェイスに NAT 変換されている場合は、表示されません。

この出力は、コールがこの CTI デバイスと 172.29.1.88 にある別の電話機の間に確立されていることを示します。他の電話機の RTP および RTCP 受信ポートは、UDP 26822 および 26823 です。脅威に対する防御 デバイスは 2 番目の電話機と CallManager に関連する CTIQBE セッション レコードを維持できないため、他の電話機は、CallManager

と同じインターフェイス上にあります。CTI デバイス側のアクティブ コール レッグは、Device ID 27 および Call ID 0 で確認できます。

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **inspect ctiqbe** | CTIQBE アプリケーション インスペクションをイネーブルにします。 |
| **show service-policy** | サービスポリシーの情報と統計を表示します。 |
| **show conn** | さまざまな接続タイプの接続状態を表示します。 |

# show ctl-provider

ユニファイドコミュニケーションで使用されるCTLプロバイダーの設定を表示するには、**show ctl-provider** コマンドを使用します。

**show ctl-provider** ［*name*］

## 構文の説明

| | |
|---|---|
| *name* | （オプション）この CTL プロバイダーのみの情報を表示します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

### 例

次に、CTL プロバイダーの設定を表示する例を示します。

```
> show ctl-provider
!
ctl-provider my-ctl
 client interface inside address 192.168.1.55
 client interface inside address 192.168.1.56
 client username admin password gWe.oMSKmeGtelxS encrypted
 export certificate ccm-proxy
!
```

# show curpriv

診断 CLI セッションの現在のユーザー権限を表示するには、**show curpriv** コマンドを使用します。

**show curpriv**

## 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

**show curpriv** コマンドは、現在の特権レベルを表示します。特権レベルの数値が小さいほど、特権レベルが低いことを示しています。

この情報は、**configure user** コマンドで定義されたユーザーには適用されません。これらは **system support diagnostistic-cli** セッション内のユーザーの権限です。これらの権限は変更できません。

### 例

次に、ログインしているユーザーの権限を表示する例を示します。これらの権限は診断 CLI に適用され、configure コマンドを使用する機能には適用されません。enable_1 ユーザーの権限は設定できません。これらの権限は、**Basic** と **Config** の両方の権限で同じです。

```
> show curpriv
Username : enable_1
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
```

# show d-show h

# show database

システムデータベースに関する情報を表示するには、**show database** コマンドを使用します。

**show database** {**processes** | **slow-query-log**}

## 構文の説明

| | |
|---|---|
| **processes** | 現在実行中のデータベースクエリに関する情報を表示します。 |
| **slow-query-log** | データベースのスロークエリログを表示します。 |

## 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、データベースプロセス情報を表示する例を示します。

```
> show database processes
Database Processes:
        Id :  3
      User :  barnyard
      Host :  localhost
  Database :  sfsnort
   Command :  Sleep
      Time :  6
     State :  Null
      Info :  Null
--------------------------------------------------------------
(...Remaining output truncated...)
```

# show ddns update

DDNS 更新方法に関する情報を表示するには、**show ddns update interface** コマンドを使用します。

**show ddns update** {**interface** [*interface-name*] | **method** [*method-name*]}

## 構文の説明

| | |
|---|---|
| **interface** [*interface-name*] | 脅威に対する防御 インターフェイスに割り当てられているメソッドを表示します。必要に応じて、インターフェイス名を指定し、指定したインターフェイスに関する情報のみを表示することもできます。 |
| **method** [*method-name*] | DDNS 更新方式に関する情報を表示します。必要に応じて、メソッドの名前を入力して、入力したメソッドに関する情報のみを表示することもできます。 |

## 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。 |
| 6.7 | Web 更新方式の場合、**interface** キーワードの出力には、最後に更新された FQDN/IP アドレスマッピングが含まれます。**method** キーワードに、Web 更新方式の出力が追加されました。 |

### 例

次に、内部インターフェイスに割り当てられている DDNS 方式を表示する例を示します。

```
> show ddns update interface inside
Dynamic DNS Update on inside:
  Update Method Name            Update Destination
  ddns-2                        not available
>
```

次の例は、Web タイプの更新が成功したことを示しています。

```
> show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Success
FQDN : ftd1.example.com
IP addresses(s): 10.10.32.45,2001:DB8::1
```

次の例は、Web タイプの更新が失敗したことを示しています。

```
> show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Could not establish a connection to the server
```

次の例は、DNS サーバーから Web タイプの更新のエラーが返されたことを示しています。

```
> show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Server error (Error response from server)
```

次の例は、IP アドレスが設定されていないか DHCP 要求が失敗したために、Web 更新がまだ試行されていないことを示しています。

```
> show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update Not attempted
```

次に、ddns-2 という名前の DDNS 方式を表示する例を示します。

```
> show ddns update method ddns-2
Dynamic DNS Update Method: ddns-2
  IETF standardized Dynamic DNS 'A' and 'PTR' records update
  Maximum update interval: 0 days 0 hours 10 minutes 0 seconds
>
```

次の例は、Web 更新方式の詳細を示しています。

```
> show ddns update method web1

Dynamic DNS Update Method: web1
 Dynamic DNS updated via HTTP(s) protocols
  URL used to update record:
https://cdarwin:*****@ddns.cisco.com/update?hostname=<h>&myip=<a>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show running-config ddns** | 実行コンフィギュレーションに設定されているすべての DDNS 方式のタイプおよび間隔を表示します。 |

# show debug

現在のデバッグ設定を表示するには、**show debug** コマンドを使用します。

**show debug** ［*command* ［*keywords*］］

## 構文の説明

| | |
|---|---|
| *command* | （任意）現在の設定を表示する **debug** コマンドを指定します。 |
| キーワード | （任意）各コマンドにおいて、コマンドに続くキーワードは、関連する **debug** コマンドによってサポートされるキーワードと同一です。 |

## 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

各コマンドにおいて、コマンドに続くキーワードは、関連する **debug** コマンドによってサポートされるキーワードと同一です。サポートされているシンタックスの詳細を確認する場合は、キーワードの位置に ? を入力します。

次に例を示します。

- **show debug ?** 使用可能なコマンドが一覧表示されます。
- **show debug tcp ?** TCP デバッグに使用可能なキーワードが一覧表示されます。

### 例

次の例では、TCP デバッグを有効にして、デバッグステータスを表示します。

```
> debug tcp
debug tcp  enabled at level 1
> show debug tcp
debug tcp  enabled at level 1
debug tcp  enabled at level 1 (persistent)
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **debug** | デバッグを有効にします。 |

# show debug

現在のデバッグ設定を表示するには、**show debug** コマンドを使用します。

**show debug** ［*command* ［*keywords*］］

## 構文の説明

| | |
|---|---|
| *command* | （任意）現在の設定を表示する **debug** コマンドを指定します。 |
| キーワード | （任意）各コマンドにおいて、コマンドに続くキーワードは、関連する **debug** コマンドによってサポートされるキーワードと同一です。 |

## 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

各コマンドにおいて、コマンドに続くキーワードは、関連する **debug** コマンドによってサポートされるキーワードと同一です。サポートされているシンタックスの詳細を確認する場合は、キーワードの位置に ? を入力します。

次に例を示します。

- **show debug ?** 使用可能なコマンドが一覧表示されます。
- **show debug tcp ?** TCP デバッグに使用可能なキーワードが一覧表示されます。

### 例

次の例では、TCP デバッグを有効にして、デバッグステータスを表示します。

```
> debug tcp
debug tcp  enabled at level 1
> show debug tcp
debug tcp  enabled at level 1
debug tcp  enabled at level 1 (persistent)
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **debug** | デバッグを有効にします。 |

# show dhcpd

DHCP のバインディング、状態、および統計情報を表示するには、**show dhcpd** コマンドを使用します。

**show dhcpd** {**binding** [*IP_address*] | **state** | **statistics**}

## 構文の説明

| | |
|---|---|
| **binding** | 所定のサーバー IP アドレスおよび関連するクライアント ハードウェア アドレスについてのバインディング情報とリースの長さを表示します。 |
| *IP_address* | 指定した IP アドレスのバインディング情報を表示します。 |
| **state** | DHCP サーバーの状態（現在のコンテキストでイネーブルかどうか、各インターフェイスについてイネーブルかどうかなど）を表示します。 |
| **statistics** | 統計情報（アドレス プール、バインディング、期限切れバインディング、不正な形式のメッセージ、送信済みメッセージ、および受信メッセージなどの数）を表示します。 |

## 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

オプションの IP アドレスを **show dhcpd binding** コマンドに含めると、その IP アドレスのバインディングだけが表示されます。

### 例

次に、**show dhcpd binding** コマンドの出力例を示します。

```
> show dhcpd binding
IP Address Client-id         Lease Expiration  Type
10.0.1.100 0100.a0c9.868e.43 84985 seconds     automatic
```

次に、**show dhcpd state** コマンドの出力例を示します。この例では、外部インターフェイスは DHCP クライアントですが、他の多くのインターフェイスは DHCP サーバーとして機能しています。

```
> show dhcpd state
Context  Configured as DHCP Server
Interface outside, Configured for DHCP CLIENT
Interface inside1_2, Configured for DHCP SERVER
Interface inside1_3, Configured for DHCP SERVER
Interface inside1_4, Configured for DHCP SERVER
Interface inside1_5, Configured for DHCP SERVER
```

```
Interface inside1_6, Configured for DHCP SERVER
Interface inside1_7, Configured for DHCP SERVER
Interface inside1_8, Not Configured for DHCP
Interface diagnostic, Not Configured for DHCP
Interface inside, Configured for DHCP SERVER
```

次に、**show dhcpd statistics** コマンドの出力例を示します。

```
> show dhcpd statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Address pools        1
Automatic bindings   1
Expired bindings     1
Malformed messages   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         1
DHCPREQUEST          2
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

Message              Sent
BOOTREPLY            0
DHCPOFFER            1
DHCPACK              1
DHCPNAK              1
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear dhcpd** | DHCP サーバー バインディングおよび統計情報カウンタをクリアします。 |
| **show running-config dhcpd** | 現在の DHCP サーバー コンフィギュレーションを表示します。 |

# show dhcprelay

DHCP リレーエージェントの状態と統計情報を表示するには、**show dhcprelay state** コマンドを使用します。

**show dhcprelay** {**state** | **statistics**}

## 構文の説明

| | |
|---|---|
| **state** | 各インターフェイスの DHCP リレーエージェントの状態を表示します。 |
| **statistics** | DHCP リレーの統計情報を表示します。 |

## 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、**show dhcprelay state** コマンドの出力例を示します。

```
> show dhcprelay state

Context  Configured as DHCP Relay
Interface outside, Not Configured for DHCP
Interface infrastructure, Configured for DHCP RELAY SERVER
Interface inside, Configured for DHCP RELAY
```

次に、**show dhcprelay statistics** コマンドの出力例を示します。

```
> show dhcprelay statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Packets Relayed
BOOTREQUEST          0
DHCPDISCOVER         7
DHCPREQUEST          3
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

BOOTREPLY            0
DHCPOFFER            7
DHCPACK              3
DHCPNAK              0
```

関連コマンド

| Command | 説明 |
| --- | --- |
| **clear dhcprelay statistics** | DHCP リレー エージェントの統計カウンタをクリアします。 |
| **show dhcpd** | DHCP サーバーの統計情報と状態情報を表示します。 |

# show diameter

各 Diameter 接続の状態情報を表示するには、**show diameter** コマンドを使用します。

**show diameter**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.2 | このコマンドが導入されました。 |

## 使用上のガイドライン

Diameter接続の状態情報を表示するには、Diameter トラフィックを検査する必要があります。Diameter トラフィックを検査するには、Management Center で FlexConfig を設定する必要があります。

### 例

次に、**show diameter** コマンドの出力例を示します。

```
> show diameter
Total active diameter sessions: 5
Session 3638
       ==========
       ref_count: 1 val = .; 1096298391; 2461;
           Protocol : diameter Context id : 0
           From inside:211.1.1.10/45169 to outside:212.1.1.10/3868
...
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear service-policy** | サービス ポリシーの統計情報をクリアします。 |

# show disk

脅威に対する防御 デバイスのフラッシュメモリの内容のみを表示するには、**show disk** コマンドを使用します。

**show disk**
**show** {**disk0:** | **disk1:**} [**filesys** | **all** | **controller**]

## 構文の説明

| | |
|---|---|
| {**disk0:** \| **disk1:**} | 内部フラッシュメモリ（disk0:）または外部フラッシュメモリ（disk1:）を指定します。番号を指定せずに **show disk** コマンドを入力すると、ファイルシステムに関する情報が表示されます。 |
| **all** | フラッシュメモリの内容と、ファイルシステムおよびコントローラに関する情報を表示します。 |
| **controller** | フラッシュコントローラのモデル番号を表示します。 |
| **filesys** | コンパクト フラッシュ カードについての情報を表示します。 |

## コマンド デフォルト

デフォルトでは、このコマンドはファイルシステム情報を表示します。

## 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

次の例は、ファイルシステムに関する情報を表示する方法を示しています。

```
> show disk
Filesystem        Size  Used Avail Use% Mounted on
tmpfs             3.9G  440K  3.9G   1% /run
tmpfs             3.9G  168K  3.9G   1% /var/volatile
none              3.8G  9.4M  3.8G   1% /dev
/dev/sdb1         7.4G  104M  7.3G   2% /mnt/disk0
/dev/mapper/root  3.7G  943M  2.6G  27% /ngfw
/dev/mapper/var    81G  4.0G   73G   6% /home
tmpfs             3.9G     0  3.9G   0% /dev/cgroups
```

次に、**show disk0:** コマンドの出力例を示します。

```
> show disk0:
--#--  --length--  -----date/time------  path
   48  107030784   Oct 05 2016 02:10:26  os.img
   49  33          Oct 11 2016 21:32:16  .boot_string
   50  150484      Oct 06 2016 15:36:02  install.log
   11  4096        Oct 06 2016 15:58:16  log
   13  1544        Oct 13 2016 18:59:06  log/asa-appagent.log
   16  4096        Oct 06 2016 15:59:07  crypto_archive
```

```
   51  4096        Oct 06 2016 15:59:12  coredumpinfo
   52  59          Oct 06 2016 15:59:12  coredumpinfo/coredump.cfg
   53  36          Oct 06 2016 16:04:47  enable_configure
   56  507281      Oct 20 2016 18:10:20  crashinfo-test_20161020_181021_UTC

7935832064 bytes total (7827599360 bytes free)
```

次に、**show disk0: filesys** コマンドの出力例を示します。

```
> show disk0: filesys

******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:          245
   Number of Cylinders      1022
   Sectors per Cylinder       62
   Sector Size               512
   Total Sectors          15524180
```

次に、**show disk0: controller** コマンドの出力例を示します。

```
> show disk0: controller

Flash Model: ATA Micron_M500DC_MT
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **dir** | ディレクトリの内容を表示します。 |

# show disk-manager

システムの各部分（サイロ、低水位、高水位など）のディスク使用状況の詳細情報を表示するには、**show disk-manager** コマンドを使用します。

**show disk-manager**

## 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、ディスクマネージャ情報の表示例を示します。

```
> show disk-manager
Silo                                Used        Minimum     Maximum
Temporary Files                     0 KB        499.197 MB  1.950 GB
Action Queue Results                0 KB        499.197 MB  1.950 GB
User Identity Events                0 KB        499.197 MB  1.950 GB
UI Caches                           4 KB        1.462 GB    2.925 GB
Backups                             0 KB        3.900 GB    9.750 GB
Updates                             0 KB        5.850 GB    14.625 GB
Other Detection Engine              0 KB        2.925 GB    5.850 GB
Performance Statistics              33 KB       998.395 MB  11.700 GB
Other Events                        0 KB        1.950 GB    3.900 GB
IP Reputation & URL Filtering       0 KB        2.437 GB    4.875 GB
Archives & Cores & File Logs        0 KB        3.900 GB    19.500 GB
Unified Low Priority Events         1.329 MB    4.875 GB    24.375 GB
RNA Events                          0 KB        3.900 GB    15.600 GB
File Capture                        0 KB        9.750 GB    19.500 GB
Unified High Priority Events        0 KB        14.625 GB   34.125 GB
IPS Events                          0 KB        11.700 GB   29.250 GB
```

# show dns

完全修飾ドメイン名（FQDN）ネットワークオブジェクトの現在解決済みのDNSアドレス、または管理インターフェイスの DNS サーバーの設定を表示するには、**show dns** コマンドを使用します。

**show dns** ［**host** *fqdn* | **system**］

## 構文の説明

| | |
|---|---|
| **host** *fqdn* | 指定された完全修飾ドメイン名（FQDN）のみに関する情報を表示します。 |
| **system** | 管理インターフェイスに設定された DNS サーバーと検索ドメインを表示します。 |

## コマンド デフォルト

**system** キーワードを含めない場合、このコマンドはアクセスコントロールルールで使用されるすべての FQDN ネットワークオブジェクトの DNS 解決を表示します。

## 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。 |
| 6.3 | FQDNベースのアクセスコントロールルールのサポートが追加されました。 |

### 例

次に、管理アドレスの DNS 設定を表示する例を示します。

```
> show dns system
search example.com
nameserver 72.163.47.11
```

次の例は、アクセスコントロールルールで使用される FQDN ネットワークオブジェクトのDNS解決を示しています。FQDNオブジェクトは、ルールで使用されている場合にのみ解決されます。オブジェクトを定義するだけでは、名前のDNSルックアップは開始されません。

```
> show dns
Name:   www.example1.com
  Address: 10.1.3.1                          TTL 00:03:01
  Address: 10.1.3.3                          TTL 00:00:36
  Address: 10.4.1.2                          TTL 00:01:01
Name: www.example2.com
  Address: 10.2.4.1                          TTL 00:25:13
  Address: 10.5.2.1                          TTL 00:25:01
Name: server.ddns-exampleuser.com
  Address: fe80::21e:8cff:feb5:4faa          TTL 00:00:41
  Address: 10.10.10.2                        TTL 00:25:01
```

次に、**show dns host** コマンドの出力例を示します。

```
> show dns host www.example1.com
Name:   www.example1.com
  Address: 10.1.3.1                              TTL 00:03:01
  Address: 10.1.3.3                              TTL 00:00:36
  Address: 10.4.1.2                              TTL 00:01:01
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear dns** | FQDN ネットワークオブジェクトの DNS 解決を削除します。 |
| **show network** | 管理インターフェイスの設定を表示します。 |

# show dns-hosts

DNS キャッシュを表示するには、**show dns-hosts** コマンドを使用します。DNS キャッシュには、DNS サーバーからのダイナミックに学習されたエントリおよび手動で入力された名前と IP アドレスが含まれます。

**show dns-hosts**

## 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、**show dns-hosts** コマンドの出力例を示します。

```
> show dns-hosts
Host                    Flags      Age Type   Address(es)
ns2.example.com         (temp, OK) 0    IP    10.102.255.44
ns1.example.com         (temp, OK) 0    IP    192.168.241.185
snowmass.example.com    (temp, OK) 0    IP    10.94.146.101
server.example.com      (temp, OK) 0    IP    10.94.146.80
```

次の表で各フィールドについて説明します。

**表 *25 : show dns-hosts* の各フィールド**

| フィールド | 説明 |
|---|---|
| ホスト（Host） | ホスト名を表示します。 |
| Flags | 次の組み合わせとしてエントリのステータスを表示します。<br>• temp：このエントリは DNS サーバーから取得されたため、一時的です。デバイスは、非アクティブになって 72 時間後にこのエントリを削除します。<br>• perm：このエントリは name コマンドを使用して追加されたため、永続的です。<br>• OK：このエントリは有効です。<br>• ??：このエントリは疑わしいため、再検証が必要です。<br>• EX：このエントリは期限切れです。 |
| Age | このエントリが最後に参照されてからの時間数を表示します。 |
| タイプ | DNS レコードのタイプを表示します。この値は常に IP です。 |

| フィールド | 説明 |
|---|---|
| Address(es) | IP アドレス。 |

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear dns-hosts** | DNS キャッシュをクリアします。 |

# show eigrp events

EIGRP イベントログを表示するには、**show eigrp events** コマンドを使用します。

**show eigrp** ［*as-number*］ **events** ［{*start end*} | **type**］

## 構文の説明

| | |
|---|---|
| *as-number* | （任意）イベント ログを表示している EIGRP プロセスの自律システム番号を指定します。脅威に対する防御 デバイスがサポートする EIGRP ルーティングプロセスは 1 つだけであるため、自律システム番号を指定する必要はありません。 |
| *end* | （任意）出力されるエントリを、インデックス番号 *start* で開始され、インデックス番号 *end* で終了するエントリに限定します。 |
| *start* | （任意）ログ エントリのインデックス番号を指定する数値。開始番号を指定すると、出力は指定されたイベントで開始し、*end* 引数で指定されたイベントで終了します。有効な値は、1 ～ 500 です。 |
| **type** | （任意）記録されるイベントを表示します。 |

## コマンド デフォルト

start および end を指定しない場合、すべてのログ エントリが表示されます。

## 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

**show eigrp events** の出力では最大 500 件のイベントが表示されます。イベントが最大数に到達すると、新しいイベントは出力の末尾に追加され、古いイベントは出力の先頭から削除されます。

**clear eigrp events** コマンドを使用して、EIGRP イベントログをクリアできます。

**show eigrp events type** コマンドは、EIGRP イベントのロギングステータスを表示します。デフォルトでは、ネイバー変更、ネイバー警告、およびDUAL FSMメッセージが記録されます。DUAL FSM イベントのロギングはディセーブルにできません。

### 例

次に、**show eigrp events** コマンドの出力例を示します。

```
> show eigrp events

Event information for AS 100:
1    12:11:23.500 Change queue emptied, entries: 4
2    12:11:23.500 Metric set: 10.1.0.0/16 53760
3    12:11:23.500 Update reason, delay: new if 4294967295
4    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5    12:11:23.500 Update reason, delay: metric chg 4294967295
```

```
6    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7    12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8    12:11:23.500 Find FS: 10.1.0.0/16 4294967295
9    12:11:23.500 Rcv update met/succmet: 53760 28160
10   12:11:23.500 Rcv update dest/nh: 10.1.0.0/16 10.130.60.248
11   12:11:23.500 Metric set: 10.1.0.0/16 4294967295
```

次に、**show eigrp events** コマンドで開始番号と終了番号を定義したときの出力例を示します。

```
> show eigrp events 3 8

Event information for AS 100:
3    12:11:23.500 Update reason, delay: new if 4294967295
4    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5    12:11:23.500 Update reason, delay: metric chg 4294967295
6    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7    12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8    12:11:23.500 Find FS: 10.1.0.0/16 4294967295
```

次に、EIGRP イベントログのエントリがない場合の **show eigrp events** コマンドの出力例を示します。

```
> show eigrp events

Event information for AS 100:  Event log is empty.
```

次に、**show eigrp events type** コマンドの出力例を示します。

```
> show eigrp events type

EIGRP-IPv4 Event Logging for AS 100:
      Log Size          500
      Neighbor Changes  Enable
      Neighbor Warnings Enable
      Dual FSM          Enable
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear eigrp events** | EIGRP イベント ロギング バッファをクリアします。 |

# show eigrp interfaces

EIGRP ルーティングに参加しているインターフェイスを表示するには、**show eigrp interfaces** コマンドを使用します。

**show eigrp** ［*as-number*］ **interfaces** ［*if-name*］［**detail**］

## 構文の説明

| | |
|---|---|
| *as-number* | （任意）アクティブ インターフェイスを表示する EIGRP プロセスの自律システム番号を指定します。脅威に対する防御デバイスがサポートする EIGRP ルーティングプロセスは 1 つだけであるため、自律システム番号を指定する必要はありません。 |
| **detail** | （任意）詳細情報を表示します。 |
| *if-name* | （任意）インターフェイスの名前。インターフェイス名を指定すると、指定されたインターフェイスに表示が制限されます。 |

## コマンド デフォルト

インターフェイス名を指定しない場合、すべての EIGRP インターフェイスの情報が表示されます。

## 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

**show eigrp interfaces** コマンドを使用して、EIGRP がアクティブなインターフェイスを判別し、それらのインターフェイスに関連している EIGRP に関する情報を学習します。

インターフェイスが指定された場合、そのインターフェイスのみが表示されます。指定されない場合、EIGRP を実行しているすべてのインターフェイスが表示されます。

自律システムが指定された場合、指定された自律システムについてのルーティング プロセスのみが表示されます。指定されない場合、すべての EIGRP プロセスが表示されます。

### 例

次に、**show eigrp interfaces** コマンドの出力例を示します。

```
> show eigrp interfaces

EIGRP-IPv4 interfaces for process 100

                    Xmit Queue    Mean   Pacing Time   Multicast   Pending
Interface   Peers   Un/Reliable   SRTT   Un/Reliable   Flow Timer  Routes
mgmt          0         0/0          0      11/434          0          0
outside       1         0/0        337       0/10           0          0
inside        1         0/0         10       1/63         103          0
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

**表 *26 : show eigrp interfaces* のフィールドの説明**

| フィールド | 説明 |
|---|---|
| process | EIGRP ルーティング プロセスの自律システム番号です。 |
| Peers | 直接接続されているピアの数。 |
| Xmit Queue Un/Reliable | 信頼性の低い送信キューおよび信頼性の高い送信キューに残っているパケットの数。 |
| Mean SRTT | 平均のスムーズ ラウンドトリップ時間間隔（秒）。 |
| Pacing Time Un/Reliable | EIGRP パケット（信頼性の低いパケットおよび信頼性の高いパケット）をインターフェイスに送信するタイミングを決定するために使用されるペーシング時間（秒）。 |
| Multicast Flow Timer | 脅威に対する防御 デバイスがマルチキャスト EIGRP パケットを送信する最大秒数。 |
| Pending Routes | 送信キュー内で送信を待機しているパケット内のルートの数。 |

# show eigrp neighbors

EIGRP ネイバーテーブルを表示するには、**show eigrp neighbors** コマンドを使用します。

**show eigrp** ［*as-number*］ **neighbors** ［**detail** | **static**］［*if-name*］

## 構文の説明

| | |
|---|---|
| *as-number* | （任意）ネイバー エントリを削除する EIGRP プロセスの自律システム番号を指定します。脅威に対する防御 デバイスがサポートする EIGRP ルーティングプロセスは 1 つだけであるため、自律システム番号を指定する必要はありません。 |
| **detail** | （任意）詳細なネイバー情報を表示します。 |
| *if-name* | （任意）インターフェイスの名前。インターフェイス名を指定する場合、そのインターフェイスを介して学習されたすべてのネイバーテーブル エントリが表示されます。 |
| **static** | （任意）静的に定義された EIGRP ネイバーを表示します。 |

## コマンド デフォルト

インターフェイス名を指定しない場合、すべてのインターフェイスを介して学習されたネイバーが表示されます。

## 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

**clear eigrp neighbors** コマンドを使用して、動的に学習されたネイバーを EIGRP ネイバーテーブルからクリアできます。**static** キーワードを使用しない限り、スタティックネイバーは出力に含まれません。

### 例

次に、**show eigrp neighbors** コマンドの出力例を示します。

```
> show eigrp neighbors

EIGRP-IPv4 Neighbors for process 100

Address                 Interface     Holdtime Uptime   Q      Seq  SRTT  RTO
                                      (secs)   (h:m:s)  Count  Num  (ms)  (ms)
172.16.81.28            Ethernet1     13       0:00:41  0      11   4     20
172.16.80.28            Ethernet0     14       0:02:01  0      10   12    24
172.16.80.31            Ethernet0     12       0:02:02  0      4    5     20
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *27 : show eigrp neighbors* フィールドの説明

| フィールド | 説明 |
|---|---|
| process | EIGRP ルーティング プロセスの自律システム番号です。 |
| Address | EIGRP ネイバーの IP アドレス。 |
| インターフェイス | 脅威に対する防御 デバイスがネイバーから hello パケットを受信するインターフェイス。 |
| Holdtime | 脅威に対する防御 デバイスがダウンと宣言されるまでにネイバーからの応答を待機する時間の長さ（秒単位）。このホールドタイムは、hello パケットでネイバーから受信し、別の hello パケットをネイバーから受信するまで減少し始めます。<br>ネイバーがデフォルトのホールド タイムを使用している場合は、この数値は 15 未満です。ピアがデフォルト以外のホールドタイムを設定している場合は、デフォルト以外のホールド タイムが表示されます。<br>この値が 0 に達すると、脅威に対する防御 デバイスは、ネイバーを到達不能と見なします。 |
| アップタイム（Uptime） | 脅威に対する防御 デバイスがこのネイバーからの応答を最初に受信してからの経過時間（時:分:秒）。 |
| Q Count | 脅威に対する防御デバイスが送信を待機している EIGRP パケット（アップデート、クエリー、応答）の数。 |
| Seq Num | ネイバーから受信した最後のアップデート、クエリー、または応答パケットのシーケンス番号。 |
| SRTT | スムーズ ラウンドトリップ時間。これは、EIGRP パケットをこのネイバーに送信し、脅威に対する防御 デバイスがそのパケットの確認応答を受信するために必要なミリ秒数です。 |
| RTO | Retransmission Timeout（再送信のタイムアウト）（ミリ秒）。これは、脅威に対する防御 デバイスが再送信キューからネイバーにパケットを再送信するまでに待機する時間です。 |

次に、 **show eigrp neighbors static** コマンドの出力例を示します。

```
> show eigrp neighbors static

EIGRP-IPv4 neighbors for process 100
Static Address                Interface
192.168.1.5                   management
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *28 : show ip eigrp neighbors static* のフィールドの説明

| フィールド | 説明 |
|---|---|
| process | EIGRP ルーティング プロセスの自律システム番号です。 |
| Static Address | EIGRP ネイバーの IP アドレス。 |
| インターフェイス | 脅威に対する防御デバイスがネイバーから hello パケットを受信するインターフェイス。 |

次に、**show eigrp neighbors detail** コマンドの出力例を示します。

```
> show eigrp neighbors detail

EIGRP-IPv4 neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q Seq Tye
                                            (sec)         (ms)       Cnt Num
3   1.1.1.3                 Et0/0             12 00:04:48 1832  5000  0  14
   Version 12.2/1.2, Retrans: 0, Retries: 0
   Restart time 00:01:05
0   10.4.9.5                Fa0/0             11 00:04:07  768  4608  0  4   S
   Version 12.2/1.2, Retrans: 0, Retries: 0
2   10.4.9.10               Fa0/0             13 1w0d        1  3000  0  6   S
   Version 12.2/1.2, Retrans: 1, Retries: 0
1   10.4.9.6                Fa0/0             12 1w0d        1  3000  0  4   S
   Version 12.2/1.2, Retrans: 1, Retries: 0
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *29 : show ip eigrp neighbors details* のフィールドの説明

| フィールド | 説明 |
|---|---|
| process | EIGRP ルーティング プロセスの自律システム番号です。 |
| H | このカラムは、指定されたネイバーとの間で確立されたピアリング セッションの順番を示します。順番は、0 から始まる連続した番号で指定されます。 |
| Address | EIGRP ネイバーの IP アドレス。 |
| インターフェイス | 脅威に対する防御デバイスがネイバーから hello パケットを受信するインターフェイス。 |

| フィールド | 説明 |
|---|---|
| Holdtime | 脅威に対する防御 デバイスがダウンと宣言されるまでにネイバーからの応答を待機する時間の長さ（秒単位）。このホールド タイムは、hello パケットでネイバーから受信し、別の hello パケットをネイバーから受信するまで減少し始めます。<br>ネイバーがデフォルトのホールド タイムを使用している場合は、この数値は 15 未満です。ピアがデフォルト以外のホールド タイムを設定している場合は、デフォルト以外のホールド タイムが表示されます。<br>この値が 0 に達すると、脅威に対する防御 デバイスは、ネイバーを到達不能と見なします。 |
| アップタイム（Uptime） | 脅威に対する防御 デバイスがこのネイバーからの応答を最初に受信してからの経過時間（時:分:秒）。 |
| SRTT | スムーズラウンドトリップ時間。これは、EIGRP パケットをこのネイバーに送信し、脅威に対する防御 デバイスがそのパケットの確認応答を受信するために必要なミリ秒数です。 |
| RTO | Retransmission Timeout（再送信のタイムアウト）（ミリ秒）。これは、脅威に対する防御 デバイスが再送信キューからネイバーにパケットを再送信するまでに待機する時間です。 |
| Q Count | 脅威に対する防御 デバイスが送信を待機している EIGRP パケット（アップデート、クエリー、応答）の数。 |
| Seq Num | ネイバーから受信した最後のアップデート、クエリー、または応答パケットのシーケンス番号。 |
| Version | 指定されたピアが実行中のソフトウェア バージョン。 |
| Retrans | パケットを再送した回数。 |
| Retries | パケットの再送を試行した回数。 |
| Restart time | 指定されたネイバーが再起動してからの経過時間（時:分:秒）。 |

# show eigrp topology

EIGRP トポロジテーブルを表示するには、**show eigrp topology** コマンドを使用します。

**show eigrp** ［*as-number*］ **topology** ［*ip-addr* ［*mask*］ | **active** | **all-links** | **pending** | **summary** | **zero-successors**］

## 構文の説明

| | |
|---|---|
| **active** | （任意）EIGRP トポロジ テーブル内のアクティブ エントリのみ表示します。 |
| **all-links** | （任意）EIGRP トポロジ テーブル内のすべてのルート（フィジブル サクセサでない場合も）を表示します。 |
| *as-number* | （任意）EIGRP プロセスの自律システム番号を指定します。脅威に対する防御 デバイスがサポートする EIGRP ルーティングプロセスは 1 つだけであるため、自律システム番号を指定する必要はありません。 |
| *ip-addr* | （オプション）表示するトポロジ テーブルからの IP アドレスを定義します。マスクと一緒に指定した場合、エントリの詳細な説明が提供されます。 |
| *mask* | （オプション）*ip-addr* 引数に適用するネットワーク マスクを定義します。 |
| **pending** | （任意）ネイバーからの更新を待機しているか、ネイバーへの応答を待機している、EIGRP トポロジ テーブル内のすべてのエントリを表示します。 |
| **summary** | （任意）EIGRP トポロジ テーブルの要約を表示します。 |
| **zero-successors** | （任意）EIGRP トポロジ テーブル内の使用可能なルートを表示します。 |

## コマンド デフォルト

フィジブル サクセサであるルートのみが表示されます。**all-links** キーワードを使用すると、フィージブルサクセサでないものも含めたすべてのルートが表示されます。

## 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

**clear eigrp topology** コマンドを使用して、ダイナミックエントリをトポロジテーブルから削除できます。

### 例

次に、**show eigrp topology** コマンドの出力例を示します。

```
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 10.2.1.0 255.255.255.0, 2 successors, FD is 0
          via 10.16.80.28 (46251776/46226176), Ethernet0
          via 10.16.81.28 (46251776/46226176), Ethernet1
P 10.2.1.0 255.255.255.0, 1 successors, FD is 307200
          via Connected, Ethernet1
          via 10.16.81.28 (307200/281600), Ethernet1
          via 10.16.80.28 (307200/281600), Ethernet0
```

次の表に、この出力で表示される重要なフィールドについて説明します。

**表 *30 : show eigrp topology* のフィールド情報**

| フィールド | 説明 |
|---|---|
| Codes | このトポロジ テーブル エントリの状態。Passive および Active は、この宛先に関する EIGRP 状態を示し、Update、Query、および Reply は、送信中のパケットのタイプを示します。 |
| P - Passive | ルートは良好だと認識され、この宛先についての EIGRP 計算は実行されません。 |
| A - Active | この宛先についての EIGRP 計算が実行されます。 |
| U - Update | この宛先に更新パケットが送信されたことを示します。 |
| Q - Query | この宛先にクエリー パケットが送信されたことを示します。 |
| R - Reply | この宛先に応答パケットが送信されたことを示します。 |
| r - Reply status | ソフトウェアがクエリーを送信し、応答を待機しているときに設定されるフラグ。 |
| address mask | 宛先の IP アドレスとマスク。 |
| successors | サクセサの数。この数値は、IP ルーティング テーブル内のネクストホップの数に対応します。「successors」が大文字で表示される場合、ルートまたはネクスト ホップは遷移状態です。 |

| フィールド | 説明 |
|---|---|
| FD | フィジブル ディスタンス。フィジブル ディスタンスは、宛先に到達するための最適なメトリックか、ルートがアクティブだったときに認識された最適なメトリックです。この値はフィジビリティ条件チェックに使用されます。レポートされたルータのディスタンス（スラッシュの後のメトリック）がフィジブル ディスタンスより小さい場合、フィジビリティ条件が満たされて、そのパスはフィジブル サクセサになります。ソフトウェアによってパスがフィジブル サクセサだと判断されると、その宛先にクエリーを送信する必要はありません。 |
| via | この宛先についてソフトウェアに通知したピアの IP アドレス。これらのエントリの最初の n 個（n はサクセサの数）は、現在のサクセサです。リスト内の残りのエントリはフィジブル サクセサです。 |
| (cost/adv_cost) | 最初の数値は宛先へのコストを表すEIGRP メトリックです。2 番めの数値はこのピアがアドバタイズした EIGRP メトリックです。 |
| interface | 情報の学習元のインターフェイス。 |

次に、IP アドレスとともに使用した **show eigrp topology** の出力例を示します。出力は内部ルートについてのものです。

```
> show eigrp topology 10.2.1.0 255.255.255.0
EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.2.1.0
255.255.255.0

    State is Passive, Query origin flag is 1, 1 Successor(s), FD is 281600
    Routing Descriptor Blocks:
        0.0.0.0 (Ethernet0/0), from Connected, Send flag is 0x0
            Composite metric is (281600/0), Route is Internal
            Vector metric:
                Minimum bandwidth is 10000 Kbit
                Total delay is 1000 microseconds
                Reliability is 255/255
                Load is 1/255
                Minimum MTU is 1500
                Hop count is 0
```

次に、IP アドレスとともに使用した **show eigrp topology** の出力例を示します。出力は外部ルートについてのものです。

```
> show eigrp topology 10.4.80.0 255.255.255.0
EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.4.80.0

255.255.255.0

    State is Passive, Query origin flag is 1, 1 Successor(s), FD is 409600
    Routing Descriptor Blocks:
        10.2.1.1 (Ethernet0/0), from 10.2.1.1, Send flag is 0x0
            Composite metric is (409600/128256), Route is External
            Vector metric:
                Minimum bandwidth is 10000 Kbit
                Total delay is 6000 microseconds
```

```
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1500
    Hop count is 1
External data:
    Originating router is 10.89.245.1
    AS number of route is 0
    External protocol is Connected, external metric is 0
    Administrator tag is 0 (0x00000000)
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear eigrp topology** | ダイナミックに検出されたエントリを EIGRP トポロジ テーブルからクリアします。 |

# show eigrp traffic

送受信される EIGRP パケットの数を表示するには、**show eigrp traffic** コマンドを使用します。

**show eigrp** ［*as-number*］ **traffic**

## 構文の説明

| | |
|---|---|
| *as-number* | （任意）イベント ログを表示している EIGRP プロセスの自律システム番号を指定します。脅威に対する防御 デバイスがサポートする EIGRP ルーティングプロセスは 1 つだけであるため、自律システム番号を指定する必要はありません。 |

## 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

**clear eigrp traffic** コマンドを使用すると、EIGRP トラフィックの統計情報をクリアできます。

### 例

次に、**show eigrp traffic** コマンドの出力例を示します。

```
> show eigrp traffic
EIGRP-IPv4 Traffic Statistics for AS 100
  Hellos sent/received: 218/205
  Updates sent/received: 7/23
  Queries sent/received: 2/0
  Replies sent/received: 0/2
  Acks sent/received: 21/14
  Input queue high water mark 0, 0 drops
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
  Hello Process ID: 1719439416
  PDM Process ID: 1719439824
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

**表 *31 : show eigrp traffic* フィールドの説明**

| フィールド | 説明 |
|---|---|
| process | EIGRP ルーティング プロセスの自律システム番号です。 |
| Hellos sent/received | 送受信された hello パケットの数 |
| Updates sent/received | 送受信されたアップデート パケットの数 |
| Queries sent/received | 送受信されたクエリー パケットの数 |
| Replies sent/received | 送受信された応答パケットの数 |

| フィールド | 説明 |
| --- | --- |
| Acks sent/received | 送受信された確認応答（ACK）パケットの数 |
| Input queue high water mark/drops | 最大受信しきい値に接近している受信パケット数および廃棄パケットの数 |
| SIA-Queries sent/received | 送受信された Stuck-in-active クエリー。 |
| SIA-Replies sent/received | 送受信された Stuck-in-active 応答。 |

# show environment

システムコンポーネントのシステム環境情報を表示するには、**show environment** コマンドを使用します。

（注） このコマンドは、Firepower 2100、4100、および 9300 シリーズデバイスではサポートされていません。FXOS CLI に接続し、このコマンドの代わりに **show env** コマンドを使用します。

**show environment** ［**alarm-contact** | **driver** | **fans** | **power-supplies** | **power_consumption** | **voltage** | **temperature** ［**accelerator** | **chassis** | **cpu** | **io-hub** | **mother-board** | **power-supply**］］

## 構文の説明

| | |
|---|---|
| **alarm-contact** | （オプション）ISA 3000 デバイス上の入力アラーム コンタクトの動作ステータスを表示します。 |
| **driver** | （オプション）環境モニタリング（IPMI）ドライバ ステータスを表示します。ドライバ ステータスは次のいずれかになります。<br>• RUNNING：ドライバは動作中です。<br>• STOPPED：エラーが原因でドライバが停止しています。 |
| **fans** | （任意）冷却ファンの動作ステータスを表示します。ステータスは次のいずれかになります。<br>• OK：ファンは正常に動作中です。<br>• Failed：ファンが故障しているため交換が必要です。 |

| | |
|---|---|
| **power-supplies** | （任意）電源の動作ステータスを表示します。各電源モジュールのステータスは次のいずれかになります。<br>• OK：電源は正常に動作中です。<br>• Failed：電源が故障しているため交換が必要です。<br>• Not Present：指定された電源が設置されていません。<br>電源モジュールの冗長性ステータスも表示されます。冗長性ステータスは次のいずれかになります。<br>• OK：ユニットはリソースが完全な状態で正常に動作中です。<br>• Lost：ユニットに冗長性はありませんが、最低限のリソースで正常に動作中です。これ以上の障害が発生した場合は、システムはシャットダウンされます。<br>• N/A：ユニットは電源の冗長性に対応するように設定されていません。 |
| **power_consumption** | （任意）電力消費値を表示します。 |
| **voltage** | （任意）CPU 電圧チャネル 1 ～ 24 の値を表示します。動作ステータスは除きます。 |
| **temperature** | （任意）プロセッサとシャーシの温度およびステータスを表示します。温度は摂氏で示されます。出力を特定のエリア：**accelerator**、**chassis**、**cpu**、**io-hub**、**motherboard**、**power-supply** に限定するキーワードを含めることができます。<br>ステータスは次のいずれかになります。<br>• OK：温度は通常の動作範囲内（70 度未満）です。<br>• Critical：温度は通常の動作範囲外です。70 ー 80 は Warm と見なされます。 80 ー 90 は Critical であり、90 を超えると Unrecoverable と見なされます。 |

## コマンド デフォルト

キーワードが指定されていない場合は、ドライバを除くすべての動作情報が表示されます。

## 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。 |
| 6.3 | ISA 3000 用に **alarm-contact** キーワードが追加されました。 |

## 使用上のガイドライン

デバイスの物理コンポーネントの動作環境情報を表示できます。この情報には、ファンおよび電源の動作ステータスと、CPU およびシャーシの温度およびステータスが含まれます。ISA 3000 デバイスには、入力アラーム コンタクトに関する情報が含まれています。

### 例

次に、**show environment** コマンドの一般的な出力例を示します。

```
> show environment
Cooling Fans:
------------------------------------
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 6900 RPM - OK  (Power Supply Fan)
   Right Slot (PS1): 7000 RPM - OK  (Power Supply Fan) Power Supplies:
------------------------------------
   Power Supply Unit Redundancy: OK
   Temperature:
   --------------------------------
   Left Slot (PS0): 26 C - OK  (Power Supply Temperature)
   Right Slot (PS1): 27 C - OK  (Power Supply Temperature)
   Cooling Fans:
   --------------------------------
   Left Slot (PS0): 6900 RPM - OK  (Power Supply Fan)
   Right Slot (PS1): 7000 RPM - OK  (Power Supply Fan)
Temperature:
------------------------------------
   Processors:
   --------------------------------
   Processor 1: 44.0 C - OK  (CPU1 Core Temperature)
   Processor 2: 45.0 C - OK  (CPU2 Core Temperature)
   Chassis:
   --------------------------------
   Ambient 1: 28.0 C - OK  (Chassis Front Temperature)
   Ambient 2: 40.5 C - OK  (Chassis Back Temperature)
   Ambient 3: 28.0 C - OK  (CPU1 Front Temperature)
   Ambient 4: 36.50 C - OK  (CPU1 Back Temperature)
   Ambient 5: 34.50 C - OK  (CPU2 Front Temperature)
   Ambient 6: 43.25 C - OK  (CPU2 Back Temperature)
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 26 C - OK  (Power Supply Temperature)
   Right Slot (PS1): 27 C - OK  (Power Supply Temperature)
```

次に、**show environment driver** コマンドの出力例を示します。

```
> show environment driver
Cooling Fans:
------------------------------------
   Chassis Fans:
   --------------------------------
   Cooling Fan 1: 5888 RPM - OK
   Cooling Fan 2: 5632 RPM - OK
   Cooling Fan 3: 5888 RPM - OK
   Power Supplies:
   --------------------------------
   Left Slot (PS0): N/A
   Right Slot (PS1): 8448 RPM - OK
Power Supplies:
```

```
-----------------------------------
   Left Slot (PS0): Not Present
   Right Slot (PS1): Present
   Left Slot (PS0): N/A
   Right Slot (PS1): 33 C - OK
   Left Slot (PS0): N/A
   Right Slot (PS1): 8448 RPM - OK
Temperature:
-----------------------------------
   Processors:
   --------------------------------
   Processor 1: 70.0 C - OK
   Chassis:
   --------------------------------
   Ambient 1: 36.0 C - OK  (Chassis Back Temperature)
   Ambient 2: 31.0 C - OK  (Chassis Front Temperature)
   Ambient 3: 39.0 C - OK  (Chassis Back Left Temperature)
   Power Supplies:
   --------------------------------
   Left Slot (PS0): N/A
   Right Slot (PS1): 33 C - OK
Voltage:
-----------------------------------
   Channel 1:  1.168 V -  (CPU Core 0.46V-1.4V)
   Channel 2: 11.954 V -  (12V)
   Channel 3:  4.998 V -  (5V)
   Channel 4:  3.296 V -  (3.3V)
   Channel 5:  1.496 V -  (DDR3 1.5V)
   Channel 6:  1.048 V -  (PCH 1.5V)
```

次に、show environment alarm-contact コマンドの出力例を示します。

```
> show environment alarm-contact
ALARM CONTACT 1
   Status:      not asserted
   Description: external alarm contact 1
   Severity:    minor
   Trigger:     closed
ALARM CONTACT 2
   Status:      not asserted
   Description: external alarm contact 2
   Severity:    minor
   Trigger:     closed
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear facility-alarm output** | 出力リレーの電源を切り、LED のアラーム状態をクリアします。 |
| **show facility-alarm** | トリガーされたアラームのステータス情報を表示します。 |
| **show version** | ハードウェアおよびソフトウェアのバージョンを表示します。 |

# show facility-alarm

ISA 3000 デバイスのトリガーされたアラームを表示するには、**show facility-alarm** コマンドを使用します。

**show facility-alarm** {**relay** | **status** [**major** | **minor** | **info**]}

## 構文の説明

| | |
|---|---|
| **relay** | アラーム出力リレーを通電状態にしたアラームを表示します。 |
| **status**[**major** \|**minor** \|**info**] | トリガーされたすべてのアラームを表示します。リストを制限するには、次のキーワードを追加します。<br>• **major**：すべてのメジャーシビラティ（重大度）のアラームが表示されます。<br>• **minor**：すべてのマイナーシビラティ（重大度）のアラームが表示されます。<br>• **info**：すべてのアラームが表示されます。このキーワードを使用すると、キーワードを使用しない場合と同じ出力になります。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

## 使用上のガイドライン

アラーム出力リレーを通電したアラームだけを表示するには、**relay** キーワードを使用します。出力アラームリレーは、トリガーされたアラームを有効にするよう設定したかどうかに基づいて通電されます。アラーム出力リレーを通電すると、接続しているデバイス（点滅光やブザーなど）がアクティブになります。

アラームアクションが外部アラーム出力リレーをトリガーしたかどうかに関わらず、トリガーされたすべてのアラームを表示するには、**status** キーワードを使用します。

次の表は出力の列について示しています。

| カラム | 説明 |
|---|---|
| ソース（Source） | アラームがトリガーされたデバイス。通常は、デバイスで設定されているホスト名です。 |
| Severity | [Major] または [minor] です。 |
| 説明 | トリガーされたアラームのタイプ。たとえば、温度、アラームの外部連絡先、冗長電源など。 |
| Relay | 外部アラーム出力リレーが通電または非通電のどちらであったか。外部出力アラームは、アラーム設定に基づいてトリガーされます。 |

| カラム | 説明 |
|---|---|
| 時刻 | トリガーされたアラームのタイムスタンプ。 |

### 例

次に、**show facility-alarm relay** コマンドの出力例を示します。

```
> show facility-alarm relay
Source    Severity   Description                            Relay      Time
firepower minor      external alarm contact 1 triggered  Energized  06:56:50 UTC Mon Sep
 22 2014
```

次に、**show facility-alarm status** コマンドの出力例を示します。

```
> show facility-alarm status info
Source    Severity  Description                          Relay         Time
firepower minor external alarm contact 1 triggered  Energized     06:56:50 UTC Mon Sep
22 2014
firepower minor Temp below Secondary Threshold      De-energized  06:56:49 UTC Mon Sep
22 2014
firepower major Redundant pwr missing or failed     De-energized  07:00:19 UTC Mon Sep
22 2014
firepower major Redundant pwr missing or failed     De-energized  07:00:19 UTC Mon Sep
22 2014

> show facility-alarm status major
Source    Severity  Description                          Relay         Time
firepower major     Redundant pwr missing or failed   De-energized  07:00:19 UTC Mon Sep
 22 2014
firepower major     Redundant pwr missing or failed   De-energized  07:00:19 UTC Mon Sep
 22 2014


> show facility-alarm status minor
Source    Severity  Description                          Relay         Time
firepower minor     external alarm contact 1 triggered  Energized     06:56:50 UTC Mon
Sep 22 2014
firepower minor     Temp below Secondary Threshold      De-energized  06:56:49 UTC Mon
Sep 22 2014
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear facility-alarm output** | 出力リレーの電源を切り、LED のアラーム状態をクリアします。 |
| **show alarm settings** | すべてのグローバル アラーム設定を表示します。 |
| **show environment alarm-contact** | 入力アラーム コンタクトのステータスを表示します。 |

# show failover

ユニットのフェールオーバーステータスに関する情報を表示するには、**show failover** コマンドを使用します。

**show failover** ［ **group** *num* ｜ **history** ［ **details** ］ ｜ **interface** ｜ **state** ｜ **trace** ［ オプション ］｜ **statistics** ｜ **details** ］

## 構文の説明

| | |
|---|---|
| **group** *num* | 指定されたフェールオーバー グループの実行状態を表示します。 |
| **history** ［**details**］ | フェールオーバー履歴を表示します。フェールオーバー履歴には、過去のフェールオーバーでの状態変更や、状態変更の理由が表示されます。この情報は、トラブルシューティングに役立ちます。<br>**details** キーワードを追加すると、ピアユニットのフェールオーバー履歴が表示されます。これには、フェールオーバーでのピア ユニットの状態変化や、その状態変化の理由が含まれます。<br>履歴情報は、デバイスのリブート時にクリアされます。 |
| **interface** | フェールオーバーおよびステートフル リンク情報を表示します。 |
| **state** | 両方のフェールオーバー ユニットのフェールオーバー状態を表示します。表示される情報は、ユニットのプライマリまたはセカンダリ ステータス、ユニットのアクティブ/スタンバイ ステータス、最後にレポートされたフェールオーバーの理由などがあります。障害の理由が解消されても、障害の理由は出力に残ります。 |
| **trace** [*options* ] | （任意）フェールオーバーイベントトレースを表示します。オプションには、フェールオーバーイベントトレースをレベル（1 ～ 5）で表示するオプションが含まれます。<br>• **critical** ：フェールオーバーの重要なイベントトレースをフィルタ処理（レベル = 1）<br>• **debugging**：フェールオーバーのデバッグトレースをフィルタ処理（デバッグレベル = 5）<br>• **error**：フェールオーバーの内部例外をフィルタ処理（レベル = 2）<br>• **informational**：フェールオーバーの情報トレースをフィルタ処理（レベル = 4）<br>• **warning**：フェールオーバーの警告をフィルタ処理（レベル=3） |
| **statistics** | フェールオーバー コマンドインターフェイスの送信および受信パケット数を表示します。 |

| | |
|---|---|
| **details** | 高可用性ペアを構成するペアのフェールオーバーの詳細を表示します。 |

## 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。 |
| 6.2.3 | **history details** キーワードが追加されました。 |
| 6.4 | 次のオブジェクトの静的カウントが追加されました。<br>• Rule DB B-Sync<br>• Rule DB P-Sync<br>• Rule DB Delete |
| 7.0 | **details** キーワードが追加されました。 |

## 使用上のガイドライン

**show failover** コマンドは、ダイナミック フェールオーバー情報、インターフェイスステータス、およびステートフル フェールオーバーの統計情報を表示します。

IPv4 と IPv6 の両方のアドレスがインターフェイスで設定されている場合は、両方のアドレスが出力に表示されます。インターフェイスには複数の IPv6 アドレスを設定できるため、リンクローカル アドレスのみが表示されます。インターフェイスに IPv4 アドレスが設定されていない場合、出力の IPv4 アドレスは 0.0.0.0 として表示されます。インターフェイスに IPv6 アドレスが設定されていない場合、アドレスは単純に出力から省かれます。

Stateful Failover Logical Update Statistics 出力は、ステートフル フェールオーバーがイネーブルの場合のみ表示されます。「xerr」および「rerr」の値はフェールオーバーのエラーではなく、パケット送受信エラーの数を示します。

**show failover** コマンド出力で、ステートフル フェールオーバーの各フィールドには次の値があります。

- Stateful Obj の値は次のとおりです。
  - xmit：送信されたパケットの数を示します。
  - xerr：送信エラーの数を示します。
  - rcv：受信したパケットの数を示します。
  - rerr：受信エラーの数を示します。
- 各行は、次に示す特定のオブジェクト スタティック カウントを表します。
  - General：すべてのステートフル オブジェクトの合計を示します。
  - sys cmd：**login** や **stay alive** などの論理的なシステム更新コマンドを示します。

- up time：脅威に対する防御 デバイスの（アクティブな 脅威に対する防御 がスタンバイ 脅威に対する防御 デバイスに渡す）アップタイムの値を示します。
- RPC services：リモート プロシージャ コール接続情報。
- TCP conn：ダイナミック TCP 接続情報。
- UDP conn：ダイナミック UDP 接続情報。
- ARP tbl：ダイナミック ARP テーブル情報。
- Xlate_Timeout：接続変換タイムアウト情報を示します。
- IPv6 ND tbl：IPv6 ネイバー探索テーブル情報。
- VPN IKE upd：IKE 接続情報。
- VPN IPSEC upd：IPSec 接続情報。
- VPN CTCP upd：cTCP トンネル接続情報。
- VPN SDI upd：SDI AAA 接続情報。
- VPN DHCP upd：トンネル型 DHCP 接続情報。
- SIP Session：SIP シグナリング セッション情報。
- Route Session：ルート同期アップデートの LU 統計情報
- Rule DB B-Sync：ルールデータベースの一括同期が実行された回数と、対応するエラー（存在する場合）を示します。
- Rule DB P-Sync：ルールデータベースの周期的な同期が実行された回数と、この操作に関するエラー（存在する場合）を示します。
- Rule DB Delete：ルールデータベース削除メッセージが送信された回数と、この操作に関するエラー（存在する場合）を示します。

フェールオーバー IP アドレスを入力しないと、**show failover** コマンドでは IP アドレスが 0.0.0.0 と表示され、インターフェイスのモニタリングが「待機」状態のままになります。フェールオーバーを機能させるにはフェールオーバー IP アドレスを設定する必要があります。

次の表に、フェールオーバーに関するインターフェイスの状態についての説明を示します。

**表 *32*：フェールオーバー インターフェイス状態**

| 状態 | 説明 |
|---|---|
| 標準 | インターフェイスは稼働中で、ピア ユニットの対応するインターフェイスから hello パケットを受信中です。 |

| 状態 | 説明 |
|---|---|
| Normal (Waiting) | インターフェイスは稼働中ですが、ピアユニットの対応するインターフェイスから hello パケットをまだ受信していません。インターフェイスのスタンバイ IP アドレスが設定されていること、および 2 つのインターフェイス間の接続が存在することを確認してください。<br>フェールオーバーインターフェイスがダウンしたときにも、この状態を確認できます。 |
| Normal (Not-Monitored) | インターフェイスは動作中ですが、フェールオーバープロセスによってモニターされていません。モニターされていないインターフェイスの障害によってフェールオーバーはトリガーされません。 |
| No Link | 物理リンクがダウンしています。 |
| No Link (Waiting) | 物理リンクがダウンし、インターフェイスはピアユニットの対応するインターフェイスから hello パケットをまだ受信していません。リンクが復元した後、スタンバイ IP アドレスがそのインターフェイスに設定されているかどうか、および 2 つのインターフェイス間が接続されているかどうかを確認します。 |
| No Link (Not-Monitored) | 物理リンクがダウンしていますが、フェールオーバープロセスによってモニターされていません。モニターされていないインターフェイスの障害によってフェールオーバーはトリガーされません。 |
| Link Down | 物理リンクは動作中ですが、インターフェイスは管理上ダウンしています。 |
| Link Down (Waiting) | 物理リンクは動作中ですが、インターフェイスは管理上ダウンしており、インターフェイスはピア ユニットの対応するインターフェイスから hello パケットをまだ受信していません。インターフェイスを稼働状態にした後、スタンバイ IP アドレスがインターフェイスに設定されているかどうか、および 2 つのインターフェイスが接続されているかどうかを確認します。 |
| Link Down (Not-Monitored) | 物理リンクは動作中ですが、インターフェイスは管理上ダウンしており、フェールオーバープロセスによってモニターされていません。モニターされていないインターフェイスの障害によってフェールオーバーはトリガーされません。 |
| Testing | ピア ユニットの対応するインターフェイスから hello パケットが届かないため、インターフェイスはテスト モードです。 |

| 状態 | 説明 |
|---|---|
| 不合格 | インターフェイスのテストに失敗し、インターフェイスは障害が発生したとしてマークされます。インターフェイスの障害によってフェールオーバー基準が満たされた場合、インターフェイスの障害によって、セカンダリ ユニットまたはフェールオーバー グループへのフェールオーバーが発生します。 |

### 例

アクティブ/スタンバイフェールオーバーでの **show failover** コマンドの出力例を次に示します。

```
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Failover On
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.7(0)74, Mate 9.7(0)74
Serial Number: Ours 9A41CKDXQJU, Mate 9A3MFP0H1CP
Last Failover at: 19:23:17 UTC Oct 26 2016
    This host: Primary - Active
        Active time: 589 (sec)
        slot 0: empty
          Interface diagnostic (0.0.0.0): Normal (Waiting)
          Interface outside (192.168.77.1): Normal (Waiting)
          Interface inside (192.168.87.1): Normal (Waiting)
        slot 1: snort rev (1.0)  status (up)
        slot 2: diskstatus rev (1.0)  status (up)
    Other host: Secondary - Standby Ready
        Active time: 0 (sec)
          Interface diagnostic (0.0.0.0): Normal (Waiting)
          Interface outside (0.0.0.0): Normal (Waiting)
          Interface inside (0.0.0.0): Normal (Waiting)
        slot 1: snort rev (1.0)  status (up)
        slot 2: diskstatus rev (1.0)  status (up)
Stateful Failover Logical Update Statistics
    Link : failover GigabitEthernet0/2 (up)
    Stateful Obj       xmit       xerr       rcv        rerr
    General            45         0          44         0
    sys cmd            44         0          44         0
    up time            0          0          0          0
    RPC services       0          0          0          0
    TCP conn           0          0          0          0
    UDP conn           0          0          0          0
    ARP tbl            0          0          0          0
    Xlate_Timeout      0          0          0          0
    IPv6 ND tbl        0          0          0          0
    VPN IKEv1 SA       0          0          0          0
    VPN IKEv1 P2       0          0          0          0
    VPN IKEv2 SA       0          0          0          0
    VPN IKEv2 P2       0          0          0          0
    VPN CTCP upd       0          0          0          0
```

```
    VPN SDI upd         0           0           0           0
    VPN DHCP upd        0           0           0           0
    SIP Session         0           0           0           0
    SIP Tx              0           0           0           0
    SIP Pinhole         0           0           0           0
    Route Session       0           0           0           0
    Router ID           0           0           0           0
    User-Identity       1           0           0           0
    CTS SGTNAME         0           0           0           0
    CTS PAC             0           0           0           0
    TrustSec-SXP        0           0           0           0
    IPv6 Route          0           0           0           0
    STS Table           0           0           0           0
    Rule DB B-Sync      0           0           1           0
    Rule DB P-Sync      5           0           1           0
    Rule DB Delete      12          0           5           0

    Logical Update Queue Information
                Cur   Max  Total
    Recv Q:     0     10    44
    Xmit Q:     0     11    238
```

アクティブ/スタンバイセットアップでの **show failover state** コマンドの出力例を次に示します。

```
> show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Negotiation    Backplane Failure        15:44:56 UTC Jun 20 2016
Other host -   Secondary
               Not Detected   Comm Failure             15:36:30 UTC Jun 20 2016

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

次の表で、**show failover state** コマンドの出力について説明します。

表 *33 : show failover state* の出力の説明

| フィールド | 説明 |
|---|---|
| Configuration State | コンフィギュレーションの同期化の状態を表示します。<br>スタンバイユニットで可能なコンフィギュレーション状態は、次のとおりです。<br>• **Config Syncing - STANDBY**：コンフィギュレーションの同期が実行されているときに設定されます。<br>• **Interface Config Syncing - STANDBY**<br>• **Sync Done - STANDBY**：スタンバイユニットが、アクティブユニットとのコンフィギュレーションの同期を完了したときに設定されます。<br>アクティブユニットで可能なコンフィギュレーション状態は、次のとおりです。<br>• **Config Syncing**：スタンバイユニットに対してコンフィギュレーションの同期を実行しているアクティブユニット上で設定されます。<br>• **Interface Config Syncing**<br>• **Sync Done**：アクティブユニットが、スタンバイユニットに対してコンフィギュレーションの同期を正常に完了したときに設定されます。<br>• **Ready for Config Sync**：スタンバイユニットがコンフィギュレーションの同期を受信する準備が完了したという信号を送るときにアクティブユニット上で設定されます。 |
| Communication State | MAC アドレスの同期化のステータスを表示します。<br>• **Mac set**：MAC アドレスがピアユニットからこのユニットに対して同期されました。<br>• **Updated Mac**：MACアドレスが更新され、他のユニットに対して同期する必要がある場合に使用されます。また、ユニットが遷移期間中に、ピア ユニットから同期化されたローカル MAC アドレスを更新する場合にも使用されます。 |
| Date/Time | 障害の日付およびタイムスタンプを表示します。 |

| フィールド | 説明 |
|---|---|
| Last Failure Reason | 最後にレポートされた障害の理由を表示します。この情報は、障害の条件が解消されてもクリアされません。この情報は、フェールオーバーが発生した場合にのみ変更されます。<br>可能な障害の理由は次のとおりです。<br>• **Interface Failure**：障害が発生したインターフェイスの数がフェールオーバー基準を満たしたため、フェールオーバーが発生しました。<br>• **Comm Failure**：フェールオーバーリンクに障害が発生したか、ピアがダウンしています。<br>• **Backplane Failure** |
| 状態 | ユニットの Primary/Secondary および Active/Standby ステータスを表示します。 |
| This host/Other host | This host は、コマンドが実行されたデバイスについての情報を示します。Other host は、フェールオーバーのペアとなる他のデバイスについての情報を示します。 |

プライマリユニットでの **show failover history** コマンドの出力例を次に示します。

```
> show failover history
==========================================================================
From State                To State                  Reason
==========================================================================
14:29:59 UTC Nov 11 2017
Not Detected              Negotiation               No Error

14:30:36 UTC Nov 11 2017
Negotiation               Cold Standby              Detected an Active mate

14:30:38 UTC Nov 11 2017
Cold Standby              Sync Config               Detected an Active mate

14:30:47 UTC Nov 11 2017
Sync Config               Sync File System          Detected an Active mate

14:30:47 UTC Nov 11 2017
Sync File System          Bulk Sync                 Detected an Active mate

14:31:00 UTC Nov 11 2017
Bulk Sync                 Standby Ready             Detected an Active mate

14:31:39 UTC Nov 11 2017
Standby Ready             Failed                    Interface check
                                                    This host:1
                                                    single_vf: OUTSIDE
                                                    Other host:0

14:31:46 UTC Nov 11 2017
Failed                    Standby Ready             Interface check
```

```
                                                    This host:0
                                                    Other host:0

14:33:36 UTC Nov 11 2017
Standby Ready              Just Active              HELLO not heard from mate

14:33:36 UTC Nov 11 2017
Just Active                Active Drain             HELLO not heard from mate

14:33:36 UTC Nov 11 2017
Active Drain               Active Applying Config   HELLO not heard from mate

14:33:36 UTC Nov 11 2017
Active Applying Config     Active Config Applied    HELLO not heard from mate

14:33:36 UTC Nov 11 2017
Active Config Applied      Active                   HELLO not heard from mate

==========================================================================
```

セカンダリユニットでの **show failover history** コマンドの出力例を次に示します。

```
> show failover history
==========================================================================
From State                 To State                 Reason
==========================================================================
17:17:29 UTC Nov 10 2017
Not Detected               Negotiation              No Error

17:18:06 UTC Nov 10 2017
Negotiation                Cold Standby             Detected an Active mate

17:18:08 UTC Nov 10 2017
Cold Standby               Sync Config              Detected an Active mate

17:18:17 UTC Nov 10 2017
Sync Config                Sync File System         Detected an Active mate

17:18:17 UTC Nov 10 2017
Sync File System           Bulk Sync                Detected an Active mate

17:18:30 UTC Nov 10 2017
Bulk Sync                  Standby Ready            Detected an Active mate

17:19:09 UTC Nov 10 2017
Standby Ready              Failed                   Interface check
                                                    This host:1
                                                    single_vf: OUTSIDE
                                                    Other host:0

17:19:21 UTC Nov 10 2017
Failed                     Standby Ready            Interface check
                                                    This host:0
                                                    Other host:0

==========================================================================
```

各エントリには、状態変更が発生した時刻および日付、開始状態、結果状態、および状態変更の理由が示されます。最も新しいエントリが表示の末尾に配置されます。古いエントリが上部に表示されます。最大で60エントリを表示できます。エントリが最

大数に到達した場合、最も古いエントリが出力の上部から削除され、新しいエントリが末尾に追加されます。

エラーの理由には、トラブルシューティングに役立つ詳細情報が含まれています。これには、インターフェイス チェック、フェールオーバー状態チェック、状態の進行の失敗、およびサービス モジュールの失敗があります。

次に、**show failover history details** コマンドの出力例を示します。

```
>show failover history details
==========================================================================
From State                 To State                   Reason
==========================================================================
09:58:07 UTC Jan 18 2017
Not Detected               Negotiation                No Error

09:58:10 UTC Jan 18 2017
Negotiation                Just Active                No Active unit found

09:58:10 UTC Jan 18 2017
Just Active                Active Drain               No Active unit found

09:58:10 UTC Jan 18 2017
Active Drain               Active Applying Config     No Active unit found

09:58:10 UTC Jan 18 2017
Active Applying Config    Active Config Applied       No Active unit found

09:58:10 UTC Jan 18 2017
Active Config Applied     Active                      No Active unit found

==========================================================================

PEER History Collected at 09:58:54 UTC Jan 18 2017
=======================PEER-HISTORY=======================================
From State                 To State                   Reason
=========================PEER-HISTORY=====================================
09:57:46 UTC Jan 18 2017
Not Detected               Negotiation                No Error

09:58:19 UTC Jan 18 2017
Negotiation                Cold Standby               Detected an Active mate

09:58:21 UTC Jan 18 2017
Cold Standby             Sync Config                  Detected an Active mate

09:58:29 UTC Jan 18 2017
Sync Config              Sync File System             Detected an Active mate

09:58:29 UTC Jan 18 2017
Sync File System         Bulk Sync                    Detected an Active mate

09:58:42 UTC Jan 18 2017
Bulk Sync                Standby Ready                Detected an Active mate

=========================PEER-HISTORY=====================================
```

**show failover history details** コマンドは、ピアのフェールオーバーの履歴を要求し、ユニットのフェールオーバー履歴とピアの最新のフェールオーバー履歴を出力します。

1 秒以内にピアが応答しない場合は、最後に収集されたフェールオーバー履歴情報が表示されます。

次の表に、フェールオーバーの状態を示します。状態には永続的と一時的の 2 つのタイプがあります。永続的な状態とは、障害などの何らかの出来事によって状態変更が発生するまで、ユニットが維持できる状態のことです。一時的な状態とは、ユニットが永続的な状態に到達するまでの間に経過する状態です。

**表 *34 :* フェールオーバーの状態**

| States | 説明 |
|---|---|
| Disabled | フェールオーバーはディセーブルです。これは安定したステートです。 |
| 不合格 | ユニットは障害状態です。これは安定したステートです。 |
| Negotiation | ユニットはピアとの接続を確立し、ピアとネゴシエートして、ソフトウェア バージョンの互換性を判別し、Active/Standby ロールを決定します。ネゴシエートされたロールに基づき、ユニットはスタンバイ ユニット状態またはアクティブ ユニット状態になるか、障害状態になります。これは一時的なステートです。 |
| Not Detected | ASA はピアの存在を検出できません。このことは、フェールオーバーがイネーブルな状態で ASA が起動されたが、ピアが存在しない、またはピアの電源がオフである場合に発生する可能性があります。 |
| **スタンバイ ユニット状態** | |
| Cold Standby | ユニットはピアがアクティブ状態に到達するのを待機します。ピア ユニットがアクティブ状態に到達すると、このユニットは Standby Config 状態に進みます。これは一時的なステートです。 |
| Sync Config | ユニットはピア ユニットから実行コンフィギュレーションを要求します。コンフィギュレーションの同期化中にエラーが発生した場合、ユニットは初期化状態に戻ります。これは一時的なステートです。 |
| Sync File System | ユニットはピア システムとファイル システムを同期化します。これは一時的なステートです。 |
| Bulk Sync | ユニットはピアから状態情報を受信します。この状態は、ステートフル フェールオーバーがイネーブルの場合にのみ発生します。これは一時的なステートです。 |
| Standby Ready | ユニットは、アクティブ ユニットに障害が発生した場合に引き継ぐ準備が完了しています。これは安定したステートです。 |

| States | 説明 |
|---|---|
| **アクティブ ユニット状態** | |
| Just Active | ユニットがアクティブユニットになったときの最初の状態です。この状態にあるとき、ユニットがアクティブになること、および IP アドレスと MAC アドレスをインターフェイスに設定することをピアに通知するメッセージがピアに送信されます。これは一時的なステートです。 |
| Active Drain | ピアからのキュー メッセージが廃棄されます。これは一時的なステートです。 |
| Active Applying Config | ユニットはシステム コンフィギュレーションを適用します。これは一時的なステートです。 |
| Active Config Applied | ユニットはシステム コンフィギュレーションの適用を完了しました。これは一時的なステートです。 |
| Active | ユニットはアクティブで、トラフィックを処理しています。これは安定したステートです。 |

それぞれの状態変更の後に状態変更の理由が続きます。この理由は、ユニットが一時的な状態から永続的な状態に進んでも、通常同じままになります。次に、可能性がある状態変更の理由を示します。

- エラーなし
- CI config cmd によって設定されている
- フェールオーバー状態チェック
- フェールオーバー インターフェイスの準備ができた
- HELLO が受信されない
- 他のユニットのソフトウェア バージョンが異なっている
- 他のユニットの動作モードが異なっている
- 他のユニットのライセンスが異なっている
- 他のユニットのシャーシ コンフィギュレーションが異なっている
- 他のユニットのカード コンフィギュレーションが異なっている
- 他のユニットからアクティブ状態を要求された
- 他のユニットからスタンバイ状態を要求された
- 他のユニットが、このユニットに障害があるとレポートした
- 他のユニットが、そのユニットに障害があるとレポートした

- コンフィギュレーションの不一致
- アクティブ ユニットが検出された
- アクティブ ユニットが検出されなかった
- コンフィギュレーションの同期化が行われた
- 通信障害から回復した
- 他のユニットの VLAN コンフィギュレーションが異なっている
- VLAN コンフィギュレーションを確認できない
- コンフィギュレーションの同期化が不完全である
- コンフィギュレーションの同期化に失敗した
- インターフェイス チェック
- このユニットの通信が失敗した
- フェールオーバー メッセージの ACK を受信しなかった
- 同期後の学習状態で他のユニットが動作しなくなった
- ピアの電源が検出されない
- フェールオーバー ケーブルがない
- HA 状態の進行に失敗した
- サービス カード障害が検出された
- 他のユニットのサービス カードに障害が発生した
- このユニットのサービス カードはピアと同様である
- LAN インターフェイスが未設定状態になった
- ピア ユニットがリロードされた
- シリアル ケーブルから LAN ベース fover に切り替わった
- コンフィギュレーション同期化の状態を確認できない
- 自動更新要求
- 原因不明

次に、**show failover interface** コマンドの出力例を示します。デバイスのフェールオーバー インターフェイスに IPv6 アドレスが設定されています。

```
> show failover interface
        interface folink GigabitEthernet0/2
                System IP Address: 2001:a0a:b00::a0a:b70/64
                My IP Address    : 2001:a0a:b00::a0a:b70
```

```
                Other IP Address : 2001:a0a:b00::a0a:b71
```

次に、高可用性ペアのピアデバイスからの **show failover details** コマンドの出力例を示します。

```
> show failover details
        Failover On
Failover unit Secondary
Failover LAN Interface: HA-LINK GigabitEthernet0/3 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
1 Hold Interval Success: 12 Failure: 0
2 Hold Interval Success: 15 Failure: 0
3 Hold Interval Success: 15 Failure: 0
4 Hold Interval Success: 15 Failure: 0
5 Hold Interval Success: 15 Failure: 0
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 311 maximum
Interface: management
        1 Hold Success: 0 Failure: 0
        2 Hold Success: 0 Failure: 0
        3 Hold Success: 0 Failure: 0
        4 Hold Success: 0 Failure: 0
        5 Hold Success: 0 Failure: 0
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 99.16(2)10, Mate 99.16(2)10
Serial Number: Ours 9A7WJNE35T5, Mate 9A3497TXPU6
Last Failover at: 06:56:25 UTC Jan 25 2021
        This host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASAv hw/sw rev (/99.16(2)10) status (Up Sys)
                  Interface management (203.0.113.130/fe80::250:56ff:feb7:4927): Unknown
 (Waiting)
                slot 1: snort rev (1.0)  status (up)
                snort poll success:2877 miss:0
                slot 2: diskstatus rev (1.0)  status (up)

                disk poll success:2877 miss:0
        Other host: Primary - Active
                Active time: 2910 (sec)
                  Interface management (203.0.113.130): Unknown (Waiting)
                slot 1: snort rev (1.0)  status (up)
                peer snort poll success:2877 miss:0
                slot 2: diskstatus rev (1.0)  status (up)

                peer disk poll success:2877 miss:0

Stateful Failover Logical Update Statistics
        Link : HA-LINK GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         379        0          380        0
        sys cmd         379        0          379        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        Xlate_Timeout   0          0          0          0
        IPv6 ND tbl     0          0          0          0
```

```
VPN IKEv1 SA    0          0          0          0
VPN IKEv1 P2    0          0          0          0
VPN IKEv2 SA    0          0          0          0
VPN IKEv2 P2    0          0          0          0
VPN CTCP upd    0          0          0          0
VPN SDI upd     0          0          0          0
VPN DHCP upd    0          0          0          0
SIP Session     0          0          0          0
SIP Tx  0       0          0          0
SIP Pinhole     0          0          0          0
Route Session   0          0          0          0
Router ID       0          0          0          0
User-Identity   0          0          1          0
CTS SGTNAME     0          0          0          0
CTS PAC         0          0          0          0
TrustSec-SXP    0          0          0          0
IPv6 Route      0          0          0          0
```

次に、**show failover trace** コマンドのフェールオーバー警告出力の例を示します。

```
> show failover trace warning
        Warning:Output can be huge. Displaying in pager mode
        Oct 14 UTC 20:56:56.345 [CABLE]    [ERROR]fover: peer rcvd down ifcs info
        Oct 14 UTC 20:56:56.345 [CABLE]    [ERROR]fover: peer has  1  down ifcs
        Oct 14 UTC 20:56:56.345 [CABLE]    [ERROR]fover: peer rcvd down ifcs info
        Oct 14 UTC 20:56:56.345 [CABLE]    [ERROR]fover: peer has  1  down ifcs
        Oct 14 UTC 20:56:56.345 [CABLE]    [ERROR]fover: peer rcvd down ifcs info
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show running-config failover** | 現在のコンフィギュレーションの **failover** コマンドを表示します。 |

# show failover exec

指定したユニットの **failover exec** コマンドモードを表示するには、**show failover exec** コマンドを使用します。

**show failover exec** {**active** | **standby** | **mate**}

## 構文の説明

| | |
|---|---|
| **active** | アクティブユニットの **failover exec** コマンドモードを表示します。 |
| **mate** | ピアユニットの **failover exec** コマンドモードを表示します。 |
| **standby** | スタンバイユニットの **failover exec** コマンドモードを表示します。 |

## 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

**failover exec** コマンドは、指定したデバイスとのセッションを確立します。脅威に対する防御は CLI 設定をサポートしていませんが、デフォルトでは、このセッションはグローバル コンフィギュレーション モードになります。このモードの情報は、脅威に対する防御 とは無関係です。

**show failover exec** コマンドを使用すると、指定したデバイスのコマンドモードが表示されます。**failover exec** コマンドを使用して送信されたコマンドは、このモードで実行されます。

### 例

次に、**show failover exec** コマンドの出力例を示します。

```
> show failover exec mate
Standby unit Failover EXEC is at config mode
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **failover exec** | フェールオーバー ペアの指定されたユニット上で、入力されたコマンドを実行します。 |

# show file

ファイルシステムに関する情報を表示するには、**show file** コマンドを使用します。

**show file** ［**descriptors** | **system** | **information** *filename*］

## 構文の説明

| | |
|---|---|
| **descriptors** | 開かれているファイル記述子をすべて表示します。 |
| **information** *filename* | パートナーアプリケーションパッケージファイルなど、指定したファイルについての情報を表示します。 |
| **system** | ディスク ファイル システムについて、サイズ、利用可能なバイト数、メディアのタイプ、フラグ、およびプレフィックス情報を表示します。 |

## 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、**show file system** コマンドの出力例を示します。

```
> show file system
File Systems:
     Size(b)     Free(b)      Type      Flags  Prefixes
* 7935832064    7828107264    disk      rw      disk0: flash:
             -             -  disk      rw      disk1:
             -             -  network   rw      tftp:
             -             -  opaque    rw      system:
             -             -  network   ro      http:
             -             -  network   ro      https:
             -             -  network   rw      scp:
             -             -  network   rw      ftp:
             -             -  network   wo      cluster:
             -             -  stub      ro      cluster_trace:
             -             -  network   rw      smb:
```

次に、**show file information** コマンドの出力例を示します。

```
> show file information install.log
disk0:/install.log:
  type is ascii text
  file size is 150484 bytes
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **dir** | ディレクトリの内容を表示します。 |
| **pwd** | 現在の作業ディレクトリを表示します。 |

# show firewall

現在のファイアウォール モード（ルーテッドまたはトランスペアレント）を表示するには、**show firewall** コマンドを使用します。

**show firewall**

## 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、**show firewall** コマンドの出力例を示します。

```
> show firewall
Firewall mode: Router
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure firewall** | ファイアウォール モードを設定します。 |
| **show mode** | 現在のコンテキストモード（シングルまたはマルチ）を表示します。 |

# show flash

内部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。

**show flash:** ［**all** | **controller** | **filesys**］

（注） 脅威に対する防御 では、**flash** キーワードに エイリアス **disk0** が使用されます。

## 構文の説明

| | |
|---|---|
| **all** | すべてのフラッシュの情報を表示します。 |
| **controller** | ファイル システム コントローラの情報を表示します。 |
| **filesys** | ファイル システムの情報を表示します。 |

## 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、**show flash:** コマンドの出力例を示します。

```
> show flash:
--#--  --length--  -----date/time------  path
   48  107030784   Oct 05 2016 02:10:26  os.img
   49  33          Oct 06 2016 16:15:24  .boot_string
   50  150484      Oct 06 2016 15:36:02  install.log
   11  4096        Oct 06 2016 15:58:16  log
   13  1065        Oct 06 2016 15:59:13  log/asa-appagent.log
   16  4096        Oct 06 2016 15:59:07  crypto_archive
   51  4096        Oct 06 2016 15:59:12  coredumpinfo
   52  59          Oct 06 2016 15:59:12  coredumpinfo/coredump.cfg
   53  36          Oct 06 2016 16:04:47  enable_configure

7935832064 bytes total (7828107264 bytes free)
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **dir** | ディレクトリの内容を表示します。 |
| **show disk0:** | 内部フラッシュメモリの内容を表示します。 |
| **show disk1:** | 外部フラッシュメモリカードの内容を表示します。 |

# show flow-export counters

NetFlow 統計情報およびエラーデータのランタイムカウンタを表示するには、**show flow-export counters** コマンドを使用します。

**show flow-export counters**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

### 例

次に、NetFlow のランタイムカウンタを表示する方法の例を示します。

```
> show flow-export counters

destination: inside 209.165.200.224 2055
 Statistics:
  packets sent                       1000
 Errors:
  block allocation failure              0
  invalid interface                     0
  template send failure                 0
  no route to collector                 0
  source port allocation                0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear flow-export counters** | NetFlow のランタイム カウンタをすべてゼロにリセットします。 |

# show flow-offload

フロー、カウンタ、統計、およびオフロードされたフローに関する情報を表示するには、**show flow-offload** コマンドを使用します。

このコマンドは Firepower 4100/9300 シャーシ の 脅威に対する防御で使用できます。

**show flow-offload** {**flow**[**count**|**detail**]|**dynamic**[**count**|**detail**]|**static**[**count**|**detail**]|**info**[**detail**]|**statistics**}

## 構文の説明

| | |
|---|---|
| **flow**[**dynamic**|**static**]|[**count**|**detail**] | パラメータを指定しない場合、使用中の静的および動的フロー、最大使用率、オフロード率、および衝突数が表示されます。<br>動的フローまたは静的フローのカウンタ、統計、および情報のみを表示するには、**dynamic** キーワードか **static** キーワードを追加します。<br>オプションで次のキーワードを追加できます。<br>• **count**：オフロードされているアクティブなフローとオフロードされている作成済みのフローの数を表示します。<br>• **detail**：オフロードされているアクティブなフローとそれらの書き換えルールとデータを表示します。 |
| **info**[**detail**] | 動的フローオフロードの現在の状態。ポートの使用状況の要約などの追加情報を取得するには、**detail** キーワードを追加します。 |
| **statistics** | パケット数、正常な送信、およびエラー。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

## 使用上のガイドライン

フロー、カウンタ、統計、およびフローオフロードに関する情報を表示するには、**show flow-offload** コマンドを使用します。

**clear flow-offload** コマンドを使用して、カウンタまたは統計をクリアします。

**show flow-offload flow** コマンドの出力例を次に示します。オフロードされたフローは、送信元と宛先の IP アドレス、ポート、およびプロトコルをハッシュすることによって計算されるインデックス番号によって識別されます。システムが現在アクティブなオフロードされたフローと同じインデックスを持つフローをオフロードしようとすると、衝突が発生します。この場合、新しいフローはオフロードされませんが、最初のフローはオフロードされたままになります。

```
>show flow-offload flow
Total offloaded flow stats: 1 in use, 5 most used, 100% offloaded, 0 collisions
```

```
UDP intfc 103 src 10.1.1.2:41110 dest 20.1.1.2:5001, dynamic, timestamp 162810457, packets
 84040, bytes 127404640
```

**show flow-offload flow count** コマンドの出力例を次に示します。

```
>show flow-offload flow count
Total offloaded flow stats:  4 in use, 20 most used, 10% offloaded, 0 collisions
```

**show flow-offload flow detail** コマンドの出力例を次に示します。rw(*number*) は、MAC または VLAN などの標準ヘッダーフィールドがその特定のオフロードフローに対して書き換えられたことを示します。

```
>show flow-offload flow detail
Total offloaded flow stats: 2 in use, 6 most used, 100% offloaded, 0 collisions
TCP vlan 711 intfc 101 src 172.16.1.3:21766 dest 9.9.1.3:80, dynamic, timestamp 217959066,
 packets 633139, bytes 43053452
    node 0, ft index 58197, queue_id 727
    rw(0): cmd '  replace', offset  0, bytes 12, data(x) 90E2 BA01 8E29 B0AA 7730 097B
    rw(1): cmd 'increment', offset 46, bytes  4, data(x) 422AC658
```

**show flow-offload dynamic** コマンドの出力例を次に示します。

```
>show flow-offload flow dynamic
Dynamically offloaded flow stats: 2 in use, 6 most used, 100% offloaded, 0 collisions
    TCP vlan 711 intfc 101 src 172.16.1.3:21809 dest 9.9.1.3:80, dynamic, timestamp
218392513, packets 14741, bytes 1002388
    TCP vlan 911 intfc 102 src 9.9.1.3:80 dest 172.16.1.3:21809, dynamic, timestamp
218392534, packets 16794, bytes 23972345
```

**show flow-offload dynamic count** コマンドの出力例を次に示します。

```
>show flow-offload flow dynamic count
Dynamically offloaded flow stats: 2 in use, 6 most used, 100% offloaded, 0 collisions
```

**show flow-offload dynamic detail** コマンドの出力例を次に示します。

```
>show flow-offload flow dynamic detail
Total offloaded flow stats: 4 in use, 20 most used, 10% offloaded, 0 collisions
TCP intfc 134 src 9.9.1.3:80 dest 192.168.0.3:5240, static, timestamp 142633202, packets
 442870, bytes 630342730
TCP intfc 133 src 192.168.0.3:5240 dest 9.9.1.3:80, static, timestamp 142633204, packets
 442971, bytes 28350144
TCP intfc 136 src 9.9.1.4:80 dest 192.168.0.4:7240, dynamic, timestamp 142633876, packets
 82870, bytes 10342730
TCP intfc 135 src 192.168.0.4:7240 dest 9.9.1.4:80, dynamic, timestamp 142633877, packets
 82971, bytes 350144
```

**show flow-offload info** コマンドの出力例を次に示します。**Current running state** はフローオフロードの現在の状態であり、将来の実装のために予約されています（この時点で値はできません）。**User configured state** は、管理対象デバイスがリブートされた場合のフローオフロードの状態です。（現在、これらの値は常に同じです）**Dynamic flow offload** は、動的フローオフロードの現在の状態です。

```
>show flow-offload flow info
Current running state        : Enabled
User configured state        : Enabled
Dynamic flow offload         : Enabled
```

**show flow-offload info detail** コマンドの出力例を次に示します。

```
> show flow-offload flow info detail
Current running state        : Enabled
User configured state        : Enabled
Dynamic flow offload       : Enabled
```

```
Offload App                 : Running
Offload allocated cores     : S0[ 1] S1[ 13]
Offload reserved Nic        : 9 22
Max PKT burst               : 32
Port-0 details :
        RX queue number     :            149
        FQ queue number     :            727
        Keep alive counter  :         142327
Port-1 details :
        RX queue number     :            147
        FQ queue number     :            725
        Keep alive counter  :         142328
```

**show flow-offload statistics** コマンドの出力例を次に示します。**VNIC** は、動的フローがオフロードされるハードウェアを指します。

```
> show flow-offload statistics
Packet stats of port : 0
    Tx Packet count                 :      16483549549
    Rx Packet count                 :      16483549549
    Dropped Packet count            :                0
    VNIC transmitted packet         :      16483549549
    VNIC transmitted bytes          :   12389816183297
    VNIC Dropped packets            :                0
    VNIC erroneous received         :                0
    VNIC CRC errors                 :                0
    VNIC transmit failed            :                0
    VNIC multicast received         :                0
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **configure flow-offload** | 動的フローオフロードを有効または無効にします。 |
| **clear flow-offload** | 動的フローオフロードのカウンタまたは統計をクリアします。 |

# show flow-offload-ipsec

IPsec フローのオフロードに関する情報を表示するには、 **show flow-offload-ipsec** を使用します。

**show flow-offload-ipsec** { **info** | **option-table** | **statistics** }

## 構文の説明

| | |
|---|---|
| **info** | IPsec フローオフロードの現在の設定状態に関する情報を表示します。 |
| **option-table** | IPsec フローオフロードで使用される Content Addressable Memory（CAM）のテーブル情報を表示します。この情報はデバッグにのみ使用され、エンドユーザーにとっては意味はありません。 |
| **statistics** | オフロードされたフローの Content Addressable Memory（CAM）の統計を表示します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2 | このコマンドが導入されました。 |

### 例

次に、IPsec フローオフロードの現在の設定状態を表示する例を示します。

```
ciscoasa# show flow-offload-ipsec info
IPSec offload : Enabled
Egress optimization: Enabled
```

次に、統計を表示する例を示します。

```
> show flow-offload-ipsec statistics

        Packet stats of Pipe 0
        ----------------------
        Rx Packet count                          :               0
        Tx Packet count                          :               0
        Error Packet count                       :               0
        Drop Packet count                        :               0

        CAM stats of Pipe 0
        ----------------------
        Option ID Table CAM Hit Count            :              38
        Option ID Table CAM Miss Count           :             154
        Tunnel Table CAM Hit Count               :               0
        Tunnel Table CAM Miss Count              :               0
        6-Tuple CAM Hit Count                    :               0
        6-Tuple CAM Miss Count                   :              38
```

次に、オプションテーブルを表示する例を示します。

```
> show flow-offload-ipsec option-table
        instance_id:256 interface_id:124 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:123 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:122 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:121 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:120 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:119 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:118 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:117 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:156 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:157 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:158 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:159 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:112 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:111 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:110 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:109 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:108 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:107 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:106 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:105 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:104 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:103 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:102 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:101 action:0 logic_id_opt:0 subinterface_id_opt:0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear flow-offload-ipsec** | IPsec フローオフロードの統計をクリアします。 |

# show fqdn

完全修飾ドメイン名（FQDN）ネットワークオブジェクトの名前解決に関するトラブルシューティング情報を表示するには、**show fqdn** コマンドを使用します。

**show fqdn** ［**id** ［*fqdn_id*］ | **ip** ［*ip_address*］］

## 構文の説明

| | |
|---|---|
| **id** [*fqdn_id*] | FQDN ネットワークオブジェクトに関連付けられた ID 番号に基づいて情報を表示します。ID はシステムによって割り当てられます。必要に応じて ID 値を含めることができます。ID 値は、**show running-config** コマンドの出力を調べることで確認できます。たとえば、次のオブジェクトの ID 番号は 1001 です。<br><br>`object network www.example.com`<br>` fqdn www.example.com id 1001` |
| **ip** [*ip_address*] | DNS サーバーから取得した IP アドレスに基づいて情報を表示します。必要に応じて、IP アドレスを入力できます。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | 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、トラブルシューティングの目的で使用します。FQDN と IP アドレスのマッピング方法を確認するには、このコマンドの代わりに **show dns** コマンドを使用します。

**show fqdn** コマンドは、各オブジェクトのシステム提供の ID 番号を介して、特定のネットワークオブジェクトに名前解決を関連付ける詳細情報を表示します。

### 例

次に、オブジェクト ID と IP アドレスの FQDN マッピングを表示する例を示します。

```
> show fqdn

FQDN IP Table:
ip=10.1.45.1, object=Testobj-1, domain=www.cisco.com, hits=10,
           id=45893456,63987645

ip=2001::134, object=Testobj-1, domain=www.cisco.com, hits=10,
          id=45893456

FQDN ID Table:
id=45893456, object=Testobj-1, domain=www.cisco.com
           ip=10.1.45.1, ip=34.12.45.189
           ip6=2001::134

id=23987645, object=Testobj-2, domain=www.google.com
```

```
ip=20.11.65.121, ip=101.2.4.69
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear dns** | FQDN ネットワークオブジェクトの DNS 解決を削除します。 |
| **show dns** | FQDN ネットワークオブジェクトの DNS 解決を表示します。 |
| **show running-config** | 実行設定を表示します。 |

# show fragment

IP フラグメント再構成モジュールの動作データを表示するには、**show fragment** を入力します。

**show fragment** ［*interface*］

**構文の説明**

| | |
|---|---|
| *interface* | （任意）脅威に対する防御のインターフェイスを指定します。 |

**コマンド デフォルト**

interface が指定されていない場合、このコマンドはすべてのインターフェイスに適用されます。

**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。 |
| 6.7 | show fragment コマンドの出力が拡張され、IP フラグメント関連のドロップ カウンタとエラーカウンタが含まれるようになりました。 |

### 例

次に、IP フラグメント再構築モジュールの動作データを表示する方法の例を示します。

```
> show fragment
Interface: inside
Configuration: Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
Run-time stats: Queue: 0, Full assembly: 12
Drops: Size overflow: 0, Timeout: 0,
Chain overflow: 0, Fragment queue threshold exceeded: 0,
Small fragments: 0, Invalid IP len: 0,
Reassembly overlap: 26595, Fraghead alloc failed: 0,
SGT mismatch: 0, Block alloc failed: 0,
Invalid IPV6 header: 0
```

それぞれの説明は次のとおりです。

- [Size]：デフォルトとして設定した任意のポイントで、フラグメントデータベース（インターフェイスごと）に存在できるブロックの最大数。
- チェーン（Chain）：完全な IP パケットをフラグメント化する場合の最大フラグメント数を指定します。デフォルトは 24 です。
- タイムアウト（Timeout）：フラグメント化されたパケット全体が到着するのを待機する最大秒数を指定します。デフォルトは 5 秒です。
- リアセンブル（Reassembly）：仮想（virtual）または完全（full）。デフォルトは virtual です。IP フラグメントが ASA で終了する場合やアプリケーション レベルでインスペクションを必要とする場合には、完全（物理的）にリアセンブルされます。必要に応じて、完全（物理的）にリアセンブルされたパケットは、出力インターフェイスで再度フラグメント化できます。

- [Size Overflow]：任意の時点でフラグメントデータベースに存在できるブロックの最大数に達しました。オーバーフローカウンタでは、フラグメントデータベースのデフォルトサイズに達したことによるドロップ数が測定されます。このカウンタには、キューサイズ（最大 DB サイズの 2/3）が原因でドロップされたフラグメントの数は含まれません。
- [Timeout]：再構築が完了する前にフラグメントチェーンがタイムアウトしました。
- [Chain limit]：個々のフラグメントチェーンの制限に達しました。
- [Fragment queue threshold exceeded]：フラグメントデータベースのしきい値（インターフェイスあたりのキューサイズの 2/3）を超過しています。
- [Small fragments]：フラグメントオフセットが 0 より大きく 16 より小さい場合。
- [Invalid packet len]：無効な IP パケット長（例、パケット長 > 65535）。
- [Reassembly overlap]：重複またはオーバーラップしているフラグメントが検出されました。
- [Fraghead alloc failed]：フラグメントヘッドの割り当てに失敗しました。Fraghead には、IP パケットのすべてのフラグメントのチェーンが維持されます。
- [SGT mismatch]：同じ IP パケットのフラグメント間で SGT 値が一致しませんでした。
- [Block alloc failed]：完全な再構築の割り当てに失敗しました。
- [Invalid IPV6 header]：完全な再構築中に無効な IPV6 ヘッダーが検出されました。

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear configure fragment** | IP フラグメント再構成コンフィギュレーションをクリアし、デフォルトにリセットします。 |
| **clear fragment** | IP フラグメント再構成モジュールの動作データをクリアします。 |
| **show running-config fragment** | IP フラグメント再構成コンフィギュレーションを表示します。 |

# show gc

ガーベッジ コレクション プロセスの統計情報を表示するには、**show gc** コマンドを使用します。

**show gc**

## 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、**show gc** コマンドの出力例を示します。

```
> show gc

Garbage collection process stats:
Total tcp conn delete response             :            0
Total udp conn delete response             :            0
Total number of zombie cleaned             :            0
Total number of embryonic conn cleaned     :            0
Total error response                       :            0
Total queries generated                    :            0
Total queries with conn present response   :            0
Total number of sweeps                     :          946
Total number of invalid vcid               :            0
Total number of zombie vcid                :            0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear gc** | ガーベッジ コレクション プロセスの統計情報を削除します。 |

# show h225

脅威に対する防御 デバイスで確立された H.225 セッションの情報を表示するには、**show h225** コマンドを使用します。

**show h225**

## 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

**show h225** コマンドは、デバイスで確立された H.225 セッションの情報を表示します。

異常なほど多くの接続が存在する場合は、デフォルトのタイムアウト値または設定した値に基づいてセッションがタイムアウトしているかどうか確認します。タイムアウトしていなければ問題があるので、調査が必要です。

### 例

次に、**show h225** コマンドの出力例を示します。

```
> show h225
Total H.323 Calls: 1
1 Concurrent Call(s) for
    Local:   10.130.56.3/1040   Foreign: 172.30.254.203/1720
    1. CRV 9861
    Local:   10.130.56.3/1040   Foreign: 172.30.254.203/1720
0 Concurrent Call(s) for
    Local:   10.130.56.4/1050   Foreign: 172.30.254.205/1720
```

この出力は、ローカルエンドポイント 10.130.56.3 と外部ホスト 172.30.254.203 との間で 脅威に対する防御 デバイスを通過するアクティブな H.323 コールが 1 つ存在し、これらのエンドポイントの間には、コールの CRV（Call Reference Value）が 9861 の同時コールが 1 つ存在することを示しています。

ローカル エンドポイント 10.130.56.4 と外部ホスト 172.30.254.205 に対して、同時コールは 0 です。つまり H.225 セッションがまだ存在しているものの、このエンドポイント間にはアクティブ コールがないことを意味します。この状況は、**show h225** コマンドを実行したときに、コールはすでに終了しているものの、H.225 セッションがまだ削除されていない場合に発生する可能性があります。または、2 つのエンドポイントが、「maintainConnection」を TRUE に設定しているため、TCP 接続をまだ開いたままにしていることを意味する可能性もあります。したがって、「maintainConnection」を再度 FALSE に設定するまで、またはコンフィギュレーション内の H.225 タイムアウト値に基づくセッションのタイムアウトが起こるまで、セッションは開いたままになります。

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show h245** | スロースタートを使用しているエンドポイントによってデバイスで確立された H.245 セッションの情報を表示します。 |
| **show h323 ras** | デバイスで確立された H.323 RAS セッションの情報を表示します。 |

# show h245

スロースタートを使用しているエンドポイントによって 脅威に対する防御 デバイスを越えて確立された H.245 セッションの情報を表示するには、**show h245** コマンドを使用します。

**show h245**

## 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

**show h245** コマンドは、スロースタートを使用しているエンドポイントが 脅威に対する防御 デバイスを越えて確立した H.245 セッションの情報を表示します。（スロースタートでは、コールの 2 つのエンドポイントが H.245 用に別の TCP コントロール チャネルを開きます。ファスト スタートは、H.245 メッセージが H.225 コントロール チャネルで H.225 メッセージの一部として交換された場合です。

### 例

次に、**show h245** コマンドの出力例を示します。

```
> show h245
Total: 1
        LOCAL           TPKT    FOREIGN         TPKT
1       10.130.56.3/1041        0       172.30.254.203/1245    0
        MEDIA: LCN 258 Foreign 172.30.254.203 RTP 49608 RTCP 49609
                       Local   10.130.56.3 RTP 49608 RTCP 49609
        MEDIA: LCN 259 Foreign 172.30.254.203 RTP 49606 RTCP 49607
                       Local   10.130.56.3 RTP 49606 RTCP 49607
```

脅威に対する防御 デバイスを越えてアクティブな H.245 コントロールセッションが、現在 1 つあります。ローカル エンドポイントは、10.130.56.3 であり、TPKT 値が 0 であることから、このエンドポイントからの次のパケットには TPKT ヘッダーがあると予測します。（TKTP ヘッダーは、各 H.225/H.245 メッセージの先頭の 4 バイト ヘッダーです。このヘッダーで、この 4 バイトのヘッダーを含むメッセージの長さがわかります）。外部のホストのエンドポイントは、172.30.254.203 であり、TPKT 値が 0 であることから、このエンドポイントからの次のパケットには TPKT ヘッダーがあると予測します。

これらのエンドポイント間でネゴシエートされるメディアは、論理チャネル番号（LCN）が 258 で、外部の RTP IP アドレス/ポート ペアが 172.30.254.203/49608、RTCP IP アドレス/ポートが 172.30.254.203/49609、ローカルの RTP IP アドレス/ポート ペアが 10.130.56.3/49608、RTCP ポートが 49609 です。

値が 259 の 2 番めの LCN は、外部の RTP IP アドレス/ポート ペアが 172.30.254.203/49606、RTCP IP アドレス/ポート ペアが 172.30.254.203/49607、ローカルの RTP IP アドレス/ポート ペアが 10.130.56.3/49606、RTCP ポートが 49607 です。

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show h245** | スロースタートを使用しているエンドポイントによって 脅威に対する防御 デバイスを越えて確立された H.245 セッションの情報を表示します。 |
| **show h323 ras** | 脅威に対する防御 デバイスを越えて確立された H.323 RAS セッションの情報を表示します。 |

# show h323

H.323 接続の情報を表示するには、**show h323** コマンドを使用します。

**show h323** {**ras** | **gup**}

## 構文の説明

| | |
|---|---|
| **ras** | 脅威に対する防御 デバイスを越えてゲートキーパーとその H.323 エンドポイントの間に確立されている H.323 RAS セッションを表示します。 |
| **gup** | H323 ゲートウェイ アップデート プロトコル接続に関する情報を表示します。 |

## 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

**show h323 ras** コマンドは、脅威に対する防御 デバイスを越えてゲートキーパーとその H.323 エンドポイントの間に確立されている H.323 RAS セッションの情報を表示します。

### 例

次に、**show h323 ras** コマンドの出力例を示します。

```
> show h323 ras

Total: 1
        GK                      Caller
        172.30.254.214          10.130.56.14
```

この出力は、ゲートキーパー 172.30.254.214 とそのクライアント 10.130.56.14 の間にアクティブな登録が 1 つあることを示しています。

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show h245** | スロースタートを使用しているエンドポイントによって 脅威に対する防御 デバイスを越えて確立された H.245 セッションの情報を表示します。 |

# show hardware-bypass

ISA 3000 における現在のハードウェアバイパスのステータスを表示するには、**show hardware-bypass** コマンドを使用します。

**show hardware-bypass**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

### 例

次に、**show hardware-bypass** コマンドの出力例を示します。

```
> show hardware-bypass
                          Status              Powerdown           Powerup
GigabitEthernet 1/1-1/2   Disable             Disable             Disable
GigabitEthernet 1/3-1/4   Disable             Disable             Disable

Pairing supported on these interfaces: gig1/1 & gig1/2, gig1/3 & gig1/4
```

# show high-availability config

高可用性（フェールオーバー）設定の情報を表示するには、**show high-availability config** コマンドを使用します。

**show high-availability config**

## 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

**show high-availability config** コマンドは **show failover** コマンドのエイリアスです。詳細については、**show failover** のリファレンスページを参照してください。

### 例

次の例は、アクティブ/スタンバイ フェールオーバー モードのデバイスのフェールオーバー設定を示しています。

```
> show high-availability config
Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.7(0)74, Mate 9.7(0)74
Serial Number: Ours 9A41CKDXQJU, Mate 9A3MFP0H1CP
Last Failover at: 19:23:17 UTC Oct 26 2016
        This host: Primary - Active
                Active time: 2009 (sec)
                slot 0: empty
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface outside (192.168.77.1): Normal (Waiting)
                  Interface inside (192.168.87.1): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface outside (0.0.0.0): Normal (Waiting)
                  Interface inside (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)

Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         235        0          234        0
        sys cmd         234        0          234        0
```

```
up time          0           0           0           0
RPC services     0           0           0           0
TCP conn         0           0           0           0
UDP conn         0           0           0           0
ARP tbl          0           0           0           0
Xlate_Timeout    0           0           0           0
IPv6 ND tbl      0           0           0           0
VPN IKEv1 SA     0           0           0           0
VPN IKEv1 P2     0           0           0           0
VPN IKEv2 SA     0           0           0           0
VPN IKEv2 P2     0           0           0           0
VPN CTCP upd     0           0           0           0
VPN SDI upd      0           0           0           0
VPN DHCP upd     0           0           0           0
SIP Session      0           0           0           0
SIP Tx           0           0           0           0
SIP Pinhole      0           0           0           0
Route Session    0           0           0           0
Router ID        0           0           0           0
User-Identity    1           0           0           0
CTS SGTNAME      0           0           0           0
CTS PAC          0           0           0           0
TrustSec-SXP     0           0           0           0
IPv6 Route       0           0           0           0
STS Table        0           0           0           0

Logical Update Queue Information
                 Cur     Max     Total
Recv Q:          0       10      234
Xmit Q:          0       11      1200
```

次の例は、デバイスが現在フェールオーバー用に設定されていない場合の表示内容を示しています。フェールオーバーがオフであることを示す最初の行は、この出力で唯一意味のある部分です。

```
> show high-availability config
Failover Off
Failover unit Secondary
Failover LAN Interface: not Configured
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 12 of 160 maximum
MAC Address Move Notification Interval not set
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show failover** | フェールオーバー（ハイアベイラビリティ）設定を示します。 |

# show https-access-list

**show https-access-list** コマンドは、デバイスに設定されている HTTPS アクセスリストを表示します。

**show https-access-list**

## 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

HTTPS アクセスリストによって、**configure network ipv4**/**ipv6** コマンドで設定された管理インターフェイスへの HTTPS 接続を確立できるアドレスが決定されます。HTTPS 接続は、ローカルマネージャである Device Manager を使用してデバイスを設定および管理するために使用します。

データインターフェイスへの through-the-box トラフィックや HTTPS アクセスは、このアクセスリストによって制御されません。

### 例

管理インターフェイスの HTTPS アクセスリストの例を次に示します。

```
> show https-access-list
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:https
ACCEPT     tcp      anywhere             anywhere             state NEW tcp dpt:https
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **configure https-access-list** | 管理インターフェイスに HTTPS アクセスリストを設定します。 |

# show i

# show idb

インターフェイスリソースを表す内部データ構造であるインターフェイス記述子ブロックのステータスに関する情報を表示するには、**show idb** コマンドを使用します。

**show idb**

## 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、**show idb** コマンドの出力例を示します。

```
> show idb
Maximum number of Software IDBs 2252.  In use(total) 16. In use(active) 16

                    HWIDBs     SWIDBs
             Active 15         15
           Inactive 1          1
         Total IDBs 16         16
 Size each (bytes) 984         1512
        Total bytes 15744      24192

HWIDB#  1 0xdacf1420  Virtual0
HWIDB#  2 0xdac4da20  GigabitEthernet1/1
HWIDB#  3 0xdac5aa20  GigabitEthernet1/2
HWIDB#  4 0xdac651b0  GigabitEthernet1/3
HWIDB#  5 0xdac6f940  GigabitEthernet1/4
HWIDB#  6 0xdac7a0d0  GigabitEthernet1/5
HWIDB#  7 0xdac84860  GigabitEthernet1/6
HWIDB#  8 0xdac8eff0  GigabitEthernet1/7
HWIDB#  9 0xdac99780  GigabitEthernet1/8
HWIDB# 10 0xdacbda00  Internal-Control1/1
HWIDB# 11 0xdaca3f10  Internal-Data1/1
HWIDB# 12 0xdacb3260  Internal-Data1/2
HWIDB# 13 0xdacc81a0  Internal-Data1/3
HWIDB# 14 0xd409e4e0  Internal-Data1/4
HWIDB# 15 0xd409d090  Management1/1

SWIDB#  1 0xdacf1840 0x00000041 Virtual0 UP UP
SWIDB#  2 0xdac4de40 0x00000002 GigabitEthernet1/1 UP DOWN
SWIDB#  3 0xdac5ae40 0x00000003 GigabitEthernet1/2 UP DOWN
SWIDB#  4 0xdac655d0 0xffffffff GigabitEthernet1/3 DOWN DOWN
SWIDB#  5 0xdac6fd60 0xffffffff GigabitEthernet1/4 DOWN DOWN
SWIDB#  6 0xdac7a4f0 0xffffffff GigabitEthernet1/5 DOWN DOWN
SWIDB#  7 0xdac84c80 0xffffffff GigabitEthernet1/6 DOWN DOWN
SWIDB#  8 0xdac8f410 0xffffffff GigabitEthernet1/7 DOWN DOWN
SWIDB#  9 0xdac99ba0 0xffffffff GigabitEthernet1/8 DOWN DOWN
SWIDB# 10 0xdacbde20 0x0000003f Internal-Control1/1 UP UP
SWIDB# 11 0xdaca4330 0x00000043 Internal-Data1/1 UP UP
SWIDB# 12 0xdacb3680 0xffffffff Internal-Data1/2 UP UP
SWIDB# 13 0xdacc85c0 0x00000044 Internal-Data1/3 UP UP
SWIDB# 14 0xdacae210 0x00000045 Internal-Data1/4 UP UP
```

```
SWIDB# 15 0xd409d4b0 0x00000004 Management1/1 UP UP
```

次の表で各フィールドについて説明します。

**表 *35 : show idb stats* の各フィールド**

| フィールド | 説明 |
|---|---|
| HWIDBs | すべての HWIDB の統計情報を表示します。HWIDB は、システム内の各ハードウェア ポートについて作成されます。 |
| SWIDBs | すべての SWIDB の統計情報を表示します。SWIDB は、システム内の各メインおよびサブインターフェイスについて、およびコンテキストに割り当てられている各インターフェイスについて作成されます。<br>他の一部の内部ソフトウェア モジュールも IDB を作成します。 |
| HWIDB# | ハードウェア インターフェイス エントリを示します。IDB シーケンス番号、アドレス、およびインターフェイス名が各行に表示されます。 |
| SWIDB# | ソフトウェア インターフェイス エントリを示します。IDB シーケンス番号、アドレス、対応する vPif ID、およびインターフェイス名が各行に表示されます。 |
| PEER IDB# | コンテキストに割り当てられているインターフェイスを示します。IDB シーケンス番号、アドレス、対応する vPif ID、コンテキスト ID、およびインターフェイス名が各行に表示されます。 |

## 関連コマンド

| Command | 説明 |
|---|---|
| **show interface** | インターフェイスの実行時ステータスと統計情報を表示します。 |

# show identity-subnet-filter

ユーザから IP へ、およびセキュリティグループタグ（SGT）から IP へのマッピングの受信時に除外されたサブネットを表示するには、**show identity-subnet-filter** コマンドを使用します。

**show identity-subnet-filter**

## 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。 |

## 使用上のガイドライン

**show identity-subnet-filter** コマンドは、ユーザから IP およびセキュリティグループタグ（SGT）から IP へのマッピングから現在除外されているすべてのサブネットを表示します。

### 例

次に、現在除外されているサブネットがない場合の **show identity-subnet-filter** コマンドの出力例を示します。

```
> show identity-subnet-filter

Subnet filter file doesn't exist
```

次に、一部のサブネットが現在除外されている場合の **show identity-subnet-filter** コマンドの出力例を示します。

```
> show identity-subnet-filter

Subnet filters are:
2001:db8::2/64
192.0.2.0/24
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **configure identity-subnet-filter** | ユーザから IP および SGT から IP のマッピングからサブネットを除外します。 |

# show igmp groups

脅威に対する防御デバイスに直接接続されている受信者、およびIGMPを通じて学習された受信者を含むマルチキャストグループを表示するには、**show igmp groups** コマンドを使用します。

**show igmp groups** ［［**reserved** | *group*］［*if_name*］［**detail**］］ | **summary**］

## 構文の説明

| | |
|---|---|
| **detail** | （任意）ソースの詳細説明を出力します。 |
| *group* | （任意）IGMP グループのアドレス。このオプション引数を含めると、表示は指定されたグループに限定されます。 |
| *if_name* | （任意）指定されたインターフェイスについてのグループ情報を表示します。 |
| **reserved** | （任意）予約されたグループについての情報を表示します。 |
| **summary** | （任意）グループ加入の要約情報を表示します。 |

## 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

オプションの引数およびキーワードをすべて省略すると、**show igmp groups** コマンドは、直接接続されたすべてのマルチキャストグループを、グループアドレス、インターフェイスタイプ、およびインターフェイス番号別に表示します。

### 例

次に、**show igmp groups** コマンドの出力例を示します。

```
> show igmp groups

IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
224.1.1.1        inside               00:00:53  00:03:26  192.168.1.6
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show igmp interface** | インターフェイスのマルチキャスト情報を表示します。 |

# show igmp interface

インターフェイスのマルチキャスト情報を表示するには、**show igmp interface** コマンドを使用します。

**show igmp interface** ［*if_name*］

## 構文の説明

| | |
|---|---|
| *if_name* | （任意）選択したインターフェイスについての IGMP グループ情報を表示します。 |

## 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

オプションの if_name 引数を省略すると、**show igmp interface** コマンドはすべてのインターフェイスに関する情報を表示します。

### 例

次に、**show igmp interface** コマンドの出力例を示します。

```
> show igmp interface inside

inside is up, line protocol is up
 Internet address is 192.168.37.6, subnet mask is 255.255.255.0
 IGMP is enabled on interface
 IGMP query interval is 60 seconds
 Inbound IGMP access group is not set
 Multicast routing is enabled on interface
 Multicast TTL threshold is 0
 Multicast designated router (DR) is 192.168.37.33
 No multicast groups joined
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show igmp groups** | 脅威に対する防御 デバイスに直接接続されている受信者、および IGMP を通じて学習された受信者を含むマルチキャストグループを表示します。 |

# show igmp traffic

IGMP トラフィック統計情報を表示するには、**show igmp traffic** コマンドを使用します。

**show igmp traffic**

## 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、**show igmp traffic** コマンドの出力例を示します。

```
> show igmp traffic

IGMP Traffic Counters
Elapsed time since counters cleared: 00:02:30
                               Received     Sent
Valid IGMP Packets                3           6
Queries                           2           6
Reports                           1           0
Leaves                            0           0
Mtrace packets                    0           0
DVMRP packets                     0           0
PIM packets                       0           0

Errors:
Malformed Packets                 0
Martian source                    0
Bad Checksums                     0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear igmp counters** | すべての IGMP 統計カウンタをクリアします。 |
| **clear igmp traffic** | IGMP トラフィック カウンタをクリアします。 |

# show inline-set

デバイスで設定されているインラインセット（IPS 専用インターフェイス）に関する情報を表示するには、**show inline-set** コマンドを使用します。

**show inline-set** ［*inline-set-name* | **mac-address-table**］

## 構文の説明

| | |
|---|---|
| *inline-set-name* | （任意）指定されたインラインセットに関する情報を表示します。名前を含めない場合は、すべてのインラインセットが表示されます。 |
| **mac-address-table** | （任意）インラインセットの MAC アドレスブリッジを表示します。 |

## 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、**show inline-set** コマンドの出力例を示します。

```
> show inline-set
Inline-set ips-inline
  Mtu is 1500 bytes
  Fail-open for snort down is on
  Fail-open for snort busy is off
  Tap mode is off
  Propagate-link-state option is off
  hardware-bypass mode is disabled
  Interface-Pair[1]:
    Interface: GigabitEthernet0/3 "inline-inside"
      Current-Status: UP
    Interface: GigabitEthernet0/4 "inline-outside"
      Current-Status: DOWN
    Bridge Group ID: 504
```

# show interface

IP インターフェイスの統計情報を表示するには、**show interface** コマンドを使用します。

**show interface** ［{*physical_interface* | **redundant***number*}［**.***subinterface*］ | *interface_name* | **BVI** *id* | ］［**summary** | **stats** | **detail**］

## 構文の説明

| | |
|---|---|
| **BVI** *id* | （任意）指定されたブリッジ仮想インターフェイス（BVI）の統計情報を表示します。BVI 番号（1 ー 250）を入力します。 |
| **detail** | （任意）インターフェイスの詳細な情報を表示します。この情報には、インターフェイスが追加された順序、設定されている状態、実際の状態、非対称ルーティングの統計情報（有効になっている場合）が含まれます。<br>すべてのインターフェイスを表示すると、システム通信に使用される内部インターフェイスに関する情報も表示されます。内部インターフェイスをユーザーが設定することはできません。情報はデバッグのみを目的としています。 |
| *interface_name* | （任意）論理名でインターフェイスを指定します。 |
| *physical_interface* | （任意）インターフェイス ID（**gigabitethernet0/1** など）を指定します。使用可能なインターフェイスは、デバイスモデルによって異なります。デバイスで使用可能な名前を表示するには、パラメータなしで show interface コマンドを使用します。 |
| **redundant***number* | （任意）冗長インターフェイス ID（**redundant1** など）を指定します。 |
| **stats** | （デフォルト）インターフェイス情報および統計情報を表示します。このキーワードはデフォルトであるため、このキーワードはオプションです。 |
| **summary** | （任意）いずれかのインターフェイスに関する情報を表示します。 |
| サブインターフェイス | （任意）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。 |

## コマンド デフォルト

いずれのオプションも識別しない場合、このコマンドは、内部インターフェイスを除くすべてのインターフェイスについての基本的な統計情報を表示します。

## 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。 |
| 6.2 | **BVI** キーワードが追加されました。 |

| リリース | 変更内容 |
|---|---|
| 6.7 | データインターフェイスで Management Center アクセスを設定したときに、Internal-Data0/1 "nlp_int_tap"インターフェイスの **detail** キーワードに出力が追加されました。 |

## 使用上のガイドライン

サブインターフェイスについて表示される統計情報の数は、物理インターフェイスについて表示される統計情報の数のサブセットです。

（注） Hardware カウントと Traffic Statistics カウントでは、送信または受信されるバイト数が異なります。

Hardware カウントでは、この量はハードウェアから直接取得され、レイヤ 2 パケットのサイズが反映されます。一方、Traffic Statistics では、レイヤ 3 パケットのサイズが反映されます。

カウントの差はインターフェイス カード ハードウェアの設計に基づいて異なります。

たとえば、ファスト イーサネット カードの場合、レイヤ 2 カウントはイーサネット ヘッダーを含むため、トラフィック カウントよりも 14 バイト大きくなります。ギガビット イーサネット カードの場合、レイヤ 2 カウントはイーサネット ヘッダーと CRC の両方を含むため、トラフィック カウントよりも 18 バイト大きくなります。

出力の説明については、「例」を参照してください。

### 例

次に、**show interface** コマンドの出力例を示します。

```
> show interface
Interface GigabitEthernet1/1 "outside", is down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        MAC address e865.49b8.97f2, MTU 1500
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
  Traffic Statistics for "outside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
```

```
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet1/2 "inside", is down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        MAC address e865.49b8.97f3, MTU 1500
        IP address 192.168.45.1, subnet mask 255.255.255.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet1/3 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f4, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface GigabitEthernet1/4 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f5, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
```

```
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface GigabitEthernet1/5 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f6, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface GigabitEthernet1/6 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f7, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface GigabitEthernet1/7 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f8, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
```

```
Interface GigabitEthernet1/8 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f9, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface Management1/1 "diagnostic", is up, line protocol is up
  Hardware is en_vtun rev00, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
        Input flow control is unsupported, output flow control is off
        MAC address e865.49b8.97f1, MTU 1500
        IP address unassigned
        14247681 packets input, 896591753 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (0/0)
        output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "diagnostic":
        14247685 packets input, 697121911 bytes
        0 packets output, 0 bytes
        5054964 packets dropped
      1 minute input rate 2 pkts/sec,  131 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 2 pkts/sec,  108 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
        Management-only interface. Blocked 0 through-the-device packets
```

次の表は、各フィールドの説明を示しています。

**表 *36 : show interface* の各フィールド**

| フィールド | 説明 |
|---|---|
| インターフェイス ID | インターフェイス ID。 |

| フィールド | 説明 |
|---|---|
| “*interface_name*” | 論理インターフェイス名。名前を設定しない場合、Hardware行の下に次のメッセージが表示されます。<br><br>`Available but not configured via nameif` |
| is *state* | 管理ステートは次のとおりです。<br>• up：インターフェイスはシャットダウンされません。<br>• administratively down：インターフェイスは意図的にシャットダウンされています。 |
| Line protocol is state | 回線ステータスは次のとおりです。<br>• up：動作するケーブルがネットワーク インターフェイスに接続されています。<br>• down：ケーブルが正しくないか、インターフェイス コネクタに接続されていません。 |
| VLAN 識別子 | サブインターフェイスの場合、VLAN ID。 |
| ハードウェア | インターフェイスのタイプ、最大帯域幅、遅延、デュプレックス方式、および速度。リンクがダウンしている場合は、デュプレックス方式と速度は設定値が表示されます。リンクが動作している場合、これらのフィールドには実際の設定がカッコで囲まれて設定値とともに表示されます。 |
| Media-type | （常に表示されるわけではない）RJ-45 や SFP などのインターフェイス メディア タイプを表示します。 |
| message area | 一部の状況で、メッセージが表示される場合もあります。次の例を参照してください。<br>• 名前を設定しないと、次のメッセージが表示されます。「Available but not configured via nameif」<br>• インターフェイスが冗長インターフェイスのメンバの場合、次のメッセージが表示されます。「Active member of Redundant5」 |
| MAC address | インターフェイスの MAC アドレス。 |
| Site Specific MAC address | クラスタリングの場合に、使用中のサイト固有の MAC アドレスを表示します。 |
| MTU | このインターフェイス上で許可されるパケットの最大サイズ（バイト単位）。インターフェイス名を設定しない場合、このフィールドには「MTU not set」と表示されます。 |

| フィールド | 説明 |
|---|---|
| IP address | 静的なインターフェイス IP アドレスか、DHCP サーバーから受信したインターフェイス IP アドレス。 |
| サブネット マスク | IP アドレスのサブネット マスク。 |
| Packets input | このインターフェイスで受信したパケットの数。 |
| Bytes | このインターフェイスで受信したバイト数。 |
| No buffer | ブロック割り当てからの失敗の数。 |
| Received: | |
| Broadcasts | 受信したブロードキャストの数。 |
| Input errors | 次に示すタイプを含めた入力エラーの総数。入力に関係する他のエラーも入力エラーのカウントが増加する原因になります。また、一部のデータグラムは複数のエラーを含んでいることもあります。したがって、この合計数は、次に示すタイプについて表示されるエラーの数を超えることがあります。 |
| Runts | 最小のパケット サイズ（64 バイト）よりも小さいために廃棄されたパケットの数。ラントは通常、コリジョンによって発生します。不適切な配線や電気干渉によって発生することもあります。 |
| Giants | 最大パケット サイズを超えたため廃棄されるパケットの数。たとえば、1518 バイトよりも大きいイーサネット パケットはジャイアントと見なされます。 |
| CRC | 巡回冗長検査エラーの数。ステーションがフレームを送信すると、フレームの末尾に CRC を付加します。この CRC は、フレーム内のデータに基づくアルゴリズムから生成されます。送信元と宛先の間でフレームが変更された場合、システムは CRC が一致しないことを通知します。CRC の数値が高いことは、通常、コリジョンの結果であるか、ステーションが不良データを送信することが原因です。 |
| Frame | フレーム エラーの数。不良フレームには、長さが正しくないパケットや、フレーム チェックサムが正しくないパケットがあります。このエラーは通常、コリジョンまたはイーサネット デバイスの誤動作が原因です。 |
| Overrun | インターフェイスのデータ処理能力を入力レートが超えたため、ハードウェアバッファに受信したデータをインターフェイスが処理できなかった回数。 |
| Ignored | このフィールドは使用されません。値は常に 0 です。 |

| フィールド | 説明 |
|---|---|
| 中断 | このフィールドは使用されません。値は常に 0 です。 |
| L2 decode drops | 名前がまだ設定されていないか、無効な VLAN ID を持つフレームが受信されたためにドロップされたパケットの数。冗長インターフェイス構成のスタンバイインターフェイスでは、このインターフェイスに名前が設定されていないため、数が増加する可能性があります。 |
| Packets output | このインターフェイスに送信されたパケットの数。 |
| Bytes | このインターフェイスに送信されたバイトの数。 |
| Underruns | インターフェイスが処理できる速度よりも速くトランスミッタが動作した回数。 |
| Output Errors | 設定されたコリジョンの最大数を超えたため送信されなかったフレームの数。このカウンタは、ネットワーク トラフィックが多い場合にのみ増加します。 |
| Collisions | イーサネット コリジョン（単一および複数のコリジョン）が原因で再送信されたメッセージの数。これは通常、過渡に延長した LAN で発生します（イーサネット ケーブルまたはトランシーバ ケーブルが長すぎる、ステーション間のリピータが2つよりも多い、またはマルチポート トランシーバのカスケードが多すぎる場合）。衝突するパケットは、出力パケットによって 1 回だけカウントされます。 |
| Interface resets | インターフェイスがリセットされた回数。インターフェイスで3秒間送信できなかった場合、システムはインターフェイスをリセットして送信を再開します。この間隔では、接続状態が維持されます。インターフェイスのリセットは、インターフェイスがループバックまたはシャットダウンする場合も発生します。 |
| Babbles | 未使用。（「バブル」は、トランスミッタが最長フレームの送信に要した時間よりも長くインターフェイスに留まっていたことを意味します）。 |

| フィールド | 説明 |
|---|---|
| Late collisions | 通常のコリジョン ウィンドウの外側でコリジョンが発生したため、送信されなかったフレームの数。レイト コリジョンは、パケットの送信中に遅れて検出されるコリジョンです。これは通常発生しません。2つのイーサネットホストが同時に通信しようとした場合、早期にパケットが衝突して両者がバックオフするか、2 番めのホストが 1 番めのホストの通信状態を確認して待機します。<br><br>レイトコリジョンが発生すると、デバイスは割り込みを行ってイーサネット上にパケットを送信しようとしますが、脅威に対する防御 デバイスはパケットの送信を部分的に完了しています。脅威に対する防御 デバイスは、パケットの最初の部分を保持するバッファを解放した可能性があるため、パケットを再送しません。このことはあまり問題になりません。その理由は、ネットワーキング プロトコルはパケットを再送することでコリジョンを処理する設計になっているためです。ただし、レイト コリジョンはネットワークに問題が存在することを示しています。一般的な問題は、リピータで接続された大規模ネットワーク、および仕様の範囲を超えて動作しているイーサネット ネットワークです。 |
| Deferred | リンク上のアクティビティが原因で送信前に保留されたフレームの数。 |
| input reset drops | リセットが発生したときにRXリングでドロップしたパケットの数をカウントします。 |
| output reset drops | リセットが発生したときにTXリングでドロップしたパケットの数をカウントします。 |
| Rate limit drops | ギガビット以外の速度でインターフェイスを設定して、設定に応じて 10 Mbps または 100 Mbps を超えて送信しようとした場合にドロップされたパケットの数。 |
| Lost carrier | 送信中に搬送波信号が消失した回数。 |
| No carrier | 未使用。 |
| Input queue (curr/max packets): | 入力キュー内のパケットの数（現行値と最大値）。 |
| ハードウェア | ハードウェア キュー内のパケットの数。 |
| Software | ソフトウェア キュー内のパケットの数。ギガビット イーサネット インターフェイスでは使用できません。 |
| Output queue (curr/max packets): | 出力キュー内のパケットの数（現行値と最大値）。 |

| フィールド | 説明 |
|---|---|
| ハードウェア | ハードウェア キュー内のパケットの数。 |
| Software | ソフトウェア キュー内のパケットの数。 |
| input queue (blocks free curr/low) | curr/low エントリは、インターフェイスの受信（入力）記述子リング上の現在のスロットおよび使用可能な all-time-lowest スロットの番号を示します。これらは、メイン CPU によって更新されるため、all-time-lowest（インターフェイス統計情報が削除されるか、またはデバイスがリロードされるまで）の水準点はあまり正確ではありません。 |
| output queue (blocks free curr/low) | curr/low エントリは、インターフェイスの送信（出力）記述子リング上の現在のスロットおよび使用可能な all-time-lowest スロットの番号を示します。これらは、メイン CPU によって更新されるため、all-time-lowest（インターフェイス統計情報が削除されるか、またはデバイスがリロードされるまで）の水準点はあまり正確ではありません。 |
| Traffic Statistics: | 受信、送信、またはドロップしたパケットの数。 |
| Packets input | 受信したパケットの数とバイトの数。 |
| Packets output | 送信したパケットの数とバイトの数。 |
| Packets dropped | ドロップしたパケットの数。このカウンタは通常、高速セキュリティパス（ASP）上でドロップしたパケットについて増分します（たとえば、アクセス リスト拒否が原因でパケットをドロップした場合など）。<br>インターフェイス上でドロップが発生する原因については、**show asp drop** コマンドを参照してください。 |
| 1 minute input rate | 過去1分間に受信したパケットの数（パケット/秒およびバイト/秒）。 |
| 1 minute output rate | 過去1分間に送信したパケットの数（パケット/秒およびバイト/秒）。 |
| 1 minute drop rate | 過去 1 分間にドロップしたパケットの数（パケット/秒）。 |
| 5 minute input rate | 過去5分間に受信したパケットの数（パケット/秒およびバイト/秒）。 |
| 5 minute output rate | 過去5分間に送信したパケットの数（パケット/秒およびバイト/秒）。 |
| 5 minute drop rate | 過去 5 分間にドロップしたパケットの数（パケット/秒）。 |

| フィールド | 説明 |
|---|---|
| Redundancy Information: | 冗長インターフェイスについて、メンバー物理インターフェイスを示します。アクティブ インターフェイスの場合はインターフェイス ID の後に「(Active)」と表示されます。<br>メンバーをまだ割り当てていない場合、次の出力が表示されます。<br>`Members unassigned` |
| Last switchover | 冗長インターフェイスの場合、アクティブ インターフェイスがスタンバイ インターフェイスにフェールオーバーした時刻を表示します。 |

（注） **show interface detail** コマンドの結果に示されている入力レートと出力レートが、Management Center ユーザーインターフェイスのインターフェイスモジュールに表示される入出力のトラフィックレートとは異なる場合があります。

このインターフェイスモジュールは、Snort パフォーマンスモニタリングからの値に従ってトラフィックレートを表示します。Snort パフォーマンスモニタリングとインターフェイス統計のサンプリング間隔は異なります。このサンプリング間隔の違いにより、Management Center ユーザーインターフェイスと **show interface detail** コマンドの結果のスループット値が異なります。

次に、**show interface detail** コマンドの出力例を示します。次に、すべてのインターフェイス（プラットフォームに存在する場合は内部インターフェイスを含む）についての詳細なインターフェイス統計情報および非対称ルーティング統計情報（有効にされている場合）を表示する例を示します。

```
> show interface detail
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 000b.fcf8.c44e, MTU 1500
        IP address 10.86.194.60, subnet mask 255.255.254.0
        1330214 packets input, 124580214 bytes, 0 no buffer
        Received 1216917 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        9 L2 decode drops
        124863 packets output, 86956597 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max packets): hardware (0/7)
        output queue (curr/max packets): hardware (0/13)
  Traffic Statistics for "outside":
        1330201 packets input, 99995120 bytes
        124863 packets output, 84651382 bytes
        525233 packets dropped
  Control Point Interface States:
        Interface number is 1
        Interface config status is active
        Interface state is active
```

```
Interface Internal-Data0/0 "", is up, line protocol is up
  Hardware is i82547GI rev00, BW 1000 Mbps, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        MAC address 0000.0001.0002, MTU not set
        IP address unassigned
        6 packets input, 1094 bytes, 0 no buffer
        Received 6 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops, 0 demux drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max packets): hardware (0/2) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
   Control Point Interface States:
        Interface number is unassigned
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
 (Full-duplex), (1000 Mbps)
 Input flow control is unsupported, output flow control is unsupported
 MAC address 0000.0100.0001, MTU 1500
 IP address 169.254.1.1, subnet mask 255.255.255.248
 37 packets input, 2822 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 pause input, 0 resume input
 0 L2 decode drops
 5 packets output, 370 bytes, 0 underruns
 0 pause output, 0 resume output
 0 output errors, 0 collisions, 0 interface resets
 0 late collisions, 0 deferred
 0 input reset drops, 0 output reset drops
 input queue (blocks free curr/low): hardware (0/0)
 output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
 37 packets input, 2304 bytes
 5 packets output, 300 bytes
 37 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
 Interface number is 14
 Interface config status is active
 Interface state is active
[...]
```

次の表で、**show interface detail** コマンドによって表示される追加フィールドについて説明します。

***表 37 : show interface detail* の各フィールド**

| フィールド | 説明 |
|---|---|
| Demux drops | （内部データインターフェイスのみ）他のインターフェイスからのパケットを 脅威に対する防御 デバイスで逆多重化できなかったためドロップしたパケットの数。 |

| フィールド | 説明 |
|---|---|
| Control Point Interface States: | |
| Interface number | デバッグに使用される0から始まる番号で、このインターフェイスが作成された順番を示します。 |
| Interface config status | 管理ステートは次のとおりです。<br>• active：インターフェイスはシャット ダウンされていません。<br>• not active：インターフェイスは意図的にシャットダウンされています。 |
| インターフェイスの状態 | インターフェイスの実際の状態。この状態は通常、上記の config status と一致します。高可用性を設定した場合、脅威に対する防御 デバイスは必要に応じてインターフェイスを動作状態またはダウン状態にするため、不一致が生じる可能性があります。 |
| Asymmetrical Routing Statistics: | |
| Received X1 packets | このインターフェイスで受信した ASR パケットの数。 |
| Transmitted X2 packets | このインターフェイスで送信した ASR パケットの数。 |
| Dropped X3 packets | このインターフェイスでドロップした ASR パケットの数。パケットは、パケットを転送しようとしたときにインターフェイスがダウン状態の場合にドロップされることがあります。 |

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear interface** | **show interface** コマンドのカウンタをクリアします。 |
| **show interface ip brief** | インターフェイスの IP アドレスとステータスを表示します。 |

# show interface ip brief

インターフェイスの IP アドレスとステータスを表示するには、**show interface ip brief** コマンドを使用します。

**show interface** [ [*physical_interface*[**.***subinterface*] | *interface_name* | **BVI** *id* | ] **ip brief**

## 構文の説明

| | |
|---|---|
| **BVI** *id* | （任意）指定されたブリッジ仮想インターフェイス（BVI）の統計情報を表示します。BVI 番号（1 ー 250）を入力します。 |
| *interface_name* | （任意）インターフェイス名を指定します。 |
| *physical_interface* | （任意）インターフェイス ID（**gigabitethernet0/1** など）を指定します。 |
| サブインターフェイス | （任意）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。 |

## コマンド デフォルト

インターフェイスを指定しない場合、内部インターフェイスを含むすべてのインターフェイスが表示されます。

## 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。 |
| 6.2 | **BVI** キーワードが追加されました。 |

### 例

次に、**show ip brief** コマンドの出力例を示します。

```
> show interface ip brief
    Interface                  IP-Address      OK? Method  Status                Protocol

    Control0/0                  127.0.1.1       YES CONFIG  up                      up
    GigabitEthernet0/0          209.165.200.226 YES CONFIG  up                      up
    GigabitEthernet0/1          unassigned      YES unset   administratively down down
    GigabitEthernet0/2          10.1.1.50       YES manual  administratively down down
    GigabitEthernet0/3          192.168.2.6     YES DHCP    administratively down down
    Management0/0               209.165.201.3   YES CONFIG  up
```

次の例は、ほとんどのインターフェイスが BVI の一部である場合のアドレスを表示しています。メンバーインターフェイスには、親 BVI と同じアドレスが設定されています。

```
> show interface ip brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet1/1         unassigned      YES DHCP   down                  down
```

```
GigabitEthernet1/2         192.168.1.1     YES unset  down                  down
GigabitEthernet1/3         192.168.1.1     YES unset  down                  down
GigabitEthernet1/4         192.168.1.1     YES unset  down                  down
GigabitEthernet1/5         192.168.1.1     YES unset  down                  down
GigabitEthernet1/6         192.168.1.1     YES unset  down                  down
GigabitEthernet1/7         192.168.1.1     YES unset  down                  down
GigabitEthernet1/8         192.168.1.1     YES unset  down                  down
Internal-Control1/1        127.0.1.1       YES unset  up                    up
Internal-Data1/1           unassigned      YES unset  up                    up
Internal-Data1/2           unassigned      YES unset  down                  down
Internal-Data1/3           unassigned      YES unset  up                    up
Internal-Data1/4           169.254.1.1     YES unset  up                    up
Management1/1              unassigned      YES unset  up                    up
BVI1                       192.168.1.1     YES manual up                    up
```

次の表では、出力フィールドについて説明されています。

**表 *38 : show interface ip brief* の各フィールド**

| フィールド | 説明 |
|---|---|
| インターフェイス（Interface） | インターフェイス ID。<br>すべてのインターフェイスを表示すると、システム通信に使用される内部インターフェイスに関する情報も表示されます。内部インターフェイスをユーザーが設定することはできません。情報はデバッグのみを目的としています。 |
| IP-Address | インターフェイスの IP アドレス。 |
| OK? | この列は使用されておらず、常に「Yes」と表示されます。 |
| Method | インターフェイスが IP アドレスを受信した方法。値は次のとおりです。<br>• unset：IP アドレスは設定されていません。<br>• manual：インターフェイスには静的アドレスが設定されています。<br>• CONFIG：スタートアップ コンフィギュレーションからロードしました。<br>• DHCP：DHCP サーバーから受信しました。 |
| Status | 管理ステートは次のとおりです。<br>• up：インターフェイスはシャットダウンされません。<br>• down：インターフェイスは起動しておらず、意図的にシャットダウンもされていません。<br>• administratively down：インターフェイスは意図的にシャットダウンされています。 |

| フィールド | 説明 |
| --- | --- |
| Protocol | 回線ステータスは次のとおりです。<br>• up：動作するケーブルがネットワーク インターフェイスに接続されています。<br>• down：ケーブルが正しくないか、インターフェイス コネクタに接続されていません。 |

## 関連コマンド

| Command | 説明 |
| --- | --- |
| **show interface** | インターフェイスの実行時ステータスと統計情報を表示します。 |

# show inventory

製品 ID（PID）、バージョン ID（VID）、およびシリアル番号（SN）が割り当てられているネットワークデバイスにインストールされているすべてのシスコ製品に関する情報を表示するには、**show inventory** コマンドを使用します。

**show inventory** ［*slot_id*］

## 構文の説明

| | |
|---|---|
| *slot_id* | （オプション）モジュール ID またはスロット番号（0 ～ 3）を指定します。 |

## コマンド デフォルト

項目のインベントリを表示するスロットを指定しない場合は、すべてのモジュール（電源モジュールを含む）のインベントリ情報が表示されます。

## 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

**show inventory** コマンドは、各シスコ製品に関するンベントリ情報を UDI 形式で取得および表示します。UDI形式とは、製品ID（PID）、バージョンID（VID）、およびシリアル番号（SN）という 3 つの異なるデータ要素の組み合わせです。

PIDは製品を発注するための名前で、従来は「製品名」または「部品番号」と呼ばれていました。これは、正しい交換部品を発注するために使用する ID です。

VIDは製品のバージョンです。製品が変更されると、VIDは、製品の変更通知を管理する業界ガイドラインである Telcordia GR-209-CORE から定めた厳格なプロセスに従って増分されます。

SN はベンダー固有の製品の通し番号です。それぞれの製品には工場で割り当てた独自のシリアル番号があり、現場では変更できません。シリアル番号は、製品の個々の固有のインスタンスを識別するための手段です。シリアル番号は、デバイスのさまざまなコンポーネントに応じてその長さが異なる場合があります。

UDI では各製品をエンティティと呼びます。シャーシなどの一部のエンティティには、スロットのようなサブエンティティがあります。各エンティティは、シスコエンティティごとに階層的に配置された論理的な表示順で別々の行に表示されます。

オプションを指定せずに **show inventory** コマンドを使用すると、ネットワーキングデバイスに取り付けられており、PID が割り当てられているシスコエンティティのリストが表示されます。

シスコ エンティティに PID が割り当てられていない場合、そのエンティティは取得または表示されません。

ASA 5500-X シリーズのハードウェア上の制限により、シリアル番号が表示されない場合があります。これらのモデルの PCI-E I/O（NIC）オプション カードの UDI 表示では、カード タイ

プは 2 つのみですが、出力はシャーシタイプに応じて 6 通りになります。これは、指定されたシャーシに応じて異なる PCI-E ブラケット アセンブリが使用されるためです。次に、各 PCI-E I/O カード アセンブリについて予想される出力を示します。たとえば、Silicom SFP NIC カードが検出された場合、UDI 表示はこのカードが取り付けられているデバイスによって決定されます。VID および S/N の値は N/A です。これは、これらの値が電子的に格納されていないためです。

ASA 5512-X または 5515-X 内の 6 ポート SFP イーサネット NIC カードの場合：

```
Name: "module1", DESCR: "ASA 5512-X/5515-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-A    , VID: N/A, SN: N/A
```

ASA 5525-X 内の 6 ポート SFP イーサネット NIC カードの場合：

```
Name: "module1", DESCR: "ASA 5525-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-B    , VID: N/A, SN: N/A
```

ASA 5545-X または 5555-X 内の 6 ポート SFP イーサネット NIC カードの場合：

```
Name: "module1", DESCR: "ASA 5545-X/5555-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-C    , VID: N/A, SN: N/A
```

ASA 5512-X または 5515-X 内の 6 ポート銅線イーサネット NIC カードの場合：

```
Name: "module1", DESCR: "ASA 5512-X/5515-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-A    , VID: N/A, SN: N/A
```

ASA 5525-X 内の 6 ポート銅線イーサネット NIC カードの場合：

```
Name: "module1", DESCR: "ASA 5525-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-B    , VID: N/A, SN: N/A
```

ASA 5545-X または 5555-X 内の 6 ポート銅線イーサネット NIC カードの場合：

```
Name: "module1", DESCR: "ASA 5545-X/5555-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-C    , VID: N/A, SN: N/A
```

### 例

次に、キーワードや引数を指定していない **show inventory** コマンドの出力例を示します。この出力例には、それぞれに PID が割り当てられている 脅威に対する防御 デバイスに取り付けられているシスコ エンティティのリストが表示されます。

```
> show inventory
Name: "Chassis", DESCR: "ASA 5508-X with FirePOWER services, 8GE, AC, DES"
PID: ASA5508           , VID: V01     , SN: JMX1923408S

Name: "Storage Device 1", DESCR: "ASA 5508-X SSD"
```

```
PID: ASA5508-SSD       , VID: N/A     , SN: MXA184205MC
```

次の表で、この出力で表示されるフィールドについて説明します。

**表 *39 : show inventory* のフィールドの説明**

| フィールド | 説明 |
|---|---|
| 名前 | シスコ エンティティに割り当てられた物理名（テキスト ストリング）。たとえば、コンソール、SSP、または「1」などの簡易コンポーネント番号（ポートまたはモジュールの番号）など、デバイスの物理コンポーネント命名構文に応じて異なります。RFC 2737 の entPhysicalName MIB 変数に相当します。 |
| DESCR | オブジェクトを特徴付けるシスコ エンティティの物理的な説明。RFC 2737 の entPhysicalDesc MIB 変数に相当します。 |
| PID | エンティティ製品 ID。RFC 2737 の entPhysicalModelName MIB 変数に相当します。 |
| VID | エンティティのバージョン番号。RFC 2737 の entPhysicalHardwareRev MIB 変数に相当します。 |
| SN | エンティティのシリアル番号。RFC 2737 の entPhysicalSerialNum MIB 変数に相当します。 |

# show ip address

インターフェイス IP アドレス（トランスペアレントモードの場合は管理 IP アドレス）を表示するには、**show ip address** コマンドを使用します。

**show ip address** [[*physical_interface*[**.***subinterface*] | *interface_name* | ]

## 構文の説明

| | |
|---|---|
| *interface_name* | （任意）インターフェイス名を指定します。 |
| *physical_interface* | （任意）**gigabit**ethernet0/1 などのインターフェイス ID を指定します。 |
| サブインターフェイス | （任意）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。 |

## コマンド デフォルト

インターフェイスを指定しない場合、出力にはすべてのインターフェイス IP アドレスが表示されます。

## 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

このコマンドは、ハイ アベイラビリティを設定するときのためのプライマリ IP アドレス（表示では「System」と記載される）と現在の IP アドレスを表示します。ユニットがアクティブの場合、システム IP アドレスと現在の IP アドレスは一致します。ユニットがスタンバイの場合、現在の IP アドレスにはスタンバイ アドレスが表示されます。

IP アドレスはデータインターフェイス専用です。このコマンドは、診断インターフェイス上の管理インターフェイスのシステムの IP アドレスは表示しません（トランスペアレントモードの管理インターフェイスとは異なります）。情報には、診断インターフェイスの IP アドレス情報（設定されている場合）が含まれます。管理インターフェイスに関する情報を表示するには、**show network** コマンドを使用します。

### 例

次に、**show ip address** コマンドの出力例を示します。

```
> show ip address
System IP Addresses:
Interface               Name         IP address      Subnet mask       Method
GigabitEthernet0/0      mgmt         10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1      inside       10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40   outside      209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3      dmz          209.165.200.225 255.255.255.224   manual
Current IP Addresses:
Interface               Name         IP address      Subnet mask       Method
GigabitEthernet0/0      mgmt         10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1      inside       10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40   outside      209.165.201.2   255.255.255.224   DHCP
```

```
GigabitEthernet0/3       dmz            209.165.200.225 255.255.255.224   manual
```

次の表で各フィールドについて説明します。

**表 *40 : show ip address* の各フィールド**

| フィールド | 説明 |
|---|---|
| インターフェイス（Interface） | インターフェイス ID。 |
| 名前 | インターフェイス名。 |
| IP address | インターフェイスの IP アドレス。 |
| サブネット マスク | IP アドレスのサブネット マスク。 |
| Method | インターフェイスが IP アドレスを受信した方法。値は次のとおりです。<br>• unset：IP アドレスは設定されていません。<br>• manual：インターフェイスには静的アドレスが設定されています。<br>• CONFIG：スタートアップ コンフィギュレーションからロードしました。<br>• DHCP：DHCP サーバーから受信しました。 |

## 関連コマンド

| Command | 説明 |
|---|---|
| **show interface** | インターフェイスの実行時ステータスと統計情報を表示します。 |
| **show interface ip brief** | インターフェイスの IP アドレスとステータスを表示します。 |

# show ip address dhcp

インターフェイスに対する DHCP リースまたはサーバーに関する詳細情報を表示するには、**show ip address dhcp** コマンドを使用します。

**show ip address** {*physical_interface*[**.***subinterface*] | *interface_name*} **dhcp server**
**show ip address** {*physical_interface*[**.***subinterface*] | *interface_name*} **dhcp lease** [**proxy** | **server**] [**summary**]

## 構文の説明

| | |
|---|---|
| *interface_name* | インターフェイス名を指定します。 |
| **lease** | DHCP リースに関する情報を表示します。 |
| *physical_interface* | インターフェイス ID（**gigabitethernet0/1** など）を指定します。 |
| **proxy** | IPL テーブル内のプロキシ エントリを表示します。 |
| **server** | IPL テーブル内のサーバー エントリを表示します。 |
| サブインターフェイス | 論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。 |
| **summary** | エントリの要約を表示します。 |

## 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、**show ip address dhcp lease** コマンドの出力例を示します。

```
> show ip address outside dhcp lease
Temp IP Addr:209.165.201.57 for peer on interface:outside
Temp sub net mask:255.255.255.224
   DHCP Lease server:209.165.200.225, state:3 Bound
   DHCP Transaction id:0x4123
   Lease:259200 secs, Renewal:129600 secs, Rebind:226800 secs
   Temp default-gateway addr:209.165.201.1
   Temp ip static route0: dest 10.9.0.0 router 10.7.12.255
   Next timer fires after:111797 secs
   Retry count:0, Client-ID:cisco-0000.0000.0000-outside
   Proxy: TRUE  Proxy Network: 10.1.1.1
   Hostname: device1
```

次の表で各フィールドについて説明します。

表 *41 : show ip address dhcp lease* の各フィールド

| フィールド | 説明 |
|---|---|
| Temp IP Addr | インターフェイスに割り当てられている IP アドレス。 |
| Temp sub net mask | インターフェイスに割り当てられているサブネット マスク。 |
| DHCP Lease server | DHCP サーバー アドレス。 |
| state | DHCP リースの状態で、次のとおりです。<br>• [Initial]：初期化状態で、デバイスがリースを取得するプロセスを開始します。この状態は、リースが終了したか、リースのネゴシエーションに失敗したときにも表示されます。<br>• [Selecting]：デバイスは 1 つ以上の DHCP サーバーから DHCPOFFER メッセージを受信するために待機しているため、メッセージを選択できます。<br>• [Requesting]：デバイスは、要求を送信した送信先サーバーからの応答を待機しています。<br>• [Purging]：クライアントが IP アドレスを解放したか、他のエラーが発生したため、デバイスはリースを削除しています。<br>• [Bound]：デバイスは有効なリースを保持し、正常に動作しています。<br>• [Renewing]：デバイスはリースを更新しようとしています。DHCPREQUEST メッセージを現在の DHCP サーバーに定期的に送信し、応答を待機します。<br>• [Rebinding]：デバイスは元のサーバーのリースの更新に失敗したため、いずれかのサーバーから応答を受け取るか、リースが終了するまで DHCPREQUEST メッセージを送信します。<br>• [Holddown]：デバイスはリースを削除するプロセスを開始しました。<br>• [Releasing]：デバイスは IP アドレスが不要になったことを示すリリースメッセージをサーバーに送信します。 |
| DHCP transaction id | クライアントによって選択され、要求メッセージを関連付けるためにクライアントとサーバーによって使用される乱数。 |
| Lease | DHCP サーバーによって指定される、インターフェイスがこの IP アドレスを使用できる時間の長さ。 |
| Renewal | インターフェイスがこのリースを自動的に更新しようとするまでの時間の長さ。 |

| フィールド | 説明 |
|---|---|
| Rebind | 脅威に対する防御 デバイスが DHCP サーバーに再バインドしようとするまでの時間の長さ。再バインドが発生するのは、デバイスが元の DHCP サーバーと通信できず、リース期間の 87.5% を経過した場合です。デバイスは、DHCP 要求をブロードキャストすることで、使用可能な任意の DHCP サーバーに接続を試みます。 |
| Temp default-gateway addr | DHCP サーバーによって指定されるデフォルト ゲートウェイ アドレス。 |
| Temp ip static route0 | デフォルト スタティック ルート。 |
| Next timer fires after | 内部タイマーがトリガーするまでの秒数。 |
| リトライ回数 | 脅威に対する防御 デバイスがリースを確立しようとしているとき、このフィールドは、そのデバイスが DHCP メッセージの送信を試行した回数を示します。たとえば、デバイスが Selecting 状態の場合、この値はデバイスが探索メッセージを送信した回数を示します。デバイスが Requesting 状態の場合、この値はデバイスが要求メッセージを送信した回数を示します。 |
| Client-ID | サーバーとのすべての通信に使用したクライアント ID。 |
| Proxy | このインターフェイスが VPN クライアント用のプロキシ DHCP クライアントかどうかを True または False で指定します。 |
| Proxy Network | 要求されたネットワーク。 |
| Hostname | クライアントのホスト名。 |

次に、**show ip address dhcp server** コマンドの出力例を示します。

```
> show ip address outside dhcp server
   DHCP server: ANY (255.255.255.255)
    Leases:   0
    Offers:   0      Requests: 0     Acks: 0     Naks: 0
    Declines: 0      Releases: 0     Bad:  0

   DHCP server: 40.7.12.6
    Leases:   1
    Offers:   1      Requests: 17     Acks: 17     Naks: 0
    Declines: 0      Releases: 0     Bad:  0
    DNS0:   171.69.161.23,   DNS1:  171.69.161.24
    WINS0:  172.69.161.23,   WINS1: 172.69.161.23
    Subnet: 255.255.0.0   DNS Domain: cisco.com
```

次の表で各フィールドについて説明します。

表 *42 : show ip address dhcp server* の各フィールド

| フィールド | 説明 |
|---|---|
| DHCP サーバー | このインターフェイスがリースを取得した DHCP サーバー アドレス。最上位エントリ（「ANY」）はデフォルト サーバーで常に存在します。 |
| Leases | サーバーから取得したリースの数。インターフェイスの場合、リースの数は一般的に 1 です。VPN 用のプロキシを実行中のインターフェイスに対してサーバーがアドレスを提供している場合、リースは複数となります。 |
| Offers | サーバーからのオファーの数。 |
| Requests | サーバーに送信された要求の数。 |
| Acks | サーバーから受信した確認応答の数。 |
| Naks | サーバーから受信した否定応答の数。 |
| Declines | サーバーから受信した拒否の数。 |
| リリース | サーバーに送信されたリリースの数。 |
| Bad | サーバーから受信した不良パケットの数。 |
| DNS0 | DHCP サーバーから取得したプライマリ DNS サーバー アドレス。 |
| DNS1 | DHCP サーバーから取得したセカンダリ DNS サーバー アドレス。 |
| WINS0 | DHCP サーバーから取得したプライマリ WINS サーバー アドレス。 |
| WINS1 | DHCP サーバーから取得したセカンダリ WINS サーバー アドレス。 |
| Subnet | DHCP サーバーから取得したサブネット アドレス。 |
| DNS ドメイン | DHCP サーバーから取得したドメイン。 |

## 関連コマンド

| Command | 説明 |
|---|---|
| **show interface ip brief** | インターフェイスの IP アドレスとステータスを表示します。 |
| **show ip address** | インターフェイスの IP アドレスを表示します。 |

# show ip address pppoe

PPPoE 接続に関する詳細情報を表示するには、**show ip address pppoe** コマンドを使用します。

**show ip address** {*physical_interface*[**.***subinterface*] | *interface_name* | } **pppoe**

## 構文の説明

| | |
|---|---|
| *interface_name* | インターフェイス名を指定します。 |
| *physical_interface* | インターフェイス ID（**gigabitethernet0/1** など）を指定します。 |
| サブインターフェイス | 論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。 |

## 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。 |

## 関連コマンド

| Command | 説明 |
|---|---|
| **show interface ip brief** | インターフェイスの IP アドレスとステータスを表示します。 |
| **show ip address** | インターフェイスの IP アドレスを表示します。 |

# show ip audit count

監査ポリシーをインターフェイスに適用するときシグニチャの一致数を表示するには、**show ip audit count** コマンドを使用します。

**show ip audit count** ［**global** | **interface** *interface_name*］

## 構文の説明

| | |
|---|---|
| **global** | （デフォルト）すべてのインターフェイスについての一致数を表示します。 |
| **interface** *interface_name* | （任意）指定したインターフェイスについての一致数を表示します。 |

## 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

監査ポリシーは通常は設定しませんが、FlexConfig を使用して設定すると、関連する統計情報を表示できます。

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear ip audit count** | IP 監査の統計情報をクリアします。 |
| **show running-config ip audit name** | **ip audit name** コマンドの設定を表示します。**name** に加えて、**interface** と **signature** の設定を確認できます。 |

# show ip local pool

IPv4 アドレスプール情報を表示するには、**show ip local pool** コマンドを使用します。

**show ip local pool** *pool_name*

## 構文の説明

| | |
|---|---|
| *pool_name* | IPv6 アドレスプールの名前。 |

## 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

このコマンドを使用して、IPv4 アドレスプールの内容を表示します。これらのプールは、リモートアクセス VPN およびクラスタリングで使用されます。**show ipv6 local pool** を使用して、IPv6 アドレスプールを表示します。

### 例

次に、**show ip local pool** コマンドの出力例を示します。

```
> show ip local pool test-ipv4-pool
Begin           End             Mask            Free     Held     In use
10.100.10.10    10.100.10.254   255.255.255.0     245        0        0

Available Addresses:
10.100.10.10
10.100.10.11
10.100.10.12
10.100.10.13
10.100.10.14
10.100.10.15
10.100.10.16
... (remaining output redacted)...
```

# show ip verify statistics

ユニキャスト リバース パス フォワーディング（RPF）機能のためにドロップされたパケットの数を表示するには、**show ip verify statistics** コマンドを使用します。

**show ip verify statistics** ［**interface** *interface_name*］

## 構文の説明

| | |
|---|---|
| **interface** *interface_name* | （任意）指定したインターフェイスの統計情報を表示します。 |

## コマンド デフォルト

このコマンドは、すべてのインターフェイスの統計情報を表示します。

## 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

**ip verify reverse-path** 機能は通常は設定しませんが、FlexConfig を使用して設定すると、関連する統計情報を表示できます。

### 例

次に、**show ip verify statistics** コマンドの出力例を示します。

```
> show ip verify statistics
interface outside: 2 unicast rpf drops
interface inside: 1 unicast rpf drops
interface intf2: 3 unicast rpf drops
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear ip verify statistics** | ユニキャスト RPF の統計情報をクリアします。 |
| **show running-config ip verify reverse-path** | **ip verify reverse-path** の設定を表示します。 |

# show ipsec df-bit

指定されたインターフェイスの IPsec パケットの IPsec do-not-fragment（DF ビット）ポリシーを表示するには、**show ipsec df-bit** コマンドを使用します。同じ意味を持つ **show crypto ipsec df-bit** コマンドも使用できます。

**show ipsec df-bit** *interface*

## 構文の説明

| | |
|---|---|
| *interface* | インターフェイス名を指定します。 |

## 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

d f ビットの設定によって、カプセル化されたヘッダーの do-not-fragment（DF）ビットのシステムによる処理方法が決まります。IP ヘッダー内の DF ビットにより、デバイスがパケットをフラグメント化できるかどうかが決定されます。この設定に基づき、システムは暗号の適用時に外側の IPsec ヘッダーに対するクリアテキストパケットの DF ビットの設定をクリアするか、設定するか、コピーするかのいずれかを実行します。

### 例

次に、inside というインターフェイスの IPsec DF ビット ポリシーを表示する例を示します。

```
> show ipsec df-bit inside
df-bit inside copy
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipsec fragmentation** | IPsec パケットのフラグメンテーション ポリシーを表示します。 |

# show ipsec fragmentation

IPsec パケットのフラグメンテーション ポリシーを表示するには、**show ipsec fragmentation** コマンドを使用します。同じ意味を持つ **show crypto ipsec fragmentation** コマンドも使用できます。

**show ipsec fragmentation** *interface*

## 構文の説明

| | |
|---|---|
| *interface* | インターフェイス名を指定します。 |

## 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

VPNに対するパケットを暗号化する際、システムはパケット長をアウトバウンドインターフェイスの MTU と比較します。パケットの暗号化が MTU を超える場合は、パケットをフラグメント化する必要があります。このコマンドは、パケットを暗号化した後（after-encryption）、または暗号化する前（before-encryption）にシステムがパケットをフラグメント化するかどうかを表示します。暗号化前のパケットのフラグメント化は、事前フラグメント化とも呼ばれ、暗号化パフォーマンス全体を向上させるため、システムのデフォルト動作になっています。

### 例

次に、inside というインターフェイスの IPsec フラグメンテーション ポリシーを表示する例を示します。

```
> show ipsec fragmentation inside
fragmentation inside before-encryption
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipsec df-bit** | 指定したインターフェイスの DF ビット ポリシーを表示します。 |

# show ipsec policy

OSPFv3 に設定されている IPsec セキュアソケット API（SS API）セキュリティポリシーを表示するには、**show ipsec policy** コマンドを使用します。このコマンドの代替形式である **show crypto ipsec policy** を使用することもできます。

**show ipsec policy**

## 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、OSPFv3 認証と暗号方式ポリシーを表示する例を示します。

```
> show ipsec policy
Crypto IPsec client security policy data

Policy name:      OSPFv3-1-256
Policy refcount:  1
Policy flags:     0x00000000
SA handles:       sess 268382208 (0xfff3000) / in 55017 (0xd6e9) / out 90369 (0x16101)
Inbound  ESP SPI:         256 (0x100)
Outbound ESP SPI:         256 (0x100)
Inbound  ESP Auth Key:   12345678901234567890123456789012345678901234567890
Outbound ESP Auth Key:   12345678901234567890123456789012345678901234567890
Inbound  ESP Cipher Key: 123456789012345678901234567890123456789012
Outbound ESP Cipher Key: 123456789012345678901234567890123456789012
Transform set:    esp-aes esp-sha-hmac
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show crypto sockets** | セキュアなソケット情報を表示します。 |
| **show ipv6 ospf interface** | OSPFv3 インターフェイスに関する情報を表示します。 |

# show ipsec sa

IPSec セキュリティ アソシエーション（SA）のリストを表示するには、**show ipsec sa** コマンドを使用します。このコマンドの代替形式である **show crypto ipsec sa** を使用することもできます。

**show ipsec sa** ［**assigned-address** *hostname_or_IP_address* | **entry** | **identity** | **inactive** | **map** *map-name* | **peer** *peer-addr* | **spi** *spi-num*］［**detail**］

## 構文の説明

| | |
|---|---|
| **assigned-address** *hostname_or_IP_address* | （オプション）指定されたホスト名または IP アドレスの IPsec SA を表示します。 |
| **detail** | （任意）表示されているものに対する詳細なエラー情報を表示します。 |
| **entry** | （オプション）IPsec SA をピア アドレスの順に表示します。 |
| **identity** | （オプション）IPsec SA を ID の順に表示します。ESP は含まれません。これは簡略化された形式です。 |
| **inactive** | （オプション）トラフィックを渡すことができない IPsec SA を表示します。 |
| **map** *map-name* | （オプション）指定されたクリプトマップの IPsec SA を表示します。 |
| **peer** *peer-addr* | （オプション）指定されたピア IP アドレスの IPsec SA を表示します。 |
| **spi** *spi-num* | （オプション）SPI の IPsec SA を表示します。 |

## 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、IPsec SA を表示する例を示します。この表示には、割り当てられた IPv6 アドレス、およびトランスポートモードと GRE カプセル化が含まれます。

```
> show ipsec sa
interface: outside
    Crypto map tag: def, seq num: 1, local addr: 75.2.1.23

      local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
      remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
      current_peer: 75.2.1.60, username: rashmi
      dynamic allocated peer ip: 65.2.1.100
      dynamic allocated peer ip(ipv6): 2001:1000::10
```

```
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 18, #pkts decrypt: 18, #pkts verify: 18
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
  #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #TFC rcvd: 0, #TFC sent: 0
  #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
  #send errors: 0, #recv errors: 4

 local crypto endpt.: 75.2.1.23/4500, remote crypto endpt.: 75.2.1.60/64251
  path mtu 1342, ipsec overhead 62(44), override mtu 1280, media mtu 1500
  PMTU time remaining (sec): 0, DF policy: copy-df
  ICMP error validation: disabled, TFC packets: disabled
  current outbound spi: D9C00FC2
  current inbound spi : 4FCB6624

inbound esp sas:
  spi: 0x4FCB6624 (1338730020)
     transform: esp-3des esp-sha-hmac no compression
     in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
     slot: 0, conn_id: 8192, crypto-map: def
     sa timing: remaining key lifetime (sec): 28387
     IV size: 8 bytes
     replay detection support: Y
     Anti replay bitmap:
      0x0003FFFF 0xFFFFFFFF
outbound esp sas:
  spi: 0xD9C00FC2 (3653242818)
     transform: esp-3des esp-sha-hmac no compression
     in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
     slot: 0, conn_id: 8192, crypto-map: def
     sa timing: remaining key lifetime (sec): 28387
     IV size: 8 bytes
    replay detection support: Y
     Anti replay bitmap:
      0x00000000 0x00000001
```

次に、IPsec SA を表示する例を示します。この表示には使用中の設定が含められ、トンネルが OSPFv3 として示されます。

```
> show ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
      #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
```

```
inbound esp sas:
  spi: 0x1E8246FC (511854332)
     transform: esp-3des esp-md5-hmac
     in use settings ={L2L, Transport, Manual key (OSPFv3),}
     slot: 0, conn_id: 3, crypto-map: def
     sa timing: remaining key lifetime (sec): 548
     IV size: 8 bytes
     replay detection support: Y
outbound esp sas:
  spi: 0xDC15BF68 (3692412776)
     transform: esp-3des esp-md5-hmac
     in use settings ={L2L, Transport, Manual key (OSPFv3), }
     slot: 0, conn_id: 3, crypto-map: def
     sa timing: remaining key lifetime (sec): 548
     IV size: 8 bytes
     replay detection support: Y

Crypto map tag: def, local addr: 10.132.0.17

  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

（注） IPSec SA ポリシーに、フラグメンテーションは IPsec 処理の前に発生すると明記されている場合、フラグメンテーション統計情報は、フラグメンテーション前の統計情報です。SA ポリシーに、フラグメンテーションは IPsec 処理の後に発生すると明記されている場合、フラグメンテーション後の統計情報が表示されます。

次に、グローバル コンフィギュレーション モードで、def という名前のクリプト マップの IPsec SA を表示する例を示します。

```
> show ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
```

```
        replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
```

次に、キーワード **entry** に関する IPsec SA の例を示します。

```
> show ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
```

```
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
```

次に、キーワード **entry detail** を使用した IPsec SA の例を示します。

```
> show ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17
```

```
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

```
    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
>
```

次に、キーワード **identity** を使用した IPsec SA の例を示します。

```
> show ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

次に、キーワード **identity** および **detail** を使用した IPsec SA の例を示します。

```
> show ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
      #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

次の例では、IPv6 で割り当てられたアドレスに基づいて IPSec SA を表示しています。

```
> show ipsec sa assigned-address 2001:1000::10
assigned address: 2001:1000::10
    Crypto map tag: def, seq num: 1, local addr: 75.2.1.23

      local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
      remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
      current_peer: 75.2.1.60, username: rashmi
      dynamic allocated peer ip: 65.2.1.100
      dynamic allocated peer ip(ipv6): 2001:1000::10
```

```
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 326, #pkts decrypt: 326, #pkts verify: 326
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
  #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #TFC rcvd: 0, #TFC sent: 0
  #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
  #send errors: 0, #recv errors: 35

  local crypto endpt.: 75.2.1.23/4500, remote crypto endpt.: 75.2.1.60/64251
  path mtu 1342, ipsec overhead 62(44), override mtu 1280, media mtu 1500
  PMTU time remaining (sec): 0, DF policy: copy-df
  ICMP error validation: disabled, TFC packets: disabled
  current outbound spi: D9C00FC2
  current inbound spi : 4FCB6624

inbound esp sas:
  spi: 0x4FCB6624 (1338730020)
     transform: esp-3des esp-sha-hmac no compression
     in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
     slot: 0, conn_id: 8192, crypto-map: def
     sa timing: remaining key lifetime (sec): 28108
     IV size: 8 bytes
     replay detection support: Y
     Anti replay bitmap:
      0xFFFFFFFF 0xFFFFFFFF
outbound esp sas:
  spi: 0xD9C00FC2 (3653242818)
     transform: esp-3des esp-sha-hmac no compression
     in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
     slot: 0, conn_id: 8192, crypto-map: def
     sa timing: remaining key lifetime (sec): 28108
     IV size: 8 bytes
     replay detection support: Y
     Anti replay bitmap:
      0x00000000 0x00000001
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear isakmp sa** | IKE ランタイム SA データベースをクリアします。 |
| **show running-config isakmp** | アクティブなISAKMP コンフィギュレーションをすべて表示します。 |

# show ipsec sa summary

IPsec SA の要約を表示するには、**show ipsec sa summary** コマンドを使用します。

**show ipsec sa summary**

## 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、次の接続タイプ別に IPsec SA の要約を表示する例を示します。

- IPSec
- IPSec over UDP
- IPSec over NAT-T
- IPSec over TCP
- IPSec VPN ロード バランシング

```
> show ipsec sa summary
Current IPsec SA's:           Peak IPsec SA's:
IPsec            :     2        Peak Concurrent SA  :    14
IPsec over UDP   :     2        Peak Concurrent L2L :     0
IPsec over NAT-T :     4        Peak Concurrent RA  :    14
IPsec over TCP   :     6
IPsec VPN LB     :     0
Total            :    14
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear ipsec sa** | IPsec SA を完全に削除するか、特定のパラメータに基づいて削除します。 |
| **show ipsec sa** | IPsec SA のリストを表示します。 |
| **show ipsec stats** | IPsec 統計情報のリストを表示します。 |

# show ipsec stats

IPSec 統計情報のリストを表示するには、**show ipsec stats** コマンドを使用します。

**show ipsec stats**

## 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

次に、出力エントリが示す内容について説明した表を示します。

| 出力（続き） | 説明（続き） |
|---|---|
| IPsec Global Statistics | このセクションは、脅威に対する防御 デバイスがサポートする IPsec トンネルの総数に関連しています。 |
| Active tunnels | 現在接続されている IPsec トンネルの数。 |
| Previous tunnels | 接続されたことがある IPsec トンネルの数（アクティブなトンネルを含む）。 |
| 着信 | このセクションは、IPsec トンネルを介して受信した着信暗号トラフィックに関係します。 |
| Bytes | 受信した暗号トラフィックのバイト数。 |
| Decompressed bytes | 圧縮解除が実行された後に受信された暗号トラフィックのバイト数（該当する場合）。圧縮がイネーブルでない場合、このカウンタは常に上記のカウンタと等しくなるはずです。 |
| Packets | 受信された IPsec 暗号化パケットの数。 |
| Dropped packets | 受信されたがエラーのためドロップされた IPsec 暗号化パケットの数。 |
| Replay failures | 受信された IPsec 暗号化パケットについて検出されたアンチリプレイの失敗数。 |
| Authentications | 受信された IPsec 暗号化パケットについて実行された認証の成功数。 |
| Authentication failures | 受信された IPsec 暗号化パケットについて検出された認証の失敗数。 |
| Decryptions | 受信された IPsec 暗号化パケットについて実行された復号化の成功数。 |

| 出力（続き） | 説明（続き） |
|---|---|
| Decryption failures | 受信されたIPsec暗号化パケットについて検出された復号の失敗数。 |
| Decapsulated fragments needing reassembly | 再構築が必要な IP フラグメントを含む復号 IPSec パケットの数。 |
| 発信 | このセクションは、IPsec トラフィックを介して送信される発信クリアテキスト トラフィックに関係します。 |
| Bytes | IPsec トンネルを介して暗号化および送信されるクリアテキスト トラフィックのバイト数。 |
| Uncompressed bytes | IPsec トンネルを介して暗号化および送信される圧縮解除されたクリアテキスト トラフィックのバイト数。圧縮がイネーブルでない場合、このカウンタは常に上記のカウンタと等しくなるはずです。 |
| Packets | IPsec トンネルを介して暗号化および送信されるクリアテキスト パケットの数。 |
| Dropped packets | IPsecトンネルを介して暗号化および送信されるが、エラーが原因でドロップされたクリアテキスト パケットの数。 |
| Authentications | IPsec トンネルを介して送信されるパケットについて実行された認証の成功数。 |
| Authentication failures | IPsec トンネルを介して送信されるパケットについて検出された認証の失敗数。 |
| Encryptions | IPsec トンネルを介して送信されるパケットについて実行された暗号化の成功数。 |
| Encryption failures | IPsec トンネルを介して送信されるパケットについて検出された暗号化の失敗数。 |
| Fragmentation successes | 発信IPsecパケットの変換の一部として実行されたフラグメンテーション操作の成功数。 |
| Pre-fragmentation successes | 発信IPsecパケット変換の一部として実行された、成功した事前フラグメンテーション操作の数。事前フラグメンテーションは、クリアテキスト パケットが暗号化され、1 つ以上の IPsec パケットとしてカプセル化される前に行われます。 |

| 出力（続き） | 説明（続き） |
|---|---|
| Post-fragmentation successes | 発信 IPsec パケット変換の一部として実行された、成功した事前フラグメンテーション操作の数。事後フラグメンテーションは、クリアテキスト パケットが暗号化され、IPsec パケットとしてカプセル化されることによって複数の IP フラグメントが作成される前に行われます。これらのフラグメントは、復号化前に再構築する必要があります。 |
| Fragmentation failures | 発信 IPsec パケットの変換中に発生したフラグメンテーションの失敗数。 |
| Pre-fragmentation failures | 発信 IPsec パケットの変換中に発生したプリフラグメンテーションの失敗数。事前フラグメンテーションは、クリアテキスト パケットが暗号化され、1 つ以上の IPsec パケットとしてカプセル化される前に行われます。 |
| Post-fragmentation failure | 発信 IPsec パケットの変換中に発生したポストフラグメンテーションの失敗数。事後フラグメンテーションは、クリアテキストパケットが暗号化され、IPsec パケットとしてカプセル化されることによって複数の IP フラグメントが作成される前に行われます。これらのフラグメントは、復号化前に再構築する必要があります。 |
| Fragments created | IPsec の変換の一部として作成されたフラグメントの数。 |
| PMTUs sent | IPsec システムによって送信されたパス MTU メッセージの数。IPsec は、暗号化後に、IPsec トンネルを介して送信するには大きすぎるパケットを送信している内部ホストに対して PMTU メッセージを送信します。PMTU メッセージは、ホストの MTU を低くして、IPsec トンネルを介して送信するパケットのサイズを小さくすることをホストに求めるメッセージです。 |
| PMTUs recvd | IPsec システムによって受信されたパス MTU メッセージの数。IPsec は、トンネルを介して送信するパケットが大きすぎてネットワーク要素を通過できない場合、ダウンストリームのネットワーク要素からパス MTU メッセージを受信します。パス MTU メッセージを受信すると、IPsec は通常、トンネル MTU を低くします。 |
| Protocol failures | 受信した不正な形式の IPsec パケットの数。 |
| Missing SA failures | 指定された IPsec セキュリティ アソシエーションが存在しない、要求された IPsec の動作の数。 |

| 出力（続き） | 説明（続き） |
|---|---|
| System capacity failures | IPsec システムの容量が十分でないためデータ レートをサポートできないことが原因で完了できない IPsec の動作の数。 |

### 例

次の例をグローバル コンフィギュレーション モードで入力すると、IPSec 統計情報が表示されます。

```
> show ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
    Encryption failures: 0
    Fragmentation successes: 3
        Pre-fragmentation successes:2
        Post-fragmentation successes: 1
    Fragmentation failures: 2
        Pre-fragmentation failures:1
        Post-fragmentation failures: 1
    Fragments created: 10
    PMTUs sent: 1
    PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
```

IPsec フローオフロードをサポートするプラットフォームでは、出力にはオフロードフローのカウンタが表示され、通常のカウンタにはオフロードフローと非オフロードフローの合計が表示されます。

```
> show ipsec stats

IPsec Global Statistics
```

```
-----------------------
Active tunnels: 1
Previous tunnels: 1
Inbound
    Bytes: 93568
    Decompressed bytes: 0
    Packets: 86
    Dropped packets: 0
    Replay failures: 0
    Authentications: 0
    Authentication failures: 0
    Decryptions: 86
    Decryption failures: 0
    TFC Packets: 0
    Decapsulated fragments needing reassembly: 0
    Valid ICMP Errors rcvd: 0
    Invalid ICMP Errors rcvd: 0
Outbound
    Bytes: 93568
    Uncompressed bytes: 90472
    Packets: 86
    Dropped packets: 0
    Authentications: 0
    Authentication failures: 0
    Encryptions: 86
    Encryption failures: 0
    TFC Packets: 0
    Fragmentation successes: 0
        Pre-fragmentation successes: 0
        Post-fragmentation successes: 0
    Fragmentation failures: 0
        Pre-fragmentation failures: 0
        Post-fragmentation failures: 0
    Fragments created: 0
    PMTUs sent: 0
    PMTUs rcvd: 0
Offloaded Inbound
    Bytes: 93568
    Packets: 86
    Authentications: 0
    Decryptions: 86
Offloaded Outbound
    Bytes: 93568
    Packets: 86
    Authentications: 0
    Encryptions: 86
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
Inbound SA delete requests: 0
Outbound SA delete requests: 0
Inbound SA destroy calls: 0
Outbound SA destroy calls: 0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear ipsec sa** | 指定されたパラメータに基づいて、IPsec SA またはカウンタをクリアします。 |
| **show ipsec sa** | 指定されたパラメータに基づいて IPsec SA を表示します。 |

| Command | 説明 |
| --- | --- |
| **show ipsec sa summary** | IPsec SA の要約を表示します。 |

# show ipv6 access-list

このコマンドは、脅威に対する防御 ではサポートされていない機能用です。IPv6 アクセス制御は、標準アクセス コントロール ポリシーに統合されています。マネージャでポリシーを表示するか、次のコマンドを使用します。

- **show access-list**
- **show access-control-config**

# show ipv6 dhcp

DHCPv6 情報を表示するには、**show ipv6 dhcp** コマンドを使用します。

**show ipv6 dhcp** ［**client** ［**pd**］ **statistics** ｜ **interface** ［*interface_name* ［**statistics**］］ ｜ **ha statistics** ｜ **server statistics** ｜ **pool** ［*pool_name*］］

## 構文の説明

| | |
|---|---|
| **client** ［**pd**］ **statistics** | DHCPv6 クライアント統計情報を表示し、送受信されたメッセージ数の出力を表示します。DHCPv6 プレフィックス委任クライアントの統計情報を表示するには、**pd** キーワードを追加します。 |
| **interface** ［*interface_name* ［**statistics**］］ | すべてのインターフェイスの DHCPv6 情報、または必要に応じて、指定したインターフェイスの DHCPv6 情報を表示します。インターフェイスが DHCPv6 ステートレスサーバー構成用に設定されている場合、このコマンドは、サーバーによって使用されている DHCPv6 プールをリストします。インターフェイスに DHCPv6 アドレス クライアントまたはプレフィックス委任クライアントの設定がある場合、このコマンドは各クライアントの状態とサーバーから受信した値を表示します。<br>インターフェイス名を指定すると、指定したインターフェイスの DHCP サーバーまたはクライアントのメッセージ統計情報を表示するために **statistics** を追加できます。 |
| **ha statistics** | DUID 情報がフェールオーバーユニット間で同期された回数を含め、フェールオーバー ユニット間のトランザクションの統計情報を表示します。 |
| **server statistics** | DHCPv6 ステートレス サーバーの統計情報を表示します。 |
| **pool** ［*pool_name*］ | すべての DHCPv6 プール、または必要に応じて、指定したプールを表示します。 |

## 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

引数を指定しない場合、このコマンドは、DHCPv6 クライアントまたはサーバーによって使用されているデバイス DUID を表示します。

### 例

次に、**show ipv6 dhcp** コマンドの出力例を示します。

```
> show ipv6 dhcp
```

```
This device's DHCPv6 unique identifier(DUID): 00030001377E8FD91020
```

次に、**show ipv6 dhcp pool** コマンドの出力例を示します。

```
> show ipv6 dhcp pool
DHCPv6 pool: Sample-Pool
  Imported DNS server: 2004:abcd:abcd:abcd::2
  Imported DNS server: 2004:abcd:abcd:abcd::4
  Imported Domain name: relay.com
  Imported Domain name: server.com
  SIP server address: 2001::abcd:1
  SIP server domain name: sip.xyz.com
```

次に、**show ipv6 dhcp interface** コマンドの出力例を示します。

```
> show ipv6 dhcp interface
GigabitEthernet1/1 is in server mode
  Using pool: Sample-Pool

GigabitEthernet1/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:03:46
  Address State is OPEN
  Renew for address will be sent in 00:03:47
  List of known servers:
    Reachable via address: fe80::20c:29ff:fe96:1bf4
    DUID: 000100011D9D1712005056A07E06
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00030001, T1 250, T2 400
        Prefix: 2005:abcd:ab03::/48
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      IA NA: IA ID 0x00030001, T1 250, T2 400
        Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      DNS server: 2004:abcd:abcd:abcd::2
      DNS server: 2004:abcd:abcd:abcd::4
      Domain name: relay.com
      Domain name: server.com
      Information refresh time: 0
  Prefix name: Sample-PD

Management1/1 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 11:26:44
  List of known servers:
    Reachable via address: fe80::4e00:82ff:fe6f:f6f9
    DUID: 000300014C00826FF6F8
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x000a0001, T1 43200, T2 69120
        Address: 2308:2308:210:1812:2504:1234:abcd:8e5a/128
                preferred lifetime INFINITY, valid lifetime INFINITY
      Information refresh time: 0
```

次に、**show ipv6 dhcp interface outside** コマンドの出力例を示します。

```
> show ipv6 dhcp interface outside
GigabitEthernet1/2 is in client mode


 Prefix State is OPEN
 Renew will be sent in 00:02:05
 Address State is OPEN
 Renew for address will be sent in 00:02:06
 List of known servers:
   Reachable via address: fe80::20c:29ff:fe96:1bf4
   DUID: 000100011D9D1712005056A07E06
   Preference: 0
   Configuration parameters:
     IA PD: IA ID 0x00030001, T1 250, T2 400
       Prefix: 2005:abcd:ab03::/48
               preferred lifetime 500, valid lifetime 600
               expires at Nov 26 2014 03:11 PM (476 seconds)
     IA NA: IA ID 0x00030001, T1 250, T2 400
       Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
               preferred lifetime 500, valid lifetime 600
               expires at Nov 26 2014 03:11 PM (476 seconds)
     DNS server: 2004:abcd:abcd:abcd::2
     DNS server: 2004:abcd:abcd:abcd::4
     Domain name: relay.com
     Domain name: server.com
     Information refresh time: 0
 Prefix name: Sample-PD
```

次に、**show ipv6 dhcp interface outside statistics** コマンドの出力例を示します。

```
> show ipv6 dhcp interface outside statistics
DHCPV6 Client PD statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0

DHCPV6 Client address statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
```

```
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                1
 Number of Message Validation errors in received messages: 0
```

次に、**show ipv6 dhcp client statistics** コマンドの出力例を示します。

```
> show ipv6 dhcp client statistics

Protocol Exchange Statistics:
  Total number of Solicit messages sent:              4
  Total number of Advertise messages received:        4
  Total number of Request messages sent:              4
  Total number of Renew messages sent:                92
  Total number of Rebind messages sent:               0
  Total number of Reply messages received:            96
  Total number of Release messages sent:              6
  Total number of Reconfigure messages received:      0
  Total number of Information-request messages sent:  0

Error and Failure Statistics:
  Total number of Re-transmission messages sent:                  8
  Total number of Message Validation errors in received messages: 0
```

次に、**show ipv6 dhcp client pd statistics** コマンドの出力例を示します。

```
> show ipv6 dhcp client pd statistics

Protocol Exchange Statistics:


 Total number of Solicit messages sent:              1
 Total number of Advertise messages received:        1
 Total number of Request messages sent:              1
 Total number of Renew messages sent:                92
 Total number of Rebind messages sent:               0
 Total number of Reply messages received:            93
 Total number of Release messages sent:              0
 Total number of Reconfigure messages received:      0
 Total number of Information-request messages sent:  0

Error and Failure Statistics:


 Total number of Re-transmission messages sent:                  1
 Total number of Message Validation errors in received messages: 0
```

次に、**show ipv6 dhcp server statistics** コマンドの出力例を示します。

```
> show ipv6 dhcp server statistics

Protocol Exchange Statistics:
```

```
  Total number of Solicit messages received:             0
  Total number of Advertise messages sent:               0
  Total number of Request messages received:             0
  Total number of Renew messages received:               0
  Total number of Rebind messages received:              0
  Total number of Reply messages sent:                  10
  Total number of Release messages received:             0
  Total number of Reconfigure messages sent:             0
  Total number of Information-request messages received: 10
  Total number of Relay-Forward messages received:       0
  Total number of Relay-Reply messages sent:             0

Error and Failure Statistics:
  Total number of Re-transmission messages sent:                  0
  Total number of Message Validation errors in received messages: 0
```

次に、**show ipv6 dhcp ha statistics** コマンドの出力例を示します。

```
> show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              1
  DUID sync messages received:          0

DHCPv6 HA error statistics:
  Send errors:                          0
```

次に、スタンバイユニットでの **show ipv6 dhcp ha statistics** コマンドの出力例を示します。

```
> show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              0
  DUID sync messages received:          1

DHCPv6 HA error statistics:
  Send errors:                          0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear ipv6 dhcp** | DHCPv6 統計情報をクリアします。 |

# show ipv6 dhcprelay binding

リレーエージェントによって作成されたリレーバインディングエントリを表示するには、**show ipv6 dhcprelay binding** コマンドを使用します。

**show ipv6 dhcprelay binding**

## 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、**show ipv6 dhcprelay binding** コマンドの出力例を示します。

```
> show ipv6 dhcprelay binding
1 in use, 2 most used

Client: fe80::204:23ff:febb:b094 (inside)
  DUID: 000100010f9a59d1000423bbb094, Timeout in 60 seconds

Above binding is created for client with link local address of fe80::204:23ff:febb:b094
 on
the inside interface using DHCPv6 id of 000100010f9a59d1000423bbb094, and will timeout
in
60 seconds.

There will be limit of 1000 bindings for each context.
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipv6 dhcprelay statistics** | IPv6 DHCP リレー エージェントの情報を表示します。 |

# show ipv6 dhcprelay statistics

IPv6 DHCP リレーエージェントの統計情報を表示するには、**show ipv6 dhcprelay statistics** コマンドを使用します。

**show ipv6 dhcprelay statistics**

## 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、**show ipv6 dhcprelay statistics** コマンドの出力例を示します。

```
> show ipv6 dhcprelay statistics
Relay Messages:
  SOLICIT                                   1
  ADVERTISE                                 2
  REQUEST                                   1
  CONFIRM                                   1
  RENEW                                   496
  REBIND                                    0
  REPLY                                   498
  RELEASE                                   0
  DECLINE                                   0
  RECONFIGURE                               0
  INFORMATION-REQUEST                       0
  RELAY-FORWARD                           499
  RELAY-REPLY                             500

Relay Errors:
  Malformed message:                        0
  Block allocation/duplication failures:    0
  Hop count limit exceeded:                 0
  Forward binding creation failures:        0
  Reply binding lookup failures:            0
  No output route:                          0
  Conflict relay server route:              0
  Failed to add server NP rule:             0
  Unit or context is not active:            0

Total Relay Bindings Created:             498
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipv6 dhcprelay binding** | リレー エージェントによって作成されたリレー バインディング エントリを表示します。 |

# show ipv6 general-prefix

IPv6 の汎用プレフィックスを表示するには、**show ipv6 general-prefix** コマンドを使用します。

**show ipv6 general-prefix**

## 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

**show ipv6 general-prefix** コマンドを使用して、IPv6 汎用プレフィックスに関する情報を表示します。

### 例

次に、**show ipv6 general-prefix** コマンドの出力例を示します。

```
> show ipv6 general-prefix
IPv6 Prefix my-prefix, acquired via 6to4
2002:B0B:B0B::/48
 Loopback42 (Address command)
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default       N - Not advertised, C - Calendar

AD      fec0:0:0:a::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```

# show ipv6 icmp

すべてのインターフェイス上に設定されている ICMPv6 アクセス ルールを表示するには、**show ipv6 icmp** コマンドを使用します。

**show ipv6 icmp**

## 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

ICMPv6 のルールは、デバイス インターフェイスへの ICMPv6 トラフィックを制御します。これらは、through-the-box トラフィックを制御しません。これらのルールを使用して、ICMPv6 コマンド（ping など）をインターフェイスに送信できるアドレスや、送信できる ICMPv6 コマンドのタイプを制御します。これらのルールを表示するには、**show ipv6 icmp** コマンドを使用します。

### 例

次に、**show ipv6 icmp** コマンドの出力例を示します。

```
> show ipv6 icmp
ipv6 icmp permit any inside
```

# show ipv6 interface

IPv6 用に設定されたインターフェイスのステータスを表示するには、**show ipv6 interface** コマンドを使用します。

**show ipv6 interface** ［**brief**］［*if_name* ［**prefix**］］

## 構文の説明

| | |
|---|---|
| **brief** | 各インターフェイスの IPv6 ステータスおよびコンフィギュレーションの要約を表示します。 |
| *if_name* | （任意）内部または外部のインターフェイス名。指定されたインターフェイスのステータスおよびコンフィギュレーションのみが表示されます。<br>すべてのインターフェイスを表示すると、システム通信に使用される内部インターフェイスに関する情報も表示されます。内部インターフェイスをユーザーが設定することはできません。情報はデバッグのみを目的としています。 |
| **prefix** | （任意）ローカルの IPv6 プレフィックス プールから生成されるプレフィックス。プレフィックスは、IPv6 アドレスのネットワーク部分です。 |

## コマンド デフォルト

すべての IPv6 インターフェイスを表示します。

## 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

**show ipv6 interface** コマンドは、IPv6 固有である点を除き、**show interface** コマンドと同様の出力を提供します。インターフェイスのハードウェアが使用できる場合、インターフェイスはupとマークされます。インターフェイスが双方向通信を提供できる場合、回線プロトコルは upとマークされます。

インターフェイス名が指定されていない場合は、すべての IPv6 インターフェイスの情報が表示されます。インターフェイス名を指定すると、指定されたインターフェイスに関する情報が表示されます。

### 例

次に、**show ipv6 interface** コマンドの出力例を示します。

```
> show ipv6 interface outside
interface ethernet0 “outside” is up, line protocol is up
  IPv6 is enabled, link-local address is 2001:0DB8::/29 [TENTATIVE]
  Global unicast address(es):
```

```
    2000::2, subnet is 2000::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF11:6770
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
```

次に、**brief** キーワードを使用して入力した場合の **show ipv6 interface** コマンドの出力例を示します。

```
> show ipv6 interface brief
outside [up/up]
    unassigned
inside [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::a:0:0:a0a:a70
vlan101 [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::65:0:0:a0a:6570
dmz-ca [up/up]
    unassigned
```

次に、**show ipv6 interface** コマンドの出力例を示します。アドレスからプレフィックスを生成したインターフェイスの特性が表示されています。

```
> show ipv6 interface inside prefix
IPv6 Prefix Advertisements inside
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default       N - Not advertised, C - Calendar

AD      fec0:0:0:a::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```

# show ipv6 local pool

IPv6 アドレスプール情報を表示するには、**show ipv6 local pool** コマンドを使用します。

**show ipv6 local pool** *pool_name*

## 構文の説明

| | |
|---|---|
| *pool_name* | IPv6 アドレスプールの名前。 |

## 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

IPv6アドレスプールの内容を表示するには、このコマンドを使用します。これらのプールは、リモートアクセス VPN およびクラスタリングで使用されます。IPv4 アドレスプールを表示するには、**show ip local pool** を使用します。

### 例

次に、**show ipv6 local pool** コマンドの出力例を示します。

```
> show ipv6 local pool test-ipv6-pool
IPv6 Pool test-ipv6-pool
Begin Address: 2001:db8::db8:800:200c:417a
End Address: 2001:db8::db8:800:200c:4188
Prefix Length: 64
Pool Size: 15
Number of used addresses: 0
Number of available addresses: 15

Available Addresses:
2001:db8::db8:800:200c:417a
2001:db8::db8:800:200c:417b
2001:db8::db8:800:200c:417c
2001:db8::db8:800:200c:417d
2001:db8::db8:800:200c:417e
2001:db8::db8:800:200c:417f
2001:db8::db8:800:200c:4180
2001:db8::db8:800:200c:4181
2001:db8::db8:800:200c:4182
2001:db8::db8:800:200c:4183
2001:db8::db8:800:200c:4184
2001:db8::db8:800:200c:4185
2001:db8::db8:800:200c:4186
2001:db8::db8:800:200c:4187
2001:db8::db8:800:200c:4188
```

# show ipv6 mld traffic

マルチキャストリスナー検出（MLD）トラフィックカウンタ情報を表示するには、**show ipv6 mld traffic** コマンドを使用します。

**show ipv6 mld traffic**

## 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

**show ipv6 mld traffic** コマンドを使用すると、予期される数の MLD メッセージが受信および送信されたかどうかをチェックできます。**show ipv6 mld traffic** コマンドによって次の情報が提供されます。

- Elapsed time since counters cleared：カウンタがクリアされてからの経過時間。
- Valid MLD Packets：送受信された有効な MLD パケットの数。
- Queries：送受信された有効なクエリーの数。
- Reports：送受信された有効なレポートの数。
- Leaves：送受信された有効な脱退の数。
- Mtrace packets：送受信されたマルチキャスト トレース パケットの数。
- Errors：発生したエラーのタイプと数。

### 例

次に、**show ipv6 mld traffic** コマンドの出力例を示します。

```
> show ipv6 mld traffic
show ipv6 mld traffic
MLD Traffic Counters
Elapsed time since counters cleared: 00:01:19
                    Received          Sent
Valid MLD Packets   1                 3
Queries             1                 0
Reports             0                 3
Leaves              0                 0
Mtrace packets      0                 0
Errors:
Malformed Packets   0
Martian source      0
Non link-local source 0
Hop limit is not equal to 1 0
```

関連コマンド

| Command | 説明 |
| --- | --- |
| **clear ipv6 mld traffic** | すべての MLD トラフィック カウンタをリセットします。 |

# show ipv6 neighbor

IPv6 ネイバー探索キャッシュ情報を表示するには、**show ipv6 neighbor** コマンドを使用します。

**show ipv6 neighbor** ［*if_name* | *address*］

## 構文の説明

| | |
|---|---|
| *address* | （任意）指定された IPv6 アドレスについてのみネイバー探索キャッシュ情報を表示します。 |
| *if_name* | （オプション）指定されたインターフェイス名のキャッシュ情報を表示します。<br>すべてのインターフェイスを表示すると、システム通信に使用される内部インターフェイスに関する情報も表示されます。内部インターフェイスをユーザーが設定することはできません。情報はデバッグのみを目的としています。 |

## 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

**show ipv6 neighbor** コマンドによって次の情報が提供されます。

- IPv6 Address：ネイバーまたはインターフェイスの IPv6 アドレス。
- Age：アドレスが到達可能と確認されてからの経過時間（分単位）。ハイフン（-）はスタティック エントリを示します。
- Link-layer Addr：MAC アドレス。アドレスが不明の場合、ハイフン（-）が表示されます。
- State：ネイバー キャッシュ エントリの状態。

（注） 到達可能性検出は IPv6 ネイバー探索キャッシュのスタティック エントリに適用されないため、INCMP（不完全）状態と REACH（到達可能）状態の記述は、ダイナミック キャッシュ エントリとスタティック キャッシュ エントリで異なります。

次に、IPv6 ネイバー探索キャッシュのダイナミック エントリについて表示される可能性のある状態を示します。

- INCMP：（不完全）エントリに対してアドレス解決を実行中です。ネイバー送信要求メッセージがターゲットの送信要求ノード マルチキャスト アドレスに送信されましたが、対応するネイバー アドバタイズメント メッセージが受信されていません。
- REACH：（到達可能）ネイバーへの転送パスが正常に機能していることを示す肯定確認が、直近の ReachableTime ミリ秒以内に受信されました。REACH 状態になって

いる間は、パケットが送信されるときにデバイスは特別なアクションを実行しません。

- STALE：転送パスが正しく機能していたことを示す確認が最後に受信されてから経過した時間が、ReachableTime ミリ秒を超えています。STALE 状態になっている間は、パケットが送信されるまでデバイスはアクションを実行しません。
- DELAY：転送パスが正しく機能していたことを示す確認が最後に受信されてから経過した時間が、ReachableTime ミリ秒を超えています。パケットは直近の DELAY_FIRST_PROBE_TIME 秒以内に送信されました。DELAY 状態に入ってから、DELAY_FIRST_PROBE_TIME 秒以内に到達可能性確認を受信できない場合は、ネイバー送信要求メッセージが送信され、状態が PROBE に変更されます。
- PROBE：到達可能性確認が受信されるまで、RetransTimer ミリ秒ごとに、ネイバー要請メッセージを再送信することで、到達可能性確認が積極的に求められます。
- ????：不明な状態。

次に、IPv6 ネイバー探索キャッシュのスタティック エントリについて表示される可能性のある状態を示します。

- INCMP：（不完全）このエントリのインターフェイスはダウンしています。
- REACH：（到達可能）このエントリのインターフェイスは動作しています。

- インターフェイス

  アドレスに到達可能であったインターフェイス。

### 例

次に、インターフェイスを指定して入力した **show ipv6 neighbor** コマンドの出力例を示します。

```
> show ipv6 neighbor inside
IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH inside
FE80::203:A0FF:FED6:141E                    0 0003.a0d6.141e  REACH inside
3001:1::45a                                 - 0002.7d1a.9472  REACH inside
```

次に、IPv6 アドレスを指定して入力した **show ipv6 neighbor** コマンドの出力例を示します。

```
> show ipv6 neighbor 2000:0:0:4::2
IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH inside
```

関連コマンド

| Command | 説明 |
| --- | --- |
| **clear ipv6 neighbors** | スタティック エントリを除く、IPv6 ネイバー探索キャッシュ内のすべてのエントリを削除します。 |

# show ipv6 ospf

OSPFv3 ルーティングプロセスに関する一般情報を表示するには、**show ipv6 ospf** コマンドを使用します。

**show ipv6 ospf** ［*process_id*］［*area_id*］

## 構文の説明

| | |
|---|---|
| *area_id* | （オプション）指定したエリアに関する情報だけを表示します。 |
| *process_id* | （オプション）ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPFv3 ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。 |

## 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、**show ipv6 ospf** コマンドの出力例を示します。

```
> show ipv6 ospf
Routing Process “ospfv3 1” with ID 10.9.4.1
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
It is an autonomous system boundary router
Redistributing External Routes from,
   ospf 2
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipv6 ospf border-routers** | エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。 |
| **show ipv6 ospf database** | 特定のルータの OSPFv3 データベースに関係する情報の一覧を表示します。 |

# show ipv6 ospf border-routers

エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部OSPFv3ルーティング テーブル エントリを表示するには、**show ipv6 ospf border-routers** コマンドを使用します。

**show ipv6 ospf** ［*process_id*］ **border-routers**

## 構文の説明

| | |
|---|---|
| *process_id* | （オプション）ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPFv3 ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。 |

## 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

**show ipv6 ospf border-routers** コマンドを使用すると、次の設定が一覧表示されます。

- エリア内ルート
- エリア間ルート
- IPv6 アドレス
- インターフェイス タイプ
- Area ID
- SPF 番号

### 例

次に、**show ipv6 ospf border-routers** コマンドの出力例を示します。

```
> show ipv6 ospf border-routers
OSPFv3 Process 1 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 172.16.4.4 [2] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ABR, Area 1, SPF 13
i 172.16.4.4 [1] via FE80::205:5FFF:FED3:5406, POS4/0, ABR, Area 0, SPF 8
i 172.16.3.3 [1] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ASBR, Area 1, SPF 3
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipv6 ospf** | OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。 |
| **show ipv6 ospf database** | 特定のルータのOSPFv3データベースに関係する情報の一覧を表示します。 |

# show ipv6 ospf database

特定のルータの OSPFv3 データベースに関連した情報リストを表示するには、**show ipv6 ospf database** コマンドを入力します。

**show ipv6 ospf** ［*process_id*］［*area_id*］ **database** ［**external** ｜ **inter-area prefix** ｜ **inter-area-router** ｜ **network** ｜ **nssa-external** ｜ **router** ｜ **area** ｜ **as** ｜ **ref-lsa** ｜ ［*destination-router-id*］［**prefix** *ipv6-prefix*］［*link-state-id*］］［**link** ［**interface** *interface-name*］［**adv-router** *router-id*］ ｜ **self-originate**］［**internal**］［**database-summary**］

## 構文の説明

| | |
|---|---|
| **adv-router** *router-id* | （オプション）アドバタイズするルータのすべての LSA を表示します。ルータ ID は、RFC 2740 に記載された形式にする必要があり、16 ビット値をコロンで区切った 16 進数でアドレスを指定します。 |
| **area** | （オプション）エリア LSA に関する情報だけを表示します。 |
| *area_id* | （オプション）指定したエリアに関する情報だけを表示します。 |
| **as** | （オプション）不明な自律システム（AS）LSA をフィルタリングします。 |
| **database-summary** | （オプション）データベースと全体にある各エリアの各 LSA タイプの数を表示します。 |
| *destination-router-id* | （オプション）指定した宛先ルータに関する情報だけを表示します。 |
| **external** | （任意）外部 LSA の情報だけを表示します。 |
| **interface** | （オプション）インターフェイス コンテキストでフィルタリングされた LSA に関する情報を表示します。 |
| *interface-name* | （オプション）LSA のインターフェイス名を指定します。 |
| **internal** | （オプション）内部 LSA の情報だけを表示します。 |
| **inter-area prefix** | （オプション）エリア間プレフィックスに基づいた LSA の情報だけを表示します。 |
| **inter-area router** | （オプション）エリア間ルータ LSA 基づいた LSA の情報だけを表示します。 |
| **link** | （オプション）リンク LSA に関する情報を表示します。**unknown** キーワードの後に入力した場合、**link** キーワードでリンクスコープ LSA がフィルタ処理されます。 |
| *link-state-id* | （オプション）LSA を区別するために使用する整数を指定します。ネットワーク LSA およびリンク LSA では、リンクステート ID はインターフェイス インデックスに一致します。 |

| | |
|---|---|
| **network** | （オプション）ネットワーク LSA に関する情報を表示します。 |
| **nssa-external** | （オプション）Not-So-Stubby-Area（NSSA）の外部 LSA に関する情報だけを表示します。 |
| **prefix** *ipv6-prefix* | （オプション）ネイバーのリンクローカル IPv6 アドレスを表示します。IPv6 プレフィックスは、RFC 2373 に記載された形式にする必要があり、16 ビット値をコロンで区切った 16 進数でアドレスを指定します。 |
| *process_id* | （オプション）ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。 |
| **ref-lsa** | （オプション）プレフィックス LSA タイプをさらにフィルタリングします。 |
| **router** | （オプション）ルータ LSA に関する情報を表示します。 |
| **self-originate** | （オプション）ローカル ルータから自己生成 LSA だけを表示します。 |

## 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

このコマンドは、さまざまな形式で、異なる OSPFv3 LSA に関する情報を提供します。

### 例

次に、**show ipv6 ospf database** コマンドの出力例を示します。

```
> show ipv6 ospf database

            OSPFv3 Router with ID (172.16.4.4) (Process ID 1)

                Router Link States (Area 0)

ADV Router         Age         Seq#        Fragment ID   Link count  Bits
172.16.4.4         239         0x80000003  0             1           B
172.16.6.6         239         0x80000003  0             1           B

            Inter Area Prefix Link States (Area 0)

ADV Router         Age         Seq#        Prefix
172.16.4.4         249         0x80000001  FEC0:3344::/32
172.16.4.4         219         0x80000001  FEC0:3366::/32
172.16.6.6         247         0x80000001  FEC0:3366::/32
172.16.6.6         193         0x80000001  FEC0:3344::/32
172.16.6.6         82          0x80000001  FEC0::/32

            Inter Area Router Link States (Area 0)
```

```
ADV Router         Age         Seq#        Link ID    Dest RtrID
172.16.4.4         219         0x80000001  50529027   172.16.3.3
172.16.6.6         193         0x80000001  50529027   172.16.3.3

            Link (Type-8) Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Interface
172.16.4.4         242         0x80000002  14         PO4/0
172.16.6.6         252         0x80000002  14         PO4/0

            Intra Area Prefix Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Ref-lstype  Ref-LSID
172.16.4.4         242         0x80000002  0          0x2001      0
172.16.6.6         252         0x80000002  0          0x2001      0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipv6 ospf** | OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。 |
| **show ipv6 ospf border-routers** | エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。 |

# show ipv6 ospf events

OSPFv3 内部イベントの情報を表示するには、**show ipv6 ospf events** コマンドを使用します。

**show ipv6 ospf** ［*process_id*］ **events** ［*type*］

## 構文の説明

| | |
|---|---|
| *process_id* | （オプション）ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。 |
| *type* | （オプション）表示するイベント タイプのリスト。タイプを 1 つ以上指定しないと、すべてのイベントが表示されます。次のタイプでフィルタリングできます。<br>• **generic**：一般的なイベント。<br>• **interface**：インターフェイス状態変化イベント。<br>• **lsa**：LSA 到着イベントおよび LSA 生成イベント。<br>• **neighbor**：ネイバー状態変化イベント。<br>• **reverse**：逆の順序でイベントを表示。<br>• **rib**：ルータ情報ベースの更新イベント、削除イベント、および再配布イベント。<br>• **spf**：SPF のスケジューリングイベントおよびSPF 実行イベント。 |

## 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、**show ipv6 ospf events** コマンドの出力例を示します。

```
> show ipv6 ospf events

OSPFv3 Router with ID (10.1.3.2) (Process ID 10)

   1 Jul 9  18:49:34.071: Timer Exp:  ospfv3_if_ack_delayed  0xda05fad8
   2 Jul 9  18:49:31.571: Rcv Unchanged Type-0x2001 LSA, LSID 0.0.0.0, Adv-Rtr 10.1.1.2,

Seq# 80000008, Age 1, Area 10
   3 Jul 9  18:48:13.241: Generate Changed Type-0x8 LSA, LSID 2.0.0.0, Seq# 80000004,
Age    0, Area 10
   4 Jul 9  18:48:13.241: Generate Changed Type-0x2001 LSA, LSID 0.0.0.0, Seq# 80000005,

Age 0, Area 10
```

```
   5 Jul 9  18:41:18.901: End of SPF, SPF time 0ms, next wait-interval 10000ms
   6 Jul 9  18:41:18.902: Starting External processing in area 10
   7 Jul 9  18:41:18.902: Starting External processing
   8 Jul 9  18:41:18.902: Starting Inter-Area SPF in area 10
   9 Jul 9  18:41:18.902: Generic:  post_spf_intra  0x0
  10 Jul 9  18:41:18.902: RIB Delete (All Paths), Prefix 2002::/64, type Intra
  11 Jul 9  18:41:18.902: RIB Update, Prefix 5005::/64, gw ::, via inside, type Intra
  12 Jul 9  18:41:18.902: Starting Intra-Area SPF in Area 10
  13 Jul 9  18:41:18.903: Starting SPF, wait-interval 5000ms
  14 Jul 9  18:41:16.403: Timer Exp:  ospfv3_if_ack_delayed  0xda05fad8
  15 Jul 9  18:41:13.903: Schedule SPF, Area 10, Change in LSA type PLSID 0.8.0.0,
Adv-Rtr   50.100.168.192
  16 Jul 9  18:41:13.903: Rcv Changed Type-0x2009 LSA, LSID 0.8.0.0, Adv-Rtr 10.1.2.3,

Seq# 80000003, Age 1, Area 10
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipv6 ospf** | OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。 |
| **show ipv6 ospf border-routers** | エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。 |

# show ipv6 ospf flood-list

いずれかのインターフェイスを介したフラッディングを待機している OSPFv3 LSA のリストを表示するには、**show ipv6 ospf flood-list** コマンドを使用します。

**show ipv6 ospf** ［*process_id*］［*area_id*］ **flood-list** *interface-type interface-number*

## 構文の説明

| | |
|---|---|
| *area_id* | （オプション）指定したエリアに関する情報だけを表示します。 |
| *interface-number* | （オプション）LSA がフラッディングされるインターフェイス番号を指定します。 |
| *interface-type* | （オプション）LSA がフラッディングされるインターフェイス タイプを指定します。 |
| *process_id* | （オプション）ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPFv3 ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。 |

## 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

OSPFv3 パケット ペーシング情報を表示するには、このコマンドを使用します。

### 例

次に、**show ipv6 ospf flood-list** コマンドの出力例を示します。

```
> show ipv6 ospf flood-list

OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

 Interface POS4/0, Queue length 1
 Link state retransmission due in 14 msec

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
 0x2001  0               172.16.6.6      0x80000031  0      0x1971

 Interface FastEthernet0/0, Queue length 0

 Interface ATM3/0, Queue length 0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipv6 ospf** | OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。 |

| Command | 説明 |
| --- | --- |
| **show ipv6 ospf border-routers** | エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。 |

# show ipv6 ospf graceful-restart

OSPFv3 グレースフルリスタートに関する情報を表示するには、**show ipv6 ospf graceful-restart** コマンドを使用します。

**show ipv6 ospf graceful-restart**

## 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、**show ipv6 ospf graceful-restart** コマンドの出力例を示します。

```
> show ipv6 ospf graceful-restart
Routing Process "ospfv3 10"
  Graceful Restart enabled
    restart-interval limit: 240 sec
    Clustering is not configured in spanned etherchannel mode
  Graceful Restart helper support enabled
    Number of neighbors performing Graceful Restart is 0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipv6 ospf** | OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。 |

# show ipv6 ospf interface

OSPFv3 関連のインターフェイス情報を表示するには、**show ipv6 ospf interface** コマンドを入力します。

**show ipv6 ospf** ［*process_id*］［*area_id*］ **interface** ［*type-number*］［**brief**］

## 構文の説明

| | |
|---|---|
| *area_id* | （オプション）指定したエリアに関する情報だけを表示します。 |
| **brief** | （オプション）OSPFv3 インターフェイス、状態、アドレスとマスク、およびルータのエリアに関する簡単な概要情報を表示します。 |
| *process_id* | （オプション）ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。 |
| *type-number* | （オプション）インターフェイスのタイプおよび番号を指定します。 |

## 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

OSPFv3 インターフェイス、状態、アドレスとマスク、およびルータのエリアに関する概要情報を表示するには、このコマンドを使用します。

### 例

次に、**show ipv6 ospf interface** コマンドの出力例を示します。

```
> show ipv6 ospf interface
ATM3/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 13
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type POINT_TO_POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.4.4
  Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 3
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 172.16.6.6, local address 2001:0DB1:205:5FFF:FED3:6408
  Backup Designated router (ID) 172.16.3.3, local address 2001:0DB1:205:5FFF:FED3:5808
```

```
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:05
Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 12, maximum is 12
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 172.16.6.6  (Designated Router)
Suppress hello for 0 neighbor(s)
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipv6 ospf** | OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。 |
| **show ipv6 ospf border-routers** | エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。 |

# show ipv6 ospf request-list

ルータが要求したすべての LSA のリストを表示するには、**show ipv6 ospf request-list** コマンドを使用します。

**show ipv6 ospf** ［*process_id*］［*area_id*］ **request-list** ［*neighbor*］［*interface*］［*interface-neighbor*］

## 構文の説明

| | |
|---|---|
| *area_id* | （オプション）指定したエリアに関する情報だけを表示します。 |
| *interface* | （オプション）このインターフェイスからルータにより要求されるすべての LSA のリストを指定します。 |
| *interface-neighbor* | （オプション）このネイバーのインターフェイスのルータにより要求されるすべての LSA のリストを指定します。 |
| *neighbor* | （オプション）このネイバーからルータにより要求されるすべての LSA のリストを指定します。 |
| *process_id* | （オプション）ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。 |

## 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、**show ipv6 ospf request-list** コマンドの出力例を示します。

```
> show ipv6 ospf request-list

           OSPFv3 Router with ID (192.168.255.5) (Process ID 1)

 Neighbor 192.168.255.2, interface Ethernet0/0 address
FE80::A8BB:CCFF:FE00:6600

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
  1      0.0.0.0         192.168.255.3   0x800000C2  1      0x0014C5
  1      0.0.0.0         192.168.255.2   0x800000C8  0      0x000BCA
  1      0.0.0.0         192.168.255.1   0x800000C5  1      0x008CD1
  2      0.0.0.3         192.168.255.3   0x800000A9  774    0x0058C0
  2      0.0.0.2         192.168.255.3   0x800000B7  1      0x003A63
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipv6 ospf** | OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。 |

| Command | 説明 |
| --- | --- |
| **show ipv6 ospf border-routers** | エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。 |

# show ipv6 ospf retransmission-list

再送信待ちになっているすべての LSA のリストを表示するには、**show ipv6 ospf retransmission-list** コマンドを使用します。

**show ipv6 ospf** ［*process_id*］［*area_id*］ **retransmission-list** ［*neighbor*］［*interface*］［*interface-neighbor*］

## 構文の説明

| | |
|---|---|
| *area_id* | （オプション）指定したエリアに関する情報だけを表示します。 |
| *interface* | （オプション）このインターフェイスで再送信を待機しているすべての LSA のリストを指定します。 |
| *interface-neighbor* | （オプション）このネイバーからこのインターフェイスの再送信を待機しているすべての LSA のリストを表示します。 |
| *neighbor* | （オプション）このネイバーの再送信を待機しているすべての LSA のリストを指定します。 |
| *process_id* | （オプション）ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。 |

## 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、**show ipv6 ospf retransmission-list** コマンドの出力例を示します。

```
> show ipv6 ospf retransmission-list

        OSPFv3 Router with ID (192.168.255.2) (Process ID 1)

Neighbor 192.168.255.1, interface Ethernet0/0
Link state retransmission due in 3759 msec, Queue length 1

Type    LS ID           ADV RTR         Seq NO      Age    Checksum
0x2001  0               192.168.255.2   0x80000222  1      0x00AE52
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipv6 ospf** | OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。 |
| **show ipv6 ospf border-routers** | エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。 |

# show ipv6 ospf statistic

さまざまな OSPFv3 統計（SPF が実行された回数、理由、期間など）を表示するには、**show ipv6 ospf statistic** コマンドを使用します。

**show ipv6 ospf** ［*process_id*］ **statistic** ［**detail**］

## 構文の説明

| | |
|---|---|
| **detail** | （オプション）トリガー ポイントを含む詳細な SPF 情報を指定します。 |
| *process_id* | （オプション）ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。 |

## 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、**show ipv6 ospf statistic** コマンドの出力例を示します。

```
> show ipv6 ospf 10 statistic detail
Area 10: SPF algorithm executed 6 times

SPF 1 executed 04:36:56 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
       0      0      0      0      0      0      0 0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
                0            0
  LSIDs processed R:1 N:0 Prefix:0 SN:0 SA:0 X7:0
  Change record R L
  LSAs changed 2
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  49.100.168.192/0(R) 49.100.168.192/2(L)

SPF 2 executed 04:35:50 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
       0      0      0      0      0      0      0 0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
                0            0
  LSIDs processed R:2 N:1 Prefix:0 SN:0 SA:0 X7:0
  Change record R N L
  LSAs changed 5
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  50.100.168.192/0(R) 50.100.168.192/2(L) 49.100.168.192/0(R) 50.100.168.192/0(R)
  50.100.168.192/2(N)
```

# show ipv6 ospf summary-prefix

OSPFv3 プロセスで設定されているサマリーアドレスのすべての再配布情報のリストを表示するには、**show ipv6 ospf summary-prefix** コマンドを使用します。

**show ipv6 ospf** ［*process_id*］ **summary-prefix**

## 構文の説明

| | |
|---|---|
| *process_id* | （オプション）ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。 |

## 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、**show ipv6 ospf summary-prefix** コマンドの出力例を示します。

```
> show ipv6 ospf summary-prefix

OSPFv3 Process 1, Summary-prefix

FEC0::/24 Metric 16777215, Type 0, Tag 0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipv6 ospf** | OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。 |
| **show ipv6 ospf border-routers** | エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。 |

# show ipv6 ospf timers

OSPFv3 タイマー情報を表示するには、**show ipv6 ospf timers** コマンドを使用します。

**show ipv6 ospf** ［*process_id*］ **timers** ［**lsa-group** | **rate-limit**］

## 構文の説明

| | |
|---|---|
| **lsa-group** | （オプション）OSPFv3 LSA グループ情報を指定します。 |
| *process_id* | （オプション）ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。 |
| **rate-limit** | （オプション）OSPFv3 LSA のレート制限情報を指定します。 |

## 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。 |

### 例

次に、**show ipv6 ospf timers lsa-group** コマンドの出力例を示します。

```
> show ipv6 ospf timers lsa-group

OSPFv3 Router with ID (10.10.13.101) (Process ID 1)

Group size 5, Head 2, Search Index 4, Interval 240 sec
Next update due in 0:00:13
Current time 96532
Index 0 Timestamp 96546
Index 1 Timestamp 96788
Index 2 Timestamp 97048
Index 3 Timestamp 97293
Index 4 Timestamp 97548

Failure Head 0, Last 0 LSA group failure logged

            OSPFv3 Router with ID (10.10.10.102) (Process ID 5709)

Group size 5, Head 2, Search Index 4, Interval 240 sec
Next update due in 0:00:22
Current time 96532
Index 0 Timestamp 96555
Index 1 Timestamp 96801
Index 2 Timestamp 97041
Index 3 Timestamp 97287
Index 4 Timestamp 97546

Failure Head 0, Last 0 LSA group failure logged
```

# show ipv6 ospf traffic

現在使用可能なインターフェイスの OSPFv3 トラフィック関連の統計情報を表示するには、**show ipv6 ospf traffic** コマンドを使用します。

**show ipv6 ospf** ［*process_id*］ **traffic** ［*interface_name*］

## 構文の説明

| | |
|---|---|
| **interface_name** | （任意）インターフェイスの名前を指定します。特定のインターフェイスにトラフィックを分離するには、このオプションを使用します。 |
| *process_id* | （オプション）ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。 |

## 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、**show ipv6 ospf traffic** コマンドの出力例を示します。

```
> show ipv6 ospf 10 traffic inside
Interface inside

Last clearing of interface traffic counters never

OSPFv3 packets received/sent
  Type          Packets               Bytes
  RX Invalid                      0 0
  RX Hello                     1232 53132
  RX DB des                      27 896
  RX LS req                       3 216
  RX LS upd                      28 2436
  RX LS ack                      14 1064
  RX Total                     1304 57744

  TX Failed                       0 0
  TX Hello                      753 32072
  TX DB des                      27 1056
  TX LS req                       2 92
  TX LS upd                       9 1128
  TX LS ack                      15 900
  TX Total                      806 35248
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipv6 ospf** | OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。 |

| Command | 説明 |
| --- | --- |
| **show ipv6 ospf border-routers** | エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。 |

# show ipv6 ospf virtual-links

OSPFv3 仮想リンクのパラメータと現在の状態を表示するには、**show ipv6 ospf virtual-links** コマンドを使用します。

**show ipv6 ospf virtual-links**

## 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、**show ipv6 ospf virtual-links** コマンドの出力例を示します。

```
> show ipv6 ospf virtual-links

Virtual Link OSPF_VL0 to router 172.16.6.6 is up
  Interface ID 27, IPv6 address FEC0:6666:6666::
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 2, via interface ATM3/0, Cost of using 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipv6 ospf** | OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。 |
| **show ipv6 ospf border-routers** | エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。 |

# show ipv6 prefix-list

IPv6 トラフィックに一致するように設定されているプレフィックスリストを一覧表示するには、**show ipv6 prefix-list** コマンドを使用します。

**show ipv6 prefix-list** ［**detail** | **summary**］［*prefix_list_name* ［**seq** *sequence_number* | *network/length* ［**longer** | **first-match**］］］

## 構文の説明

| | |
|---|---|
| **detail** | プレフィックスリストに関する詳細を表示します。 |
| **summary** | プレフィックスリストの概要を表示します。 |
| *prefix_list_name* | プレフィックス リストの名前。 |
| **seq** *sequence_number* | （オプション）指定されたプレフィックス リストに指定されたシーケンス番号を持つプレフィックス リストのエントリだけを表示します。 |
| *network/length* [**longer** \| **first-match**] | （オプション）このネットワーク アドレスおよびプレフィックス長（ビット単位）を使用する、指定されたプレフィックス リストのすべてのエントリを表示します。<br>必要に応じて、次のキーワードのいずれかを含めることができます。<br>• **longer** 指定された network/length と一致する、または指定された network/length よりも限定的な、指定されたプレフィックスリストのエントリすべてを表示します。<br>• **first-match** 指定された network/length と一致する、指定されたプレフィックスリストの最初のエントリを表示します。 |

## 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、**show ipv6 prefix-list** コマンドの出力例を示します。

```
> show ipv6 prefix-list
ipv6 prefix-list test-ipv6-prefix: 1 entries
   seq 5 permit 2001:db8:0:cd30::/64
```

次に、要約された出力の例を示します。

```
> show ipv6 prefix-list summary
Prefix-list with the last deletion/insertion: test-ipv6-prefix
```

```
ipv6 prefix-list test-ipv6-prefix:   count: 1, range entries: 0,
sequences: 5 - 5, refcount: 2
```

次に、詳細な出力の例を示します。

```
> show ipv6 prefix-list detail
Prefix-list with the last deletion/insertion: test-ipv6-prefix
ipv6 prefix-list test-ipv6-prefix:   count: 1, range entries: 0,
sequences: 5 - 5, refcount: 2
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear ipv6 prefix-list** | IPv6 プレフィックスリストに対するヒットカウントをリセットします。 |
| **show bgp prefix-list** | ボーダー ゲートウェイ プロトコルのコンテキストに含まれるプレフィックスリストまたはプレフィックスリストのエントリに関する情報を表示します。 |
| **show prefix-list** | IPv4 プレフィックス リストに関する情報を表示します。 |

# show ipv6 route

IPv6 ルーティングテーブルの内容を表示するには、**show ipv6 route** コマンドを使用します。

**show ipv6 route** ［**vrf** *name* ｜ **all**］ ［**management-only**］［**failover**］［**cluster**］［**interface** *name*］［**ospf**］［**summary**］

## 構文の説明

| | |
|---|---|
| **managment-only** | IPv6 管理ルーティング テーブル内のルートを表示します。 |
| **cluster** | （オプション）クラスタ内の IPv6 ルーティング テーブルのシーケンス番号、IPv6 再コンバージェンス タイマーのステータス、および IPv6 ルーティング エントリのシーケンス番号を表示します。 |
| **failover** | （オプション）IPv6 ルーティング テーブルのシーケンス番号、IPv6 再コンバージェンス タイマーのステータス、および IPv6 ルーティング エントリのシーケンス番号を表示します。 |
| **interface** *name* | （オプション）IPv6 インターフェイス固有のルートを表示します。 |
| **ospf** | （オプション）OSPFv3 ルートを表示します。 |
| **summary** | （オプション）IPv6 ルート集約を表示します。 |
| ［**vrf** *name* ｜ **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してビューを特定の仮想ルータに制限できます。すべての仮想ルータのルーティングテーブルを表示するには、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータのルーティングテーブルを表示します。 |

## 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。 |
| 6.6 | ［**vrf** *name* ｜ **all**］ キーワードが追加されました。 |

## 使用上のガイドライン

**show ipv6 route** コマンドの出力は、IPv6 に固有の情報である点を除いて、**show route** コマンドの出力と類似しています。

次に、IPv6 ルーティング テーブルに表示される情報を示します。

- Codes：ルートを生成したプロトコルを示します。表示される値は次のとおりです。
  - C：接続済み
  - L：ローカル
  - S：スタティック

- R：RIP 生成
- B：BGP 生成
- I1：ISIS L1：統合 IS-IS Level 1 生成
- I2：ISIS L2：統合 IS-IS Level 2 生成
- IA：ISIS エリア間：統合 IS-IS エリア間生成

- fe80::/10：リモート ネットワークの IPv6 プレフィックスを示します。
- [0/0]：カッコ内の最初の数値は情報ソースのアドミニストレーティブ ディスタンスです。2 番目の数値はルートのメトリックです。
- via ::：リモート ネットワークへの次のルータのアドレスを指定します。
- inside：指定されたネットワークへの次のルータに到達できるインターフェイスを指定します。

### 例

次に、**show ipv6 route** コマンドの出力例を示します。

```
> show ipv6 route

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
L   fe80::/10 [0/0]
     via ::, inside
     via ::, vlan101
L   fec0::a:0:0:a0a:a70/128 [0/0]
     via ::, inside
C   fec0:0:0:a::/64 [0/0]
     via ::, inside
L   fec0::65:0:0:a0a:6570/128 [0/0]
     via ::, vlan101
C   fec0:0:0:65::/64 [0/0]
     via ::, vlan101
L   ff00::/8 [0/0]
     via ::, inside
     via ::, vlan101
S   ::/0 [0/0]
     via fec0::65:0:0:a0a:6575, vlan101
```

次に、**show ipv6 route failover** コマンドの出力例を示します。

```
> show ipv6 route failover

IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
           ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
```

```
IPv6 Routing table seq num 0
IPv6 Reconvergence timer expired

O   2009::1/128 [110/10]
     via fe80::217:94ff:fe85:4401, inside seq 0
OE2  2011::/64 [110/20]
     via fe80::217:94ff:fe85:4401, inside seq 0
S   4001::1/128 [0/0]
     via 4001::2, inside seq 0
C   7001::1/128 [0/0]
     via ::, outside seq 0
L   fe80::/10 [0/0]
     via ::, inside seq 0
     via ::, outside seq 0
L   ff00::/8 [0/0]
     via ::, inside seq 0
     via ::, outside seq 0
```

プライマリユニットでの **how ipv6 route cluster** コマンドの出力例を次に示します。

```
> show ipv6 route cluster

IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
            ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 2
IPv6 Reconvergence timer expired

OE2  2001::/58 [110/20]
     via fe80::21f:9eff:fe2a:78ba, inside seq 2
...
```

ロール変更時のセカンダリユニットにおける **show ipv6 route cluster** コマンドの出力例を次に示します。

```
> cluster master
INFO: Wait for existing master to quit. Use "show cluster info"
to check status. Use "cluster remove unit <name>" to force
master unit out of the cluster if for some reason it refuses
to quit within reasonable time
> show ipv6 route cluster

IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
            ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 3
IPv6 Reconvergence timer expires in 61 secs

OE2  2001::/58 [110/20]
     via fe80::21f:9eff:fe2a:78ba, inside seq 2
...
```

次に、redという名前の仮想ルータのルートを表示する例を示します。他の仮想ルータにリークされたスタティックルートは、キーSIで示されることに注意してください。

```
> show ipv6 route vrf red
```

```
Codes: C - Connected, L - Local, S - Static, SI - Static InterVRF
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
            ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, B - BGP, V - VPN
            I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary

IPv6 Routing Table : red - 5 entries
L   2301::/128 [0/0]
     via ::, gig0
C   2301::/64 [0/0]
     via ::, gig0
SI  2304::/64 [1/0]
     via ::, gig3
L   fe80::/10 [0/0]
     via ::, gig0
L   ff00::/8 [0/0]
     via ::, gig0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show route** | IPv4 ルーティングテーブルを表示します。 |
| **show vrf** | システムで定義されている仮想ルータを表示します。 |

# show ipv6 routers

オンリンクルータから受信したIPv6ルータアドバタイズメント情報を表示するには、**show ipv6 routers** コマンドを使用します。

**show ipv6 routers** ［*if_name*］

## 構文の説明

| | |
|---|---|
| *if_name* | （任意）情報を表示する対象となる内部インターフェイスまたは外部インターフェイス名。 |

## 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

インターフェイス名が指定されていない場合は、すべての IPv6 インターフェイスの情報が表示されます。インターフェイス名を指定すると、指定されたインターフェイスに関する情報が表示されます。

### 例

次に、インターフェイス名を指定せずに入力した **show ipv6 routers** コマンドの出力例を示します。

```
> show ipv6 routers
Router FE80::83B3:60A4 on outside, last update 3 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
    Valid lifetime -1, preferred lifetime -1
Router FE80::290:27FF:FE8C:B709 on inside, last update 0 min
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **ipv6 route** | IPv6 ルーティング テーブルにスタティック エントリを追加します。 |

# show ipv6 traffic

IPv6 トラフィックに関する統計情報を表示するには、**show ipv6 traffic** コマンドを使用します。

**show ipv6 traffic**

## 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

**clear ipv6 traffic** コマンドを使用して、トラフィックカウンタをクリアします。

### 例

次に、**show ipv6 traffic** コマンドの出力例を示します。

```
> show ipv6 traffic
IPv6 statistics:
  Rcvd:  545 total, 545 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         218 fragments, 109 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  228 generated, 0 forwarded
         1 fragmented into 2 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 168 received, 70 sent

ICMP statistics:
  Rcvd: 116 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 60 router advert, 0 redirects
        31 neighbor solicit, 25 neighbor advert
  Sent: 85 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 18 router advert, 0 redirects
        33 neighbor solicit, 34 neighbor advert

UDP statistics:
  Rcvd: 109 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 37 output

TCP statistics:
```

```
Rcvd: 85 input, 0 checksum errors
Sent: 103 output, 0 retransmitted
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear ipv6 traffic** | IPv6 トラフィック カウンタをクリアします。 |

# show isakmp sa

IKE ランタイム SA データベースを表示するには、**show isakmp sa** コマンドを使用します。

**show isakmp sa** ［**detail**］

## 構文の説明

| | |
|---|---|
| **detail** | SA データベースに関する詳細出力を表示します。 |

## 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、SA データベースに関する詳細情報を表示する例を示します。

```
> show isakmp sa detail

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear isakmp sa** | IKE ランタイム SA データベースをクリアします。 |
| **show running-config isakmp** | アクティブなISAKMPコンフィギュレーションをすべて表示します。 |

# show isakmp stats

ランタイム統計情報を表示するには、**show isakmp stats** コマンドを使用します。

Threat Defense

**show isakmp stats**

## 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

各カウンタは、関連する cikePhase1GW カウンタにマッピングします。これらのカウンタの詳細については、「CISCO-IPSEC-FLOW-MONITOR-MIB.my」を参照してください。

- Active/Standby Tunnels：cikePhase1GWActiveTunnels
- Previous Tunnels：cikePhase1GWPreviousTunnels
- In Octets：cikePhase1GWInOctets
- In Packets：cikePhase1GWInPkts
- In Drop Packets：cikePhase1GWInDropPkts
- In Notifys：cikePhase1GWInNotifys
- In P2 Exchanges：cikePhase1GWInP2Exchgs
- In P2 Exchange Invalids：cikePhase1GWInP2ExchgInvalids
- In P2 Exchange Rejects：cikePhase1GWInP2ExchgRejects
- In P2 Sa Delete Requests：cikePhase1GWInP2SaDelRequests
- Out Octets：cikePhase1GWOutOctets
- Out Packets：cikePhase1GWOutPkts
- Out Drop Packets：cikePhase1GWOutDropPkts
- Out Notifys：cikePhase1GWOutNotifys
- Out P2 Exchanges：cikePhase1GWOutP2Exchgs
- Out P2 Exchange Invalids：cikePhase1GWOutP2ExchgInvalids
- Out P2 Exchange Rejects：cikePhase1GWOutP2ExchgRejects
- Out P2 Sa Delete Requests：cikePhase1GWOutP2SaDelRequests
- Initiator Tunnels：cikePhase1GWInitTunnels
- Initiator Fails：cikePhase1GWInitTunnelFails

- Responder Fails：cikePhase1GWRespTunnelFails
- System Capacity Fails：cikePhase1GWSysCapFails
- Auth Fails：cikePhase1GWAuthFails
- Decrypt Fails：cikePhase1GWDecryptFails
- Hash Valid Fails：cikePhase1GWHashValidFails
- No Sa Fails：cikePhase1GWNoSaFails

### 例

次の例では ISAKMP 統計情報が表示されます。

```
> show isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear isakmp sa** | IKE ランタイム SA データベースをクリアします。 |
| **show running-config isakmp** | アクティブなISAKMP コンフィギュレーションをすべて表示します。 |

# show isis database

IS-IS リンクステートデータベースを表示するには、**show isis database** コマンドを使用します。

**show isis database** ［{**detail** | **verbose**} ［**ip** ［**unicast**］ | **ipv6** ［**unicast**］］ ［**topology base**］］ ［**level-1** | **level-2**］

## 構文の説明

| | |
|---|---|
| **level-1** | （任意）レベル 1 の IS-IS リンクステート データベースを示します。 |
| **level-2** | （任意）レベル 2 の IS-IS リンクステート データベースを示します。 |
| **ip** | （オプション）IPv4 アドレスファミリの IS-IS リンクステート データベースを表示します。 |
| **ipv6** | （オプション）IPv6 アドレスファミリの IS-IS リンクステート データベースを表示します。 |
| **detail** | （任意）各リンクステートパケット（LSP）のコンテンツを表示します。 |
| **verbose** | （オプション）IS-IS データベースに関する追加情報を表示します。 |
| **topology base** | （オプション）MTR トポロジを表示します。 |
| **unicast** | （オプション）ユニキャスト アドレス ファミリを表示します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

## 使用上のガイドライン

次の表では、このコマンドの出力について説明されています。

表 *43 : IS-IS* データベース出力のフィールド

| フィールド | 説明 |
|---|---|
| LSPID | リンクステートパケット（LSP）ID。最初の 6 オクテットは、LSP を生成したルータのシステム ID を形成します。<br>次のオクテットは疑似ノード ID です。このバイトが非ゼロの場合、LSP はシステムからのリンクを記述します。ゼロの場合は、LSP は、いわゆる非疑似ノード LSP です。このメカニズムは、Open Shortest Path First（OSPF）プロトコルのルータ リンクステート アドバタイズメント（LSA）に類似しています。LSP は、送信元ルータの状態を記述します。<br>各 LAN に対して、その LAN の指定ルータは疑似ノード LSP の作成およびフラッドを行い、その LAN に接続されたすべてのシステムを記述します。<br>最後のオクテットは LSP 番号です。単一の LSP に収容可能な量を超えるデータがある場合は、LSP は複数の LSP フラグメントに分割されます。各フラグメントには、異なる LSP 番号が割り当てられます。アスタリスク（*）は、その LSP が、このコマンドの送信元のシステムによって生成されたことを示します。 |
| LSP Seq Num | 他のシステムが発信元から最新情報を受信しているか判断できる、LSP のシーケンス番号。 |
| LSP Checksum | LSP パケットのチェックサム。 |
| LSP Holdtime | LSP が有効である時間（秒単位）。LSP Holdtime がゼロである場合は、LSP がパージされて、すべてのルータのリンクステート データベース（LSDB）から削除されていることを示します。この値は、パージされた LSP が、完全に削除されるまでに LSDB 内に存在する時間を示します。 |
| ATT | Attach ビット。このビットは、そのルータがレベル 2 ルータでもあるため、他のエリアに到達できることを示します。レベル 1 だけのルータ、および他のレベル 2 ルータとの接続を失ったレベル 1-2 ルータは、Attach ビットを使用して最も近いレベル 2 ルータを検出します。ルータは、最も近いレベル 2 ルータへのデフォルト ルートを示します。 |
| P | P ビット。中継システムが修復可能なエリア パーティションであるかどうかを検出します。シスコおよび他のベンダーは、エリア パーティション修復をサポートしません。 |
| OL | 過負荷ビット。IS が混雑しているかどうかを判断します。過負荷ビットがセットされると、他のルータは、ルータを計算しているときに中継ルータとしてこのシステムを使用しません。過負荷になっているルータに直接接続された宛先のパケットだけが、このルータに送信されます。 |

| フィールド | 説明 |
|---|---|
| Area Address<br>（詳細および詳細出力のみ）。 | ルータから到達可能なエリア アドレス。レベル 1 LSP の場合は、送信元ルータ上で手動により設定されるエリア アドレスになります。レベル 2 LSP の場合は、このルータが属するエリアのすべてのエリア アドレスになります。 |
| NLPID<br>（詳細および詳細出力のみ）。 | ネットワーク層プロトコル ID。 |
| Hostname<br>（詳細および詳細出力のみ）。 | ノードのホスト名。 |
| ルータ ID<br>（詳細および詳細出力のみ）。 | ノードのトラフィック エンジニアリング ルータ ID。 |
| IP Address<br>（詳細および詳細出力のみ）。 | インターフェイスの IPv4 アドレス。 |
| メトリック<br>（詳細および詳細出力のみ）。 | 発信元ルータとアドバタイズされるネイバー間の隣接のコストの IS-IS メトリック、またはアドバタイズするルータからアドバタイズされる宛先までにかかるコストのメトリック（IP アドレス、エンド システム（ES）、またはコネクションレス型ネットワーク サービス（CLNS）のプレフィックスを指定できます）。 |
| アフィニティ<br>（詳細出力のみ）。 | フラッドされているリンク属性フラグ。 |
| Physical BW<br>（詳細出力のみ）。 | リンクの帯域幅容量（ビット/秒）。 |
| Reservable BW<br>（詳細出力のみ）。 | このリンクの予約可能帯域幅。 |
| BW Unreserved<br>（詳細出力のみ）。 | 予約可能帯域幅。 |

### 例

次の例は、IS-IS データベースを示しています。

```
> show isis database

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0xea19d300     0x3d0d              674                     0/0/0
routerA.00-00     0x1b541556     0xa349               928                     0/0/0
c3.00-00              0x9257c979     0x9952              759                     0/0/0
c2.00-00             *0xef11e977     0x3188              489                     0/0/0
c2.01-00             *0xa8333f03     0xd6ea              829                     0/0/0
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0x63871f24      0xaba2               526
0/0/0
routerA.00-00     0x0d540b55      0x81d7              472                     0/0/0
routerA.00-01     0xffffff01          0xe20b            677                     0/0/0
c3.00-00              0x002e5434      0xb20a            487                     0/0/0
c2.00-00             *0x74fd1227      0xbb0f            742                     0/0/0
c2.01-00             *0x7ee72c1a      0xb506            968                     0/0/0
```

次に、IS-ISデータベースの詳細な出力例を示します。詳細出力には、各LSPの内容が表示されます。

```
> show isis database detail

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0xea19d301      0x3b0e              1189                    0/0/0

  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: c1
  IP Address:   10.22.22.1
  Metric:         10 IP 10.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
routerA.00-00       0x1b541556     0xa349               642                     0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: routerA
  IP Address:   10.22.22.5
  Metric:         10 IP 10.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
```

次に、レベル2 LSPのみの詳細な出力例を示します。エリアアドレス39.0001は、ルータが存在するエリアのアドレスです。

```
> show isis database 12 detail

IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0x63871f25      0xa9a3              1076                    0/0/0

  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: c1
```

```
  IP Address:   10.22.22.1
  Metric:         10 IS c2.01
routerA.00-00     0x0d540b56     0x7fd8                941                       0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: routerA
  IP Address:   10.22.22.5
  Metric:         10 IS c2.01
  Metric:          0 IP-External 1.1.1.0 255.255.255.0
  Metric:          0 IP-External 2.1.1.0 255.255.255.0
  Metric:          0 IP-External 2.2.2.0 255.255.255.0
  Metric:          0 IP-External 3.1.1.0 255.255.255.0
```

次に、詳細出力の例を示します。

```
> show isis database verbose

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00             *0xea19d301   0x3b0e        644               0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: c1
  IP Address:   22.22.22.1
  Metric:         10 IP 22.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
routerA.00-00         0x1b541557   0xa14a        783               0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: routerA
  IP Address:   22.22.22.5
  Metric:         10 IP 22.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear isis** | IS-IS データ構造をクリアします。 |
| **show clns** | CLNS 固有の情報を表示します。 |
| **show route isis** | IS-IS ルートを表示します。 |

# show isis hostname

IS-IS ルータの、ルータ名とシステム ID のマッピングテーブルエントリを表示するには、**show isis hostname** コマンドを使用します。

**show isis hostname**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

## 使用上のガイドライン

IS-IS ルーティング ドメインでは、各ルータはシステム ID により表されます。システム ID は、IS-IS ルータごと構成されている Network Entity Title（NET）の一部です。たとえば、NET 49.0001.0023.0003.000a.00 が設定されているルータのシステム ID が 0023.0003.000a であるとします。ネットワーク管理者にとって、ルータでのメンテナンスやトラブルシューティングの間、ルータ名とシステム ID の対応を覚えているのは難しいことです。**show isis hostname** コマンドを入力すると、ルータ名とシステム ID のマッピングテーブルに含まれるエントリが表示されます。

### 例

次の例では、ダイナミック ホスト マッピング テーブルを表示します。ダイナミック ホスト マッピング テーブルは、cisco脅威に対する防御、c2、c3 および routerA という名前のローカルルータの、ルータ名とシステム ID のマッピング テーブルエントリを表示します。このテーブルは、c3 がレベル-1 ルータであり、そのホスト名がレベル-1（L1）リンクステートプロトコル（LSP）によりアドバタイズされることも示します。c2 はレベル-2 ルータであり、そのホスト名は L2 LSP によりアドバタイズされます。cisco脅威に対する防御 のレベルの下に表示される * 記号は、これがシステムのルータ名とシステム ID のマッピング情報であることを示します。

```
> show isis hostname

Level  System ID       Dynamic Hostname  (c1)
     * 0050.0500.5005   ciscoASA
    1  0050.0500.5007   c3
    2  0050.0500.5006   routerA
    2  0050.0500.5008   c2
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear isis** | IS-IS データ構造をクリアします。 |
| **show clns** | CLNS 固有の情報を表示します。 |
| **show route isis** | IS-IS ルートを表示します。 |

# show isis lsp-log

新しい LSP をトリガーしたインターフェイスのレベル 1 およびレベル 2 の IS-IS リンクステートパケット（LSP）のログを表示するには、**show isis lsp-log** コマンドを使用します。

**show isis lsp-log**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | 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して、新しいLSPをトリガーしたインターフェイスのレベル1およびレベル 2 の IS-IS リンクステートパケット（LSP）のログを表示します。出力には次の情報が含まれます。

- [When]：LSP が生成されてからの経過時間。
- [Count]：現時点で発生しているイベントの数。
- [Interface]：LSP を再生成したインターフェイス。
- [Triggers]：LSP のフラッディングをトリガーしたイベント。次のような、LSP に可能なトリガー。
  - AREASET：アクティブ エリア セットが変更されました。
  - ATTACHFLAG：Attach ビットの状態が変更されました。
  - CLEAR：ある形式の手動の clear コマンドが送信されました。
  - CONFIG：任意のコンフィギュレーションが変更されました。
  - DELADJ：隣接関係がダウンしました。
  - DIS：DIS が変更されたか、または疑似ノードが変更されました。
  - ES：エンド システムの隣接関係が変更されました。
  - HIPPITY：LSPDB 過負荷ビットの状態が変更されました。
  - IF_DOWN：新しい LSP が必要です。
  - IP_DEF_ORIG：元のデフォルト情報が変更されました。
  - IPDOWN：直接接続されている IP プレフィックスがダウンしました。
  - IP_EXTERNAL：再配布された IP ルートが現れたか、または失われました。
  - IPIA：エリア間 IP ルートが現れたか、または失われました。
  - IPUP：直接接続されている IP プレフィックスが起動しました。
  - NEWADJ：新しい隣接関係が現れました。

- REDIST：再配信されたレベル-2 CLNS ルートが変更されました。
- RRR_INFO：RRR 帯域幅リソース情報。

### 例

次に、**show isis lsp-log** コマンドの出力例を示します。

```
> show isis lsp-log

  Level 1 LSP log
When       Count       Interface         Triggers
04:16:47     1         subint             CONFIG NEWADJ DIS
03:52:42     2         subint             NEWADJ DIS
03:52:12     1         subint             ATTACHFLAG
03:31:41     1         subint             IPUP
03:30:08     2         subint             CONFIG
03:29:38     1         subint             DELADJ
03:09:07     1         subint             DIS ES
02:34:37     2         subint             NEWADJ
02:34:07     1         subint             NEWADJ DIS

  Level 2 LSP log
When       Count       Interface         Triggers
03:09:27     1         subint             CONFIG NEWADJ
03:09:22     1         subint             NEWADJ
02:34:57     2         subint             DIS
02:34:50     1                                IPUP
02:34:27     1         subint             CONFIG DELADJ
02:13:57     1         subint             DELADJ
02:13:52     1         subint             NEWADJ
01:35:58     2         subint             IPIA
01:35:51     1                              AREASET IPIA
```

### 関連コマンド

| Command | 説明 |
|---|---|
| **clear isis** | IS-IS データ構造をクリアします。 |
| **show clns** | CLNS 固有の情報を表示します。 |
| **show route isis** | IS-IS ルートを表示します。 |

# show isis neighbors

IS-IS ネイバーに関する情報を表示するには、**show isis neighbors** コマンドを使用します。

**show isis neighbors** ［**detail**］

## 構文の説明

| | |
|---|---|
| **detail** | （任意）IS-IS ネイバーの詳細情報を表示します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

## 使用上のガイドライン

次の表で、IS-IS ネイバー情報について説明します。

**表 *44 : IS-IS* ネイバー情報**

| フィールド | 説明 |
|---|---|
| System Id | エリア内のシステムを識別する 6 バイト値。 |
| タイプ | レベルのタイプ。IS-IS ネイバーがレベル 1、レベル-1-2、またはレベル 2 のルータのいずれであるかを示します。 |
| インターフェイス | システムが学習されたインターフェイス。 |
| IP Address | ネイバー ルータの IP アドレス。 |
| 状態 | IS-IS ネイバーの状態がアップかダウンか示します。 |
| Holdtime | リンクステート パケット（LSP）のホールド時間。LSP が有効である時間（秒単位）。 |
| Circuit Id | IS-IS 近接ルータがどのようにローカル ルータに接続されているかを示す、IS-IS 近接ルータのポート ロケーション。 |
| Area Address(es) | ルータから到達可能なエリア アドレス。レベル 1 LSP の場合は、送信元ルータ上で手動により設定されるエリア アドレスになります。レベル 2 LSP の場合は、このルータが属するエリアのすべてのエリア アドレスになります。 |
| SNPA | サブネットワーク ポイント オブ アタッチメント。これはデータ リンク アドレスです。 |
| State Changed | 状態変更の時刻。 |
| LAN Priority | LAN のプライオリティ。 |

| フィールド | 説明 |
|---|---|
| Remote TID | ネイバールータトポロジ ID。 |
| Local TID | ローカルルータトポロジ ID。 |

### 例

次の例は、基本的な IS-IS ネイバー情報を示しています。

```
> show isis neighbors

System Id      Type Interface   IP Address      State Holdtime Circuit Id
routerA          L1    subint   10.22.22.5        UP    21          c2.01
routerA          L2    subint   10.22.22.5        UP    22          c2.01
c2               L1    subint   10.22.22.3        UP     9          c2.01
c2               L2    subint   10.22.22.3        UP     9          c2.01
```

次の例は、詳細な IS-IS ネイバー情報を示しています。

```
> show isis neighbors detail

System Id      Type Interface   IP Address      State Holdtime Circuit Id
routerA          L1    subint   10.22.22.5        UP    23          c2.01
  Area Address(es): 49.0001
  SNPA:       0025.8407.f2b0
  State Changed: 00:03:03
  LAN Priority: 64
  Format: Phase V
  Remote TID: 0
  Local TID:  0
  Interface name: subint
routerA          L2    subint   10.22.22.5        UP    22         c2.01
  Area Address(es): 49.0001
  SNPA:       0025.8407.f2b0
  State Changed: 00:03:03
  LAN Priority: 64
  Format: Phase V
  Remote TID: 0
  Local TID:  0
  Interface name: subint
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear isis** | IS-IS データ構造をクリアします。 |
| **show clns** | CLNS 固有の情報を表示します。 |
| **show route isis** | IS-IS ルートを表示します。 |

# show isis rib

特定のルートのパス、またはIPローカルルーティング情報ベース（RIB）に格納されているメジャーネットワーク下の全ルートのパスを表示するには、**show isis rib** コマンドを使用します。

**show isis** ［***** | **ip** ［**unicast**］ | **ipv6** ［**unicast**］］ **rib** ［**redistribution** ［**level-1** | **level-2**］］ ［*network_ip* ［*mask*］］

## 構文の説明

| | |
|---|---|
| ***** | （オプション）すべての IS-IS アドレス ファミリを表示します。 |
| **ip** | （オプション）IPv4 アドレス ファミリを表示します。 |
| **ipv6** | （オプション）IPv6 アドレス ファミリを表示します。 |
| **level-1** | （オプション） レベル 1 再配布 RIB を表示します。 |
| **level-2** | （オプション） レベル 2 再配布 RIB を表示します。 |
| *network_ip* [*mask*] | （オプション）ネットワークの RIB 情報を表示します。 |
| **redistribution** | （オプション）IS-IS IP 再配布 RIB 情報を表示します。 |
| **unicast** | （オプション）ユニキャスト アドレス ファミリを表示します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | 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して、IP グローバル RIB 内に存在する IP プレフィックスアップデートも IS-IS ローカル RIB 内で更新されたことを確認します。

### 例

次に、IS-IS ローカル RIB 内に格納されているすべてのルートを表示する例を示します。

```
> show isis rib

IPv4 local RIB for IS-IS process

IPV4 unicast topology base (TID 0, TOPOID 0x2) = = = = = = = = = = = = = =

10.10.0.0 255.255.0.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[12/524]


10.1.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[12/524]
```

```
10.3.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[13/149]
```

次に、IS-IS ローカル RIB 内に格納されている、IP アドレスが 10.3.2.0 のメジャーネットワーク 10.0.0.0 下の全ルータを表示する例を示します。

```
> show isis rib 10.3.2.0

IPv4 local RIB for IS-IS process

IPV4 unicast topology base (TID 0, TOPOID 0x2) = = = = = = = = = = = = =
Routes under majornet 10.0.0.0 255.0.0.0:

10.1.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[12/524]


10.3.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[13/149]
```

次に、IS-IS ローカル RIB 内に格納されている、IP アドレスとマスクが 10.3.2.0 255.255.255.0 のネットワーク下の全ルータを表示する例を示します。

```
> show isis rib 10.3.2.0 255.255.255.0

IPv4 local RIB for IS-IS process

IPV4 unicast topology base (TID 0, TOPOID 0x2) = = = = = = = = = = = = =

10.3.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[13/149]
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear isis** | IS-IS データ構造をクリアします。 |
| **show clns** | CLNS 固有の情報を表示します。 |
| **show route isis** | IS-IS ルートを表示します。 |

# show isis spf-log

ルータがフル最短パス優先（SPF）計算を実行した頻度と理由を表示するには、**show isis spf-log** コマンドを使用します。

**show isis** ［***** | **ip** ［**unicast**］ | **ipv6** ［**unicast**］］ **spf-log**

## 構文の説明

| | |
|---|---|
| ***** | （オプション）すべての IS-IS アドレス ファミリを表示します。 |
| **ip** | （オプション）IPv4 アドレス ファミリを表示します。 |
| **ipv6** | （オプション）IPv6 アドレス ファミリを表示します。 |
| **unicast** | （オプション）ユニキャスト アドレス ファミリを表示します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | 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、ルータがフル最短パス優先（SPF）計算を実行した頻度と理由を表示します。次の表で、出力のフィールドについて説明します。

| フィールド | 説明 |
|---|---|
| When | 今からどれくらい前（時間：分：秒）にフル SPF 計算が発生したか。直近 20 回分の発生内容が記録されます。 |
| 持続時間 | 今回の SPF 実行を完了させるために必要なミリ秒数。経過時間は実経過時間であり、CPU 時間ではありません。 |
| ノード | 今回の SPF 実行で計算されるトポロジを生成するルータおよび疑似ノード（LAN）の数。 |
| Count | 今回の SPF 実行をトリガーしたイベントの数。トポロジが変更されると、複数のリンクステート パケット（LSP）が短時間で受信されます。ルータは、フル SPF を実行するまでに 5 秒待機し、すべての新しい情報を保持できるようにします。この数は、ルータがフル SPF を実行するまで 5 秒待機する間に発生した（新しい LSP の受信のような）イベントの数を意味します。 |
| First Trigger LSP | 新しい LSP の到着でフル SPF 計算がトリガーされると、常にルータは LSP ID を保存します。LSP ID は、エリア内でルーティングが不安定である原因の手掛かりを提供できます。複数の LSP が 1 つの SPF を実行すると、最後に受信された LSP の LSP ID だけが記憶されます。 |

| フィールド | 説明 |
|---|---|
| Triggers | フル SPF 計算をトリガーしたすべての理由のリスト。トリガーに関する次の表を参照してください。 |

次の表では、考えられるトリガーについて説明しています。

| **Trigger** | 説明 |
|---|---|
| ATTACHFLAG | このルータは、レベル 2 バックボーンに接続されるているか、または、レベル 2 バックボーンとの接続を失ったばかりです。 |
| ADMINDIST | このルータの IS-IS プロセスに、別のアドミニストレーティブ ディスタンスが設定されました。 |
| AREASET | このエリアの学習されたエリア アドレスの設定が変更されました。 |
| BACKUPOVFL | IP プレフィックスが失われました。ルータはそのプレフィックスに到達するために別の方法があることを知っていますが、そのバックアップルートを保存していません。別のルートを見つける唯一の方法は、フル SPF の実行です。 |
| DBCHANGED | このルータで、**clear isis *** コマンドが発行されました。 |
| IPBACKUP | IP ルートが失われましたが、これは IS-IS を介してではなく、優れたアドミニストレーティブ ディスタンスを持つ別のプロトコルを介して学習されました。IS-IS はフル SPF を実行し、失われた IP プレフィックスまでの IS-IS ルートをインストールします。 |
| IPQUERY | このルータで、**clear ip route** コマンドが発行されました。 |
| LSPEXPIRED | リンクステート データベース（LSDB）内のいくつかの LSP の期限が切れました。 |
| LSPHEADER | LSP ヘッダー内の ATT/P/OL ビットまたは IS タイプが変更されました。 |
| NEWADJ | このルータが、別のルータとの新しい隣接関係を作成しました。 |
| NEWAREA | このルータに、新しいエリアが（Network Entity Title [NET] を介して）設定されました。 |
| NEWLEVEL | このルータに、（IS タイプを介して）新しいレベルが設定されました。 |
| NEWLSP | トポロジ内に新しいルータまたは疑似ノードが現れました。 |
| NEWMETRIC | このルータのインターフェイスに、新しいメトリックが設定されました。 |

| Trigger | 説明 |
|---|---|
| NEWSYSID | このルータに、（NET を介して）新しいシステム ID が設定されました。 |
| PERIODIC | ルータは通常、15 秒ごとの間隔でフル SPF 計算を実行します。 |
| RTCLEARED | このルータで、**clear clns route** コマンドが発行されました。 |
| TLVCODE | TLV コードの不一致であり、最新バージョンの LSP に異なる TLV が含まれていることを示します。 |
| TLVCONTENT | TLV のコンテンツが変更されました。これは通常、エリア内で隣接関係がアップまたはダウンしたこを示します。「First trigger LSP」カラムは、不安定な状態が発生した可能性のある場所を示します。 |

### 例

次に、**show isis ipv6 spf-log** コマンドの出力例を示します。

```
> show isis ipv6 spf-log

     TID 0 level 1 SPF log
  When   Duration  Nodes  Count     First trigger LSP   Triggers
00:15:46    3124     40      1          milles.00-00  TLVCODE
00:15:24    3216     41      5          milles.00-00  TLVCODE NEWLSP
00:15:19    3096     41      1          deurze.00-00  TLVCODE
00:14:54    3004     41      2          milles.00-00  ATTACHFLAG LSPHEADER
00:14:49    3384     41      1          milles.00-01  TLVCODE
00:14:23    2932     41      3          milles.00-00  TLVCODE
00:05:18    3140     41      1                        PERIODIC
00:03:54    3144     41      1          milles.01-00  TLVCODE
00:03:49    2908     41      1          milles.01-00  TLVCODE
00:03:28    3148     41      3           bakel.00-00  TLVCODE TLVCONTENT
00:03:15    3054     41      1          milles.00-00  TLVCODE
00:02:53    2958     41      1          mortel.00-00  TLVCODE
00:02:48    3632     41      2          milles.00-00  NEWADJ TLVCODE
00:02:23    2988     41      1          milles.00-01  TLVCODE
00:02:18    3016     41      1          gemert.00-00  TLVCODE
00:02:14    2932     41      1           bakel.00-00  TLVCONTENT
00:02:09    2988     41      2           bakel.00-00  TLVCONTENT
00:01:54    3228     41      1          milles.00-00  TLVCODE
00:01:38    3120     41      3            rips.03-00  TLVCONTENT
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear isis** | IS-IS データ構造をクリアします。 |
| **show clns** | CLNS 固有の情報を表示します。 |
| **show route isis** | IS-IS ルートを表示します。 |

# show isis topology

すべてのエリア内の接続された全ルータのリストを表示するには、**show isis topology** コマンドを使用します。

**show isis** ［***** | **ip** ［**unicast**］ | **ipv6** ［**unicast**］］ **topology** ［**level-1** | **level-2**］

## 構文の説明

| | |
|---|---|
| ***** | （オプション）すべての IS-IS アドレス ファミリを表示します。 |
| **ip** | （オプション）IPv4 アドレス ファミリを表示します。 |
| **ipv6** | （オプション）IPv6 アドレス ファミリを表示します。 |
| **level-1** | （オプション）レベル 1 再配布 RIB を表示します。 |
| **level-2** | （オプション）レベル 2 再配布 RIB を表示します。 |
| **unicast** | （オプション）ユニキャスト アドレス ファミリを表示します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

## 使用上のガイドライン

**show isis topology** コマンドを使用すると、すべてのエリア内の全ルータの存在およびルータ間の接続状態を確認できます。次の表でフィールドを説明します。

| フィールド | 説明 |
|---|---|
| System Id | エリア内のシステムを識別する 6 バイト値。 |
| メトリック | 送信側ルータとアドバタイズされたネイバー間の隣接関係のコスト用の IS-IS メトリック、またはアドバタイズ元のルータからアドバタイズ対象の宛先（IP アドレス、エンド システム [ES]、または CLNS プレフィックス）に到達するコスト用のメトリック。 |
| Next-Hop | ネクスト ホップ ルータのアドレス。 |
| インターフェイス | システムが学習されたインターフェイス。 |
| SNPA | サブネットワーク ポイント オブ アタッチメント。これはデータ リンク アドレスです。 |

### 例

次に、**show isis topology** コマンドの出力例を示します。

```
> show isis topology

IS-IS TID 0 paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
cisco1                  --
routerA                 10       routerA                 subint  0025.8407.f2b0
c3                      10
c2                      10            c2                subint  c08c.60e6.986f

IS-IS TID 0 paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
cisco1                  --
routerA                 10       routerA                 subint  0025.8407.f2b0
c3                      10
c2                      10            c2                subint  c08c.60e6.986f
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear isis** | IS-IS データ構造をクリアします。 |
| **show clns** | CLNS 固有の情報を表示します。 |
| **show route isis** | IS-IS ルートを表示します。 |

# show j - show o

# show jumbo-frame reservation

すべてのインターフェイスでジャンボフレームが有効になっているかどうかを表示するには、**show jumbo-frame reservation** コマンドを使用します。

**show jumbo-frame reservation**

## 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

インターフェイスのMTUを1500以上にすると、ジャンボフレーム予約が有効になります。すべての MTU を 1500 以下に戻すと、ジャンボフレーム予約は自動的に無効になります。

### 例

次に、ジャンボフレームサポートが有効になっている場合の **show jumbo-frame reservation** コマンドの出力例を示します。

```
> show jumbo-frame-reservation
Jumbo Frame Support is currently enabled
```

# show kernel

デバッグに使用できる Linux brctl ユーティリティが提供する情報を表示するには、**show kernel** コマンドを使用します。

**show kernel** {**process** | **bridge** [**mac-address** *bridge_name*] | **cgroup-controller** [**cpu** | **cpuset** | **memory**] [**detail**] | **ifconfig** | **module**}

## 構文の説明

| | |
|---|---|
| **bridge** [ **mac-address** *bridge_name*] | デバッグに使用できる各ポート上で学習された Linux ブリッジ、それらのメンバーポート、および MAC アドレス（リモート MAC アドレスを含む）を表示します。**mac-address** キーワードを使用して、特定のブリッジに関する MAC アドレスの詳細を表示できます。br0 などの使用可能なブリッジ名を表示するには、キーワードを指定せずにコマンドを使用します。 |
| **cgroup-controller** [**cpu** \| **cpuset** \| **memory**] [**detail**] | cgroup-controller の統計情報を表示します。**cpu**、**cpuset** および **memory** キーワードを使用すると、要件に応じて cgroup-controller 統計情報をフィルタリングできます。詳細情報を表示するには、detail キーワードを使用します。 |
| **ifconfig** | タップおよびブリッジ インターフェイスの統計情報を表示します。 |
| **module** | インストールおよび実行されているモジュールを表示します。 |
| **process** | デバイスで実行されているアクティブなカーネルプロセスの現在のステータスを表示します。 |

## 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

このコマンドは、カーネルで実行されるさまざまなプロセスの統計情報を表示します。

### 例

次に、**show kernel process** コマンドの出力例を示します。

```
> show kernel process
PID PPID PRI NI      VSIZE      RSS      WCHAN STAT  RUNTIME COMMAND
  1    0  16  0     991232      268 3725684979    S       78 init
  2    1  34 19          0        0 3725694381    S        0 ksoftirqd/0
  3    1  10 -5          0        0 3725736671    S        0 events/0
  4    1  20 -5          0        0 3725736671    S        0 khelper
  5    1  20 -5          0        0 3725736671    S        0 kthread
  7    5  10 -5          0        0 3725736671    S        0 kblockd/0
  8    5  20 -5          0        0 3726794334    S        0 kseriod
 66    5  20  0          0        0 3725811768    S        0 pdflush
 67    5  15  0          0        0 3725811768    S        0 pdflush
```

```
 68    1  15  0          0        0 3725824451    S         2 kswapd0
 69    5  20 -5          0        0 3725736671    S         0 aio/0
171    1  16  0     991232       80 3725684979    S         0 init
172  171  19  0     983040      268 3725684979    S         0 rcS
201  172  21  0    1351680      344 3725712932    S         0 lina_monitor
202  201  16  0 1017602048   899932 3725716348    S       212 lina
203  202  16  0 1017602048   899932          0    S         0 lina
204  203  15  0 1017602048   899932          0    S         0 lina
205  203  15  0 1017602048   899932 3725712932    S         6 lina
206  203  25  0 1017602048   899932          0    R 13069390 lina
>
```

次の表で各フィールドについて説明します。

**表 *45 : show kernel process* のフィールド**

| フィールド | 説明 |
|---|---|
| PID | プロセス ID。 |
| PPID | 親プロセス ID。 |
| PRI | プロセスのプライオリティ。 |
| NI | プライオリティの計算に使用されるナイス値。値は 19（最大ナイス値）～ -19（最小ナイス値）の範囲です。 |
| VSIZE | 仮想メモリのサイズ（バイト単位）。 |
| RSS | プロセスの Resident Set Size（KB 単位）。 |
| WCHAN | プロセスが待機しているチャネル。 |
| STAT | プロセスの状態。<br>• R：実行中<br>• S：割り込み可能な待機状態でスリープ中<br>• D：割り込み不可能なディスク スリープで待機中<br>• Z：ゾンビ<br>• T：トレースまたは停止（信号による）<br>• P：ページング |
| RUNTIME | プロセスがユーザーモードまたはカーネルモードでスケジュールされている jiffy の数。実行時間は utime と stime の合計です。 |
| COMMAND | プロセス名。 |

次に、**show kernel module** コマンドの出力例を示します。

```
> show kernel module

Module                  Size  Used by    Tainted: P
cpp_base              861808  2
kvm_intel              44104  8
kvm                   174304  1 kvm_intel
msrif                   4180  0
tscsync                 3852  0
```

次に、**show kernel ifconfig** コマンドの出力例を示します。

```
> show kernel ifconfig

br0       Link encap:Ethernet  HWaddr 42:9E:B8:6C:1F:23
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1708 (1.6 KiB)  TX bytes:0 (0.0 B)

br1       Link encap:Ethernet  HWaddr 6A:03:EC:BA:89:26
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.255.255.255
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

tap0      Link encap:Ethernet  HWaddr 6A:0C:48:32:FE:F4
          inet addr:127.0.2.2  Bcast:127.255.255.255  Mask:255.0.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:148 errors:0 dropped:0 overruns:0 frame:0
          TX packets:186 errors:0 dropped:13 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:10320 (10.0 KiB)  TX bytes:12452 (12.1 KiB)

tap1      Link encap:Ethernet  HWaddr 8E:E7:61:CF:E9:BD
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:259 errors:0 dropped:0 overruns:0 frame:0
          TX packets:187 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:19368 (18.9 KiB)  TX bytes:14638 (14.2 KiB)

tap2      Link encap:Ethernet  HWaddr 6A:03:EC:BA:89:26
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

tap3      Link encap:Ethernet  HWaddr 42:9E:B8:6C:1F:23
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:187 errors:0 dropped:0 overruns:0 frame:0
          TX packets:256 errors:0 dropped:3 overruns:0 carrier:0
```

```
          collisions:0 txqueuelen:500
          RX bytes:14638 (14.2 KiB)  TX bytes:19202 (18.7 KiB)

tap4      Link encap:Ethernet  HWaddr 6A:5C:60:BC:9C:ED
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

次に、**show kernel bridge** コマンドの出力例を示します。

```
> show kernel bridge

bridge name     bridge id               STP enabled     interfaces
br0             8000.000000040001       no              tap1
                                                        tap3
br1             8000.84b261b192bd       no              tap2
                                                        tap4
                                                        tap5
```

次に、**show kernel bridge mac-address** コマンドの出力例を示します。

```
> show kernel bridge mac-address br1

port no    mac addr       is local?   ageing timer
 1    00:21:d8:cb:dc:f7    no          12.93
 3    00:22:bd:d8:7d:da    no          12.93
 2    26:d2:9f:51:a4:90    yes          0.00
 1    4e:a4:e0:73:1f:ab    yes          0.00
 3    52:04:38:3d:79:c0    yes          0.00
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show module** | デバイスにインストールされているモジュールに関する情報を表示します。 |

# show lacp

EtherChannel LACP 情報（トラフィック統計情報、システム ID、およびネイバーの詳細など）を表示するには、次のコマンドを入力します。

**show lacp** {*channel_group_number* {**counters** | **internal** ［**detail**］ | **neighbor** ［**detail**］} | **neighbor** ［**detail**］ | **sys-id**}

## 構文の説明

| | |
|---|---|
| *channel_group_number* | EtherChannel チャネルグループ番号を 1 ～ 48 の範囲で指定して、このチャネルグループに関する情報のみを表示します。 |
| **counters** | 送受信された LACPDU 数およびマーカー数のカウンタを表示します。 |
| **detail** | 項目の詳細を表示します。 |
| **internal** | 内部情報を表示します。 |
| **neighbor** | ネイバー情報を表示します。 |
| **sys-id** | LACP システム ID を表示します。 |

## 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、**show lacp sys-id** コマンドの出力例を示します。

```
> show lacp sys-id
32768,001c.c4e5.cfee
```

次に、**show lacp counters** コマンドの出力例を示します。

```
> show lacp counters

              LACPDUs         Marker      Marker Response    LACPDUs
Port       Sent   Recv     Sent   Recv    Sent    Recv      Pkts Err
--------------------------------------------------------------------
Channel group: 1
Gi3/1      736    728      0      0        0      0         0
Gi3/2      739    730      0      0        0      0         0
Gi3/3      739    732      0      0        0      0         0
```

次に、**show lacp internal** コマンドの出力例を示します。

```
> show lacp internal
```

```
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl      32768         0x1       0x1     0x302       0x3d
Gi3/2     SA      bndl      32768         0x1       0x1     0x303       0x3d
Gi3/3     SA      bndl      32768         0x1       0x1     0x304       0x3d
```

次に、**show lacp neighbor** コマンドの出力例を示します。

```
> show lacp neighbor

Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1 neighbors

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x0       0x1      0x306       0x3d
Gi3/2     SA      bndl       32768         0x0       0x1      0x303       0x3d
Gi3/3     SA      bndl       32768         0x0       0x1      0x302       0x3d
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show port-channel** | EtherChannel 情報が、詳細に 1 行のサマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。 |
| **show port-channel load-balance** | ポートチャネル負荷分散情報が、指定のパラメータ セットに対するハッシュ結果および選択されたメンバー インターフェイスとともに表示されます。 |

# show lacp cluster

cLACP システムの MAC と ID を表示するには、**show lacp cluster** コマンドを使用します。

**show lacp cluster** {**system-mac** | **system-id**}

## 構文の説明

| | |
|---|---|
| **system-mac** | システム ID と、それが自動生成されたのか手動入力されたのかを表示します。 |
| **system-id** | システム ID およびプライオリティを表示します。 |

## 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、**show lacp cluster system-mac** コマンドの出力例を示します。

```
> show lacp cluster system-mac
lacp cluster system MAC is automatically generated: a300.010a.010a.
```

次に、**show lacp cluster system-id** コマンドの出力例を示します。

```
> show lacp cluster system-id
5    ,a300.010a.010a
```

# show last-upgrade status

最後のシステム ソフトウェア アップグレードのステータスに関する情報を表示するには、**show last-upgrade status** コマンドを使用します。

**show last-upgrade status**

## 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。 |

### 例

次の例は、最後のアップグレードが成功したことを示しています。実際の出力では、x.y.0 は実際のバージョン番号に置き換えられます。

```
> show last-upgrade status
Upgrade from 6.7.0 to x.y.0 was successful.
Time started: Tue Dec  3 23:50:31 UTC 2020
```

次の例は、最後のアップグレードがキャンセルされたことを示しています。実際の出力では、x.y.0 は実際のバージョン番号に置き換えられます。

```
> show last-upgrade status
Upgrade from 6.7.0 to x.y.0 failed.
Time started: Tue Dec  3 23:50:31 UTC 2020
Cancel Upgrade was successful.
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **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。 |
| **upgrade** | システム ソフトウェア アップグレードをキャンセル、復元、または再試行します。 |

# show lisp eid

EID テーブルを表示するには、**show lisp eid** コマンドを使用します。

**show lisp eid** ［**site-id** *id*］

## 構文の説明

| | |
|---|---|
| **site-id** *id* | 特定のサイトの EID のみを表示します。 |

## 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

デバイスは、EID とサイト ID を関連付ける EID テーブルを保持します。

### 例

次に、**show lisp eid** コマンドの出力例を示します。

```
> show lisp eid
LISP EID       Site ID
10.44.33.105        2
10.44.33.201        2
192.168.11.1        4
192.168.11.2        4
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear cluster info flow-mobility counters** | フロー モビリティ カウンタをクリアします。 |
| **clear lisp eid** | ASA EID テーブルから EID を削除します。 |
| **show cluster info flow-mobility counters** | フロー モビリティ カウンタを表示します。 |
| **show conn** | LISP フロー モビリティの対象となるトラフィックを表示します。 |
| **show service-policy** | サービス ポリシーを表示します。 |

# show lldp

インターフェイスの Link Layer Discovery Protocol（LLDP）のステータスを表示するには、**show lldp** コマンドを使用します。

（注） Firepower 1100 では LLDP のみがサポートされます。

**show lldp** { **neighbors** | **statistics** | **status** } *interface_id*

## 構文の説明

| | |
|---|---|
| *interface_id* | インターフェイス ID を指定します。 |
| **neighbors** | LLDP ネイバーシップが確立されているかどうかを示します。 |
| **statistics** | LLDP の統計を表示します。 |
| **status** | LLDP が有効になっているかどうかを示します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1 | このコマンドが導入されました。 |

## 使用上のガイドライン

**via** フィールドには、アクティブな場合は LLDP が表示され、LLDP が無効になっているか、または機能していない場合は Unknown と表示されます。

### 例

次に、**show lldp neighbors** コマンドの出力例を示します。

```
> show lldp neighbors

------------------------------------------------------------------------------
LLDP neighbors:
------------------------------------------------------------------------------
Interface: lldp-Eth1_6, via: LLDP, RID: 1, Time: 0 day, 00:00:18
  Chassis:
    ChassisID: mac 8c:60:4f:58:c1:ac
    SysName: ruintpo
    SysDescr: Cisco Nexus Operating System (NX OS) Software 7.0(1)N1(1)
 TAC support: http://www.cisco.com /tac
 Copyright (c) 2002-2014, Cisco Systems, Inc. All rights reserved.
    MgmtIP: 10.225.126.91
    Capability: Bridge, on
  Port:
    PortID: local Eth1/37
    PortDescr: Ethernet1/37
    TTL: 30
------------------------------------------------------------------------------
```

次に、**show lldp statistics** コマンドの出力例を示します。

```
> show lldp statistics interface Ethernet 1/6
-------------------------------------------------------------------------------
LLDP statistics:
-------------------------------------------------------------------------------
Interface: lldp-Eth1_6
  Transmitted: 115
  Received: 116
  Discarded: 0
  Unrecognized: 0
  Ageout: 0
  Inserted: 0
  Deleted: 0
-------------------------------------------------------------------------------
```

次に、**show lldp status** コマンドの出力例を示します。

```
> show lldp status interface Ethernet 1/6
-------------------------------------------------------------------------------
LLDP interfaces:
-------------------------------------------------------------------------------
Interface: lldp-Eth1_6, via: unknown, Time: 18795 days, 05:38:39
  Chassis:
    ChassisID: mac 42:8f:14:a8:2f:c5
    SysName: firepower
    SysDescr: Cisco Firepower 1150 Threat Defense 7.1.0 1558
    MgmtIP: 127.128.254.1
    MgmtIP: fd00:0:0:1::3
    Capability: Bridge, on
    Capability: Router, off
    Capability: Wlan , off
    Capability: Station, off
  Port:
    PortID: mac 34:12:78:56:01:03
    PortDescr: Ethernet1/6
    TTL: 120
-------------------------------------------------------------------------------
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show interface** | インターフェイスの統計を表示します。 |

# show local-host

ローカルホストのネットワーク状態を表示するには、**show local-host** コマンドを使用します。

**show local-host** ［*hostname* | *ip_address*］［**detail**］［**all**］［**brief**］［**connection** {**sctp** | **tcp** | **udp** | **embryonic**} *start*［*-end*］］［**zone**］

## 構文の説明

| | |
|---|---|
| **all** | （廃止）デバイスに接続するローカルホストと、デバイスから接続するローカルホストが含まれます。 |
| **brief** | （オプション）ローカル ホストに関する簡潔な情報を表示します。 |
| **connection** {**sctp** \| **tcp** \| **udp** \| **embryonic**} *start*[*-end*] | （廃止）番号と接続のタイプに基づいて、初期、TCP、UDP、または SCTP のフィルタを適用します。start の数値は、そのタイプの最小接続数を示します。-end の数値を含めると、10-100 などの範囲を指定できます。これらのフィルタは個別に使用することも、組み合わせて使用することもできます。 |
| **detail** | （任意）アクティブな xlate およびネットワーク接続の詳細情報を含めた、ローカルホスト情報の詳細なネットワーク状態を表示します。 |
| *hostname* \| *ip_address* | （オプション）ローカル ホスト名または IPv4/IPv6 アドレスを指定します。 |
| **zone** | （オプション）ゾーンごと、またはインラインセットごとにローカルホストを指定します。 |

## 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。 |
| 7.0 | 廃止されたキーワード：**all**、**connection** |

## 使用上のガイドライン

**show local-host** コマンドを使用すると、ローカルホストのネットワーク状態を表示できます。ローカルホストは、脅威に対する防御デバイスにトラフィックを送信するか、またはそのデバイスを通じてトラフィックを転送する任意のホストに対して作成されます。

7.0 以降を実行しているシステムでは、このコマンドの代わりに **show conn address** コマンドを使用することを検討してください。

このコマンドを使用すると、ローカルホストの変換スロットおよび接続スロットを表示できます。変換情報には、ホストに割り当てられた PAT ポートのブロックが含まれます。

このコマンドでは、接続の制限数も表示されます。接続制限が設定されていない場合、値として 0 が表示され、制限は適用されません。

TCP 代行受信が設定されている場合に、SYN 攻撃が発生すると、**show local-host** コマンド出力では、代行受信された接続の数が使用回数に計上されます。このフィールドは通常、完全なオープン接続のみを表示します。

**show local-host** コマンド出力では、静的接続を使用するホストに対して最大初期接続の制限値（TCP 代行受信の水準点）が設定されている場合に、**TCP embryonic count to host counter** が使用されます。このカウンタは、他のホストからこのホストに向かう初期接続の合計を示します。この合計が設定された最大制限値を超過すると、このホストへの新規接続に TCP 代行受信が適用されます。

### 例

次に、**show local-host** コマンドの出力例を示します。

```
> show local-host

Interface mgmt: 2 active, 2 maximum active, 0 denied
local host: <10.24.250.191>,
    SCTP flow count/limit = 0/unlimited
    TCP flow count/limit = 1/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited
local host: <10.44.64.65>,
    SCTP flow count/limit = 0/unlimited
    TCP flow count/limit = 1/unlimited
    TCP embryonic count to host = 1
    TCP intercept watermark = unlimited
    UDP flow count/limit = 5/unlimited
Interface inside: 0 active, 0 maximum active, 0 denied
Interface outside: 0 active, 0 maximum active, 0 denied
Interface any: 0 active, 0 maximum active, 0 denied
```

次に、ローカル ホストのネットワーク状態の例を示します。

```
> show local-host all

Interface outside: 1 active, 2 maximum active, 0 denied
local host: <11.0.0.4>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
Interface inside: 1 active, 2 maximum active, 0 denied
local host: <17.3.8.2>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
```

```
Interface NP Identity Ifc: 2 active, 4 maximum active, 0 denied
local host: <11.0.0.3>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
local host: <17.3.8.1>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464
```

次の例では、特定のホストに関する情報に続けて、そのホストの詳細情報を示しています。

```
> show local-host 10.1.1.91
Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited

Xlate:
PAT Global 192.150.49.1(1024) Local 10.1.1.91(4984)

Conn:
TCP out 192.150.49.10:21 in 10.1.1.91:4984 idle 0:00:07 bytes 75 flags UI Interface
outside: 1 active, 1 maximum active, 0 denied

> show local-host 10.1.1.91 detail
Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited

Xlate:
TCP PAT from inside:10.1.1.91/4984 to outside:192.150.49.1/1024 flags ri

Conn:
TCP outside:192.150.49.10/21 inside:10.1.1.91/4984 flags UI Interface outside: 1 active,
1 maximum active, 0 denied
```

次に、少なくとも 4 つの UDP 接続および同時に 1 ～ 10 の TCP 接続を確立するすべてのホストの例を示します。

```
> show local-host connection udp 4 tcp 1-10
Interface mng: 0 active, 3 maximum active, 0 denied
Interface INSIDE: 4 active, 5 maximum active, 0 denied
local host: <10.1.1.11>,
       TCP flow count/limit = 1/unlimited TCP embryonic count to host = 0 TCP intercept
       watermark = unlimited UDP flow count/limit = 4/unlimited
Xlate:
       Global 192.168.1.24 Local 10.1.1.11 Conn: UDP out 192.168.1.10:80 in
       10.1.1.11:1730 idle 0:00:21 bytes 0 flags - UDP out 192.168.1.10:80 in
       10.1.1.11:1729 idle 0:00:22 bytes 0 flags - UDP out 192.168.1.10:80 in
       10.1.1.11:1728 idle 0:00:23 bytes 0 flags - UDP out 192.168.1.10:80 in
       10.1.1.11:1727 idle 0:00:24 bytes 0 flags - TCP out 192.168.1.10:22 in
       10.1.1.11:27337 idle 0:01:55 bytes 2641 flags UIO Interface OUTSIDE: 3 active, 5
       maximum active, 0 denied
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear local-host** | **show local-host** コマンドによって表示されるローカルホストからのネットワーク接続を解放します。 |

# show log-events-to-ramdisk

RAM ディスクへの接続イベントのロギングステータスを表示するには、**show log-events-to-ramdisk** コマンドを使用します。

**show log-events-to-ramdisk**

## 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、接続イベントを RAM ディスクにロギングしているか、SSD にロギングしているかを示します。RAM ディスクロギングは、すべてのハードウェアモデルでサポートされているわけではありません。RAM ディスクロギングは、**configure log-events-to-ramdisk** コマンドを使用して設定します。

### 例

次の例は、このハードウェアモデルでは RAM ディスクへのロギングがサポートされていないことを示しています。

```
> show log-events-to-ramdisk
This command is not available on this platform.
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure log-events-to-ramdisk** | RAM ディスクへの接続イベントのロギングを有効または無効にします。 |

# show logging

バッファ内のログまたはその他のロギング設定を表示するには、**show logging** コマンドを使用します。

**show logging** ［**message** ［*syslog_id* | **all**］ | **asdm** | **flow-export-syslogs** | **queue** | **setting** | **unified-client** ［**statistics**］ ］

## 構文の説明

| | |
|---|---|
| **all** | （任意）すべての syslog メッセージ ID と、有効か無効かを表示します。 |
| **asdm** | （任意）このキーワードは、Device Manager では機能しません。これは、ASA ソフトウェアデバイスを設定する ASDM に関連しています。 |
| **flow-export-syslogs** | （オプション。情報も NetFlow によってキャプチャされるすべての syslog メッセージを表示します。 |
| **message** [*syslog_id* \| **all**] | （任意）syslog ID または all を指定しない場合、このキーワードを指定するとデフォルト以外のレベルのメッセージが表示されます。また、メッセージを ID で表示したり、すべての syslog メッセージの情報を表示したりできます。 |
| **queue** | （任意）syslog メッセージ キューを表示します。 |
| **setting** | （任意）ロギング設定を表示します。ロギング バッファは表示されません。 |
| *syslog_id* | （任意）表示するメッセージ番号を指定します。 |
| **unified-client** [**statistics**] | loggerD サービスステータス、syslog クライアント登録情報、loggerD ハートビートの詳細、syslog クライアント制御/データおよびエラー統計情報など、syslog クライアントのステータスに関する詳細な統計情報を表示します。 |

## 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。 |
| 6.3 | **unified-client** [**statistics**] キーワードが追加されました。 |

## 使用上のガイドライン

内部バッファへのロギングを有効にしている場合、キーワードを指定せずに **show logging** コマンドを実行すると、現在のメッセージバッファと現在の設定が表示されます。

**show logging queue** コマンドでは、次の内容を表示できます。

- キュー内のメッセージ数

- キュー内に記録されたメッセージの最大数
- 処理に利用できるブロック メモリがなかったために廃棄されたメッセージ数
- トラップおよび他の syslog メッセージごとに別々のキュー

（注） ゼロは、設定するキュー サイズとして許容される数値であり、最大許容キュー サイズを示します。設定されたキューサイズが 0 の場合、**show logging queue** コマンドの出力に実際のキューサイズが表示されます。

**show logging flow-export-syslogs** コマンドは、次の syslog が有効か無効かを示します。NetFlow を使用する場合、これらの syslog は冗長であるため無効化できます。

| syslog メッセージ | 説明 |
|---|---|
| 106015 | 最初のパケットが SYN パケットではなかったため、TCP フローが拒否されました。 |
| 106023 | インターフェイスに付加される入力 ACL または出力 ACL によって拒否されたフロー。 |
| 106100 | ACL によって許可または拒否されたフロー。 |
| 302013 および 302014 | TCP 接続および削除。 |
| 302015 および 302016 | UDP 接続および削除。 |
| 302017 および 302018 | GRE 接続および削除。 |
| 302020 および 302021 | ICMP 接続および削除。 |
| 313001 | 脅威に対する防御 デバイスへの ICMP パケットが拒否されました。 |
| 313008 | 脅威に対する防御 デバイスへの ICMPv6 パケットが拒否されました。 |
| 710003 | 脅威に対する防御 への接続の試みが拒否されました。 |

### 例

次に、**show logging** コマンドの出力例を示します。

```
> show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: enabled
    Standby logging:disabled
    Debug-trace logging: disabled
    Console logging: level informational, 3962 messages logged
    Monitor logging: disabled
```

```
Buffer logging: disabled
Trap logging: level informational, facility 20, 20549 messages logged
    Logging to inside 10.2.5.3 tcp/50001 connected
Permit-hostdown state
History logging: disabled
Device ID: disabled
Mail logging: disabled
ASDM logging: disabled
```

（注） Syslog ロギングの有効な値は、enabled、disabled、disabled-blocking、および disabled-not blocking です。

次に、セキュア syslog サーバーが設定された **show logging** コマンドの出力例を示します。

```
> show logging
Syslog logging: disabled
    Facility:
    Timestamp logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: level debugging, 135 messages logged
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: list show _syslog, facility, 20, 21 messages logged
        Logging to inside 10.0.0.1 tcp/1500 SECURE
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging disabled
```

次に、**show logging queue** コマンドの出力例を示します。

```
> show logging queue
Logging Queue length limit: 512 msg(s)
0 msg(s) discarded due to queue overflow
0 msg(s) discarded due to memory allocation failure
Current 0 msgs on queue, 0 msgs most on queue
```

次に、**show logging message all** コマンドの出力例を示します。

```
> show logging message all
syslog 111111: default-level alerts (enabled)
syslog 101001: default-level alerts (enabled)
syslog 101002: default-level alerts (enabled)
syslog 101003: default-level alerts (enabled)
syslog 101004: default-level alerts (enabled)
syslog 101005: default-level alerts (enabled)
syslog 102001: default-level alerts (enabled)
syslog 103001: default-level alerts (enabled)
syslog 103002: default-level alerts (enabled)
syslog 103003: default-level alerts (enabled)
syslog 103004: default-level alerts (enabled)
syslog 103005: default-level alerts (enabled)
syslog 103011: default-level alerts (enabled)
syslog 103012: default-level informational (enabled)
```

次に、**show logging unified-client** コマンドの出力例を示します。

```
> show logging unified-client
Log client details:
 Name : Lina
 Id : 1331
 Init time : Fri Sep 7 07:20:14 2018
 Status : Registered
```

次に、**show logging unified-client statistics** コマンドの出力例を示します。

```
> show logging unified-client statistics
Log client details:
  Name                                          : Lina
  Id                                            : 1331
  Init time                                     : Fri Sep  7 07:20:14 2018
  Status                                        : Registered

Loggerd service up/down statistics:
  Service status                                : Up
  Instance-id                                   : 4602
  Last service down time                        : Wed Sep 12 05:17:43 2018

Log client register/unregister statistics:
  Total register messages Tx                    : 1222
  Total unregister messages Tx                  : 0
  Last register message Tx time                 : Wed Sep 12 05:40:16 2018
  Total register-ack messages Rx                : 39
  Last register-ack Rx time                     : Wed Sep 12 05:40:17 2018
  Total configuration sent messages Tx          : 14
  Number of configuration pushes                : 38

Heartbeat statistics:
  Last heartbeat Tx time                        : Wed Sep 12 06:38:33 2018
  Last Tx seqnum                                : 10019
  Total heartbeat Tx                            : 9981

Loggerd heartbeat statistics:
  Last heartbeat Rx time                        : Wed Sep 12 06:38:36 2018
  Last hearbeat Rx seqnum                       : 701
  Total heartbeat Rx                            : 5977
  Miss count                                    : 1

Log client data messages details:
  Syslogs Tx for ngfw-management                : 6554
  Syslogs Rx for data ports                     : 0
  Syslogs Tx drops for ngfw-management          : 0

Log client Control/Data channel statistics:
  Total control messages Tx                     : 11757
  Total service messages Rx                     : 98
  Total notify messages Rx                      : 6020
  Total data messages Rx                        : 0

Log-client error statistics:
  Register messages Tx                          : 2373
  Register-ack messages Rx                      : 5921
  Configuration push Tx                         : 1
  Heartbeat Tx                                  : 0
  Control channel Rx                            : 0
  Data channel Rx                               : 0
  Syslogs Rx for data ports                     : 0
```

# show mac-address-table

MAC アドレステーブルを表示するには、**show mac-address-table** コマンドを使用します。

**show mac-address-table** [*interface_name* | **count** | **static**]

## 構文の説明

| | |
|---|---|
| **count** | （任意）ダイナミックおよびスタティック エントリの合計数を一覧します。 |
| *interface_name* | （任意）MAC アドレステーブル エントリを表示するインターフェイス名を指定します。 |
| **static** | （任意）スタティック エントリのみを一覧します。 |

## コマンド デフォルト

インターフェイスを指定しない場合、すべてのインターフェイス MAC アドレス エントリが表示されます。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.1 | このコマンドが追加されました。 |
| 6.2 | Integrated Routing and Bridging を使用している場合のルーテッド ファイアウォール モードのサポートが追加されました。 |

### 例

次に、**show mac-address-table** コマンドの出力例を示します。

```
> show mac-address-table
interface    mac address     type      Time Left
-----------------------------------------------------
outside      0009.7cbe.2100  static    -
inside       0010.7cbe.6101  static    -
inside       0009.7cbe.5101  dynamic   10
```

次に、**show mac-address-table count** コマンドの出力例を示します。

```
> show mac-address-table count
Static     mac-address bridges (curr/max): 0/65535
Dynamic    mac-address bridges (curr/max): 103/65535
```

# show mac-learn

各インターフェイスに対してMACラーニングが有効か無効かを表示するには、**show mac-learn** コマンドを使用します。

**show mac-learn**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.1 | このコマンドが追加されました。 |
| 6.2 | Integrated Routing and Bridging を使用している場合のルーテッド ファイアウォール モードのサポートが追加されました。 |

## 使用上のガイドライン

デフォルトで、各インターフェイスは着信トラフィックの MAC アドレスを自動的に学習し、システムは対応するエントリを MAC アドレス テーブルに追加します。インターフェイスごとに MAC ラーニングをディセーブルにすることができます。

### 例

次に、**show mac-learn** コマンドの出力例を示します。

```
> show mac-learn
no mac-learn flood
interface                              mac learn
---------------------------------------------
 outside                                 enabled
 inside1_2                               enabled
 inside1_3                               enabled
 inside1_4                               enabled
 inside1_5                               enabled
 inside1_6                               enabled
 inside1_7                               enabled
 inside1_8                               enabled
 diagnostic                              enabled
 inside                                  enabled
```

# show managers

デバイス設定を管理している現在のマネージャを表示するには、**show managers** コマンドを使用します。

**show managers**

## 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。 |
| 7.2 | 複数のマネージャに対するサポートが追加されました。出力には、Management Center の表示名、識別子、および管理タイプ（設定または分析）が含まれるようになりました。 |

## 使用上のガイドライン

デバイス設定を管理するためにどのアプリケーションが定義されているかを確認するには、**show managers** コマンドを使用します。その後、Web ブラウザを使用してマネージャにログインできます。

**configure manager add** コマンドを使用してデバイスのリモートマネージャである Management Center を設定すると、出力にホストアドレスと登録ステータスが表示されます。登録キーおよび NAT ID は、登録が保留中の場合のみ表示されます。デバイスが高可用性ペアに登録されている場合、管理している両方の Management Center の情報が表示されます。デバイスが、スタック設定のセカンダリデバイスとして設定されている場合、管理している両方の Management Center、およびプライマリデバイスに関する情報が表示されます。

### 例

次に、Management Center リモートマネージャへの登録が完了している例を示します。

```
> show managers
Type                      : Manager
Host                      : 10.10.1.4
Display name              : 10.10.1.4
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
Management type           : Configuration
```

次に、ローカルマネージャである Device Manager が有効になっている例を示します。

```
> show managers
Managed locally.
```

次の例では、マネージャが現在設定されていないことを示しています。デバイスを設定する前に、configure manager add または configure manager local を使用してイネーブルにする必要があります。

```
> show managers
No managers configured.
```

次に、3 つのマネージャの例を示します。1 つは保留中で、現在は使用されていません。 1 つはメインの設定マネージャ（CDO）で、もう 1 つはオンプレミスの分析専用のマネージャです。

```
> show managers
Type                      : Manager
Host                      : 1.2.3.4
Display name              : 1.2.3.4
Identifier                : 1.2.3.4
Registration              : Pending

Type                      : Manager
Host                      : 10.10.1.4
Display name              : 10.10.1.4
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
Management type           : Configuration

Type                      : Manager
Host                      : 10.10.2.7
Display name              : 10.10.2.7
Identifier                : 6d3df56e-bf16-11ec-972b-b07a16ffdd03
Registration              : Completed
Management type           : Analytics
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure manager add** | リモートマネージャである Management Center を追加します。 |
| **configure manager delete** | 現在のマネージャを削除して、ノーマネージャモードを開始します。 |
| **configure manager local** | ローカルマネージャである Device Manager を有効にします。 |

# show memory

物理メモリの最大量とオペレーティングシステムで現在使用可能な空きメモリ量について要約を表示するには、**show memory** コマンドを使用します。

**show memory** ［**api** | **app-cache** | **binsize** *size* | **caller-address** | **detail** | **region** | **system** | **top-usage** ［*num*］］

## 構文の説明

| | |
|---|---|
| **api** | （オプション）システムに登録されている malloc スタック API を表示します。<br>メモリデバッグ機能（つまり、delay-free-poisoner、メモリトラッカー、またはメモリプロファイラ）がオンになっている場合、APIが出力に表示されます。 |
| **app-cache** | （オプション）アプリケーションごとのメモリ使用量を表示します。 |
| **binsize** *size* | （オプション）特定のバイナリサイズに割り当てられているチャンク（メモリブロック）の要約情報を表示します。バイナリサイズは**show memory detail** コマンド出力の「fragment size」列から取得されます。 |
| **caller-address** | **memory caller-address** コンフィギュレーションに関連する情報を表示します。 |
| **detail** | （任意）空きメモリおよび割り当て済みシステムメモリの詳細ビューを表示します。 |
| **region** | プロセスマップを表示します。 |
| **system** | デバイスの合計メモリ、使用中のメモリ、使用可能なメモリを表示します。 |
| **top-usage** [*num*] | **show memory detail** コマンドから割り当てられたフラグメントサイズの上位の数を表示します。必要に応じて、リストするバイナリサイズの数を 1 ー 64 の範囲で指定できます。デフォルトは 10 です。 |

## 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。 |
| 6.2.2 | **show memory** および **show memory detail** の出力が変更されました。 |

## 使用上のガイドライン

**show memory** コマンドで、物理メモリの最大量およびオペレーティングシステムで現在使用可能な空きメモリ量の要約を表示できます。メモリは必要に応じて割り当てられます。

SNMP を使用して **show memory** コマンドから情報を表示することもできます。

**show memory detail** の出力を **show memory binsize** コマンドとともに使用して、メモリリークをデバッグできます。

**show memory detail** コマンド出力は、要約、DMA メモリ、ヒープメモリの 3 つのセクションに分割できます。要約には、メモリ全体がどのように割り当てられているかが表示されます。DMA にリンクしていないメモリ、または予約されていないメモリは、ヒープと見なされます。Free Memory の値は、ヒープ内の未使用メモリです。Allocated memory in use の値は、割り当てられているヒープの量です。ヒープ割り当ての明細は、出力の後半で表示されます。予約メモリおよび DMA 予約メモリは、別のシステム プロセスおよび主に VPN サービスによって使用されます。

空きメモリは、空きメモリ ヒープと空きメモリ システムの 2 つの部分に分けられます。空きメモリ ヒープは、glibc ヒープ内の空きメモリ量です。glibc ヒープはオン デマンドで増減するため、空きヒープ メモリの量はシステムに残っている合計メモリを示しません。空きメモリ システムは、ASA に使用可能な空きメモリの量を表します。

予約メモリ（DMA）は、DMA のプールに予約されているメモリ量です。メモリ オーバーヘッドは、さまざまな実行プロセスの glibc オーバーヘッドおよびプロセス オーバーヘッドです。

割り当てられたメモリの統計情報の合計（バイト）列に表示される値は、**show memory detail** コマンド出力の実際の値（MEMPOOL_GLOBAL_SHARED POOL STATS）ではありません。

（注） MEMPOOL_GLOBAL_SHARED は、ブートアップ時にすべてのシステムメモリを取得しませんが、必要なときは常に、基盤となるオペレーティングシステムにメモリを要求します。同様に、大量のメモリが解放されたときは、システムにメモリが返されます。その結果、MEMPOOL_GLOBAL_SHARED のサイズは需要に応じて増減されて表示されます。割り当てを高速化するため、最小空きメモリ量は、MEMPOOL_GLOBAL_SHARED に残されます。

出力は、サイズ 49,152 のブロックが空きプールに割り当てられてから戻され、別のサイズ 131,072 のブロックが割り当てられていることを示します。この場合、空きメモリは 131,072-49,152=81,920 バイト単位で減少しますが、実際は 100,000 バイトずつ減少します（空きメモリの行を参照）。

```
> show memory detail
MEMPOOL_GLOBAL_SHARED POOL STATS:            MEMPOOL_GLOBAL_SHARED POOL STATS:
Non-mmapped bytes allocated =   1862270976   Non-mmapped bytes allocated =   1862270976
Number of free chunks       =           99   Number of free chunks       =          100
Number of mmapped regions   =            0   Number of mmapped regions   =            0
Mmapped bytes allocated     =            0   Mmapped bytes allocated     =            0
Max memory footprint        =   1862270976   Max memory footprint        =   1862270976
Keepcost                    =   1762019304   Keepcost                    =   1761869256
Max contiguous free mem     =   1762019304   Max contiguous free mem     =   1761869256
Allocated memory in use     =    100133944   Allocated memory in use     =    100233944
Free memory                 =   1762137032   Free memory                 =   1762037032
----- fragmented memory statistics -----     ----- fragmented memory statistics -----
 fragment size       count          total      fragment size       count          total
    (bytes)                       (bytes)        (bytes)                       (bytes)
---------------  ----------  -------------- ---------------  ----------  --------------

        32768            1          33176           32768            1          33176
                                                     49152            1          50048
```

```
   1762019304             1     1762019304*     1761869256             1     1761869256*
----- allocated memory statistics -----      ----- allocated memory statistics -----
 fragment size       count          total     fragment size       count          total
    (bytes)                        (bytes)       (bytes)                        (bytes)
---------------  ----------  -------------- ----------------  ----------  --------------

        49152            10         491520           49152             9         442368
        65536           125        8192000           65536           125        8192000
        98304             3         294912           98304             3         294912
       131072            18        2359296          131072            19        2490368
```

次の出力では、131,072 の代わりにサイズ 150,000 のブロックが割り当てられたことを確認します。

```
> show memory binsize 131072
MEMPOOL_DMA pool bin stats:
MEMPOOL_GLOBAL_SHARED pool bin stats:
pc = 0x8eda524, size = 150000   , count = 1
pc = 0x8f08054, size = 163904   , count = 1
pc = 0x846e477, size = 139264   , count = 1
pc = 0x8068691, size = 393216   , count = 3
pc = 0x8eea09b, size = 131072   , count = 1
pc = 0x88ca830, size = 141212   , count = 1
pc = 0x9589e93, size = 593580   , count = 4
pc = 0x9589bd2, size = 616004   , count = 4
pc = 0x8f2e060, size = 327808   , count = 2
pc = 0x8068284, size = 182000   , count = 1

0x8eda524 <logger_buffer_init_int+148 at syslog/main.c:403>
```

**show memory detail** コマンドの出力に合計バイト数の概算が示されるのは仕様によるものです。これには次の 2 つの理由があります。

- 各フラグメントサイズに対して、すべてのフラグメントの合計を取得する必要があると、単一のフラグメントサイズの割り当て数が非常に多くなることで、パフォーマンスに影響する可能性があり、かつ、正確な値を取得するには、数千ものチャンクを実行することが必要になります。
- 各 binsize に対して、二重にリンクされた割り当てリスト全体を確認する必要があり、割り当ては多数存在する可能性があります。この場合、CPU を長期間占有できないため、割り当てを定期的に停止する必要があります。割り当てを再開した後、他のプロセスがメモリを割り当てまたは割り当て解除したことによって、メモリ状態が変化している可能性があります。このため、合計バイト列には、実際の値ではなく近似値が示されます。

### 例

次に、**show memory** コマンドの出力例を示します。

```
> show memory
Free memory:        2986716635 bytes (64%)
Used memory:        1646723072 bytes (36%)
-------------      ------------------
Total memory:       4633439707 bytes (100%)
```

```
Note: Free memory is the free system memory. Additional memory may
      be available from memory pools internal to the ASA process.
      Use 'show memory detail' to see this information, but use it
      with care since it may cause CPU hogs and packet loss under load.
>
```

次に、システムレベルのメモリ使用状況を表示する例を示します。

```
> show memory system
             total       used       free     shared    buffers     cached
Mem:       3982640    3014544     240200          0     159932     567964
-/+ buffers/cache:    3014544     968096
Swap:      3998716     137704    3861012
```

次に、**show memory detail** コマンドの出力例を示します。

```
> show memory detail

Heap Memory:
   Free Memory:
      Heapcache Pool:                        3804848 bytes (  0% )
      Global Shared Pool:                   67372768 bytes (  1% )
      System:                             2986716635 bytes ( 64% )
   Used Memory:
      Heapcache Pool:                      308670800 bytes (  7% )
      Global Shared Pool:                       6432 bytes (  0% )
      Reserved (Size of DMA Pool):         499122176 bytes ( 11% )
      Reserved for messaging:                2097152 bytes (  0% )
      System Overhead:                     765648896 bytes ( 17% )
-----------------------------------     ----------------
   Total Memory:                       4633439707 bytes ( 100% )

Warning:  The information reported here is computationally expensive to
          determine, and may result in CPU hogs and performance impact.

------------------------------------------------------------------------
MEMPOOL_MSGLYR POOL STATS:

Non-mmapped bytes allocated =      2097152
Number of free chunks       =            1
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =      2097152
Keepcost                    =      2092768
Max contiguous free mem     =      2092768
Allocated memory in use     =         4288
Free memory                 =      2092864

----- fragmented memory statistics -----

(...Remaining output truncated...)
```

次に、バイナリサイズ 8192 に割り当てられたチャンクの例を示します。

```
> show memory binsize 8192
MEMPOOL_HEAPCACHE_0 pool bin stats:
pc = 0x7efc3f80e508, size = 773406   , count = 92
pc = 0x7efc3e3c5013, size = 189152   , count = 23
pc = 0x7efc405df64f, size = 287036   , count = 32
```

```
pc = 0x7efc3f9ef622, size = 8128     , count = 1
pc = 0x7efc3f4fd5f5, size = 871744   , count = 106
pc = 0x7efc3f4fd8b7, size = 82240    , count = 10
pc = 0x7efc3f18c3e6, size = 20272    , count = 2
pc = 0x7efc3f557139, size = 8192     , count = 1
pc = 0x7efc3e3f1697, size = 8344     , count = 1
pc = 0x7efc3e0506f6, size = 8192     , count = 1
MEMPOOL_DMA pool bin stats:
pc = 0x7efc3e1cca68, size = 10240    , count = 1
MEMPOOL_GLOBAL_SHARED pool bin stats:
```

次に、**show memory api** コマンドの出力例を示します。これは、メモリトラッカーおよび Delayed-Free-Poisoner メモリ機能がアクティブであることを示しています。

```
> show memory api
Resource Manager (0) ->
Tracking (0) ->
Delayed-free-poisoner (0) ->
Core malloc package (0)
```

次に、システムレベルのメモリ使用状況を表示する例を示します。

```
> show memory system
             total       used       free     shared    buffers     cached
Mem:       3982640    3014544     240200          0     159932     567964
-/+ buffers/cache:    3014544     968096
Swap:      3998716     137704    3861012
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show memory profile** | 脅威に対する防御のメモリ使用状況（プロファイリング）に関する情報を表示します。 |

# show memory all

物理メモリの最大量と Lina と Snort の両方のオペレーティングシステムで現在使用可能な空きメモリ量について要約を表示するには、**show memory all** コマンドを使用します。

**show memory all**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | このコマンドが導入されました。 |

## 使用上のガイドライン

**show memory all** コマンドで、物理メモリの最大量およびオペレーティングシステムで現在使用可能な空きメモリ量の要約を表示できます。メモリは必要に応じて割り当てられます。

```
> show memory all
Data Path:
Free memory:        3161408675 bytes (72%)
Used memory:        1203826208 bytes (28%)
-------------     ------------------
Total memory:       4365234883 bytes (100%)
Inspection Engine:
Free memory:                  0 bytes ( 0%)
Used memory:                  0 bytes ( 0%)
-------------     ------------------
Total memory:                 0 bytes (100%)
System:
Free memory:                  0 bytes ( 0%)
Used memory:                  0 bytes ( 0%)
-------------     ------------------
Total memory:                 0 bytes (100%)
```

# show memory delayed-free-poisoner

**memory delayed-free-poisoner** キューの使用状況の要約を表示するには、**show memory delayed-free-poisoner** コマンドを使用します。

**show memory delayed-free-poisoner**

## 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

この機能を有効にするには、**memory delayed-free-poisoner enable** コマンドを使用します。キューおよび統計情報をクリアするには、**clear memory delayed-free-poisoner** コマンドを使用します。

### 例

次に、**show memory delayed-free-poisoner** コマンドの出力例を示します。

```
> memory delayed-free-poisoner enable
> show memory delayed-free-poisoner
delayed-free-poisoner settings:
 delayed-free-poisoner threshold 100
 delayed-free-poisoner desired-fragment-size 102400
 delayed-free-poisoner desired-fragment-count 16
 delayed-free-poisoner watchdog-percent 50
delayed-free-poisoner statistics:
                  136064:  current memory in queue
                     500:  current queue length
                       0:  frees dequeued
                     280:  frees not queued for size
                       0:  frees not queued for locking
                       0:  successful validate runs
                       0:  aborted validate runs
                   never:  time of last validate
                       0:  threshold defragment operations
                       0:  size and/or count defragment operations
                       0:  watchdog-aborts
```

# show memory logging

メモリ使用状況のロギングを表示するには、**show memory logging** コマンドを使用します。

**show memory logging** ［**wrap** | **brief** | **include** ［*option*］］

## 構文の説明

| | |
|---|---|
| **brief** | （オプション）要約されたメモリ使用状況のロギングを表示します。 |
| **include** *option* | （任意）指定されたフィールドのみを出力に含めます。フィールドのキーワードは任意の順序で指定できますが、必ず次の順序で表示されます。オプションを含めない場合、出力は**include**の代わりに**brief**を指定した場合と同じになります。<br>• **process**<br>• **time**<br>• **operator**（free/malloc/など）<br>• **address**<br>• **size**<br>• **callers**<br>出力形式は、次のとおりです。<br>process=[XXX] time=[XXX] oper=[XXX] address=0xXXXXXXXX size=XX @ XXXXXXXX<br>XXXXXXXX XXXXXXXX XXXXXXXX<br>最大4つの発信者アドレスが表示されます。例に示すように、処理の種類（番号）が出力に列挙されます。 |
| **wrap** | （オプション）メモリ使用状況のロギングのラップされたデータを表示します。これらの重複するデータが表示されたり保存されたりしないように、重複するデータは、このコマンドの入力後に消去されます。 |

## 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

**show memory logging** コマンドを使用して、メモリログ情報を表示します。最初に、**memory logging** コマンドを使用してこのロギングを有効にする必要があります。

### 例

次に、**show memory logging** コマンドの出力例を示します。

```
> memory logging 1024
> show memory logging
Number of free                          203989
Number of calloc                        83703
Number of malloc                        120286
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 407978
Buffer size: 1024 (73816 x2 bytes)
process=[cli_xml_server] time=[19:23:42.030] oper=[malloc] addr=0x00007efc358373c0 size=72

@ 0x00007efc3f8e9404 0x00007efc3f80e508 0x00007efc3f4d3cea 0x00007efc3e037f0c
process=[cli_xml_server] time=[19:23:42.030] oper=[free] addr=0x00007efc358373c0 size=72

@ 0x00007efc3f80e9c0 0x00007efc3f4d3fb8 0x00007efc3e037fb0 0x00007efc3f4d537d
(...Remaining output truncated...)
```

次に、**show memory logging brief** コマンドの出力例を示します。

```
> show memory logging brief
Number of free                          223195
Number of calloc                        91624
Number of malloc                        131572
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 446391
Buffer size: 1024 (73816 x2 bytes)
```

### 関連コマンド

| Command | 説明 |
|---|---|
| **memory logging** | メモリ ロギングをイネーブルにします。 |

# show memory profile

脅威に対する防御デバイスのメモリ使用状況（プロファイリング）に関する情報を表示するには、**show memory profile** コマンドを使用します。

**show memory profile** ［**status** | **peak** ［**detail** | **collated**］］

## 構文の説明

| | |
|---|---|
| **collated** | （任意）表示されるメモリ情報を整形します。 |
| **detail** | （任意）メモリの詳細情報を表示します。 |
| **peak** | （オプション）「使用中」のバッファではなく、ピーク キャプチャ バッファを表示します。 |
| **status** | （任意）メモリ プロファイリングとピーク キャプチャ バッファの現在の状態を表示します。 |

## 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

**show memory profile** コマンドを使用して、メモリ使用状況レベルとメモリリークをトラブルシューティングします。プロファイリングが停止されている場合でも、プロファイルバッファの内容を表示できます。プロファイリングを開始すると、バッファは自動的にクリアされます。

（注） メモリプロファイリングを有効にすると、脅威に対する防御デバイスのパフォーマンスが一時的に低下する場合があります。

### 例

次に、**show memory profile** コマンドの出力例を示します。

```
> show memory profile
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 0
```

**show memory profile detail** コマンドの出力は、6 つのデータ列と 1 つのヘッダー列に区分され、左揃えで表示されています。ヘッダー列には、先頭のデータ列に対応するメモリ バケットのアドレスが表示されます（16 進数）。データ自体は、バケット アドレスにあるテキストまたはコードが保持しているバイト数です。データ カラム内のピリオド（.）は、このバケットのテキストによってメモリが保持されていないことを意味します。行内の他のカラムは、前のカラムから増分値に従って増分したバケット

アドレスを表しています。たとえば、最初の行の先頭のデータ カラムのアドレス バケットは 0x001069e0 です。最初の行の 2 番めのデータ カラムのアドレス バケットは 0x001069e4 で、以降も同様に増分していきます。通常は、ヘッダー カラムにあるアドレスが次のバケット アドレスです。これは、前の行の最後のデータ カラムのアドレスに増分値を加算したものです。使用状況が含まれない行は表示されません。このような非表示になる行が、複数連続していることもあります。この場合は、ヘッダー カラムに 3 個のピリオド（...）で示されます。

次に、**show memory profile peak detail** コマンドの出力例を示します。このコマンドでは、ピークキャプチャバッファと、対応するバケットアドレスにあるテキスト/コードが保持しているバイト数を表示します。

```
> show memory profile peak detail
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
...
0x001069e0 . 24462 . . . .
...
0x00106d88 . 1865870 . . . .
...
0x0010adf0 . 7788 . . . .
...
0x00113640 . . . . 433152 .
...
0x00116790 2480 . . . . .
(...output truncated...)
```

次に、**show memory profile peak collated** コマンドの出力例を示します。

```
> show memory profile peak collated
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
24462 0x001069e4
1865870 0x00106d8c
7788 0x0010adf4
433152 0x00113650
2480 0x00116790
<More>
```

次に、**show memory profile peak** コマンドの出力例を示します。このコマンドでは、ピークキャプチャバッファを表示します。

```
> show memory profile peak
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
```

次に、**show memory profile status** コマンドの出力例を示します。このコマンドでは、メモリプロファイリングとピークキャプチャバッファの現在の状態を表示します。

```
> show memory profile status
InUse profiling: ON
Peak profiling: OFF
Memory used by profile buffers: 11518860 bytes
```

```
Profile:
0x00100020-0x00bfc3a8(00000004)
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **memory profile enable** | メモリ使用状況（メモリ プロファイリング）のモニタリングをイネーブルにします。 |
| **memory profile text** | プロファイルするメモリのプログラム テキスト範囲を設定します。 |
| **clear memory profile** | メモリ プロファイリング機能によって保持されるメモリ バッファをクリアします。 |

# show memory tracking

ツールによって追跡される、現在割り当て済みのメモリを表示するには、**show memory tracking** コマンドを実行します。

**show memory tracking** ［**address** | **detail** | **dump** *tracked_address*］

## 構文の説明

| | |
|---|---|
| **address** | （任意）アドレスごとのメモリのトラッキングを表示します。 |
| **detail** | （オプション）内部メモリのトラッキング状態を表示します。 |
| **dump** *tracked_address* | （オプション）指定されたメモリトラッキングアドレス（0 ー 4294967295）のダンプを表示します。 |

## 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

**show memory tracking** コマンドを使用して、ツールにより追跡されている、現在割り当て済みのメモリを表示します。この情報を表示するには、**memory tracking enable** を使用する必要があります。

### 例

次に、**show memory tracking** コマンドの出力例を示します。

```
> show memory tracking
memory tracking by caller:
  bytes-threshold:        0
  allocates-by-threshold: 0
         65406 bytes from    49 allocates by 0x00007efc3f80e508
          3000 bytes from     1 allocates by 0x00007efc3f4e1278
           159 bytes from     1 allocates by 0x00007efc3fe9ee13
            17 bytes from     1 allocates by 0x00007efc3fe9ef4e
```

次に、**show memory tracking address** コマンドの出力例を示します。

```
> show memory tracking address
memory tracking by caller:
  bytes-threshold:        0
  allocates-by-threshold: 0
         58918 bytes from    49 allocates by 0x00007efc3f80e508
          3000 bytes from     1 allocates by 0x00007efc3f4e1278
           167 bytes from     1 allocates by 0x00007efc3fe9ee13
            17 bytes from     1 allocates by 0x00007efc3fe9ef4e
memory tracking address pool:
            32 byte region @ 0x00007efc358a06e0 allocated by 0x00007efc3f80e508
            96 byte region @ 0x00007efc351d0880 allocated by 0x00007efc3f80e508
           896 byte region @ 0x00007efc35f121c0 allocated by 0x00007efc3f80e508
          8192 byte region @ 0x00007efc35832e20 allocated by 0x00007efc3f80e508
```

```
  96 byte region @ 0x00007efc30483910 allocated by 0x00007efc3f80e508
  88 byte region @ 0x00007efc359e3960 allocated by 0x00007efc3f80e508
1036 byte region @ 0x00007efc35f04680 allocated by 0x00007efc3f80e508
  76 byte region @ 0x00007efc36024890 allocated by 0x00007efc3f80e508
  24 byte region @ 0x00007efc35fd48a0 allocated by 0x00007efc3f80e508
  32 byte region @ 0x00007efc35f04ad0 allocated by 0x00007efc3f80e508
  34 byte region @ 0x00007efc35e54e00 allocated by 0x00007efc3f80e508
8192 byte region @ 0x00007efc35834e70 allocated by 0x00007efc3f80e508
  40 byte region @ 0x00007efc36005cc0 allocated by 0x00007efc3f80e508
  11 byte region @ 0x00007efc360061e0 allocated by 0x00007efc3f80e508
  76 byte region @ 0x00007efc357a6dd0 allocated by 0x00007efc3f80e508
1024 byte region @ 0x00007efc358574f0 allocated by 0x00007efc3f80e508
  88 byte region @ 0x00007efc365b7ef0 allocated by 0x00007efc3f80e508
  56 byte region @ 0x00007efc365b7f90 allocated by 0x00007efc3f80e508
 168 byte region @ 0x00007efc365b8210 allocated by 0x00007efc3f80e508
 112 byte region @ 0x00007efc365b8300 allocated by 0x00007efc3f80e508
 112 byte region @ 0x00007efc365b83c0 allocated by 0x00007efc3f80e508
  16 byte region @ 0x00007efc365b8560 allocated by 0x00007efc3f80e508
 167 byte region @ 0x00007efc365b85c0 allocated by 0x00007efc3fe9ee13
2048 byte region @ 0x00007efc357a8610 allocated by 0x00007efc3f80e508
  88 byte region @ 0x00007efc35728be0 allocated by 0x00007efc3f80e508
  88 byte region @ 0x00007efc357a8e60 allocated by 0x00007efc3f80e508
4112 byte region @ 0x00007efc35fe90c0 allocated by 0x00007efc3f80e508
  17 byte region @ 0x00007efc365b95a0 allocated by 0x00007efc3fe9ef4e
  72 byte region @ 0x00007efc365b9600 allocated by 0x00007efc3f80e508
  72 byte region @ 0x00007efc365b9690 allocated by 0x00007efc3f80e508
  72 byte region @ 0x00007efc365b9720 allocated by 0x00007efc3f80e508
  40 byte region @ 0x00007efc365b97b0 allocated by 0x00007efc3f80e508
  24 byte region @ 0x00007efc365b9820 allocated by 0x00007efc3f80e508
   2 byte region @ 0x00007efc365b9880 allocated by 0x00007efc3f80e508
  76 byte region @ 0x00007efc35ff9aa0 allocated by 0x00007efc3f80e508
 776 byte region @ 0x00007efc35f19df0 allocated by 0x00007efc3f80e508
 512 byte region @ 0x00007efc3585a0a0 allocated by 0x00007efc3f80e508
 936 byte region @ 0x00007efc357aaea0 allocated by 0x00007efc3f80e508
  24 byte region @ 0x00007efc357ab290 allocated by 0x00007efc3f80e508
 568 byte region @ 0x00007efc3592bc40 allocated by 0x00007efc3f80e508
 512 byte region @ 0x00007efc35e5c8a0 allocated by 0x00007efc3f80e508
  40 byte region @ 0x00007efc35f2cae0 allocated by 0x00007efc3f80e508
1665 byte region @ 0x00007efc359fcda0 allocated by 0x00007efc3f80e508
 168 byte region @ 0x00007efc34fccf60 allocated by 0x00007efc3f80e508
 112 byte region @ 0x00007efc35ffd0e0 allocated by 0x00007efc3f80e508
4112 byte region @ 0x00007efc356bd340 allocated by 0x00007efc3f80e508
8208 byte region @ 0x00007efc3643d3e0 allocated by 0x00007efc3f80e508
 386 byte region @ 0x00007efc359fd470 allocated by 0x00007efc3f80e508
  72 byte region @ 0x00007efc35e4d570 allocated by 0x00007efc3f80e508
8208 byte region @ 0x00007efc359fd840 allocated by 0x00007efc3f80e508
4112 byte region @ 0x00007efc3592ded0 allocated by 0x00007efc3f80e508
3000 byte region @ 0x00007efc357ee5c0 allocated by 0x00007efc3f4e1278
  32 byte region @ 0x00007efc351be6d0 allocated by 0x00007efc3f80e508
  16 byte region @ 0x00007efc359de790 allocated by 0x00007efc3f80e508
1036 byte region @ 0x00007efc3524f080 allocated by 0x00007efc3f80e508
 512 byte region @ 0x00007efc357ff290 allocated by 0x00007efc3f80e508
 360 byte region @ 0x00007efc357ef360 allocated by 0x00007efc3f80e508
  24 byte region @ 0x00007efc357ff4e0 allocated by 0x00007efc3f80e508
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear memory tracking** | 現在収集されているすべての情報をクリアします。 |
| **memory tracking** | メモリの追跡を有効にします。 |

# show memory webvpn

WebVPN のメモリ使用状況の統計情報を生成するには、**show memory webvpn** コマンドを使用します。

**show memory webvpn** ［**allobjects** | **blocks** | **dumpstate** *filename* | **pools** | **usedobjects**］
**show memory webvpn profile** ［**clear** | **dump** *filename* | **start** | **stop**］

## 構文の説明

| | |
|---|---|
| **allobjects** | プール、ブロック、すべての使用済みオブジェクトおよび解放済みオブジェクトについて、WebVPN メモリ使用量の詳細を表示します。 |
| **blocks** | メモリ ブロックについて、WebVPN メモリ使用量の詳細を表示します。 |
| **clear** | WebVPN メモリ プロファイルをクリアします。 |
| **dump** *filename* | WebVPNメモリプロファイルを指定したファイルに出力します。ファイル名には、 disk0:、disk1:、flash:、ftp:、tftp: などの場所を含める必要があります。 |
| **dumpstate** *filename* | WebVPNメモリ状態を指定したファイルに出力します。ファイル名には、 disk0:、disk1:、flash:、ftp:、tftp: などの場所を含める必要があります。 |
| **pools** | メモリ プールについて、WebVPNメモリ使用量の詳細を表示します。 |
| **profile** | WebVPN メモリ プロファイルを収集して、ファイルに出力します。 |
| **start** | WebVPN メモリ プロファイルの収集を開始します。 |
| **stop** | WebVPN メモリ プロファイルの収集を停止します。 |
| **usedobjects** | 使用済みオブジェクトについて、WebVPNメモリ使用量の詳細を表示します。 |

## 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、**show memory webvpn allobjects** コマンドの出力例を示します。

```
> show memory webvpn allobjects
Arena 0x36b14f8 of 4094744 bytes (61 blocks of size 66048), maximum 134195200
130100456 free bytes (97%; 1969 blocks, zone 0)
Arena is dynamically allocated, not contiguous
```

```
Features: GroupMgmt: SET, MemDebugLog: unset
Pool 0xd719a78 ("cp_entries" => "pool for class cpool entries") (next 0xd6d91d8)
Size: 66040 (1% of current, 0% of limit)
Object frame size: 32
Load related limits: 70/50/30
Callbacks: !init/!prep/!f2ca/!dstr/!dump
Blocks in use:
Block 0xd719ac0..0xd729cb8 (size 66040), pool "cp_entries"
Watermarks { 0xd7098f8 <= 0xd70bb60 <= 0xd719a60 } = 57088 ready
Block size 66040 not equal to arena block 66048 (realigned-to-8)
Used objects: 0
Top allocated count: 275
Objects dump:
0. Object 0xd70bb50: FREED (by "jvclass_pool_free")
```

# show mfib

マルチキャスト転送情報ベースの情報を表示するには、**show mfib** コマンドを使用します。

**show mfib** ［*source_or_group* ［*group*］］［**cluster** | **count** | **verbose**］
**show mfib** ［**active** ［*kbps*］ | **cluster-stats** | **interface** | **status** | **summary**］
**show mfib reserved** ［**active** ［*kbps*］ | **cluster** | **count** | **verbose**］

## 構文の説明

| | |
|---|---|
| [**active** [*kbps*] | （任意）アクティブなマルチキャスト送信元を表示します。（任意）kbps を指定して、表示対象をこの値以上のマルチキャストストリームに限定できます。デフォルトは 4 で、値の範囲は 0 ～ 4294967295 です。 |
| **cluster** | （オプション）MFIB のエポック番号と現在のタイマー値を表示します。送信元とグループの両方を指定する場合、**cluster** は指定できません。 |
| **cluster-stats** | （任意）MFIB クラスタ同期統計情報を表示します。 |
| **count** | （任意）MFIB ルートおよびパケットカウントデータを表示します。このコマンドは、パケットのドロップに関する統計情報を表示します。 |
| **interface** | （任意）MFIB プロセスに関連するインターフェイスのパケット統計情報を表示します。 |
| **reserved** | （任意）予約済みグループの MFIB エントリ（224.0.0.0 ～ 224.0.0.225 の範囲）を表示します。 |
| *source_or_group* [*group*] | （任意）送信元またはグループの IPv4、IPv6、または名前。両方を指定する場合は、最初に送信元を指定します。送信元アドレスはユニキャストアドレスです。 |
| **status** | （任意）一般的な MFIB 設定と動作ステータスを表示します。 |
| **summary** | （任意）MFIB のエントリとインターフェイスの数に関する要約情報を表示します。 |
| **verbose** | （任意）転送エントリおよびインターフェイスに関する詳細情報を表示します。 |

## コマンド デフォルト

任意の引数を指定しないと、すべてのグループの情報が表示されます。

## 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、**show mfib** コマンドの出力例を示します。

```
> show mfib 224.0.2.39
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

次に、**show mfib verbose** コマンドの出力例を示します。

```
> show mfib verbose
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.1.40) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/8) Flags: K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

次に、**show mfib count** コマンドの出力例を示します。

```
> show mfib count
MFIB global counters are :
* Packets [no input idb] : 0
* Packets [failed route lookup] : 0
* Packets [Failed idb lookup] : 0
* Packets [Mcast disabled on input I/F] : 0
```

次に、**show mfib active** コマンドの出力例を示します。出力には、PPS のレートに正または負の数値が表示されます。負の数値は、RPF パケットが失敗した場合、またはルータが発信インターフェイス（OIF）リストを使用して RPF パケットをモニターしている場合に表示されます。このような現象が発生している場合は、マルチキャスト ルーティングに問題がある可能性があります。

```
> show mfib active
Active IP Multicast Sources - sending >= 4 kbps

Group: 224.2.127.254, (sdr.cisco.com)
   Source: 192.168.28.69 (mbone.ipd.anl.gov)
     Rate: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)
```

```
Group: 224.2.201.241, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)

Group: 224.2.207.215, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
```

次に、**show mfib interface** コマンドの出力例を示します。

```
> show mfib interface
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
MFIB interface       status    CEF-based output
                             [configured,available]
           Ethernet0   up    [        no,       no]
           Ethernet1   up    [        no,       no]
           Ethernet2   up    [        no,       no]
```

次に、**show mfib status** コマンドの出力例を示します。

```
> show mfib status
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
```

次に、**show mfib summary** コマンドの出力例を示します。

```
> show mfib summary
IPv6 MFIB summary:

  54     total entries [1 (S,G), 7 (*,G), 46 (*,G/m)]

  17     total MFIB interfaces
```

次に、**show mfib reserved** コマンドの出力例を示します。

```
> show mfib reserved
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.0.0/4) Flags: C K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/24) Flags: K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.1) Flags:
   Forwarding: 0/0/0/0, Other: 0/0/0
   outside Flags: IC
   dmz Flags: IC
   inside Flags: IC
```

関連コマンド

| Command | 説明 |
|---|---|
| **clear mfib counters** | MFIB ルータ パケット カウンタをクリアします。 |
| **show mroute active** | アクティブなマルチキャスト ストリームを表示します。 |
| **show mroute count** | マルチキャスト ルート カウンタを表示します。 |
| **show mroute summary** | マルチキャスト ルーティング テーブルの要約情報を表示します。 |

# show mgcp

Media Gateway Control Protocol（MGCP）の設定およびセッション情報を表示するには、**show mgcp** コマンドを使用します。

**show mgcp {commands** | **sessions**} [**detail**]

## 構文の説明

| | |
|---|---|
| **commands** | コマンド キュー内の MGCP コマンドの数を表示します。 |
| **detail** | （任意）各コマンドまたはセッションに関する追加情報を出力に表示します。 |
| **sessions** | 既存の MGCP セッションの数を表示します。 |

## 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

MGCP情報を表示するには、MGCP トラフィックを検査する必要があります。MGCP トラフィックを検査するには、Management Center で FlexConfig を設定する必要があります。

### 例

次に、**show mgcp** コマンドオプションの例を示します。

```
> show mgcp commands
1 in use, 1 most used, 200 maximum allowed
CRCX, gateway IP: host-pc-2, transaction ID: 2052, idle: 0:00:07

> show mgcp commands detail
1 in use, 1 most used, 200 maximum allowed
CRCX, idle: 0:00:10
       Gateway IP | host-pc-2
       Transaction ID  2052
       Endpoint name | aaln/1
       Call ID | 9876543210abcdef
       Connection ID |
       Media IP | 192.168.5.7
       Media port | 6058

> show mgcp sessions
1 in use, 1 most used
Gateway IP host-pc-2, connection ID 6789af54c9, active 0:00:11

> show mgcp sessions detail
1 in use, 1 most used
Session active 0:00:14
       Gateway IP | host-pc-2
       Call ID | 9876543210abcdef
       Connection ID | 6789af54c9
       Endpoint name | aaln/1
```

```
Media lcl port  6166
Media rmt IP | 192.168.5.7
Media rmt port  6058
```

# show mini-coredump status

ミニコアダンプ生成の設定を表示するには、**show mini-coredump status** コマンドを入力します。

**show mini-coredump status**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | このコマンドが導入されました。 |

## 使用上のガイドライン

ミニコアダンプの生成はデフォルトで有効になっています。

Snort 3 プロセスは、そのマルチスレッドの性質により、巨大なコアファイルをダンプします。これらのダンプは、ハードディスクに書き込まれるまでに時間がかかります。コアが書き込まれて新しいプロセスが開始されるまで、Snort のトラフィック検査は中断されます。ミニコアダンプを作成すると、時間の遅延が回避されます。ミニコアダンプには、デバッグに役立つスタックとメモリ値の重要な詳細が含まれています。

### 例

次に、ミニコアダンプの生成が無効になっている場合の例を示します。

```
> show mini-coredump status
minicoredump feature status : Disabled
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure mini-coredump** | ミニコアダンプの生成を有効または無効にします。 |

# show mode

システムのセキュリティ コンテキスト モードを表示するには、**show mode** コマンドを使用します。

**show mode**

## 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

脅威に対する防御 デバイスは、シングルコンテキストのみをサポートしています。マルチ コンテキスト モードはサポートされていません。

### 例

次に、セキュリティ コンテキスト モードを表示する例を示します。

```
> show mode
Security context mode: single
```

# show model

デバイスのハードウェアモデルを表示するには、**show model** コマンドを使用します。

**show model**

## 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、デバイスモデルの例を示します。

```
> show model
Cisco ASA5516-X Threat Defense
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show serial-number** | デバイスのシリアル番号を表示します。 |
| **show version** | ソフトウェアおよびその他のデバイスのバージョン情報を表示します。 |

# show module

脅威に対する防御 デバイスにインストールされているモジュールに関する情報を表示するには、ユーザー EXEC モードで **show module** コマンドを使用します。

**show module** ［*id* ［**details** | **recover** | **log console**］］ | **all**］

## 構文の説明

| | |
|---|---|
| **all** | （デフォルト）すべてのモジュールの情報を表示します。これはデフォルトです。 |
| **details** | （オプション）モジュールのリモート管理設定などの追加情報を表示します。 |
| *id* | モジュール ID を指定します。パラメータなしで show module を使用すると、使用可能なスロット番号（通常は 0 と 1）が表示されます。 |
| **log console** | （オプション）モジュールのログ情報を表示します。このオプションは、すべてのモジュールで有効なわけではありません。 |
| **recover** | （オプション）モジュール復旧の設定を表示します。 |

## コマンド デフォルト

デフォルトでは、すべてのモジュールの情報が表示されます。

## 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

このコマンドは、脅威に対する防御デバイスにインストールされているモジュールに関する情報を表示します。脅威に対する防御 自体もディスプレイにモジュールとして表示されます（スロット 0）。デバイスが追加モジュールをサポートするかどうかは、デバイスモデルによって異なります。

**show module details** コマンドの出力は、インストールされているモジュールによって異なります。

ソフトウェアモジュールを設定できるモデルの場合、**show module** コマンドは可能なすべてのモジュールを一覧表示します。ステータス情報は、これらの 1 つがインストールされているかどうかを表示します。

### 例

次に、脅威に対する防御 ソフトウェアを実行している ASA 5516-X の出力例を示します。脅威に対する防御 はソフトウェアモジュールをサポートしていないため、このデバイスでは通常、スロット 1 は不明になります。

```
> show module
```

```
Mod  Card Type                                    Model              Serial No.
---- -------------------------------------------- ------------------ -----------
   0 ASA 5516-X with FirePOWER services, 8GE, AC, ASA5516            JAD1939056I
   1 Unknown                                      N/A                JAD1939056I

Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   0 84b2.61b1.92be to 84b2.61b1.92c6  1.0          1.1.3        97.1(0)60
   1 84b2.61b1.92bd to 84b2.61b1.92bd  N/A          N/A

Mod  SSM Application Name           Status           SSM Application Version
---- ------------------------------ ---------------- --------------------------
   1 Unknown                        No Image Present Not Applicable

Mod  Status             Data Plane Status     Compatibility
---- ------------------ --------------------- -------------
   0 Up Sys             Not Applicable
   1 Unresponsive       Not Applicable
```

次の表に、出力に表示される各フィールドを示します。

**表 *46 : show module* の出力フィールド**

| フィールド | 説明 |
|---|---|
| Mod | モジュール番号、0 または 1。 |
| Card Type | カードのタイプ。モジュール0に表示されるデバイスの場合、タイプはプラットフォーム モデルです。スロット 1 の場合は、追加のモジュールです（存在する場合）。 |
| モデル | このモジュールのモデル番号。 |
| Serial No. | シリアル番号。 |
| MAC Address Range | このモジュールにおけるインターフェイスの MAC アドレス範囲。 |
| Hw Version | ハードウェアのバージョン。 |
| Fw Version | ファームウェアのバージョン。 |
| Sw Version | ソフトウェアのバージョン。これは 脅威に対する防御 バージョンではありません。脅威に対する防御 ソフトウェアのコンポーネントである ASA ソフトウェアのバージョンです。**show version** コマンドを使用して 脅威に対する防御 のバージョンを確認します。 |
| SSM Application Name | セキュリティ サービス モジュールで実行されているアプリケーションの名前。 |
| SSM Application Version | セキュリティ サービス モジュールで実行されているアプリケーションのバージョン。 |

| フィールド | 説明 |
| --- | --- |
| Status | モジュール 0 のデバイスの場合、ステータスは Up Sys です。スロット 1 のモジュールのステータスは、次のいずれかになります。<br>• Initializing：モジュールが検出され、デバイスによって制御通信が初期化されています。<br>• Up：モジュールがデバイスによる初期化を完了しました。<br>• Unresponsive：このモジュールとの通信中にデバイスでエラーが発生しました。<br>• Reloading：モジュールがリロード中です。<br>• Shutting Down：モジュールをシャットダウンしています。<br>• Down：モジュールがシャットダウンされました。<br>• Recover：モジュールが回復イメージをダウンロードしようとしています。<br>• No Image Present：モジュールソフトウェアがインストールされていません。 |
| Data Plane Status | データ プレーンの現在の状態。 |
| 互換性 | 残りのデバイスに関連したモジュールの互換性。 |

# show monitor-interface

フェールオーバーのためにモニター対象にするインターフェイスの情報を表示するには、**show monitor-interface** コマンドを使用します。

**show monitor-interface**

## 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

インターフェイスには複数の IPv6 アドレスを設定できるため、**show monitor-interface** コマンドではリンクローカルアドレスのみが表示されます。IPv4 と IPv6 の両方のアドレスがインターフェイスで設定されている場合は、両方のアドレスが出力に表示されます。インターフェイスに IPv4 アドレスが設定されていない場合、出力の IPv4 アドレスは 0.0.0.0 として表示されます。インターフェイスに IPv6 アドレスが設定されていない場合、アドレスは単純に出力から省かれます。

モニター対象のフェールオーバー インターフェイスには、次のステータスが設定されます。

- (Waiting)（Unknown (Waiting) などのように他のステータスと結合）：インターフェイスはピア装置上の対応するインターフェイスから hello パケットをまだ受信していません。
- Unknown：初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合もあります。
- Normal：インターフェイスはトラフィックを受信しています。ステータスが Normal (Waiting) である場合、インターフェイスのスタンバイ IP アドレスが設定されていること、および 2 つのインターフェイス間の接続が存在することを確認してください。
- Testing：ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。
- Link Down：インターフェイスまたは VLAN は管理上ダウンしています。
- No Link：インターフェイスの物理リンクがダウンしています。
- Failed：インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

### 例

次に、**show monitor-interface** コマンドの出力例を示します。

```
> show monitor-interface
 This host: Primary - Active
  Interface inside (192.168.1.13): Normal (Monitored)
  Interface outside (192.168.2.13): Normal (Monitored)
 Other host: Secondary - Standby Ready
```

```
Interface inside (192.168.1.14): Normal (Monitored)
Interface outside (192.168.2.14): Normal (Monitored)
```

# show mrib client

MRIB クライアント接続の情報を表示するには、**show mrib client** コマンドを使用します。

**show mrib client** ［**filter**］［**name** *client_name*］

## 構文の説明

| | |
|---|---|
| **filter** | （任意）クライアント フィルタを表示します。各クライアントが所有するMRIBフラグと、各クライアントが関連するフラグに関する情報を表示するために使用します。 |
| **name** *client_name* | （任意）PIM または IGMP など、MRIB のクライアントとして動作するマルチキャスト ルーティング プロトコルの名前。 |

## 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

**filter** オプションを使用して、さまざまな MRIB クライアントが登録されているルートおよびインターフェイス レベル フラグの変更を表示します。このコマンド オプションからは、MRIB クライアントが所有するフラグも表示されます。

### 例

次に、**show mrib client** コマンドで **filter** キーワードを指定した場合の出力例を示します。

```
> show mrib client filter
MFWD:0 (connection id 0)
interest filter:
entry attributes: S C IA D
interface attributes: F A IC NS DP SP
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
groups:
include 0.0.0.0/0
interfaces:
include All
igmp:77964 (connection id 1)
ownership filter:
interface attributes: II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
pim:49287 (connection id 5)
interest filter:
entry attributes: E
interface attributes: SP II ID LI LD
```

```
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
entry attributes: L S C IA D
interface attributes: F A IC NS DP
groups:
include 0.0.0.0/0
interfaces:
include All
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show mrib route** | MRIB テーブルのエントリを表示します。 |

# show mrib route

MRIB テーブル内のエントリを表示するには、**show mrib route** コマンドを使用します。

**show mrib route** [[[*source* | *****] [*group*[/*prefix-length*]]] | **summary**]

## 構文の説明

| | |
|---|---|
| ***** | （任意）共有ツリー エントリを表示します。 |
| /*prefix-length* | （任意）MRIB ルートのプレフィックス長。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。 |
| *group* | （任意）グループの IP アドレスまたは名前。 |
| *source* | （任意）ルート送信元の IP アドレスまたは名前。 |
| **summary** | MRIB テーブル エントリの要約を表示します。 |

## 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

MFIB テーブルには、MRIB から更新されるエントリとフラグのサブセットが保持されます。フラグは、マルチキャストパケットの転送ルールのセットに従って、転送およびシグナリングの動作を決定します。

インターフェイスとフラグのリストに加えて、各ルートエントリにはさまざまなカウンタが表示されます。バイト数は、転送されたバイトの合計数です。パケット数は、このエントリについて受信されたパケット数です。**show mfib count** コマンドは、ルートから独立したグローバルカウンタを表示します。

### 例

次に、**show mrib route** コマンドの出力例を示します。

```
> show mrib route
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept, D - Drop
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
LD - Local Disinterest
(*,224.0.0.0/4) RPF nbr: 10.11.1.20 Flags: L C
   Decapstunnel0 Flags: NS

(*,224.0.0.0/24) Flags: D

(*,224.0.1.39) Flags: S
```

```
(*,224.0.1.40) Flags: S
   POS0/3/0/0 Flags: II LI

(*,238.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS LI
   Decapstunnel0 Flags: A

(*,239.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS
   Decapstunnel0 Flags: A
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show mfib count** | MFIB テーブルのルートとパケット数データを表示します。 |

# show mroute

IPv4 マルチキャスト ルーティング テーブルを表示するには、**show mroute** コマンドを使用します。

**show mroute** ［*group* ［*source*］ | **reserved**］［**active** ［*rate*］ | **count** | **pruned** | **summary**］

## 構文の説明

| | |
|---|---|
| **active** *rate* | （任意）アクティブなマルチキャスト送信元のみを表示します。アクティブな送信元とは、指定された *rate* 以上で送信を実行している送信元です。*rate* が指定されていない場合、アクティブな送信元は 4 kbps 以上のレートで送信を実行している送信元です。 |
| **count** | （任意）グループと送信元に関する統計情報を表示します。この情報には、パケットの数、1 秒あたりのパケット数、パケットの平均サイズ、および 1 秒あたりのビット数が含まれています。 |
| *group* | （任意）DNS ホスト テーブルで定義されているマルチキャスト グループの IP アドレスまたは名前。 |
| **pruned** | （任意）プルーニングされたルートを表示します。 |
| **reserved** | （任意）予約済みグループを表示します。 |
| *source* | （任意）送信元のホスト名または IP アドレス。 |
| **summary** | （任意）マルチキャスト ルーティング テーブル内の各エントリの要約を 1 行で表示します。 |

## 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

**show mroute** コマンドは、マルチキャスト ルーティング テーブルの内容を表示します。デバイスは、PIM プロトコルメッセージ、IGMP レポート、およびトラフィックに基づいて (S,G) および (*,G) エントリを作成して、マルチキャスト ルーティング テーブルにデータを入力します。アスタリスク（*）は、すべての送信元アドレスを示し、「S」は単一ソース アドレスを示し、「G」は宛先マルチキャスト グループ アドレスを示します。(S,G) エントリを作成する場合、ソフトウェアはユニキャスト ルーティング テーブル内で（RPF を経由して）見つかった宛先グループへの最適パスを使用します。

実行コンフィギュレーション内の **mroute** コマンドを表示するには、**show running-config mroute** コマンドを使用します。

### 例

次に、**show mroute** コマンドの出力例を示します。

```
> show mroute

Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 239.1.1.40), 08:07:24/never, RP 0.0.0.0, flags: DPC
  Incoming interface: Null
  RPF nbr: 0.0.0.0
  Outgoing interface list:
    inside, Null, 08:05:45/never
    tftp, Null, 08:07:24/never

(*, 239.2.2.1), 08:07:44/never, RP 140.0.0.70, flags: SCJ
  Incoming interface: outside
  RPF nbr: 140.0.0.70
  Outgoing interface list:
    inside, Forward, 08:07:44/never
```

**show mroute** の出力には、次のフィールドが含まれています。

- Flags：エントリに関する情報を提供します。
  - D（Dense）：エントリはデンス モードで動作しています。
  - S（Sparse）：エントリはスパース モードで動作しています。
  - B（Bidir Group）：マルチキャスト グループが双方向モードで動作していることを示します。
  - s（SSM Group）：マルチキャスト グループが SSM の IP アドレス範囲内であることを示します。このフラグは、SSM の範囲が変更されるとリセットされます。
  - C（Connected）：マルチキャスト グループのメンバーは、直接接続されたインターフェイス上に存在します。
  - L（Local）：デバイス自体が、マルチキャストグループのメンバです。グループは、（設定済みのグループに対する）igmp join-group コマンドによってローカルに加入されています。
  - I（Received Source Specific Host Report）：(S,G) エントリが (S,G) レポートによって作成されたことを示します。この (S,G) レポートは IGMP によって作成された可能性があります。このフラグが設定されるのは、DR に対してのみです。
  - P（Pruned）：ルートがプルーニングされています。ソフトウェアは、この情報を保持して、ダウンストリーム メンバーが送信元に加入できるようにします。
  - R（RP-bit set）：(S,G) エントリが RP をポイントしていることを示します。

- F（Register flag）：ソフトウェアがマルチキャスト送信元に登録されていることを示します。
- T（SPT-bit set）：パケットが最短パス送信元ツリーで受信されていることを示します。
- J（Join SPT）：(*,G) エントリの場合、共有ツリーの下方向に流れるトラフィックの速度が、グループの SPT しきい値設定を超えていることを示します（デフォルトの SPT しきい値設定は 0 kbps です）。J - Join 最短パスツリー（SPT）フラグが設定されている場合に、共有ツリーの下流で次の (S,G) パケットが受信されると、送信元の方向に (S,G) join がトリガーされます。これにより、デバイスは送信元ツリーに加入します。

  (S, G) エントリの場合、グループの SPT しきい値を超過したためにエントリが作成されたことを示します。(S,G) エントリに J - Join SPT フラグが設定されている場合、デバイスは送信元ツリー上のトラフィック速度をモニターします。送信元ツリーのトラフィック速度がグループの SPT しきい値を下回っている状況が 1 分以上継続した場合、デバイスはこの送信元の共有ツリーに再び切り替えようとします。

（注） デバイスは共有ツリー上のトラフィック速度を測定し、この速度とグループの SPT しきい値を 1 秒ごとに比較します。トラフィック速度が SPT しきい値を超えた場合は、トラフィック速度の次の測定が行われるまで、(*,G) エントリに J - Join SPT フラグが設定されます。共有ツリーに次のパケットが着信し、新しい測定間隔が開始されると、フラグが解除されます。

  グループにデフォルトの SPT しきい値（0 Kbps）が使用されている場合、(*, G) エントリには常に J - Join SPT フラグが設定され、解除されません。デフォルトの SPT しきい値が使用されている場合に、新しい送信元からトラフィックを受信すると、デバイスは最短パス送信元ツリーにただちに切り替えます。

- Timers:Uptime/Expires：Uptime は、エントリが IP マルチキャスト ルーティング テーブルに格納されていた期間（時間、分、秒）をインターフェイスごとに示します。Expires は、IP マルチキャスト ルーティング テーブルからエントリが削除されるまでの期間（時間、分、秒）をインターフェイスごとに示します。
- Interface state：着信インターフェイスまたは発信インターフェイスの状態を示します。
  - Interface：着信インターフェイスまたは発信インターフェイスのリストに表示されるインターフェイス名。

  - State：アクセス リストまたは Time to Live（TTL）しきい値による制限があるかどうかに応じて、インターフェイス上で転送、プルーニング、ヌル値化のいずれの処理がパケットに対して実行されるかを示します。

- (*, 239.1.1.40) と (* , 239.2.2.1)：IP マルチキャスト ルーティング テーブルのエントリ。エントリは、送信元の IP アドレスと、それに続くマルチキャスト グループの IP アドレスで構成されます。送信元の位置に置かれたアスタリスク（*）は、すべての送信元を意味します。
- RP：RP のアドレス。スパース モードで動作するルータおよびアクセス サーバーの場合、このアドレスは常に 224.0.0.0 です。
- Incoming interface：送信元からのマルチキャスト パケットが着信する予定のインターフェイス。パケットがこのインターフェイスに着信しなかった場合、廃棄されます。
- RPF nbr：送信元に対するアップストリーム ルータの IP アドレス。
- Outgoing interface list：パケット転送時に使用されるインターフェイス。

## 関連コマンド

| Command | 説明 |
|---|---|
| **show running-config mroute** | 設定されているマルチキャスト ルートを表示します。 |

# show nameif

インターフェイスの論理名を表示するには、**show nameif** コマンドを使用します。

**show nameif** ［*physical_interface*［**.***subinterface*］ | **zone**］

## 構文の説明

| | |
|---|---|
| *physical_interface* | （任意）インターフェイス ID（**gigabitethernet0/1** など）を指定します。 |
| サブインターフェイス | （任意）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。 |
| **zone** | （任意）ゾーン名とインラインセット名を表示します。 |

## コマンド デフォルト

インターフェイスを指定しない場合、このコマンドはすべてのインターフェイス名を表示します。

## 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

インターフェイスに割り当てられた名前を表示するには、このコマンドを使用します。インターフェイスには、任意の構成設定で使用できるように名前を付ける必要があります。インターフェイスのセキュリティレベルも表示されます。脅威に対する防御の場合、セキュリティレベルは常に 0 です。

**zone** キーワードを追加すると、[Zone Name] 列に、インターフェイスが属するインラインセットまたはトラフィックゾーンが表示されます。トラフィックゾーンはセキュリティゾーンと同じではないため、パッシブインターフェイスやインラインセットがない場合、インターフェイスがルーテッドセキュリティゾーンまたはスイッチドセキュリティゾーンに属していても、この列は空になる可能性があります。各インターフェイスが含まれるセキュリティゾーンを判別するには、デバイスマネージャを使用します。

### 例

次に、**show nameif** コマンドの出力例を示します。

```
> show nameif
Interface               Name                    Security
GigabitEthernet1/1      outside                   0
GigabitEthernet1/2      inside1_2                 0
GigabitEthernet1/3      inside1_3                 0
GigabitEthernet1/4      inside1_4                 0
GigabitEthernet1/5      inside1_5                 0
GigabitEthernet1/6      inside1_6                 0
GigabitEthernet1/7      inside1_7                 0
GigabitEthernet1/8      inside1_8                 0
```

```
Management1/1            diagnostic                0
BVI1                     inside                    0
```

次に、ゾーンのメンバーシップを表示する出力例を示します。この例では、2 つのインターフェイスがインラインセットにあり、1 つのインターフェイスがパッシブトラフィックゾーンにあります。

```
> show nameif zone
Interface                Name                      Zone Name           Security
GigabitEthernet0/0       passive                   passive-security-zone
                                                                              0
GigabitEthernet0/1       in                        is-154                    0
GigabitEthernet0/2       out                       is-154                    0
Management0/0            diagnostic                                          0
```

# show nat

NAT ポリシーの統計情報を表示するには、**show nat** コマンドを使用します。

**show nat** ［**interface** *name*］［*ip_addr* ［*mask*］ | ｛**object** | **object-group**｝ *name*］［**translated** ［**interface** *name*］｛*ip_addr* ［*mask*］ | ｛**object** | **object-group**｝ *name*｝］［**detail**］

## 構文の説明

| | |
|---|---|
| **detail** | （任意）オブジェクト フィールドの追加詳細拡張を含めます。 |
| **interface** *name* | （任意）送信元インターフェイスを指定します。 |
| *ip_addr* [*mask*] | （オプション）IP アドレスおよびサブネット マスクを指定します。 |
| **object** *name* | （任意）ネットワーク オブジェクトまたはサービス オブジェクトを指定します。 |
| **object-group** *name* | （任意）ネットワーク オブジェクト グループを指定します。 |
| **translated** | （オプション）変換されたパラメータを指定します。 |

## 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

**show nat** コマンドを使用して、NAT ポリシーの実行時表示を表示します。**detail** オプション キーワードを使用して、オブジェクトを拡張し、オブジェクト値を表示します。追加のセレクタフィールドを使用して、**show nat** コマンド出力を制限することができます。

出力には、隠しコマンドも含むすべての NAT コマンドが表示されます。たとえば、データインターフェイスをゲートウェイとして使用するように管理インターフェイスを設定すると、非表示の仮想インターフェイス（たとえば nlp_int_tap ）に対して非表示の NAT ルールが作成され、管理インターフェイスと各データインターフェイス間の通信が可能になります。これらのルールは、Device Manager の NAT テーブルには反映されません。また、データインターフェイスへの管理接続を許可する HTTPS/SSH 管理アクセスルールの非表示のルールも表示されます。これは、Device Manager の管理アクセステーブルには反映されますが、NAT テーブルには反映されません。バージョン 7.0 以降、システムが独自に使用するために作成するルールはセクション 0 に記載されています。

### 例

次に、**show nat** コマンドの出力例を示します。

```
> show nat
   Manual NAT Policies (Section 1)
   1 (any) to (any) source dynamic S S' destination static D' D
       translate_hits = 0, untranslate_hits = 0
```

```
   Auto NAT Policies (Section 2)
   1 (inside) to (outside) source dynamic A 2.2.2.2
       translate_hits = 0, untranslate_hits = 0

   Manual NAT Policies (Section 3)
   1 (any) to (any) source dynamic C C' destination static B' B service R R'
       translate_hits = 0, untranslate_hits = 0

> show nat detail
   Manual NAT Policies (Section 1)
   1 (any) to (any) source dynamic S S' destination static D' D
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 1.1.1.2/32, Mapped: 2.2.2.3/32
       Destination - Real: 10.10.10.0/24, Mapped: 20.20.20.0/24

   Auto NAT Policies (Section 2)
   1 (inside) to (outside) source dynamic A 2.2.2.2
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 1.1.1.1/32, Mapped: 2.2.2.2/32

   Manual NAT Policies (Section 3)
   1 (any) to (any) source dynamic C C' destination static B' B service R R'
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 11.11.11.10-11.11.11.11, Mapped: 192.168.10.10/32
       Destination - Real: 192.168.1.0/24, Mapped: 10.75.1.0/24
       Service - Real: tcp source eq 10 destination eq ftp-data , Mapped: tcp source eq
       100 destination eq 200
```

次に、**show nat detail** コマンドの IPv6 および IPv4 での出力例を示します。

```
> show nat detail
1 (in) to (outside) source dynamic inside_nw outside_map destination static inside_map
any
translate_hits = 0, untranslate_hits = 0
Source - Origin: 2001::/96, Translated: 192.168.102.200-192.168.102.210
Destination - Origin: 2001::/96, Translated: 0.0.0.0/0
```

次に、セクション 0 のシステム定義ルールの例を示します。

```
> show nat detail
Manual NAT Policies Implicit (Section 0)
1 (nlp_int_tap) to (inside) source static nlp_server_0_snmp_intf3 interface  service udp
 snmp snmp
    translate_hits = 1, untranslate_hits = 1
    Source - Origin: 169.254.1.2/32, Translated: 10.1.1.122/24
    Service - Protocol: udp Real: snmp Mapped: snmp
2 (nlp_int_tap) to (inside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 169.254.1.2/32, Translated: 10.1.1.122/24

Manual NAT Policies (Section 1)
1 (inside) to (any) source dynamic obj_man interface
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.3.3.3/32, Translated: 10.1.1.122/24
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear nat counters** | NAT ポリシー カウンタをクリアします。 |

# show nat divert-table

NAT 迂回テーブルの統計情報を表示するには、**show nat divert-table** コマンドを使用します。

**show nat divert-table** ［**ipv6**］［**interface** *interface_name*］

## 構文の説明

| | |
|---|---|
| **divert-table** | NAT 迂回テーブルを表示します。 |
| **ipv6** | （オプション）迂回テーブルの IPv6 エントリを表示します。 |
| **interface** *interface_name* | （オプション）指定した送信元インターフェイスに出力を限定します。 |

## 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

**show nat divert-table** コマンドを使用して、NAT 迂回テーブルの実行時表現を表示します。迂回テーブルの IPv6 エントリを表示するには、**ipv6** オプションキーワードを使用します。特定の発信元インターフェイスの NAT 迂回テーブルを表示するには、**interface** オプションキーワードを使用します。

迂回テーブルには、隠しコマンドも含むすべての NAT コマンドが表示されます。たとえば、データインターフェイスをゲートウェイとして使用するように管理インターフェイスを設定すると、非表示の仮想インターフェイス（たとえば nlp_int_tap ）に対して非表示の NAT ルールが作成され、管理インターフェイスと各データインターフェイス間の通信が可能になります。これらのルールは、Device Manager の NAT テーブルには反映されません。

### 例

次に、**show nat divert-table** コマンドの出力例を示します。

```
> show nat divert-table
Divert Table
id=0xad1521b8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=10.86.119.255, mask=255.255.255.255, port=0-0
        input_ifc=outside, output_ifc=NP Identity Ifc
id=0xad1523a8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=10.86.116.0, mask=255.255.255.255, port=0-0
        input_ifc=outside, output_ifc=NP Identity Ifc
id=0xad1865c0, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=192.168.255.255, mask=255.255.255.255, port=0-0
        input_ifc=amallio-wizard, output_ifc=NP Identity Ifc
id=0xad1867b0, domain=twice-nat section=1 ignore=no
```

```
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=192.168.0.0, mask=255.255.255.255, port=0-0
        input_ifc=amallio-wizard, output_ifc=NP Identity Ifc
id=0xad257bf8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=172.27.48.255, mask=255.255.255.255, port=0-0
        input_ifc=folink, output_ifc=NP Identity Ifc
id=0xad257db8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=172.27.48.0, mask=255.255.255.255, port=0-0
        input_ifc=folink, output_ifc=NP Identity Ifc
```

次に、**show nat divert ipv6** コマンドの出力例を示します。

```
> show nat divert ipv6
Divert Table
id=0xcb9ea518, domain=divert-route
type=static, hits=0, flags=0x21, protocol=0
src ip/id=2001::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
dst ip/id=2001::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
input_ifc=in, output_ifc=outside
id=0xcf24d4b8, domain=divert-route
type=static, hits=0, flags=0x20, protocol=0
src ip/id=::/::, port=0-0
dst ip/id=2222::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
input_ifc=in, output_ifc=mgmt
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear nat counters** | NAT ポリシー カウンタをクリアします。 |
| **show nat** | NAT ポリシーの実行時表現を表示します。 |

# show nat pool

NAT プールの使用状況を表示するには、**show nat pool** コマンドを使用します。

**show nat pool** ［ **interface** *if-name* ［ **ip** *address* ］ | **ip** *address* | **detail** ］

**show nat pool cluster** ［ **summary** | **interface** *if-name* ［ **ip** *address* ］ | **ip** *address* ］

## 構文の説明

| | |
|---|---|
| **cluster** | （任意）クラスタリングが有効になっている場合、オーナーユニットとバックアップユニットへの PAT アドレスの現在の割り当てを表示します。<br>（6.7 以降）クラスタ内のユニット間におけるポートブロックの分布を表示するには、**summary** キーワードを含めます。 |
| **interface** *if_name* | 指定したインターフェイスのプールに対する表示を制限します。（任意）**ip** キーワードを含めると、表示をさらに制限できます。 |
| **ip** *address* | 表示を PAT プールから指定した IP アドレスに制限します。 |
| **detail** | クラスタ内のポートブロックの使用状況と分布に関する情報を表示します。このキーワードは、ユニットがクラスタメンバーの場合にのみ表示されます。cluster キーワードと一緒に使用することはできません。 |

## 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。 |
| 6.7 | 次のキーワードが追加されました。**interface**、**ip**、**detail**、**summary** |

## 使用上のガイドライン

（6.7 未満）NAT プールは、マッピングされたプロトコル/IP アドレス/ポート範囲ごとに作成されます。ポート範囲は、デフォルトでは 1 ～ 511、512 ～ 1023、および 1024 ～ 65535 です。フラットな範囲のポートを使用するように PAT プールを設定すると、表示される範囲の数は少なくなり、範囲の幅は広くなります。

（6.7以降）6.7以降、ポート範囲はデフォルトでフラットであり、必要に応じて予約済みポート（1 ー 1023）をプールに含めることができます。クラスタ化されたシステムの場合、PAT プールは、512 のポートのブロックでクラスタメンバーに分散されます。

各 NAT プールは、最後に使用された後、少なくとも 10 分間存在します。10 分間のホールドダウンタイマーは、**clear xlate** で変換をクリアするとキャンセルされます。

## 例

次に、**show running-config object network** コマンドによって表示される、ダイナミック PAT ルールによって作成された NAT プールの出力例を示します

```
> show running-config object network
object network myhost
 host 10.10.10.10
 nat (pppoe2,inside) dynamic 10.76.11.25

> show nat pool
TCP inside, address 10.76.11.25, range 1-511, allocated 0
TCP inside, address 10.76.11.25, range 512-1023, allocated 0
TCP inside, address 10.76.11.25, range 1024-65535, allocated 1
```

次に、PAT プールに **flat** オプションを使用した場合の **show nat pool** コマンドの出力例を示します。**include-reserve** キーワードを指定しないと、2 つの範囲が示されます。低い方の範囲は、1024 未満の送信元ポートが同じポートにマッピングされているときに使用されます。

```
> show nat pool
ICMP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1-1024, allocated 0
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1024-65535, allocated 2
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1-1024, allocated 0
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1024-65535, allocated 2
```

次に、PAT プールに **flat include-reserve** オプションを使用した場合の **show nat pool** コマンドの出力例を示します。

```
> show nat pool
ICMP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
```

（6.7 未満）次に、PAT プールに **extended flat include-reserve** オプションを使用した場合の **show nat pool** コマンドの出力例を示します。重要な項目はカッコで囲まれたアドレスです。これらは拡張 PAT に使用される宛先アドレスです。

```
ICMP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
ICMP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.99), range 1-65535,
allocated 2
TCP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535,
allocated 1
UDP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535,
allocated 1
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
ICMP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535,
allocated 1
TCP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.99), range 1-65535,
allocated 2
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
```

（6.7以降）次の例は、ブロックを所有するユニットとブロックのバックアップユニットを含む、クラスタ内のポートブロックの分布（ポート範囲を示す）とその使用状況を示しています。

```
> show nat pool cluster
IP outside_a:src_map_a 174.0.1.20
               [1536 - 2047], owner A, backup B
               [8192 - 8703], owner A, backup B
               [4089 - 4600], owner B, backup A
               [11243 - 11754], owner B, backup A
IP outside_a:src_map_a 174.0.1.21
               [1536 - 2047], owner A, backup B
               [8192 - 8703], owner A, backup B
               [4089 - 4600], owner B, backup A
               [11243 - 11754], owner B, backup A
IP outside_b:src_map_b 174.0.1.22
               [6656 - 7167], owner A, backup B
               [13312 - 13823], owner A, backup B
               [20480 - 20991], owner B, backup A
               [58368 - 58879], owner B, backup A
IP outside_b:src_map_b 174.0.1.23
               [46592 - 47103], owner A, backup B
               [52224 - 52735], owner A, backup B
               [62976 - 63487], owner B, backup A
```

（6.7 以降）次の例は、クラスタ内でのプール割り当ての概要を示しています。

```
> show nat pool cluster summary
port-blocks count display order: total, unit-A, unit-B, unit-C, unit-D
IP outside_a:src_map_a, 174.0.1.20 (128 - 32/32/32/32)
IP outside_a:src_map_a, 174.0.1.21 (128 - 36/32/32/28)
IP outside_b:src_map_b, 174.0.1.22 (128 - 31/32/32/33)
```

（6.7 以降）次の例は、クラスタ内のプールに関する PAT プールの詳細な使用状況を示しています。詳細な出力を表示する場合、バックアップポート範囲がアスタリスクで示されます。例：range 63464-62975, assigned 27 *

```
> show nat pool detail
TCP PAT pool outside_a, address 174.0.1.1
                range 1536-2047, allocated 56
                range 8192-8703, allocated 16
UDP PAT pool outside_a, address 174.0.1.1
                range 1536-2047, allocated 12
                range 8192-8703, allocated 25
 TCP PAT pool outside_b, address 174.0.2.1
                range 47104-47615, allocated 39
                range 62464-62975, allocated 9
UDP PAT pool outside_b, address 174.0.2.1
                range 47104-47615, allocated 35
                range 62464-62975, allocated 27
```

（6.7以降）次の例は、ビューを特定のデバイス上の特定のインターフェイスに限定する方法を示しています。

```
> show nat pool interface outside_b ip 174.0.2.1
TCP PAT pool outside_b, address 174.0.2.1, range 1-511, allocated 0
TCP PAT pool outside_b, address 174.0.2.1, range 512-1023, allocated 12
TCP PAT pool outside_b, address 174.0.2.1, range 1024-65535, allocated 48
```

```
UDP PAT pool outside_b, address 174.0.2.1, range 1-511, allocated 6
UDP PAT pool outside_b, address 174.0.2.1, range 512-1023, allocated 8
UDP PAT pool outside_b, address 174.0.2.1, range 1024-65535, allocated 62
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show nat** | NAT ポリシーの統計情報を表示します。 |

# show nat proxy-arp

NAT プロキシ ARP テーブルを表示するには、**show nat proxy-arp** コマンドを使用します。

**show nat proxy-arp** ［**ipv6**］［**interface** *name*］

## 構文の説明

| | |
|---|---|
| **ipv6** | （オプション）プロキシ ARP テーブルの IPv6 エントリを表示します。 |
| **interface** *name* | （オプション）指定した送信元インターフェイスに出力を限定します。 |

## 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

NAT プロキシ ARP テーブルの実行時表現を表示するには、**show nat proxy-arp** コマンドを使用します。

プロキシ ARP テーブルには、隠しコマンドも含むすべての NAT コマンドが表示されます。たとえば、データインターフェイスをゲートウェイとして使用するように管理インターフェイスを設定すると、非表示の仮想インターフェイス（たとえばnlp_int_tap）に対して非表示のNATルールが作成され、管理インターフェイスと各データインターフェイス間の通信が可能になります。これらのルールは、Device Manager の NAT テーブルには反映されません。

### 例

次に、**show nat proxy-arp** コマンドの出力例を示します。

```
> show nat proxy-arp
Nat Proxy-arp Table
id=0x00007f4ce491a010, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_8) to (outside) source dynamic any-ipv4 interface
id=0x00007f4cdc6138d0, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_7) to (outside) source dynamic any-ipv4 interface
id=0x00007f4ce491d2e0, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_6) to (outside) source dynamic any-ipv4 interface
id=0x00007f4cdc618a10, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_5) to (outside) source dynamic any-ipv4 interface
id=0x00007f4d019c9e70, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_4) to (outside) source dynamic any-ipv4 interface
id=0x00007f4cdc61b300, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_3) to (outside) source dynamic any-ipv4 interface
id=0x00007f4ce49261f0, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_2) to (outside) source dynamic any-ipv4 interface
```

関連コマンド

| Command | 説明 |
| --- | --- |
| **clear nat counters** | NAT ポリシー カウンタをクリアします。 |
| **show nat** | NAT ポリシーの実行時表現を表示します。 |

# show network

管理インターフェイスの属性を表示するには、**show network** コマンドを使用します。

**show network**

## 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。 |
| 6.7 | このコマンドは、管理と Management Center の両方のアクセス データ インターフェイスのネットワーク設定を表示します。 |

## 使用上のガイドライン

このコマンドを使用して、**configure network** コマンドを使用して設定した管理インターフェイスのプロパティを表示します。

ゲートウェイとしてデータインターフェイスを使用するように管理アドレスを設定すると、ゲートウェイは「data-interface」として表示されます。

### 例

次に、**show network** コマンドの出力例を示します。

```
> show network
===============[ System Information ]===============
Hostname                  : 5516X-4
DNS Servers               : 208.67.220.220,208.67.222.222
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces
IPv6 Default route
  Gateway                 : data-interfaces

======================[ br1 ]=======================
State                     : Enabled
Link                      : Up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 28:6F:7F:D3:CB:8D
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.99.10.4
Netmask                   : 255.255.255.0
Gateway                   : 10.99.10.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

===============[ Proxy Information ]================
State                     : Disabled
Authentication            : Disabled

======[ System Information - Data Interfaces ]======
```

```
DNS Servers                :
Interfaces                 : GigabitEthernet1/1

===============[ GigabitEthernet1/1 ]===============
State                      : Enabled
Link                       : Up
Name                       : outside
MTU                        : 1500
MAC Address                : 28:6F:7F:D3:CB:8F
----------------------[ IPv4 ]----------------------
Configuration              : Manual
Address                    : 10.89.5.29
Netmask                    : 255.255.255.192
Gateway                    : 10.89.5.1
----------------------[ IPv6 ]----------------------
Configuration              : Disabled
```

# show network-dhcp-server

管理インターフェイスでDHCPサーバーのステータスを表示するには、**show network-dhcp-server** コマンドを使用します。

**show network-dhcp-server**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.2 | このコマンドが導入されました。 |

## 使用上のガイドライン

管理インターフェイスのオプションのDHCPサーバーのステータスを表示するには、このコマンドを使用します。DHCP サーバーを設定するには、**configure network ipv4 dhcp-server-enable** コマンドを使用します。

出力には、DHCPサーバーが有効か無効かが示されます。有効な場合は、アドレスプールも表示されます。

### 例

次に、DHCP サーバーを設定し、そのステータスを表示する例を示します。

```
> show network-dhcp-server
DHCP Server Disabled
> configure network ipv4 dhcp-server-enable 192.168.45.46 192.168.45.254
DHCP Server Enabled
> show network-dhcp-server
DHCP Server Enabled
192.168.45.46-192.168.45.254
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure network ipv4 dhcp-server-enable** | 管理インターフェイスに DHCP サーバーを設定します。 |
| **configure network ipv4 dhcp-server-disable** | 管理インターフェイスの DHCP サーバーを無効にします。 |

# show network-static-routes

管理インターフェイスに対して設定されたスタティックルートを表示するには、**show network-static-routes** コマンドを使用します。

**show network-static-routes**

## 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

管理インターフェイスのスタティックルートは、複数の管理インターフェイスを設定するときに使用されます。これらのルートには、デフォルトゲートウェイは含まれません。単一の管理インターフェイスを使用している場合、通常、追加のスタティックルートはありません。

このコマンドで表示されるルートは、管理インターフェイス専用です。データインターフェイスでは使用されません。through-the-box トラフィックには使用されません。

### 例

次の例は、管理インターフェイスに追加のスタティックルートがないことを示しています。デフォルトゲートウェイが唯一のルートです。

```
> show network-static-routes
No static routes currently configured.
```

次に、スタティックルートを削除する方法の例を示します。

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                : br1
Destination              : 10.1.1.0
Gateway                  : 192.168.0.254
Netmask                  : 255.255.255.0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure network static-routes** | 管理インターフェイスのスタティックルートを設定します。 |

# show ntp

現在の Network Time Protocol（NTP）サーバー、および設定を表示するには、**show ntp** コマンドを使用します。

**show ntp**

## 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、NTP サーバーに関する基本情報を表示します。より広範な情報が必要な場合は、**system support ntp** コマンドを使用します。このコマンドには、このコマンドの出力と、NTP プロトコルで記載される標準 NTP コマンド **ntpq** の出力が含まれています。

### 例

次に、NTP 設定を表示する例を示します。

```
> show ntp
NTP Server                : 209.208.79.69
Status                    : Available
Offset                    : -1.614 (milliseconds)
Last Update               : 578 (seconds)

NTP Server                : 45.127.112.2  (clocka.ntpjs.org)
Status                    : Available
Offset                    : -1.355 (milliseconds)
Last Update               : 874 (seconds)

NTP Server                : 198.58.105.63  (ha81.smatwebdesign.com)
Status                    : Not Available
Offset                    : -4.942 (milliseconds)
Last Update               : 369 (seconds)

NTP Server                : 204.9.54.119  (ntp.your.org)
Status                    : Being Used
Offset                    : 0.312 (milliseconds)
Last Update               : 962 (seconds)
```

次の例は、**system support ntp** コマンドを使用して追加情報を取得する方法を示しています。NTP 同期を確認する必要がある場合は、このコマンドを使用します。

「Results of 'ntpq -pn」の部分を探します。たとえば、次のように表示されます。

```
> system support ntp
... output redacted ...
Results of 'ntpq -pn'
remote                    : +216.229.0.50
refid                     : 129.7.1.66
st                        : 2
t                         : u
```

```
when                        : 704
poll                        : 1024
reach                       : 377
delay                       : 90.455
offset                      : 2.954
jitter                      : 2.473
... remaining output redacted ...
```

この例では、NTP サーバのアドレスの前の「+」は、潜在的な候補であることを示します。アスタリスク * は、現在の時刻源のピアを示します。

NTP デーモン（NTPD）は、各ピアから取得される 8 つのサンプルのスライディングウィンドウを使用して、1 つのサンプルをピックアップします。その後、クロック選択によって正しいチャイマーと不正なティッカーが特定されます。次に、NTPD がラウンドトリップ距離を特定します（候補のオフセットをラウンドトリップ遅延の半分以上にすることはできません）。接続の遅延、パケットの損失、またはサーバーの問題が発生して1つまたはすべての候補が拒否されると、同期中に長い遅延が生じます。また、調整にも非常に長い時間がかかります。クロック規律アルゴリズムによって、クロック オフセットおよびオシレータ エラーを解決する必要がありますが、これには数時間かかる可能性があります。

（注） refid が .LOCL. の場合は、ピアが無規律のローカルクロックであることを示します。つまり、時間設定にそのローカルクロックのみを使用します。選択したピアが .LOCL の場合、Device Manager は NTP 接続を常に黄色（非同期）にマークします。通常 NTP は、より適切な候補を利用できる場合、.LOCL. 候補を選択しません。そのため、サーバーを 3 つ以上設定する必要があります。

## 関連コマンド

| Command | 説明 |
|---|---|
| **system support ntp** | NTP の詳細なトラブルシューティング情報を表示します。 |

# show object

ヒットカウントや IP アドレスなど、ネットワークサービス オブジェクトに関する情報を表示するには、**show object** コマンドを使用します。

**show object** ［ **id** *object_name* | **network-service** ［ **detail** ］］

## 構文の説明

| | |
|---|---|
| **id** *name* | （オプション）表示するオブジェクトの名前。大文字と小文字が区別されます。たとえば、「object-name」は「Object-Name」と一致しません。 |
| **network-service**［**detail**］ | （オプション）すべてのネットワークサービス オブジェクトを表示します。オブジェクトメンバーに関連付けられているキャッシュされた IP アドレスを表示するには、detail キーワードを含めます。 |

## コマンド デフォルト

パラメータを指定しない場合、すべてのオブジェクトが表示されます。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1 | このコマンドが導入されました。 |

### 例

次に、Cisco という名前のネットワークサービス オブジェクトの詳細を表示する例を示します。app-id（アプリケーション ID）は内部番号です。hitcnt（ヒット カウント）の数字のみが、関連メトリックとして表示されます。

```
> show object id Cisco
object network-service "Cisco" dynamic
 description Official website for Cisco.
 app-id 2655
 domain cisco.com (bid=0) ip (hitcnt=0)
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear object** | ネットワークサービス オブジェクトのヒットカウントをクリアします。 |
| **show object-groups** | ネットワークサービス オブジェクト グループとヒットカウントを表示します。 |

# show object-group

オブジェクトグループのタイプがネットワーク オブジェクトグループまたはネットワークサービス オブジェクトグループである場合にオブジェクトグループの情報と関連するヒットカウントを表示するには、**show object-group** コマンドを使用します。すべてのタイプのオブジェクトグループを表示するには、パラメータなしでコマンドを使用します。

**show object-group** [ **count** | **interface** | **network** | **security** | **service** | **id** *name* ]

**show object-group network-service** [ *group_name* [ **network-service-member** *member_name* [ **dns** *domain_name* ] ] [ **detail** ]

## 構文の説明

| | |
|---|---|
| **count** | （オプション）オブジェクトグループの数とそれらのグループ内のオブジェクトの数、およびそれらの使用状況に関連する統計を表示します。 |
| **detail** | ネットワークサービス オブジェクトについて、オブジェクトメンバーに関連付けられているキャッシュされた IP アドレスを表示します。 |
| **dns** *domain_name* | （オプション）名前とメンバーを指定したネットワークサービス オブジェクトについて、そのメンバーの特定のドメインに情報を制限します。例、example.com。 |
| **id** *name* | （オプション）オブジェクト グループを名前で特定します。 |
| **interface** | （任意）インターフェイスタイプのオブジェクト。 |
| **network** | （オプション）ネットワークタイプのオブジェクト。 |
| **network-service** [*group_name* ] | （オプション）ネットワークサービス オブジェクト。オブジェクト名を指定して単一のオブジェクトに情報を制限できます。 |
| **network-service-member** *member_name* | （オプション）名前を指定したネットワークサービス オブジェクトについて、そのオブジェクトの特定のメンバーに情報を制限します。 |
| **security** | （オプション）セキュリティタイプのオブジェクト。 |
| **service** | （任意）サービスタイプのオブジェクト。 |

## 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。 |
| 7.1 | **network-service** キーワードと関連パラメータが追加されました。 |
| 7.2 | **count** キーワードが追加されました。 |

### 例

次に、「Anet」という名前のネットワーク オブジェクト グループについての情報を表示する、**show object-group** コマンドの出力例を示します。

```
> show object-group id Anet
Object-group network Anet (hitcnt=10)
   Description OBJ SEARCH ALG APPLIED
   network-object 1.1.1.0 255.255.255.0 (hitcnt=4)
   network-object 2.2.2.0 255.255.255.0 (hitcnt=6)
```

次に、サービスグループに関する情報を表示する、**show object-group** コマンドの出力例を示します。

```
> show object-group service
object-group service B-Serobj
   description its a service group
   service-object tcp eq bgp
```

次に、ネットワークサービス オブジェクトとそのヒットカウントを表示する例を示します。ネットワークサービス グループ ID（nsg-id）、アプリケーション ID（app-id）、bid などの各種の識別子は内部のインデックス番号であり、無視してかまいません。

```
> show object-group network-service FMC_NSG_4294969442
object-group network-service FMC_NSG_4294969442 (nsg-id 512/1)
 network-service-member "Facebook" dynamic
  description Facebook is a social networking service.
  app-id 629
  domain connect.facebook.net (bid=214491) ip (hitcnt=0)
  domain facebook.com (bid=370809) ip (hitcnt=0)
  domain fbcdn.net (bid=490321) ip (hitcnt=0)
  domain fbcdn-photos-a.akamaihd.net (bid=548791) ip (hitcnt=0)
  domain fbcdn-photos-e-a.akamaihd.net (bid=681143) ip (hitcnt=0)
  domain fbcdn-photos-b-a.akamaihd.net (bid=840741) ip (hitcnt=0)
  domain fbstatic-a.akamaihd.net (bid=1014669) ip (hitcnt=0)
  domain fbexternal-a.akamaihd.net (bid=1098051) ip (hitcnt=0)
  domain fbcdn-profile-a.akamaihd.net (bid=1217875) ip (hitcnt=0)
  domain fbcdn-creative-a.akamaihd.net (bid=1379985) ip (hitcnt=0)
  domain channel.facebook.com (bid=1524617) ip (hitcnt=0)
  domain fbcdn-dragon-a.akamaihd.net (bid=1683343) ip (hitcnt=0)
  domain contentcache-a.akamaihd.net (bid=1782703) ip (hitcnt=0)
  domain facebook.net (bid=1868733) ip (hitcnt=0)
 network-service-member "Google+ Videos" dynamic
  description Video sharing among Google+ community.
  app-id 2881
  domain plus.google.com (bid=2068293) ip (hitcnt=0)
 network-service-member "Instagram" dynamic
  description Mobile phone photo sharing.
  app-id 1233
  domain instagram.com (bid=2176667) ip (hitcnt=0)
 network-service-member "LinkedIn" dynamic
  description Career oriented social networking.
  app-id 713
  domain linkedin.com (bid=2317259) ip (hitcnt=0)
>
```

次の例はオブジェクトカウントを示したものであり、オブジェクトグループの数、グループに含まれるオブジェクトの数、および ACL や NAT などで使用されているオブジェクトの数を確認できます。この情報はオブジェクトグループ検索機能のパフォーマンスに関連するものです。

```
ciscoasa(config)# show object-group count

Object Group Name                       Group Count Dyn Count V4 CNT     V6 CNT      ACL
CNT    NAT CNT    OG in OG
network    i28Z-route                   68          0           68          0           0
         0          0
network    i28Z-VRF-BGP-PEERS           4           0           4           0           2
         0          0
network    EXCH-BGP-PEERS               4           0           4           0           2
         0          0
network    obgr_SUBNETS_NO_ACL          112         0           112         0           0
         0          0
network    obgr_SUBNETS_ACL_ASAMgmt     1           0           1           0           0
         0          0
network    obgr_CLIENTS_ACL_ASAMgmt     8           0           8           0           1
         0          0
network    obgr_SUBNETS_CGS_vMotion     1           0           1           0           0
         0          0
network    obgr_CLIENTS_CGS_vMotion     9           0           9           0           1
         0          0
network    obgr_SUBNETS_UPMCOD_CGS      17          0           17          0           0
         0          0
network    obgr_CLIENTS_UPMCOD_CGS      90          0           90          0           1
         0          0
network    obgr_CLIENTS_10.68.0.0_16    2           0           2           0           1
         0          0
network    obgr_CLIENTS_10.68.1.198_31  4           0           4           0           1
         0          0
network    obgr_CLIENTS_10.68.73.133    7           0           7           0           1
         0          0
network    asa_zabbix_proxies           4           0           4           0           1
         0          0

Total Summary
Object-group count                          14
Object-group object count                   331
Object-group Dynamic count                  0
Object-group IPv4 count                     331
Object-group IPv6 count                     0
Object-group Used in ACL                    9
Object-group Used in NAT                    0
Object-group Unused                         5
Object-group Internal                       0
Object-group Dummy                          0
Redundant object-group in Network           4
Redundant object-group in IfC               0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear object-group** | 指定されたオブジェクトグループのネットワークオブジェクトのヒットカウントをクリアします。 |
| **show access-list** | すべてのアクセスリスト、関連拡張アクセスリストエントリ、およびヒットカウントを表示します。 |

| Command | 説明 |
| --- | --- |
| **show object** | ネットワークサービスオブジェクトとヒットカウントを表示します。 |

# show ospf

OSPF ルーティングプロセスに関する一般情報を表示するには、**show ospf** コマンドを使用します。

**show ospf** ［**vrf** *name* | **all**］ ［*pid* ［*area_id*］］

## 構文の説明

| | |
|---|---|
| *area_id* | （任意）OSPF アドレス範囲に関連付けられているエリアの ID。 |
| *pid* | （任意）OSPF プロセスの ID。 |
| ［**vrf** *name* \| **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* \| **all**］ キーワードが追加されました。 |

### 例

次に、**show ospf** コマンドの出力例を示します。ここでは、特定の OSPF ルーティングプロセスに関する一般情報を表示する例を示しています。

```
> show ospf 5
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
```

次に、**show ospf** コマンドの出力例を示します。ここでは、すべての OSPF ルーティングプロセスに関する一般情報を表示する例を示しています。

```
> show ospf
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
```

```
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x     0
Number of opaque AS LSA 0. Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0

Routing Process "ospf 12" with ID 172.23.59.232 and Domain ID 0.0.0.12
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x     0
Number of opaque AS LSA 0. Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0
```

# show ospf border-routers

ABR および ASBR までの内部 OSPF ルーティング テーブル エントリを表示するには、**show ospf border-routers** コマンドを使用します。

**show ospf border-routers** ［**vrf** *name* | **all**］

## 構文の説明

| | |
|---|---|
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |

### 例

次に、**show ospf border-routers** コマンドの出力例を示します。

```
> show ospf border-routers

OSPF Process 109 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 192.168.97.53 [10] via 192.168.1.53, fifth, ABR, Area 0, SPF 20
i 192.168.103.51 [10] via 192.168.96.51, outside, ASBR, Area 192.168.12.0, SPF 14
i 192.168.103.52 [10] via 192.168.96.51, outside, ABR/ASBR, Area 192.168.12.0, SPF 14
```

# show ospf database

OSPF トポロジデータベースに格納されている情報を表示するには、**show ospf database** コマンドを使用します。

**show ospf** ［**vrf** *name* ｜ **all**］ ［*pid* ［*area_id*］］ **database** ［**router** ｜ **network** ｜ **summary** ｜ **asbr-summary** ｜ **external** ｜ **nssa-external**］［*lsid*］［**internal**］［**self-originate** ｜ **adv-router** *addr*］
**show ospf** ［*pid* ［*area_id*］］ **database database-summary**

## 構文の説明

| | |
|---|---|
| *addr* | （任意）ルータのアドレス。 |
| **adv-router** | （任意）アドバタイズされたルータ。 |
| *area_id* | （任意）OSPF アドレス範囲に関連付けられているエリアの ID。 |
| **asbr-summary** | （任意）ASBR リストの要約を表示します。 |
| **database** | データベース情報を表示します。 |
| **database-summary** | （任意）データベース全体の要約リストを表示します。 |
| **external** | （任意）指定した自律システムの外部のルートを表示します。 |
| **internal** | （任意）指定した自律システム内部のルート。 |
| *lsid* | （任意）LSA ID。 |
| **network** | （任意）ネットワークに関する OSPF データベース情報を表示します。 |
| **nssa-external** | （任意）外部の Not-So-Stubby Area リストを表示します。 |
| *pid* | （任意）OSPF プロセスの ID。 |
| **router** | （任意）ルータを表示します。 |
| **self-originate** | （任意）指定した自律システムに関する情報を表示します。 |
| **summary** | （任意）リストの要約を表示します。 |
| ［**vrf** *name* ｜ **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | [**vrf** *name* | **all**] キーワードが追加されました。 |

### 例

次に、**show ospf database** コマンドの出力例を示します。

```
> show ospf database
OSPF Router with ID(192.168.1.11) (Process ID 1)

                Router Link States(Area 0)
Link ID   ADV Router   Age   Seq# Checksum Link count
192.168.1.8 192.168.1.8 1381 0x8000010D    0xEF60 2
192.168.1.11 192.168.1.11 1460 0x800002FE    0xEB3D 4
192.168.1.12 192.168.1.12 2027 0x80000090    0x875D 3
192.168.1.27 192.168.1.27 1323 0x800001D6    0x12CC 3

                Net Link States(Area 0)
Link ID ADV Router   Age   Seq# Checksum
172.16.1.27 192.168.1.27 1323 0x8000005B    0xA8EE
172.17.1.11 192.168.1.11 1461 0x8000005B    0x7AC

                Type-10 Opaque Link Area Link States (Area 0)
Link ID ADV Router   Age Seq# Checksum Opaque ID
10.0.0.0 192.168.1.11 1461 0x800002C8    0x8483   0
10.0.0.0 192.168.1.12 2027 0x80000080    0xF858   0
10.0.0.0 192.168.1.27 1323 0x800001BC    0x919B   0
10.0.0.1 192.168.1.11 1461 0x8000005E    0x5B43   1
```

次に、**show ospf database asbr-summary** コマンドの出力例を示します。

```
> show ospf database asbr-summary
OSPF Router with ID(192.168.239.66) (Process ID 300)
Summary ASB Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1463
Options: (No TOS-capability)
LS Type: Summary Links(AS Boundary Router)
Link State ID: 172.16.245.1 (AS Boundary Router address)
Advertising Router: 172.16.241.5
LS Seq Number: 80000072
Checksum: 0x3548
Length: 28
Network Mask: 0.0.0.0
TOS: 0 Metric: 1
```

次に、**show ospf database router** コマンドの出力例を示します。

```
> show ospf database router
OSPF Router with id(192.168.239.66) (Process ID 300)
Router Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1176
```

```
Options: (No TOS-capability)
LS Type: Router Links
Link State ID: 10.187.21.6
Advertising Router: 10.187.21.6
LS Seq Number: 80002CF6
Checksum: 0x73B7
Length: 120
AS Boundary Router
Number of Links: 8
Link connected to: another Router (point-to-point)
(link ID) Neighboring Router ID: 10.187.21.5
(Link Data) Router Interface address: 10.187.21.6
Number of TOS metrics: 0
TOS 0 Metrics: 2
```

次に、**show ospf database network** コマンドの出力例を示します。

```
> show ospf database network
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Net Link States(Area 0.0.0.0)
LS age: 1367
Options: (No TOS-capability)
LS Type: Network Links
Link State ID: 10.187.1.3 (address of Designated Router)
Advertising Router: 192.168.239.66
LS Seq Number: 800000E7
Checksum: 0x1229
Length: 52
Network Mask: 255.255.255.0
Attached Router: 192.168.239.66
Attached Router: 10.187.241.5
Attached Router: 10.187.1.1
Attached Router: 10.187.54.5
Attached Router: 10.187.1.5
```

次に、**show ospf database summary** コマンドの出力例を示します。

```
> show ospf database summary
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Summary Net Link States(Area 0.0.0.0)
LS age: 1401
Options: (No TOS-capability)
LS Type: Summary Links(Network)
Link State ID: 10.187.240.0 (summary Network Number)
Advertising Router: 10.187.241.5
LS Seq Number: 80000072
Checksum: 0x84FF
Length: 28
Network Mask: 255.255.255.0 TOS: 0 Metric: 1
```

次に、 **show ospf database external** コマンドの出力例を示します。

```
> show ospf database external
OSPF Router with id(192.168.239.66) (Autonomous system 300)

                  Displaying AS External Link States
LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
```

```
Link State ID: 172.16.0.0 (External Network Number)
Advertising Router: 10.187.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0

      Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 1
Forward Address: 0.0.0.0
External Route Tag: 0
```

# show ospf events

OSPF 内部イベントの情報を表示するには、**show ospf events** コマンドを使用します。

**show ospf** ［**vrf** *name* | **all**］ ［*process_id*］ **events** ［*type*］

## 構文の説明

| | |
|---|---|
| *process_id* | （オプション）ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。 |
| *type* | （オプション）表示するイベント タイプのリスト。タイプを 1 つ以上指定しないと、すべてのイベントが表示されます。次のタイプでフィルタリングできます。<br>• **generic**：一般的なイベント。<br>• **interface**：インターフェイス状態変化イベント。<br>• **lsa**：LSA 到着イベントおよび LSA 生成イベント。<br>• **neighbor**：ネイバー状態変化イベント。<br>• **reverse**：逆の順序でイベントを表示。<br>• **rib**：ルータ情報ベースの更新イベント、削除イベント、および再配布イベント。<br>• **spf**：SPF のスケジューリングイベントおよびSPF 実行イベント。 |
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |

### 例

次に、**show ospf events** コマンドの出力例を示します。

```
> show ospf events
```

```
          OSPF Router with ID (192.168.77.1) (Process ID 5)

1 Apr 27 16:33:23.556: RIB Redist, dest 0.0.0.0, mask 0.0.0.0, Up
2 Apr 27 16:33:23.556: Rescanning RIB:  0x00x0
3 Apr 27 16:33:23.556: Service Redist scan:  0x00x0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ospf** | OSPF ルーティング プロセスのすべての設定を表示します。 |
| **show ospf border-routers** | エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）への内部 OSPF ルーティング テーブル エントリを表示します。 |

# show ospf flood-list

いずれかのインターフェイスを介したフラッディングを待機しているOSPF LSAのリストを表示するには、**show ospf flood-list** コマンドを使用します。

**show ospf flood-list** ［**vrf** *name* | **all**］ *interface_name*

## 構文の説明

| | |
|---|---|
| *interface_name* | ネイバー情報を表示するインターフェイスの名前。 |
| ［**vrf** *name* \| **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらのVRF関連キーワードのいずれも含めない場合、コマンドはグローバルVRF仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* \| **all**］ キーワードが追加されました。 |

### 例

次に、**show ospf flood-list** コマンドの出力例を示します。

```
> show ospf flood-list outside

  Interface outside, Queue length 20
  Link state flooding due in 12 msec

  Type  LS ID          ADV RTR          Seq NO       Age   Checksum
     5  10.2.195.0     192.168.0.163    0x80000009   0     0xFB61
     5  10.1.192.0     192.168.0.163    0x80000009   0     0x2938
     5  10.2.194.0     192.168.0.163    0x80000009   0     0x757
     5  10.1.193.0     192.168.0.163    0x80000009   0     0x1E42
     5  10.2.193.0     192.168.0.163    0x80000009   0     0x124D
     5  10.1.194.0     192.168.0.163    0x80000009   0     0x134C
```

# show ospf interface

OSPF 関連のインターフェイス情報を表示するには、**show ospf interface** コマンドを入力します。

**show ospf interface** ［**vrf** *name* | **all**］ ［*interface_name*］

## 構文の説明

| | |
|---|---|
| *interface_name* | （任意）OSPF 関連の情報を表示するインターフェイスの名前。 |
| ［**vrf** *name* \| **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## コマンド デフォルト

インターフェイスを指定しない場合は、すべてのインターフェイスに関する OSPF 情報が表示されます。

## 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。 |
| 6.6 | ［**vrf** *name* \| **all**］ キーワードが追加されました。 |

### 例

次に、**show ospf interface** コマンドの出力例を示します。

```
> show ospf interface outside
out is up, line protocol is up
  Internet Address 10.0.3.4 mask 255.255.255.0, Area 0
  Process ID 2, Router ID 10.0.3.4, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10 msec, Dead 1, Wait 1, Retransmit 5
    Hello due in 5 msec
    Wait time before Designated router selection 0:00:11
  Index 1/1, flood queue length 0
  Next 0x00000000(0)/0x00000000(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

# show ospf neighbor

OSPF ネイバー情報をインターフェイス単位で表示するには、**show ospf neighbor** コマンドを使用します。

**show ospf neighbor** ［**vrf** *name* | **all**］ ［**detail** | *interface_name* ［*nbr_router_id*］］

## 構文の説明

| | |
|---|---|
| **detail** | （任意）指定したルータに関する詳細な情報を表示します。 |
| *interface_name* | （任意）ネイバー情報を表示するインターフェイスの名前。 |
| *nbr_router_id* | （任意）ネイバー ルータのルータ ID。 |
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |

### 例

次に、**show ospf neighbor** コマンドの出力例を示します。ここでは、インターフェイスごとの OSPF ネイバー情報を表示する例を示しています。

```
> show ospf neighbor outside

Neighbor 192.168.5.2, interface address 10.225.200.28
    In the area 0 via interface outside
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 10.225.200.28 BDR is 10.225.200.30
    Options is 0x42
    Dead timer due in 00:00:36
    Neighbor is up for 00:09:46
  Index 1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

次に、**show ospf neighbor detail** コマンドの出力例を示します。指定された OSPF ネイバーの詳細情報を表示する方法を示します。

```
> show ospf neighbor detail

Neighbor 25.1.1.60, interface address 15.1.1.60
    In the area 0 via interface inside
    Neighbor priority is 1, State is FULL, 46 state changes
    DR is 15.1.1.62 BDR is 15.1.1.60
    Options is 0x12 in Hello (E-bit, L-bit)
    Options is 0x52 in DBD (E-bit, L-bit, O-bit)
    LLS Options is 0x1 (LR), last OOB-Resync 00:03:07 ago
    Dead timer due in 0:00:24
    Neighbor is up for 01:42:15
    Index 5/5, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

# show ospf nsf

OSPFv2 関連の NSF 情報を表示するには、**show ospf nsf** コマンドを入力します。

**show ospf nsf** ［**vrf** *name* | **all**］

## 構文の説明

| | |
|---|---|
| ［**vrf** *name* \| **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* \| **all**］ キーワードが追加されました。 |

### 例

次に、**show ospf nsf** コマンドの出力例を示します。

```
> show ospf nsf
Routing Process "ospf 10"
Non-Stop Forwarding enabled
    Clustering is not configured in spanned etherchannel mode
IETF NSF helper support enabled
Cisco NSF helper support enabled
    OSPF restart state is
    Handle 1, Router ID 25.1.1.60, checkpoint Router ID 0.0.0.0
    Config wait timer interval 10, timer not running
    Dbase wait timer interval 120, timer not running
```

# show ospf request-list

ルータによって要求されたすべての LSA のリストを表示するには、**show ospf request-list** コマンドを使用します。

**show ospf request-list** ［**vrf** *name* | **all**］ *nbr_router_id interface_name*

## 構文の説明

| | |
|---|---|
| *interface_name* | ネイバー情報を表示するインターフェイスの名前。このインターフェイスからルータによって要求されたすべての LSA のリストを表示します。 |
| *nbr_router_id* | ネイバー ルータのルータ ID。このネイバーからルータによって要求されたすべての LSA のリストを表示します。 |
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |

### 例

次に、**show ospf request-list** コマンドの出力例を示します。

```
> show ospf request-list 192.168.1.12 inside

         OSPF Router with ID (192.168.1.11) (Process ID 1)

  Neighbor 192.168.1.12, interface inside address 172.16.1.12

  Type   LS ID          ADV RTR        Seq NO       Age   Checksum
     1   192.168.1.12   192.168.1.12   0x8000020D   8     0x6572
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ospf retransmission-list** | 再送信を待機しているすべての LSA のリストを表示します。 |

# show ospf retransmission-list

特定のネイバーおよびインターフェイスに対する再送信を待機しているすべての LSA のリストを表示するには、**show ospf retransmission-list** コマンドを使用します。

**show ospf retransmission-list** ［**vrf** *name* | **all**］ *nbr_router_id interface_name*

## 構文の説明

| | |
|---|---|
| *interface_name* | ネイバー情報を表示するインターフェイスの名前。 |
| *nbr_router_id* | ネイバー ルータのルータ ID。 |
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |

### 例

次に、外部インターフェイス上の 192.168.1.11 ネイバールータに対する **show ospf retransmission-list** コマンドの出力例を示します。

```
> show ospf retransmission-list 192.168.1.11 outside

         OSPF Router with ID (192.168.1.12) (Process ID 1)

 Neighbor 192.168.1.11, interface outside address 172.16.1.11

 Link state retransmission due in 3764 msec, Queue length 2
 Type   LS ID          ADV RTR        Seq NO       Age   Checksum
    1   192.168.1.12   192.168.1.12   0x80000210   0     0xB196
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ospf request-list** | ルータによって要求されたすべての LSA のリストを表示します。 |

# show ospf rib

OSPF ルータ情報ベース（RIB）を表示するには、**show ospf rib** コマンドを使用します。

**show ospf** ［**vrf** *name* | **all**］ ［*process_id* ［*area_id*］］ **rib** ［*network_prefix* ［*network_mask*］］ | **detail** | **redistribution** ［*network_prefix* ［*network_mask*］］ | **detail**］］

## 構文の説明

| | |
|---|---|
| *process_id* | （任意）OSPF プロセスの ID。 |
| *area_id* | （任意）OSPF アドレス範囲に関連付けられているエリアの ID。 |
| *network_prefix* [*network_mask*] | （オプション）表示するルータのネットワーク プレフィックスおよびオプションでマスク。次に例を示します。<br>10.100.10.1<br>10.100.10.0 255.255.255.0 |
| **detail** | （オプション）RIB に関する詳細情報を表示します。 |
| **redistribution** | （オプション）再配布情報を表示します。ネットワークプレフィックスとマスクを指定するか、redistribution キーワードの後ろに **detail** キーワードを指定することもできます。 |
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |

# show ospf statistics

さまざまなOSPF統計（SPFが実行された回数、理由、期間など）を表示するには、**show ospf statistics** コマンドを使用します。

**show ospf** ［**vrf** *name* ｜ **all**］ ［*process_id*］ **statistics** ［**detail**］

## 構文の説明

| | |
|---|---|
| **detail** | （オプション）トリガー ポイントを含む詳細な SPF 情報を指定します。 |
| *process_id* | （オプション）ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティング プロセスがイネーブルになっている場合に、管理上割り当てられる番号です。 |
| ［**vrf** *name* ｜ **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* ｜ **all**］ キーワードが追加されました。 |

### 例

次に、**show ospf statistics** コマンドの出力例を示します。

```
> show ospf 10 statistics detail
Area 10: SPF algorithm executed 6 times

SPF 1 executed 04:36:56 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
       0      0      0      0      0      0      0 0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
               0            0
  LSIDs processed R:1 N:0 Prefix:0 SN:0 SA:0 X7:0
  Change record R L
  LSAs changed 2
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  49.100.168.192/0(R) 49.100.168.192/2(L)

SPF 2 executed 04:35:50 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
```

```
     0      0      0      0      0      0      0 0
RIB manipulation time (in msec):
RIB Update    RIB Delete
             0             0
LSIDs processed R:2 N:1 Prefix:0 SN:0 SA:0 X7:0
Change record R N L
LSAs changed 5
Changed LSAs. Recorded is Advertising Router, LSID and LS type:
50.100.168.192/0(R) 50.100.168.192/2(L) 49.100.168.192/0(R) 50.100.168.192/0(R)
50.100.168.192/2(N)
```

# show ospf summary-address

OSPF プロセスで設定されているすべてのサマリーアドレス再配布情報のリストを表示するには、**show ospf summary-address** コマンドを使用します。

**show ospf summary-address** ［**vrf** *name* | **all**］

## 構文の説明

| | |
|---|---|
| ［**vrf** *name* \| **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* \| **all**］ キーワードが追加されました。 |

### 例

次に、**show ospf summary-address** コマンドの出力例を示します。この例は、ID が 5 である OSPF プロセスに対してサマリーアドレスが設定される前に、すべてのサマリーアドレス再配布情報のリストを表示する方法を示しています。

```
> show ospf 5 summary-address

OSPF Process 2, Summary-address

10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 0
10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 10
```

# show ospf traffic

特定の OSPF インスタンスによって処理（送信または受信）されたパケットのさまざまなタイプのリストを表示するには、**show ospf traffic** コマンドを使用します。

**show ospf traffic** ［**vrf** *name* | **all**］

## 構文の説明

| | |
|---|---|
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |

## 使用上のガイドライン

このコマンドを使用すると、デバッグを有効にすることなく、処理されるさまざまなタイプの OSPF パケットのスナップショットを取得できます。2 つの OSPF インスタンスが設定されている場合、**show ospf traffic** コマンドを使用すると、両方のインスタンスの統計情報が各インスタンスのプロセス ID とともに表示されます。**show ospf** *process_id* **traffic** コマンドを使用して、シングルインスタンスの統計情報を表示することもできます。

### 例

次に、**show ospf traffic** コマンドの出力例を示します。

```
> show ospf traffic

OSPF statistics (Process ID 70):

       Rcvd: 244 total, 0 checksum errors
             234 hello, 4 database desc, 1 link state req
             3 link state updates, 2 link state acks
       Sent: 485 total
             472 hello, 7 database desc, 1 link state req
             3 link state updates, 2 link state acks
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ospf virtual-links** | OSPF 仮想リンクのパラメータと現在の状態を表示します。 |

# show ospf virtual-links

OSPF 仮想リンクのパラメータと現在の状態を表示するには、**show ospf virtual-links** コマンドを使用します。

**show ospf virtual-links** ［**vrf** *name* | **all**］

## 構文の説明

| | |
|---|---|
| ［**vrf** *name* | **all**］ | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してコマンドを特定の仮想ルータに制限できます。すべての仮想ルータにコマンドを作用させる場合は、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータに適用されます。 |

## 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。 |
| 6.6 | ［**vrf** *name* | **all**］ キーワードが追加されました。 |

### 例

次に、**show ospf virtual-links** コマンドの出力例を示します。

```
> show ospf virtual-links

Virtual Link to router 192.168.101.2 is up
Transit area 0.0.0.1, via interface Ethernet0, Cost of using 10
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Adjacency State FULL
```

# show p - show r

# show packet tracer

pcap トレース出力に関する情報を表示するには、**show packet tracer** コマンドを使用します。

**show packet-tracer pcap trace** ［ **packet-number** *number* | **summary** | **detailed** | **status** ］

## 構文の説明

| | |
|---|---|
| **packet-number** | （オプション）pcapの単一のパケットのトレース出力を表示します。 |
| **summary** | （オプション）pcap のサマリーを表示します。 |
| **detailed** | （オプション）pcap のすべてのパケットのトレース出力を表示します。 |
| **status** | （オプション）pcap トレースの現在の実行状態を表示します。 |

## コマンド デフォルト

デフォルトの動作や値はありません。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1 | pcap トレースの出力を含むようにコマンドが拡張されました。 |

## 使用上のガイドライン

**show packet-tracer** コマンドは、パケットトレーサの出力を表示します。**pcap trace** コマンドを使用すると、PCAP ファイルに対して最後に実行されたパケットトレーサのトレースバッファ出力を表示できます。

### 例

次に、**show packet-tracer pcap trace summary** コマンドの出力例を示します。

```
> show packet-tracer pcap trace summary
      1: 02:38:01.265123       6.1.1.100.51944 > 9.1.1.100.80: S 542888804:542888804(0)
 win 29200 <mss 1460,sackOK,timestamp 2526545680 0,nop,wscale 7>
     2: 02:38:01.271317      9.1.1.100.80 > 6.1.1.100.51944: S 2281169942:2281169942(0)
 ack 542888805 win 28960 <mss 1380,sackOK,timestamp 2526520070 2526545680,nop,wscale 7>

      3: 02:38:01.271638       6.1.1.100.51944 > 9.1.1.100.80: . ack 2281169943 win 229
 <nop,nop,timestamp 2526545682 2526520070>

               Total packets: 3
       Packets replayed: 3
       Result: Allow
       Start time: Mar 28 04:51:54
       Total time taken: 10247935ns
     show packet-tracer pcap trace packet-number 1 detailed
     1: 02:38:01.265123 0050.56a9.81e5 0050.56a9.60e1 0x0800 Length: 74
      6.1.1.100.51944 > 9.1.1.100.80: S [tcp sum ok] 542888804:542888804(0) win 29200
<mss 1460,sackOK,timestamp 2526545680 0,nop,wscale 7> (DF) (ttl 64, id 54388)
      Phase: 1
      Type: ACCESS-LIST
      Subtype:
      Result: ALLOW
```

```
Time Spent: 12345 ns
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
 in  id=0x154523db3ce0, priority=1, domain=permit, deny=false
                hits=92, user_data=0x0, cs_id=0x0, l3_type=0x8
                src mac=0000.0000.0000, mask=0000.0000.0000
                dst mac=0000.0000.0000, mask=0100.0000.0000
                input_ifc=inside, output_ifc=any
 …
 …
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **packet tracer** | ファイアウォールの現在の設定に対して5～6組のパケットを生成します。 |

# show packet-statistics

Cisco Secure Firewall 3100 でのパケットドロップに関するポリシー以外の情報を表示するには、**show packet-statistics** コマンドを使用します。Threat Defense でこのコマンドをシステム診断モードで実行します。

**show packet-statistics** { **interface id** *slot port* } [ **breakout** *port* | { **brief** | **no brief** } ]

## 構文の説明

| | |
|---|---|
| **interface id***slotport* | 統計が表示されるスロット番号とポート番号を含むインターフェイス名。 |
| **breakout** | （任意）イーサネットのポート番号のブレークアウト。 |
| **brief** | （任意）ゼロカウンタ値を除いた出力を表示します。 |

## コマンド デフォルト

デフォルトの動作や値はありません。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2 | このコマンドが追加されました。 |

## 使用上のガイドライン

**show packet-statistics** コマンドは、複数の送信元のパケット損失データを照合して表示します。出力は、パケットがドロップされた場所を特定するのに役立ちます。このコマンドは、次のデバッグコマンドの出力を統合します。

- **show portmanager counters ethernet <slot> <port>**
- **show queuing interface ethernet <slot> <port>**
- **show portmanager counters internal <slot> <port>**
- **show queuing interface internal <slot> <port>**
- **show portmanager switch counters packet-trace**
- **show npu-accel statistics**
- **show interface detail**
- **show asp drop**

統合された出力は、トラフィックがデバイスに到達したときのデータパスのシーケンスで表示されます。さらに、統合された出力が他の CLI の出力によって壊されたり、中断されたりはしません。

特定のインターフェイスの出力を制限するには、*slot/port* と **breakout***port* を使用します。これらの変数とキーワードは、外部スイッチポートと Lina インターフェイスにのみ適用されます。他のインターフェイスの場合、これらの変数は無視されます。

## 例

次に、**show packet-statistics** コマンドの出力例を示します。

```
$ show packet-statistics ethernet 2/1/1 no brief

====================== show portmanager switch counters packet-trace ======================


       Counter                              Description
---------------------- ------------------------------------------------------------
goodOctetsRcv          Number of ethernet frames received that are not bad
                       ethernet frames or MAC Control pkts
badOctetsRcv           Sum of lengths of all bad ethernet frames received
gtBrgInFrames          Number of packets received
gtBrgVlanIngFilterDisc Number of packets discarded due to VLAN Ingress Filtering
gtBrgSecFilterDisc     Number of packets discarded due to
                       Security Filtering measures
gtBrgLocalPropDisc     Number of packets discarded due to reasons other than
                       VLAN ingress and Security filtering
dropCounter            Ingress Drop Counter
outUcFrames            Number of unicast packets transmitted
outMcFrames            Number of multicast packets transmitted. This includes
                       registered multicasts, unregistered multicasts
                       and unknown unicast packets
outBcFrames            Number of broadcast packets transmitted
brgEgrFilterDisc       Number of IN packets that were Bridge Egress filtered
txqFilterDisc          Number of IN packets that were filtered
                       due to TxQ congestion
outCtrlFrames          Number of out control packets
                       (to cpu, from cpu and to  analyzer)
egrFrwDropFrames       Number of packets dropped due to egress
                       forwarding restrictions
goodOctetsSent         Sum of lengths of all good ethernet
                       frames sent from this MAC


        Counter            Source port- 0/0    Destination port- 0/0
-----------------------  --------------------  ---------------------
goodOctetsRcv                    ---                    ---
badOctetsRcv                      ---                    ---

                                       Ingress counters
gtBrgInFrames                    9515                   9515
gtBrgVlanIngFilterDisc             0                      0
gtBrgSecFilterDisc                 0                      0
gtBrgLocalPropDisc                 0                      0
dropCounter                      319           Only for source-port

                                       Egress counters
outUcFrames                       12                     12
outMcFrames                     8176                   8176
outBcFrames                     1008                   1008
brgEgrFilterDisc                   0                      0
txqFilterDisc                      0                      0
outCtrlFrames                      0                      0
egrFrwDropFrames                   0                      0

goodOctetsSent                    ---                    ---

Error at clearing mac counters0/0: GT_BAD_PARAM = Illegal parameter in function called
```

```
------------------------------------------------------------

====================== show npu-accel statistics ======================
module: kc25-pcie, pipe: 0
--------------------------
reg_pcie_rcv_reg_access_rd_tlp_cnt = 28374275
reg_pcie_rcv_reg_access_wr_tlp_cnt = 3810207

module: kc25-eth, pipe: 0
-------------------------
stat_rx_bip_err_0 = 0
stat_rx_bip_err_1 = 0
stat_rx_bip_err_2 = 0
stat_rx_bip_err_3 = 0
stat_rx_framing_err_0 = 0
stat_rx_framing_err_1 = 0
stat_rx_framing_err_2 = 0
stat_rx_framing_err_3 = 0
stat_rx_bad_code = 0
stat_tx_frame_error = 0
stat_tx_total_packets = 0
stat_tx_total_good_packets = 0
stat_tx_total_bytes = 0
stat_tx_total_good_bytes = 0
stat_tx_packet_64_bytes = 0
stat_tx_packet_65_127_bytes = 0
stat_tx_packet_128_255_bytes = 0
stat_tx_packet_256_511_bytes = 0
stat_tx_packet_512_1023_bytes = 0
stat_tx_packet_1024_1518_bytes = 0
stat_tx_packet_1519_1522_bytes = 0
stat_tx_packet_1523_1548_bytes = 0
stat_tx_packet_1549_2047_bytes = 0
stat_tx_packet_2048_4095_bytes = 0
stat_tx_packet_4096_8191_bytes = 0
stat_tx_packet_8192_9215_bytes = 0
stat_tx_packet_large = 0
stat_tx_packet_small = 0
stat_tx_bad_fcs = 0
stat_tx_unicast = 0
stat_tx_multicast = 0
stat_tx_broadcast = 0
stat_tx_vlan = 0
stat_tx_pause = 0
stat_tx_user_pause = 0
stat_rx_total_packets = 964
stat_rx_total_good_packets = 964
stat_rx_total_bytes = 264439
stat_rx_total_good_bytes = 264439
stat_rx_packet_64_bytes = 0
stat_rx_packet_65_127_bytes = 35
stat_rx_packet_128_255_bytes = 0
stat_rx_packet_256_511_bytes = 929
stat_rx_packet_512_1023_bytes = 0
stat_rx_packet_1024_1518_bytes = 0
stat_rx_packet_1519_1522_bytes = 0
stat_rx_packet_1523_1548_bytes = 0
stat_rx_packet_1549_2047_bytes = 0
stat_rx_packet_2048_4095_bytes = 0
stat_rx_packet_4096_8191_bytes = 0
stat_rx_packet_8192_9215_bytes = 0
stat_rx_packet_large = 0
stat_rx_undersize = 0
```

```
stat_rx_fragment = 0
stat_rx_oversize = 0
stat_rx_toolong = 0
stat_rx_jabber = 0
stat_rx_bad_fcs = 0
stat_rx_packet_bad_fcs = 0
stat_rx_stomped_fcs = 0
stat_rx_unicast = 0
stat_rx_multicast = 0
stat_rx_broadcast = 964
stat_rx_vlan = 0
stat_rx_pause = 0
stat_rx_user_pause = 0
stat_rx_inrangeerr = 0
stat_rx_truncated = 0
eth_tx_good_pkt_cnt = 0
eth_tx_err_pkt_cnt = 0
eth_rx_good_pkt_cnt = 964
eth_tx_fifo_sbit_err_cnt = 0
eth_tx_fifo_dbit_err_cnt = 0
eth_rx_fifo_sbit_err_cnt = 0
eth_rx_fifo_dbit_err_cnt = 0

module: kc25-nic, pipe: 0
-------------------------
nic_top_in_pkt_cnt = 964
nic_top_tm_out_pkt_cnt = 971
nic_top_inband_flow_tbl_pkt_cnt = 7
nic_top_inband_stat_pkt_cnt = 0
tm_shared_mem_sbiterr_pkt_cnt = 0
tm_shared_mem_dbiterr_pkt_cnt = 0
tm_pkt_buf_sbiterr_pkt_cnt = 0
tm_pkt_buf_dbiterr_pkt_cnt = 0
tm_out_fifo_sbiterr_pkt_cnt = 0
tm_out_fifo_dbiterr_pkt_cnt = 0
tm_qm_mem_parerr_pkt_cnt = 0
tm_budm_mem_parerr_pkt_cnt = 0
tm_qm_taildrop_pkt_cnt = 0
tm_h2c_desc_mem_sbiterr_pkt_cnt = 0
tm_h2c_desc_mem_dbiterr_pkt_cnt = 0
tm_c2h_desc_mem_sbiterr_pkt_cnt = 0
tm_c2h_desc_mem_dbiterr_pkt_cnt = 0
tm_inband_fifo_sbiterr_pkt_cnt = 0
tm_inband_fifo_dbiterr_pkt_cnt = 0
tm_egr_fifo_sbiterr_pkt_cnt = 0
tm_egr_fifo_dbiterr_pkt_cnt = 0

Traffic Manager per Q statistics
qid             input pkts           output pkts   input tail-drop cnt
  0                     49                    49                     0
  1                      0                     0                     0
  2                     66                    66                     0
  3                      0                     0                     0
  4                     42                    42                     0
  5                      0                     0                     0
  6                     64                    64                     0
  7                      0                     0                     0
  8                      0                     0                     0
  9                     42                    42                     0
 10                      0                     0                     0
 11                     64                    64                     0
 12                      0                     0                     0
 13                     64                    64                     0
 14                      0                     0                     0
```

```
 15                    64                    64                    0
 16                     0                     0                    0
 17                    88                    88                    0
 18                     0                     0                    0
 19                    24                    24                    0
 20                     0                     0                    0
 21                    64                    64                    0
 22                    40                    40                    0
 23                    64                    64                    0
 24                    42                    42                    0
 25                    42                    42                    0
 26                    42                    42                    0
 27                     0                     0                    0
 28                     0                     0                    0
 29                    39                    39                    0
 30                    64                    64                    0
 31                     0                     0                    0
 32                     0                     0                    0
 33                     0                     0                    0
 34                     0                     0                    0
 35                     0                     0                    0
 36                     0                     0                    0
 37                     0                     0                    0
 38                     0                     0                    0
 39                     0                     0                    0
 40                     0                     0                    0
 41                     0                     0                    0
 42                     0                     0                    0
 43                     0                     0                    0
 44                     0                     0                    0
 45                     0                     0                    0
 46                     0                     0                    0
 47                     0                     0                    0
 48                     0                     0                    0
 49                     0                     0                    0
 50                     0                     0                    0
 51                     0                     0                    0
 52                     0                     0                    0
 53                     0                     0                    0
 54                     0                     0                    0
 55                     0                     0                    0
 56                     0                     0                    0
 57                     0                     0                    0
 58                     0                     0                    0
 59                     0                     0                    0
 60                     0                     0                    0
 61                     0                     0                    0
 62                     0                     0                    0
 63                     0                     0                    0

module: kc25-ingress-pkt-classifier, pipe: 0
-------------------------------------------
cla_opt_tbl_hit_cmd_cnt = 0
cla_opt_tbl_miss_cmd_cnt = 958
cla_tunnel_tbl_hit_cmd_cnt = 0
cla_tunnel_tbl_miss_cmd_cnt = 0
cla_6_tuple_tbl_hit_cmd_cnt = 0
cla_6_tuple_tbl_miss_cmd_cnt = 0
cla_4_tuple_tbl_hit_cmd_cnt = 0
cla_4_tuple_tbl_miss_cmd_cnt = 0
cla_bypass_in_cmd_cnt = 6
cla_non_bypass_in_cmd_cnt = 958
cla_rss_lookup_cmd_cnt = 958
cla_rss_bypass_cmd_cnt = 6
```

```
cla_opt_tbl_sbiterr_pkt_cnt = 0
cla_opt_tbl_dbiterr_pkt_cnt = 0
cla_tunnel_tbl_sbiterr_pkt_cnt = 0
cla_tunnel_tbl_dbiterr_pkt_cnt = 0
cla_6_tuple_tbl_sbiterr_pkt_cnt = 0
cla_6_tuple_tbl_dbiterr_pkt_cnt = 0
cla_4_tuple_tbl_sbiterr_pkt_cnt = 0
cla_4_tuple_tbl_dbiterr_pkt_cnt = 0
cla_vf_dma_qid_ram_dbiterr_pkt_cnt = 0
inbf_ram_sbiterr_cnt = 0
inbf_ram_dbiterr_cnt = 0
inbf_rx_request_pkt_cnt = 270327
inbf_tx_response_pkt_cnt = 7
inbf_parser_regrd_cnt = 1
inbf_cmdgen_regrd_cnt = 1
inbf_cmdgen_regwr_cnt = 302068967
inbf_rx_err0_pkt_cnt = 0
inbf_rx_err1_pkt_cnt = 0
inbf_rx_err2_pkt_cnt = 0
inbf_rx_err3_pkt_cnt = 0
inbf_rx_err4_pkt_cnt = 0
inbf_exec_cmd_err_cnt = 0
inbf_wdata_err_cnt = 0
inbf_act_tbl_timeout_cnt = 0
cla_ipsec_sn_tbl_parerr_pkt_cnt = 0
stat_fifo_parerr_pkt_cnt = 0
stat_ag_ram_dbiterr_pkt_cnt = 0
stat_acc_ram_dbiterr_pkt_cnt = 0
stat_ddr_rl_ram_dbiterr_pkt_cnt = 0
stat_ag_ram_sbiterr_pkt_cnt = 0
stat_acc_ram_sbiterr_pkt_cnt = 0
stat_ddr_rl_ram_sbiterr_pkt_cnt = 0
inbs_ram_dbiterr_cnt = 0
stat_in_rx_pkt_cnt = 0
acc_cache_access_col_cnt = 0
acc_cache_insert_fail_cnt = 0
acc_cache_replace_cnt = 0
acc_cache_cpu_col_cnt = 0
ddr_rx_pkt_cnt = 0
ddr_rl_cache_insert_fail_cnt = 0
ddr_rl_cache_insert_update_cnt = 0
ddr_read_cnt = 0
ddr_write_cnt = 0
inbs_rx_request_pkt_cnt = 0
inbs_tx_response_pkt_cnt = 0
inbs_stat_collect_cnt = 0
inbs_rx_err0_pkt_cnt = 0
inbs_rx_err1_pkt_cnt = 0
inbs_rx_err2_pkt_cnt = 0
inbs_rx_err3_pkt_cnt = 0
inbs_rx_err4_pkt_cnt = 0
inbs_exec_cmd_err_cnt = 0
inbs_stat_collect_timeout_err_cnt = 0
key_tbl_dbiterr_pkt_cnt = 0
ts_tbl_dbiterr_pkt_cnt = 0
act_tbl_sbiterr_pkt_cnt = 0
act_tbl_dbiterr_pkt_cnt = 0

module: kc25-ingress-pkt-processor, pipe: 0
-------------------------------------------
proc_pkt_in_cnt = 964
proc_nic_pkt_out_cnt = 964
proc_egr_pkt_out_cnt = 0
proc_ilk_pkt_out_cnt = 0
```

```
proc_cap_be_pkt_out_cnt = 0
proc_cap_ae_pkt_out_cnt = 0
proc_cap_tail_drop_cnt = 0
proc_instr_drop_pkt_cnt = 0
proc_err_ar_drop_pkt_cnt = 0
proc_pkt_in_fifo_sbiterr_pkt_cnt = 0
proc_pkt_in_fifo_dbiterr_pkt_cnt = 0
proc_rwe_data_fifo_sbiterr_pkt_cnt = 0
proc_rwe_data_fifo_dbiterr_pkt_cnt = 0
proc_pkt_out_fifo_sbiterr_pkt_cnt = 0
proc_pkt_out_fifo_dbiterr_pkt_cnt = 0
proc_cap_be_pkt_fifo_sbiterr_pkt_cnt = 0
proc_cap_be_pkt_fifo_dbiterr_pkt_cnt = 0
proc_cap_ae_pkt_fifo_sbiterr_pkt_cnt = 0
proc_cap_ae_pkt_fifo_dbiterr_pkt_cnt = 0
proc_cks_chk_tcp_udp_err_pkt_cnt = 0
proc_cks_chk_ip_err_pkt_cnt = 0
proc_cks_chk_both_err_pkt_cnt = 0

module: kc25-ingress-pkt-parser, pipe: 0
----------------------------------------
par_hi_pri_q_good_pkt_cnt = 0
par_hi_pri_q_err_pkt_cnt = 0
par_hi_pri_q_taildrop_pkt_cnt = 0
par_md_pri_q_good_pkt_cnt = 0
par_md_pri_q_err_pkt_cnt = 0
par_md_pri_q_taildrop_pkt_cnt = 0
par_lo_pri_q_good_pkt_cnt = 964
par_lo_pri_q_err_pkt_cnt = 0
par_lo_pri_q_taildrop_pkt_cnt = 0
par_hi_pri_q_sbiterr_pkt_cnt = 0
par_hi_pri_q_dbiterr_pkt_cnt = 0
par_md_pri_q_sbiterr_pkt_cnt = 0
par_md_pri_q_dbiterr_pkt_cnt = 0
par_lo_pri_q_sbiterr_pkt_cnt = 0
par_lo_pri_q_dbiterr_pkt_cnt = 0

module: kc25-egress-scheduler, pipe: 0
---------------------------------------
egr_rx_ingr_good_pkt_cnt = 0
egr_rx_octeon_good_pkt_cnt = 0
egr_rx_all_good_pkt_cnt = 0
egr_rx_ingr_err_pkt_cnt = 0
egr_rx_octeon_err_pkt_cnt = 0
egr_rx_ingr_drop_pkt_cnt = 0
egr_rx_octeon_drop_pkt_cnt = 0
egr_tx_ingr_pkt_cnt = 0
egr_tx_octeon_pkt_cnt = 0
egr_tx_all_pkt_cnt = 0
egr_ingr_pktbuf_ecc_sbiterr_cnt = 0
egr_ingr_pktbuf_ecc_dbiterr_cnt = 0
egr_ingr_schefifo_ecc_sbiterr_cnt = 0
egr_ingr_schefifo_ecc_dbiterr_cnt = 0
egr_octeon_pktbuf_ecc_sbiterr_cnt = 0
egr_octeon_pktbuf_ecc_dbiterr_cnt = 0
egr_octeon_schefifo_ecc_sbiterr_cnt = 0
egr_octeon_schefifo_ecc_dbiterr_cnt = 0


------------------------------------------------------------

======================      show asp drop       ======================

Frame drop:
```

```
  Slowpath security checks failed (sp-security-failed)                    148
  FP L2 rule drop (l2_acl)                                                493
  Interface is down (interface-down)                                        2

Last clearing: Never

Flow drop:

Last clearing: Never

======================  show interface detail   ======================

Interface Ethernet1/1 "outside", is down, line protocol is down
  Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
 Full-Duplex, 1000 Mbps
 MAC address 6c13.d509.5194, MTU 1500
 IP address unassigned
 Auto-Negotiation is turned on
 0 packets input, 0 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 pause input, 0 resume input
 0 packets output, 0 bytes, 0 underruns
 0 pause output, 0 resume output
 0 output errors, 0 collisions, 0 interface resets
 0 late collisions, 0 deferred
 0 input reset drops, 0 output reset drops
  Traffic Statistics for "outside":
 0 packets input, 0 bytes
 0 packets output, 0 bytes
 0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
 Interface number is 5
 Interface config status is active
 Interface state is not active
```

# show pager

CLI セッションの現在のページ長、つまり出力が一時停止する前に表示される行数を「--More --」付きで表示するには、**show pager** コマンドを使用します。

**show pager**

（注） 脅威に対する防御 CLI のページ長は設定できません。

## 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、**show pager** コマンドの出力例を示します。脅威に対する防御 CLI ではページ長を設定できないため、出力にはページャがないことが示されます。

```
> show pager
no pager
```

# show packet debugs

保存されたデバッグログをデータベースから取得して表示するには、**show packet debugs** コマンドを使用します。一部のリリースでは、このコマンドはハイフンで区切られている（**show packet-debugs**）場合があります。

**show packet debugs** ［ **match** ［ *protocol* ］ ［ *source-ip* ］［ *source-port* ］［ *dest-ip* ］ ［ *dest-port* ］ ［ **module** *module-id* ］ ［ **packet-id** *packet-id* ］ ［ **severity** *0-7* ］［ **time-start** *time* ］ ［ **time-end** *time* ］］

## 構文の説明

| | |
|---|---|
| **match** | 接続をフィルタリングするために入力された次の 1 つ以上のオプションと照合します。送信元 IP、宛先 IP、送信元ポート、宛先ポート、またはプロトコル。 |
| *protocol* | プロトコルの名前。 |
| *source-ip* | 送信元の IP アドレス。 |
| *source-port* | 送信元のポート番号。 |
| *dest-ip* | 宛先の IP アドレス。 |
| *dest-port* | 宛先のポート番号。 |
| **module** *module-id* | デバッグログをフィルタリングするモジュール名。 |
| **packet-id** *packet-id* | デバッグログをフィルタリングする一意のパケット ID。 |
| **severity** *0 ～ 7* | 次のいずれかのシビラティ（重大度）レベル：<br>• 0（致命的）：システム使用不可<br>• 1（アラート）：迅速な対処が必要<br>• 2（重大）：重大な状態<br>• 3（エラー）：エラー状態<br>• 4（警告）：警告状態<br>• 5（通知）：正常だが重要な状態<br>• 6（情報）：情報メッセージのみ<br>• 7（デバッグ）：Debug（デバッグ）メッセージのみ |
| **time-start** *time* | 指定した開始時刻以降のすべてのログを返します。 |
| **time-end** *time* | 指定した時刻より前のすべてのログを返します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.4 | このコマンドが導入されました。 |

## 使用上のガイドライン

**show packet debugs** コマンドを使用して、保存されたデバッグログをデータベースから取得して表示します。

[]内のキーワードはすべてオプションです。特定のキーワードが入力されていない場合、そのキーワードはanyであると見なされます。すべてのデバッグは、タイムスタンプの昇順で表示されます。

### 例

次の例では、TCP デバッグを有効にして、デバッグステータスを表示します。

```
> show packet debugs
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **debug** | デバッグを有効にします。 |

# show parser dump

**show parser dump** コマンドは、内部用またはシスコ テクニカルサポート用です。

# show password encryption

パスワード暗号化の構成設定を表示するには、**show password encryption** コマンドを使用します。

**show password encryption**

## 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

脅威に対する防御 では、マスターパスワードの暗号化は設定できません。そのため、このコマンドを実行すると、パスワード暗号化が無効になっており、マスターキーハッシュが設定されていないことが常に表示されます。

キーが保存されている場合、キーハッシュの横に「saved」が表示されます。キーがない場合、またはキーが実行コンフィギュレーションから削除された場合、ハッシュ値の代わりに「Not set」が表示されます。

### 例

次に、**show password encryption** コマンドの出力例を示します。

```
> show password encryption
Password Encryption: Disabled
Master key hash: Not set(saved)
```

# show path-monitoring

パスモニタリング出力に関する情報を表示するには、**show path monitoring** コマンドを使用します。

**show path-monitoring** ［ **interface** *name* ］［ **detail** ］

## 構文の説明

| | |
|---|---|
| **Interface***name* | パスモニタリングメトリックが表示されるインターフェース |
| **detail** | （任意）パスモニタリングメトリックに関する詳細情報を表示します。 |

## コマンド デフォルト

デフォルトの動作や値はありません。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1 | 指定されたインターフェイスのパスモニタリングの詳細を表示するコマンドが導入されました。 |

## 使用上のガイドライン

**show path-monitoring** コマンドは、指定された出力インターフェイスのパスモニタリング出力を表示します。

### 例

次に、*outside 1* インターフェイスの **show path-monitoring** コマンドの出力例を示します。

```
firepower# show path-monitoring interface outside1
Interface: outside1
Remote peer: 90.2.1.1
    Version: 14275
    Remote peer reachable: Yes
    RTT average: 1407 microsecond(s)
    Jitter: 1218 microsecond(s)
    Packet loss: 0%
    MOS: 4.40
    Last updated: 1 second(s) ago
```

次に、*outside 1* インターフェイスの **show path-monitoring detail** コマンドの出力例を示します。

```
firepower#
firepower# show path-monitoring interface outside1 detail
Interface: outside1
Remote peer: 90.2.1.1
    Version: 14275
    Remote peer reachable: Yes
    RTT average: 1407 microsecond(s)
    Jitter: 1218 microsecond(s)
    Packet loss: 0%
```

```
MOS: 4.40
Last updated: 8 second(s) ago

Internal data:
    Total probes sent: 418553
    Total probes pending: 0
    Current probes pending: 0
    Current RTT sum: 51674
    Current RTT square sum: 154410282
    Flags: 0x2
    Current queue index: 14
    Index:  0, Timestamp:               0, RTT:     962
    Index:  1, Timestamp:               0, RTT:    1096
    Index:  2, Timestamp:               0, RTT:    1056
    Index:  3, Timestamp:               0, RTT:    1457
    Index:  4, Timestamp:               0, RTT:    1078
    Index:  5, Timestamp:               0, RTT:    1114
    Index:  6, Timestamp:               0, RTT:    1570
    Index:  7, Timestamp:               0, RTT:    6865
    Index:  8, Timestamp:               0, RTT:    1035
    Index:  9, Timestamp:               0, RTT:    1334
    Index: 10, Timestamp:               0, RTT:    1090
    Index: 11, Timestamp:               0, RTT:    1099
    Index: 12, Timestamp:               0, RTT:    1429
    Index: 13, Timestamp:               0, RTT:    1048
    Index: 14, Timestamp:               0, RTT:     985
    Index: 15, Timestamp:               0, RTT:    1002
    Index: 16, Timestamp:               0, RTT:    1013
    Index: 17, Timestamp:               0, RTT:    1741
    Index: 18, Timestamp:               0, RTT:    1231
    Index: 19, Timestamp:               0, RTT:    1517
    Index: 20, Timestamp:               0, RTT:    7780
    Index: 21, Timestamp:               0, RTT:    1018
    Index: 22, Timestamp:               0, RTT:    1036
    Index: 23, Timestamp:               0, RTT:    2369
    Index: 24, Timestamp:               0, RTT:    1120
    Index: 25, Timestamp:               0, RTT:    1062
    Index: 26, Timestamp:               0, RTT:    1088
    Index: 27, Timestamp:               0, RTT:    1073
    Index: 28, Timestamp:               0, RTT:    1060
    Index: 29, Timestamp:               0, RTT:    1071
    Index: 30, Timestamp:               0, RTT:    1116
    Index: 31, Timestamp:               0, RTT:    1075
    Index: 32, Timestamp:               0, RTT:    1084
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **policy-route** | インターフェイスにポリシーベースルーティングを設定します。 |

# show pclu

**show pclu** コマンドは、内部用またはシスコ テクニカルサポート用です。

# show perfmon

デバイスのパフォーマンスに関する情報を表示するには、**show perfmon** コマンドを使用します。

**show perfmon** ［**detail**］

## 構文の説明

| | |
|---|---|
| **detail** | （任意）追加の統計情報を表示します。これらの統計情報は Cisco Unified Firewall MIB のグローバル接続オブジェクトとプロトコルごとの接続オブジェクトにより収集された情報と一致します。 |

## 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

**perfmon** コマンドは、指定した間隔でパフォーマンス統計情報を連続的に表示します。**show perfmon** コマンドを使用すると、すぐに情報を表示できます。

### 例

次に、**show perfmon detail** コマンドの出力例を示します。

```
> show perfmon detail
PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
TCP Fixup            0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
TCP Intercept        0/s          0/s
SETUP RATES:
Connections for 1 minute = 0/s; 5 minutes = 0/s
TCP Conns for 1 minute = 0/s; 5 minutes = 0/s
UDP Conns for 1 minute = 0/s; 5 minutes = 0/s
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **perfmon** | 指定した間隔で詳細なパフォーマンス モニター情報を表示します。 |

# show perfstats

デバイスのパフォーマンスに関する統計情報を表示するには、**show perfstats** コマンドを使用します。

**show perfstats**

## 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

**show perfstats** コマンドは、検出エンジンのパフォーマンス情報を表示します。使用可能なエンジンのリストが表示されますので、統計情報を表示するエンジンを選択します。その後、いくつかのプロファイルが表示されますので、コンテンツを表示するプロファイルを選択します。

これらのファイルは、Management Center によってリモートで管理されるシステムに有効です。通常、これらのファイルには、ローカルマネージャである Device Manager を使用して管理されるシステムのコンテンツはありません。

ファイル全体を表示しない場合は、Crtl + C を使用して表示を停止します。ファイルのコンテンツが長くなる可能性があります。

### 例

```
> show perfstats
Available DEs:
  1 - Primary Detection Engine (703006f4-8ff6-11e6-bb6e-8f2d5febf243)
  0 - Cancel and return to CLI

Select a DE to profile: 1
Available now files:
  1 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/2016-10-13
  2 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/2016-10-16
  3 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/2016-10-11
  4 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/2016-10-15
  5 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/2016-10-14
  6 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/2016-10-12
  7 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/instance-1/now
  0 - Cancel and return to DE selection

Select a now file: 7
Mon Oct 17 00:05:00 2016
                 Pkts Recv: 162
                 Pkts Drop: 0
            Block Verdicts: 0
                 Mbits/Sec: 0.001
                 Drop Rate: 0%
                Alerts/Sec: 0
          Total Alerts/Sec: 0
(...remaining content truncated...)
```

# show pim bsr-router

ブートストラップルータ（BSR）情報を表示するには、**show pim bsr-router** コマンドを使用します。

**show pim bsr-router**

## 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、**show pim bsr-router** コマンドの出力例を示します。

```
> show pim bsr-router
PIMv2 Bootstrap information
This system is a candidate BSR
  Candidate BSR interface GigabitEthernet0/0 is down - BSR messages not originated
  Candidate RP: 4.4.4.1(GigabitEthernet0/0), GigabitEthernet0/0 is down - not advertised
```

# show pim df

ランデブーポイント（RP）またはインターフェイスについて、双方向 DF の「勝者」を表示するには、**show pim df** コマンドを使用します。

**show pim df** ［**winner**］［*rp_address* | *interface_name*］

## 構文の説明

| | |
|---|---|
| *rp_address* | 次のいずれか 1 つを指定できます。<br>• ドメインネームシステム（DNS）ホストテーブルで定義されている RP の名前。<br>• RP の IP アドレス。これは、4 分割ドット付き 10 進表記のマルチキャスト IP アドレスです。 |
| *interface_name* | インターフェイスの物理名または論理名。 |
| **winner** | （任意）DF 選出の勝者をインターフェイスごと、RP ごとに表示します。 |

## 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

このコマンドは、RP への勝者のメトリックも表示します。

### 例

次に、**show pim df** コマンドの出力例を示します。

```
> show pim df
RP           Interface   DF Winner   Metrics

172.16.1.3   Loopback3   172.17.3.2  [110/2]
172.16.1.3   Loopback2   172.17.2.2  [110/2]
172.16.1.3   Loopback1   172.17.1.2  [110/2]
172.16.1.3   inside      10.10.2.3   [0/0]
172.16.1.3   inside      10.10.1.2   [110/2]
```

# show pim group-map

グループからプロトコルへのマッピングテーブルを表示するには、**show pim group-map** コマンドを使用します。

**show pim group-map** ［**info-source** | **rp-timers**］［*group*］

## 構文の説明

| | |
|---|---|
| *group* | （任意）次のいずれかを指定できます。<br>• DNS ホストテーブルで定義されているマルチキャストグループの名前。<br>• マルチキャストグループの IPv4 または IPV6 アドレス。 |
| **info-source** | （任意）グループ範囲情報の情報源を表示します。 |
| **rp-timers** | （オプション）グループから RP へのマッピングのアップタイムと有効期限タイマーが表示されます。 |

## コマンド デフォルト

すべてのグループについて、グループからプロトコルへのマッピングを表示します。

## 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

このコマンドは、RP について、グループとプロトコルとのアドレス マッピングをすべて表示します。マッピングは、デバイス上でさまざまなクライアントから学習されます。

デバイスの PIM 実装は、さまざまな特殊エントリをマッピングテーブルで保持しています。Auto-rp グループ範囲は、スパース モード グループ範囲から明確に拒否されます。SSM グループ範囲もスパース モードには入りません。リンクローカル マルチキャスト グループ（224.0.0.0 ～ 224.0.0.225。224.0.0.0/24 として定義）も、スパース モード グループ範囲から拒否されます。最後のエントリは、所定の RP でスパース モードに入っている残りすべてのグループを示します。

### 例

次に、**show pim group-map** コマンドの出力例を示します。

```
> show pim group-map
Group Range      Proto   Client Groups   RP address   Info

224.0.1.39/32*   DM      static 1        0.0.0.0
224.0.1.40/32*   DM      static 1        0.0.0.0
224.0.0.0/24*    NO      static 0        0.0.0.0
232.0.0.0/8*     SSM     config 0        0.0.0.0
224.0.0.0/4*     SM      autorp 1        10.10.2.2    RPF: POS01/0/3,10.10.3.2
```

1 行めと 2 行めで、Auto-RP グループ範囲がスパース モード グループ範囲から明確に拒否されています。

3 行めでは、リンク ローカル マルチキャスト グループ（224.0.0.0 ～ 224.0.0.255。224.0.0.0/24 として定義）もスパース モード グループ範囲から拒否されています。

4 行めでは、PIM 送信元特定マルチキャスト（PIM-SSM）グループ範囲が 232.0.0.0/8 にマッピングされています。

最後のエントリは、残りすべてのグループがスパース モードに入って、RP 10.10.3.2 にマッピングされたことを示しています。

# show pim interface

PIM のインターフェイス固有情報を表示するには、**show pim interface** コマンドを使用します。

**show pim interface** ［*interface_name* | **state-off** | **state-on**］

## 構文の説明

| | |
|---|---|
| *interface_name* | （任意）インターフェイスの名前。この引数を指定すると、表示される情報は指定したインターフェイスに関するものだけになります。 |
| **state-off** | （任意）PIM がディセーブルになっているインターフェイスを表示します。 |
| **state-on** | （任意）PIM がイネーブルになっているインターフェイスを表示します。 |

## コマンド デフォルト

インターフェイスを指定しない場合は、すべてのインターフェイスに関する PIM 情報が表示されます。

## 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

脅威に対する防御 デバイス自体が PIM ネイバーです。したがって、このコマンドの出力にあるネイバー数カラムでは、ネイバー数が実際の数よりも 1 つ多く表示されます。

### 例

次に、内部インターフェイスに関する PIM 情報を表示する例を示します。

```
> show pim interface inside
Address    Interface      Ver/     Nbr     Query      DR     DR
                          Mode     Count   Intvl      Prior
172.16.1.4 inside         v2/S     2       100 ms     1      172.16.1.4
```

# show pim join-prune statistic

PIM join/prune の集約統計を表示するには、**show pim join-prune statistic** コマンドを使用します。

**show pim join-prune statistic** ［*interface_name*］

## 構文の説明

| | |
|---|---|
| *interface_name* | （任意）インターフェイスの名前。この引数を指定すると、表示される情報は指定したインターフェイスに関するものだけになります。 |

## コマンド デフォルト

インターフェイスを指定しない場合は、すべてのインターフェイスについて、加入とプルーニングに関する統計情報が表示されます。

## 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

PIM join/prune に関する統計情報をクリアするには、 **clear pim counters** コマンドを使用します。

### 例

次に、**show pim join-prune statistic** コマンドの出力例を示します。

```
> show pim join-prune statistic
PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface          Transmitted             Received
             inside   0 /    0 /    0         0 /    0 /    0
   GigabitEthernet1   0 /    0 /    0         0 /    0 /    0
          Ethernet0   0 /    0 /    0         0 /    0 /    0
          Ethernet3   0 /    0 /    0         0 /    0 /    0
   GigabitEthernet0   0 /    0 /    0         0 /    0 /    0
          Ethernet2   0 /    0 /    0         0 /    0 /    0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear pim counters** | PIM トラフィック カウンタをクリアします。 |

# show pim neighbor

PIM ネイバーテーブルのエントリを表示するには、**show pim neighbor** コマンドを使用します。

**show pim neighbor** ［**count** ｜ **detail**］［*interface*］

## 構文の説明

| | |
|---|---|
| *interface* | （任意）インターフェイスの名前。この引数を指定すると、表示される情報は指定したインターフェイスに関するものだけになります。 |
| **count** | （任意）PIM ネイバーの合計数、および各インターフェイスの PIM ネイバーの数を表示します。 |
| **detail** | （任意）upstream-detection hello オプションを通じて学習した、ネイバーの追加アドレスを表示します。 |

## 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

このコマンドは、このルータが PIM の hello メッセージを通じて学習した PIM ネイバーを特定するために使用します。また、このコマンドは、インターフェイスが指定ルータ（DR）であること、およびネイバーで双方向処理が可能になるタイミングも示します。

脅威に対する防御 デバイス自体が PIM ネイバーです。したがって、脅威に対する防御 インターフェイスがこのコマンドの出力に表示されます。脅威に対する防御 デバイスの IP アドレスは、アドレスの次にアスタリスク（*）を付けて示されています。

### 例

次に、**show pim neighbor** コマンドの出力例を示します。

```
> show pim neighbor inside
Neighbor Address    Interface    Uptime     Expires   DR  pri  Bidir
10.10.1.1           inside       03:40:36   00:01:41  1        B
10.10.1.2*          inside       03:41:28   00:01:32  1   (DR) B
```

# show pim range-list

PIM の範囲リスト情報を表示するには、**show pim range-list** コマンドを使用します。

**show pim range-list** ［**config**］［*rp_address*］

## 構文の説明

| | |
|---|---|
| **config** | PIM CLI 範囲リスト情報を表示します。 |
| *rp_address* | 次のいずれか 1 つを指定できます。<br>• ドメインネームシステム（DNS）ホストテーブルで定義されているランデブーポイント（RP）の名前。<br>• RP の IP アドレス。これは、4 分割ドット付き 10 進表記のマルチキャスト IP アドレスです。 |

## 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

このコマンドは、マルチキャスト転送モードからグループへのマッピングを特定するために使用されます。出力には、この範囲のランデブー ポイント（RP）のアドレスも示されます（該当する場合）。

### 例

次に、**show pim range-list** コマンドの出力例を示します。

```
> show pim range-list
config SSM Exp: never Src: 0.0.0.0
  230.0.0.0/8 Up: 03:47:09
config BD RP: 172.16.1.3 Exp: never Src: 0.0.0.0
  239.0.0.0/8 Up: 03:47:16
config BD RP: 172.18.1.6 Exp: never Src: 0.0.0.0
  239.100.0.0/16 Up: 03:47:10
config SM RP: 172.18.2.6 Exp: never Src: 0.0.0.0
  235.0.0.0/8 Up: 03:47:09
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show pim group-map** | グループから PIM モードへのマッピング、およびアクティブな RP の情報を表示します。 |

# show pim topology

PIM トポロジテーブル情報を表示するには、**show pim topology** コマンドを使用します。

**show pim topology** ［**reserved** | **route-count** ［**detail**］ | *group* ［*source*］］

## 構文の説明

| | |
|---|---|
| **reserved** | 予約済みグループの PIM トポロジ テーブルの情報を表示します。 |
| **route-count** | PIM トポロジテーブルにあるルート数を表示します。 |
| **detail** | （任意）グループごとに、数に関する詳細な情報を表示します。 |
| *group* | （任意）次のいずれかを指定できます。<br>• DNS ホストテーブルで定義されているマルチキャストグループの名前。<br>• マルチキャストグループの IPv4 または IPV6 アドレス。 |
| *source* | （任意）次のいずれかを指定できます。<br>• DNS ホストテーブルで定義されているマルチキャスト送信元の名前。<br>• マルチキャスト送信元の IPv4 または IPV6 アドレス。 |

## コマンド デフォルト

すべてのグループと送信元のトポロジ情報が表示されます。

## 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

PIM トポロジ テーブルは、所定のグループのさまざまなエントリ、(*, G)、(S, G)、(S, G)RPT をそれぞれのインターフェイス リストとともに表示するために使用します。

PIM は、これらのエントリの内容を MRIB を通じてやり取りします。MRIB は、PIM などのマルチキャスト ルーティング プロトコルと、インターネット グループ管理プロトコル（IGMP）などのローカル メンバーシップ プロトコルとの通信における仲介手段であり、システムのマルチキャスト転送エンジンです。

MRIB は、所定の (S, G) エントリについて、どのインターフェイスでデータ パケットを受け取る必要があるか、どのインターフェイスでデータ パケットを転送する必要があるかを示します。また、転送時にはマルチキャスト転送情報ベース（MFIB）テーブルを使用して、パケットごとの転送アクションを決定します。

（注） 転送情報を表示するには、**show mfib route** コマンドを使用します。

例

次に、**show pim topology** コマンドの出力例を示します。

```
> show pim topology
IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR
(*,224.0.1.40) DM Up: 15:57:24 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags: LH DSS
  outside            15:57:24  off LI LH

(*,224.0.1.24) SM Up: 15:57:20 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:20  fwd LI LH

(*,224.0.1.60) SM Up: 15:57:16 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:16  fwd LI LH
```

次に、**show pim topology reserved** コマンドの出力例を示します。

```
> show pim topology reserved
IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Disinterest,
    II - Internal Interest, ID - Internal Disinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary

(*,224.0.0.1) L-Local Up: 00:02:26 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags:
  outside            00:02:26  off II

(*,224.0.0.3) L-Local Up: 00:00:48 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags:
  inside             00:00:48  off II
```

次に、**show pim topology route-count** コマンドの出力例を示します。

```
> show pim topology route-count
PIM Topology Table Summary
  No. of group ranges = 5
  No. of (*,G) routes = 0
  No. of (S,G) routes = 0
  No. of (S,G)RPT routes = 0
```

関連コマンド

| Command | 説明 |
| --- | --- |
| **show mrib route** | MRIB テーブルを表示します。 |

# show pim traffic

PIM トラフィックカウンタを表示するには、**show pim traffic** コマンドを使用します。

**show pim traffic**

## 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

PIM トラフィックカウンタをクリアするには、 **clear pim counters** コマンドを使用します。

### 例

次に、**show pim traffic** コマンドの出力例を示します。

```
> show pim traffic

PIM Traffic Counters
Elapsed time since counters cleared: 3d06h

                                Received     Sent
Valid PIM Packets                      0        9485
Hello                                  0        9485
Join-Prune                             0           0
Register                               0           0
Register Stop                          0           0
Assert                                 0           0
Bidir DF Election                      0           0

Errors:
Malformed Packets                                  0
Bad Checksums                                      0
Send Errors                                        0
Packet Sent on Loopback Errors                     0
Packets Received on PIM-disabled Interface         0
Packets Received with Unknown PIM Version          0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear pim counters** | PIM トラフィック カウンタをクリアします。 |

# show pim tunnel

PIM トンネルインターフェイスに関する情報を表示するには、**show pim tunnel** コマンドを使用します。

**show pim tunnel** ［*interface_name*］

## 構文の説明

| | |
|---|---|
| *interface_name* | （任意）インターフェイスの名前。この引数を指定すると、表示される情報は指定したインターフェイスに関するものだけになります。 |

## コマンド デフォルト

インターフェイスを指定しない場合は、すべてのインターフェイスについて PIM トンネル情報が表示されます。

## 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

PIM レジスタパケットは、仮想カプセル化トンネルインターフェイスを経由して、送信元の最初のホップ DR ルータからランデブーポイント（RP）に送信されます。RP では、仮想カプセル化解除トンネルを使用して、PIM レジスタ パケットの受信インターフェイスを表現します。このコマンドは、両方のタイプのインターフェイスについてトンネル情報を表示します。

レジスタ トンネルは、（PIM レジスタ メッセージ内に）カプセル化された、送信元からのマルチキャスト パケットです。送信元は、共有ツリーを経由して、配布のために RP に送信されます。登録が適用されるのは、SM に対してのみです。SSM および双方向 PIM には適用されません。

### 例

次に、**show pim tunnel** コマンドの出力例を示します。

```
> show pim tunnel

Interface     RP Address    Source Address

Encapstunne   l0 10.1.1.1   10.1.1.1
Decapstunne   l0 10.1.1.1   -
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show pim topology** | PIM トポロジ テーブルを表示します。 |

# show policy-list

設定されたポリシーリストとポリシーリストエントリに関する情報を表示するには、**show policy-list** コマンドを使用します。

**show policy-list** ［*policy_list_name*］

## 構文の説明

| | |
|---|---|
| *policy_list_name* | （オプション）指定されたポリシー リストに関する情報を表示します。 |

## 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

ルート マップの一致基準として BGP ルーティングにポリシー リストを使用します。

### 例

次に、**show policy-list** コマンドの出力例を示します。

```
> show policy-list

policy-list policy_list_2 permit
  Match clauses:
    ip address prefix-lists: prefix_1

policy-list policy_list_1 permit
  Match clauses:
    ip address (access-lists): test
    interface inside
```

# show policy-route

ポリシーベースのルーティング設定を表示するには、**show policy-route** コマンドを使用します。

**show policy-route**

## 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、**show policy-route** コマンドの出力例を示します。

```
> show policy-route
Interface Route map
GigabitEthernet0/0   equal-access
```

# show port-channel

EtherChannel 情報を詳細な 1 行のサマリー形式で表示する場合、またはポートとポートチャネルの情報を表示する場合は、**show port-channel** コマンドを使用します。

**show port-channel** ［*channel_group_number*］［**brief** | **detail** | **port** | **protocol** | **summary**］

## 構文の説明

| | |
|---|---|
| **brief** | （デフォルト）短い情報を表示します。 |
| *channel_group_number* | （オプション）EtherChannel チャネル グループ番号を 1 ～ 48 の範囲で指定して、このチャネル グループに関する情報だけを表示します。 |
| **detail** | （オプション）詳細な情報を表示します。 |
| **port** | （オプション）各インターフェイスの情報を表示します。 |
| **protocol** | （オプション）イネーブルにした場合、LACP などの EtherChannel プロトコルを表示します。 |
| **summary** | （オプション）ポートチャネルの要約を表示します。 |

## コマンド デフォルト

デフォルトは **brief** です。

## 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、**show port-channel** コマンドの出力例を示します。

```
> show port-channel
        Channel-group listing:
        ----------------------

Group: 1
----------
Ports: 3   Maxports = 16
Port-channels: 1 Max Port-channels = 48
Protocol: LACP/ active
Minimum Links: 1
Maximum Bundle: 8
Load balance: src-dst-ip
```

次に、**show port-channel summary** コマンドの出力例を示します。

```
> show port-channel summary

Number of channel-groups in use: 1
```

```
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1             LACP    Gi3/1   Gi3/2   Gi3/3
```

次に、**show port-channel detail** コマンドの出力例を示します。

```
> show port-channel detail
        Channel-group listing:
        ----------------------

Group: 1
----------
Ports: 3   Maxports = 16
Port-channels: 1 Max Port-channels = 48
Protocol: LACP/ active
Minimum Links: 1
Maximum Bundle: 8
Load balance: src-dst-ip

       Ports in the group:
       -------------------
Port: Gi3/1
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/1     SA      bndl      32768         0x1       0x1     0x302       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
-------------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x0       0x1      0x306       0x3d

Port: Gi3/2
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/2     SA      bndl      32768         0x1       0x1     0x303       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
-------------------------------------------------------------------------------------
Gi3/2     SA      bndl       32768         0x0       0x1      0x303       0x3d
```

```
Port: Gi3/3
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/3     SA      bndl      32768         0x1       0x1     0x304       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
-------------------------------------------------------------------------------------
Gi3/3     SA      bndl       32768         0x0       0x1      0x302       0x3d
```

次に、**show port-channel port** コマンドの出力例を示します。

```
> show port-channel port
        Channel-group listing:
        ----------------------

Group: 1
----------
       Ports in the group:
       -------------------
Port: Gi3/1
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/1     SA      bndl      32768         0x1       0x1     0x302       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
-------------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x0       0x1      0x306       0x3d

Port: Gi3/2
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.
```

```
Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/2     SA      bndl      32768         0x1       0x1     0x303       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/2     SA      bndl       32768         0x0       0x1      0x303       0x3d

Port: Gi3/3
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/3     SA      bndl      32768         0x1       0x1     0x304       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/3     SA      bndl       32768         0x0       0x1      0x302       0x3d
```

次に、**show port-channel protocol** コマンドの出力例を示します。

```
> show port-channel protocol
        Channel-group listing:
        ----------------------
Group: 1
----------
Protocol: LACP
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show lacp** | LACP 情報（トラフィック統計情報、システム ID、ネイバーの詳細など）を表示します。 |
| **show port-channel load-balance** | ポートチャネル負荷分散情報が、指定のパラメータ セットに対するハッシュ結果および選択されたメンバー インターフェイスとともに表示されます。 |

# show port-channel load-balance

EtherChannel で、現在のポートチャネル ロードバランス アルゴリズムを表示する場合、また任意で特定のパラメータセットに選択されたメンバーインターフェイスを表示する場合は、**show port-channel load-balance** コマンドを入力します。

**show port-channel** *channel_group_number* **load-balance** [**hash-result** {{**ip** | **ipv6** | **mac** | **l4port** | **mixed**} *parameters* | **vlan-only** *number*}]

## 構文の説明

| | |
|---|---|
| *channel_group_number* | EtherChannel チャネル グループ番号を 1 ～ 48 の範囲で指定します。 |
| **hash-result** | （オプション）現在のロード バランシング アルゴリズムに入力した値をハッシュした後で選択されたメンバー インターフェイスを表示します。 |
| **ip** | （オプション）IPv4 パケット パラメータを指定します。 |
| **ipv6** | （オプション）IPv6 パケット パラメータを指定します。 |
| **l4port** | （オプション）ポート パケット パラメータを指定します。 |
| **mac** | （オプション）MAC アドレス パケット パラメータを指定します。 |
| **mixed** | （オプション）IP または IPv6 パラメータの組み合わせを、ポートまたは VLAN ID（あるいはその両方）とともに指定します。 |
| パラメータ | （オプション）パケット パラメータ。タイプによって異なります。たとえば、ip の場合、送信元 IP アドレス、宛先 IP アドレス、または VLAN ID（あるいはそれらの組み合わせ）を指定できます。 |
| **vlan-only** *number* | （オプション）パケットの VLAN ID を 0 ～ 4095 の範囲で指定します。 |

## 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

デフォルトでは、デバイスはパケットの送信元および宛先IPアドレス（**src-dst-ip**）に従って、インターフェイスでのパケットのロードをバランスします。

このコマンドでは、現在のロード バランシング アルゴリズムを表示できますが、**hash-result** キーワードを使用すると、さらに、特定のパラメータを含むパケットに対してどのメンバーインターフェイスが選択されるかをテストできます。このコマンドでテストできるのは、現在のロード バランシング アルゴリズムに対してだけです。たとえば、アルゴリズムが src-dst-ip の場合は、IPv4 または IPv6 の送信元 IP アドレスおよび宛先 IP アドレスを入力します。現在のアルゴリズムで使用されていない他の引数を入力した場合、それらの引数は無視され、アルゴ

リズムで実際に使用されている未入力の値が 0 にデフォルト設定されます。たとえば、アルゴリズムが vlan-src-ip の場合、次のように入力します。

```
show port-channel 1 load-balance hash-result ip source 10.1.1.1 vlan 5
```

次のように入力した場合、vlan-src-ip アルゴリズムでは送信元 IP アドレス 0.0.0.0 および VLAN 0 が想定され、入力した値は無視されます。

```
show port-channel 1 load-balance hash-result l4port source 90 destination 100
```

### 例

次に、**show port-channel 1 load-balance** コマンドの出力例を示します。

```
> show port-channel 1 load-balance
EtherChannel Load-Balancing Configuration:
       src-dst-ip

EtherChannel Load-Balancing Addresses UsedPer-Protocol:
Non-IP: Source XOR Destination MAC address
 IPv4: Source XOR Destination IP address
 IPv6: Source XOR Destination IP address
```

次に、**show port-channel 1 load-balance hash-result** コマンドの出力例を示します。ここでは、入力したパラメータが現在のアルゴリズム（src-dst-ip）と一致しています。

```
> show port-channel 1 load-balance hash-result ip source 10.1.1.1 destination 10.5.5.5
Would select GigabitEthernet2/1 based on algorithm src-dst-ip
```

次に、**show port-channel 1 load-balance hash-result** コマンドの出力例を示します。ここでは、入力したパラメータが現在のアルゴリズム（src-dst-ip）と一致しておらず、ハッシュでは 0 の値が使用されます。

```
> show port-channel 1 load-balance hash-result l4port source 5
Would select GigabitEthernet3/2 of Port-channel1 based on algorithm src-dst-ip
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show lacp** | LACP 情報（トラフィック統計情報、システム ID、ネイバーの詳細など）が表示されます。 |
| **show port-channel** | EtherChannel 情報が、詳細に 1 行のサマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。 |

# show power inline

PoEインターフェイスを持つモデルの場合、インターフェイスの電源の状態を表示するには、**show power inline** コマンドを使用します。

（注） Firepower 1010 でのみサポートされています。

**show power inline**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.5 | このコマンドが導入されました。 |

## 使用上のガイドライン

PoE インターフェイスを使用して、IP フォンまたはワイヤレス アクセス ポイントなどの電源を必要するデバイスを接続します。Firepower 1010 の場合、イーサネット 1/7 および 1/8 で PoE+ をサポートしています。

### 例

次に、Firepower 1010 での **show power inline** コマンドの出力例を示します。

```
> show power inline
   Interface     Power   Class   Current (mA)   Voltage (V)
   ---------     -----   -----   ------------   -----------
   Ethernet1/1   n/a     n/a     n/a            n/a
   Ethernet1/2   n/a     n/a     n/a            n/a
   Ethernet1/3   n/a     n/a     n/a            n/a
   Ethernet1/4   n/a     n/a     n/a            n/a
   Ethernet1/5   n/a     n/a     n/a            n/a
   Ethernet1/6   n/a     n/a     n/a            n/a
   Ethernet1/7   On      4       121.00         53.00
   Ethernet1/8   On      4       88.00          53.00
```

次の表は、各フィールドの説明を示しています。

表 *47 : show power inline* のフィールド

| フィールド | 説明 |
|---|---|
| インターフェイス（Interface） | 脅威に対する防御上のすべてのインターフェイスを表示します。PoE が使用できないインターフェイスも含みます。 |
| 電源 | 電源が On か Off かを示します。デバイスに電源が必要でない場合、インターフェイスにデバイスがない場合、またはインターフェイスがシャットダウンしている場合、値は Off になります。インターフェイスが PoE をサポートしていない場合、値は n/a です。 |

| フィールド | 説明 |
|---|---|
| クラス | 接続されているデバイスの PoE クラスを表示します。 |
| 電流（mA） | 使用中の電流を表示します。 |
| 電圧（V） | 使用中の電圧を表示します。 |

# show prefix-list

IPv4 トラフィックに一致するように設定されているプレフィックスリストを一覧表示するには、**show prefix-list** コマンドを使用します。

**show prefix-list** ［**detail** | **summary**］［*prefix_list_name* ［**seq** *sequence_number* | *network/length* ［**longer** | **first-match**］］］

## 構文の説明

| | |
|---|---|
| **detail** | プレフィックスリストに関する詳細を表示します。 |
| **summary** | プレフィックスリストの概要を表示します。 |
| *prefix_list_name* | プレフィックス リストの名前。 |
| **seq** *sequence_number* | （オプション）指定されたプレフィックス リストに指定されたシーケンス番号を持つプレフィックス リストのエントリだけを表示します。 |
| *network/length* [**longer** \| **first-match**] | （オプション）このネットワーク アドレスおよびネットマスク長（ビット単位）を使用する、指定したプレフィックス リストのすべてのエントリを表示します。ネットワーク マスクの長さは 0 ～ 32 です。<br>必要に応じて、次のキーワードのいずれかを含めることができます。<br>• **longer** 指定された network/length と一致する、または指定された network/length よりも限定的な、指定されたプレフィックスリストのエントリすべてを表示します。<br>• **first-match** 指定された network/length と一致する、指定されたプレフィックスリストの最初のエントリを表示します。 |

## 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

「test」という名前のプレフィックスリストを含む **show prefix-list** コマンドの出力例を次に示します。

```
> show prefix-list detail test

prefix-list test:   Description: test-list
   count: 1, range entries: 0, sequences: 1 - 1, refcount: 3

   seq 1 permit 2.0.0.0/8 (hit count: 0, refcount: 1)
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear prefix-list** | IPプレフィックスリストに対するヒットカウントをリセットします。 |
| **show bgp prefix-list** | Border Gateway Protocol のコンテキストに含まれるプレフィックスリストまたはプレフィックス リスト エントリに関する情報を表示します。 |
| **show ipv6 prefix-list** | IPv6 プレフィックス リストについての情報を表示します。 |

# show priority-queue

インターフェイスのプライオリティキューの設定または統計情報を表示するには、**show priority-queue** コマンドを使用します。

**show priority-queue** {**config** | **statistics**} [*interface_name*]

## 構文の説明

| | |
|---|---|
| **config** | インターフェイス プライオリティ キューのキューおよび TX-ring の制限を表示します。 |
| *interface_name* | （オプション）構成、またはベストエフォート キューおよび低遅延キューの統計の詳細を表示するインターフェイスの名前を指定します。 |
| **statistics** | ベストエフォート キューおよび低遅延キューの統計の詳細を表示します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

### 例

次に、test という名前のインターフェイスの統計情報の例を示します。この出力で、BE はベストエフォート キュー、LLQ は低遅延キューを表しています。

```
> show priority-queue statistics test

Priority-Queue Statistics interface test

Queue Type         = BE
Packets Dropped    = 0
Packets Transmit   = 0
Packets Enqueued   = 0
Current Q Length   = 0
Max Q Length       = 0

Queue Type         = LLQ
Packets Dropped    = 0
Packets Transmit   = 0
Packets Enqueued   = 0
Current Q Length   = 0
Max Q Length       = 0
```

次に、設定されているすべてのインターフェイスのプライオリティ キューの構成を表示する例を示します。

```
> show priority-queue config

Priority-Queue Config interface inside
```

```
                current         default         range
queue-limit     0               2048            0 - 2048
tx-ring-limit   4294967295              511             3 - 511

Priority-Queue Config interface test
                current         default         range
queue-limit     0               2048            0 - 2048
tx-ring-limit   4294967295              511             3 - 511

Priority-Queue Config interface outside
                current         default         range
queue-limit     0               2048            0 - 2048
tx-ring-limit   4294967295              511             3 - 511

Priority-Queue Config interface bgmember1
                current         default         range
queue-limit     0               2048            0 - 2048
tx-ring-limit   4294967295              511             3 - 511
```

| Command | 説明 |
|---|---|
| **clear priority-queue statistics** | プライオリティキューの統計情報をゼロにリセットします。 |

# show processes

デバイスで動作しているプロセスのリストを表示するには、**show processes** コマンドを使用します。

**show processes** ［**cpu-hog** | **cpu-usage** ［**non-zero**］［**sorted**］ | **internals** | **memory** | **system**］

## 構文の説明

| | |
|---|---|
| **cpu-hog** | CPU を占有しているプロセス（CPU の使用時間が 100 ミリ秒を超えているプロセス）の番号および詳細を表示します。 |
| **cpu-usage** | 過去 5 秒間、1 分間、および 5 分間に各プロセスで使用された CPU のパーセンテージを表示します。 |
| **internals** | 各プロセスの内部詳細を表示します。 |
| **memory** | 各プロセスのメモリ割り当てを表示します。 |
| **non-zero** | （任意）CPU 使用状況がゼロではないプロセスを表示します。 |
| **sorted** | （オプション）プロセスの CPU 使用状況をソートして表示します。 |
| **system** | （任意）システムで現在実行中のプロセスに関する情報を表示します。 |

## 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

プロセスは、数個の命令だけを必要とする軽量スレッドです。次に示すように、**show processes** コマンドを使用すると、デバイス上で実行されているプロセスのリストが表示されます。

| コマンド | 表示されるデータ | 説明 |
|---|---|---|
| **show processes** | PC | プログラム カウンタ。 |
| **show processes** | SP | スタック ポインタ。 |
| **show processes** | STATE | スレッド キューのアドレス。 |
| **show processes** | Runtime | スレッドが CPU クロック サイクルに基づいて実行されている時間（ミリ秒）。クロックティック（10 ミリ秒の精度）ではなく CPU クロック サイクル（10 ナノ秒未満の精度）に基づいてプロセスの CPU 使用状況を完全かつ正確に計算するため、精度は 1 ミリ秒以内です。 |

| コマンド | 表示されるデータ | 説明 |
|---|---|---|
| **show processes** | SBASE | スタック ベース アドレス。 |
| **show processes** | Stack | 現在使用中のバイト数とスタックの合計サイズ。 |
| **show processes** | プロセス | スレッドの機能。 |
| **show processes cpu-usage** | MAXHOG | 最大 CPU 占有実行時間（ミリ秒）。 |
| **show processes cpu-usage** | NUMHOG | CPU 占有実行数。 |
| **show processes cpu-usage** | LASTHOG | 最後の CPU 占有実行時間（ミリ秒）。 |
| **show processes cpu-usage** | PC | CPU 占有プロセスの命令ポインタ。 |
| **show processes cpu-usage** | Traceback | CPU 占有プロセスのスタック トレース。Traceback には最大で 14 のアドレスを設定できます。 |
| **show processes internals** | Invoked Calls | スケジューラがプロセスを実行した回数。 |
| **show processes internals** | Giveups | プロセスが CPU をスケジューラに返還した回数。 |

**show processes cpu-usage** コマンドを使用すると、デバイス上で CPU を使用している可能性のある特定のプロセスを絞り込むことができます。**sorted** コマンドおよび **non-zero** コマンドを使用すると、**show processes cpu-usage** コマンドの出力をさらにカスタマイズできます。

スケジューラと合計サマリー行で、**show proccesses** コマンドを 2 回連続で実行し、その出力を比較して次のことを判断できます。

- CPU の 100% の消費。
- スレッドのランタイム差分と合計ランタイム差分とを比較して決定された、各スレッドで使用されている CPU のパーセンテージ。

デバイスは、多くの異なる実行スレッドを備えた単一のプロセスとして稼働します。このコマンドの出力は、実際に、スレッド単位でメモリ割り当てと空きメモリを示します。これらのスレッドは、データフローおよびデバイスの操作に関する他の操作において連携して動作するため、他のスレッドがメモリブロックを開放している間、別のスレッドがそのブロックを割り当てることができます。出力の最後の行には、すべてのスレッドの合計カウントが含まれます。割り当てと空きメモリとの差異を監視することで、メモリ リークの可能性を追跡するために、唯一この行を使用できます。

### 例

次に、実行中のプロセスのリストを表示する例を示します。コマンド出力はラップします。

```
> show processes
```

```
    PC                 SP                 STATE                 Runtime
SBASE
Stack Process TID
Mwe 0x00007f9ae994881e 0x00007f9acb9d6e18 0x00007f9b027e1340         0 0x00007f9acb9cf030
32000/32768 zone_background_idb 140
Mwe 0x00007f9ae91d64ae 0x00007f9ae7659cd8 0x00007f9b027e1340         0 0x00007f9ae7652030
27568/32768 WebVPN KCD Process 14
Msi 0x00007f9aea3f8c04 0x00007f9acba86e48 0x00007f9b027e1340      2917 0x00007f9acba7f030
29944/32768 vpnlb_timer_thread 131
```

次に、システムプロセスを一覧表示する例を示します。

```
> show processes system
  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
23302 root       0 -20 1896m 558m 101m S  198  7.1  16939:07 lina
 8330 admin     20   0 15240 1188  852 R    2  0.0   0:00.01 top
23148 root      20   0 29780 2876 1268 S    2  0.0  41:27.25 UEChanneld
(...output truncated...)
```

次に、各プロセスで使用されているCPUのパーセンテージを表示する例を示します。

```
> show processes cpu-usage non-zero
PC         Thread       5Sec     1Min     5Min   Process
0x00007f9ae8abcc76   0x00007f9ad04cf7a0     0.2%     0.0%     0.0%   Environment Monitor
Process
```

次に、CPU を占有しているプロセスの数および詳細を表示する例を示します。

```
> show processes cpu-hog
Process:      cli_xml_server, NUMHOG: 12, MAXHOG: 30, LASTHOG: 2
LASTHOG At:   17:37:08 UTC Oct 28 2016
PC:           0x00007f9ae9b11539 (suspend)
Call stack:   0x00007f9ae9b11539  0x00007f9ae9caf084  0x00007f9ae9caf9d0
              0x00007f9ae8736425  0x00007f9ae9b13346  0x00007f9ae9b15ab4
              0x00007f9ae8730ead  0x00007f9ae87663ec  0x00007f9ae6eccde0
              0x00007f9ac4a46120  0x31223d646920696c
(...output truncated...)
```

次に、各プロセスのメモリ割り当てを表示する例を示します。

```
> show processes memory

------------------------------------------------------------------------------
Allocs      Allocated             Frees       Freed                 Process
             (bytes)                           (bytes)
------------------------------------------------------------------------------
0           0                     0           0                     *System Main*
0           0                     0           0                     QoS Support Module
0           0                     0           0                     SSL
0           0                     0           0                     vpnfol_thread_sync
22          8636                  78          3728                  DHCP Network Scope
Monitor
7           40459                 0           0                     Integrity FW Task
0           0                     0           0                     uauth_urlb clean
2           64                    0           0                     arp_timer
8450        233220                0           0                     HDD Health Monitor
14638       1659384               14509       1570750               PTHREAD-23518
```

```
0           0                     6           1926                   DHCP Client
(...output truncated...)
```

次に、各プロセスの内部詳細を表示する例を示します。

```
> show processes internals
     Invoked      Giveups  Max_Runtime  Process
           1            0        0.002  zone_background_idb
           2            0        0.163  WebVPN KCD Process
      507512            0        0.060  vpnlb_timer_thread
           2            0        0.057  vpnlb_thread
     2029820            0        0.130  vpnfol_thread_unsent
      507455            0        0.137  vpnfol_thread_timer
(...output truncated...)
```

# show process-tree

ツリー関係にあるシステムプロセスを表示するには、**show process-tree** コマンドを使用します。

**show process-tree**

## 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

このコマンドの出力は、主にシスコ テクニカルサポートに関連しています。

### 例

次に、プロセスツリーの表示例を示します。

```
> show process-tree
init(1)-+-acpid(23138)
        |-agetty(23726)
        |-crond(23141)
        |-dbus-daemon(23119)
        |-login(23727)---clish(6394)
        |-nscd(14445)-+-{nscd}(14448)
        |             |-{nscd}(14449)
        |             |-{nscd}(14450)
        |             |-{nscd}(14451)
        |             |-{nscd}(14452)
        |             `-{nscd}(14453)
(...remaining output truncated...)
```

# show ptp

高精度時間プロトコル（PTP）の統計情報とクロック情報を表示するには、**show ptp** コマンドを使用します。

**show ptp** {**clock** | **port** [*interface_name*]}

## 構文の説明

| | |
|---|---|
| **clock** | PTP クロックのプロパティを表示します。 |
| **port** [*interface_name*] | インターフェイスの PTP ポート情報を表示します。必要に応じて、インターフェイス名を指定し、指定したインターフェイスに関する情報のみを表示することもできます。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.5 | このコマンドが導入されました。 |

### 例

次に、PTP が設定されていない例を示します。PTP パケットはデバイスを通過できますが、デバイスは PTP クロックを使用しません。

```
> show ptp clock
 No clock information is available in PTP forwarding mode.
> show ptp port
 No clock information is available in PTP forwarding mode.
```

次に、PTP クロック プロパティを表示する例を示します。

```
> show ptp clock
PTP CLOCK INFO
PTP Device Type: Transparent Clock
Operation mode: One Step
Clock Identity: 0:8:2F:FF:FE:E8:43:81
Clock Domain: 0
Number of PTP ports: 4
```

次に、PTP 対応のすべてのインターフェイスの PTP ポート情報を表示する例を示します。

```
> show ptp port
PTP PORT DATASET: GigabitEthernet1/1
Port identity: clock identity: 0:8:2F:FF:FE:E8:43:81
Port identity: port number: 1
PTP version: 2
Port state: Enabled

PTP PORT DATASET: GigabitEthernet1/2
Port identity: clock identity: 0:8:2F:FF:FE:E8:43:81
Port identity: port number: 2
PTP version: 2
```

```
Port state: Disabled

PTP PORT DATASET: GigabitEthernet1/3
Port identity: clock identity: 0:8:2F:FF:FE:E8:43:81
Port identity: port number: 3
PTP version: 2
Port state: Disabled

PTP PORT DATASET: GigabitEthernet1/4
Port identity: clock identity: 0:8:2F:FF:FE:E8:43:81
Port identity: port number: 4
PTP version: 2
Port state: Enabled
```

# show quota

現在のセッションのクォータ統計情報を表示するには、**show quota** コマンドを使用します。

**show quota** ［**management-session**］

## 構文の説明

| | |
|---|---|
| **management-session** | 現在の管理セッションの統計情報を表示します。 |

## 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

脅威に対する防御 で管理セッションクォータを設定することはできません。このコマンドは常に制限なしと表示するはずです。

### 例

次に、クォータ統計情報の例を示します。

```
> show quota
quota management-session limit 0
quota management-session warning level 0
quota management-session level 0
quota management-session high water 0
quota management-session errors 0
quota management-session warnings 0
```

# show raid

RAID 内の SSD のステータスを表示するには、**show raid** コマンドを使用します。

（注） このコマンドは、Cisco Secure Firewall 3100 でのみサポートされています。

**show raid**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1 | このコマンドが導入されました。 |

### 例

次に、RAID 内の 2 つの SSD の表示例を示します。

```
> show raid
Virtual Drive
ID:                           1
Size (MB):                    858306
Operability:                  operable
Presence:                     equipped
Lifecycle:                    available
Drive State:                  optimal
Type:                         raid
Level:                        raid1
Max Disks:                    2
Meta Version:                 1.0
Array State:                  active
Sync Action:                  idle
Sync Completed:               unknown
Degraded:                     0
Sync Speed:                   none

RAID member Disk:
Device Name:                  nvme0n1
Disk State:                   in-sync
Disk Slot:                    1
Read Errors:                  0
Recovery Start:               none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                  nvme1n1
Disk State:                   in-sync
Disk Slot:                    2
Read Errors:                  0
Recovery Start:               none
Bad Blocks:
Unacknowledged Bad Blocks:
```

次の表示例は、RAID 内の 1 つの SSD を示しています。disk2 は存在せず、RAID は「degraded:」と表示されます。

```
> show raid
Virtual Drive
ID:                          1
Size (MB):                   858306
Operability:                 degraded
Presence:                    equipped
Lifecycle:                   available
Drive State:                 degraded
Type:                        raid
Level:                       raid1
Max Disks:                   2
Meta Version:                1.0
Array State:                 active
Sync Action:                 idle
Sync Completed:              unknown
Degraded:                    1
Sync Speed:                  none

RAID member Disk:
Device Name:                 nvme0n1
Disk State:                  in-sync
Disk Slot:                   1
Read Errors:                 0
Recovery Start:              none
Bad Blocks:
Unacknowledged Bad Blocks:
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure raid** | SSD を RAID に追加または RAID から削除します。 |
| **show ssd** | SSD ステータスを表示します。 |

# show random-password, random-strong-password

パスワードの変更時に使用できるパスワードを生成するには、次のいずれかのコマンドを使用します。

**show** { **random-password** | **random-strong-password** } *length*

## 構文の説明

| | |
|---|---|
| **random-password** | 特殊文字を含まないランダムなパスワードを生成します。 |
| **random-strong-password** | 強力なランダムパスワード、つまり特殊文字を含むパスワードを生成します。 |
| *length* | 生成されるパスワードの長さを 8 ～ 127 文字で指定します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | このコマンドが導入されました。 |

## 使用上のガイドライン

パスワードの生成は、FXOS プラットフォームでのみ機能します。独自のパスワードを考えたくない場合は、これらのコマンドをパスワードの変更と組み合わせて使用できます。

コマンドを入力すると、ランダムなパスワードが表示されます。パスワードをコピー/貼り付けするか、メモしてください。次のキーストロークがどのような種類であっても、パスワードは出力から消去されるため、別のユーザーがパスワードを取得することはできません。

### 例

次に、生成されたパスワードを使用して joeuser のパスワードを変更する例を示します。最初に、**show user** を使用して、最小パスワード長と強力なパスワードが必要かどうかを決定します。この場合、最小長（MinL）は 8 文字で、パスワードの強度（Str）は有効になっています。次に、12 文字の（最小長を超える）強力なパスワードを生成します。これをクリップボードにコピーしてから、別のユーザーのパスワードを変更するときは **configure user password**、自分がログインしているパスワードを変更するときは **configure password** のいずれかを change password コマンドに貼り付けます。

```
> show user
Login       UID   Auth Access  Enabled Reset   Exp  Warn    Grace MinL Str Lock Max
joeuser    1001  Local Config  Enabled   Yes   180     7  Disabled    8 Ena   No   5
> show random-strong-password 12
4j9@!GEhnL>V
> configure user password joeuser
Enter new password for user joeuser: <paste not shown>
Confirm new password for user joeuser: <paste not shown>
```

次に、FXOS 以外のプラットフォーム、または FXOS のバージョンがランダムパスワードの生成に対応していない FXOS プラットフォームでパスワードを生成しようとしている場合の例を示します。

```
> show random-strong-password 12
Password generator is not available.
```

| Command | 説明 |
|---|---|
| **configure password** | ログインしているユーザーのパスワードを設定します。 |
| **configure user minpasswdlength** | 新しいユーザーを追加します。 |
| **configure user password** | 指定したユーザーのパスワードを設定します。 |
| **configure user strength-check** | 強力なパスワード要件を設定します。 |
| **show user** | ユーザーアカウントを表示します。 |

# show resource types

デバイスが使用状況の追跡対象にしているリソース タイプを表示するには、**show resource types** コマンドを使用します。

**show resource types**

## 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、リソース タイプの例を示します。

```
> show resource types
Rate limited resource types:
  Conns                     Connections/sec
  Inspects                  Inspects/sec
  Syslogs                   Syslogs/sec

Absolute limit types:
  Conns                     Connections
  Hosts                     Hosts
  IPSec                     IPSec Mgmt Tunnels
  Mac-addresses             MAC Address table entries
  ASDM                      ASDM Connections
  SSH Client                SSH Client Sessions
  SSH Server                SSH Server Sessions
  Storage                   Storage Limit Size of context directory in MB
  Telnet                    Telnet Sessions
  Xlates                    XLATE Objects
  Routes                    Routing Table Entries
  All                       All Resources
  Other VPN Sessions        Other VPN Sessions
  Other VPN Burst           Allowable burst for Other VPN Sessions
  AnyConnect                AnyConnect Premium licensed sessions
  AnyConnect Burst          Allowable burst for AnyConnect Premium licensed sessions
  IKEv1 in-negotiation      Allowable in negotiation IKEv1 SAs
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear resource usage** | リソース使用状況の統計情報をクリアします。 |
| **show resource usage** | デバイスのリソース使用状況を表示します。 |

# show resource usage

デバイスのリソース使用状況を表示するには、**show resource usage** コマンドを使用します。

**show resource usage** ［**all** | **detail**］［**resource** {［**rate**］ *resource_name* | **all**}］［**counter** *counter_name* ［*count_threshold*］］

## 構文の説明

| | |
|---|---|
| **all** | すべてのタイプ。 |
| *count_threshold* | 表示するリソースの使用回数を設定します。デフォルトは1です。リソースの使用状況がここで設定する回数を下回っている場合、そのリソースは表示されません。カウンタ名に all を指定した場合、count_threshold は現在の使用状況に適用されます。すべてのリソースを表示するには、count_threshold を 0 に設定します。 |
| **counter** *counter_name* | 次のカウンタ タイプの数を表示します。<br>• **current**：リソースのアクティブな同時発生インスタンス数、またはリソースの現在のレートを表示します。<br>• **peak**：ピーク時のリソースの同時発生インスタンス数、またはピーク時のリソースのレートを表示します。これらは、統計情報が **clear resource usage** コマンドまたはデバイスのリブートによって最後にクリアされた時点から計測されます。<br>• **denied**：Limit 列に表示されるリソース制限を超えたために拒否されたインスタンスの数を表示します。<br>• **all**：（デフォルト）すべての統計情報を表示します。 |
| **detail** | 管理できないリソースを含むすべてのリソースのリソース使用状況を表示します。たとえば、TCP 代行受信の数を表示できます。 |
| **resource** {［**rate**］ *resource_name* \| **all**} | 特定のリソースの使用状況を表示します。すべてのリソースに対して **all** を指定します。リソースの使用状況を表示するには、rate を指定します。rate で測定されるリソースには、**conns**、**inspects**、および **syslogs** があります。これらのリソースの種類を指定する場合は、**rate** キーワードを指定する必要があります。**conns** リソースは、同時接続としても測定されます。1 秒あたりの接続を表示するには、rate キーワードのみを使用します。リソース名のリストについては、「使用上のガイドライン」を参照してください。 |

## 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

**resource** キーワードを使用する場合のリソースには、次の種類があります。

- **asdm**：このキーワードに関連する機能は、脅威に対する防御 ではサポートされていません。
- **conns**：任意の 2 つのホスト間の TCP または UDP 接続（1 つのホストと他の複数ホストとの間の接続を含む）。
- **hosts**：脅威に対する防御 デバイスを介して接続できるホスト。
- **ipsec**：IPSec 管理トンネル。
- **mac-addresses**：トランスペアレント ファイアウォール モードでは、MAC アドレステーブルで許可される MAC アドレス数。
- **rate**：レート測定リソース。**conns**、**inspects**、または **syslogs** を指定します。
- **routes**：ルーティング テーブル エントリ。
- **ssh**：SSH セッション。
- **storage**：ストレージサイズ制限（MB 単位）。
- **telnet**：Telnet セッション。
- **vpn** ：VPN リソース。
- **vpn anyconnect**：AnyConnect Premium ライセンスの制限。
- **vpn ikev1 in-negotiation**：ネゴシエーション中の IKEv1 セッションの数。
- **VPN Other**：サイト間 VPN セッション。
- **VPN Burst Other**：サイト間 VPN バーストセッション。
- **xlates**：NAT 変換。

### 例

次に、すべてのリソースのリソース使用状況を表示する **show resource usage** コマンドの出力例を示します。デバイスはシングルコンテキストモードであるため、コンテキストは [System] として表示されます。

```
> show resource usage
Resource                Current         Peak      Limit        Denied Context
Syslogs [rate]                0          144        N/A             0 System
Conns                         0            5     100000             0 System
Xlates                        0            5        N/A             0 System
Hosts                         0            8        N/A             0 System
Conns [rate]                  0            1        N/A             0 System
Inspects [rate]               0            3        N/A             0 System
Mac-addresses                 0            4      16384             0 System
Routes                        9            9  unlimited             0 System
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear resource usage** | リソース使用状況の統計情報をクリアします。 |
| **show resource types** | リソース タイプのリストを表示します。 |

# show rip database

RIP トポロジデータベースに格納されている情報を表示するには、**show rip database** コマンドを使用します。

**show rip database** ［*ip_addr* ［*mask*］］

## 構文の説明

| | |
|---|---|
| *ip_addr* | （任意）指定したネットワーク アドレスの表示ルートを制限します。 |
| *mask* | （任意）オプションのネットワーク アドレスのネットワーク マスクを指定します。 |

## 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

RIP データベースには RIP を通じて学習されたルートがすべて含まれます。このデータベースに表示されるルートはルーティング テーブルには必ずしも表示されません。

### 例

次に、**show rip database** コマンドの出力例を示します。

```
> show rip database

10.0.0.0/8    auto-summary
10.11.11.0/24    directly connected, GigabitEthernet0/2
10.1.0.0/8    auto-summary
10.11.0.0/16    int-summary
10.11.10.0/24    directly connected, GigabitEthernet0/3
192.168.1.1/24
    [2] via 10.11.10.5, 00:00:14, GigabitEthernet0/3
```

次に、ネットワークアドレスとマスクを指定した、**show rip database** コマンドの出力例を示します。

```
> show rip database 172.19.86.0 255.255.255.0
172.19.86.0/24
    [1] via 172.19.67.38, 00:00:25, GigabitEthernet0/2
    [2] via 172.19.70.36, 00:00:14, GigabitEthernet0/3
```

# show rollback-status

Management Center から送信された最新のロールバックジョブ（存在する場合）のステータスを表示するには、**show rollback-status** コマンドを使用します。

**show rollback-status**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

## 使用上のガイドライン

Management Center が展開ジョブ中に設定変更をロールバックする必要がある場合、デバイスに要求を送信した後、Management Center からデバイスへの管理接続がリセットされます。このコマンドを使用して、ロールバックジョブのステータスを確認できます。

ロールバックジョブは、実行構成ファイルで設定されたコマンドのみに関連します。Snort 設定はロールバックされません。

デバイスが高可用性モードで実行されている場合は、アクティブユニットのみでこのコマンドを使用します。クラスタでは、このコマンドはマスターユニットのみで使用できます。

この情報には次のものがあります。

- [Status]：最新のロールバックジョブのステータス。
  - [None]：ロールバックジョブは要求されていません。
  - [In Progress]：システムがロールバック要求を受信し、ロールバックジョブが進行中です。
  - [Succeeded]：ロールバックが正常に完了しました。
  - [Reverted]：Device Manager から送信された設定へのロールバックに失敗しました。システムは、最後に保存された設定に戻ります。
  - [Failed]：ロールバックはエラーが発生して完了しました。
- [Start Time/End Time]：ジョブの開始時刻と終了時刻。N/A は、ジョブがなかったことを意味します。終了時刻の場合、N/A はジョブがまだ進行中であることを意味する場合もあります。

### 例

次の例は、ロールバックジョブが要求されていない通常の状況を示しています。

```
> show rollback-status
        Status      : None
        Start Time  : N/A
        End Time    : N/A
```

関連コマンド

| Command | 説明 |
| --- | --- |
| **show running-config** | 実行構成ファイルで定義されている構成を表示します。 |

# show route

データインターフェイスのルーティングテーブルを表示するには、**show route** コマンドを使用します。

**show route** ［ **vrf** *name* ｜ **all** ］ **summary** ［ **management-only** ］ ［ **cluster** ｜ **failover** ｜ *ip_address* ［ *mask* ］ ［ **longer-prefixes** ］ ｜ **bgp** ［ *as_number* ］ ｜ **connected** ｜ **eigrp** ［ *process_id* ］ ｜ **isis** ｜ **ospf** ［ *process_id* ］ ｜ **rip** ｜ **static** ｜ **summary** ｜ **zone** ］

## 構文の説明

| | |
|---|---|
| **bgp** *as_number* | （オプション）ルーティング情報ベース（RIB）エポック番号（シーケンス番号）、現在のタイマー値、および BGP ルートのネットワーク記述子ブロック エポック番号（シーケンス番号）を表示します。AS 番号は、表示対象を指定の AS 番号を使用するルートエントリに限定します。 |
| **cluster** | （オプション）ルーティング情報ベース（RIB）エポック番号（シーケンス番号）、現在のタイマー値、およびネットワーク記述子ブロック エポック番号（シーケンス番号）を表示します。 |
| **connected** | （任意）接続されているルートを表示します。 |
| **eigrp** *process_id* | （任意）EIGRP ルートを表示します。ただし、脅威に対する防御 は EIGRP をサポートしていません。 |
| **failover** | （オプション）フェールオーバーが発生してスタンバイ ユニットがアクティブ ユニットになった場合の、ルーティング テーブルおよびルーティング エントリの現在のシーケンス番号を表示します。 |
| *interface_name* | （オプション）指定したインターフェイスを使用するルート エントリを表示します。 |
| *ip_address mask* | （オプション）指定された宛先へのルートを表示します。 |
| **isis** | （オプション）IS-IS ルートを表示します。 |
| **longer-prefixes** | （オプション）指定された ip_address/mask ペアに一致するルートのみを表示します。 |
| **management-only** | （オプション）IPv4 管理ルーティング テーブル内のルートを表示します。 |
| **ospf** *process_id* | （オプション）OSPF ルートを表示します。 |
| **rip** | （オプション）RIP ルートを表示します。 |
| **static** | （任意）スタティック ルートを表示します。 |
| **summary** | （任意）ルーティング テーブルの現在の状態を表示します。 |

| | |
|---|---|
| ［**vrf***name* ｜ **all**］ **summary** | Virtual Route Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、**vrf** *name* キーワードを使用してビューを特定の仮想ルータに制限できます。すべての仮想ルータのルーティングテーブルを表示するには、**all** キーワードを含めます。これらの VRF 関連キーワードのいずれも含めない場合、コマンドはグローバル VRF 仮想ルータのルーティングテーブルを表示します。summary キーワードを使用して、すべての VRF のルート情報を表示できます。 |
| **zone** | （オプション）ゾーン インターフェイスのルートを表示します。 |

## 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。 |
| 6.6 | ［**vrf** *name* ｜ **all**］ キーワードが追加されました。 |

## 使用上のガイドライン

**show route** コマンドの出力は、IPv4 に固有の情報である点を除いて、**show ipv6 route** コマンドの出力と類似しています。表示されるルートは、仮想管理インターフェイスではなく、データインターフェイス専用です。管理インターフェイスのデフォルトゲートウェイを表示するには、**show network** コマンドを使用します。管理インターフェイスのルートを表示するには、**show network-static-routes** コマンドを使用します。

（注） 脅威に対する防御 デバイスでこれらの機能が設定されていない場合、**clustering** キーワードと **failover** キーワードは表示されません。

**show route** コマンドは、新しい接続の最適なルートを表示します。許可される TCP SYN をバックアップ インターフェイスに送信すると、脅威に対する防御 は同じインターフェイスを使用してのみ応答できます。そのインターフェイスの RIB にデフォルトルートがない場合、デバイスは隣接情報がないためにパケットをドロップします。**show running-config route** コマンドで表示されるよう設定されたものはすべて、システム内で特定のデータ構造で管理されます。

**show asp table routing** コマンドを使用して、バックエンド インターフェイスに固有のルーティング テーブルを確認できます。この設計は OSPF や EIGRP と同様であり、プロトコル固有のルート データベースは、「最適」ルートだけを表示するグローバル ルーティング テーブルとは異なります。この動作は設計によるものです。

### 例

次に、**show route** コマンドの出力例を示します。

```
> show route

Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
```

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

C    10.86.194.0 255.255.255.0 is directly connected, outside
C    10.40.10.0 255.255.255.0 is directly connected, inside
C    192.168.2.0 255.255.255.0 is directly connected, faillink
C    192.168.3.0 255.255.255.0 is directly connected, statelink
```

次に、**show route failover** コマンドの出力例を示します。これは、フェールオーバー後のスタンバイユニットへの OSPF および EIGRP ルートの同期を示しています。

```
> show route failover

Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area

       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0
Routing table sequence number 1
Reconvergence timer 00.20 (Running)

S    10.10.10.0 255.0.0.0 [1/0] via 10.10.10.1, mgmt, seq 1
                        [1/0] via 10.10.10.2, mgmt, seq 1
D    209.165.200.224 255.255.255.0 [90/28416] via 200.165.200.225, 0:00:15, outside, seq
 1

O   198.51.100.0 255.255.255.0 [110/28416] via 198.51.100.10, 0:24:45, inside, seq 0

D   10.65.68.220 255.255.255.255 [1/0] via 10.76.11.1, mgmt, seq 1
```

次に、**show route cluster** コマンドの出力例を示します。

```
> show route cluster
Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area

       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

Routing table seq num 2
Reconvergence timer expires in 52 secs

C    70.0.0.0 255.255.255.0 is directly connected, cluster, seq 1
C    172.23.0.0 255.255.0.0 is directly connected, tftp, seq 1
C    200.165.200.0 255.255.255.0 is directly connected, outside, seq 1
```

```
C    198.51.100.0 255.255.255.0 is directly connected, inside, seq 1
O   198.51.100.0 255.255.255.0 [110/28416] via 198.51.100.10, 0:24:45, inside, seq 2
D   209.165.200.224 255.255.255.0 [90/28416] via 200.165.200.225, 0:00:15, outside, seq
 2
```

次に、**show route summary** コマンドの出力例を示します。

```
> show route summary

IP routing table maximum-paths is 3
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
connected       0           2           0           176         576
static          1           0           0           88          288
bgp 2           0           0           0           0           0
  External: 0 Internal: 0 Local: 0
internal        1                                               408
Total           2           2           0           264         1272
```

次の例では、Virtual Routing and Forwarding（VRF）を有効にした場合のすべての仮想ルータのルートを表示します。この例では、最初に示されているグローバルルータに加えて、2 つの仮想ルータ（test1 と test2）があります。

```
> show route all

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is not set

C        192.168.0.0 255.255.255.0 is directly connected, inside1
L        192.168.0.100 255.255.255.255 is directly connected, inside1


Routing Table: test1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is not set

C        10.10.10.0 255.255.255.0 is directly connected, outside
L        10.10.10.10 255.255.255.255 is directly connected, outside


Routing Table: test2
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
```

```
       SI - Static InterVRF
Gateway of last resort is not set

C        20.20.20.0 255.255.255.0 is directly connected, inside
L        20.20.20.20 255.255.255.255 is directly connected, inside
```

次に、redという名前の仮想ルータのルートを表示する例を示します。他の仮想ルータにリークされたスタティックルートは、キーSIで示されることに注意してください。

```
> show route vrf red

Routing Table: red
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is not set

C        2.1.1.0 255.255.255.0 is directly connected, gig0
L        2.1.1.2 255.255.255.255 is directly connected, gig0
S        7.0.0.0 255.0.0.0 [1/0] via 8.1.1.1, gig0
SI       11.0.0.0 255.0.0.0 [1/0] is directly connected, gig3
```

次に、すべてのVRFのルートの要約を表示する例を示します。

```
> show route all summary
IP routing table maximum-paths is 8
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
connected            0           4           0           352         1184
static               1           0           0           88          296
ospf 1               0           0           0           0           0
  Intra-area: 0 Inter-area: 0 External-1: 0 External-2: 0
  NSSA External-1: 0 NSSA External-2: 0
internal                2                                               792
Total                   3           4           0           440         2272


Routing Table: v1
IP routing table maximum-paths is 8
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
connected            0           2           0           176         592
static               0           0           0           0           0
ospf 12              0           0           0           0           0
  Intra-area: 0 Inter-area: 0 External-1: 0 External-2: 0
  NSSA External-1: 0 NSSA External-2: 0
internal                1                                               416
Total                   1           2           0           176         1008


Routing Table: v2
IP routing table maximum-paths is 8
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
connected            0           2           0           176         592
static               0           0           0           0           0
ospf 13              0           0           0           0           0
  Intra-area: 0 Inter-area: 0 External-1: 0 External-2: 0
  NSSA External-1: 0 NSSA External-2: 0
```

```
internal                1                                               416
Total                   1           2           0           176         1008
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipv6 route** | IPv6 ルーティングテーブルを表示します。 |
| **show vrf** | システムで定義されている仮想ルータを表示します。 |

# show route-map

ルートマップ情報を表示するには、**show route-map** コマンドを使用します。

**show route-map** ［**all** | **dynamic** ［**application** ［*application*］ | **detail** | *route_map*］ | *route_map*］

## 構文の説明

| | |
|---|---|
| **all** | スタティックルートマップとダイナミックルートマップの両方に関する情報を表示します。 |
| **dynamic** | ダイナミックルートマップに関する情報のみを表示します。 |
| **application** *application* | ルートマップを作成したアプリケーション。 |
| *route_map* | ルート マップ名。 |

## 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、**show route-map dynamic** コマンドの出力例を示します。

```
> show route-map dynamic
route-map MIP-10/24/06-05:23:46.091-1-MPATH_1, permit, sequence 0, identifier 54943520
  Match clauses:
    ip address (access-lists): VOICE
  Set clauses:
    interface Tunnel0
  Policy routing matches: 0 packets, 0 bytes
 Current active dynamic routemaps = 1
```

# show rule hits

アクセス コントロール ポリシーおよびプレフィルタポリシーの評価済みルールすべてのルールヒット情報を表示するには、**show rule hits** コマンドを使用します。

**show rule hits** [ **id** *number* | **raw** | **cumulative** | **node-wise** ] [ **gt** *#hit-count* | **lt** *#hit-count* | **range** *#hit-count1 #hit-count2* ]

## 構文の説明

| | |
|---|---|
| **cumulative** | （任意）すべてのクラスタまたは高可用性（HA）ノードでのルールヒットの累積合計を表示します。ヒットカウントはノードごとに計算されるため、合計にはクラスタまたはHAペア全体のヒット数の合計が表示されます。 |
| **id***number* | （任意）ルールの ID。この引数を含めると、表示される情報は指定されたルールに限定されます。ID を指定すると、他のオプションは指定できません。<br>ルール ID を識別するには、**show access-list** コマンドを使用します。 |
| **node-wise** | （任意）クラスタまたはHAペアのユニットごとの現在のヒットカウントを表示します。 |
| **raw** | （任意）.csv 形式でルールヒット情報を表示します。 |
| **gt** *#hit-count* | （任意）ヒットカウントが *#hit-count* より大きいすべてのルールを表示します。 |
| **lt** *#hit-count* | （任意）ヒットカウントが *#hit-count* より小さいすべてのルールを表示します。 |
| **range** *#hit-count1 #hit-count2* | （任意）*#hit-count1* と *#hit-count2* の間のヒットカウントを持つすべてのルールを表示します。 |

## コマンド デフォルト

ルール ID を指定しない場合、すべてのルールのルールヒット情報が表示されます。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.4 | このコマンドが導入されました。 |
| 7.2 | **cumulative** および **node-wise** キーワードが追加されました。 |

## 使用上のガイドライン

ルールヒット情報は、アクセスコントロールルールとプレフィルタルールのみを対象としています。

アクセス制御またはプレフィルタポリシーを表示するときにローカルまたはリモートのデバイスマネージャを使用すると、ルールヒット情報をより簡単に表示できます。このコマンドで表示されるルールヒット情報は、実際のルールに基づいており、ルールを部分的に実装するため

に生成された ACL のアクセス制御エントリ（ACE）には基づいていないことに注意してください。したがって、このコマンドで表示されるヒットカウント情報は、**show access-list** コマンドで表示されるヒットカウントとは異なります。

ルール ID を識別するには、**show access-list** コマンドを使用します。ただし、このコマンドの出力にすべてのルールが表示されているわけではありません。Management Center 管理対象デバイスの場合は、次の URL で REST API GET 操作を使用すると、すべてのルールとそれらのルールの ID を確認できます。

- `/api/fmc_config/v1/domain/{domainUUID}/policy/accesspolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true`
- `/api/fmc_config/v1/domain/{domainUUID}/policy/prefilterpolicies/{containerUUID}/operational/hitcounts?filter="deviceId:{deviceId}"&expanded=true`

### 例

次に、ルールヒット情報を表示する例を示します。

```
> show rule hits
RuleID            Hit Count       First Hit Time(UTC)       Last Hit Time(UTC)
-------------------------------------------------------------------------------------
268436979            1            22:01:39 Jan 25 2019      22:01:39 Jan 25 2019
268436980            1            22:01:51 Jan 25 2019      22:01:51 Jan 25 2019
268436981            2            22:02:00 Jan 25 2019      22:02:02 Jan 25 2019
268436925            2            22:01:53 Jan 25 2019      22:04:51 Jan 25 2019
```

次の例では、クラスタまたは HA ペアのすべてのユニットのヒットカウントの要約が表示されます。

```
> show rule hits cumulative

RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)

-------------------------------------------------------------------------------------
111116               2                   10:03:55 Apr 12 2021     10:04:02 Apr 12 2021

111117               1                   10:03:59 Apr 12 2021     10:03:59 Apr 12 2021
111119               1                   10:04:05 Apr 12 2021     10:04:05 Apr 12 2021
```

次の例では、クラスタまたはHAペアの各ユニットのヒットカウントが表示されます。ヒットカウントは、デバイスごとに個別に保持されます。

```
> show rule hits node-wise

Active/Control node rule hits:

RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)

-------------------------------------------------------------------------------------
111116               1                   10:03:55 Apr 12 2021     10:03:55 Apr 12 2021

111117               1                   10:03:59 Apr 12 2021     10:03:59 Apr 12 2021
```

```
Standby/Data node rule hits:

RuleID               Hit Count           First Hit Time(UTC)     Last Hit Time(UTC)

--------------------------------------------------------------------------------

111116               1                   10:04:02 Apr 12 2021     10:04:02 Apr 12 2021

111119               1                   10:04:05 Apr 12 2021     10:04:05 Apr 12 2021
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear rule hits** | アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報をクリアし、ゼロにリセットします。 |
| **show cluster rule hits** | クラスタ内のすべてのノードから、アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報をクリアし、ゼロにリセットします。 |
| **cluster exec show rule hits** | クラスタの各ノードから、アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報を分離形式で表示します。 |
| **cluster exec clear rule hits** | クラスタ内のすべてのノードから、アクセス コントロール ポリシーおよびプレフィルタポリシーのすべての評価済みルールのルールヒット情報をクリアし、ゼロにリセットします。 |

# show running-config

デバイスで現在実行されている設定を表示するには、**show running-config** コマンドを使用します。

**show running-config** ［**all**］［*command*］

## 構文の説明

| | |
|---|---|
| **all** | デフォルトを含め、動作設定全体を表示します。 |
| *command* | 特定のコマンドに関連付けられたコンフィギュレーションを表示します。使用可能なコマンドについては、**show running-config ?** を使用して CLI のヘルプを参照してください。<br>（注） 脅威に対する防御 は、CLI ヘルプに記載されているすべてのコマンドを直接サポートしているわけではありません。特定のオプションの設定がない場合があります。一部のオプションは、Management Center の FlexConfig を使用してのみ設定できます。 |

## 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

**show running-config** コマンドは、デバイスのメモリにあるアクティブなコンフィギュレーション（保存されたコンフィギュレーションの変更を含む）を表示します。これらのコマンドを直接設定することはできません。代わりに、デバイスを制御するマネージャ（Management Center や Device Manager など）で設定します。

ただし、これは部分的な設定です。ASA ソフトウェア コンフィギュレーション コマンドのみを使用して設定できる内容を示していますが、一部のコマンドは 脅威に対する防御 に固有のコマンドである場合があります。これらのコマンドは脅威に対する防御 に移植されています。したがって、実行コンフィギュレーションの情報はトラブルシューティングの補助手段としてのみ使用してください。Management Center デバイスマネージャは、デバイス設定を分析する主な手段として使用します。

### 例

次に、**show running-config** コマンドの出力例を示します。

```
> show running-config
: Saved

:
: Serial Number: XXXXXXXXXXX
: Hardware:   ASA5512, 4096 MB RAM, CPU Clarkdale 2793 MHz, 1 CPU (2 cores)
:
```

```
NGFW Version 6.1.0
!
hostname firepower
enable password $sha512$5000$Col980QPR9VVq/VYoAkGJw==$ZvzuZDNpcvvEP/DGbBqytA== pbkdf2
strong-encryption-disable
names

!
interface GigabitEthernet0/0
 nameif outside
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 192.168.10.1 255.255.255.0
 ipv6 enable
!
interface GigabitEthernet0/1
 shutdown
 nameif inside
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 192.168.1.1 255.255.255.0
 ipv6 enable
!
interface GigabitEthernet0/2
 shutdown
 nameif dmz
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 192.168.2.1 255.255.255.0
 ipv6 enable
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 no nameif
 no security-level
 no ip address
!
ftp mode passive
ngips conn-match vlan-id
access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority
```

```
 Policy
access-list CSM_FW_ACL_ remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ advanced permit ipinip any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id
9998
access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544 rule-id
9998
access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: Initial AC Policy -
Default/1
access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434432
access-list CSM_IPSEC_ACL_1 extended permit ip any6 any6
!
tcp-map UM_STATIC_TCP_MAP
  tcp-options range 6 7 allow
  tcp-options range 9 18 allow
  tcp-options range 20 255 allow
  tcp-options md5 clear
  urgent-flag allow
!
no pager
logging enable
logging timestamp rfc5424
logging buffered informational
logging flash-minimum-free 1024
logging flash-maximum-allocation 3076
no logging message 106015
no logging message 313001
no logging message 313008
no logging message 106023
no logging message 710003
no logging message 106100
no logging message 302015
no logging message 302014
no logging message 302013
no logging message 302018
no logging message 302017
no logging message 302016
no logging message 302021
no logging message 302020
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 8192
access-group CSM_FW_ACL_ global
as-path access-list 2 deny 100$
as-path access-list 2 permit 200$
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:00:30
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
```

```
aaa proxy-limit disable
no snmp-server location
no snmp-server contact
no snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
no sysopt connection permit-vpn
crypto ipsec ikev1 transform-set CSM_TS_1 esp-des esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map CSM_outside_map 1 match address CSM_IPSEC_ACL_1
crypto map CSM_outside_map 1 set peer 10.10.10.10
crypto map CSM_outside_map 1 set ikev1 transform-set CSM_TS_1
crypto map CSM_outside_map 1 set reverse-route
crypto map CSM_outside_map interface outside
crypto ca trustpool policy
crypto ikev1 enable outside
crypto ikev1 policy 160
 authentication pre-share
 encryption des
 hash sha
 group 5
 lifetime 86400
telnet timeout 5
console timeout 0
dynamic-access-policy-record DfltAccessPolicy
tunnel-group 10.10.10.10 type ipsec-l2l
tunnel-group 10.10.10.10 ipsec-attributes
 ikev1 pre-shared-key *****
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP
 parameters
  eool action allow
  nop action allow
  router-alert action allow
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options UM_STATIC_IP_OPTIONS_MAP
 class class-default
  set connection advanced-options UM_STATIC_TCP_MAP
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:167911f11cbf1140edeffcb0f9b17f01
```

```
: end
>
```

BFD グローバル設定を表示するには、出力修飾子を使用して BFD 関連の設定をフィルタリングします。次に、出力修飾子を使用した **show running-config bfd** コマンドの出力例を示します。

```
ciscoftd# show running-config bfd
bfd map ipv4 1.1.1.1/24 1.1.1.2/32 name2
```

次に、出力修飾子を使用した **show running-config bfd-template** コマンドの出力例を示します。

```
ciscoftd# show running-config bfd-template
bfd-template single-hop bfd_template
interval min-tx 50 min-rx 50 multiplier 3
!
bfd-template single-hop bfd_template_auth
interval min-tx 50 min-rx 50 multiplier 3
authentication md5 ***** key-id 8
!
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show access-control-config** | アクセス コントロール ポリシーに関するサマリー情報を表示します。 |

# show s - sz

# show sctp

現在の Stream Control Transmission Protocol（SCTP）Cookie とアソシエーションを表示するには、**show sctp** コマンドを使用します。

**show sctp** ［**detail**］

## 構文の説明

| | |
|---|---|
| **detail** | SCTP アソシエーションに関する詳細情報を表示します。 |

## 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

**show sctp** コマンドは、SCTP Cookie とアソシエーションに関する情報を表示します。

Management Center から FlexConfig を使用して SCTP インスペクションを有効にすると、このコマンドで SCTP 情報を表示できます。

### 例

次に、**show sctp** コマンドの出力例を示します。

```
> show sctp

AssocID: 2279da7a
Local:  192.168.107.11/20001 (ESTABLISHED)
Remote: 192.168.108.11/40174 (ESTABLISHED)

AssocID: 4924f520
Local:  192.168.107.11/20001 (ESTABLISHED)
Remote: 192.168.108.11/40200 (ESTABLISHED)
```

次に、**show sctp detail** コマンドの出力例を示します。

```
> show sctp detail

AssocID: 8b7e3ffb
Local:  192.168.100.56/3868 (ESTABLISHED)
    Receiver Window: 48000
    Cumulative TSN: 5cb6cd9b
    Next TSN: 5cb6cd9c
    Earliest Outstanding TSN: 5cb6cd9c
    Out-of-Order Packet Count: 0
Remote: 192.168.200.78/3868 (ESTABLISHED)
    Receiver Window: 114688
    Cumulative TSN: 5cb6cd98
    Next TSN: 0
    Earliest Outstanding TSN: 5cb6cd9c
    Out-of-Order Packet Count: 0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show local-host** | インターフェイスごとに、デバイス経由で接続を確立しているホストの情報を表示します。 |
| **show service-policy inspect sctp** | SCTP インスペクションの統計情報を表示します。 |
| **show traffic** | インターフェイスごとに、接続とインスペクションの統計情報を表示します。 |

# show serial-number

プリント基板（PCB）のシリアル番号を表示するには、**show serial-number** コマンドを使用します。このコマンドは仮想デバイスでは使用できません。

**show serial-number**

## 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

**show serial-number** コマンドを使用して、プリント基板のシリアル番号を表示します。この情報は、**show version system** および **show running-config** の出力にも表示されます。

**show inventory** コマンドを使用して、シャーシのシリアル番号を表示します。

### 例

次に、シリアル番号を表示する例を示します。この例の番号は無効な番号に変更されています。

```
> show serial-number
XXX175078X5
```

# show service-policy

サービスポリシーの統計情報を表示するには、**show service-policy** コマンドを使用します。

**show service-policy** ［**global** | **interface** *intf*］［**cluster flow-mobility** | **inspect** *inspection* ［*arguments*］ | **police** | **priority** | **set connection** ［**details**］ | **sfr** | **shape** | **user-statistics**］
**show service-policy** ［**global** | **interface** *intf*］［**flow** *protocol* {**host** *src_host* | *src_ip src_mask*} ［**eq** *src_port*］ {**host** *dest_host* | *dest_ip dest_mask*} ［**eq** *dest_port*］［*icmp_number* | *icmp_control_message*］］

## 構文の説明

| | |
|---|---|
| **cluster flow-mobility** | （オプション）脅威に対する防御 クラスタのフローモビリティに関するステータス情報を表示します。 |
| *dest_ip dest_mask* | **flow** キーワードの場合、宛先 IP アドレスおよびトラフィックフローのネットマスク。 |
| **details** | （オプション）**set connection** キーワードの場合、クライアントごとの接続制限が有効な場合に、クライアントごとの接続情報を表示します。 |
| **eq** *dest_port* | **flow** キーワードの場合、フローの宛先ポートに相当します。 |
| **eq** *src_port* | （オプション）**flow** キーワードの場合、フローの送信元ポートに相当します。 |
| **flow** *protocol* | （オプション）5 つのタプル（プロトコル、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポート）で識別される特定フローに一致するポリシーを示します。このコマンドを利用すると、サービス ポリシー コンフィギュレーションによって、必要なサービスが特定の接続に提供されることを確認できます。 |
| **global** | （オプション）出力をグローバル ポリシーに制限します。 |
| **host** *dest_host* | **flow** キーワードの場合、トラフィックフローのホスト宛先 IP アドレス。 |
| **host** *src_host* | **flow** キーワードの場合、トラフィックフローのホスト送信元 IP アドレス。 |
| *icmp_control_message* | （オプション）プロトコルとして ICMP を指定した場合の **flow** キーワードに対して、トラフィックフローの ICMP 制御メッセージを指定します。 |
| *icmp_number* | （オプション）プロトコルとして ICMP を指定した場合の **flow** キーワードに対して、トラフィックフローの ICMP プロトコル番号を指定します。 |

| | |
|---|---|
| **inspect** *inspection* [*arguments*] | （オプション）**inspect** コマンドを含むポリシーに関する詳細情報を表示します。詳細出力では、一部の **inspect** コマンドはサポートされません。すべてのインスペクションを表示するには、**show service-policy inspect ?** コマンドを使用します。各インスペクションで使用できる引数は異なります。詳細については、CLIヘルプを参照してください。 |
| **interface** *intf* | （オプション）*intf* 引数で指定したインターフェイスに適用されるポリシーを表示します。*intf* はインターフェイス名です。 |
| **police** | （オプション）**police** コマンドを含むポリシーに関する詳細情報を表示します。 |
| **priority** | （オプション）**priority** コマンドを含むポリシーに関する詳細情報を表示します。 |
| **set connection** | （オプション）**set connection** コマンドを含むポリシーに関する詳細情報を表示します。 |
| **sfr** | （オプション）ASA Firepower モジュールのポリシーに関する詳細情報を表示します。このキーワードは 脅威に対する防御 には有効ではありません。 |
| **shape** | （オプション）**shape** コマンドを含むポリシーに関する詳細情報を表示します。 |
| *src_ip src_mask* | **flow** キーワードの場合、送信元IPアドレスおよびトラフィックフローで使用されるネットマスク。 |
| **user-statistics** | （オプション）**user-statistics** コマンドを含むポリシーに関する詳細情報を表示します。このキーワードは 脅威に対する防御 には有効ではありません。 |

## コマンド デフォルト

引数を指定しない場合、このコマンドはすべてのグローバルポリシーおよびインターフェイスポリシーを表示します。

## 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

**show service-policy** コマンドの出力に表示される初期接続の数は、特定のトラフィッククラスに関して定義されたトラフィックマッチング用のインターフェイスに対する初期接続の現在の数を示しています。「embryonic-conn-max」フィールドには、トラフィッククラスに設定された最大初期接続の制限値が表示されます。表示される現在の初期接続数が最大値と等しい場合、または最大値を超えている場合は、新しい TCP 接続がトラフィックに一致すると、その接続に対して TCP 代行受信が適用されます。

コンフィギュレーションに対してサービスポリシーの変更を加えた場合は、すべての新しい接続で新しいサービスポリシーが使用されます。既存の接続では、その接続が確立された時点で設定されていたポリシーの使用が続行されます。**show** コマンドの出力には、古い接続に関するデータが含まれていません。すべての接続が新しいポリシーを確実に使用するように、現在の接続を解除し、新しいポリシーを使用して再度接続できるようにします。**clear conn** コマンドまたは **clear local-host** コマンドを参照してください。

Management Center または Device Manager を使用してサービスポリシーを直接設定することはできません。さまざまな接続設定を編集したり、QoS ポリシーを設定したりすると、一部が間接的に変更されます。**configure inspection** コマンドを使用して、有効にするデフォルトのインスペクションを調整することもできます。Management Center で FlexConfig を使用してサービスポリシーを設定する場合、このコマンドは設定に関連した統計を表示します。

（注） **inspect icmp** ポリシーと **inspect icmp error** ポリシーの場合、パケット数にはエコー要求パケットと応答パケットのみが含まれます。

### 例

次に、**show service-policy** コマンドの出力例を示します。

```
> show service-policy
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: ftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: h323 h225 _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop
0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: h323 ras _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: rsh, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: rtsp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: esmtp _default_esmtp_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: sqlnet, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: skinny , packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: sunrpc, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: xdmcp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: sip , packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
```

```
      Inspect: netbios, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: tftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: ip-options UM_STATIC_IP_OPTIONS_MAP, packet 0, lock fail 0, drop 0,
reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
    Class-map: class-default
      Default Queueing      Set connection policy:         drop 0
      Set connection advanced-options: UM_STATIC_TCP_MAP
        Retransmission drops: 0                   TCP checksum drops : 0
        Exceeded MSS drops  : 0                   SYN with data drops: 0
        Invalid ACK drops   : 0                   SYN-ACK with data drops: 0
        Out-of-order (OoO) packets : 0            OoO no buffer drops: 0
        OoO buffer timeout drops : 0              SEQ past window drops: 0
        Reserved bit cleared: 0                   Reserved bit drops : 0
        IP TTL modified     : 0                   Urgent flag cleared: 0
        Window varied resets: 0
        TCP-options:
          Selective ACK cleared: 0                Timestamp cleared  : 0
          Window scale cleared : 0
          Other options cleared: 0
          Other options drops: 0
```

複数のCPUコアを搭載しているデバイスの場合は、ロック失敗用のカウンタがあります。共有されるデータ構造と変数は複数のコアによって使用可能なため、それらを保護するためにロック メカニズムが使用されます。コアはロックの取得に失敗すると、ロックの取得を再試行します。ロック失敗カウンタは、試行が失敗するごとに増分されます。

```
> show service-policy
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      ...
      Inspect: esmtp _default_esmtp_map, packet 96716502, lock fail 7, drop 25,
reset-drop 0
      Inspect: sqlnet, packet 2526511491, lock fail 21, drop 2362, reset-drop 0
```

次に、GTP インスペクションの統計情報を表示するコマンドを示します。出力については、例に続く表の中で説明します。

```
> show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support               0     msg_too_short             0
  unknown_msg                       0     unexpected_sig_msg        0
  unexpected_data_msg               0     ie_duplicated             0
  mandatory_ie_missing              0     mandatory_ie_incorrect    0
  optional_ie_incorrect             0     ie_unknown                0
  ie_out_of_order                   0     ie_unexpected             0
  total_forwarded                  67     total_dropped             1
  signalling_msg_dropped            1     data_msg_dropped          0
  signalling_msg_forwarded         67     data_msg_forwarded        0
  total created_pdp                33     total deleted_pdp         32
  total created_pdpmcb             31     total deleted_pdpmcb      30
  total dup_sig_mcbinfo             0     total dup_data_mcbinfo    0
  no_new_sgw_sig_mcbinfo            0     no_new_sgw_data_mcbinfo   0
  pdp_non_existent                  1
```

表 *48 : GPRS GTP* 統計情報

| カラムのヘッダー | 説明 |
|---|---|
| version_not_support | サポートされていない GTP バージョン フィールドを持つパケットの数を表示します。 |
| msg_too_short | 長さが 8 バイトより短いパケットの数を表示します。 |
| unknown_msg | 不明なタイプのメッセージ数を表示します。 |
| unexpected_sig_msg | 予期しないシグナリング メッセージ数を表示します。 |
| unexpected_data_msg | 予期しないデータ メッセージ数を表示します。 |
| mandatory_ie_missing | 必須情報要素（IE）が欠落しているメッセージ数を表示します。 |
| mandatory_ie_incorrect | 不正な形式の必須情報要素（IE）を持つメッセージ数を表示します。 |
| optional_ie_incorrect | 無効なオプション情報要素（IE）を持つメッセージ数を表示します。 |
| ie_unknown | 不明な情報要素（IE）を持つメッセージ数を表示します。 |
| ie_out_of_order | 順番どおりでない情報要素（IE）を持つメッセージ数を表示します。 |
| ie_unexpected | 予期しない情報要素（IE）を持つメッセージを表示します。 |
| ie_duplicated | 重複した情報要素（IE）を持つメッセージ数を表示します。 |
| optional_ie_incorrect | 不正な形式のオプション情報要素（IE）を持つメッセージ数を表示します。 |
| total_dropped | ドロップされたメッセージの合計数を表示します。 |
| signalling_msg_dropped | ドロップされた信号メッセージ数を表示します。 |
| data_msg_dropped | ドロップされたデータ メッセージ数を表示します。 |
| total_forwarded | 転送されたメッセージの合計数を表示します。 |
| signalling_msg_forwarded | 転送された信号メッセージ数を表示します。 |
| data_msg_forwarded | 転送されたデータ メッセージ数を表示します。 |
| total created_pdp | 作成されたパケット データ プロトコル（PDP）またはベアラー コンテキストの合計数を表示します。 |

| カラムのヘッダー | 説明 |
|---|---|
| total deleted_pdp | 削除されたパケット データ プロトコル（PDP）またはベアラー コンテキストの合計数を表示します。 |
| total created_pdpmcb<br>total deleted_pdpmcb<br>total dup_sig_mcbinfo<br>total dup_data_mcbinfo<br>no_new_sgw_sig_mcbinfo<br>no_new_sgw_data_mcbinfo | これらのフィールドは、実装機能である PDP マスター制御ブロックの使用に関連しています。これらのカウンタは、トラブルシューティング向けにシスコテクニカルサポートによって使用され、エンドユーザーには直接の関係はありません。 |
| pdp_non_existent | 存在しない PDP コンテキストに対して受信したメッセージ数を表示します。 |

次に、PDP コンテキストに関する情報を表示するコマンドを示します。

```
> show service-policy inspect gtp pdp-context
4 in use, 5 most used
Version v1,   TID 050542012151705f,  MS Addr 2005:a00::250:56ff:fe96:eec,
SGSN Addr 10.0.203.22,      Idle 0:52:01,   Timeout 3:00:00,   APN ssenoauth146
Version v2,   TID 0505420121517056,  MS Addr 100.100.100.102,
SGW Addr 10.0.203.24,      Idle 0:00:05,   Timeout 3:00:00,   APN ssenoauth146
Version v2,   TID 0505420121517057,  MS Addr 100.100.100.103,
SGW Addr 10.0.203.25,      Idle 0:00:04,   Timeout 3:00:00,   APN ssenoauth146
Version v2,   TID 0505420121517055,  MS Addr 100.100.100.101,
SGW Addr 10.0.203.23,      Idle 0:00:06,   Timeout 3:00:00,   APN ssenoauth146
```

次の表で、**show service-policy inspect gtp pdp-context** コマンドの出力について説明します。

**表 *49 : PDP* コンテキスト**

| カラムのヘッダー | 説明 |
|---|---|
| バージョン | GTP のバージョンを表示します。 |
| TID | トンネル識別子を表示します。 |
| MS Addr | モバイル ステーションのアドレスを表示します。 |
| SGSN Addr<br>SGW Addr | サービング ゲートウェイ サービス ノード（SGSN）またはサービング ゲートウェイ（SGW）を表示します。 |
| Idle | PDP またはベアラー コンテキストが使用されていない期間を表示します。 |
| APN | アクセス ポイント名を表示します。 |

関連コマンド

| Command | 説明 |
| --- | --- |
| **clear service-policy** | サービスポリシーの統計情報をすべてクリアします。 |
| **configure inspection** | デフォルトの検査を有効または無効にします。 |
| **show running-config service-policy** | 実行コンフィギュレーションに設定されているサービス ポリシーを表示します。 |

# show shun

回避情報を表示するには、**show shun** コマンドを使用します。

**show shun** ［*src_ip* | **statistics**］

## 構文の説明

| | |
|---|---|
| *src_ip* | （任意）このアドレスに関する情報を表示します。 |
| **statistics** | （任意）インターフェイスの回避統計を表示します。 |

## 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、**show shun** コマンドの出力例を示します。

```
> show shun
shun (outside) 10.1.1.27 10.2.2.89 555 666 6
shun (inside1) 10.1.1.27 10.2.2.89 555 666 6
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear shun** | 現在イネーブルにされている回避をすべてディセーブルにし、回避統計をクリアします。 |
| **shun** | 新規接続を抑制し、既存のすべての接続からのパケットを不許可にすることにより、攻撃元ホストへのダイナミック応答をイネーブルにします。 |

# show sip

SIP セッションを表示するには、**show sip** コマンドを使用します。

**show sip**

## 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

**show sip** コマンドは、脅威に対する防御 デバイスを越えて確立されている SIP セッションの情報を表示します。

### 例

次に、**show sip** コマンドの出力例を示します。

```
> show sip
Total: 2
call-id c3943000-960ca-2e43-228f@10.130.56.44
 | state Call init, idle 0:00:01
call-id c3943000-860ca-7e1f-11f7@10.130.56.45
 | state Active, idle 0:00:06
```

次の例では、脅威に対する防御 デバイス上の 2 つの SIP セッションが表示されています（Total フィールドを参照）。各 call-id が 1 つのコールを表します。

最初のセッションは、call-id c3943000-960ca-2e43-228f@10.130.56.44 で、Call Init 状態にあります。これは、このセッションはまだコールセットアップ中であることを示しています。コール設定が完了するのは、ACK が確認されてからです。このセッションは、1 秒間アイドル状態でした。

2番目のセッションは、Active状態です。ここでは、コールセットアップは完了して、エンドポイントはメディアを交換しています。このセッションは、6 秒間アイドル状態でした。

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show conn** | さまざまな接続タイプの接続状態を表示します。 |

# show skinny

SCCP（Skinny）セッションに関する情報を表示するには、**show skinny** コマンドを使用します。

**show skinny** ［**audio** | **video**］

## 構文の説明

| | |
|---|---|
| **audio** | SCCP オーディオセッションの表示 |
| **video** | SCCP ビデオセッションの表示 |

## 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、次の条件における **show skinny** コマンドの出力例を示します。デバイスを越えて 2 つのアクティブな Skinny セッションが設定されています。最初の Skinny セッションは、ローカルアドレス 10.0.0.11 にある内部 Cisco IP 電話と 172.18.1.33 にある外部 Cisco Unified Communications Manager の間に確立されています。TCP ポート 2000 は Cisco Unified Communications Manager です。2 番目の Skinny セッションは、ローカルアドレス 10.0.0.22 にある別の内部 Cisco IP 電話と同じ Cisco Unified Communications Manager の間に確立されています。

```
> show skinny
MEDIA 10.0.0.22/20798         172.18.1.11/22948
LOCAL                   FOREIGN                 STATE
-----------------------------------------------------------------
1       10.0.0.11/52238         172.18.1.33/2000                1
  MEDIA 10.0.0.11/22948         172.18.1.22/20798
2       10.0.0.22/52232         172.18.1.33/2000                1
  MEDIA 10.0.0.22/20798         172.18.1.11/22948
```

この出力から、両方の内部 Cisco IP Phone の間でコールが確立されていることがわかります。最初と 2 番目の電話機の RTP リスン ポートは、それぞれ UDP 22948 と 20798 です。

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show conn** | さまざまな接続タイプの接続状態を表示します。 |

# show sla monitor

インターネット プロトコル サービス レベル契約（IP SLA）に関する情報を表示するには、**show sla monitor** コマンドを使用します。

**show sla monitor** {**configuration** | **operational-state**} [*sla_id*]

## 構文の説明

| | |
|---|---|
| **configuration** | SLA の設定値（デフォルト値を含む）を表示します。 |
| **operational-state** | SLA 動作の動作状態を表示します。 |
| *sla_id* | （任意）SLA 動作の ID 番号。有効な値は 1 ～ 2147483647 です。 |

## コマンド デフォルト

SLA ID が指定されていない場合は、すべての SLA 動作の設定値が表示されます。

## 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

**show running-config sla monitor** コマンドを使用して、実行コンフィギュレーションの SLA 動作コマンドを確認します。

### 例

次に、**show sla monitor configuration** コマンドの出力例を示します。SLA 動作 124 の設定値が表示されます。**show sla monitor configuration** コマンドの出力に続いて、同じ SLA 動作の **show running-config sla monitor** コマンドの出力が表示されます。

```
> show sla monitor configuration 124

SA Agent, Infrastructure Engine-II
Entry number: 124
Owner:
Tag:
Type of operation to perform: echo
Target address: 10.1.1.1
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 1000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 3
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
```

```
> show running-config sla monitor 124

sla monitor 124
 type echo protocol ipIcmpEcho 10.1.1.1 interface outside
 timeout 1000
 frequency 3
sla monitor schedule 124 life forever start-time now
```

次に、**show sla monitor operational-state** コマンドの出力例を示します。

```
> show sla monitor operational-state

Entry number: 124
Modification time: 14:42:23.607 EST Wed Mar 22 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 4043
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 18:04:26.609 EST Wed Mar 22 2006
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0       RTTMin: 0       RTTMax: 0
NumOfRTT: 0     RTTSum: 0       RTTSum2: 0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show running-config sla monitor** | 実行コンフィギュレーションの SLA 動作コンフィギュレーション コマンドを表示します。 |

# show snmp-server

デバイスで設定されたSNMPサーバーの情報を表示するには、**show snmp-server**コマンドを使用します。

**show snmp-server** {**engineID** | **group** | **host** | **statistics** | **user** [*username*]}

## 構文の説明

| | |
|---|---|
| **engineID** | SNMP エンジンの ID を表示します。 |
| **group** | 設定されている SNMP グループの名前、使用するセキュリティモデル、さまざまなビューのステータス、および各グループのストレージタイプを表示します。 |
| **host** | ホストグループに属する設定済みの SNMP ホストの名前、使用されているインターフェイスおよび使用されている SNMP のバージョンを表示します。 |
| **statistics** | SNMP サーバー統計情報を表示します。 |
| **user** [*username*] | SNMP ユーザーの特性に関する情報を表示します。必要に応じて、ユーザー名を指定して、そのユーザーに情報を制限できます。 |

## 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

SNMP エンジンは、ローカル デバイス上に配置できる SNMP のコピーです。エンジン ID は、各 SNMP エージェントごとに割り当てられる固有の値です。エンジン ID は設定できません。エンジン IDの長さは25バイトで、このIDは暗号化されたパスワードの生成に使用されます。フェールオーバー ペアでは、エンジン ID がピアと同期化されます。

SNMP ユーザーおよびSNMP グループは、SNMP の View-based Access Control Model（VACM）に従って使用されます。使用されるセキュリティ モデルは、SNMP グループによって決まります。SNMPユーザーは、SNMPグループのセキュリティ モデルに一致する必要があります。各 SNMP グループ名とセキュリティ レベルのペアは一意である必要があります。

（注） 統計には、SNMPモジュールへの入出力パケットに関する情報が表示されます。パケットが出力されたからといって、宛先に到達したということではありません。ルートの問題、介在するファイアウォール、接続されていないインターフェイスなどにより、出力パケットの送信が妨げられる可能性があります。パケットが SNMP サーバーに到達していない場合は、**show asp drop** や **show logging** などのコマンドを使用して他の問題を確認します。

### 例

次に、**show snmp-server engineid** コマンドの出力例を示します。

```
> show snmp-server engineid
Local SNMP engineID: 80000009fe85f8fd882920834a3af7e4ca79a0a1220fe10685
```

次に、**show snmp-server group** コマンドの出力例を示します。

```
> show snmp-server group
groupname: public                              security model:v1
readview : <no readview specified>             writeview: <no writeview specified>
notifyview: <no readview specified>
row status: active

groupname: public                              security model:v2c
readview : <no readview specified>             writeview: <no writeview specified>
notifyview: *<no readview specified>
row status: active

groupname: privgroup                     security model:v3 priv
readview : def_read_view                 writeview: <no writeview specified>
notifyview: def_notify_view
row status: active
```

次に、デバイスをポーリングしているアクティブなホストのみを表示する **show snmp-server host** コマンドの出力例を示します。

```
> show snmp-server host
host ip = 10.10.10.3, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.6, interface = mgmt  poll community ***** version 2c
```

次に、**show snmp-server user** コマンドの出力例を示します。

```
> show snmp-server user authuser
User name: authuser
Engine ID: 000000090200000000C025808
storage-type: nonvolatile       active access-list: N/A
Rowstatus: active
Authentication Protocol: MD5
Privacy protocol: DES
Group name: VacmGroupName
```

この出力には次の情報が表示されます。

- ユーザー名。SNMP ユーザーの名前を識別するストリングです。
- エンジン ID。デバイス上の SNMP のコピーを識別する文字列です。
- ストレージタイプ。デバイスの揮発性メモリまたは一時メモリに設定が格納されているか、あるいは不揮発性メモリまたは永続メモリに格納されているかを示します。非揮発性メモリまたは永続メモリに格納されている場合、デバイスをオフにして再度オンにした場合でも設定は存続します。

- アクティブなアクセス リスト。SNMP ユーザーに関連付けられている標準の IP アクセス リストです。
- Rowstatus。ユーザーがアクティブか非アクティブかを示します。
- 認証プロトコル。使用されている認証プロトコルを示します。選択できるのは、MD5、SHA、なしのいずれかです。ソフトウェア イメージで認証がサポートされていない場合、このフィールドは表示されません。
- プライバシー プロトコル。DES によるパケット暗号化がイネーブルかどうかを示します。ソフトウェア イメージでプライバシーがサポートされていない場合、このフィールドは表示されません。
- グループ名。ユーザーが属している SNMP グループを示します。SNMP グループは、View-based Access Control Model（VACM）に従って定義されます。

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear snmp-server statistics** | SNMP パケットの入力カウンタおよび出力カウンタをクリアします。 |
| **show running-config snmp-server** | SNMP サーバー コンフィギュレーションを表示します。 |

# show snort counters

Snortプリプロセッサ接続の統計情報を表示するには、**show snort counters** コマンドを使用します。

**show snort counters** {**action** | **stream** | **sip** | **ssl** | **smtp** | **vrf**} {**all** | **instance***x*}

## 構文の説明

| | |
|---|---|
| **action** | アクション、制限、および判定に関する Snort のインスタンスレベルの統計情報を表示します。 |
| **stream** | ストリームプリプロセッサの統計情報を表示します。 |
| **sip** | SIP プリプロセッサの統計情報を表示します。 |
| **ssl** | SSL プリプロセッサの統計情報を表示します。 |
| **smtp** | SMTP プリプロセッサの統計情報を表示します。 |
| **vrf** | 各仮想ルータを通過するライブセッションの数を表示します。 |
| **all** | システム内のすべての Snort インスタンスの統計情報を表示します。たとえば、**show snort counters action all**、**show snort counters smtp all** などです。 |
| **instance***x* | システム内の選択した Snort インスタンスの統計情報を表示します。たとえば、**show snort counters smtp instance 11** のようになります。使用可能なインスタンス番号を確認するには、**show snort instances** コマンドを使用します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |
| 6.6 | **vrf** キーワードが追加されました。 |

## 使用上のガイドライン

システムの Snort インスタンスの統計情報を表示するには、このコマンドを使用します。これらの統計情報は、情報提供やデバッグの目的で使用できます。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。**show snort counters action all** コマンドを使用して、システム内のすべての Snort インスタンスのアクション、制限、および判定に関する Snort のインスタンスレベルの統計情報を表示します。使用可能なインスタンス番号を確認するには、**show snort instances** コマンドを使用します。

次に、システム内のすべての Snort インスタンスのアクション、制限、および判定に関する Snort のインスタンスレベルの統計情報を表示する例を示します。

```
> show snort counters action all
Instance : 1
------------

Action Stats are not available
 Total Action Processed:           0

...

================================================================================

Instance : 16
------------

Action Stats:
     Alerts:            0 (  0.000%)
     Logged:            0 (  0.000%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
      Event:            0
      Alert:            0
Verdicts:
      Allow:       220009 (100.000%)
      Block:         5076 (  2.307%)
    Replace:            0 (  0.000%)
  Whitelist:            0 (  0.000%)
  Blacklist:            0 (  0.000%)
     Ignore:            0 (  0.000%)
      Retry:            0 (  0.000%)

================================================================================
```

次に、スチーム統計情報の例を示します。

```
> show snort counters stream all
Instance : 1
------------

Stream statistics not available
 Total sessions: 0
================================================================================

...

Instance : 16
------------

Stream statistics:
            Total sessions: 665
              TCP sessions: 665
              UDP sessions: 0
             ICMP sessions: 0
               IP sessions: 0
                TCP Prunes: 0
                UDP Prunes: 0
               ICMP Prunes: 0
```

```
                IP Prunes: 0
TCP StreamTrackers Created: 0
TCP StreamTrackers Deleted: 0
             TCP Timeouts: 661
             TCP Overlaps: 0
       TCP Segments Queued: 0
     TCP Segments Released: 0
       TCP Rebuilt Packets: 0
         TCP Segments Used: 0
              TCP Discards: 0
                  TCP Gaps: 0
      UDP Sessions Created: 0
      UDP Sessions Deleted: 0
              UDP Timeouts: 0
              UDP Discards: 0
                    Events: 0
          Internal Events: 0
          TCP Port Filter
                 Filtered: 0
                Inspected: 0
                  Tracked: 910736
          UDP Port Filter
                 Filtered: 0
                Inspected: 0
                  Tracked: 0

===============================================================================
```

次に、Snort インスタンス 1 の SMTP 統計情報の例を示しています。

```
> show snort counters smtp instance 1
Instance : 1
------------

SMTP Preprocessor Statistics
  Total sessions                                    : 80
  Max concurrent sessions                           : 1
  Base64 attachments decoded                        : 0
  Total Base64 decoded bytes                        : 0
  Quoted-Printable attachments decoded              : 0
  Total Quoted decoded bytes                        : 0
  UU attachments decoded                            : 0
  Total UU decoded bytes                            : 0
  Non-Encoded MIME attachments extracted            : 0
  Total Non-Encoded MIME bytes extracted            : 0

===============================================================================
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear snort statistics** | Snort インスペクションの統計情報をクリアします。 |
| **show snort statistics** | Snort によってトラフィックが検査されたときに、さまざまな Snort 判定で一致したパケットの数を表示します。 |
| **show snort tls-offload** | ハードウェアの検査エンジン（Snort）によって暗号化および復号化されたパケット関連の統計情報を表示します。 |

# show snort instances

他の **show snort** コマンドで使用できる Snort インスタンス番号のリストを表示するには、**show snort instances** コマンドを使用します。

**show snort instances**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

### 例

次に、Snort インスタンスのリストを表示する例を示します。

```
> show snort instances
Total number of instances available - 2

+----------+---------+
| INSTANCE |   PID   |
+----------+---------+
|    1     |   2787  |
|    2     |   2788  |
+----------+---------+
```

# show snort preprocessor-memory-usage

Snortインスタンスごとの Snortプリプロセッサのメモリ使用状況の統計情報を表示するには、**show snort preprocessor-memory-usage** コマンドを使用します。

**show snort preprocessor-memory-usage** *instance_ID* {**all** | **imap** | **pop** | **smtp**}

## 構文の説明

| | |
|---|---|
| *instance_ID* | Snortインスタンスの ID 番号。システムでアクティブなインスタンス ID 番号のリストを取得するには、**show snort instances** コマンドを使用します。 |
| **all** | すべてのプリプロセッサの統計情報を表示します。 |
| **imap** | IMAP プリプロセッサの統計情報のみを表示します。 |
| **pop** | POP プリプロセッサの統計情報のみを表示します。 |
| **smtp** | SMTP プリプロセッサの統計情報のみを表示します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

### 例

次に、Snortインスタンス 1 の SMTP プリプロセッサの統計情報を表示する例を示します。管理者パスワードの入力を求められます。

```
> show snort preprocessor-memory-usage 1 smtp

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

Password:

Snort Memory Usage for: Instance-1
----------------------------------


Memory Statistics of SMTP on: Fri Jul 12 09:13:02 2019

SMTP Session Statistics:
       Total Sessions seen: 0
   Max concurrent sessions: 0
   Current Active sessions: 0

   Memory Pool:
```

```
        Free Memory:
            SMTP Mime Pool:       17968000 bytes
                 SMTP Pool:              0 bytes
        Used Memory:
            SMTP Mime Pool:              0 bytes
                 SMTP Pool:              0 bytes
        -------------------       ---------------
        Total Memory:             17968000 bytes

   Heap Memory:
                    Session:              0 bytes
              Configuration:          16784 bytes
              --------------         ------------
               Total Memory:          16784 bytes
               No of allocs:             38 times
                 IP sessions:            30 times
-----------------------------------------------------
```

# show snort statistics

Snortによってトラフィックが検査されたときに、さまざまなSnort判定で一致したパケットの数を表示するには、**show snort statistics** コマンドを使用します。

**show snort statistics**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.0.1 | 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して、アクセスポリシー設定と侵入ルール設定に関する Snort インスペクションの結果を表示します。このコマンドは通常、予期しない Snort インスペクション動作をデバッグするときに使用されます。統計には、次の情報が含まれています。

- Passed Packets：Lina から Snort に送信されたパケットの数。
- Blocked Packets：Lina でブロックされ、Snort に送信されなかったパケットの数。
- Injected Packets：Snort が作成し、トラフィックストリームに追加したパケットの数。たとえば、リセットアクションを伴うブロックを設定すると、Snort は接続をリセットするためのパケットを生成します。
- Packets bypassed（Snort Down or Snort Busy）：Snort インスペクションを必要とするパケットを許可するようにシステムを設定しているものの、Snort がインスペクションを実行できない場合、これらのカウンタには、Snort がダウンしているかビジー状態であるためにパケットを処理できないときにインスペクションをバイパスしたパケットの数が表示されます。

⚠

**注意** フローがバイパスされる（インスペクションなしで渡される）と、これらのビジーカウンタおよびダウンカウンタは、バイパスされたセッションが終了するまで増加し続けます。この増加は、Snortがビジーまたはダウン状態ではなくなってからも続く場合があります。たとえば、数日間続く持続的な TCP 接続が、Snort がビジーまたはダウン状態の間もパケットを送信する場合、カウンタは数日間増加を続け、Snort が再開した後も増加し続けます。

- Fast-forwarded flows：ポリシーによって高速転送されたため、検査されなかったフローの数。
- Blacklisted flows：Snort によってドロップされた、ポリシー設定からのフローの数。
- Start-of-flow events：Lina プロセスは、フローを Snort に送信せずに高速パスするときに、Snort にフロー開始イベントを送信します。これらのイベントは、Snort が接続を追跡し、接続イベントを報告するのに役立ちます。

- End-of-flow events：高速パスフローが終了すると、Lina プロセスはフロー終了イベントを Snort に送信します。
- Denied flow events：Lina プロセスは、Snort に送信する前にフローをドロップすることを決定すると、拒否されたフローイベントを Snort に送信します。
- Frames forwarded to Snort before drop：NGIPS インターフェイスのみで有効です。これは Snort に転送されドロップされたパケットの数です。Lina プロセスが何らかの理由（無効な TCP ヘッダー長、無効な UDP 長、無効な IP 長）でフレームをドロップすることに決定すると、可視性のため、フレームが Snort にも送信されます。
- Inject packets dropped：Snort がトラフィックストリームに追加したパケットのうち、ドロップされたパケット数。

### 例

次のサンプルトランスクリプトは、**show snort statistics** コマンドによって表示される情報を示しています。

```
show snort statistics
Packet Counters:
  Passed Packets                                      6
  Blocked Packets                                     321
  Injected Packets                                    284
  Packets bypassed (Snort Down)                       0
  Packets bypassed (Snort Busy)                       0

Flow Counters:
  Fast-Forwarded Flows                                0
  Blacklisted Flows                                   0

Miscellaneous Counters:
  Start-of-Flow events                                0
  End-of-Flow events                                  0
  Denied flow events                                  0
  Frames forwarded to Snort before drop               0
  Inject packets dropped                              0
```

次の例では、すべてのトラフィックをブロックしてリセットするようにアクセス コントロール ポリシーが設定されている場合について考慮します。Lina はリセットを処理できないため、パケットを Snort に渡して、クライアントとサーバー両方へのリセットをブロックおよび送信させます。

- Passed packets：Lina から Snort に渡された 8 つのパケットを表示します。
- Injected packets：クライアントとサーバーに送信された 2 つのパケットを表示します。
- Blacklisted flows：Snort が Lina にブロックするように指示したフローを表示します。

（注） この例では、*blocked* パケットは存在しません。

```
> show snort statistics
Packet Counters:
  Passed Packets                                         8
  Blocked Packets                                        0
  Injected Packets                                       2
  Packets bypassed (Snort Down)                          0
  Packets bypassed (Snort Busy)                          0

Flow Counters:
  Fast-Forwarded Flows                                   0
  Blacklisted Flows                                      3

Miscellaneous Counters:
  Start-of-Flow events                                   0
  End-of-Flow events                                     0
  Denied flow events                                     0
  Frames forwarded to Snort before drop                  0
  Inject packets dropped                                 0
```

次の例では、アクセス コントロール ポリシーに、FTP ポートに一致する 1 つのルールとブロックアクションがあり、HTTP アプリケーションに一致する別のルールと許可アクションが存在する場合について考慮します。

- Passed packets：Lina が許可ルールのパケットを Snort に送信するため、60 個の HTTP パケットが表示されます。
- Denied flow events：FTP ポート照合で Lina が処理した 2 つのデータおよび制御チャネルパケットを表示します。

（注） この例では、*blocked* パケットは存在しません。

```
> show snort statistics
Packet Counters:
  Passed Packets                                        60
  Blocked Packets                                        0
  Injected Packets                                       0
  Packets bypassed (Snort Down)                          0
  Packets bypassed (Snort Busy)                          0

Flow Counters:
  Fast-Forwarded Flows                                   0
  Blacklisted Flows                                      0

Miscellaneous Counters:
  Start-of-Flow events                                   0
  End-of-Flow events                                     0
  Denied flow events                                     2
  Frames forwarded to Snort before drop                  0
```

```
Inject packets dropped                                    0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear snort statistics** | Snort インスペクションの統計情報をクリアします。 |
| **configure snort preserve-connection** | Snort プロセスがダウンした場合に、ルーテッドインターフェイスとトランスペアレント インターフェイスで既存の TCP/UDP 接続を維持するかどうかを指定します。 |

# show snort tls-offload

ハードウェアの検査エンジン（Snort）によって暗号化および復号化されたパケット関連の統計情報を表示するには、**show snort tls-offload** コマンドを使用します。このコマンドは、SSL ハードウェア アクセラレーションをサポートする次の管理対象デバイスでのみ使用できます。

- Threat Defense を搭載した Firepower 2100
- を搭載した Firepower 4100/9300 Threat Defense

  Firepower 4100/9300 Threat Defense コンテナインスタンスでの TLS 暗号化アクセラレーションのサポートの詳細については、『*FXOS Configuration Guide*』を参照してください。

仮想アプライアンス上および上記以外のハードウェアでの TLS 暗号化アクセラレーション はサポートされていません。

**show snort tls-offload [proxy | tracker | description]**

## 構文の説明

| | |
|---|---|
| **proxy** | （オプション）プロキシの統計情報のみを表示します。 |
| **tracker** | （オプション）トラッカーの統計情報のみを表示します。 |
| **description** | （オプション）プロキシとトラッカーの両方のカウンタの説明を表示します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.2.3 | 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して、Snort のプロキシおよびトラッカーコンポーネントの詳細な統計情報を表示します。これらの統計情報は、情報提供やデバッグの目的で使用できます。カウンタの説明を表示するには、**show snort tls-offload description** コマンドを使用します。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

次に、**show snort tls-offload** コマンドの例を示します。

```
====== Tracker Statistics ======
TOTAL_CONNECTION                  2774
TOTAL_RSA_KEY_EXCHANGE_4K         2774
TOTAL_CIPHER_SUITE_ENCR_AES       2774
TOTAL_CIPHER_SUITE_HASH_SHA1      2774
TOTAL_CKE_PMS_DECRYPTED           2774
TOTAL_RECORD_DECRYPTED            363001
TOTAL_RECORD_ENCRYPTED            363001
TOTAL_CONNECTION_W_DUR (<0.5s)    2771
AVG_CONNECTION_DURATION   (ms)    184
AVG_HANDSHAKE_TIME        (ms)    37
AVG_CKE_PMS_DECRYPT_TIME (us)     21402
```

```
AVG_RECORD_DECRYPT_TIME  (us)    619
AVG_RECORD_ENCRYPT_TIME  (us)    477
PEAK_CONNECTION_DURATION (ms)    400
PEAK_HANDSHAKE_TIME      (ms)    62
CONCURRENT_CONNECTION/Peak       3/3
CPS_ATTEMPTED/Peak               7/8
CPS_COMPLETED/Peak               8/8
CKE_PMS_DECRYPTING_Q/Peak        0/2
SKE_DH_PARAM_SIGNING_Q/Peak      0/0
RECORD_ENCRYPTING_Q/Peak         1/25
RECORD_DECRYPTING_Q/Peak         1/2
======= Proxy Statistics =======
TOTAL_CONNECTION(LW+FP)          15855
TOTAL_CONNECTION_FP              15853
CONNECTION_FP_RECV_FIN           31697
CONNECTION_FP_RECV_RST           27
CONNECTION_LW_RECV_FIN           2
CONCURRENT_CONNECTION_LW/Peak    0/2
CONCURRENT_CONNECTION_FP/Peak    3/7
BYPASS_NOT_ENOUGH_MEM            0
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear snort tls-offload** | 統計カウンタをクリアします。 |
| **debug snort tls-offload** | すべてのSnortプロセスのすべてのタイプのエラーデバッグメッセージを表示します。 |

# show software authenticity

ソフトウェアの真正性情報を表示するには、**show software authenticity** コマンドを使用します。

**show software authenticity** {**development** | **file** *filename* | **keys** | **running**}

## 構文の説明

| | |
|---|---|
| **development** | 開発キー署名付きイメージのロードが有効か無効かを表示します。 |
| **file** *filename* | 特定のイメージ ファイルのソフトウェア認証に関連したデジタル署名情報を表示します。 |
| **keys** | SPI フラッシュに保存されている開発キーとリリースキーに関する情報を表示します。 |
| **running** | 現在実行中のイメージファイルのソフトウェア認証に関連したデジタル署名情報を表示します。 |

## 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

ファイルおよび実行中のイメージの出力には、次の情報が含まれています。

- メモリ内のファイルの名前であるファイル名。
- 表示されるイメージのタイプであるイメージ タイプ。
- 署名者情報によって、次のようなシグニチャ情報が指定されます。
  - 一般名。ソフトウェア メーカーの名前です。
  - 組織単位。ソフトウェア イメージが展開されるハードウェアを示します。
  - 組織名。ソフトウェア イメージの所有者です。
- 証明書シリアル番号。デジタル署名の証明書シリアル番号です。
- ハッシュ アルゴリズム。デジタル署名確認に使用されるハッシュ アルゴリズムのタイプを示します。
- 署名アルゴリズム。デジタル署名確認に使用される署名アルゴリズムのタイプを識別します。
- キー バージョン。確認に使用されるキー バージョンを示します。

### 例

次に、**show software authenticity development** コマンドの出力例を示します。

```
> show software authenticity development
Loading of development images is disabled
```

次に、**show software authenticity file** コマンドの出力例を示します。この例では、ファイルは開発イメージです。デバイスで現在実行中のイメージファイルに関して、**show software authenticity running** と同じ出力が表示されます。

```
> show software authenticity file os.img
File Name                     : disk0:/os.img
Image type                    : Development
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 57F4610F
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
```

次に、show software authenticity keys コマンドの出力例を示します。

```
> show software authenticity keys
Public Key #1 Information
-------------------------
Key Type              : Release (Primary)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        96:A2:E6:E4:51:4D:4A:B0:F0:EF:DB:41:82:A6:AC:D0:
        FC:11:40:C2:F0:76:10:19:CE:D0:16:7D:26:73:B1:55:
        FE:42:FE:5D:5F:4D:A5:D5:29:7F:91:EC:91:4D:9B:33:
        54:4B:B8:4D:85:E9:11:2D:79:19:AA:C5:E7:2C:22:5E:
        F6:66:27:98:1C:5A:84:5E:25:E7:B9:09:80:C7:CD:F4:
        13:FB:32:6B:25:B5:22:DE:CD:DC:BE:65:D5:6A:99:02:
        95:89:78:8D:1A:39:A3:14:C9:32:EE:02:4C:AB:25:D0:
        38:AD:E4:C9:C6:6B:28:FE:93:C3:0A:FE:90:D4:22:CC:
        FF:99:62:25:57:FB:A7:C6:E4:A5:B2:22:C7:35:91:F8:
        BB:2A:19:42:85:8F:5E:2E:BF:A0:9D:57:94:DF:29:45:
        AA:31:56:6B:7C:C4:5B:54:FE:DE:30:31:B4:FC:4E:0C:
        9D:D8:16:DB:1D:3D:8A:98:6A:BB:C2:34:8B:B4:AA:D1:
        53:66:FF:89:FB:C2:13:12:7D:5B:60:16:CA:D8:17:54:
        7B:41:1D:31:EF:54:DB:49:40:1F:99:FB:18:38:03:EE:
        2D:E8:E1:9F:E6:B2:C3:1C:55:70:F4:F3:B2:E7:4A:5A:
        F5:AA:1D:03:BD:A1:C3:9F:97:80:E6:63:05:27:F2:1F
Exponent              : 65537
Key Version           : A
Public Key #2 Information
-------------------------
Key Type              : Development (Primary)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        E1:61:22:18:6D:0D:A3:D8:C8:54:62:0D:8D:9A:0E:09:
        05:C8:02:5C:B6:51:47:C7:23:AF:1D:1E:AC:8D:9D:0E:
        DD:30:3C:50:26:F6:E8:26:F9:D7:69:D2:1E:DA:4E:24:
        99:D4:A5:A6:13:68:8D:B0:53:39:02:61:64:81:70:94:
        27:A3:31:A5:05:95:63:AF:EA:EB:26:AB:39:8C:31:6A:
        DD:13:22:22:41:A7:3A:FC:19:80:BE:FC:13:2A:C1:39:
        E0:E6:70:1B:DE:4F:69:EB:92:84:34:23:61:AE:46:53:
        C4:68:4E:DE:A3:98:F6:2E:5A:B5:AC:18:05:90:37:80:
        7C:3E:08:E3:03:83:91:30:11:29:E3:12:B0:26:23:AC:
```

```
        0A:C0:DE:31:9D:4B:14:D8:A6:78:B8:B5:84:04:EA:C7:
        FB:CF:C1:DD:16:75:82:FC:1B:5C:FF:B7:C0:36:88:E3:
        3E:BE:44:82:65:2F:66:FF:25:1A:FA:2C:B2:03:17:16:
        0D:C8:33:4F:13:C6:62:D8:53:FC:11:1A:9C:3C:10:EE:
        09:32:FE:38:C2:A2:E2:56:E5:ED:93:89:40:46:B9:E4:
        B3:9C:68:76:B0:BF:0D:FD:33:E6:F6:8C:26:D9:FF:F9:
        DA:B5:D4:86:81:B4:D1:3B:5E:81:1E:20:9F:BE:6E:B7
Exponent              : 65537
Key Version           : A
Public Key #3 Information
--------------------------
Key Type              : Release (Backup)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        96:A2:E6:E4:51:4D:4A:B0:F0:EF:DB:41:82:A6:AC:D0:
        FC:11:40:C2:F0:76:10:19:CE:D0:16:7D:26:73:B1:55:
        FE:42:FE:5D:5F:4D:A5:D5:29:7F:91:EC:91:4D:9B:33:
        54:4B:B8:4D:85:E9:11:2D:79:19:AA:C5:E7:2C:22:5E:
        F6:66:27:98:1C:5A:84:5E:25:E7:B9:09:80:C7:CD:F4:
        13:FB:32:6B:25:B5:22:DE:CD:DC:BE:65:D5:6A:99:02:
        95:89:78:8D:1A:39:A3:14:C9:32:EE:02:4C:AB:25:D0:
        38:AD:E4:C9:C6:6B:28:FE:93:C3:0A:FE:90:D4:22:CC:
        FF:99:62:25:57:FB:A7:C6:E4:A5:B2:22:C7:35:91:F8:
        BB:2A:19:42:85:8F:5E:2E:BF:A0:9D:57:94:DF:29:45:
        AA:31:56:6B:7C:C4:5B:54:FE:DE:30:31:B4:FC:4E:0C:
        9D:D8:16:DB:1D:3D:8A:98:6A:BB:C2:34:8B:B4:AA:D1:
        53:66:FF:89:FB:C2:13:12:7D:5B:60:16:CA:D8:17:54:
        7B:41:1D:31:EF:54:DB:49:40:1F:99:FB:18:38:03:EE:
        2D:E8:E1:9F:E6:B2:C3:1C:55:70:F4:F3:B2:E7:4A:5A:
        F5:AA:1D:03:BD:A1:C3:9F:97:80:E6:63:05:27:F2:1F
Exponent              : 65537
Key Version           : A
Public Key #4 Information
--------------------------
Key Type              : Development (Backup)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        E1:61:22:18:6D:0D:A3:D8:C8:54:62:0D:8D:9A:0E:09:
        05:C8:02:5C:B6:51:47:C7:23:AF:1D:1E:AC:8D:9D:0E:
        DD:30:3C:50:26:F6:E8:26:F9:D7:69:D2:1E:DA:4E:24:
        99:D4:A5:A6:13:68:8D:B0:53:39:02:61:64:81:70:94:
        27:A3:31:A5:05:95:63:AF:EA:EB:26:AB:39:8C:31:6A:
        DD:13:22:22:41:A7:3A:FC:19:80:BE:FC:13:2A:C1:39:
        E0:E6:70:1B:DE:4F:69:EB:92:84:34:23:61:AE:46:53:
        C4:68:4E:DE:A3:98:F6:2E:5A:B5:AC:18:05:90:37:80:
        7C:3E:08:E3:03:83:91:30:11:29:E3:12:B0:26:23:AC:
        0A:C0:DE:31:9D:4B:14:D8:A6:78:B8:B5:84:04:EA:C7:
        FB:CF:C1:DD:16:75:82:FC:1B:5C:FF:B7:C0:36:88:E3:
        3E:BE:44:82:65:2F:66:FF:25:1A:FA:2C:B2:03:17:16:
        0D:C8:33:4F:13:C6:62:D8:53:FC:11:1A:9C:3C:10:EE:
        09:32:FE:38:C2:A2:E2:56:E5:ED:93:89:40:46:B9:E4:
        B3:9C:68:76:B0:BF:0D:FD:33:E6:F6:8C:26:D9:FF:F9:
        DA:B5:D4:86:81:B4:D1:3B:5E:81:1E:20:9F:BE:6E:B7
Exponent              : 65537
Key Version           : A
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show version** | ソフトウェア バージョン、ハードウェア コンフィギュレーション、ライセンス キー、および関連する稼働時間データを表示します。 |

# show ssd

SSD のステータスを表示するには、**show ssd** コマンドを使用します。

（注） このコマンドは、Cisco Secure Firewall 3100 でのみサポートされています。

**show ssd**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1 | このコマンドが導入されました。 |

### 例

次の表示例は、SSD に関する情報を示しています。

```
> show ssd
Local Disk: 1
Name: nvme0n1
Size(MB): 858306
Operability:
operable
Presence:
equipped
Model: Micron_7300_MTFDHBE960TDF
Serial: MSA244302N0
Drive State: online
SED Support:
yes
SED State:
unlocked
SED Auth Status: ok
RAID action: none
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure raid** | SSD を RAID に追加または RAID から削除します。 |
| **show raid** | RAID ステータスを表示します。 |

# show ssh-access-list

管理インターフェイスの SSH アクセスリスト設定を表示するには、**show ssh-access-list** コマンドを使用します。

**show ssh-access-list**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.0.1 | このコマンドが導入されました。 |

## 使用上のガイドライン

管理インターフェイスの SSH アクセスリスト設定を表示するには、このコマンドを使用します。アクセスリストにより、ユーザーが管理 IP アドレスへの SSH 接続を試行できる IP アドレスが決定されます。このリストは、データインターフェイスへの SSH アクセスを制御しません。

### 例

次に、**show ssh-access-list** コマンドからのデフォルトの出力例を示します。このアクセスリストは、任意の IP アドレスから管理 IP アドレスへの SSH 接続を許可します。実際に SSH 接続を完了するには、あらゆるユーザーが有効なユーザー名/パスワードを入力する必要があります。

```
> show ssh-access-list
ACCEPT     tcp  --  anywhere            anywhere            state NEW tcp dpt:ssh
ACCEPT     tcp      anywhere            anywhere            state NEW tcp dpt:ssh
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure ssh-access-list** | 管理インターフェイスの SSH アクセスリストを設定します。 |

# show ssl

アクティブな SSL セッションおよび使用可能な暗号に関する情報を表示するには、**show ssl** コマンドを使用します。

**show ssl** ［**cache** | **ciphers** ［*level*］ | **errors** ［**trace**］ | **mib** ［**64**］ | **objects**］

## 構文の説明

| | |
|---|---|
| **cache** | （オプション）SSL セッション キャッシュの統計情報を表示します。 |
| **ciphers** | （オプション）使用可能な SSL 暗号を表示します。暗号強度を示す特定のレベルで使用可能な暗号のみを表示するには、level キーワードを含めます。考えられるレベルは次のとおりです（強度の昇順）。<br>• **all**<br>• **low**<br>• **medium** （レベルを指定しない場合のデフォルト）<br>• **fips**<br>• **high** （TLSv1.2 にのみ適用） |
| **errors** [**trace**] | （オプション）SSL エラーを表示します。各エラーのトレース情報を含めるには、trace キーワードを含めます。 |
| **mib** [**64**] | （オプション）SSL MIB の統計情報を表示します。64 ビットカウンタの統計情報を表示するには、64 キーワードを含めます。 |
| **objects** | （オプション）SSL オブジェクトの統計情報を表示します。 |

## 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

このコマンドは、現在の SSLv3 以上のセッションに関する情報を表示します。情報には、有効になっている暗号の順序、無効化された暗号、使用されている SSL トラストポイント、証明書認証が有効かどうかが含まれます。これらの設定は、管理インターフェイスではなく、データインターフェイスの SSL 接続用です。

### 例

次に、**show ssl** コマンドの出力例を示します。

```
> show ssl
Accept connections using SSLv3 or greater and negotiate to TLSv1 or greater
Start connections using TLSv1 and negotiate to TLSv1 or greater
SSL DH Group: group2 (1024-bit modulus)
```

```
SSL ECDH Group: group19 (256-bit EC)

SSL trust-points:
  Self-signed (RSA 2048 bits RSA-SHA256) certificate available
  Self-signed (EC 256 bits ecdsa-with-SHA256) certificate available
Certificate authentication is not enabled
```

次に、**show ssl ciphers** コマンドの出力例を示します。

```
> show ssl ciphers
Current cipher configuration:
default (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1.1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1.2 (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
```

```
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
dtlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
>
```

# show ssl-policy-config

現在適用されている SSL ポリシーの設定（ポリシーの説明、デフォルトのロギング設定、有効なすべての SSL ルールとルールの設定など）、信頼できる CA 証明書、および復号化不可能なトラフィックのアクションを表示するには、**show ssl-policy-config** コマンドを使用します。

**show ssl-policy-config**

## 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

Management Center で SSL ポリシーを設定し、そのポリシーをデバイスに割り当てられたアクセス コントロール ポリシーにアタッチします。このコマンドを使用すると、デバイスを通過するトラフィックで SSL 復号化用に設定されたアクションに関する情報を表示できます。

### 例

次の例は、デバイスに SSL ポリシーを設定していない場合に表示される内容を示しています。

```
> show ssl-policy-config
SSL policy not yet applied.
```

次の例は、設定された SSL ポリシーを示しています。

```
> show ssl-policy-config
===============[ General SSL Policy ]===============

=================[ Default Action ]=================
Default Action            : Do Not Decrypt

======[ Category: admin_category (Built-in) ]=======

=====[ Category: standard_category (Built-in) ]=====

----------[ Block unwanted applications ]-----------
State                     : Enabled
Action                    : Block
Source Zones              : outside_zone
Destination Zones         : dmz_zone
Applications              : HTTP/SSL Tunnel (3860)

=======[ Category: root_category (Built-in) ]=======

============[ Trusted CA Certificates ]=============

Cisco-Trusted-Authorities (group)
                              thawte-Primary-Root-CA
                              UTN-DATACorp-SGC
                              Chambers-of-Commerce-Root-2008
                              Izenpe.com-1
```

```
                                    A-Trust-Qual-02
                                    A-Trust-nQual-03
                                    Common-Policy
                                    Starfield-Root-Certificate-Authority-G2
                                    GeoTrust-Primary-Certification-Authority
                                    Certum-Trusted-Network-CA
                                    UTN-USERFirst-Object

C_US-O_VeriSign-Inc.-OU_Class-3-Public-Primary-Certification-Authority-G2-OU_
c-1998-VeriSign-Inc.-For-authorized-use-only-OU_VeriSign-Trust-Network
                                    CA-Disig-Root-R1
                                    C_US-O_Equifax-OU_Equifax-Secure-Certificate-Authority
                                    Thawte-Server-CA-1
                                   VeriSign-Class-3-Public-Primary-Certification-Authority-G3

                                    COMODO-Certification-Authority
                                   VeriSign-Class-3-Public-Primary-Certification-Authority-G5

                                    UTN-USERFirst-Client-Authentication-and-Email
                                    TC-TrustCenter-Universal-CA-III
                                    Cisco-Root-CA-2048
                                    Staat-der-Nederlanden-Root-CA-G2

(...Remaining trusted CA certificates removed...)

==============[ Undecryptable Actions ]===============
Unsupported Cipher Suite  : Inherit Default Action
Unknown Cipher Suite      : Inherit Default Action
Compressed Session        : Inherit Default Action
Uncached Session ID       : Inherit Default Action
SSLv2 Session             : Inherit Default Action
Handshake Error           : Inherit Default Action
Decryption Error          : Block
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show access-policy-config** | 現在設定されているアクセス コントロール ポリシーに関する情報を表示します。 |

# show ssl-protocol

ローカルデバイスマネージャ（Device Manager ）への HTTPS アクセス用に現在設定されている SSL プロトコルを表示するには、**show ssl-protocol** コマンドを使用します。

**show ssl-protocol**

## 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

このコマンドを使用して、管理インターフェイス用に設定されている SSL プロトコルを表示します。これらは、ローカルマネージャである Device Manager を開くために使用される HTTPS 接続用に許可されているプロトコルです。それらの SSL プロトコルは、リモートマネージャには使用されません。

SSL プロトコルを設定するには、**configure ssl-protocol** コマンドを使用します。

### 例

次に、ローカルマネージャを使用しているときに現在定義されている SSL プロトコルを表示する例を示します。

```
> show ssl-protocol
The supported ssl protocols are TLSv1.1 TLSv1.2
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure ssl-protocol** | 管理インターフェイスへの HTTPS アクセス用の SSL プロトコルを設定します。 |

# show startup-config

スタートアップ コンフィギュレーションを表示する、またはスタートアップ コンフィギュレーションがロードされたときのエラーを表示するには、**show startup-config** コマンドを使用します。

**show startup-config** ［**errors**］

## 構文の説明

| | |
|---|---|
| **errors** | （任意）スタートアップ コンフィギュレーションがロードされたときに生成されたエラーを表示します。 |

## 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

**show startup-config** コマンドは、スタートアップシステム設定を表示します。これらのコマンドを直接設定することはできません。代わりに、デバイスを制御するマネージャ（Management Center や Device Manager など）で設定します。

ただし、これは部分的な設定です。ASA ソフトウェア コンフィギュレーション コマンドのみを使用して設定できる内容を示していますが、一部のコマンドは 脅威に対する防御 に固有のコマンドである場合があります。これらのコマンドは 脅威に対する防御 に移植されています。したがって、スタートアップ コンフィギュレーションの情報はトラブルシューティングの補助手段としてのみ使用してください。デバイスマネージャは、デバイス設定を分析する主な手段として使用します。

### 例

次に、**show startup-config** コマンドの出力例を示します。

```
> show startup-config
: Saved

:
: Serial Number: JAD192100RG
: Hardware:   ASA5508, 8192 MB RAM, CPU Atom C2000 series 2000 MHz, 1 CPU (8 cores)
: Written by enable_1 at 20:39:10.749 UTC Tue Jun 28 2016
!
NGFW Version 6.1.0
!
hostname firepower
enable password 8Ry2YjIyt7RRXU24 encrypted
names

(...Output Truncated...)
```

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。 |

# show summary

デバイスに関して最もよく使用される情報（バージョン、タイプ、UUID など）のサマリーを表示するには、**show summary** コマンドを使用します。

**show summary**

## 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

サマリー情報には、基本的な **show version** の出力に加えて、適用されたポリシーと Snort バージョン情報のリストが含まれます。

### 例

次に、サマリー情報の表示例を示します。

```
> show summary
--------[ ftd1.example.com ]---------
Model                     : Cisco ASA5512-X Threat Defense (75) Version 6.1.0 (Build
2007)
UUID                      : 703006f4-8ff6-11e6-bb6e-8f2d5febf243
Rules update version      : 2016-03-28-001-vrt
VDB version               : 271
-----------------------------------------------------

------------------[ policy info ]-------------------
Access Control Policy     : Initial AC Policy
Intrusion Policy          : Balanced Security and Connectivity

-----------------------------------------------------

---------------[ snort version info ]---------------
Snort Version             : 2.9.10 GRE (Build 20)
libpcap Version           : 1.1.1
PCRE Version              : 7.6 2008-01-28
ZLIB Version              : 1.2.8
-----------------------------------------------------
```

# show sunrpc-server active

NFS や NIS などの Sun RPC サービス用に開いているピンホールを表示するには、**show sunrpc-server active** コマンドを使用します。

**show sunrpc-server active**

## 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、**show sunrpc-server active** コマンドの出力例を示します。

```
> show sunrpc-server active
        LOCAL           FOREIGN                 SERVICE TIMEOUT
        -----------------------------------------------
        192.168.100.2/0 209.165.200.5/32780     100005 00:10:00
```

LOCAL カラムのエントリは、内部インターフェイスのクライアントまたはサーバーの IP アドレスを示します。FOREIGN カラムの値は、外部インターフェイスのクライアントまたはサーバーの IP アドレスを示します。

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear sunrpc-server active** | NFS や NIS などの Sun RPC サービス用に開いているピンホールをクリアします。 |
| **show running-config sunrpc-server** | SunRPC サービス コンフィギュレーションに関する情報を表示します。 |

# show switch mac-address-table

スイッチの MAC アドレステーブルを表示するには、**show switch mac-address-table** コマンドを使用します。

（注） Firepower 1010 でのみサポートされています。

**show switch mac-address-table**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.5 | このコマンドが導入されました。 |

## 使用上のガイドライン

スイッチ MAC アドレス テーブルには、スイッチ ハードウェア内の各 VLAN のトラフィックに適用する MAC アドレスとスイッチ ポートのマッピングが保持されます。このブリッジ MAC アドレス テーブルには、VLAN 間を通過するトラフィックに適用する MAC アドレスと VLAN インターフェイスのマッピングが保持されます。

MAC アドレス エントリは 5 分経過するとエージング アウトします。

### 例

次に、**show switch mac-address-table** コマンドの出力例を示します。

```
> show switch mac-address-table
Legend: Age - entry expiration time in seconds
 Mac Address | VLAN | Type | Age | Port
-----------------------------------------------------
 000e.0c4e.2aa4 | 0001 | dynamic | 287 | Et1/1
 0012.d927.fb03 | 0001 | dynamic | 287 | Et1/1
 0013.c4ca.8a8c | 0001 | dynamic | 287 | Et1/1
 00b0.6486.0c14 | 0001 | dynamic | 287 | Et1/1
 00d0.2bff.449f | 0001 | static | - | In0/1
 0100.5e00.000d | 0001 | static multicast | - | In0/1,Et1/1-8
Total Entries: 6
```

次の表は、各フィールドの説明を示しています。

***表 50 : show switch mac-address-table のフィールド***

| フィールド | 説明 |
|---|---|
| Mac Address | MAC アドレスを表示します。 |
| VLAN | MAC アドレスに関連付けられている VLAN を表示します。 |

| フィールド | 説明 |
|---|---|
| タイプ | MAC アドレスを、ダイナミックに学習するか、スタティック マルチキャスト アドレスとして学習するか、またはスタティックに学習するかを示します。スタティック エントリは、内部バックプレーン インターフェイスの場合にのみ該当します。 |
| Age | MACアドレステーブル内にあるダイナミック エントリの経過時間を表示します。 |
| Port | この MAC アドレスのホストに到達できるスイッチ ポートを表示します。 |

## 関連コマンド

| Command | 説明 |
|---|---|
| **show switch vlan** | VLAN と物理 MAC アドレスの関連付けを表示します。 |

# show switch vlan

VLAN および関連するスイッチポートを表示するには、**show switch vlan** コマンドを使用します。

（注） Firepower 1010 でのみサポートされています。

**show switch vlan**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.5 | 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、組み込みスイッチを持つモデル専用です。他のモデルの場合は、**show vlan** コマンドを使用します。

### 例

次に、**show switch vlan** コマンドの出力例を示します。

```
> show switch vlan

VLAN Name                            Status    Ports
---- --------------------------------- --------- -------------
100  inside                            up        Et1/1, Et1/2
200  outside                           up        Et1/8
300  -                                 down      Et1/2, Et1/3
400  backup                            down      Et1/4
```

次の表は、各フィールドの説明を示しています。

表 *51 : show switch vlan* のフィールド

| フィールド | 説明 |
|---|---|
| VLAN | VLAN 番号を表示します。 |
| 名前 | VLANインターフェイスの名前を表示します。名前が設定されていない場合、またはVLANインターフェイスがない場合は、ダッシュ（-）が表示されます。 |
| Status（ステータス） | スイッチ内のVLANとトラフィックを送受信するためのステータス（upまたはdown）を表示します。VLANがアップ状態になるには、そのVLANで少なくとも1つのスイッチ ポートがアップ状態である必要があります。 |

| フィールド | 説明 |
| --- | --- |
| ポート | 各 VLAN に割り当てられたスイッチ ポートを表示します。1 つのスイッチ ポートが複数の VLAN にリストされている場合、そのポートはトランク ポートです。上記の出力例で、Ethernet 1/2 は VLAN 100 および VLAN 300 を伝送するトランクポートです。 |

## 関連コマンド

| Command | 説明 |
| --- | --- |
| **show switch mac-address-table** | スイッチ MAC アドレステーブルを表示します。 |

# show tcpstat

TCP スタックおよびデバイスで終端している TCP 接続のステータスを（デバッグのために）表示するには、**show tcpstat** コマンドを使用します。

**show tcpstat**

## 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

**show tcpstat** コマンドを使用すると、TCP スタックおよびデバイスで終端している TCP 接続のステータスを表示できます。次の表に、表示される TCP 統計情報の説明を示します。

表 *52 : show tcpstat* コマンドの *TCP* 統計情報

| 統計 | 説明 |
|---|---|
| tcb_cnt | TCP ユーザーの数。 |
| proxy_cnt | TCP プロキシの数。TCP プロキシは、ユーザー認可で使用されます。 |
| tcp_xmt pkts | TCP スタックが送信したパケットの数。 |
| tcp_rcv good pkts | TCP スタックが受信した正常なパケットの数。 |
| tcp_rcv drop pkts | TCP スタックがドロップした受信パケットの数。 |
| tcp bad chksum | チェックサムに誤りがあった受信パケットの数。 |
| tcp user hash add | ハッシュ テーブルに追加された TCP ユーザーの数。 |
| tcp user hash add dup | 新しい TCP ユーザーをハッシュ テーブルに追加しようとしたとき、そのユーザーがすでにテーブル内に存在していた回数。 |
| tcp user srch hash hit | 検索時にハッシュ テーブル内でTCPユーザーが検出された回数。 |
| tcp user srch hash miss | 検索時にハッシュ テーブル内で TCP ユーザーが検出されなかった回数。 |
| tcp user hash delete | TCP ユーザーがハッシュ テーブルから削除された回数。 |
| tcp user hash delete miss | TCPユーザーを削除しようとしたとき、そのユーザーがハッシュ テーブル内で検出されなかった回数。 |
| lip | TCP ユーザーのローカル IP アドレス。 |
| fip | TCP ユーザーの外部 IP アドレス。 |

| 統計 | 説明 |
|---|---|
| lp | TCP ユーザーのローカル ポート。 |
| fp | TCP ユーザーの外部ポート。 |
| st | TCP ユーザーの状態（RFC 793 を参照）。表示される値は次のとおりです。<br><br>1 CLOSED<br>2 LISTEN<br>3 SYN_SENT<br>4 SYN_RCVD<br>5 ESTABLISHED<br>6 FIN_WAIT_1<br>7 FIN_WAIT_2<br>8 CLOSE_WAIT<br>9 CLOSING<br>10 LAST_ACK<br>11 TIME_WAIT |
| rexqlen | TCP ユーザーの再送信キューの長さ。 |
| inqlen | TCP ユーザーの入力キューの長さ。 |
| tw_timer | TCP ユーザーの time_wait タイマーの値（ミリ秒）。 |
| to_timer | TCP ユーザーの非アクティビティ タイムアウト タイマーの値（ミリ秒）。 |
| cl_timer | TCP ユーザーのクローズ要求タイマーの値（ミリ秒）。 |
| per_timer | TCP ユーザーの持続タイマーの値（ミリ秒）。 |
| rt_timer | TCP ユーザーの再送信タイマーの値（ミリ秒）。 |
| tries | TCP ユーザーの再送信回数。 |

## 例

次に、TCP スタックのステータスを表示する例を示します。

```
> show tcpstat
                 CURRENT MAX      TOTAL
tcb_cnt          2       12       320
proxy_cnt        0       0        160

tcp_xmt pkts = 540591
tcp_rcv good pkts = 6583
tcp_rcv drop pkts = 2
tcp bad chksum = 0
tcp user hash add = 2028
tcp user hash add dup = 0
```

```
tcp user srch hash hit = 316753
tcp user srch hash miss = 6663
tcp user hash delete = 2027
tcp user hash delete miss = 0

lip = 203.0.113.45 fip = 192.0.2.12 lp = 443 fp = 2567 st = 4 rexqlen = 0
in0
  tw_timer = 0 to_timer = 179000 cl_timer = 0 per_timer = 0
  rt_timer = 0 tries 0
```

| Command | 説明 |
|---|---|
| **show conn** | 使用されている接続と使用可能な接続を表示します。 |

# show tech-support

テクニカル サポート アナリストが診断時に使用する情報を表示するには、**show tech-support** コマンドを使用します。

**show tech-support**

## 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。 |
| 7.1 | **show access-list element-count** および **show asp rule-engine** からの出力が追加されました。 |

## 使用上のガイドライン

**show tech-support** コマンドでは、テクニカル サポート アナリストが問題を診断する場合に役立つ情報が表示されます。

### 例

次に、テクニカル サポート分析に使用される情報を表示する例を示します。出力は、先頭のみが表示されるように短縮されます。この出力は非常に長いため、結果が表示されるまでに時間がかかります。

```
> show tech-support

-------------[ ftd1.example.com ]--------------
Model                     : Cisco ASA5508-X Threat Defense (75) Version 6.1.0 (B
uild 226)
UUID                      : 43235986-2363-11e6-b278-aff0a43948fe
Rules update version      : 2016-03-28-001-vrt
VDB version               : 270
------------------------------------------------

Cisco Adaptive Security Appliance Software Version 9.6(1)72

Compiled on Fri 20-May-16 13:36 PDT by builders
System image file is "disk0:/os.img"
Config file at boot was "startup-config"

firepower up 3 days 16 hours

Hardware:   ASA5508, 8192 MB RAM, CPU Atom C2000 series 2000 MHz, 1 CPU (8 cores
)
Internal ATA Compact Flash, 8192MB
BIOS Flash M25P64 @ 0xfed01000, 16384KB
Encryption hardware device : Cisco ASA Crypto on-board accelerator (revision 0x1
)
(...Remaining output truncated...)
```

# show threat-detection memory

実行コンフィギュレーションで **threat-detection statistics** コマンドによって有効にされた高度な脅威検出統計情報で使用されるメモリを表示するには、**show threat-detection memory** コマンドを使用します。

**show threat-detection memory**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

## 使用上のガイドライン

一部の統計情報は大量のメモリを使用して、システムのパフォーマンスに影響を与えることがあります。このコマンドを使用すると、必要に応じてコンフィギュレーションを調整できるようにメモリ使用率をモニターできます。

FlexConfig を使用して、**threat-detection statistics** コマンドを設定します。

### 例

次に、**show threat-detection memory** コマンドの出力例を示します。

```
> show threat-detection memory
Cached chunks:
       CACHE TYPE              BYTES USED
TD Host                          70245888
TD Port                              2724
TD Protocol                          1476
TD ACE                                728
TD Shared counters                  14256
============================
Subtotal TD Chunks               70265072


Regular memory                 BYTES USED
TD Port                              33824
TD Control block                    162064
============================
Subtotal Regular Memory             195888


Total TD memory:                 70460960
```

| Command | 説明 |
|---|---|
| **show running-config all threat-detection** | 脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。 |
| **show threat-detection statistics host** | ホストの統計情報を表示します。 |

| Command | 説明 |
| --- | --- |
| **show threat-detection statistics port** | ポートの統計情報を表示します。 |
| **show threat-detection statistics protocol** | プロトコルの統計情報を表示します。 |
| **show threat-detection statistics top** | 上位 10 位までの統計情報を表示します。 |

# show threat-detection rate

**threat-detection basic-threat** コマンドを使用して（FlexConfig を使用）基本的な脅威検出を有効にすると、**show threat-detection rate** コマンドを使用して統計情報を表示できます。

**show threat-detection rate** ［**min-display-rate** *events_per_second*］［**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**］

## 構文の説明

| | |
|---|---|
| **acl-drop** | （任意）アクセス リストで拒否されたためにドロップされたパケットのレートを表示します。 |
| **bad-packet-drop** | （任意）パケット形式に誤りがあって（invalid-ip-header または invalid-tcp-hdr-length など）拒否されたためにドロップされたパケットのレートを表示します。 |
| **conn-limit-drop** | （任意）接続制限（システム全体のリソース制限および設定された制限の両方）を超えたためにドロップされたパケットのレートを表示します。 |
| **dos-drop** | （任意）DoS 攻撃（無効な SPI やステートフル ファイアウォール チェック不合格など）を検出したためにドロップされたパケットのレートを表示します。 |
| **fw-drop** | （任意）基本ファイアウォール チェックに不合格だったためにドロップされたパケットのレートを表示します。このオプションは、このコマンドのファイアウォールに関連したパケット ドロップをすべて含む複合レートです。interface-drop、inspect-drop、scanning-threat など、ファイアウォールに関連しないドロップ レートは含まれません。 |
| **icmp-drop** | （任意）疑わしい ICMP パケットが検出されたためにドロップされたパケットのレートを表示します。 |
| **inspect-drop** | （任意）アプリケーション インスペクションに不合格だったパケットが原因でドロップされたパケットのレート制限を表示します。 |
| **interface-drop** | （任意）インターフェイスの過負荷が原因でドロップされたパケットのレート制限を表示します。 |
| **min-display-rate** *events_per_second* | （任意）最小表示レート（1 秒あたりのイベント数）を超えた統計情報だけが表示されるように制限します。0 ～ 2147483647 の範囲で指定します。 |

| | |
|---|---|
| **scanning-threat** | （任意）スキャン攻撃が検出されたためにドロップされたパケットのレートを表示します。このオプションでは、たとえば最初の TCP パケットが SYN パケットでない、またはスリーウェイ ハンドシェイクで TCP 接続に失敗したなどのスキャン攻撃をモニターします。フルスキャン脅威検出では、このスキャン攻撃レート情報を収集し、ホストを攻撃者として分類して自動的に排除することによって対処します。 |
| **syn-attack** | （オプション）TCP SYN 攻撃や戻りデータなしの UDP セッション攻撃など、不完全なセッションが原因でドロップされたパケットのレートを表示します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

## 使用上のガイドライン

ディスプレイの出力には、次の情報が表示されます。

- 固定された期間の平均レート（イベント数/秒）
- 終了した最後のバースト間隔における現在のバースト レート（イベント数/秒）。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうの間隔。
- レートが制限を超えた回数。
- 固定された期間におけるイベントの合計数

システムは、平均レート間隔内でイベントカウントを30回計算します。つまり、システムは、合計 30 回の完了バースト間隔で、各バースト期間の終わりにレートをチェックします。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が10分の場合、バースト間隔は 10 秒です。最後のバースト間隔が 3:00:00 から 3:00:10 までであった場合に **show** コマンドを 3:00:15 に使用すると、最後の 5 秒分の情報は出力に含まれません。

このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、システムは、最後の 59 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニターできます。

### 例

次に、**show threat-detection rate** コマンドの出力例を示します。

```
> show threat-detection rate

                        Average(eps)    Current(eps) Trigger         Total events
  10-min ACL  drop:                0               0       0                   16
  1-hour ACL  drop:                0               0       0                  112
  1-hour SYN attck:                5               0       2                21438
```

```
10-min  Scanning:                0          0      29                193
1-hour  Scanning:              106          0      10             384776
1-hour Bad  pkts:               76          0       2             274690
10-min  Firewall:                0          0       3                 22
1-hour  Firewall:               76          0       2             274844
10-min DoS attck:                0          0       0                  6
1-hour DoS attck:                0          0       0                 42
10-min Interface:                0          0       0                204
1-hour Interface:               88          0       0             318225
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear threat-detection rate** | 基本脅威検出の統計情報をクリアします。 |
| **show running-config all threat-detection** | 脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。 |
| **show threat-detection statistics** | 脅威検出の統計情報を表示します。 |

# show threat-detection scanning-threat

（FlexConfig を使用して）**threat-detection scanning-threat** コマンドで脅威検出のスキャンを有効にした場合は、**show threat-detection scanning-threat** コマンドを使用して攻撃者およびターゲットとして分類されたホストを表示します。

**show threat-detection scanning-threat** ［**attacker** | **target**］

## 構文の説明

| | |
|---|---|
| **attacker** | （任意）攻撃元ホストの IP アドレスを表示します。 |
| **target** | （オプション）攻撃対象ホストの IP アドレスを表示します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

### 例

次に、**show threat-detection scanning-threat** コマンドの出力例を示します。

```
> show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0 (l21)
    192.168.1.249 (l21)
Latest Attacker Host & Subnet List:
    192.168.10.234 (outside)
    192.168.10.0 (outside)
    192.168.10.2 (outside)
    192.168.10.3 (outside)
    192.168.10.4 (outside)
    192.168.10.5 (outside)
    192.168.10.6 (outside)
    192.168.10.7 (outside)
    192.168.10.8 (outside)
    192.168.10.9 (outside)
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear threat-detection scanning-threat** | スキャンする脅威の攻撃者とターゲットのリストをクリアします。 |
| **show running-config all threat-detection** | 脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。 |
| **show threat-detection statistics** | 脅威検出の統計情報を表示します。 |
| **shun** | 脅威の攻撃者のスキャンなど、指定されたホストからの接続をブロックします。 |

# show threat-detection shun

（FlexConfig を使用して）**threat-detection scanning-threat** コマンドで脅威検出のスキャンを有効にし、攻撃元ホストを自動的に回避した場合は、**show threat-detection shun** コマンドを使用すると、現在回避されているホストが表示されます。

**show threat-detection scanning-host**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

## 使用上のガイドライン

回避対象からホストを除外するには、**clear threat-detection shun** コマンドを使用します。

### 例

次に、**show threat-detection shun** コマンドの出力例を示します。

```
> show threat-detection shun
Shunned Host List:
(outside) src-ip=10.0.0.13 255.255.255.255
(inside) src-ip=10.0.0.13 255.255.255.255
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear threat-detection shun** | 自動的に回避されるホストのリストをクリアします。 |
| **show running-config all threat-detection** | 脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。 |
| **show threat-detection scanning-threat** | スキャンする脅威の攻撃者とターゲットを表示します。 |
| **show threat-detection statistics** | 脅威検出の統計情報を表示します。 |
| **shun** | 脅威の攻撃者のスキャンなど、指定されたホストからの接続をブロックします。 |

# show threat-detection statistics

**threat-detection statistics** コマンド（FlexConfig を使用）で脅威の統計情報を有効にする場合は、**show threat-detection statistics** コマンドを使用して統計情報を表示します。わかりやすくするため、次の図では主要なキーワードとオプションを個別に示しています。

**show threat-detection statistics** ［**min-display-rate** *eps*］ **host** ［*ip_address* ［*mask*］］

**show threat-detection statistics** ［**min-display-rate** *eps*］ **port** ［*start_port*［*-end_port*］］

**show threat-detection statistics** ［**min-display-rate** *eps*］ **protocol** ［*number* | *name*］

**show threat-detection statistics** ［**min-display-rate** *eps*］ **top** ［**access-list** | **host** | **port-protocol**］［**rate-1** | **rate-2** | **rate-3**］ | **tcp-intercept** ［**all**］［**detail**］［**long**］］

## 構文の説明

| | |
|---|---|
| **host** [*ip_address* [*mask*]] | ホストの統計情報を表示します。必要に応じて、IP アドレスを指定して特定のホストの統計情報を表示できます。ホストのサブネットマスクを含めることができます。<br>FlexConfig を使用して **threat-detection statistics host** コマンドを設定し、ホストの統計情報を有効にします。 |
| **min-display-rate** *eps* | （任意）最小表示レート（1 秒あたりのイベント数）を超えた統計情報だけが表示されるように制限します。0 ～ 2147483647 の範囲で指定します。 |
| **port** [*start_port*[*-end_port*]] | TCP/UDP ポートの統計情報を表示します。必要に応じて、単一のポートまたはポートの範囲（0 ー 65535）を指定できます。<br>FlexConfig を使用して **threat-detection statistics port** コマンドを設定し、ポートの統計情報を有効にします。 |
| **protocol** [*number* | *name*] | プロトコルの統計情報を表示します。必要に応じて、数字または名前でプロトコルを指定できます。使用できる数字は 0ー255 です。次のいずれかの名前を使用できます。ah、eigrp、esp、gre、icmp、igmp、igrp、ip ipinip、ipsec、nos、ospf、pcp、pim、pptp、snp、tcp、udp<br>FlexConfig を使用して **threat-detection statistics protocol** コマンドを設定し、プロトコルの統計情報を有効にします。 |

| | |
|---|---|
| **top** [**access-list** \| **host** \| **port-protocol**] [**rate-1** \| **rate-2** \| **rate-3**] | 統計情報を有効にしたオプションに応じて、上位10件のアクセスルール、ホスト、およびポート/プロトコルを表示します。次のキーワードを使用して、表示を絞り込むことができます。<br>• **access-list** 許可 ACE と拒否 ACE の両方を含む、パケットに一致する上位 10 件の ACE を表示します。**threat-detection basic-threat** コマンドを使用して基本脅威検出を有効にすると、**show threat-detection rate access-list** コマンドを使用してアクセスリストの拒否を追跡できます。<br>• **host** 一定期間ごとに上位 10 件のホスト統計情報を表示します。脅威の検出アルゴリズムにより、フェールオーバー リンクまたはステート リンクに使用するインターフェイスは、上位 10 のホストの 1 つとして表示される可能性があります。この現象は、フェールオーバー リンクとステート リンクの両方に 1 つのインターフェイスを使用するときに発生する可能性が高くなります。これは正常な動作であり、この IP アドレスが表示されても無視してかまいません。<br>• **port-protocol** TCP/UDP ポートタイプと IP プロトコルタイプを組み合わせた上位 10 件の統計情報を表示します。TCP（プロトコル 6）と UDP（プロトコル 17）は、IP プロトコルの表示に含まれていません。<br>• **rate-1**、**rate-2**、**rate-3** は、指定した固定レート期間の統計情報のみを表示します。指定できる最小間隔は 1、最大間隔は 3 です。たとえば、ディスプレイに直前の 1 時間、8 時間、および 24 時間の統計情報が表示されるとします。その場合、レート 1 は 1 時間、レート 2 は 8 時間、レート 3 は 24 時間を表します。 |
| **top tcp-intercept**[**all**] [**detail**] [**long**] | TCP代行受信の統計情報を表示します。表示には、攻撃を受けて保護された上位 10 サーバーが含まれます。次のキーワードを含めることができます。<br>• **all** トレースされているすべてのサーバーの履歴データを表示します。<br>• **detail** 履歴サンプリングデータを表示します。<br>• **long** サーバーの実際の IP アドレスおよび変換後の IP アドレスとともに、統計情報の履歴を long 形式で表示します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

## 使用上のガイドライン

脅威検出統計情報には、許可およびドロップされたトラフィック レートが表示されます。

ディスプレイの出力には、次の情報が表示されます。

- 固定された期間の平均レート（イベント数/秒）
- 終了した最後のバースト間隔における現在のバースト レート（イベント数/秒）。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうの間隔。
- レートを超過した回数（ドロップされたトラフィックの統計情報の場合に限る）
- 固定された期間におけるイベントの合計数

システムは、平均レート間隔内でイベントカウントを30回計算します。つまり、システムは、合計 30 回の完了バースト間隔で、各バースト期間の終わりにレートをチェックします。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が20分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。

このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30個目）のイベント数よりすでに多くなっている場合です。この場合、システムは、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニターできます。

次の表に、TCP代行受信の表示を除く、すべてのコマンドの出力を示します。この出力の説明については、TCP 代行受信の例を参照してください。

| フィールド | 説明 |
|---|---|
| 上<br>Name, ID | 上位レポートの場合、この列にはアクセス制御エントリの名前または番号、ホストの IP アドレス、またはポートやプロトコルの名前/ID 番号が表示されます。<br>エントリは固定レート間隔でグループ化され、該当期間内で「0」（最大数）から「9」（最小数）にランク付けされます。10 の順位すべてについて十分な統計情報がない場合、指定した間隔に関して表示される項目が 10 未満になることがあります。<br>ホストおよびポートプロトコルの場合、グループ化は、固定間隔あたりの送受信済みバイト数およびパケット数に基づいて行われます。 |

| フィールド | 説明 |
|---|---|
| Average(eps) | 各間隔における平均レート（イベント数/秒）を表示します。<br><br>システムは、各バースト期間の終わりにこの数を保存します。合計で 30 回分の完了したバースト間隔における数を保存します。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に show コマンドを使用すると、最後の 5 秒間は出力に含まれません。<br><br>このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、システムは、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニターできます。 |
| Current(eps) | 終了した最後のバースト間隔における現在バースト レート（イベント数/秒）を表示します。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうです。Average(eps) の説明で示された例の場合、現在レートは 3:19:30 ～ 3:20:00 のレートです。 |
| Trigger | ドロップされたパケット レートの制限値を超過した回数が表示されます。送受信バイトとパケットの行で指定された有効なトラフィックの場合、この値は常に0です。これは、有効なトラフィックをトリガーするレート制限がないためです。 |
| Total events | 各レート間隔におけるイベントの合計数を表示します。現在進行中の未完了バースト間隔は、合計イベント数に含まれません。このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、システムは、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニターできます。 |

| フィールド | 説明 |
| --- | --- |
| Entry heading | 統計情報は、見出しの下に固定間隔でグループ化されます。見出しには、次の行で説明される情報を含めることができます。一般に、エントリの見出しは次の要素から始まります。<br>• ホスト、およびホスト IP アドレス。<br>• ポート番号やポート名。80/HTTP など。<br>• プロトコル番号またはプロトコル名。ICMP など。<br>• 上位レポートの場合、固定間隔および統計タイプ。アクセスリストの場合、見出しは表示が ACL ヒットに関するものであることを示します。 |
| tot-ses | ホストがデータベースに追加された時点以降のホストにおける合計セッション数を表示します。 |
| act-ses | ホスト、ポート、またはプロトコルが現在関係しているアクティブなセッションの合計数を表示します。 |
| fw-drop<br>（ホストのみ） | ファイアウォールでのドロップ数を表示します。ファイアウォール ドロップは、基本脅威検出で追跡されたすべてのファイアウォール関連のパケットドロップを含む組み合わせレートです。これには、アクセス リストでの拒否、不良パケット、接続制限の超過、DoS 攻撃パケット、疑わしい ICMP パケット、TCP SYN 攻撃パケット、および戻りデータなしの UDP セッション攻撃パケットなどが含まれます。インターフェイスの過負荷、アプリケーション インスペクションで不合格のパケット、スキャン攻撃の検出など、ファイアウォールに関連しないパケット ドロップは含まれていません。 |
| insp-drop<br>（ホストのみ） | アプリケーション インスペクションに不合格になったためにドロップされたパケット数を表示します。 |
| null-ses<br>（ホストのみ） | ヌル セッションの数を表示します。ヌル セッションとは、タイムアウトするまでの 30 秒以内に完了しなかった TCP SYN セッションと、セッションが開始されてから 3 秒以内にサーバーからデータの送信がなかった UDP セッションです。 |
| bad-acc<br>（ホストのみ） | 閉じられた状態のホストのポートに対する不正なアクセスの試行回数を表示します。ポートがヌルセッション状態（上記を参照）であると判定されると、ホストのポート状態は HOST_PORT_CLOSE に設定されます。そのホストのポートにアクセスしようとするクライアントはすべて、タイムアウトを待たずにすぐ不正アクセスとして分類されます。 |

| フィールド | 説明 |
|---|---|
| 20-min、1-hour、8-hour、および 24-hour | これらの固定レート間隔における統計情報を表示します。<br>• Sent byte、Sent pkts：ホスト、ポート、またはプロトコルから正常に送信されたバイト数またはパケット数を表示します。<br>• Sent drop：スキャン攻撃の一部であったためにドロップされた、ホスト、ポート、またはプロトコルから送信されたパケット数を表示します。<br>• Recv byte、pkts：ホスト、ポート、またはプロトコルに正常に受信されたバイト数またはパケット数を表示します。<br>• Recv drop：スキャン攻撃の一部であったためにドロップされた、ホスト、ポート、またはプロトコルに受信されたパケット数を表示します。 |

### 例

次に、**show threat-detection statistics host** コマンドの出力例を示します。

```
> show threat-detection statistics host

                            Average(eps)    Current(eps) Trigger         Total events
Host:10.0.0.1: tot-ses:289235 act-ses:22571 fw-drop:0 insp-drop:0 null-ses:21438 bad-acc:0

  1-hour Sent byte:               2938               0       0             10580308
  8-hour Sent byte:                367               0       0             10580308
 24-hour Sent byte:                122               0       0             10580308
  1-hour Sent pkts:                 28               0       0               104043
  8-hour Sent pkts:                  3               0       0               104043
 24-hour Sent pkts:                  1               0       0               104043
  20-min Sent drop:                  9               0       1                10851
  1-hour Sent drop:                  3               0       1                10851
  1-hour Recv byte:               2697               0       0              9712670
  8-hour Recv byte:                337               0       0              9712670
 24-hour Recv byte:                112               0       0              9712670
  1-hour Recv pkts:                 29               0       0               104846
  8-hour Recv pkts:                  3               0       0               104846
 24-hour Recv pkts:                  1               0       0               104846
  20-min Recv drop:                 42               0       3                50567
  1-hour Recv drop:                 14               0       1                50567
Host:10.0.0.0: tot-ses:1 act-ses:0 fw-drop:0 insp-drop:0 null-ses:0 bad-acc:0
  1-hour Sent byte:                  0               0       0                  614
  8-hour Sent byte:                  0               0       0                  614
 24-hour Sent byte:                  0               0       0                  614
  1-hour Sent pkts:                  0               0       0                    6
  8-hour Sent pkts:                  0               0       0                    6
 24-hour Sent pkts:                  0               0       0                    6
  20-min Sent drop:                  0               0       0                    4
  1-hour Sent drop:                  0               0       0                    4
  1-hour Recv byte:                  0               0       0                  706
  8-hour Recv byte:                  0               0       0                  706
```

```
 24-hour Recv byte:                  0               0       0                  706
  1-hour Recv pkts:                  0               0       0                    7
```

次に、**show threat-detection statistics port** コマンドの出力例を示します。

```
> show threat-detection statistics port

                           Average(eps)    Current(eps) Trigger         Total events
80/HTTP: tot-ses:310971 act-ses:22571
  1-hour Sent byte:                2939               0       0             10580922
  8-hour Sent byte:                 367           22043       0             10580922
 24-hour Sent byte:                 122            7347       0             10580922
  1-hour Sent pkts:                  28               0       0               104049
  8-hour Sent pkts:                   3             216       0               104049
 24-hour Sent pkts:                   1              72       0               104049
  20-min Sent drop:                   9               0       2                10855
  1-hour Sent drop:                   3               0       2                10855
  1-hour Recv byte:                2698               0       0              9713376
  8-hour Recv byte:                 337           20236       0              9713376
 24-hour Recv byte:                 112            6745       0              9713376
  1-hour Recv pkts:                  29               0       0               104853
  8-hour Recv pkts:                   3             218       0               104853
 24-hour Recv pkts:                   1              72       0               104853
  20-min Recv drop:                  24               0       2                29134
  1-hour Recv drop:                   8               0       2                29134
```

次に、**show threat-detection statistics protocol** コマンドの出力例を示します。

```
> show threat-detection statistics protocol

                           Average(eps)    Current(eps) Trigger         Total events
ICMP: tot-ses:0 act-ses:0
  1-hour Sent byte:                   0               0       0                 1000
  8-hour Sent byte:                   0               2       0                 1000
 24-hour Sent byte:                   0               0       0                 1000
  1-hour Sent pkts:                   0               0       0                   10
  8-hour Sent pkts:                   0               0       0                   10
 24-hour Sent pkts:                   0               0       0                   10
```

次に、**show threat-detection statistics top access-list** コマンドの出力例を示します。

```
> show threat-detection statistics top access-list

                   Top    Average(eps)    Current(eps) Trigger         Total events
  1-hour ACL hits:
              100/3[0]             173               0       0               623488
              200/2[1]              43               0       0               156786
              100/1[2]              43               0       0               156786
  8-hour ACL hits:
              100/3[0]              21            1298       0               623488
              200/2[1]               5             326       0               156786
              100/1[2]               5             326       0               156786
```

次に、**show threat-detection statistics top port-protocol** コマンドの出力例を示します。

```
> show threat-detection statistics top port-protocol

Top          Name   Id    Average(eps)    Current(eps) Trigger      Total events
  1-hour Recv byte:
 1         gopher   70              71               0       0          32345678
 2  btp-clnt/dhcp   68              68               0       0          27345678
```

```
 3         gopher   69              65              0       0          24345678
 4    Protocol-96 * 96              63              0       0          22345678
 5      Port-7314 7314              62              0       0          12845678
 6 BitTorrent/trc 6969              61              0       0          12645678
 7     Port-8191-65535              55              0       0          12345678
 8           SMTP  366              34              0       0           3345678
 9         IPinIP *  4              30              0       0           2345678
10          EIGRP * 88              23              0       0           1345678
  1-hour Recv pkts:
...
...
  8-hour Recv byte:
...
...
  8-hour Recv pkts:
...
...
 24-hour Recv byte:
...
...
 24-hour Recv pkts:
...
...

Note: Id preceded by * denotes the Id is an IP protocol type
```

次に、**show threat-detection statistics top host** コマンドの出力例を示します。

```
> show threat-detection statistics top host

                   Top    Average(eps)    Current(eps) Trigger         Total events
  1-hour Sent byte:
          10.0.0.1[0]            2938              0       0             10580308
  1-hour Sent pkts:
          10.0.0.1[0]              28              0       0               104043
  20-min Sent drop:
          10.0.0.1[0]               9              0       1                10851
  1-hour Recv byte:
          10.0.0.1[0]            2697              0       0              9712670
  1-hour Recv pkts:
          10.0.0.1[0]              29              0       0               104846
  20-min Recv drop:
          10.0.0.1[0]              42              0       3                50567
  8-hour Sent byte:
          10.0.0.1[0]             367              0       0             10580308
  8-hour Sent pkts:
          10.0.0.1[0]               3              0       0               104043
  1-hour Sent drop:
          10.0.0.1[0]               3              0       1                10851
  8-hour Recv byte:
          10.0.0.1[0]             337              0       0              9712670
  8-hour Recv pkts:
          10.0.0.1[0]               3              0       0               104846
  1-hour Recv drop:
          10.0.0.1[0]              14              0       1                50567
 24-hour Sent byte:
          10.0.0.1[0]             122              0       0             10580308
 24-hour Sent pkts:
          10.0.0.1[0]               1              0       0               104043
 24-hour Recv byte:
          10.0.0.1[0]             112              0       0              9712670
 24-hour Recv pkts:
          10.0.0.1[0]               1              0       0               104846
```

次に、**show threat-detection statistics top tcp-intercept** コマンドの出力例を示します。

```
> show threat-detection statistics top tcp-intercept

Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
 Time)>
------------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

次の表で、TCP 代行受信の出力について説明します。

| フィールド | 説明 |
|---|---|
| Monitoring window size | 統計情報のためにシステムがデータをサンプリングする期間を表示します。デフォルトは 30 分です。この設定は、FlexConfig を使用して **threat-detection statistics tcp-intercept rate-interval** コマンドで変更できます。システムは、この間隔でデータを 30 回サンプリングします。 |
| Sampling interval | サンプリング間の間隔を表示します。この値は、常にレート間隔を 30 で割った数値になります。 |
| ランク | 1 ～ 10 位のランキングを表示します。1 位は最も攻撃を受けたサーバーで、10 位は最も攻撃が少なかったサーバーです。 |
| Server IP:Port | 攻撃を受けているサーバーの IP アドレスおよびポートを表示します。 |
| インターフェイス | サーバーが攻撃を受けているインターフェイスを表示します。 |
| Ave Rate | サンプリング期間中の攻撃の平均レートを 1 秒あたりの攻撃数で表示します。 |
| Cur Rate | 現在の攻撃レート（1 秒あたりの攻撃数）を表示します。 |
| Total | 攻撃の合計数を表示します。 |
| Source IP | 攻撃者の IP アドレスを表示します。 |
| Last Attack Time | 最後の攻撃が発生した時間を表示します。 |

次に、**show threat-detection statistics top tcp-intercept long** コマンドの出力例を示します。実際の IP アドレスが括弧内に表示されています

```
> show threat-detection statistics top tcp-intercept long

Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port (Real IP:Real Port)> <Interface> <Ave Rate> <Cur Rate> <Total>
<Source IP (Last Attack Time)>
------------------------------------------------------------------------------
1    10.1.0.2:6025 (209.165.200.227:6025) inside 18 709 33911 10.0.0.201 (0 secs ago)
2    10.1.0.2:6026 (209.165.200.227:6026) inside 18 709 33911 10.0.0.201 (0 secs ago)
3    10.1.0.2:6027 (209.165.200.227:6027) inside 18 709 33911 10.0.0.201 (0 secs ago)
4    10.1.0.2:6028 (209.165.200.227:6028) inside 18 709 33911 10.0.0.201 (0 secs ago)
5    10.1.0.2:6029 (209.165.200.227:6029) inside 18 709 33911 10.0.0.201 (0 secs ago)
6    10.1.0.2:6030 (209.165.200.227:6030) inside 18 709 33911 10.0.0.201 (0 secs ago)
7    10.1.0.2:6031 (209.165.200.227:6031) inside 18 709 33911 10.0.0.201 (0 secs ago)
8    10.1.0.2:6032 (209.165.200.227:6032) inside 18 709 33911 10.0.0.201 (0 secs ago)
9    10.1.0.2:6033 (209.165.200.227:6033) inside 18 709 33911 10.0.0.201 (0 secs ago)
10   10.1.0.2:6034 (209.165.200.227:6034) inside 18 709 33911 10.0.0.201 (0 secs ago)
```

次に、サンプリングデータを表示する **show threat-detection statistics top tcp-intercept detail** コマンドの出力例を示します。サンプリングデータは、30 のサンプリング期間あたりの攻撃数です。

```
> show threat-detection statistics top tcp-intercept detail

Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
 Time)>
------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1877 9502 3379276 <various> Last: 10.0.0.45 (0 secs ago)
     Sampling History (30 Samplings):
             95348      95337      95341      95339      95338      95342
             95337      95348      95342      95338      95339      95340
             95339      95337      95342      95348      95338      95342
             95337      95339      95340      95339      95347      95343
             95337      95338      95342      95338      95337      95342
             95348      95338      95342      95338      95337      95343
             95337      95349      95341      95338      95337      95342
             95338      95339      95338      95350      95339      95570
             96351      96351      96119      95337      95349      95341
             95338      95337      95342      95338      95338      95342
......
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear threat-detection statistics** | 脅威検出の統計情報をクリアします。 |
| **show running-config all threat-detection** | 脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。 |

# show time

デバイスの UTC およびローカルの時刻と日付を表示するには、**show time** コマンドを使用します。

**show time**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.0.1 | このコマンドが導入されました。 |

### 例

次に、**show time** コマンドの出力例を示します。

```
> show time
UTC -       Wed Aug  3 17:04:06 UTC 2016
Localtime - Wed Aug 03 13:04:06 EDT 2016
```

# show time-range

すべての時間範囲オブジェクトの設定を表示するには、**show time-range** コマンドを使用します。

（注） このコマンドは、デバイスの時刻を表示しません。デバイス時刻を表示するには、`show time` を使用します。

**show time-range timezone** ［ *name* ］

## 構文の説明

| | |
|---|---|
| *name* | （オプション）この時間範囲オブジェクトの情報のみを表示します。 |
| **timezone** | 時間範囲ポリシーに設定されたタイムゾーンを表示するには、timezone を使用します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |
| 6.6 | timezone キーワードが追加されました。 |

### 例

次に、時間範囲オブジェクトの設定を表示する例を示します。この例では、work-hours という名前のオブジェクトが 1 つあります。inactive は、オブジェクトが使用されていないことを意味します。

```
> show time-range

time-range entry: work-hours (inactive)
   periodic weekdays 9:00 to 17:00
```

次に、**show time-range timezone** コマンドの出力例を示します。

```
> show time-range timezone
Time-range Clock:
------------------------------
13:20:22.852 tzname Tue Aug 18 2020
```

# show tls-proxy

暗号化された検査の TLS プロキシおよびセッション情報を表示するには、**show tls-proxy** コマンドを使用します。

**show tls-proxy** ［*tls_name* | **session** ［**host** *host_address* | **detail** ［**cert-dump**］ | **count** | **statistics**］］

## 構文の説明

| | |
|---|---|
| **count** | セッション カウンタだけを表示します。 |
| **detail** [**cert-dump**] | 各 SSL レッグおよび LDC の暗号を含む詳細な TLS プロキシ情報を表示します。**cert-dump** キーワードを追加して、ローカルダイナミック証明書（LDC）の 16 進ダンプを取得します。<br>また、これらのキーワードは、**host** オプションとともに使用できます。 |
| **host** *host_address* | 関連付けられたセッションを表示する特定のホストの IPv4 または IPv6 アドレスを指定します。 |
| **session** | アクティブな TLS プロキシ セッションを表示します。 |
| **statistics** | TLS セッションをモニターおよび管理するための統計情報を表示します。 |
| *tls_name* | 表示する TLS プロキシの名前。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

## 使用上のガイドライン

このコマンドで表示できる TLS プロキシは、暗号化されたアプリケーション検査用に設定されているプロキシだけです。プロキシは、SIP、SCCP（Skinny）、または Diameter インスペクションに適用されます。これらの TLS プロキシは、SSL 復号化または VPN ポリシーとは関係ありません。

### 例

次に、**show tls-proxy** コマンドの出力例を示します。

```
> show tls-proxy
TLS-Proxy 'proxy': ref_cnt 1, seq#1
      Server proxy:
             Trust-point: local_ccm
      Client proxy:
             Local dynamic certificate issuer: ldc_signer
             Local dynamic certificate key-pair: phone_common
             Cipher-suite <unconfigured>
```

```
      Run-time proxies:
             Proxy 0x448b468: Class-map: skinny_ssl, Inspect: skinny
                   Active sess 1, most sess 4, byte 3244
```

次に、**show tls-proxy session** コマンドの出力例を示します。

```
> show tls-proxy session
outside 133.9.0.211:51291 inside 195.168.2.200:2443 P:0x4491a60(proxy)
S:0x482e790 byte 3388
```

次に、**show tls-proxy session detail** コマンドの出力例を示します。

```
> show tls-proxy session detail
1 in use, 1 most used
outside 133.9.0.211:50433 inside 195.168.2.200:2443 P:0xcba60b60(proxy) S:0xcbc10748
byte 1831704
      Client: State SSLOK  Cipher AES128-SHA Ch 0xca55efc8 TxQSize 0 LastTxLeft 0 Flags
 0x1
      Server: State SSLOK  Cipher AES128-SHA Ch 0xca55efa8 TxQSize 0 LastTxLeft 0 Flags
 0x9
Local Dynamic Certificate
      Status: Available
      Certificate Serial Number: 29
      Certificate Usage: General Purpose
      Public Key Type: RSA (1024 bits)
      Issuer Name:
             cn=TLS-Proxy-Signer
      Subject Name:
             cn=SEP0002B9EB0AAD
             o=Cisco Systems Inc
             c=US
      Validity Date:
            start date: 00:47:12 PDT Feb 27 2007
            end   date: 00:47:12 PDT Feb 27 2008
      Associated Trustpoints:
```

次に、**show tls-proxy session statistics** コマンドの出力例を示します。

```
> show tls-proxy session stastics
TLS Proxy Sessions (Established: 600)
    Mobility:                                      0
Per-Session Licensed TLS Proxy Sessions
(Established: 222, License Limit: 3000)
    SIP:                                           2
    SCCP:                                         20
    DIAMETER:                                    200
Total TLS Proxy Sessions
    Established:                                 822
    Platform Limit:                             1000
```

# show track

セキュリティレベル合意（SLA）トラッキングプロセスが追跡したオブジェクトに関する情報を表示するには、**show track** コマンドを使用します。

**show track** ［*track-id*］

## 構文の説明

| | |
|---|---|
| *track-id* | トラッキング エントリ オブジェクト ID 番号（1 ~ 500）。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.3 | このコマンドが導入されました。 |

### 例

次に、**show track** コマンドの出力例を示します。

```
> show track

Track 5
      Response Time Reporter 124 reachability
      Reachability is UP
      2 changes, last change 03:41:16
      Latest operation return code: OK
      Tracked by:
                  STATIC-IP-ROUTING 0
```

# show traffic

インターフェイスの送信アクティビティおよび受信アクティビティを表示するには、**show traffic** コマンドを使用します。

**show traffic**

## 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

**show traffic** コマンドは、**show traffic** コマンドが最後に入力された時点またはデバイスがオンラインになった時点以降に、各インターフェイスを通過したパケットの数とバイト数を表示します。秒数は、デバイスが直前のリブート以降、オンラインになってからの経過時間です（直前のリブート以降に **clear traffic** コマンドが入力されていない場合）。コマンドが入力されていた場合は、コマンドが入力された時点からの経過時間となります。

統計情報は、インターフェイス名に基づいて最初に表示されます。名前付きインターフェイスの後に、物理インターフェイスに基づいて統計情報が表示されます。インターフェイスには、システムが内部通信に使用する非表示の仮想インターフェイスが含まれることがあります。

### 例

次に、単体のインターフェイスの統計情報を示す**show traffic**コマンドの省略された出力例を示します。各インターフェイスは同じ統計情報を表示します。

```
> show traffic
...
diagnostic:
        received (in 102.080 secs):
                2048 packets     204295 bytes
                20 pkts/sec      2001 bytes/sec
        transmitted (in 102.080 secs):
                2048 packets       204056 bytes
                20 pkts/sec      1998 bytes/sec
      1 minute input rate 122880 pkts/sec,  5775360 bytes/sec
      1 minute output rate 122887 pkts/sec,  5775389 bytes/sec
      1 minute drop rate, 3 pkts/sec
      5 minute input rate 118347 pkts/sec,  5562309 bytes/sec
      5 minute output rate 119221 pkts/sec,  5603387 bytes/sec
      5 minute drop rate, 11 pkts/sec
...
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear traffic** | 送信アクティビティと受信アクティビティのカウンタをリセットします。 |

# show upgrade

システムソフトウェアのアップグレードに関する情報を表示するには、**show upgrade** コマンドを使用します。

**show upgrade** { **revert-info** | **status** [ **detail** ] [ **continuous** ] }

## 構文の説明

| | |
|---|---|
| **revert-info** | 使用可能なバージョンがある場合は、復元して使用できるシステムのバージョンを表示します。使用可能な復元バージョンがない場合は、**upgrade revert** コマンドを使用できません。 |
| **status** | アップグレードのステータスを表示します。次のオプションキーワードを含めることができます。<br>• **detail**<br>ステータス情報の概要に加えて、アップグレードログを表示します。<br>• **continuous**<br>生成されたアップグレードメッセージを表示します。このキーワードは単独で使用することもできますが、detail キーワードと組み合わせて使用することもできます。 |

## 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。 |

## 使用上のガイドライン

ステータスには以下が含まれることがあります。

- 進行中のアップグレードはありません。
- メジャーアップグレードが進行中です。
- パッチアップグレードが進行中です。
- ホットフィックス アップグレードが進行中です。
- メジャーアップグレードに失敗しました。「cancel」を実行して回復します。

  リブートは、アップグレード失敗の段階によって発生する場合と発生しない場合があります。
- メジャーアップグレードに失敗しました。デバイスをリブートして回復します。

### 例

次の例は、現在進行中のアップグレードのステータスを示しています。完了したアップグレードのステータスを表示するには、**show last-upgrade status** コマンドを使用します。

```
> show upgrade status
Upgrade from 6.3.0 to 6.7.0 in progress (11% progress, time remaining 8 mins)
Time started: Tue Dec  3 23:50:31 UTC 2020
Current state: Tue Dec  3 23:51:01 UTC 2020 Running script 200_pre/001_check_reg.pl...
```

次の例は、復元に関する情報を示しています。この例では、復元できるバージョンが存在します。使用可能なバージョンがない場合、「No version is available for revert」というメッセージが表示されます。

```
> show upgrade revert-info
You can revert to version 6.4.0-102
at 2020-03-20T22:49:43+0000

It uses 4946MB of disk space.

Version 6.4.0-102 is available for revert.
```

## 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。 |
| **upgrade** | システム ソフトウェア アップグレードをキャンセル、復元、または再試行します。 |

# show user

デバイスのコマンドラインインターフェイス（CLI）にアクセスするためのユーザーアカウントを表示するには、**show user** コマンドを使用します。

**show user** ［*username1* ［*usernam2*］［...］］

## 構文の説明

| | |
|---|---|
| *username1* [*usernam2*] [...] | （オプション）1 つ以上のスペースで区切られたユーザー名。名前を指定しない場合は、すべてのユーザーが表示されます。 |

## 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

ユーザーごとに次の情報が表示されます。**configure user add** コマンドを使用してユーザーアカウントを作成します。

- Login：ログイン名。
- UID：ユーザー ID（数字）。
- Auth：ユーザーの認証方法。Local と Remote（ディレクトリサーバー経由）のいずれか。
- Access：ユーザーの権限レベル。Basic と Config のいずれか。この設定を変更するには、**configure user access** コマンドを使用します。
- Enabled：ユーザーがアクティブかどうか。Enabled と Disabled のいずれか。この設定を変更するには、**configure user enable**/**disable** コマンドを使用します。
- Reset：ユーザーが次回ログイン時にアカウントパスワードを変更する必要があるかどうか。Yes と No のいずれか。この設定を変更するには、**configure user forcereset** コマンドを使用します。
- Exp：ユーザーのパスワード変更が必要になるまでの日数。Never は、パスワードが期限切れにならないことを示します。この設定を変更するには、**configure user aging** コマンドを使用します。
- Warn：パスワードの有効期限が切れる前に、ユーザーがパスワードの変更を警告される日数。N/A は、警告が適用されないことを示します。この設定を変更するには、**configure user aging** コマンドを使用します。
- Grace：猶予期間。期限が切れた後にユーザーがパスワードを変更できる日数です。Disabled は猶予期間がないことを意味します。猶予期間は、FXOS を実行しているデバイスにのみ適用されます。この設定を変更するには、**configure user aging** コマンドを使用します。
- Str：ユーザーのパスワードが強度チェックの基準を満たす必要があるかどうか。Dis（無効）と Ena（有効）のいずれか。このオプションを設定するには、**configure user strengthcheck** コマンドを使用します。

- Lock：ログインの失敗が多すぎた場合に、ユーザーのアカウントをロックするかどうか。ユーザーアカウントのロックを解除するには、**configure user unlock** コマンドを使用します。
- Max：ユーザーのアカウントがロックされる前に許容されるログイン失敗の最大回数。N/A は、アカウントをロックできないことを示します。この設定を変更するには、configure user maxfailedlogins コマンドを使用します。

### 例

次に、CLI アクセス用に定義されたユーザーを表示する例を示します。

```
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
admin2            1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

次に、外部ユーザーと猶予期間を含める例を示します。

```
> show user
Login          UID   Auth Access  Enabled Reset   Exp   Warn    Grace  MinL Str Lock Max
admin          100  Local Config  Enabled    No  10000     7  Disabled    8 Ena   No N/A
extuser        501 Remote Config Disabled   N/A  99999     7  Disabled    1 Dis   No N/A
joeuser       1000  Local Config  Enabled   Yes    180     7         7    8 Dis   No
5
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **configure user add** | CLI アクセス用のユーザーアカウントを追加します。 |

# show version

ハードウェアモデル、ソフトウェアバージョン、UUID、侵入ルール更新バージョン、および VDB バージョンを表示するには、**show version** コマンドを使用します。

**show version** ［**detail** | **system**］

## 構文の説明

| | |
|---|---|
| **detail** | **show version** と **show version detail** は同じ情報を表示します。 |
| **system** | このキーワードは、**show version** によって表示される情報に付加的なシステム情報を追加します。 |

## 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。 |
| 7.1 | システムの起動（ブート）にかかった時間に関する情報が出力に追加されました。 |

## 使用上のガイドライン

**show version** コマンドと **show version detail** コマンドは、同じ基本的なシステム情報を表示します。**show version system** コマンドは、この情報に加えて、最後のリブート以降の動作時間やより具体的なハードウェア情報などの付加的なシステム情報を表示します。

### 例

次の例は、基本的な **show version** の出力を示しています。

```
> show version
-------------------[ firepower ]---------------------
Model : Secure Firewall Management Center for VMware (66) Version 7.2.0 (Build 1405)
UUID : 78ddf634-3754-11ec-87dd-ace5f9ec4cdc
Rules update version : 2022-01-11-001-vrt
LSP version : lsp-rel-20220111-1030
VDB version : 348
-----------------------------------------------------
```

**show version system** コマンドの次の出力例では、**show version** コマンドと同じ出力に付加的な情報が追加されています。

```
> show version system
-------------[ example-sfr.example.com ]--------------
Model                     : Cisco ASA5508-X Threat Defense (75) Version 6.1.0 (Build
226)
UUID                      : 43235986-2363-11e6-b278-aff0a43948fe
Rules update version      : 2016-03-28-001-vrt
VDB version               : 270
-----------------------------------------------------

Cisco Adaptive Security Appliance Software Version 9.6(1)72
```

```
Compiled on Fri 20-May-16 13:36 PDT by builders
System image file is "disk0:/os.img"
Config file at boot was "startup-config"

firepower up 36 days 21 hours

Hardware:   ASA5508, 8192 MB RAM, CPU Atom C2000 series 2000 MHz, 1 CPU (8 cores
)
Internal ATA Compact Flash, 8192MB
BIOS Flash M25P64 @ 0xfed01000, 16384KB

Encryption hardware device : Cisco ASA Crypto on-board accelerator (revision 0x1
)
                             Number of accelerators: 1

 1: Ext: GigabitEthernet1/1  : address is e865.49b8.97f2, irq 255
 2: Ext: GigabitEthernet1/2  : address is e865.49b8.97f3, irq 255
 3: Ext: GigabitEthernet1/3  : address is e865.49b8.97f4, irq 255
 4: Ext: GigabitEthernet1/4  : address is e865.49b8.97f5, irq 255
 5: Ext: GigabitEthernet1/5  : address is e865.49b8.97f6, irq 255
 6: Ext: GigabitEthernet1/6  : address is e865.49b8.97f7, irq 255
 7: Ext: GigabitEthernet1/7  : address is e865.49b8.97f8, irq 255
 8: Ext: GigabitEthernet1/8  : address is e865.49b8.97f9, irq 255
 9: Int: Internal-Data1/1    : address is e865.49b8.97f1, irq 255
10: Int: Internal-Data1/2    : address is 0000.0001.0002, irq 0
11: Int: Internal-Control1/1 : address is 0000.0001.0001, irq 0
12: Int: Internal-Data1/3    : address is 0000.0001.0003, irq 0
13: Ext: Management1/1       : address is e865.49b8.97f1, irq 0
14: Int: Internal-Data1/4    : address is 0000.0100.0001, irq 0

Serial Number: JAD192100RG
Configuration register is 0x1
Image type                : Release
Key Version               : A
Configuration last modified by enable_1 at 12:44:37.849 UTC Mon Jul 25 2016
```

バージョン 7.1 以降では、システムの起動にかかった時間を確認できます。この情報は、システムの稼働時間のステータスの後に表示されます。

```
> show version system
---------------------[ ftdv1 ]----------------------
Model                     : Cisco Firepower Threat Defense for VMware (75) Version 7.1.0
 (Build 1519)
UUID                       : b964ed5e-92c0-11eb-aaa2-cfab359c2436
LSP version                : lsp-rel-20210310-2255
VDB version                : 338
----------------------------------------------------

Cisco Adaptive Security Appliance Software Version 99.17(1)135
SSP Operating System Version 82.11(1.277i)

Compiled on Thu 25-Mar-21 00:49 GMT by builders
System image file is "boot:/asa99171-135-smp-k8.bin"
Config file at boot was "startup-config"

ftdv1 up 6 days 22 hours
Start-up time 5 secs

(remaining output redacted)
```

# show vlan

脅威に対する防御 デバイスに設定されているすべての VLAN を表示するには、**show vlan** コマンドを使用します。

**show vlan** ［**mapping** ［*primary_id*］］

## 構文の説明

| | |
|---|---|
| **mapping** | （オプション）プライマリ VLAN にマッピングされたセカンダリ VLAN を表示します。 |
| *primary_id* | （オプション）特定のプライマリ VLAN のセカンダリ VLAN を表示します。 |

## 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、設定されている VLAN を表示する例を示します。

```
> show vlan
10-11,30,40,300
```

次に、各プライマリ VLAN にマッピングされたセカンダリ VLAN を表示する例を示します。

```
> show vlan mapping
Interface                       Secondary VLAN ID                       Mapped VLAN
ID
0/1.100                         200                                             300
0/1.100                         201                                             300
0/2.500                         400                                             200
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear interface** | **show interface** コマンドのカウンタをクリアします。 |
| **show interface** | インターフェイスの実行時ステータスと統計情報を表示します。 |

# show vm

Threat Defense Virtual デバイス上の仮想プラットフォーム情報を表示するには、**show vm** コマンドを使用します。

**show vm**

## 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、VMware についての情報を表示する例を示します。

```
> show vm

Virtual Platform Resource Status
--------------------------------
Number of vCPUs           :  4
Processor Memory          :  8192 MB
Hypervisor                :  VMware
```

# show vpdn

PPPoE または L2TP のような仮想プライベート ダイヤルアップ ネットワーク（VPDN）接続のステータスを表示するには、**show vpdn** コマンドを使用します。

**show vpdn** {**group** *name* | **pppinterface id** *number* | **session** {**l2tp** | **pppoe**} **id** *number* {**packets** | **state** | **window**} | **tunnel** {**l2tp** | **pppoe**} **id** *number* {**packets** | **state** | **summary** | **transport**} | **username** *name*}

## 構文の説明

| | |
|---|---|
| **group** *name* | VPDN グループのコンフィギュレーションを表示します。 |
| **id** *number* | （オプション）指定された ID を持つ VPDN セッションに関する情報を表示します。 |
| **l2tp** | （オプション）L2TP に関するセッションまたはトンネルの情報を表示します。 |
| **packets** | セッションまたはトンネル パケットの情報を表示します。 |
| **pppinterface** | PPP インターフェイス情報を表示します。 |
| **pppoe** | （オプション）PPPoE に関するセッションまたはトンネルの情報を表示します。 |
| **session** | セッション情報を表示します。 |
| **state** | セッションまたはトンネルの状態の情報を表示します。 |
| **summary** | トンネルの概要を表示します。 |
| **transport** | トンネルのトランスポート情報を表示します。 |
| **tunnel** | トンネル情報を表示します。 |
| **username** *name* | ユーザー情報を表示します。 |
| **window** | セッション ウィンドウ情報を表示します。 |

## 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

VPDN PPPoE 接続または L2TP 接続をトラブルシューティングするには、このコマンドを使用します。

### 例

次に、**show vpdn session** コマンドの出力例を示します。

```
> show vpdn session
PPPoE Session Information (Total tunnels=1 sessions=1)
Remote Internet Address is 10.0.0.1
  Session state is SESSION_UP
    Time since event change 65887 secs, interface outside
    PPP interface id is 1
    6 packets sent, 6 received, 84 bytes sent, 0 received
```

次に、**show vpdn tunnel** コマンドの出力例を示します。

```
> show vpdn tunnel
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 0, 1 active sessions
   time since change 65901 secs
   Remote Internet Address 10.0.0.1
   Local Internet Address 199.99.99.3
```

# show vpn load-balancing

このコマンドは使用しないでください。脅威に対する防御でサポートされていない機能に関連しています。

# show vpn-sessiondb

VPNセッションに関する情報を表示するには、いずれかの**show vpn-sessiondb**コマンドを使用します。

**show vpn-sessiondb** ［**detail**］［**full**］｛**anyconnect** | **l2l** | **ra-ikev1-ipsec** | **ra-ikev2-ipsec**｝［**filter** *criteria*］［**sort** *criteria*］
**show vpn-sessiondb** ［**detail**］［**full**］ **index** *index-number*
**show vpn-sessiondb failover**
**show vpn-sessiondb ospfv3** ［**filter ipaddress** *IP_address*］［**sort ipaddress**］

## 構文の説明

| | |
|---|---|
| **anyconnect** | AnyConnect VPN クライアントセッションを表示します。 |
| **detail** | （任意）セッションに関する詳細情報を表示します。たとえば、IPsecセッションに対して detail オプションを使用すると、IKE ハッシュ アルゴリズム、認証モード、キー再生成間隔などの詳細情報が表示されます。<br>detail および full オプションを指定すると、脅威に対する防御 デバイスはマシンで読み取り可能な形式で詳細な出力を表示します。 |
| **failover** | フェールオーバー IPSec トンネルのセッション情報を表示します。 |
| **filter** *filter_criteria* | （任意）指定したフィルタオプションに従って、出力をフィルタ処理します。オプションのリストについては、「使用上のガイドライン」を参照してください。 |
| **full** | （任意）連続した、短縮されていない出力を表示します。出力のレコード間には \| 文字と \|\| ストリングが表示されます。 |
| **index** *indexnumber* | インデックス番号を指定して、単一のセッションを表示します。セッションのインデックス番号を指定します。範囲は 1 ～ 65535 です。 |
| **l2l** | VPN の LAN-to-LAN セッション情報を表示します。 |
| **ospfv3** | OSPFv3 セッション情報を表示します。 |
| **ra-ikev1-ipsec** | IPsec IKEv1 セッションを表示します。 |
| **ra-ikev2-ipsec** | IKEv2 リモート アクセス クライアント接続の詳細を表示します。 |
| **sort** *sort_criteria* | （任意）指定するソート オプションに従って出力をソートします。オプションのリストについては、「使用上のガイドライン」を参照してください。 |

## 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

次のオプションを使用して、セッションに関する表示内容をフィルタ処理およびソートできます。フィルタ処理およびソートできる値は、リストするセッションタイプによって異なります。

| フィルタ/ソート オプション | 説明 |
|---|---|
| **filter a-ipaddress** *IP_address* | 出力をフィルタリングして、指定した割り当て済み IP アドレス（複数可）に関する情報だけを表示します。<br>次と併用：**anyconnect**、**ra-ikev2-ipsec** |
| **sort a-ipaddress** | 割り当て済み IP アドレスで表示内容をソートします。<br>次と併用：**anyconnect**、**ra-ikev2-ipsec** |
| **filter a-ipversion** {**v4** \| **v6**} | IPv4 または IPv6 アドレスが割り当てられたセッションのみを表示するように出力をフィルタ処理します。<br>使用対象：**anyconnect**、**ra-ikev2-ipsec** |
| **filter encryption** *encryption_algorithm* | 出力をフィルタ処理して、指定した暗号化アルゴリズムを使用しているセッションに関する情報のみを表示します。使用可能なメソッドを確認するには、? を使用します。<br>次と併用：**anyconnect**、**l2l**、**ra-ikev2-ipsec** |
| **sort encryption** | セッションで使用される暗号化アルゴリズムで出力をソートします。<br>次と併用：**anyconnect**、**l2l**、**ra-ikev2-ipsec** |
| **filter inactive** | アイドル状態であり、（ハイバネーション、モバイルデバイス切断などによって）接続が切断された可能性がある非アクティブなセッションをフィルタ処理します。TCP キープアライブが AnyConnect クライアントからの応答なしで 脅威に対する防御 デバイスから送信されると、非アクティブなセッションの数が増加します。各セッションには、SSL トンネルがドロップした時間でタイムスタンプが付けられます。セッションが SSL トンネルを介してアクティブにトラフィックを渡している場合、00:00m:00s が表示されます。<br>次と併用： **anyconnect**<br>（注） 脅威に対する防御 デバイスは、バッテリ寿命を節約するために一部のデバイス（iPhone、iPad、iPod など）に TCP キープアライブを送信しないため、障害検出で切断とスリープが区別されません。そのため、非アクティブなカウンタは設計によって 00:00:00 のままになります。 |
| **sort inactivity** | 非アクティブなセッションでソートします。<br>次と併用： **anyconnect** |

| フィルタ/ソート オプション | 説明 |
|---|---|
| **filter ipaddress** *IP_address* | 出力をフィルタリングして、指定した内部 IP アドレス（複数可）に関する情報だけを表示します。<br>次と併用：**l2l**、**ospfv3** |
| **sort ipaddress** | 内部 IP アドレスで表示内容をソートします。<br>次と併用：**l2l**、**ospfv3** |
| **filter ipversion** {**v4** \| **v6**} | 出力をフィルタ処理して、IPv4 または IPv6 アドレスを割り当てられたエンドポイントから開始されるセッションのみを表示します。<br>次と併用： **l2l** |
| **filter name** *username* | 出力をフィルタ処理して、指定したユーザー名のセッションを表示します。<br>次と併用：**anyconnect**、**l2l**、**ra-ikev2-ipsec** |
| **sort name** | ユーザー名のアルファベット順に表示内容をソートします。<br>次と併用：**anyconnect**、**l2l**、**ra-ikev2-ipsec** |
| **filter p-ipaddress** *IP_address* | 出力をフィルタ処理して、指定したパブリック外部 IP アドレスに関する情報のみを表示します。<br>次と併用：**anyconnect**、**ra-ikev2-ipsec** |
| **sort p-ipaddress** | パブリック外部 IPアドレスで表示内容をソートします。<br>次と併用：**anyconnect**、**ra-ikev2-ipsec** |
| **filter p-ipversion** {**v4** \| **v6**} | 出力をフィルタ処理して、パブリック IPv4 または IPv6 アドレスを割り当てられたエンドポイントから開始されるセッションのみを表示します。<br>次と併用：**anyconnect**、**ra-ikev2-ipsec** |
| **filter protocol** *name* | 出力をフィルタ処理して、指定したプロトコルを使用しているセッションに関する情報のみを表示します。使用可能なプロトコルを確認するには、**?** を使用します。<br>次と併用：**anyconnect**、**l2l**、**ra-ikev2-ipsec** |
| **sort protocol** | プロトコルで表示内容をソートします。<br>次と併用：**anyconnect**、**l2l**、**ra-ikev2-ipsec** |

次の表で、出力に表示される可能性のあるフィールドについて説明します。

| フィールド | 説明 |
|---|---|
| Auth Mode | このセッションを認証するためのプロトコルまたはモード。 |
| Bytes Rx | システムがリモートのピアまたはクライアントから受信した合計バイト数。 |
| Bytes Tx | システムがリモートのピアまたはクライアントに送信した合計バイト数。 |
| クライアント タイプ | リモート ピア上で実行されるクライアント ソフトウェア（利用できる場合）。 |
| Client Ver | リモート ピア上で実行されるクライアント ソフトウェアのバージョン。 |
| Connection | 接続名またはプライベート IP アドレス。 |
| D/H Group | Diffie-Hellman グループ。IPsec SA 暗号キーを生成するためのアルゴリズムおよびキー サイズ。 |
| 持続時間 | セッションのログイン時刻から直前の画面リフレッシュまでの経過時間（HH:MM:SS）。 |
| EAPoUDP Session Age | 正常に完了した直前のポスチャ確認からの経過秒数。 |
| カプセル化 | IPsec ESP（暗号ペイロード プロトコル）の暗号化と認証（つまり、ESP を適用した元の IP パケットの一部）を適用するためのモード。 |
| 暗号化 | このセッションが使用しているデータ暗号化アルゴリズム（ある場合）。 |
| EoU Age (T) | EAPoUDP セッションの経過時間。正常に完了した直前のポスチャ確認からの経過秒数。 |
| Filter Name | セッション情報の表示を制限するよう指定されたユーザー名。 |
| ハッシュ | パケットのハッシュを生成するためのアルゴリズム。IPsec データ認証に使用されます。 |
| Hold Left (T) | Hold-Off Time Remaining。直前のポスチャ確認が正常に完了した場合は、0 秒です。それ以外の場合は、次回のポスチャ確認試行までの秒数です。 |
| Hold-Off Time Remaining | 直前のポスチャ確認が正常に完了した場合は、0 秒です。それ以外の場合は、次回のポスチャ確認試行までの秒数です。 |
| IKE Neg Mode | キー情報を交換し、SA を設定するための IKE（IPsec フェーズ 1）モード（アグレッシブまたはメイン）。 |

| フィールド | 説明 |
|---|---|
| IKE Sessions | IKE（IPsec フェーズ 1）セッションの数で、通常は 1。これらのセッションにより、IPsec トラフィックのトンネルが確立されます。 |
| 索引 | このレコードの固有識別情報。 |
| IP Addr | このセッションのリモート クライアントに割り当てられたプライベート IP アドレス。このアドレスは、「内部」または「仮想」IP アドレスとも呼ばれています。このアドレスを使用すると、クライアントはプライベート ネットワーク内のホストと見なされます。 |
| IPsec Sessions | IPsec（フェーズ 2）セッション（トンネル経由のデータ トラフィック セッション）の数。各 IPsec リモート アクセス セッションには、2 つの IPsec セッションがあります。1 つはトンネル エンドポイントで構成されるセッション、もう 1 つはトンネル経由で到達可能なプライベート ネットワークで構成されるセッションです。 |
| ライセンス情報 | 共有 SSL VPN ライセンスに関する情報を表示します。 |
| Local IP Addr | トンネルのローカルエンドポイント（システム上のインターフェイス）に割り当てられた IP アドレス。 |
| Login Time | セッションにログインした日時（MMM DD HH:MM:SS）。時刻は 24 時間表記で表示されます。 |
| NAC Result | ネットワーク アドミッション コントロール ポスチャ検証の状態。次のいずれかを指定できます。<br>• [Accepted]：ACS は正常にリモート ホストのポスチャを検証しました。<br>• [Rejected]：ACS はリモート ホストのポスチャの検証に失敗しました。<br>• [Exempted]：脅威に対する防御 デバイスに設定されたポスチャ検証免除リストに従って、リモートホストはポスチャの検証を免除されています。<br>• [Non-Responsive]：リモート ホストは EAPoUDP Hello メッセージに応答しませんでした。<br>• [Hold-off]：ポスチャ検証に成功した後、脅威に対する防御 デバイスとリモートホストの EAPoUDP 通信が切断されました。<br>• [N/A]：VPN NAC グループ ポリシーに従い、リモート ホストの NAC はディセーブルにされています。<br>• [Unknown]：ポスチャ検証が進行中です。 |

| フィールド | 説明 |
|---|---|
| NAC Sessions | ネットワーク アドミッション コントロール（EAPoUDP）セッションの数。 |
| Packets Rx | システムがリモートピアから受信したパケット数。 |
| Packets Tx | システムがリモートピアに送信したパケット数。 |
| PFS Group | 完全転送秘密グループ番号。 |
| Posture Token | Access Control Server 上で設定可能な情報テキスト ストリング。ACS は、情報提供のためにシステムにポスチャトークンをダウンロードして、システムモニタリング、レポート、デバッグ、およびロギングを支援します。一般的なポスチャ トークンは、Healthy、Checkup、Quarantine、Infected、または Unknown です。 |
| Protocol | セッションが使用しているプロトコル。 |
| Public IP | クライアントに割り当てられた、公開されているルーティング可能な IP アドレス。 |
| リダイレクト URL | ポスチャ検証またはクライアントレス認証に続いて、ACS はセッションのアクセスポリシーをシステムにダウンロードします。Redirect URL は、アクセス ポリシー ペイロードのオプションの一部です。システムは、リモートホストのすべての HTTP（ポート 80）要求および HTTPS（ポート 443）要求を Redirect URL（存在する場合）にリダイレクトします。アクセスポリシーに Redirect URL が含まれていない場合、脅威に対する防御 デバイスはリモートホストからの HTTP 要求および HTTPS 要求をリダイレクトしません。<br><br>Redirect URL は、IPsec セッションが終了するか、ポスチャ再検証が実行されるまで有効です。ACS は、異なる Redirect URL が含まれるか、Redirect URL が含まれない新しいアクセス ポリシーをダウンロードします。 |
| Rekey Int（T または D） | IPsec（IKE）SA 暗号キーの有効期限。T 値は時間でのライフタイム、D 値は送信済みデータでのライフタイムです。リモート アクセス VPN では T 値のみが表示されます。 |
| Rekey Left（T または D） | IPsec（IKE）SA 暗号キーの残りのライフタイム。T 値は時間でのライフタイム、D 値は送信済みデータでのライフタイムです。リモート アクセス VPN では T 値のみが表示されます。 |
| Rekey Time Interval | IPsec（IKE）SA 暗号キーの有効期限。 |
| Remote IP Addr | トンネルのリモート エンドポイント（リモート ピア上のインターフェイス）に割り当てられた IP アドレス。 |

| フィールド | 説明 |
|---|---|
| Reval Int (T) | Revalidation Time Interval。正常に完了した各ポスチャ確認間に、設ける必要のある間隔（秒単位）。 |
| Reval Left (T) | Time Until Next Revalidation。直前のポスチャ確認試行が正常に完了しなかった場合は 0 です。それ以外の場合は、Revalidation Time Interval と、正常に完了した直前のポスチャ確認からの経過秒数との差です。 |
| Revalidation Time Interval | 正常に完了した各ポスチャ確認間に、設ける必要のある間隔（秒単位）。 |
| Session ID | セッション コンポーネント（サブセッション）の ID。各 SA には独自の ID があります。 |
| Session Type | セッションのタイプ（LAN-to-LAN または Remote）。 |
| SQ Int (T) | Status Query Time Interval。正常に完了した各ポスチャ確認またはステータス クエリー応答から、次回のステータス クエリー応答までの間に空けることができる秒数です。ステータスクエリーは、直前のポスチャ確認以降にホストでポスチャが変化したかどうかを確認するために、システムがリモートホストに発行する要求です。 |
| Status Query Time Interval | 正常に完了した各ポスチャ確認またはステータス クエリー応答から、次回のステータス クエリー応答までの間に空けることができる秒数です。ステータスクエリーは、直前のポスチャ確認以降にホストでポスチャが変化したかどうかを確認するために、システムがリモートホストに発行する要求です。 |
| Time Until Next Revalidation | 直前のポスチャ確認試行が正常に完了しなかった場合は 0 です。それ以外の場合は、Revalidation Time Interval と、正常に完了した直前のポスチャ確認からの経過秒数との差です。 |
| Tunnel Group | 属性値を求めるために、このトンネルが参照するトンネル グループの名前。 |
| UDP Dst Port<br>または<br>UDP Destination Port | リモート ピアが使用する UDP のポート番号。 |
| UDP Src Port<br>または<br>UDP Source Port | UDP 用に使用されるポート番号。 |
| Username | セッションを確立したユーザーのログイン名。 |

| フィールド | 説明 |
|---|---|
| VLAN | このセッションに割り当てられた出力 VLAN インターフェイス。システムは、すべてのトラフィックをこの VLAN に転送します。グループポリシーまたは継承されたグループポリシーのいずれかによって値が指定されます。 |

## 例

次に、**show vpn-sessiondb** コマンドの出力例を示します。

```
> show vpn-sessiondb
--------------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------------
                             Active : Cumulative : Peak Concur : Inactive
                            ------------------------------------------------
AnyConnect Client           :      1 :         12 :           3 :        0
  SSL/TLS/DTLS              :      1 :         12 :           3 :        0
Clientless VPN              :      0 :          6 :           2
  Browser                   :      0 :          6 :           2
--------------------------------------------------------------------------------
Total Active and Inactive   :      1            Total Cumulative :     18
Device Total VPN Capacity   :    250
Device Load                 :     0%
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Tunnels Summary
--------------------------------------------------------------------------------
                             Active : Cumulative : Peak Concurrent
                            ------------------------------------------------
Clientless                  :      0 :          7 :               2
AnyConnect-Parent           :      1 :         11 :               3
SSL-Tunnel                  :      1 :         12 :               3
DTLS-Tunnel                 :      1 :         12 :               3
--------------------------------------------------------------------------------
Totals                      :      3 :         42
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
IPv6 Usage Summary
--------------------------------------------------------------------------------
Active : Cumulative : Peak Concurrent
-------------------------------------------
AnyConnect SSL/TLS/DTLS : : :
IPv6 Peer : 1 : 41 : 2
Tunneled IPv6 : 1 : 70 : 2
AnyConnect IKEv2 : : :
IPv6 Peer : 0 : 4 : 1
Clientless : : :
IPv6 Peer : 0 : 1 : 1
--------------------------------------------------------------------------------
```

次に、**show vpn-sessiondb detail** コマンドの出力例を示します。

```
> show vpn-sessiondb detail
--------------------------------------------------------------------------------
```

```
VPN Session Summary
------------------------------------------------------------------------------
                             Active : Cumulative : Peak Concur : Inactive
                            ----------------------------------------------
AnyConnect Client           :      1 :         12 :           3 :        0
  SSL/TLS/DTLS              :      1 :         12 :           3 :        0
Clientless VPN              :      0 :          6 :           2
  Browser                   :      0 :          6 :           2
------------------------------------------------------------------------------
Total Active and Inactive   :      1             Total Cumulative :     18
Device Total VPN Capacity   :    250
Device Load                 :     0%
------------------------------------------------------------------------------

------------------------------------------------------------------------------
Tunnels Summary
------------------------------------------------------------------------------
                             Active : Cumulative : Peak Concurrent
                            ----------------------------------------------
Clientless                  :      0 :          7 :               2
AnyConnect-Parent           :      1 :         11 :               3
SSL-Tunnel                  :      1 :         12 :               3
DTLS-Tunnel                 :      1 :         12 :               3
------------------------------------------------------------------------------
Totals                      :      3 :         42
------------------------------------------------------------------------------
```

次に、**show vpn-sessiondb detail l2l** コマンドの出力例を示します。

```
> show vpn-sessiondb detail l2l
Session Type: LAN-to-LAN Detailed

Connection : 172.16.0.0
Index : 1
IP Addr : 172.16.0.0
Protocol : IKEv2 IPsec
Encryption : IKEv2: (1)AES256 IPsec: (1)AES256
Hashing : IKEv2: (1)SHA1 IPsec: (1)SHA1
Bytes Tx : 240 Bytes Rx : 160
Login Time : 14:50:35 UTC Tue May 1 2017
Duration : 0h:00m:11s
IKEv2 Tunnels: 1
IPsec Tunnels: 1

IKEv2:
Tunnel ID : 1.1
UDP Src Port : 500 UDP Dst Port : 500
Rem Auth Mode: preSharedKeys
Loc Auth Mode: preSharedKeys
Encryption : AES256 Hashing : SHA1
Rekey Int (T): 86400 Seconds Rekey Left(T): 86389 Seconds
PRF : SHA1 D/H Group : 5
Filter Name :
IPv6 Filter :

IPsec:
Tunnel ID : 1.2
Local Addr : 10.0.0.0/255.255.255.0
Remote Addr : 209.165.201.30/255.255.255.0
Encryption : AES256 Hashing : SHA1
Encapsulation: Tunnel PFS Group : 5
Rekey Int (T): 120 Seconds Rekey Left(T): 107 Seconds
```

```
Rekey Int (D): 4608000 K-Bytes Rekey Left(D): 4608000 K-Bytes
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Bytes Tx : 240 Bytes Rx : 160
Pkts Tx : 3 Pkts Rx : 2

NAC:
Reval Int (T): 0 Seconds Reval Left(T): 0 Seconds
SQ Int (T) : 0 Seconds EoU Age(T) : 13 Seconds
Hold Left (T): 0 Seconds Posture Token:
Redirect URL :
```

次に、**show vpn-sessiondb detail index 1** コマンドの出力例を示します。

```
> show vpn-sessiondb detail index 1

Session Type: Remote Detailed

Username : user1
Index : 1
Assigned IP : 192.168.2.70 Public IP : 10.86.5.114
Protocol : IPsec Encryption : AES128
Hashing : SHA1
Bytes Tx : 0 Bytes Rx : 604533
Client Type : WinNT Client Ver : 4.6.00.0049
Tunnel Group : bxbvpnlab
Login Time : 15:22:46 EDT Tue May 10 2005
Duration : 7h:02m:03s
Filter Name :
NAC Result : Accepted
Posture Token: Healthy
VM Result : Static
VLAN : 10

IKE Sessions: 1 IPsec Sessions: 1 NAC Sessions: 1

IKE:
Session ID : 1
UDP Src Port : 500 UDP Dst Port : 500
IKE Neg Mode : Aggressive Auth Mode : preSharedKeysXauth
Encryption : 3DES Hashing : MD5
Rekey Int (T): 86400 Seconds Rekey Left(T): 61078 Seconds
D/H Group : 2

IPsec:
Session ID : 2
Local Addr : 0.0.0.0
Remote Addr : 192.168.2.70
Encryption : AES128 Hashing : SHA1
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds Rekey Left(T): 26531 Seconds
Bytes Tx : 0 Bytes Rx : 604533
Pkts Tx : 0 Pkts Rx : 8126

NAC:
Reval Int (T): 3000 Seconds Reval Left(T): 286 Seconds
SQ Int (T) : 600 Seconds EoU Age (T) : 2714 Seconds
Hold Left (T): 0 Seconds Posture Token: Healthy
Redirect URL : www.cisco.com
```

次に、**show vpn-sessiondb ospfv3** コマンドの出力例を示します。

```
> show vpn-sessiondb ospfv3

Session Type: OSPFv3 IPsec

Connection :
Index : 1 IP Addr : 0.0.0.0
Protocol : IPsec
Encryption : IPsec: (1)none Hashing : IPsec: (1)SHA1
Bytes Tx : 0 Bytes Rx : 0
Login Time : 15:06:41 EST Wed Feb 1 2017
Duration : 1d 5h:13m:11s
```

次に、**show vpn-sessiondb detail ospfv3** コマンドの出力例を示します。

```
> show vpn-sessiondb detail ospfv3

Session Type: OSPFv3 IPsec Detailed

Connection :
Index : 1 IP Addr : 0.0.0.0
Protocol : IPsec
Encryption : IPsec: (1)none Hashing : IPsec: (1)SHA1
Bytes Tx : 0 Bytes Rx : 0
Login Time : 15:06:41 EST Wed Feb 1 2017
Duration : 1d 5h:14m:28s
IPsec Tunnels: 1

IPsec:
Tunnel ID : 1.1
Local Addr : ::/0/89/0
Remote Addr : ::/0/89/0
Encryption : none Hashing : SHA1
Encapsulation: Transport
Idle Time Out: 0 Minutes Idle TO Left : 0 Minutes
Bytes Tx : 0 Bytes Rx : 0
Pkts Tx : 0 Pkts Rx : 0
NAC:
Reval Int (T): 0 Seconds Reval Left(T): 0 Seconds
SQ Int (T) : 0 Seconds EoU Age(T) : 105268 Seconds
Hold Left (T): 0 Seconds Posture Token:
Redirect URL :
```

次に、**show vpn-sessiondb detail anyconnect** コマンドの出力例を示します。

```
> show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : userab Index : 2
Assigned IP : 65.2.1.100 Public IP : 75.2.1.60
Assigned IPv6: 2001:1000::10
Protocol : IKEv2 IPsecOverNatT AnyConnect-Parent
License : AnyConnect Premium
Encryption : IKEv2: (1)3DES IPsecOverNatT: (1)3DES AnyConnect-Parent: (1)none
Hashing : IKEv2: (1)SHA1 IPsecOverNatT: (1)SHA1 AnyConnect-Parent: (1)none
Bytes Tx : 0 Bytes Rx : 21248
Pkts Tx : 0 Pkts Rx : 238
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy Tunnel Group : test1
Login Time : 22:44:59 EST Tue Aug 13 2017
```

```
Duration : 0h:02m:42s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 2.1
Public IP : 75.2.1.60
Encryption : none Hashing : none
Auth Mode : userPassword
Idle Time Out: 400 Minutes Idle TO Left : 397 Minutes
Conn Time Out: 500 Minutes Conn TO Left : 497 Minutes
Client OS : Windows
Client Type : AnyConnect
Client Ver : 3.1.05050

IKEv2:
Tunnel ID : 2.2
UDP Src Port : 64251 UDP Dst Port : 4500
Rem Auth Mode: userPassword
Loc Auth Mode: rsaCertificate
Encryption : 3DES Hashing : SHA1
Rekey Int (T): 86400 Seconds Rekey Left(T): 86241 Seconds
PRF : SHA1 D/H Group : 2
Filter Name : mixed1
Client OS : Windows

IPsecOverNatT:
Tunnel ID : 2.3
Local Addr : 75.2.1.23/255.255.255.255/47/0
Remote Addr : 75.2.1.60/255.255.255.255/47/0
Encryption : 3DES Hashing : SHA1
Encapsulation: Transport, GRE
Rekey Int (T): 28400 Seconds Rekey Left(T): 28241 Seconds
Idle Time Out: 400 Minutes Idle TO Left : 400 Minutes
Conn Time Out: 500 Minutes Conn TO Left : 497 Minutes
Bytes Tx : 0 Bytes Rx : 21326
Pkts Tx : 0 Pkts Rx : 239

NAC:
Reval Int (T): 0 Seconds Reval Left(T): 0 Seconds
SQ Int (T) : 0 Seconds EoU Age(T) : 165 Seconds
Hold Left (T): 0 Seconds Posture Token:
Redirect URL :
```

次に、**show vpn-sessiondb ra-ikev2-ipsec** コマンドの出力例を示します。

```
> show vpn-sessiondb detail ra-ikev2-ipsec

Session Type: Generic Remote-Access IKEv2 IPsec Detailed

Username : IKEV2TG Index : 1
Assigned IP : 95.0.225.200 Public IP : 85.0.224.12
Protocol : IKEv2 IPsec
License : AnyConnect Essentials
Encryption : IKEv2: (1)3DES IPsec: (1)AES256
Hashing : IKEv2: (1)SHA1 IPsec: (1)SHA1
Bytes Tx : 0 Bytes Rx : 17844
```

```
Pkts Tx : 0 Pkts Rx : 230
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GroupPolicy_IKEV2TG Tunnel Group : IKEV2TG
Login Time : 11:39:54 UTC Tue May 6 2017
Duration : 0h:03m:17s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 5f00e105000010005368ca0a
Security Grp : none

IKEv2 Tunnels: 1
IPsec Tunnels: 1
```

次に、**show vpn-sessiondb anyconnect** コマンドの出力例を示します。

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : user1                  Index        : 19576
Assigned IP  : 192.168.3.243          Public IP    : 192.168.10.61
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel:
(1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 15060                  Bytes Rx     : 20631
Group Policy : DfltGrpPolicy          Tunnel Group : Ad_group
Login Time   : 09:24:53 UTC Fri Apr 7 2017
Duration     : 0h:03m:20s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a8013804c7800058e75ae5
Security Grp : none                   Tunnel Zone  : 0
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear vpn-sessiondb statistics** | VPN セッション統計をクリアします。 |
| **show vpn-sessiondb ratio** | VPN セッションの暗号化またはプロトコルの比率を表示します。 |
| **show vpn-sessiondb summary** | 現在のセッションの総数、各タイプの現在のセッション数、最大累積セッション数、合計累積セッション数、最大同時セッション数など、セッションのサマリーを表示します。 |

# show vpn-sessiondb ratio

現在のセッションについて、プロトコルごと、または暗号化アルゴリズムごとの比率をパーセンテージで表示するには、**show vpn-sessiondb ratio** コマンドを使用します。

**show vpn-sessiondb ratio** {**encryption** | **protocol**} [**filter** *groupname* ]

## 構文の説明

| | |
|---|---|
| **encryption** | 各暗号化方式を使用しているセッションの数とセッションの割合を表示します。 |
| **protocol** | 各 VPN プロトコルを使用しているセッションの数とセッションの割合を表示します。 |
| **filter** *groupname* | （オプション）出力をフィルタリングして、指定するトンネルグループについてのみセッションの比率を表示します。 |

## 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、暗号化に基づくセッションの比率を表示する例を示します。

```
> show vpn-sessiondb ratio encryption

Filter Group         : All
Total Active Sessions: 5
Cumulative Sessions  : 9
Encryption               Tunnels        Percent
none                     0                0%
DES                      0                0%
3DES                     0                0%
RC4                      0                0%
AES128                   4               80%
AES192                   1               20%
AES256                   0                0%
AES-GCM-128              0                0%
AES-GCM-192              0                0%
AES-GCM-256              0                0%
AES-GMAC-128             0                0%
AES-GMAC-192             0                0%
AES-GMAC-256             0                0%
```

次に、プロトコルに基づくセッションの比率を表示する例を示します。

```
> show vpn-sessiondb ratio protocol

Filter Group         : All
Total Active Tunnels : 3
Cumulative Tunnels   : 42
```

```
Protocol                Tunnels         Percent
IKEv1                   0                 0%
IKEv2                   0                 0%
IPsec                   0                 0%
IPsecLAN2LAN            0                 0%
IPsecLAN2LANOverNatT    0                 0%
IPsecOverNatT           0                 0%
IPsecOverTCP            0                 0%
IPsecOverUDP            0                 0%
L2TPOverIPsec           0                 0%
L2TPOverIPsecOverNatT   0                 0%
Clientless              0                 0%
Port-Forwarding         0                 0%
IMAP4S                  0                 0%
POP3S                   0                 0%
SMTPS                   0                 0%
AnyConnect-Parent       1                33%
SSL-Tunnel              1                33%
DTLS-Tunnel             1                33%
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show vpn-sessiondb** | VPN セッションに関する情報を表示します。 |
| **show vpn-sessiondb summary** | 現在のセッションの総数、各タイプの現在のセッション数、最大累積セッション数、合計累積セッション数、最大同時セッション数など、セッションのサマリーを表示します。 |

# show vpn-sessiondb summary

アクティブセッションの数の概要を表示するには、**show vpn-sessiondb summary** コマンドを使用します。

**show vpn-sessiondb summary**

## 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

次の表に、Active Sessions サマリーおよび Session Information サマリーに含まれるフィールドの説明を示します。

| フィールド | 説明 |
|---|---|
| Concurrent Limit | このシステムで許可された、同時にアクティブにできるセッションの最大数。 |
| Cumulative Sessions | システムが最後に起動またはリセットされたとき以降の全タイプのセッション数。 |
| LAN-to-LAN | 現在アクティブな IPsec LAN-to-LAN セッションの数。 |
| Peak Concurrent | システムが最後に起動またはリセットされたとき以降に同時にアクティブだった、全タイプのセッションの最大数。 |
| Percent Session Load | 使用中の VPN セッション割り当てのパーセンテージ。この値は、Total Active Sessions を利用可能なセッションの最大数で除算した値に等しく、パーセンテージで表示されます。 |
| リモートアクセス | ra-ikev1-ipsec：現在アクティブな IKEv1 IPsec リモートアクセスユーザー、L2TP over IPsec、および IPsec through NAT セッションの数。 |
| Total Active Sessions | 現在アクティブな全タイプのセッションの数。 |

### 例

次に、**show vpn-sessiondb summary** コマンドの出力例を示します。

```
> show vpn-sessiondb summary
-------------------------------------------------------------------------
VPN Session Summary
-------------------------------------------------------------------------
Active : Cumulative : Peak Concur : Inactive
-----------------------------------------
OSPFv3 IPsec : 1 : 1 : 1
-------------------------------------------------------------------------
```

```
Total Active and Inactive : 1 Total Cumulative : 1
Device Total VPN Capacity : 10000
Device Load : 0%
------------------------------------------------------------------------
```

次に、一般的な IKEv2 IPsec リモートアクセスセッションに関する **show vpn-sessiondb summary** コマンドの出力例を示します。

```
> show vpn-sessiondb summary
------------------------------------------------------------------------
VPN Session Summary
------------------------------------------------------------------------
Active : Cumulative : Peak Concur : Inactive
----------------------------------------------
Generic IKEv2 Remote Access : 1 : 1 : 1
------------------------------------------------------------------------
Total Active and Inactive : 1 Total Cumulative : 1
Device Total VPN Capacity : 250
Device Load : 0%
------------------------------------------------------------------------

------------------------------------------------------------------------
Tunnels Summary
------------------------------------------------------------------------
Active : Cumulative : Peak Concurrent
----------------------------------------------
IKEv2 : 1 : 1 : 1
IPsec : 1 : 1 : 1
------------------------------------------------------------------------
Totals : 2 : 2
------------------------------------------------------------------------
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show vpn-sessiondb** | VPN セッションに関する情報を表示します。 |
| **show vpn-sessiondb ratio** | VPN セッションの暗号化またはプロトコルの比率を表示します。 |

# show vrf

システムで定義されている仮想ルータの情報を表示するには、**show vrf** コマンドを使用します。

**show vrf** ［**counters** | **lock**］

## 構文の説明

| | |
|---|---|
| **counters** | （任意）このシステムで許可されるユーザー定義の仮想ルータの最大数と、設定されている実際の仮想ルータの数を表示します。最大数 doc にはグローバル仮想ルータは含まれません。たとえば、最大数が 4 の場合、上限の合計は 5 となります。 |
| **lock** | （任意）VRF ロック情報を表示します。 |

## コマンド デフォルト

キーワードを指定しないと、現在の仮想ルータと各仮想ルータに割り当てられているインターフェイスが表示されます。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.6 | このコマンドが導入されました。 |

## 使用上のガイドライン

Virtual Route Forwarding（VRF）を有効にした場合は、**show vrf** コマンドを使用して、システムで定義された仮想ルータに関する基本情報を表示します。各仮想ルータのルーティングテーブルを表示するには、IPv4 ルーティングテーブルでは **show route vrf** *name* コマンドを使用し、IPv6 ルーティングテーブルでは **show ipv6 route vrf** *name* を使用します。

### 例

次に、仮想ルータと各ルータに割り当てられたインターフェイスを表示する例を示します。

```
> show vrf

Name            VRF ID          Description             Interfaces
vrf1            1                                       inside
                                                        inside_2
vrf2            2                                       inside_3
                                                        inside_4
```

次の例は、このシステムで許可される仮想ルータの最大数と、仮想ルータの現在の数を示しています。仮想ルータが IPv4、IPv6、またはその両方であるかどうかは、各仮想ルータ内のインターフェイスに割り当てる IP アドレスによって異なります。最大数はユーザー定義の仮想ルータを指すことに注意してください。この例では、VMware システムの場合、許容される上限の合計は 15 です（グローバル仮想ルータが 1 つ、ユーザー定義ルータが 14）。

```
> show vrf counters
Maximum number of VRFs supported: 14
Maximum number of IPv4 VRFs supported: 14
Maximum number of IPv6 VRFs supported: 14
Current number of VRFs: 2
Current number of VRFs in delete state: 0
```

次に、VRF ロック情報の例を示します。

```
> show vrf lock

VRF Name: single_vf; VRF id = 0 (0x0)
VRF lock count: 1
VRF Name: vrf1; VRF id = 1 (0x1)
VRF lock count: 2
VRF Name: vrf2; VRF id = 2 (0x2)
VRF lock count: 2
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show ipv6 route** | IPv6 ルーティングテーブルを表示します。 |
| **show route** | IPv4 ルーティングテーブルを表示します。 |

# show wccp

Web Cache Communication Protocol（WCCP）に関連するグローバル統計情報を表示するには、**show wccp** コマンドを使用します。

**show wccp** {**web-cache** | *service_number*} [**buckets** | **detail** | **service** | **view** | **hash** *dest_addr source_addr dest_port source_port*]
**show wccp** [**interfaces** [**detail**]]

## 構文の説明

| | |
|---|---|
| **buckets** | （オプション）サービスグループのバケット割り当て情報を表示します。 |
| **detail** | （任意）ルータおよびすべての Web キャッシュに関する情報を表示します。 |
| **hash** *dest_addr source_addr dest_port source_port* | （オプション）指定された接続の WCCP ハッシュを表示します。<br>• *dest_addr* は宛先ホストの IP アドレスです。<br>• *source_addr* は送信元ホストの IP アドレスです。<br>• *dest_port* は宛先ホストのポートです。<br>• *source_port* は送信元ホストのポートです。 |
| **interfaces** [**detail**] | （オプション）WCCP リダイレクトインターフェイスを表示します。インターフェイス コンフィギュレーションの detail キーワードが含まれます。 |
| **service** | （オプション）サービスグループの定義情報を表示します。 |
| *service-number* | キャッシュが制御する Web キャッシュサービスグループの ID 番号。番号は、0 ～ 254 です。Cisco Cache Engine を使用する Web キャッシュの場合、逆プロキシ サービスの値には 99 を指定します。 |
| **view** | （オプション）特定のサービスグループの他のメンバーが検出されたかどうかを表示します。 |
| **web-cache** | Web キャッシュ サービスの統計情報を指定します。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.2 | このコマンドが導入されました。 |

### 例

次に、WCCP 情報を表示する例を示します。

```
> show wccp
Global WCCP information:
    Router information:
        Router Identifier:                   -not yet determined-
        Protocol Version:                    2.0
    Service Identifier: web-cache
        Number of Cache Engines:             0
        Number of routers:                   0
        Total Packets Redirected:            0
        Redirect access-list:                foo
        Total Connections Denied Redirect:   0
        Total Packets Unassigned:            0
        Group access-list:                   foobar
        Total Messages Denied to Group:      0
        Total Authentication failures:       0
        Total Bypassed Packets Received:     0
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear wccp** | WCCP 統計情報をクリアします。 |

# show webvpn

リモートアクセス VPN に関する情報を表示するには、**show webvpn** コマンドを使用します。

**show webvpn** {**anyconnect** | **debug-condition** | **group-alias** [*tunnel_group*] | **group-url** [*tunnel_group*] | **statistics**}

## 構文の説明

| | |
|---|---|
| **anyconnect** | クライアントエンドポイントにダウンロード可能な AnyConnect イメージに関する情報を表示します。 |
| **debug-condition** | **debug webvpn condition** コマンドによって設定されている現在のデバッグ条件を表示します。 |
| **group-alias** [*tunnel_group*] | トンネルグループ（接続プロファイル）のエイリアスを表示します。オプションとして、トンネルグループの名前を指定し、指定したグループに関する情報のみを表示することもできます。各グループには複数のエイリアスがあることも、エイリアスがまったくないこともあります。 |
| **group-url** [*tunnel_group*] | トンネルグループ（接続プロファイル）の URL を表示します。オプションとして、トンネルグループの名前を指定し、指定したグループに関する情報のみを表示することもできます。各グループには複数の URL があることも、URL がまったくないこともあります。 |
| **statistics** | WebVPN イベントに関するデータを表示します。 |

## 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。 |
| 7.1 | 外部ブラウザパケットに関する情報が AnyConnect の出力に追加されました。 |

### 例

**show webvpn anyconnect** コマンドの出力例を次に示します。

```
> show webvpn anyconnect
1. disk0:/csm/anyconnect-win-4.2.06014-k9.pkg 1 cfg-regex=/Windows/
  CISCO STC win2k+
  4,2,06014
  Hostscan Version 4.2.06014
  Thu 10/06/2016 14:40:31.34

1 AnyConnect Client(s) installed
```

次に、SAML 認証で使用されている場合は、外部ブラウザパッケージが含まれている **show webvpn anyconnect** の例を示します。

```
> show webvpn anyconnect
1. disk0:/anyconnpkgs/anyconnect-win-4.10.01075-webdeploy-k9.pkg 2 dyn-regex=/Windows
NT/
  CISCO STC win2k+
  4,10,01075
  Hostscan Version 4.10.01075
  Wed 04/28/2021 12:36:03.98

1 AnyConnect Client(s) installed

2. disk0:/externalbrowserpkgs/external-sso-98.161.00015-webdeploy-k9.pkg
  Cisco AnyConnect External Browser Headend Package
  98.161.00015
  Wed 05/05/21 15:49:27.817381
```

**show webvpn debug-condition** コマンドの出力例を次に示します。

```
> show webvpn debug-condition
INFO: Webvpn conditional debug is turned ON
INFO: IP address filters:
INFO: 10.100.10.10/32
```

**show webvpn group-alias** コマンドの出力例を次に示します。

```
> show webvpn group-alias
Tunnel Group: Ad_group   Group Alias: ad_group enabled
Tunnel Group: Radius_group   Group Alias: Radius_group enabled
Tunnel Group: Cert_auth   Group Alias: cert_auth enabled
```

**show webvpn group-url** コマンドの出力例を次に示します。

```
> show webvpn group-url
http://www.cisco.com
https://ger1.example.com
https://ger2.example.com
```

**show webvpn statistics** コマンドの出力例を次に示します。

```
> show webvpn statistics
Total number of objects served  0
 html                           0
 js                             0
 css                            0
 vb                             0
 java archive                   0
 java class                     0
 image                          0
 undetermined                   0
Server compression statistics
 Decompression success from server                  0
 Unsolicited compression from server                0
 Unsupported compression algorithm used by server   0
 Decompression failure for server responses         0
IOBuf failure statistics
```

```
uib_create_with_channel                          0
uib_create_with_string                           0
uib_create_with_string_and_channel               0
uib_transfer                                     0
uib_add_filter                                   0
uib_yyread                                       0
uib_read                                         0
uib_set_buffer_max                               0
uib_set_eof_symbol                               0
uib_get_capture_handle                           0
uib_set_capture_handle                           0
uib_buflen                                       0
uib_bufptr                                       0
uib_buf_endptr                                   0
uib_get_buf_offset                               0
uib_get_buf_offset_addr                          0
uib_get_nth_char                                 0
uib_consume                                      0
uib_advance_bufptr                               0
uib_eof                                          0
```

# show xlate

NAT セッション（xlates または変換）の情報を表示するには、**show xlate** コマンドを使用します。

**show xlate** ［**global** *ip1*［*-ip2*］［**netmask** *mask*］］［**local** *ip1*［*-ip2*］［**netmask** *mask*］］［**gport** *port1*［*-port2*］］［**lport** *port1*［*-port2*］］［**interface** *if_name*］［**type** *type*］
**show xlate count**

## 構文の説明

| | |
|---|---|
| **count** | 変換数を表示します。 |
| **global** *ip1*[*-ip2*] | （任意）アクティブな変換をマッピングされた IP アドレスまたはアドレスの範囲別に表示します。 |
| **gport** *port1*[*-port2*] | （任意）アクティブな変換をマッピングされたポートまたはポートの範囲別に表示します。 |
| **interface** *if_name* | （任意）アクティブな変換をインターフェイス別に表示します。 |
| **local** *ip1*[*-ip2*] | （任意）アクティブな変換を実際の IP アドレスまたはアドレスの範囲別に表示します。 |
| **lport** *port1*[*-port2*] | （任意）アクティブな変換を実際のポートまたはポートの範囲別に表示します。 |
| **netmask** *mask* | （任意）マッピングされた、または実際の IP アドレスを限定するネットワーク マスクを指定します。 |
| **type** *type* | （任意）アクティブな変換をタイプ別に表示します。次のタイプを 1 つ以上入力できます。<br>• **static**<br>• **portmap**<br>• **dynamic**<br>• **twice-nat**（別名、手動 NAT）<br>複数のタイプを指定する場合は、タイプをカンマで区切ります。 |

## 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

**show xlate** コマンドは、変換スロットの内容を表示します。xlate には、デバイスマネージャの NAT ルールテーブルに表示されない、内部インターフェイス用に生成されたものを含めることができます。これらは内部処理に必要です。

VPN クライアント コンフィギュレーションがイネーブルで、内部ホストが DNS 要求を送信している場合に **show xlate** コマンドを実行すると、1 つのスタティック変換に対応する複数の xlate が表示されることがあります。

クラスタリング環境では、PAT セッションを処理するために、最大 3 つの xlate が、クラスタ内の異なるノードに複製される可能性があります。1 つの xlate は、接続を所有するユニットで作成されます。1 つの xlate は、PAT アドレスをバックアップするために別のユニットで作成されます。最後の 1 つの xlate は、フローを複製するディレクタにあります。バックアップとディレクタが同じユニットである場合、3 つではなく 2 つの xlate が作成されることがあります。

### 例

次に、**show xlate** コマンドの出力例を示します。nlp_int_tap の初期 PAT xlate は、Device Manager が管理インターフェイスアドレスではなく 192.168.1.1 にアクセスできるようにする HTTPS アクセスルールに関連しています。これらは、デバイスマネージャの NAT テーブルにルールが表示されない内部 NAT xlate です。

```
> show xlate
13 in use, 14 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_2:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_3:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_4:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_5:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_6:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_7:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_8:0.0.0.0/0
    flags sIT idle 0:30:10 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_7:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_6:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_5:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_4:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_3:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_2:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
```

次に、IPv4 から IPv6 への変換を示す **show xlate** コマンドの出力例を示します。

```
> show xlate
14 in use, 14 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
```

```
(...other entries removed...)
NAT from outside:0.0.0.0/0 to inside1_8:2001:db8::/96
    flags s idle 0:01:36 timeout 0:00:00
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear xlate** | 現在の変換および接続情報をクリアします。 |
| **show conn** | すべてのアクティブ接続を表示します。 |
| **show local-host** | ローカル ホスト ネットワーク情報を表示します。 |

# show zone

トラフィックゾーン情報を表示するには、**show zone** コマンドを使用します。

**show zone** ［*name*］

## 構文の説明

| | |
|---|---|
| *name* | （オプション）トラフィックゾーンの名前。 |

## 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

トラフィックゾーンは、セキュリティゾーンとまったく同じではありません。パッシブセキュリティゾーンもトラフィックゾーンとして自動的に生成されますが、ルーテッドおよびスイッチ ドセキュリティ ゾーンは生成されません。トラフィックゾーンは、トラフィックのロードバランシング（等コストマルチパス（ECMP）ルーティングを使用）、ルートの冗長性、および複数のインターフェイス間での非対称ルーティングのために使用できます。

ゾーン設定の残りの部分を表示するには、**show running-config zone** および **show running-config interface** コマンドを使用します。

### 例

次に、設定されたトラフィックゾーンを表示する例を示します。この例では、トラフィックゾーンはパッシブインターフェイス用です。等コストマルチパスルーティングのゾーンの場合、ゾーンタイプは ecmp になります。インターフェイスの設定は次のとおりです。**zone-member** コマンドは、インターフェイスをゾーンのメンバーとして設定します。

```
> show zone passive-security-zone
Zone: passive-security-zone passive
    Security-level: 0
    Zone member(s): 1
      passive                       GigabitEthernet0/0

> show running-config interface gigabitethernet0/0
!
interface GigabitEthernet0/0
 mode passive
 nameif passive
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 zone-member krjones-passive-security-zone
```

関連コマンド

| Command | 説明 |
|---|---|
| **clear conn zone** | ゾーン接続をクリアします。 |
| **clear local-host zone** | ゾーンのホストをクリアします。 |
| **show interface** | インターフェイスの実行時ステータスと統計情報を表示します。 |
| **show local-host zone** | ゾーン内のローカル ホストのネットワーク状態を表示します。 |
| **show nameif zone** | インターフェイスのゾーンまたはインライン セット メンバーシップを表示します。 |

# shun

攻撃元ホストからの接続をブロックするには、**shun** コマンドを使用します。shun を無効にするには、このコマンドの **no** 形式を使用します。

**shun** *source_ip* ［*dest_ip source_port dest_port* ［*protocol*］］［**vlan** *vlan_id*］
**no shun** *source_ip* ［**vlan** *vlan_id*］

## 構文の説明

| | |
|---|---|
| *dest_port* | （任意）送信元 IP アドレスに shun を適用するときにドロップする現在の接続の宛先ポートを指定します。 |
| *dest_ip* | （任意）送信元 IP アドレスに shun を適用するときにドロップする現在の接続の宛先アドレスを指定します。 |
| *protocol* | （任意）送信元 IP アドレスに shun を適用するときにドロップする現在の接続の IP プロトコル（UDP や TCP など）を指定します。デフォルトでは、プロトコルは 0（すべてのプロトコル）です。 |
| *source_ip* | 攻撃元ホストのアドレスを指定します。送信元 IP アドレスのみを指定した場合、このアドレスからの今後のすべての接続はドロップされます。現在の接続はそのまま維持されます。現在の接続をドロップし、かつ shun を適用するには、その接続についての追加パラメータを指定します。その送信元 IP アドレスからの今後のすべての接続には、宛先パラメータに関係なく、shun がそのまま維持されます。 |
| *source_port* | （任意）送信元 IP アドレスに shun を適用するときにドロップする、現在の接続の送信元ポートを指定します。 |
| **vlan** *vlan_id* | （任意）送信元ホストが配置されている VLAN ID を指定します。 |

## コマンド デフォルト

デフォルトのプロトコルは 0（すべてのプロトコル）です。

## 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

**shun** コマンドを使用すると、攻撃元ホストからの接続をブロックできます。該当する送信元 IP アドレスからの今後の接続すべては、手動でブロッキング機能が削除されるまで、ドロップされ、ログに記録されます。**shun** コマンドのブロッキング機能は、指定したホストアドレスとの接続が現在アクティブかどうかに関係なく適用されます。

宛先アドレス、送信元ポート、宛先ポート、およびプロトコルを指定すると、一致する接続がドロップされ、かつ、その送信元 IP アドレスからの今後のすべての接続に shun が適用されます。この場合、これらの特定の接続パラメータと一致する接続だけでなく、今後のすべての接続が回避されます。

**shun** コマンドは、送信元 IP アドレスごとに 1 つのみ使用できます。

**shun** コマンドは攻撃をダイナミックにブロックするために使用されるため、脅威に対する防御 デバイス コンフィギュレーションには表示されません。

インターフェイス コンフィギュレーションが削除されると、そのインターフェイスに付加されているすべての shun も削除されます。

### 例

次に、攻撃ホスト（10.1.1.27）が攻撃対象（10.2.2.89）に TCP で接続する例を示します。この接続は、脅威に対する防御デバイスの接続テーブル内で次のように記載されています。

```
10.1.1.27, 555-> 10.2.2.89, 666 PROT TCP
```

次のオプションを使用して、**shun** コマンドを適用します。

```
> shun 10.1.1.27 10.2.2.89 555 666 tcp
Shun 10.1.1.27 added in context: single_vf
Shun 10.1.1.27 successful
```

このコマンドにより、現在の接続が脅威に対する防御デバイスの接続テーブルから削除され、10.1.1.27からの今後のすべてのパケットは脅威に対する防御デバイスを通過できなくなります。

## 関連コマンド

| Command | 説明 |
|---|---|
| **clear shun** | 現在イネーブルにされている回避をすべてディセーブルにし、回避統計をクリアします。 |
| **show conn** | すべてのアクティブな接続を表示します。 |
| **show shun** | 回避についての情報を表示します。 |

# shutdown

デバイスをシャットダウンするには、**shutdown** コマンドを使用します。

**shutdown**

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.0.1 | このコマンドが導入されました。 |

### 例

次に、デバイスをシャットダウンしたときの **shutdown** コマンドの出力例を示します。

```
> shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': YES
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **reboot** | デバイスをリブートします。 |

# system access-control clear-rule-counts

アクセスコントロールルールのヒット数を 0 にリセットするには、**system access-control clear-rule-counts** コマンドを使用します。

**system access-control clear-rule-counts**

## 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

**system access-control clear-rule-counts** コマンドの出力例を次に示します。

```
> system access-control clear-rule-counts
Are you sure that you want to clear the rule hit counters? (y/n): y
Clearing the rule hit counters.
Success.
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **show access-control-config** | nbr_router_id interface_name |

# system generate-troubleshoot

シスコテクニカルサポートで分析するためのトラブルシューティングデータの生成を要求された場合は、**system generate troubleshoot** コマンドを使用します。

**system generate-troubleshoot** *options*

## 構文の説明

| | |
|---|---|
| オプション | 生成するトラブルシューティングデータのタイプを表示します。1つ以上のオプションを入力できます。複数のオプションを区切るには、スペースを使用します。<br>• **ALL**：次のすべてのオプションを実行します。<br>• **SNT**：Snort のパフォーマンスと設定。<br>• **PER**：ハードウェアのパフォーマンスとログ。<br>• **SYS**：システム設定、ポリシー、およびログ。<br>• **DES**：検出設定、ポリシー、およびログ。<br>• **NET**：インターフェイスとネットワーク関連データ。<br>• **VDB**：検出、認知、VDB データ、およびログ。<br>• **UPG**：データとログのアップグレード。<br>• **DBO**：すべてのデータベースデータ。<br>• **LOG**：すべてのログデータ。<br>• **NMP**：ネットワークマップ情報。 |

## 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、Snort およびハードウェアパフォーマンスのトラブルシューティング データを生成する例を示します。

```
> system generate-troubleshoot SNT PER
Starting /usr/local/sf/bin/sf_troubleshoot.pl...
Please, be patient.  This may take several minutes.
the troubleshoot options codes specified are SNT,PER.
getting filenames from [/ngfw/usr/local/sf/etc/db_updates/index]
getting filenames from [/ngfw/usr/local/sf/etc/db_updates/base-6.2.0]
Troubleshooting information successfully created at /ngfw/var/common/results-10-14-201
6--181112.tar.gz
```

関連コマンド

| Command | 説明 |
| --- | --- |
| **copy** | システムとの間でファイルをコピーします。 |
| **delete** | システムからファイルを削除します。 |

# system lockdown-sensor

エキスパートモードおよび bash シェルへのアクセスを削除するには、**system lockdown-sensor** コマンドを使用します。

**system lockdown-sensor**

## 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

**注意** このコマンドを実行すると元に戻すことはできません。エキスパートモードへのアクセスを復元する必要がある場合は、Cisco Technical Assistance Center に連絡して、ホットフィックスを入手する必要があります。

**expert** コマンドは、システムの動作環境への広範なアクセス権を管理者ユーザーに付与する bash シェルへのアクセスを提供します。セキュリティ認定方式（コモンクライテリア（CC）や Unified Capabilities Approved Products List（UC APL）など）では、システムのユーザーが利用できるアクセス権と情報を制限する要件が課されています。これらの認証要件を満たすための **expert** コマンドへのアクセスを削除するには、**system lockdown-sensor** コマンドを使用します。

（注） このコマンドを使用した後も、**expert** コマンドは現在の SSH セッションで引き続き使用できます。ログアウトしてから再度ログインし、このコマンドが削除されて機能しなくなったことを確認する必要があります。このコマンドを使用した後にログインした他のユーザーは、エキスパートモードも使用できません。

### 例

次の例では、セキュリティ要件に準拠するためにエキスパートモードへのアクセスを削除します。

```
> system lockdown-sensor
This action will remove the 'expert' command from your system for all
future CLI sessions, rendering the bash shell inaccessible.

This cannot be reversed without a support call.
Continue and remove the 'expert' command?

Please enter 'YES' or 'NO': YES
>
```

# system support コマンド

ほとんどの system support コマンドは、Cisco Technical Assistance Center のサポートを受けて、デバッグおよびトラブルシューティングを行うために使用されます。各コマンドはシスコサポートの指示に従い使用する必要があります。ただし、次のコマンドは一般的な目的で使用されます。

- system support diagnostic-cli （1162 ページ）
- system support view-files （1168 ページ）
- system support ssl-hw- コマンド （1164 ページ）

# system support ssl-client-hello- コマンド

これらのコマンドを使用すると、Transport Layer Security（TLS）1.3 から TLS 1.2 へのダウングレードの動作を決定できます。管理対象デバイスは TLS 1.3 暗号化または復号化をサポートしていないため、クライアントとサーバー間の TLS 1.3 セッションが中断し、クライアント Web ブラウザで次のようなエラーが発生する可能性があります。

**ERR_SSL_PROTOCOL_ERROR**

**SEC_ERROR_BAD_SIGNATURE**

**ERR_SSL_VERSION_INTERFERENCE**

クライアントがサーバーに接続し、ダウングレードするように変更された接続が [Do Not Decrypt SSL] ルールアクションと一致すると TLS インスペクションが判断した場合、エラーが発生する可能性があります。

これらのコマンドは、Cisco TAC に相談してから使用することを推奨します。

**system support ssl-client-hello-enabled aggressive_tls13_downgrade** { **true** | **false** }

## 構文の説明

| | |
|---|---|
| **true** | これがデフォルトです。TLS 1.3 接続は、復号化の実行に必要な場合は常にダウングレードされます。ただし、ClientHello メッセージの後に受信したデータが原因でセッションが [Do Not Decrypt] ルールに一致した場合は、セッションが失敗する可能性があります。 |
| **false** | TLS 1.3 接続は、セッションが [Do Not Decrypt] ルールに一致しない合理的な確実性がある場合にのみダウングレードされます。場合によっては、復号化が必要な TLS 接続がダウングレードされないことがあります。このような場合、トラフィックは復号化されません。代わりに、[Undecryptable Action] の [Session not cached] 設定の SSL ポリシーで指定されたアクションが実行されます。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.2.3.7 | このコマンドが導入されました。 |

# system support diagnostic-cli

追加の show コマンドやその他のトラブルシューティング コマンドを含む診断 CLI を開始するには、**system support diagnostic-cli** コマンドを使用します。

**system support diagnostic-cli**

## 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

診断 CLI には、システムのトラブルシューティングに使用できる追加の show コマンドやその他のコマンドが含まれています。診断CLIのコマンドは、ASA ソフトウェアのコマンドです。通常の 脅威に対する防御 CLI には同じコマンドが多数含まれているため、診断 CLI の追加コマンドは不要な場合があります。

診断 CLI を開始すると、通常の 脅威に対する防御 CLI とは別のセッションが開始されます。

プロンプトが変更され、システムのホスト名が表示されます。2 つのモードがあり、プロンプトに現在のモードが示されます。ユーザー EXEC モードの場合、プロンプトは次のとおりです。

```
hostname>
```

特権 EXEC モード（別名 Enable モード）の場合、プロンプトは次のようになります。このモードは、enable コマンドを使用して開始します。パスワードの入力を求められたら、Enter を押します。デフォルトでは、このモードを開始するためにパスワードを入力する必要はありません。

```
hostname#
```

診断 CLI を使用する場合は、次のヒントに留意してください。

- 診断 CLI を終了して通常の CLI に戻るには、Ctrl+a を押してから d を押します。
- 特権 EXEC モードを終了するには、**exit** コマンドを使用します。

  使用できるコマンドはモードによって異なります。特権EXECモードには、ユーザーEXECモードよりもはるかに多くのコマンドが含まれています。使用可能なコマンドを表示するには、**?**を使用します。ASA ソフトウェアのコマンドリファレンスで使用法の情報を確認できます。

  - Cisco ASA シリーズ コマンド リファレンス、A ～ H コマンド。
    https://www.cisco.com/c/ja_jp/td/docs/security/asa/asa-command-reference/A-H/cmdref1.html
  - Cisco ASA シリーズ コマンド リファレンス、I ～ R コマンド。
    https://www.cisco.com/c/ja_jp/td/docs/security/asa/asa-command-reference/I-R/cmdref2.html

  - Cisco ASA シリーズ コマンド リファレンス、S コマンド。
    https://www.cisco.com/c/ja_jp/td/docs/security/asa/asa-command-reference/S/cmdref3.html
  - Cisco ASA シリーズ コマンド リファレンス、T ～ Z コマンド および ASASM 用 IOS コマンド。
    https://www.cisco.com/c/ja_jp/td/docs/security/asa/asa-command-reference/T-Z/cmdref4.html

- 診断 CLI には、脅威に対する防御 には意味のないコマンドが含まれていることがあります。コマンドを試しても意味のある（または何らかの）情報が表示されない場合、関連する機能が設定されていないか、または 脅威に対する防御 でサポートされていない可能性があります。
- 診断 CLI では、コンフィギュレーション モードを開始できません。CLI を使用してデバイスを設定することはできません。
- 診断 CLI から離れると、次に診断 CLI を開始した際には、最後に離れたときと同じモードになります。
- ASA 5506W-X では、**session wlan** コマンドを使用してワイヤレスモジュールへの接続を開き、その CLI を使用してアクセスポイントを設定できます。この場合、特権 EXEC モードである必要があります。

## 例

次に、診断 CLI および特権 EXEC モードを開始する例を示します。**enable** コマンドの入力後にパスワードプロンプトが表示されたら、Enter を押します。デフォルトでは、特権 EXEC モードを開始するためのパスワードはありません。

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> enable
Password: <press enter, do not enter a password>
firepower#
```

# system support ssl-hw- コマンド

これらのコマンドを使用すると、バージョン 6.2.3 および 6.3 では *TLS/SSL* ハードウェア アクセラレーション、またバージョン 6.4 では *TLS* 暗号化アクセラレーション と呼ばれる機能に対してさまざまな操作を実行できます。使用可能なキーワードは、脅威に対する防御 ソフトウェアのバージョンによって異なります。

サポートされるデバイス、および機能がデフォルトで有効か無効かは、ソフトウェアバージョンによっても異なります。詳細については、『*Management Center CLI Configuration Guide*』を参照してください。

バージョン 6.2.3 および 6.3 のシンタックス：

**system support** {**ssl-hw-status** | **ssl-hw-supported-ciphers** | **ssl-hw-offload enable** | **ssl-hw-offload disable**}

バージョン 6.4 のシンタックス：

**system support ssl-hw-supported-ciphers**

## 構文の説明

| | |
|---|---|
| **ssl-hw-status** | SSL ハードウェア アクセラレーションの現在のステータスを表示します。デフォルトの状態は次のとおりです。<br>• 6.2.3：無効<br>• 6.3 および 6.4：有効 |
| **ssl-hw-supported-ciphers** | SSL ハードウェア アクセラレーションでサポートされている暗号のリストを表示します。このコマンドは、SSL ソフトウェア アクセラレーションでサポートされているすべての暗号を SSL ハードウェア アクセラレーションがサポートしているわけではないので便利です（特に、SEED 暗号と Camellia 暗号の暗号解読はサポートされていません）。 |
| **ssl-hw-offload enable** | ハードウェア アクセラレーションを有効化します。デバイスを再起動するように求められます。 |
| **ssl-hw-offload disable** | SSL ハードウェア アクセラレーションを無効化します。デバイスを再起動するように求められます。 |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 6.4 | 機能名が TLS/SSL ハードウェア アクセラレーション から TLS 暗号化アクセラレーション に変更されました。<br>次のキーワードが削除されました。<br>**ssl-hw-offload enable**<br>**ssl-hw-offload disable**<br>**ssl-hw-status** |
| 6.3 | この機能は、デフォルトでイネーブルに設定されています。 |
| 6.2.3 | このコマンドが導入されました。この機能はデフォルトで無効に設定されています。 |

## 使用上のガイドライン

（注） このセクションで説明するコマンドのうち、バージョン 6.4 に適用されるのは **system support ssl-hw-offload-supported ciphers** のみです。

SSL ハードウェア アクセラレーションに関する情報を表示したり、機能を有効または無効にしたりするには、次のコマンドを使用します。

SSL ハードウェア アクセラレーションを有効にして、暗号化と暗号解読のパフォーマンスを向上させます。

サポートされていない機能を使用する場合、または SSL ポリシーを有効にした状態で予期しないトラフィックの中断が発生した場合は、SSL ハードウェア アクセラレーションを無効にします。

SSL ハードウェア アクセラレーションによってサポートされていない機能は、次のとおりです。

- Threat Defense コンテナインスタンス が有効になっている管理対象デバイス。
- インスペクション エンジンが接続を維持するように設定されていて、インスペクション エンジンが予期せず失敗した場合は、エンジンが再起動されるまで TLS/SSL トラフィックはドロップされます。

  この動作はによって制御されます、**configure snort preserve-connection {enable | disable}** コマンド。

現在のステータスを表示するには、**system support ssl-hw-status** コマンドを使用します。

SSL ハードウェア アクセラレーションでサポートされる暗号のリストを表示するには、**system support ssl-hw-supported-ciphers** コマンドを使用します。

### 例

SSL ハードウェア アクセラレーションの現在のステータスを表示する例を次に示します。

```
> system support ssl-hw-status
Hardware Offload configuration set to Disabled
```

デバイスをリブートするプロンプトを表示して、SSL ハードウェア アクセラレーションを有効にする例を次に示します。

```
If you enable SSL hardware acceleration, you cannot:
    1.    Decrypt passive or inline tap traffic.
    2.    Preserve Do Not Decrypt connections when the inspection engine restarts.
Continue? (y/n) [n]: y


Enabling or disabling SSL hardware acceleration reboots the system. Continue? (y/n) [n]:
 y

SSL hardware acceleration will be enabled on system boot.
```

デバイスをリブートする前に、上記のすべてを確認する必要があります。

SSL ハードウェア アクセラレーションでサポートされる暗号の一部を次に示します。

```
> system support ssl-hw-supported-ciphers
CID     Cipher Suite Name                                CH_mod Keep     Support Inline
 Support Passive
-------------------------------------------------------------------------------------------------------
0x0004  TLS_RSA_WITH_RC4_128_MD5                         Yes             Yes
 Yes
0x0005  TLS_RSA_WITH_RC4_128_SHA                         Yes             Yes
 Yes
0x0009  TLS_RSA_WITH_DES_CBC_SHA                         Yes             Yes
 Yes
0x000a  TLS_RSA_WITH_3DES_EDE_CBC_SHA                    Yes             Yes
 Yes
0x000c  TLS_DH_DSS_WITH_DES_CBC_SHA                      No              No
 No
0x000d  TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA                 No              No
 No
0x000f  TLS_DH_RSA_WITH_DES_CBC_SHA                      No              No
 No
0x0010  TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA                 No              No
 No
0x0012  TLS_DHE_DSS_WITH_DES_CBC_SHA                     No              No
 No
0x0013  TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA                No              No
 No
0x0015  TLS_DHE_RSA_WITH_DES_CBC_SHA                     Yes             Yes
 No
0x0016  TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA                Yes             Yes
 No
0x0018  TLS_DH_Anon_WITH_RC4_128_MD5                     No              Yes
 No
0x001a  TLS_DH_Anon_WITH_DES_CBC_SHA                     No              Yes
```

```
 No
0x001b  TLS_DH_Anon_WITH_3DES_EDE_CBC_SHA               No              Yes
 No
0x001e  TLS_KRB5_WITH_DES_CBC_SHA                       No              No
 No
0x001f  TLS_KRB5_WITH_3DES_EDE_CBC_SHA                  No              No
 No
0x0020  TLS_KRB5_WITH_RC4_128_SHA                       No              No
 No
0x0024  TLS_KRB5_WITH_RC4_128_MD5                       No              No
 No
0x002f  TLS_RSA_WITH_AES_128_CBC_SHA                    Yes             Yes
 Yes
0x0030  TLS_DH_DSS_WITH_AES_128_CBC_SHA                 No              No
 No
0x0031  TLS_DH_RSA_WITH_AES_128_CBC_SHA                 No              No
 No
… more
```

# system support view-files

Cisco Technical Assistance Center（TAC）とともに問題を解決する際に、システムログの内容を表示するには、**system support view-files** コマンドを使用します。

**system support view-files**

## 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

**system support view-files** コマンドは、システムログを開きます。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。

コマンドは、ログを選択するためのメニューを表示します。ウィザードに移動するには、次のコマンドを使用します。

- サブディレクトリに変更するには、ディレクトリの名前を入力して、Enter を押します。
- 表示するファイルを選択するには、プロンプトで **s** と入力します。その後、ファイル名の入力が求められます。完全な名前を入力する必要があります。大文字と小文字は区別されます。ファイルリストにはログのサイズが示されます。非常に大きいログを開く前には検討が必要な場合があります。
- 「--More--」が表示されたら Space キーを押してログエントリの次のページを表示します。次のログエントリのみを表示するには Enter を押します。ログの最後に到達すると、メインメニューに戻ります。「--More--」の行には、ログのサイズと表示した量が示されます。**ログのすべてのページを表示する必要がなく、ログを閉じて、コマンドを終了するには、Ctrl+C を使用します。**
- メニュー構造のレベルを 1 つ上がるには、**b** を入力します。

ログを開いたままにして、新しいメッセージが追加されたときに確認できるようにするには、**tail-logs** コマンドを使用します。

### 例

次に、ngfw.log ファイルを表示する例を示します。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。

```
> system support view-files

===View 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 15:38:03 Starting Cisco Firepower Threat Defense ...
2016-10-06 15:38:03 Found USB flash drive /dev/sdb
2016-10-06 15:38:03 Found hard drive(s):  /dev/sda

<remaining log truncated>
```

## 関連コマンド

| Command | 説明 |
|---|---|
| **tail-logs** | ログを開き、開いたままにします。 |

# 第 III 部

# T ～ Z コマンド

# 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**<br>**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。<br><br>**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。<br>• *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。<br>• *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。<br><br>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。<br><br>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。<br><br>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。<br><br>**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*<br>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。<br>• **disk0:**/[*path*/]*filename*<br>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。<br>• **disk1:**/[*path*/]*filename*<br>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。<br>• **flash:**/[*path*/]*filename*<br>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。<br>• **ftp:**//[*user*[**:***password*]**@**]*server*[: *port*]/[*path*/]*filename*[**;type=***xx*]<br>次のキーワードの 1 つを **type** として指定できます。<br>• **ap**：ASCII 受動モード<br>• **an**：ASCII 通常モード<br>• **ip**：（デフォルト）バイナリ受動モード<br>• **in**：バイナリ通常モード<br>• **http**[**s**]**:**//[*user*[:*password*] **@**]*server*[: *port*]/[*path*/]*filename*<br>• **tftp:**//[*user*[:*password*]@]*server*[: *port*]/[*path*/]*filename*[**;int=***interface_name*]<br>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。<br>• **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。<br>• **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。<br>• **ipsec** ：IKEv1 または IKEv2 を使用する IPsec セッション。<br>• **ipseclan2lan**：IPsec LAN-to-LAN セッション。<br>• **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。